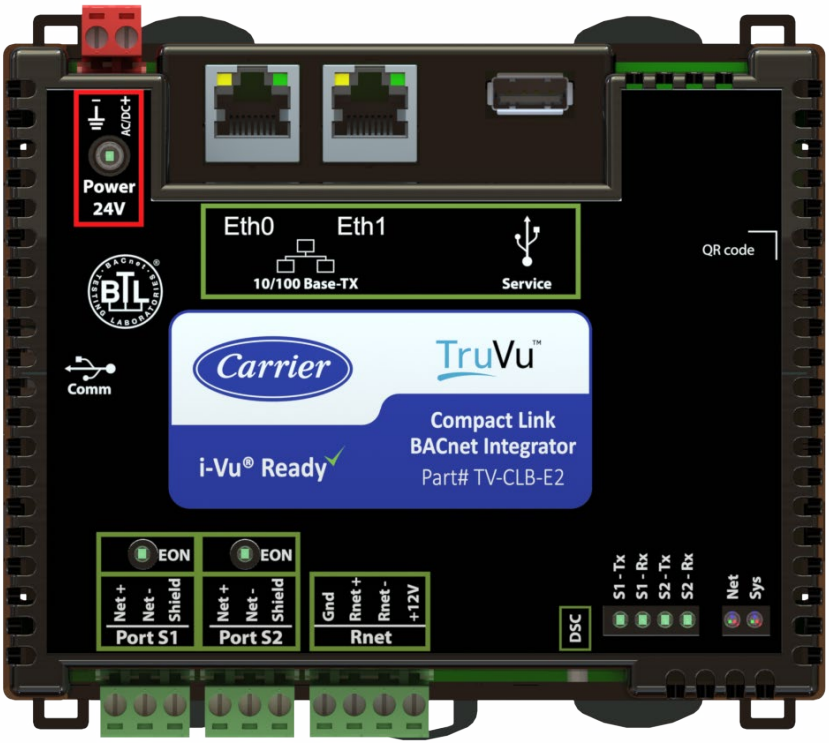
SNMP Integration Guide

For TruVu™ controllers (drv_gen5)



 • Catalog No. 11-808-1097-01 • 7/1/2025

Verify that you have the most current version of this document from **www.hvacpartners.com**, the **Carrier Partner Community** website, or your local Carrier office.

Important changes are listed in **Document revision history** at the end of this document.

Contents

Overview

You can use a Carrier TruVu™ controller to integrate SNMP device(s) with your i-Vu® system. The controller communicates via IP with the SNMP devices on your network to read and write SNMP points and receive SNMP traps.

The SNMP PPD delivers the following features:

- Support for legacy versions SNMPv1 and SNMPv2c
- Support for SNMPv3 with enhanced security
- Process traps as events
- Capture data from traps

Carrier	
Controllers	TruVu™ gateways
Driver	drv_gen5_108-04-20088.driverx or later
Read/write capability	Can read from and write to the third-party equipment
Ports	Gig-E
Third party	
Supported equipment	Any device that supports version SNMP protocol
Network media type	Ethernet
Quantity of devices you can physically connect to the Carrier controller	Up to 100

Before-you-begin checklist

You need the following items, information, and skills for the integration process:

- ☐ A points list for each SNMP device that includes the MIB variables of interest and read/write capabilities. Points lists are usually available from the third-party manufacturer's representative or website. You can also use a tool like SNMPb or SNMPWalk to identify the points available on your devices.
- ☐ A list of SNMP traps, including the actual trap data of interest, to be captured by the Carrier controller
- ☐ The IP addresses, Request Port, Trap Port, and community strings for each SNMP device
- ☐ Verification that all communication properties have been set on the SNMP devices
- ☐ Verification of Ethernet communications with the SNMP devices to which the control module connects
- ☐ Experience creating control programs in the Snap application
- ☐ Experience installing, wiring, setting up, and downloading to the Carrier controller

The integration process

Follow the steps in this document to integrate up to 100 SNMP agent devices into a i-Vu® system using the Carrier controller. To install and network the Carrier controller, see the controller's *Installation and Start-up Guide*.

1 Create a control program in the Snap application

When you create your control program, use Network Input microblocks to read object values from an SNMP agent and Network Output microblocks to write values to objects in an SNMP agent. The microblock address for each SNMP point must specify an **Agent Index** and a specific object's unique SNMP Object Identifier (OID).

To...	This network point type...	Use this microblock...
Read	Analog	ANI
		ANI2
	Binary	BNI
		BNI2
Write	Analog	ANO
		ANO2
	Binary	BNO
		BNO2

Formatting an SNMP address

Use the information below to format a valid address in each microblock that you use to read or write to a third-party point.

CAUTION
When integrating third-party devices into the i-Vu® system, most communication problems are caused by incorrect data or typing errors in the microblock's **Address** field.

TIP SNMP object identifiers (OIDs) can be lengthy. Also, there may be OIDs or OID fragments that you use often. You can configure OID shortcuts to use in your microblock address URLs that represent full OIDs or OID fragments. See the *OID Shortcuts table*.

Gather agent information

1. Create a table in Excel with the following columns: SNMP Device, Agent Index, IP Address, Request Port, Version, Profile Name, Context Engine ID, Context Name
2. List each SNMP device under the SNMP Device column.
3. Assign an **Agent Index** number to each agent. The **Agent Index** numbers will be used in the microblock address URLs to identify the devices.
4. Fill out the other columns as appropriate for each device, leaving the Profile Name column blank for now.
5. Save the file for future reference. You will configure this information into the controller after downloading the driver and connecting to the controller. See *Set up the SNMP driver properties* (page 11).

Read point

The addressing syntax for an SNMP read point is snmp://Agent_Index/Object_OID.

The Agent_Index specifies the location of the agent information in the Agent Index table.

EXAMPLE The address string snmp://1/1.3.6.1.2.1.1.3.0 used with a Network Input microblock allows us to read the OID 1.3.6.1.2.1.1.3.0 (SNMPv2-MIB::sysUpTimeInstance) from a third-party device configured in the first entry of the Agent Index Table.

Write point

The addressing syntax for an SNMP write point is the same as a read point, but allows for an optional format descriptor to specify the datatype of the object: snmp://Agent_Index/Object_OID/<fdescriptor>.

Format Descriptor

- Supported SNMP v1 datatypes are INTEGER, COUNTER, GAUGE, and TIMETICKS. See table below.
- Supported SNMP v2c and v3 datatypes are INTEGER32, COUNTER32, GAUGE32, UNSIGNED32 and TIMETICKS. See table below.

Format Descriptor	SNMP Data Format
/fI or /fi	INTEGER (default) or INTEGER32
/fC or /fc	COUNTER and COUNTER32
/fG or /fg	GAUGE, GAUGE32, and UNSIGNED32
/fT or /ft	TIMETICKS

NOTES

- If the write point's address does not include a format descriptor, the datatype will default to INTEGER for v1 and INTEGER32 for v2c and v3.
- The format descriptor in the address must match the datatype defined in the target object's MIB definition, otherwise the write request will fail.
- The floating point value of the Network Output microblock will be converted to the specified datatype before being sent in a SET request.

Capturing SNMP traps

v1 traps

Use Network Input microblocks to capture SNMP trap data from an SNMP agent. The address string includes a "t" or "t1" to indicate that it is a version 1 trap point.

EXAMPLES:

- snmp://t/Agent_Index/Enterprise_OID/Generic_Type/Specific_Type
- snmp://t1/Agent_Index/Enterprise_OID/Generic_Type/Specific_Type

NOTES:

- For Generic_Type 0-5 (ColdStart, WarmStart, LinkDown, LinkUp, AuthenticationFailure, or egpNeighborLoss), use Specific_Type 0.
- Append /r to the end of the trap's microblock address to set the value to zero when the refresh timer expires. If the /r suffix is not appended, then the trap point value persists until a new value comes in or the module is reset.

The remainder of the address syntax differs depending on the trap information needed. At a minimum, the address must specify the **Agent Index** (from the Agent Index table) to identify the device sending the trap, the trap's Enterprise OID, and the trap's Generic and Specific trap types. The microblock address may also specify a variable binding index or a variable binding index/OID combination. The various trap addressing methods are discussed below.

- **Capture Trap Type**

  To capture the receipt of a certain trap type, use a Network Analog Input or Network Binary Input microblock with the following address format:

  snmp://t/Agent_Index/Enterprise_OID/Generic_Type/Specific_Type

  When a trap is received that matches the point's agent IP address, Enterprise OID, and Generic and Specific types, the trap point is assigned the value 1.

- **Capture Numeric Variable**

  To capture the value of a variable contained in the variable bindings of a trap message, use a Network Analog Input microblock with the following address format:

  snmp://t/Agent_Index/Enterprise_OID/Generic_Type/Specific_Type/VarIndex

  A trap message can contain multiple variables in its variable binding list. VarIndex indicates the position of the variable in the variable binding list. When a trap is received that matches the point's agent IP address, Enterprise OID, and Generic and Specific types, the trap point is assigned the value of the indicated variable. For example, if VarIndex is 3, the trap point is assigned the value of the third variable in the trap's variable binding list.

  NOTE The value must be represented by a numeric datatype, for example: INTEGER, COUNTER, GAUGE, or TIMETICKS. This addressing method does not support capture of OCTET STRING or OBJECT IDENTIFIER datatypes.

- **Capture Object Identifier Fragment**

  A trap may contain non-integer values in its variable binding list, including OBJECT IDENTIFIERS (OIDs). To capture the last number in an OID (.XXX) that indicates a particular trap type or well-known trap condition, use a Network Analog Input microblock with the following address format:

  snmp://t/Agent_Index/Enterprise_OID/Generic_Type/Specific_Type/VarIndex/OID_Value

  When a trap is received that matches the point's agent IP address, Enterprise OID, and Generic and Specific types, the variable located at VarIndex in the variable binding list is analyzed to see if it matches the OID_Value specified in the point's address or is an immediate child of that OID_Value. If so, the last number in the trap's object identifier is assigned to the trap point.

  EXAMPLE If a trap point's address specifies VarIndex 3 and OID_Value as either 1.2.3.4.5 or 1.2.3.4, then when a trap message is received with OID 1.2.3.4.5 in the 3rd position of the variable binding list, the value 5 (the last number in the received trap's OID) is assigned to the trap point.

- **Specific Activate/Specific Reset**

  Once a trap message has been "captured" by a trap point in the control program, it retains the value assigned when the trap was received and parsed. A second trap point can be placed in the control program with some logic to capture the corresponding Return-to-Normal trap message and clear or reset an alarm microblock associated with the trap condition. Alternatively, to allow a single network point to be used to first activate and then clear a trap/alarm condition, the following "Specific Activate/Specific Reset" trap syntax can be used instead of a single Specific_Type:

  snmp://t/Agent_Index/Enterprise_OID/Generic_Type/saXXX/srYYY

  snmp://t/Agent_Index/Enterprise_OID/Generic_Type/saXXX/srYYY/VarIndex*

  snmp://t/Agent_Index/Enterprise_OID/Generic_Type/saXXX/srYYY/VarIndex/OID_Value*

  * These two address formats are not available in the Beta driver. They will be available in the released driver.

  EXAMPLE You can use a single Binary Network Input microblock with address snmp://t/2/1.3.6.1.4.1.13045.1.1/6/sa104/sr105 to capture two trap messages from a third-party controller (Agent Index #2). The trap message with specific type 104 is captured when the device sends a "Sensor in Low Critical State" trap message, and the binary point is activated since its address contains "/sa104". If the agent sends a trap message when the sensor state returns to normal (105), the binary point will be reset/deactivated since its address contains "/sr105." If an analog network input point had been used instead, the point's value would have been set to 1.0 (On) and then 0.0 (Off).

v2c/v3 traps

Use Network Input microblocks to capture SNMP trap data from an SNMP agent. The address string includes a "t2" to indicate that it is a version 2+ trap point.

For example, snmp://t2/Agent_Index/Enterprise_OID

Append /r to the end of the trap's microblock address to set the value to zero when the refresh timer expires. If the /r suffix is not appended, then all the trap values persist until a new value comes in or the module is reset.

v2c and v3 Traps are completely identified by their OID without the need to specify a Generic or Specific Trap type.

The remainder of the address syntax differs depending on the trap information needed. At a minimum, the address must specify the **Agent Index** (from the Agent Index Table) to identify who is sending the trap and the trap's Enterprise OID. The microblock address may also specify a variable binding or a variable binding/OID combination. The various trap addressing methods are discussed below.

- **Capture trap from Enterprise OID**

  To capture a trap received from a specific Enterprise OID, use a Network Analog Input or Network Binary Input microblock with the following address format:

  snmp://t2/Agent_Index/Enterprise_OID

  The trap point will be assigned the value of 0 on startup and will change to 1 when a trap is received with the specified Agent IP address and Enterprise OID.

- **Capture numeric variable**

  To capture the value of a variable contained in the variable binding list of a trap message, use a Network Analog Input microblock with the following address format:

  snmp://t2/Agent_Index/Enterprise_OID /VarIndex

  A trap message can contain multiple variables in its variable binding list. VarIndex indicates the position of the variable in the variable binding list. The trap point will be assigned the value of the indicated variable. For example, if VarIndex is 3, the trap point will be assigned the value of the third variable in the trap's variable binding list. The first two **varBinds** for v2c/v3 traps are **sysuptime** and **snmpTrapOid**.

  NOTE The value must be represented by a numeric datatype, for example: INTEGER32, COUNTER32, GAUGE32, UNSIGNED32, or TIMETICKS. This addressing method does not support capture of OCTET STRING or OBJECT IDENTIFIER datatypes.

- **Capture Object Identifier fragment**

  NOTE This address format is not available in the Beta driver. It will be available in the released driver.

  A trap may contain non-integer values in its variable binding list, including OBJECT IDENTIFIERS (OIDs). To capture the last number in an OID (.XXX) that indicates a particular trap type or well-known trap condition, use a Network Analog Input microblock with the following address format:

  snmp://t2/Agent_Index/Enterprise_OID/VarIndex/OID_Value

  In this case, when a trap is received that matches the point's agent IP address and Enterprise OID, the variable located at VarIndex in the variable binding list is analyzed to see if it matches the OID_Value specified in the point's address or is an immediate child of that OID_Value. If so, the last number in the trap's object identifier is assigned to the trap point.

  EXAMPLE If a trap point's address specifies VarIndex 3 and OID_Value as either 1.2.3.4.5 or 1.2.3.4, then when a trap message is received with OID 1.2.3.4.5 in the 3rd position of the variable binding list, the value 5 (the last number in the received trap's OID) is assigned to the trap point.

Editing a microblock address

You can edit a microblock address in the following places:

- In Snap in the Property Editor
- In the i-Vu® interface on the microblock's **Properties** > **Details**
- In the i-Vu® interface on the control program's **Properties** > **Network Points**

2 Download the driver and control programs

The SNMP PPD is available with driver drv_gen5_108-04-20088.driverx. To get and download the latest driver, see the controller's *Installation and Start-up Guide*.

1. On SiteBuilder's **Geographic** tree, add equipment for each of your control programs.
2. Assign the equipment to the controller by dragging each equipment from the **Geographic** tree and dropping it on the controller in the **Network** tree.
3. Click 
4. In the i-Vu® interface, download control programs to the Carrier controller.

See the “Managing third-party points and feature licenses” section of the controller’s *Installation and Start-up Guide* for instructions on how to ensure you have adequate FlexPoints licensed for your integration.

3 Set up the SNMP driver properties

The driver properties can be configured in either the:

- Controller's Service Port setup pages - See *Appendix C* (page 23).

  Or

- i-Vu® driver page - Select the controller's driver on the i-Vu® **navigation** tree.

Protocols > SNMP tab

Select the **Enabled** toggle and then configure the following tables.

Trap Ports table

The one-column table contains a list of all the ports through which traps will be received from SNMP devices.

The default port for SNMP is 162.

TIP For best performance, define as few ports as possible in this table. Each open port uses additional processing resources.

Community Strings Profiles (v1/v2) table

A Community Strings is a cleartext authentication string, similar to a password, sent with SNMP messages to allow access. A Community String Profile contains a set of three Community Strings (read-only, read-write, and SNMP trap) that are used to validate communications with a v1 or v2c device.

Create a row in a table for each unique Community String Profile required by the integrated SNMP v1/v2c agents.

Field	Description
Profile Name	The name that will be used to associate this profile with v1 or v2c agents in the *Agent Index table*.
Read Community	The string used by associated devices to restrict incoming read requests. Default is "public".
Write Community	The string used by associated devices to restrict read-write requests. Default is "private"
Trap Community	The string that restricts incoming traps received from associated devices. Default is "public".

User Security Profiles (v3) table

A User Security Profile defines a set of credentials and authentication rules used to communicate with a v3 device.

Create a row in the table for each unique User Security Profile required by the integrated SNMP v3 agents.

Field	Description
Profile Name	The name that will be used to associate this profile with v3 agents in the *Agent Index table*.
User Name	The username associated with this profile.
Authentication Protocol	Select either **No Authentication** or an authentication protocol from the drop-down.
Authentication Passphrase	If an authentication protocol was selected, enter the required authentication password.
Privacy Protocol	Select either **No Privacy** or a privacy protocol from the drop-down. An authentication protocol must be in use in order to use a privacy protocol.
Privacy Passphrase	If a privacy protocol was selected, enter the required privacy password.

Agent Index table

Create a row in the table for each integrated SNMP agent. Up to 100 agents can be defined in this table.

TIP Now that you have your security profiles configured, you can complete the Profile Name column of your agent spreadsheet. See *Formatting an SNMP address* (page 4).

To add the devices to the Agent Index table:

1. Click the Agent Index table's **Add** button until you have enough rows in the table for all your devices.
2. Copy the columns from the spreadsheet that correspond to the fields listed below.
3. Paste the data into the Agent Index table.

Field	Description
Agent Index	The number by which the agent will be referred in the microblock address. It can be any number greater than zero.
IP Address	The IP address of the SNMP device**.**
Request Port	The port on the agent device that the controller sends the request messages to. Valid range: 1-65535. Default: 161.

Version	Select the version of the SNMP protocol used to communicate with the device. • v1 - Initial SNMP implementation • v2c - Improved performance, different message formats • v3 - Enhanced security including encryption of data packets
Profile Name	The profile name of the active SNMP security profile. • For v1/v2c agents, enter a **Profile Name** from the **Community String Profiles** table • For v3 agents, enter a **Profile Name** from the **User Security Profiles** table

v3 Context Configuration

If you are using the device's default context, the two Context fields can be left blank. These fields are unavailable unless **Version** is set to v3.

- **Context Engine ID -** When specifying a context, enter the Context Engine ID as a string of hex characters, or the Context Name string, or both; this field must match the device's context.
- **Context Name -** When specifying a context, this field must match the device's context.

OID Shortcuts table

	Description
Index	The code used to insert this OID, or OID fragment, into a microblock address. An entry in this field must have the format "sN" or "SN", where N is a number 1-100. It is referenced from a network point's address by "/sN" (or "/SN"). Example snmp://2/S1/S2/.30.1 where the OID shortcut with index s1 is 1.3.6.1 and the OID shortcut with index s2 is .2.1.1 and the resulting OID is the concatenation 1.3.6.1.2.1.1.30.1 **NOTES** ○ When using the index in a microblock address, the case of the 's' (or 'S') is ignored. E.g., An OID Shortcut with index 's3' can be used in an address as either '/s3' or '/S3'. ○ If an explicit OID fragment appears in the URL, it is expected to be the final part of the OID and cannot be followed by an OID shortcut. For example, "s5/.1.2.1.2/s10" is invalid because the explicit OID string ".1.2.1.2" is followed by an OID shortcut (/s10). The OID expression "s5/s6/.3.5.7.0" is valid because the explicit portion of the OID string (".3.5.7.0") appears last. ○ When adding a new row to this table using the controller's Service Port setup pages, the next available Index number is provided. When using the I-Vu® driver page, you must enter the desired number.
OID	String of numbers divided by periods that represents a complete OID, or a fragment of an OID, to be inserted into the OID portion of a microblock address.
Description	(Optional) MIB description of the OID or OID fragment.

Connections > Gig-E Port tab

In the **Protocols** section, open the **SNMP > Advanced** section to configure the following protocol properties:

Property	Description
Interpacket Delay	Number of milliseconds the controller waits between sending request packets to the SNMP device. Valid range: 0-1000. Default: 20.
Max Pending Packets	Maximum requests that the controller can have outstanding. Once this number is reached, no more requests are sent until either a previous request receives a response, or until timeout. Valid range: 1-50. Default: 5.
Max Points Per Request	The maximum number of points to include in a single Read request. Increasing this value may improve performance but could result in communication errors if it exceeds the device's capabilities. If this occurs, lower the value until communications are stable. Valid range: 1-1000. Default: 1.

Synchronize properties with the BAS

- If you used the controller's Service Port to configure the properties:
  - If the **Restart** button is displayed, click it to restart the controller.
  - On the i-Vu® **navigation** tree, select the controller and **Upload** parameters from the controller.
- If you used the controller's driver page on the i-Vu® **navigation** tree, select the controller and **Download** parameters to the controller.

4 Connect the controller to the third-party device

Use CAT5 or higher Ethernet cables to connect the controller and the SNMP devices to a hub or switch on your network. Maximum cable length: 328 feet (100 meters).

1. Turn off the Carrier controller's power.
2. Check the communications wiring for shorts and grounds.
3. Wire the Carrier controller's Gig-E port to the network.

NOTE The Gig-E port will still be capable of BACnet communication.

4. Turn on the Carrier controller's power.
5. See the SNMP devices' Installation and Start-up Guide to connect them to the network.

5 Verify the integration is set up correctly

1 On the i-Vu® **navigation** tree, select the control program for the Carrier controller.

2 Select the **Properties** page > **Network Points** tab.

IF...	Then...
You see the point value you expect with no errors in the **Error** column	You have successfully established communication with the third-party device.
All points show question marks instead of values	The i-Vu® application is not communicating with the Carrier controller or the control program. Troubleshoot the controller's communications. See the controller's *Installation and Start-up Guide*.
Error message appears	Do one of the following actions based on the code/description in the **Error** column. • **Communications Disabled for this Microblock** - On the microblock's **Properties** page> **Details** tab, or on the **Network Points** tab, enable the microblock's **Comm Enabled** field. • **No protocol support** - Verify the **Address** in the microblock has the correct prefix: snmp:// • **Unlicensed Point** - You have configured more integration points than are licensed for this controller. See the "Managing third-party points and feature licenses" section of the controller's *Installation and Start-up Guide* for instructions on how to ensure you have adequate FlexPoints licensed for your integration. • All other errors -See *Appendix A* (page 19) for troubleshooting information for displayed error codes.
A value is incorrect	Verify that: • The **Address** in the microblock is correct. • The retrieved value is scaled properly, if necessary. For example, scaled from Celsius to Fahrenheit. Refer to the third-party manufacturer's documentation or the controller's *Installation and Start-up Guide* for scaling information.

If the above solutions do not resolve the problem, gather the following information for Technical Support:

- A diagnostic capture. See *To capture communication using Wireshark* (page 18).
- Screenshots of the driver configuration pages:
  - **Control Programs** tab
  - **Connections** > **Gig-E Port** tab, SNMP section
  - **Protocols** > **SNMP** tab
- Log files downloaded from the driver's **Advanced > Diagnostics** tab.
- A screenshot of the **Properties** page > **Network Points** tab showing addresses and errors.
- All information from a controller Modstat copied into a text file. Right-click the modstat, then select **Select All**. Press Ctrl + C to copy the information. Open Notepad and paste the copied information into a text file.
- Installation and Start-up Guide for the third-party device, if available.

To capture communication using Wireshark

Use Wireshark, a network analysis tool, to capture the Ethernet communication between the Carrier controller and the SNMP device.

PREREQUISITES

To use Wireshark to capture all Ethernet communication, provide one of the following devices:

- Ethernet hub (not a common switch)
- Port mirror on mirroring-capable switch
- Network sniffer/Test Access Port (TAP) such as SharkTap

1. Download the latest version of Wireshark from the Wireshark website (http://www.wireshark.org).
2. Run the Wireshark install program, accepting all defaults. Include WinPcap in the installation.
3. Place your capture device between the Carrier controller and the SNMP device by either:
   - Disconnecting the Carrier controller from the network and plugging its cable into the hub/TAP.

   or

   - Disconnecting the SNMP device from the network and plugging its cable into the hub/TAP.

   or

   - Configuring the mirroring port on your switch to mirror the port the Carrier controller is connected to.
4. Connect the Ethernet port of the computer running Wireshark to the hub/TAP/port mirror.
5. Identify the IP addresses of the controller and the SNMP device(s). These will be needed to decipher the capture.
6. On the computer, go to **Start > All Programs > Wireshark.**
7. From the menu bar, select **Capture > Interfaces.**
8. Click **Start** next to the interface that is connected to the network. This starts the IP capture.

   TIP Choose the interface that shows activity.
9. Allow the capture to run long enough to ensure that there is sufficient data to allow a technician to review the problem.
10. On the menu bar, select **Capture > Stop** to stop the data capture.
11. Apply the "SNMP" filter to Wireshark and verify that you have actually captured SNMP traffic.
12. Select **File > Save** and save the capture to a convenient location. Leave the **Save as type** default set to **Wireshark/tcpdump/... - libpcap (*.pcap, *.cap)**.
13. Send the file to Carrier Technical Support for analysis.

    TIP You can color code the information in the Wireshark capture file based on user-defined criteria. See *Wireshark's Help* for instructions on setting up Coloring Rules.

Appendix A - Error codes and messages

PPD error codes

The following SNMP features and commands are supported by the SNMP drivers.

Error Code/Message	Possible Causes/Solutions
	None; point is being read or written successfully.
1 - Comm Error - No Response	No response received from the SNMP device. This response could indicate that there is something wrong with the device itself or communication with the device. It can also indicate that something has been misconfigured on the **Protocols** > **SNMP** tab. Ensure that the **Agent Index** entry for this device and the associated **Community Strings** **Profiles** or **User Security Profile** have been configured with the correct values.
2 - Protocol Error - No Such Object	Response indicates that the requested object (OID) is not found in the SNMP device.
3 - Protocol Error - No Such Instance	Response indicates that the requested value is not found in the requested object (OID).
23 - Address Error - Invalid Trap Point	You must use a Network Input microblock to capture an SNMP trap. Replace the network output microblock with a network input microblock in the control logic and download to the module.
24 - Address Error - Invalid URL Syntax	The point's SNMP address did not parse correctly. Verify that the address syntax is correct for the point's type (Read, Write, or Trap). See *Formatting an SNMP address* (page 4) for details.
26 - Address Error – Invalid Agent Index	The Agent Index specified in this point's URL is invalid. Verify that the Agent Index (e.g. snmp://agent_index/...) exists in the *Agent Index table* on the **Protocols** > **SNMP** tab.

Error Code/Message	Possible Causes/Solutions
27 - Address Error – Missing or Invalid OID Expression	The SNMP MIB OID is either missing completely or is incorrectly formatted. An OID expression can be a literal string in the point address (e.g. 1.3.6.1...), a reference to an entry in the *OID Shortcuts table* (e.g. /s5), or a combination of both (e.g. s3/s4/.1.1.2.2.1.4.1). **NOTE** If an explicit OID fragment appears in the URL, it is expected to be the final part of the OID and cannot be followed by an OID shortcut. For example, "s5/.1.2.1.2/s10" is invalid because the explicit OID string ".1.2.1.2" is followed by an OID shortcut fragment (/s10). The OID expression "s5/s6/.3.5.7.0" is valid because the explicit portion of the OID string (.3.5.7.0) appears last.
28 - Address Error – Invalid OID Table Index	The index, 'N', specified in the point's OID expression "/sN" is invalid. It must be a valid entry in the *OID Shortcuts table*.
32 - Address Error – Invalid Generic Trap Value	The Generic trap value specified in this point's address must be a value between 0 and 6, inclusive. See *Capturing SNMP traps* (page 6).
33 - Address Error – Invalid Specific Trap Value	The Specific trap value specified in this point's address is invalid. If the point's Generic trap value is less than 6, the Specific trap value must be zero. If the Generic trap value is 6 (Enterprise-specific), the Specific trap value must be greater than zero. Refer to the SNMP device's MIB documentation for more details on the "specific" traps supported by the device. See *Capturing SNMP traps* (page 6).
34 - Address Error – Invalid Variable Binding Index	The trap point's variable binding index is zero. Refer to the SNMP device's SNMP documentation for more details on the variable bindings included in a particular trap message. The variable binding index should be greater than zero to identify which of the trap's multiple variable bindings is to be assigned to the trap point. See *Capturing SNMP traps* (page 6).
35 - Address Error – Unsupported Trap Version	The trap point's address specifies an invalid SNMP protocol version. The trap point's URL should begin with snmp://t/... or snmp://t1/... or snmp://t2/... See *Capturing SNMP traps* (page 6).
38 - Address Error – Reset Not Allowed	Only trap points can use the reset "/r " in the URL. See *Formatting an SNMP address* (page 4) for more details on the address syntax for read and write points.
46 – MIB Error – Unsupported Data Type	If this is a write point, the value's data format does not match the format descriptor in the address. See Write Point for more details. If this is a read point, the value it is trying to read is not an integer-based value, according to the information received in the response packet, and its value cannot be assigned to the point. Consult the SNMP device's MIB documentation for more information about the MIB data of interest.
47 - Invalid Data Received - Could Not Convert 's' To A Number	Unexpected value received from a configured trap. The microblock address indicates that a numeric value was expected, but a non-numeric value was received. Ensure that the microblock address contains the correct Enterprise OID and VarIndex (if applicable).

Error Code/Message	Possible Causes/Solutions
48 - Invalid Data Received - Value at VarIndex 'n' Is Not An OID - 's'	Unexpected value received from a configured trap. The microblock address indicates that an object identifier (OID) was expected, but the received value does not have the format of an OID. Ensure that the microblock address contains the correct Enterprise OID and VarIndex.
49 - Comm Error - Authentication Or Encryption Failure	The SNMP device could either not authenticate or decrypt the request. Verify that the User Security Profile assigned to the point's Agent Index has been configured correctly for the device.
50 - Comm Error - Not In Time Windows Failure	The SNMP device's EngineTime/EngineBootCnt has gotten out of sync with the controller. If retrying the request does not fix the issue, verify that the Context Engine ID and Context Name are correct in the Agent Index Table.

General error codes

Error Code/Message	Possible Causes/Solutions
Protocol Disabled or Unsupported	The protocol defined in the signature of the address is either unsupported by the controller or disabled. To enable a protocol that is available on the controller: 1. Select the controller's driver on the **Network** tree. 2. Click the **Protocols** tab and select the desired protocol tab (BACnet, Modbus, etc.) to enable. **NOTE** Enabling protocols requires a controller restart.
Initializing	This point is either: • In the process of being validated • Queued up for the initial read or write attempt to the third party device, • In the process of its initial read or write attempt to the third party device • Waiting for the initial response from the third party device. Once the startup process has completed, this error should switch to **No Error** or a different error that will identify any problems that may have occurred.".
No Error	The microblock is not in error. No solution needed.
Communications Disabled for this Microblock	The microblock's communications are not currently enabled. Enable the microblock's communications by checking the box under **Com Enable** in i-Vu®.

Error Code/Message	Possible Causes/Solutions
Not Linked	The microblock was not successfully linked to the object to which it is addressed. Ensure that the address is entered correctly and that the object the microblock is addressed to is functioning properly.
Programmer Error – Invalid MB State	The data integrity of the microblock was compromised. This is the default error code if none of the other errors apply. If this error is persistent, contact Technical Support to let them know there is a defect to address.
Undefined Client Microblock Error	An error occurred while the microblock was attempting to write a value. This is the default error code when something goes wrong trying to write a value over the network. If this error is persistent, contact Technical Support to let them know there is a defect to address.
Device Offline – Temporary Backoff	The device hosting the object that the microblock is attempting to interact with is not powered on. Ensure that the device hosting the object, in which the microblock is addressed to, is powered on and functioning properly.

Appendix B - Supported SNMP Protocol Data Units (PDUs)

The following SNMP PDUs are supported by the SNMP PPD.

PDU Type	V1	V2c and v3
OxAO - GET Request	X	X
OxA3 - SET Request	X	X
OxA2 - GET Response	X	X
OxA4 - TRAP	X	
OxA7 - SNMPv2-TRAP		X

Appendix C - Configuring the driver parameters by using the Service Port

You can set many driver parameters locally from the controller by using the **Service Port's** web-based controller setup interface. You can set operational parameters, such as port and communications' protocol settings, without the need to connect the i-Vu® application to the controller. Any parameters set locally through this interface take effect immediately. To connect to the controller setup pages, some controllers have an Ethernet Service Port, and some have a USB Service Port.

WARNING After setting parameters locally through the Service Port interface and then connecting the controller to the i-Vu® application, proceed carefully, as follows:

In the i-Vu® application, you must **upload** the parameters that you set locally BEFORE you **download** memory or parameters. Downloading, without uploading first, overwrites all the settings you made through the **Service Port**. Uploading first preserves those parameters.

NOTE There are a few parameters that can **only** be set through the **Service Port**, such as the controller's IP address, and these are not overwritten by a memory or parameter download from the i-Vu® application.

For more information on connecting to the Service Port, see the "Connecting to the router through the Service Port" and the "Connecting to the router through the Gig-E Port" sections of the controller's *Installation and Start-up Guide*.

Appendix D - Module Status field descriptions

Property	Description
SNMP Protocol Details	Communications: ▪ Number of data packets transmitted and received by the integrator ▪ Number of retries that resulted from failed requests ▪ Number of traps received from third-party devices

Document revision history

Important changes to this document are listed below. Minor changes such as typographical or formatting errors are not listed.

Date	Topic	Change description	Code*

* For internal use only