Microtronix
Collection Manager
User Guide 1.1.2

Microtronix Datacom Ltd.

4056 Meadowbrook Drive, Unit 126
London ON N6L 1E3
CANADA

www.microtronix.com

Tel: +1 519 690-0091
Fax: +1 519 690-0092
General Inquiries: info@microtronix.com
Sales Enquiries: sales@microtronix.com
Customer Support: support@microtronix.com

Table of Contents

1 Collection Manager Features

1.1 Overview

The ***Microtronix Collection Manager (CM)*** connects directly or indirectly to legacy Central Office (CO) voice switches to provided the following operations:

1.1.1 Call Detail Record (CDR) Polling

The ***CM*** polls for files containing CDR, AMA, EADAS, SMDR, TT, and other call/traffic data records over X.25, serial, or IP interface(s) using the polling or file transfer protocol supported by the switch. The polling process is:

- Manual and automatic/scheduled file retrieval or reception
- Optional file reformatting
- Optional file format scan
- Optional renaming
- Optional compression/encryption
- Local storage (optional network storage using NFS)
- Forwarding to billing, mediation, or other application server (push and/or pull)
- Optional back up with or without compression/encryption
- Daily backup aging

1.1.2 File management

The ***CM*** optionally provides static file management for backing up and restoring system files such as configuration and provisioning files. Manual and automatic/scheduled operations are available.

1.1.3 Command Line Interface (CLI)

The ***CM*** platform supports X.25 and serial interface conversion for remote TCP/IP terminal emulators or application processors.

1.2 Models

The Collection Manager software package may be installed on any supported Linux platform. The supported platforms and their features/restrictions are listed below.

1.2.1 Microtronix Access 1000

The Access 1000 is a standalone unit with an X.25 or serial interface for direct connection to a switch in a distributed collection system with one Gateway per switch.

1.2.2 Microtronix Access 4000

The Access 4000 is a standalone unit with 2 X.25 and/or serial interfaces for direct connection to a switch in a distributed collection system with one Gateway per switch. The second interface may be used as backup for the first interface, or used for management or CLI interface.

1.2.3 Linux x86 Server (i386, i686, x86_64)

The ***CM*** application software can be installed on Ubuntu, Redhat, and CentOS platforms to provide a centralized collection solution supporting multiple remote switches. Remote X.25/TCP gateways like the Access X.25/TCP Gateway are required for X.25/TCP conversion. An optional XOT Gateway

application is available to support remote XOT routers.

1.3 Switch Interfaces

The ***CM*** supports switches connected through TCP/IP network connections directly to the switches, or via X.25-TCP gateways and serial-TCP terminal servers. The Access 1000/4000 also has local X.25 gateway, terminal server, and synchronous server applications.

1.3.1 X.25

The Access Gateway models support direct X.25 connectivity. The x86 Server model requires external X.25/TCP gateways like the Access X.25/TCP Gateway, or XOT routers.

1.3.2 IP

All models support IP connections to the switches. FTP and SFTP are supported for soft switches, and RFC1006/TCP (ISO-TP) for legacy switches using FTAM.

1.3.3 Serial

The Access Gateway models support sync/asynchronous serial connections directly. The x86 Server model requires external serial/TCP terminal servers like the Access Terminal/Synchronous Server.

1.4 Switch Protocols

These are the supported protocols used for interfacing with the switch.

1.4.1 AFT – Nortel Automatic File Transfer

AFT is used for receiving AMA files over an X.25 interface to the switch. Commonly used on Nortel DMS-100 switches.

1.4.2 AMATPS (BX.25) - Automatic Message Accounting Teleprocessing System

AMATPS (GR-385-CORE) is used for retrieving AMA files over an X.25 interface to the switch. Commonly used on North American Siemens EWSD and Lucent 5ESS switches.

1.4.3 AMTP - Alphanumeric terminal over Ericsson MTP

AMTP converts a raw TCP/IP socket to the command line interface (CLI) of the AXE switch over an X.25 interface. Remote TCP/IP client may be a terminal emulator (like putty of WinSCP) or other application processor.

1.4.4 BUFFER – Store-and-Forward data buffer

Buffer is used to retrieve or receive raw byte-stream data over a TCP/IP socket, X.25 interface, serial interface, or synchronous interface to the switch. This method has no protocol handshake.

1.4.5 DCO (HDLC/LAT)

DCO is used for retrieving files over an HDLC/LAPB interface to a Stromberg-Carlson Digital Central Office switch.

1.4.6 EADAS - Engineering and Administrative Data Acquisition System

EADAS is used for retrieving various traffic and other data at specific timed intervals over an X.25 interface to the switch.

1.4.7 FTAM - File Transfer Access and Management

(Available by special order only – separate license fee)

FTAM (ISO 8571) is used for retrieving or receiving files over an X.25 interface (or RFC1006/TCP) to the switch.

1.4.8 FTP/IP and SFTP/IP

Standard clients/servers are used for retrieving or receiving files over IP to legacy CO switches and soft switches like Metaswitch and Cisco Call Manager.

1.4.9 LOCAL

LOCAL protocol allows files from a local directory to be forwarded to a remote server. This may be used to provide a second forwarding destination for another local collector.

1.4.10 MTP - Ericsson Message Transfer Protocol

MTP is used for retrieving or receiving files over an X.25 interface to the AXE. The collector can be configured as a client to initiate polling sessions using Server File Input (SFI) mode, or act as a server to wait for the switch to initiate a push using Server File Output (SFO) mode.

1.4.11 XFER - Nortel Data Transferral Application Protocol

XFERPRO is used for retrieving AMA, SMDR, and other types of data over an X.25 interface to the switch. Used on various Nortel switches and PBXs like the DMS-100.

1.5 File Formats

When AMA (Automatic Message Accounting) or BAF (Billing AMA Format) records are collected into files, they may be stored in their original file format or converted to a different format for compatibility with the downstream server. Other formats may be used for detecting file content problems. The possible file formats are:

1.5.1 AMATPS

Complete AMA records are packed into 1531-byte fixed size blocks with header and trailing pads. The AMA records may have Recording Office Type/ID and/or Sensor Type/ID fields suppressed. This is the file format sent by the switch when using AMATPS protocol.

1.5.2 AMATPS+fileHeader

This format is the same as AMATPS, but also includes the 20-byte primary or 14-byte secondary file header sent by the switch. Multiple 100-block “files” in the output file will each have a file header.

1.5.3 Martin Group

This is a custom AMATPS format used for compatibility with legacy Martin Group mediation/billing systems. The AMATPS blocks are rounded to the nearest multiple of 512 bytes containing actual records.

1.5.4 AMA

AMA records are packed into the file without block/file headers or trailing pads. AMA records are BAF format with Sensor Type/ID fields suppressed (two-field suppression), or Sensor and Recording Office Type/ID fields suppressed (four-field suppression).

1.5.5 BAF

Billing AMA Format records are packed into the file without block/file headers or trailing pads. When converting from AMA formats, records will have suppressed fields inserted from configured values.

1.5.6 AMADNS standard

AMA or BAF records padded into 2060-byte blocks including a 16-byte block header.

1.5.7 TT 110 byte

CDR records (Telephone Tickets) with 110 byte fixed length.

1.5.8 XFER fixed block

Records are packed into 2048 byte fixed size blocks with a block header and trailing pads after the last record. This is the file format sent by the switch when using XFER protocol.

1.5.9 XFER variable block

XFER files from the DMS may have trailing pads removed from the fixed-size blocks to create files with variable-size blocks.

1.5.10 AMACLDS

AMACLDS format files are created by the collector from AMATPS files. The AMATPS fixed-size blocks have trailing pads removed to create files with variable-size blocks, and the AMATPS block header is replaced with a 4-byte length header (same as XFER). The AMA records contained in the blocks are converted to BAF by inserting suppressed fields (sensor type/ID and recording office type/ID) as needed into each record. In addition, the collector adds header audit records (9036, 9038) at the beginning of the converted file, and trailer audit records (9037, 9039) at the end of the file.

1.6 File Processing Options

Files pulled from the switch or pushed by the switch are processed before they are forwarded to the mediation/billing server.

1.6.1 Content Scan

Files with a known format may be scanned during or after transfer to validate and/or summarize content. For example AMATPS and XFER.

1.6.2 Conversion

Files with a known format may be converted from one format to another suitable for the server. For example, AMATPS files may be converted BAF.

1.6.3 Renaming

File names may be changed from their original name to another suitable for the server. New file names may include static content, sequence number, and date/time stamps.

1.6.4 Compression

Files may be compressed (zipped) before or after forwarding to the server.

1.6.5 Encryption

Files may be encrypted using GNU Privacy Guard before or after forwarding to the server.

1.7 File Forwarding Options

Standard IP-based file transfer protocols ensure compatibility with mediation, billing, and application servers. Each collector can be configured with a unique file server IP address and file transfer protocol for client (push), or a unique account for remote client login and pull.

Files can also be moved/copied to local directories.

The supported forwarding methods are:

1.7.1 FTP

RFC959 File Transfer Protocol

1.7.2 SFTP

SSH/Secure File Transfer Protocol

1.7.3 Copy or Move to Local Directory

Collected files can be copied or moved directly to another locally-accessed directory. On the Access 1000/4000 models, this must be a mounted external USB 2.0 flash drive. NFS mounted drives may also be configured.

1.8 Poll Scheduling

The system cron scheduler allows flexible polling of each switch at any time of day, or multiple times per day as frequently as once per minute. Schedules for weekdays and weekends can also be configured. The initial schedule added to the crontab for a newly created collector configuration is midnight, local time.

1.9 Configuration and Management Interfaces

A web interface allows for configuration, management, and monitoring from any Internet browser using HTTP or HTTPS. A command line interface provides additional configuration and management tools, and may be accessed via Telnet, SSH, or serial Console port.

1.10 Internal XOT Gateway

The ***Access 1000/4000 CM*** comes complete with support for X.25 Over TCP connections to remote XOT routers. The XOT Gateway is optional on other Linux/x86 platforms.

1.11 Internal X.25-TCP/IP Gateway

The ***Access 1000/4000 CM*** has an internal X.25-TCP/IP Gateway that provides the connectivity between a local X.25 or LAPB WAN interface and the collection application.

On the Access 4000 models, the second WAN interface can also be used to provide X.25/TCP connections to other remote application servers by providing conversion between X.25 and TCP/IP devices, or X.25 encapsulation over TCP (XOT). Refer to the **Access User Guide** for details.

1.12 Internal Serial/TCP Terminal Server

The ***Access 1000/4000*** also has an internal Terminal Server that provides the connectivity between a local serial interface to the switch and the collection application or to remote management applications.

On the Access 4000 models, the second WAN interface can also be used to provide serial connections

to other remote application servers by providing conversion between serial and TCP/IP devices. Refer to the **Access User Guide** for details.

1.13 Internal Synchronous/TCP Server

The ***Access 1000/4000*** also has an internal Synchronous Server that provides the connectivity between a local synchronous interface to the switch and the collection application or to remote management applications.

On the Access 4000 models, the second WAN interface can also be used to provide synchronous/HDLC connections to other remote application servers by providing conversion between synchronous and TCP/IP devices. Refer to the **Access User Guide** for details.

2 Management Web Interface

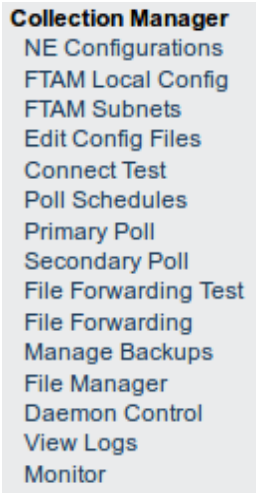
This Guide assumes that the ***CM*** is already installed and the web access already established with any standard Internet browser like Windows Internet Explorer or Mozilla Firefox.

Open the web browser, and enter the ***CM***'s IP address in the URL field. When prompted by a popup window, login using default user name: **`admin`**, and password: **`admin`**.

The home page will be displayed with the main menu down the left hand side.

2.1 Main Menu

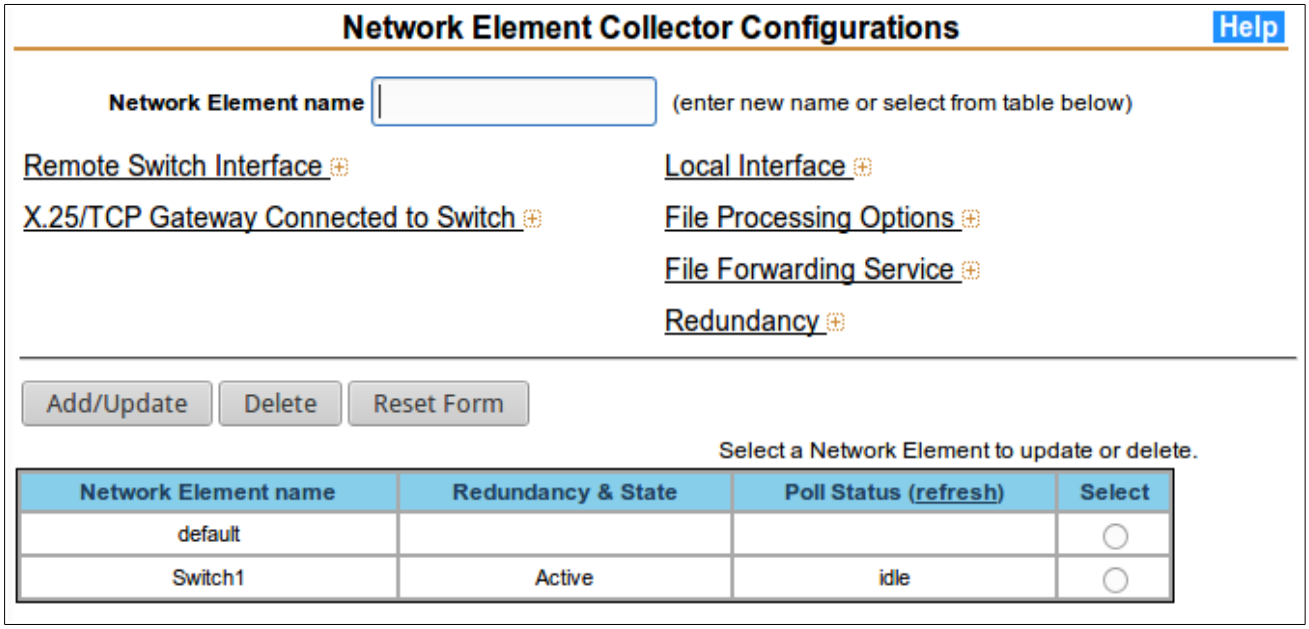
The ***CM*** can be configured and managed by selecting the main menu's Collection Manager items. Each page may have a **Help** button in the upper right corner for viewing additional information specific to that page.



Follow the home page **Help** button to find additional manuals for downloding.

3 Network Element Configuration

The Collection Manager configuration page is used to configure the switch polling parameters, connectivity, and file forwarding for each switch application to be supported. Click on the **NE Configuration** item in the main menu to display the form with default values. The page consists of a number of expandable sections that can be opened by clicking on the title for each section, followed by a table of already configured collectors.



The first collector displayed in the table (default) is the template for common default values when creating new collector configurations. Only modify the default collector when new common values are desired when creating production collector configurations. The default collector is not enabled for collection. As collectors are added, they will appear in the table, for example “Switch1”.

For the latest detailed configuration information, click the **Help** button on the page.

3.1 Network Element Name

The Network Element Name should reflect a unique name assigned to each CO switch. This name may be used to form part of the CDR output file name by using the “%n” formatting variable in the **Output Filename Format** field. It will be used for identification in syslog, SNMP event, and email notifications, if enabled.

3.1.1 Add a Collector

Enter a new name in this field to create a collector configuration for a switch. The configuration sections will expand to show all configuration options. The FTAM protocol requires the name to be 8 characters or less.

3.1.2 Update a Collector

Select the name of a collector from the table to modify it's configuration. Expand the section(s) that require modification.

3.2 Remote Switch Interface

This section shows how to configure the protocol parameters to interface with the switch. When creating a new collector configuration, first choose the Protocol used by the switch.

3.2.1 Protocols

This field configures the protocol used by the switch. Choose from the available protocols in the drop-down list when creating a new collector. The display will change to show relevant parameters.

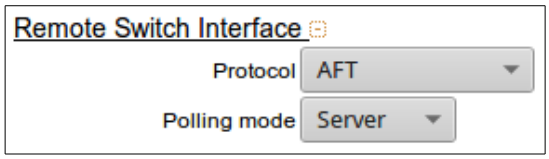
The available protocols are:

- AFT Collection of AMA files in server (SFO) mode over an X.25 interface.
- AMATPS Collection of sequential AMA files over an X.25 or BX.25 interface.
- AMTP AXE Command Line Interface over an X.25 interface.
- BUFFER Buffered collection of raw data over a TCP/IP, X.25, or serial interface.
- DCO Collection of file over an HDLC/LAPB interface
- EADAS Collection of traffic data files over an X.25 interface.
- FTAM Collection of files using ISO/FTAM over an X.25 or RFC1006/TCP/IP interface.
- FTP/IP Collection of files over a TCP/IP interface.
- LOCAL Copy files from a local directory (may be from another local collector)
- MTP Collection of files in client (SFI) or server (SFO) mode over an X.25 Interface.
- SFTP/IP Collection of files over a secure TCP/IP interface.
- XFER Collection of AMA, SMDR, or other file types over an X.25 interface.

The following sections describe each protocol.

3.2.2 AFT Server Configuration

Configuring for collection from the Nortel DMS switch consists of creating a server (SFO) for receiving files from the switch's AFT client. Select **Protocol** AFT and **Polling mode** Server

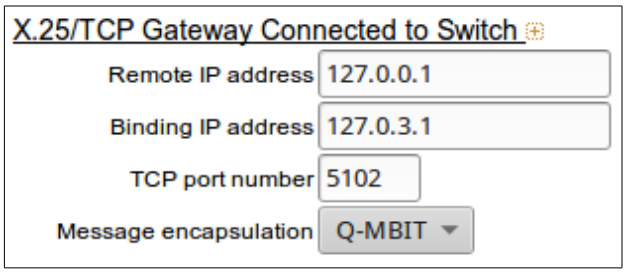


At the scheduled poll events, any new files deposited by the switch are processed and placed into the file forwarding subdirectory for transfer to the billing/mediation server.

3.2.2.1 Local (internal) X.25/TCP gateway

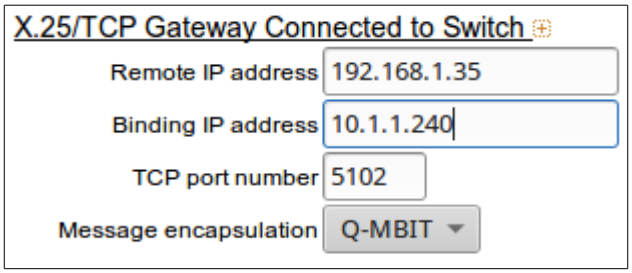
Enter the listening TCP port number in the **TCP Port Number** field of the **X.25/TCP Gateway** section. The TCP port may be bound to a local IP interface to restrict access or avoid TCP conflict. If the X.25 or XOT gateway is internal, use a loopback IP address as in the example. The **Message Encapsulation** must be set for a type that supports X.25 Q-bit packets like Q-MBIT, QRBP, or AEPN. These must agree with the setting in the X.25 to TCP Routing table corresponding to the incoming X.25 connection.

The **Remote IP address** of the external X.25 gateway may be entered for monitoring purposes. If it is the local X.25 or XOT Gateway, enter 127.0.0.1.

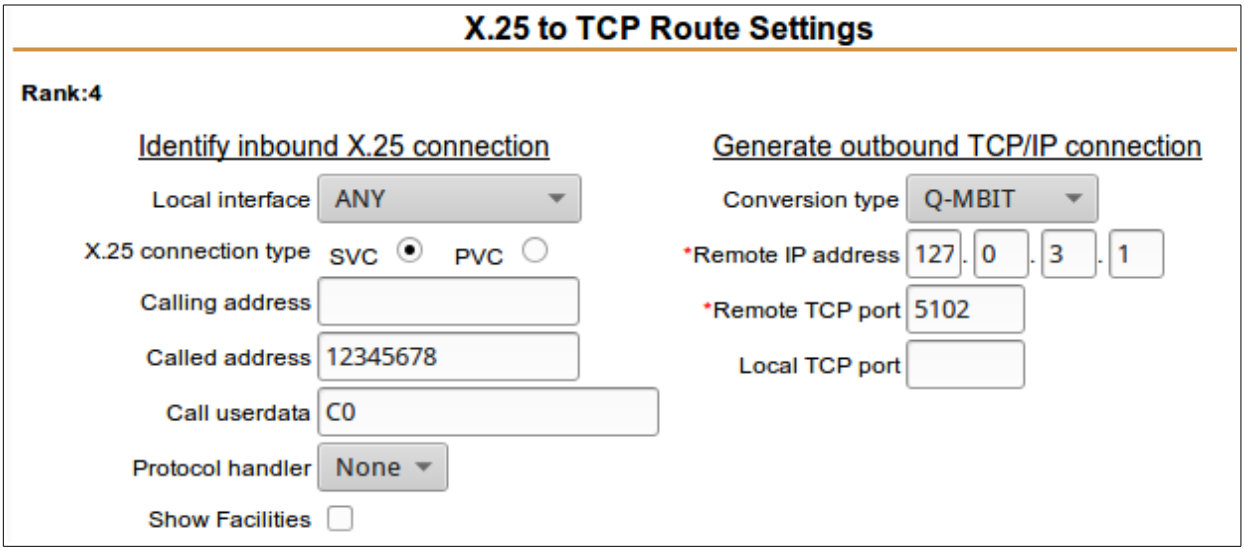


3.2.2.2 Remote (external) X.25/TCP gateway

If the X.25 gateway is external, enter it's external IP address. In the example below, the listening TCP port is bound to the unit's own IP address, 10.1.1.240, and the external gateway's IP address is 192.168.1.35.

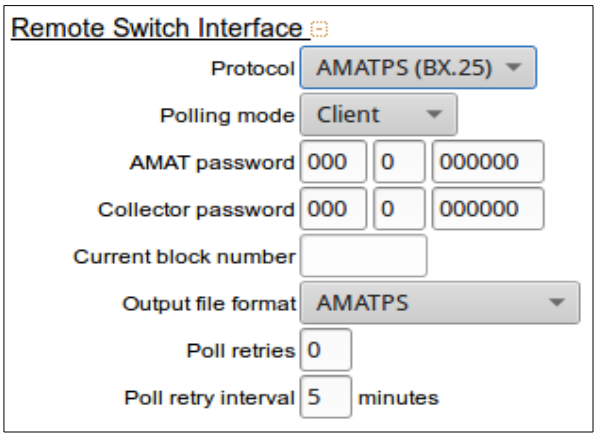


The local or remote X.25 Gateway must be configured to listen for the incoming X.25 connection, and the TCP/IP destination must match these parameters. For example, the Microtronix X.25/TCP Gateway:



3.2.3 AMATPS Client Configuration

Configuring for collection from the switch consists of creating a client for pulling files from the switch's AMAT (AMA Transmitter). Select **Protocol** AMATPS and **Polling mode** Client.



The collected file type is AMATPS which has fixed length blocks containing AMA records with collector and sensor id/type fields suppressed. The collector can convert the files into other formats using the **Output file format** parameter in the **Local Collector Interface** section.

The10-digit **Collector password** parameter, consisting of the **Recording Office type**, **unit**, and **ID** fields, is sent to the switch to request a polling session and MUST be correct for the AMAT to accept the connection. Some switches will accept all zeros.

The 10-digit **AMAT password** parameter, consisting of the **Sensor type**, **SUN**, and **ID** fields, is sent by the switch's AMAT in response to the connection request and MUST be correct for the Collection Manager to proceed with a polling connection. If set to all zeros, any password is accepted and ignored.

The **Sensor type** and **ID** fields may also be used to form part of the output filename, and/or inserted into AMA records if BAF Output Format is selected.

The type, unit and ID fields are 3, 1, 6 digits respectively.

The **Current block number** reflects the expected AMATPS block number in the next file polled. The collector automatically adjusts if the switch offers a different “next block number available”.

The **Output File Format** parameter specifies the output format or conversion of collected files. For example, blocked files may be converted to unblocked/streamlined, and AMA records may be converted to BAF.

The **Poll Retries** parameter specifies the number of retries attempted after a first failure with **Poll retry interval** minutes between polls.

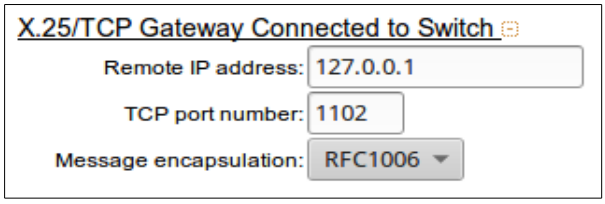
The **Poll Schedule** is initially set to midnight, but can be changed to another time of day or multiple times per day. In addition, a daily maintenance file can be retrieved by uncommenting it's default schedule.

The **X.25/TCP Gateway** parameters are used by the collector to connect to the switch's X.25 interface via a TCP/IP connection to either the local (internal) X.25/TCP Gateway or a remote X.25/TCP gateway.

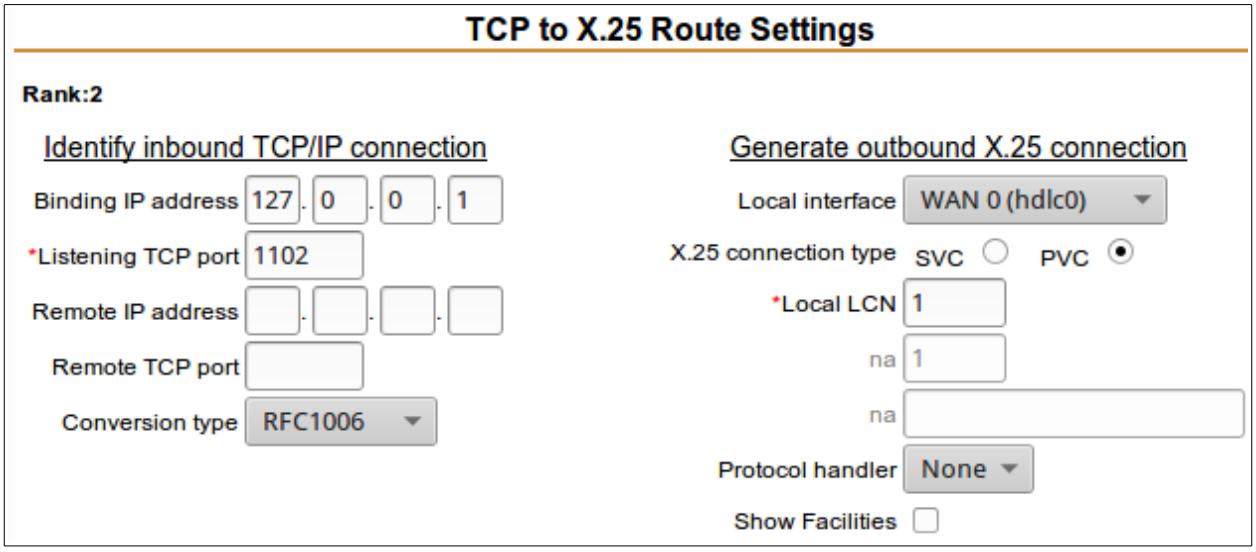
The X.25 interface of the gateway must be configured with at least one Permanent Virtual Circuit (PVC).

3.2.3.1 Local (internal) X.25/TCP gateway

The collector connects via local TCP/IP to the internal X.25/TCP Gateway application.

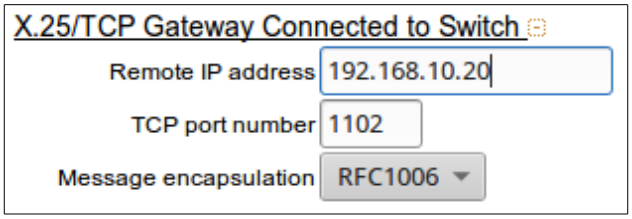


The **Remote IP Address** is set to the local IP network interface (127.x.x.x) to address the local gateway which connects directly to the X.25 interface of the switch via a WAN interface. The **TCP to X.25 Route** of the local gateway must listen on the same **TCP Port Number** and map it to PVC 1 on the X.25 interface. The **Message encapsulation** must match the **Conversion type** in the route. RFC1006 is recommended.

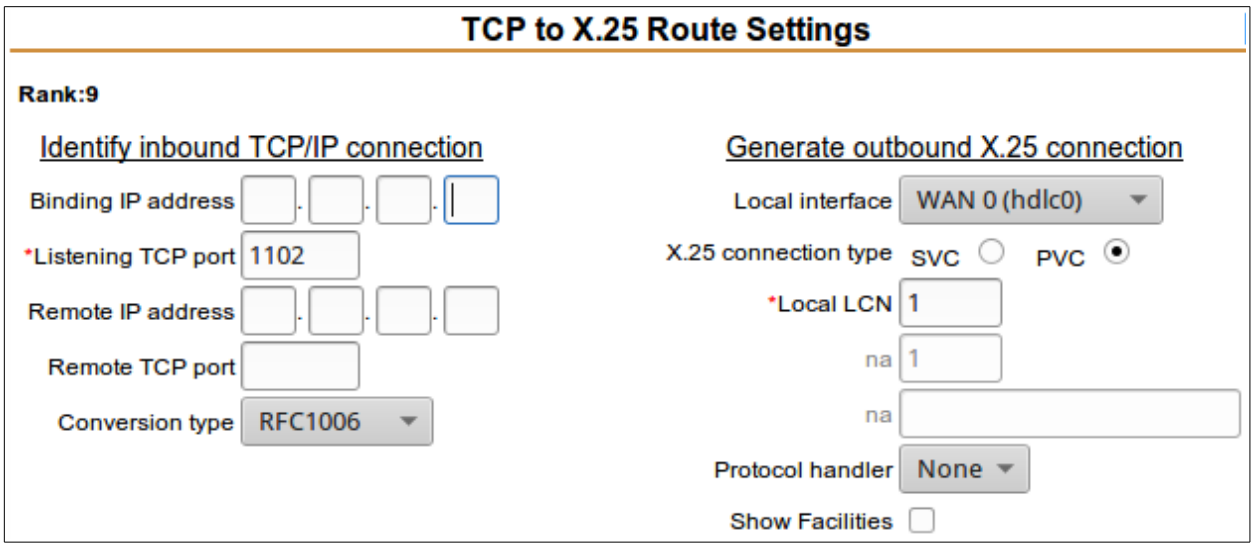


3.2.3.2 Remote (external) X.25/TCP gateway

The collector connects via external TCP/IP to the remote X.25/TCP Gateway unit.

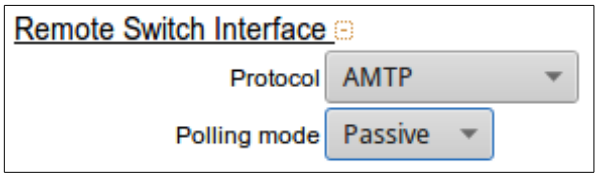


The **Remote IP Address** is set to the external IP network interface to address the remote gateway which connects to the X.25 interface of the switch via it's local X.25 interface. The TCP to X.25 route/map of the remote gateway must listen promiscuously on the **TCP Port Number** and map it to PVC 1 on the X.25 interface. For example, the Microtronix X.25/TCP Gateway:



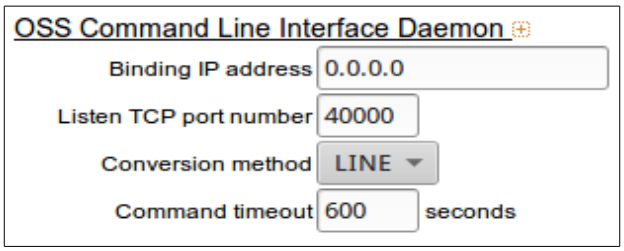
3.2.4 AMTP Command Line Interface Configuration

An Alphanumeric terminal over MTP (AMTP) command line interface (CLI) may be created for converting text to Alphanumeric MTP format toward the Ericsson AXE by selecting **Protocol** AMTP, and **Polling mode** Passive.



Remote terminal emulator

The ***CM*** waits for a connection from a remote terminal emulator to convert user commands to AMTP format towards the AXE, and deliver the text portion of the response back to the user.



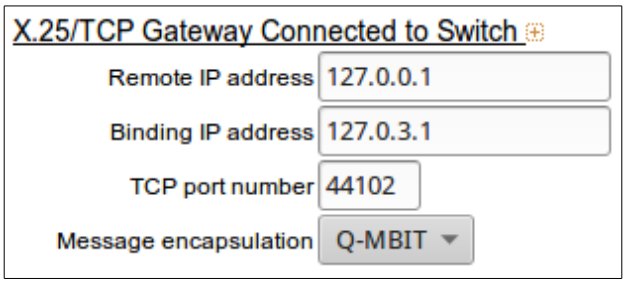
Select the TCP port number [and binding IP address] on which the CLI interface listens for TCP connections from the remote terminal emulator. A server daemon is started that waits for a user to connect, then connects to the AXE's command line interface via the X.25/TCP gateway defined below.

The daemon issues a “<” prompt to indicate readiness to accept AXE commands from the user. Commands may need to be entered in upper case.

Conversion method Line will expect the terminal emulator to delver the user's input with a trailing linefeed character. Any carriage return character inserted by the terminal emulator will be discarded. The terminal emulator should be configured for local echo and editing.

X.25/TCP Gateway

The **X.25/TCP Gateway** parameters are used to inter-connect with the switch's X.25 interface via a TCP/IP connection to/from either the local (internal) X.25/TCP Gateway or a remote X.25/TCP gateway.

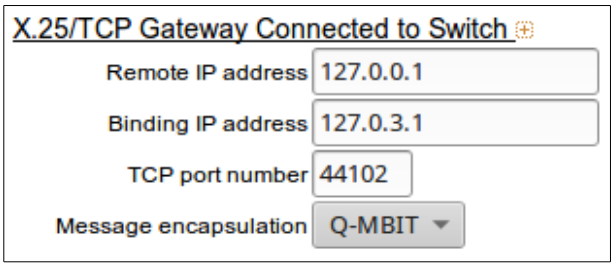


The **Remote IP Address** is set to the address of a local or remote gateway which connects directly to the X.25 interface of the switch via a WAN interface. The **TCP to X.25 Routes** section of the gateway must listen on the **TCP port number.**

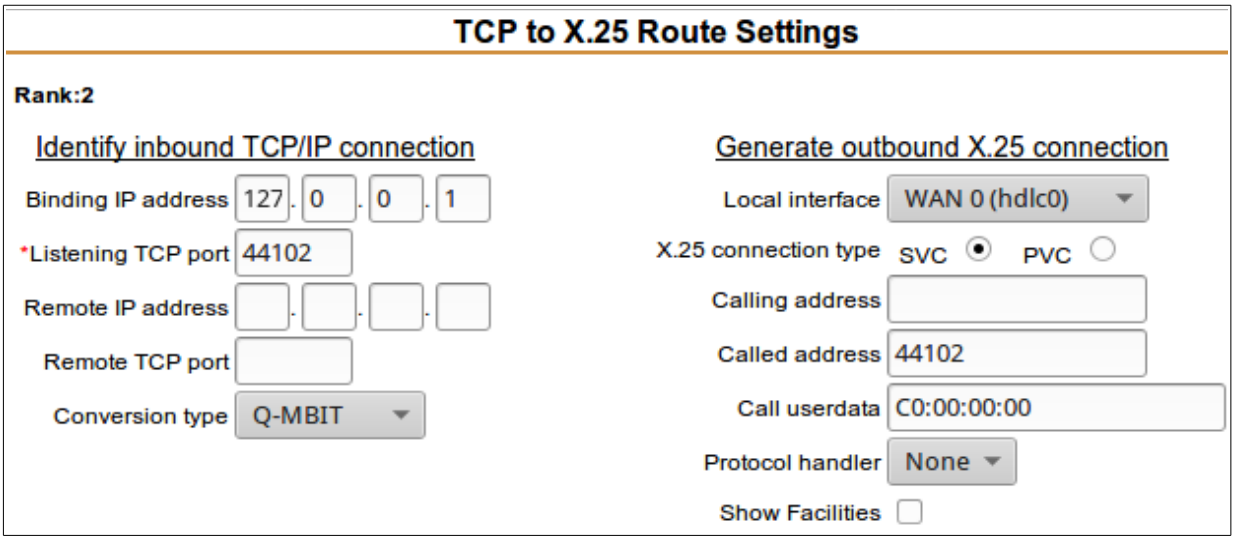
Delayed or “Ordered” reports may be delivered by the AXE at a later time via separate X.25 connection to the originator's X.25 address. These will be delivered to the originating user by configuring the X.25 TCP Gateway to listen for that X.25 address and forwarded that connection to the TCP/IP address as specified in the **Binding IP address** and **TCP port number** fields.

3.2.4.1 Local (internal) X.25/TCP gateway

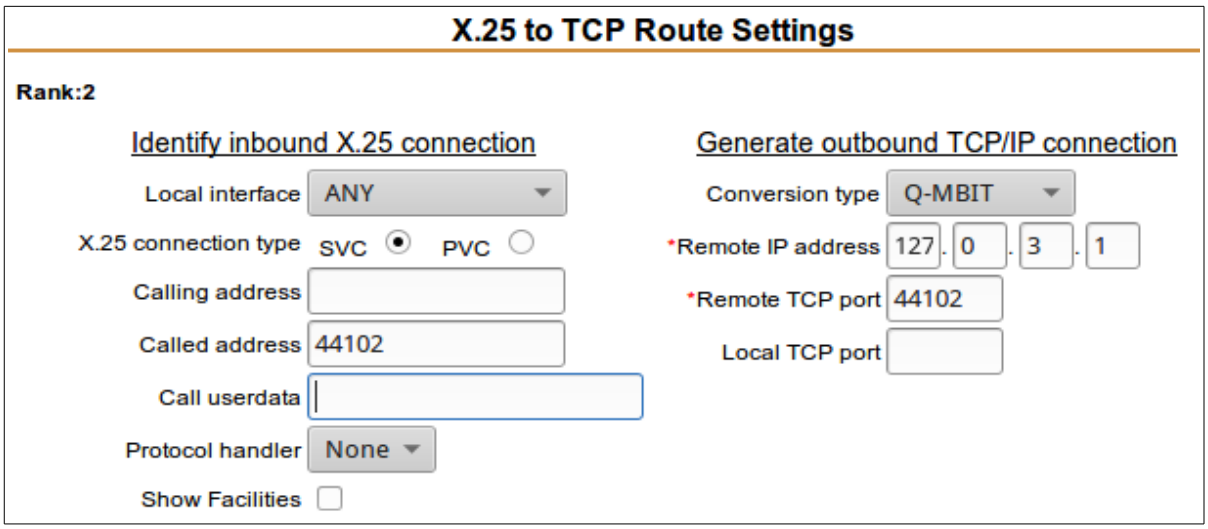
The CLI server connects via local TCP/IP to the internal X.25/TCP Gateway application.



The **Remote IP Address** is set to the local IP network interface (127.x.x.x) to address the local gateway which connects directly to the X.25 interface of the switch via a WAN interface. The **TCP to X.25 Route** of the local gateway must listen on the same **TCP Port Number** and generate a connection on the X.25 interface. The **Message encapsulation** must match the **Conversion type** in the route. Q-MBIT is recommended.

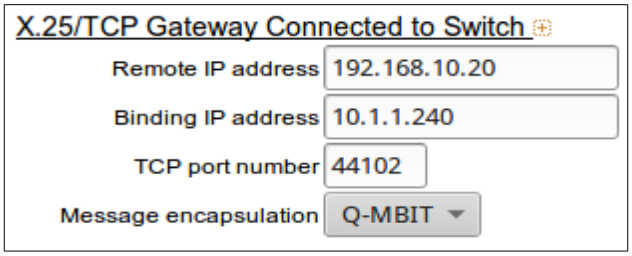


The **Binding IP address** is used to accept the connection from the AXE via the local gateway. The X.25 to TCP route must listen for the X.25 address from the AXE and generate a connection to the CLI server


X.25 to TCP Route Settings
Rank:2
Identify inbound X.25 connection
Local interface
ANY
X.25 connection type
SVC
PVC
Calling address
Called address
44102
Call userdata
Protocol handler
None
Show Facilities
Generate outbound TCP/IP connection
Conversion type
Q-MBIT
*Remote IP address
127
0
3
1
*Remote TCP port
44102
Local TCP port

3.2.4.2 Remote (external) X.25/TCP gateway

The CLI server interconnects via external TCP/IP to the remote X.25/TCP Gateway unit.

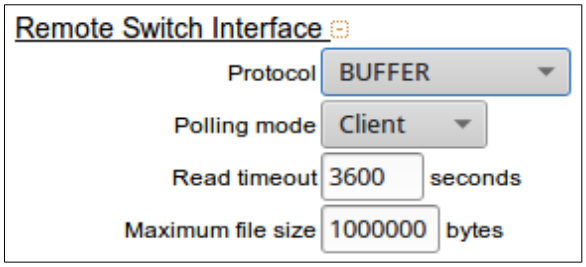


The **Remote IP Address** is set to the external IP network interface of the remote gateway which connects to the X.25 interface of the AXE via it's local X.25 interface. The TCP to X.25 route/map of the remote gateway must listen on the **TCP Port Number** and map it to the X.25 interface.

The **Binding IP address** must be set to that of the local Ethernet interface. The X.25 to TCP map of the remote gateway must map the incoming X.25 connection from the AXE to this IP and the **TCP port number** as specified above. The **Message encapsulation** method must match and must include support for both M-bit and Q-bit X.25 data packets.

3.2.5 BUFFER Client/Server Configuration

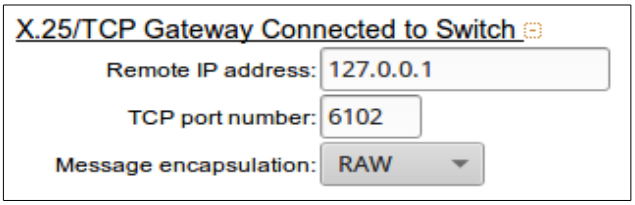
Configuring for continuous data collection from the switch consists of creating a client or server daemon for reading data from the switch's interface. Select **Protocol** BUFFER



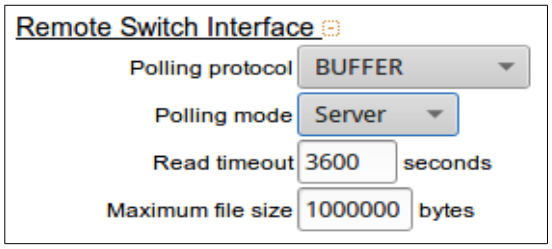
The **Read Timeout** interval is the number of seconds of idleness (no data received) before the file is closed and a new one opened.

The **Maximum File Size** value is the maximum number of bytes written to the open file before it is closed and a new one opened. A short time of idleness is allowed so that any partial “record” is not split between files.

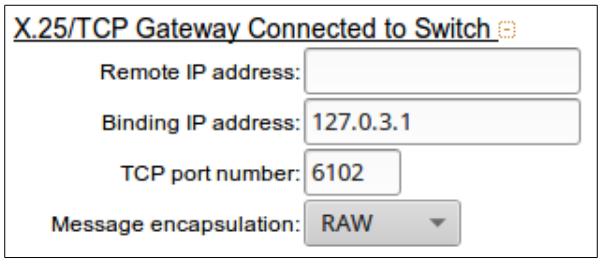
If **Polling Mode** is set to **Client,** the X.25/TCP Gateway parameters may be configured for connection to the local or a remote X.25/TCP Gateway, or to the local or remote TCP terminal server for serial connection to the switch.



If the gateway or serial server is local (internal), a local **IP Address** is used (127.x.x.x). If the gateway or serial server is remote (external), the IP Address must be external. The gateway or server must be listening on the **TCP Port Number**.

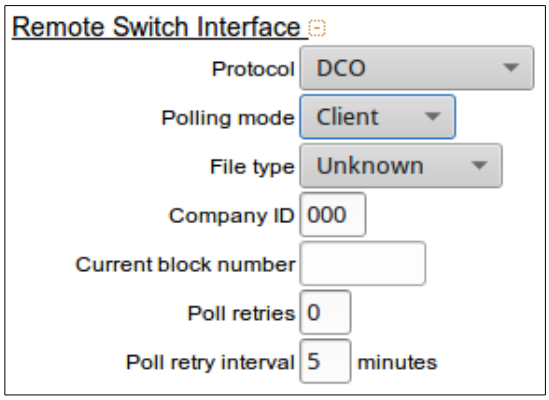


If **Polling Mode** is set to **Server**, the daemon will accept a connection from any source by configuring the **TCP Port Number** as the listening port. If the source is the local X.25/TCP gateway or the Terminal / Sync Server, the TCP port may be bound to a local interface by setting the **Binding IP Address** to 127.x.x.x. The **Remote IP address** of the external X.25 gateway may be entered for monitoring purposes.



3.2.6 DCO Client Configuration

Configuring for collection from a DCO switch consists of creating a client for pulling files from the switch's file server. Select **Protocol** DCO and **Polling mode** Client.



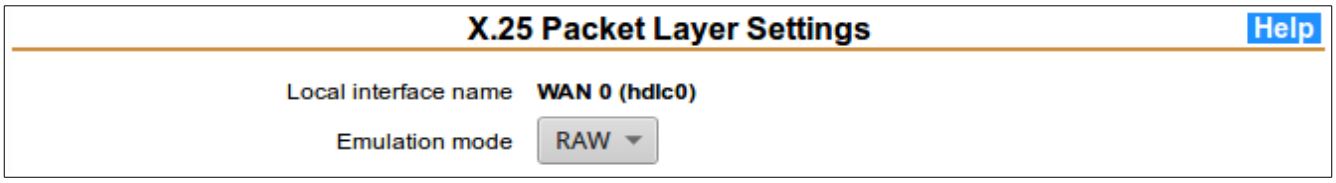
The **File type** reflects the format/type of data contained in the files collected. AMADNS may be selected, and an AMA record summary may be produced after polling.

The **Company ID** parameter, consisting of 3 digits, is exchanged with the switch and MUST be correct for the switch to accept the connection.

The **Current block number** reflects the expected data block number in the next file polled. Collection failure will occur if the number does not match that of the switch. Manual intervention will be required to recover the missing blocks using Secondary polling. The current block number file will need to be edited in the Edit Config Files web page, and the Primary poll retried.

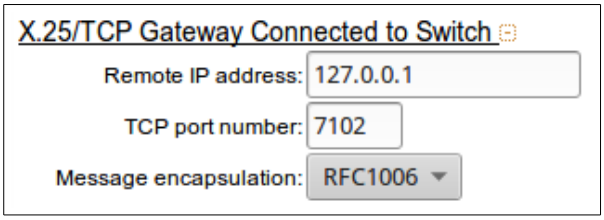
The **Poll Retries** parameter specifies the number of retries attempted after a first failure with **Poll retry interval** minutes between polls.

The **X.25/TCP Gateway** parameters are used by the collector to connect to the switch's HDLC/LAPB interface via the local (internal) or a remote X.25/TCP gateway. The X.25 interface of the gateway must be configured for RAW Emulation mode (LAPB operation).

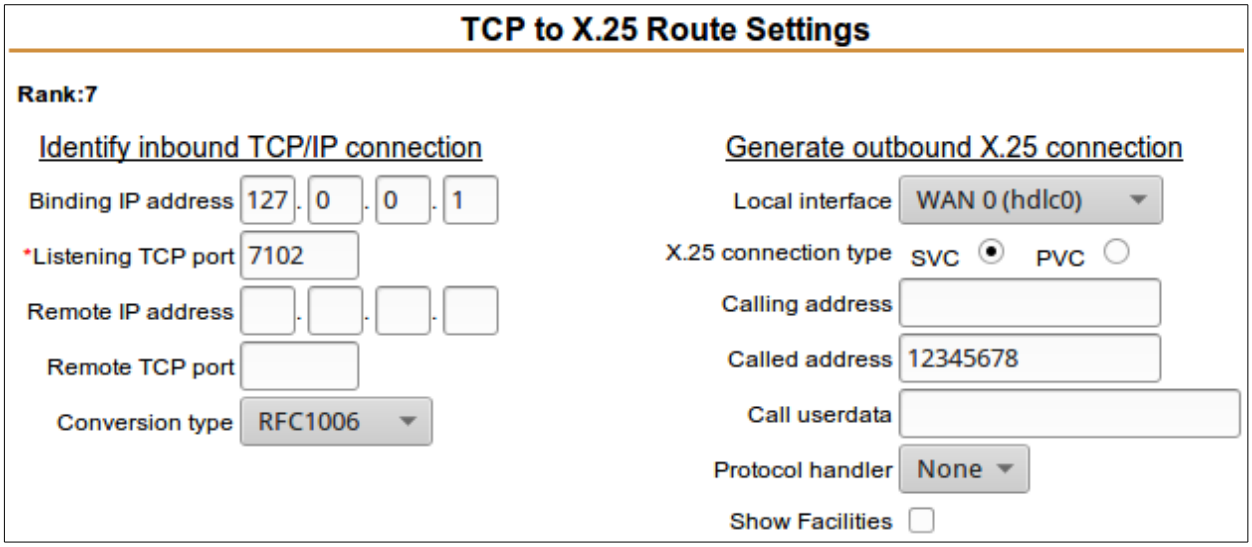


3.2.6.1 Local (internal) X.25/TCP gateway

The collector connects via local TCP/IP to the internal X.25/TCP Gateway application.

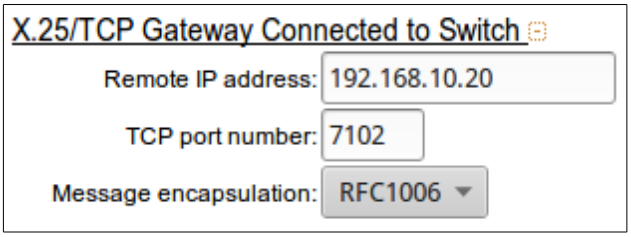


The **Remote IP Address** is set to the local IP network interface (127.x.x.x) to address the local gateway which connects directly to the HDLC/LAPB interface of the switch via a WAN interface. The **TCP to X.25 Routes** section of the internal gateway must listen on the **TCP Port Number** and map it to a WAN (LAPB) interface.

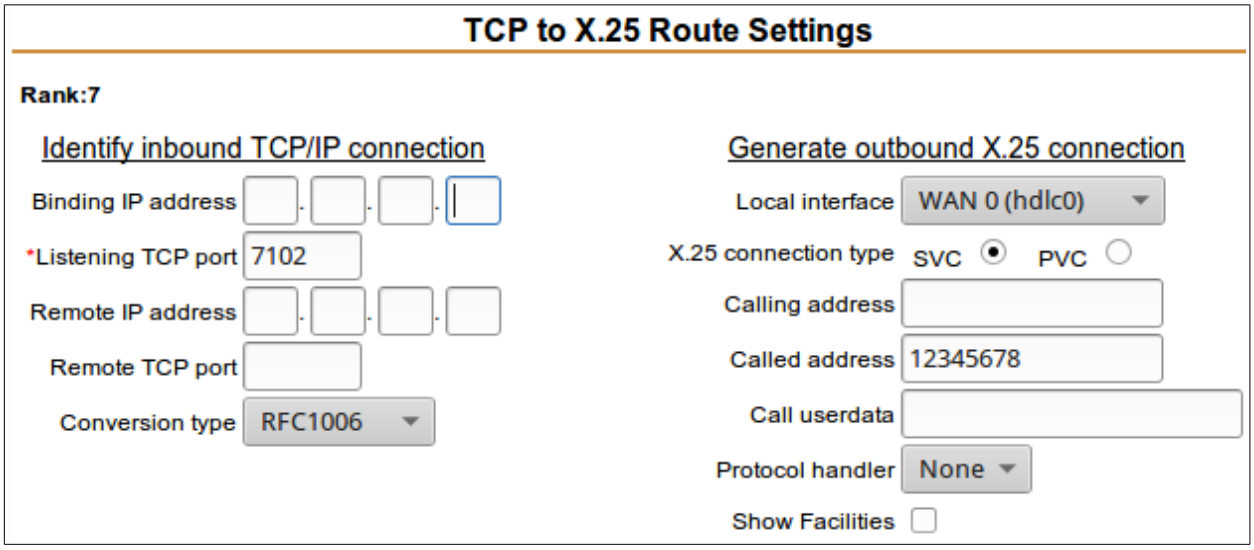


3.2.6.2 Remote (external) X.25/TCP gateway:

The collector connects via external TCP/IP to the remote X.25/TCP Gateway unit.

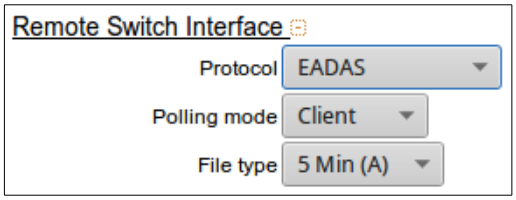


The **Remote IP Address** is set to the external IP network interface to address the remote gateway which connects to the HDLC/LAPB interface of the switch. The TCP to X.25 route/map of the remote gateway must listen on the **TCP Port Number** and map it to a (LAPB) WAN interface.



3.2.7 EADAS Client Configuration

Configuring for collection from the switch consists of creating a client for pulling files from the switch's file server. Select **Protocol** EADAS and **Polling mode** Client.

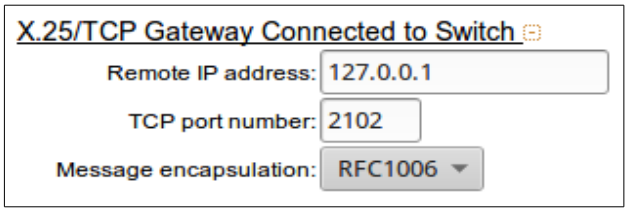


Select the traffic report type in the **File type** field. A separate collector must be created for each traffic report type desired. Each report type has it's own poll schedule (5 minutes, 30 minutes, hourly, or daily). Each also has X.25 interface and file transfer parameters that can be unique or the same.

The **X.25/TCP Gateway** parameters are used by the collector to connect to the switch's X.25 interface via the local or a remote X.25/TCP gateway.

3.2.7.1 Local (internal) X.25/TCP gateway

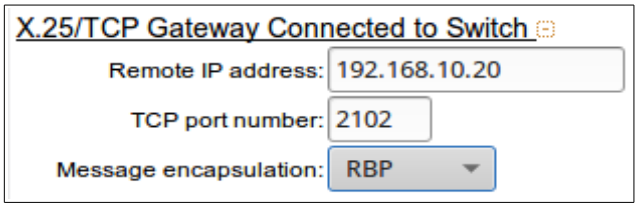
The collector connects via local TCP/IP to the internal X.25/TCP Gateway application.



The **Remote IP Address** is set to the local IP network interface to address the local gateway which connects directly to the X.25 interface of the switch via a WAN interface. The **TCP to X.25 Routes** section of the internal gateway must listen on the **TCP Port Number** (and bind to the same local IP address)

3.2.7.2 Remote (external) X.25/TCP gateway

The collector connects via external TCP/IP to the remote X.25/TCP Gateway unit.

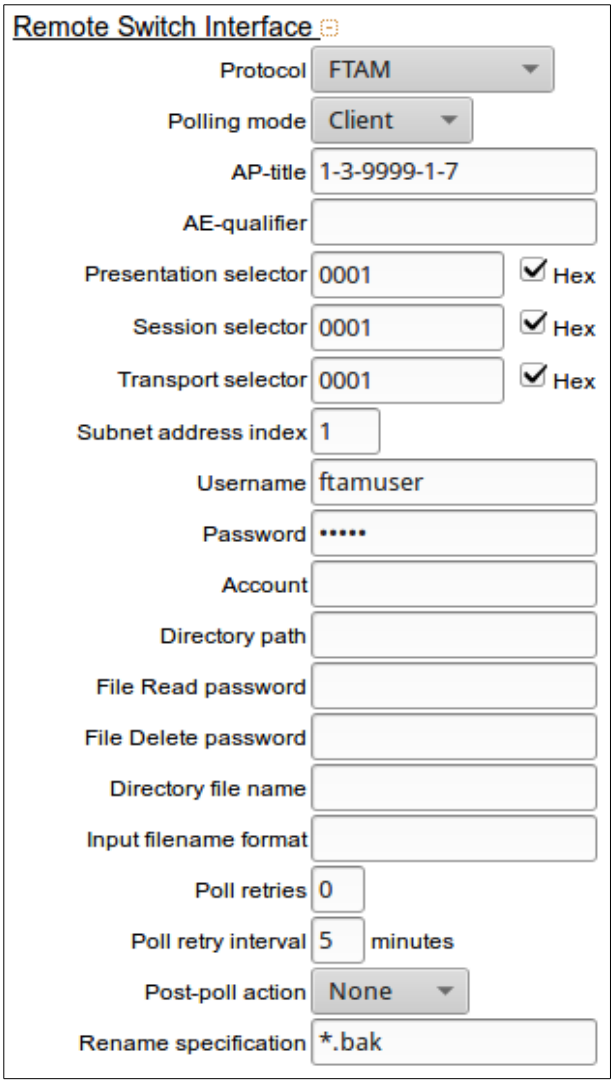


The **Remote IP Address** is set to the external IP network interface to address the remote gateway which connects to the X.25 interface of the switch via it's local interface. The TCP to X.25 route/map of the remote gateway must listen on the **TCP Port Number**.

3.2.8 FTAM Client Configuration

Note: FTAM is only available if an FTAM license is purchased.

Select **Protocol** FTAM and **Polling mode** Client to poll the switch for files.



Fill in the **AP-title**, **AE-qualifier**, **Presentation** / **Session** / **Transport Selector** fields as expected by the switch. Fill these as appropriate, paying regard to the expectation in the switch.

The **Subnet Address Index** field is the reference to the defined RFC1006 sub networks that provide the collector side of the above parameters. See the FTAM Subnets section for definitions.

The **Username**, **Password**, and **Account** fields should be filled in as necessary for the Collection Manager to login into the switch (the Account field is not normally used, so can be left blank in most cases).

The **Directory** field specifies an absolute or relative path to CDR files (may be left blank if the files are in the home directory of the user).

The **File Read Password** and **File Delete Password** fields should match the values configured in the switch (if any) to allow the corresponding file access.

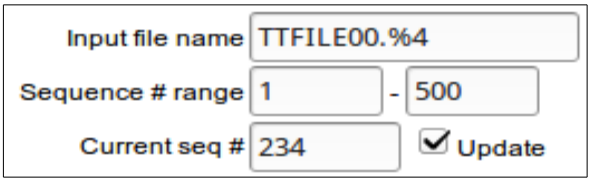
If the **Directory File Name** is defined, it will be retrieved by the collector to get the list of files available for collection on the switch. The list is scanned for those not already retrieved, and then retrieves them. The **Input filename format** fields will not be used. If this field is left blank, then the **Input Filename format** parameters will have significance

The **Input filename format** field may be used to specify the file name of the file or stream of files on the switch to poll. If defined, a retrieval of the file or stream occurs at each poll interval. If not defined, the collector will do a directory listing to find collectible files names. An **Input File Name** consists of string characters and/or a replacement variable.

Replacement variable %*n* (where *n* represents a 1, 2, …, or 9 digit sequence number)

A "**%*n***" variable in the **Input File Name** field is replaced during a poll with the **Current seq #** parameter which should match the next available file on the switch. The range of the sequence number is specified in the **Sequence # range** fields, and must match the definition on the switch.

For example, if the next available file on the switch is TTFILE00.0234 and the range on the switch is defined to be 1-500, then the number of digits is 4 and the next available file sequence number is 234:



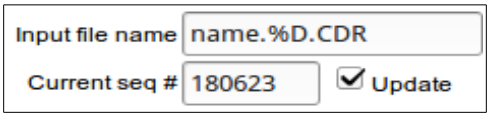
The **Current seq number** field contains the current (next) sequence number if **Input File Name** contains a "%*n*" variable. These fields MUST be given an initial value equal to the next available file in the switch. The variable will be expanded into the current sequence number when polling for that file. Successful retrieval will cause the sequence number to be incremented. The variables must one of:

- %1 – 1-digit sequence number within the defined range
- %2 – 2-digit sequence number within the defined range

  ...
- %9 – 9-digit sequence number within the defined range

Replacement variable %D – date sequence

A "**%D"** variable in the **Input File Name** field is replaced during a poll with the **Current seq #** parameter which should match the next available file on the switch. The **Current seq #** parameter must be set to match the next available file on the switch. For example, June 23, 2018:



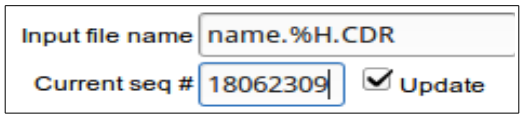
The **Current seq number** field contains the current (next) sequence number if **Input File Name** contains a "%D" variable. This field MUST be given an initial value equal to the next available file in the switch. The variable will be expanded into the current sequence number when polling for that file. Successful retrieval will cause the sequence number to be incremented. The variable must be in the format:

- %D – 6-digit date tag in the format YYMMDD, incremented daily

Replacement variable %H , %h, %d – date and time sequence

A "**%H**", "**%h**", or "**%d**" variable in the **Input File Name** field is replaced during a poll with the **Current**

seq # parameter which should match the next available file on the switch. The **Current seq #** parameter must be set to match the next available file on the switch. For example, June 23, 2018, 9AM:



The **Current seq number** field contains the current (next) sequence number if **Input File Name** contains a "%H", "%h", or "%d" variable. This field MUST be given an initial value equal to the next available file in the switch. The variable will be expanded into the current sequence number when polling for that file. Successful retrieval will cause the sequence number to be incremented. The variable may be one of:

- %H – 8-digit date+hour tag in the format YYMMDDHH, incremented by 1 hour
- %h – 8-digit date+hour tag in the format YYMMDDHH, incremented by 2 hours
- %d – 8-digit date+hour tag in the format YYMMDDHH, incremented by 24 hours (daily)

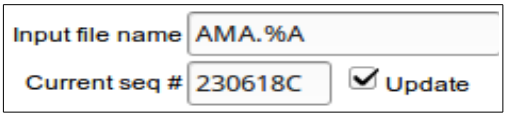
Replacement variable %A – date and letter sequence

A "**%A**" variable in the **Input File Name** field selects an incremental date and tag component in the format "DDMMYYx", where:

- DDMMYY = 2-digit day of the month, 2-digit month number, and 2-digit year
- x = A, B, C, D, E

The "x" component is incremented through the values, and resets back to "A" after "E". Each reset cases a date increment.

The **Current seq #** parameter must be set to match the next available file on the switch. For example, To set the next available file to 230618C (June 23, 2018, file "C"):



The **Post-poll Action** parameter may be configured for DELETE or RENAME to cause the collection cycle to delete the file from the switch, or rename it using the **Rename Specification** parameter so that the file is no longer available for collection. If Rename is selected, the rename specification is used to rename the file, with the "*" replaced with the original filename, and any date variables substituted accordingly (%Y, %y, %m, %d, %H, %M, %S). Setting to **None** allows the switch to leave the file available or perform an automatic rotation operation.

The **X.25/TCP Gateway** parameters are used by the collector to connect to the switch.

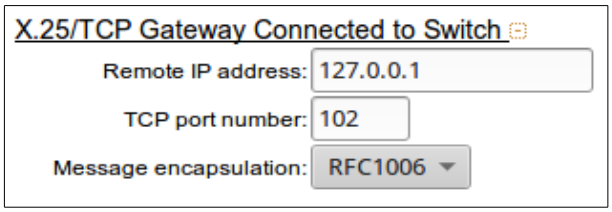
If the switch supports FTAM/X.25, the Remote IP address is that of a local or remote X.25/TCP gateway listening on the TCP port.

If the switch supports RFC1006/TCP/IP, the Remote IP address and TCP port number are those of the listening FTAM server on the switch.

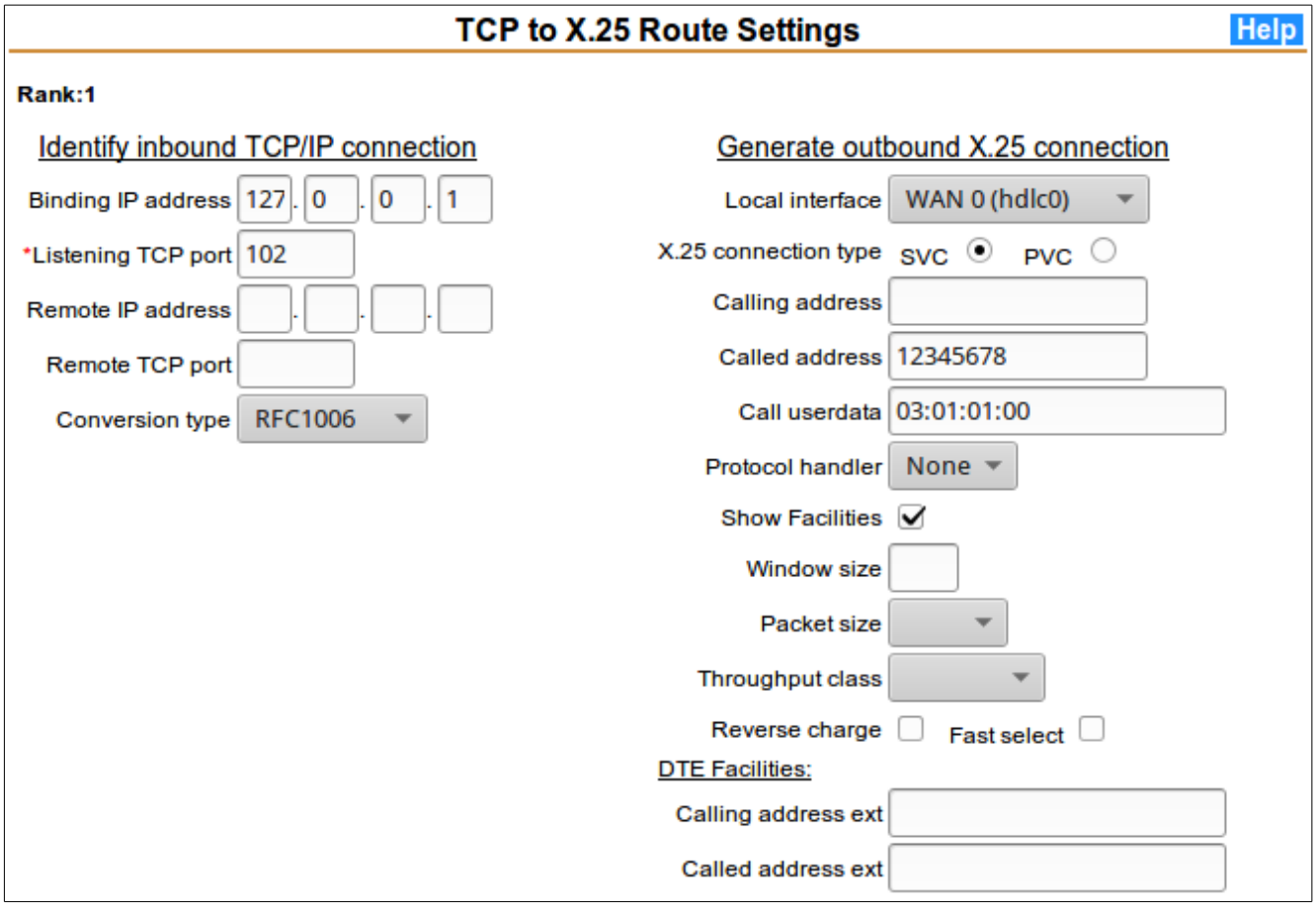
In either case, the **Message Encapsulation** must be set for RFC1006 (ISO-TP0).

3.2.8.1 Local (internal) X.25/TCP gateway

The collector connects via local TCP/IP to the internal X.25/TCP Gateway application.



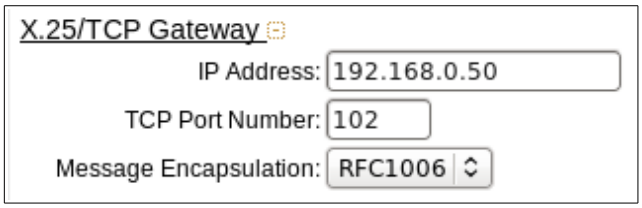
The **IP Address** is set to the local IP network interface to address the local gateway which connects directly to the X.25 interface of the switch via a WAN interface. The **TCP to X.25 Routes** section of the internal gateway must listen on the **TCP Port Number** (and bind to the same local IP address).



Note: FTAM switches frequently require specific X.25 called and calling addresses as well as DTE address extensions facilities.

3.2.8.2 Remote (external) X.25/TCP gateway

The collector connects via external TCP/IP to the remote X.25/TCP Gateway unit.

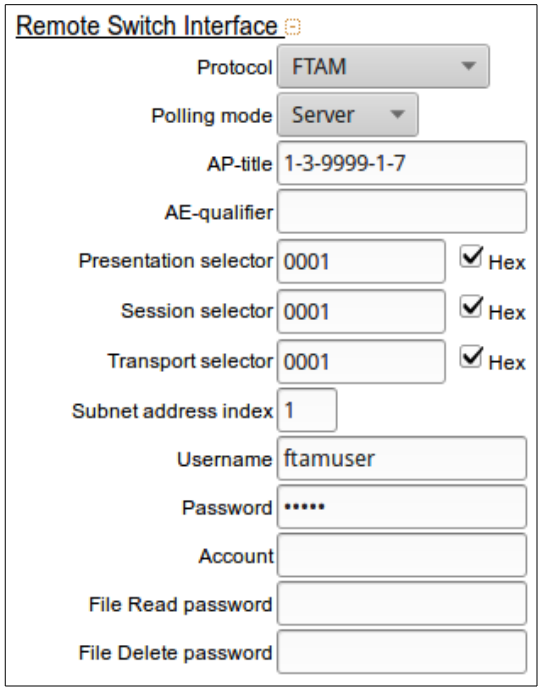


The **IP Address** is set to the external IP network interface to address the remote gateway which connects to the X.25 interface of the switch via it's local interface. The TCP to X.25 route/map of the remote gateway must listen on the **TCP Port Number**.

3.2.9 FTAM Server Configuration

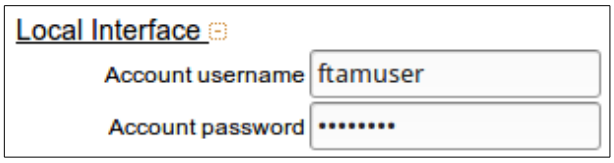
Note: FTAM is only available if an FTAM license is purchased.

Select **Protocol** FTAM and **Polling Mode** Server to accept connections and files from the switch. At the scheduled poll events, any new files are processed and put into the file forwarding subdirectory for transfer to the billing/mediation server.



Client parameters can be defined to enable manual operations if supported by the switch.

The **Account Username** and **Password** fields in the **Local Interface** section must be filled in to match those used by the switch so it can login and push files.



The **Remote IP address** of the X.25 gateway may be entered for monitoring and manual operations. If it is the local X.25 or XOT Gateway, enter 127.0.0.1.

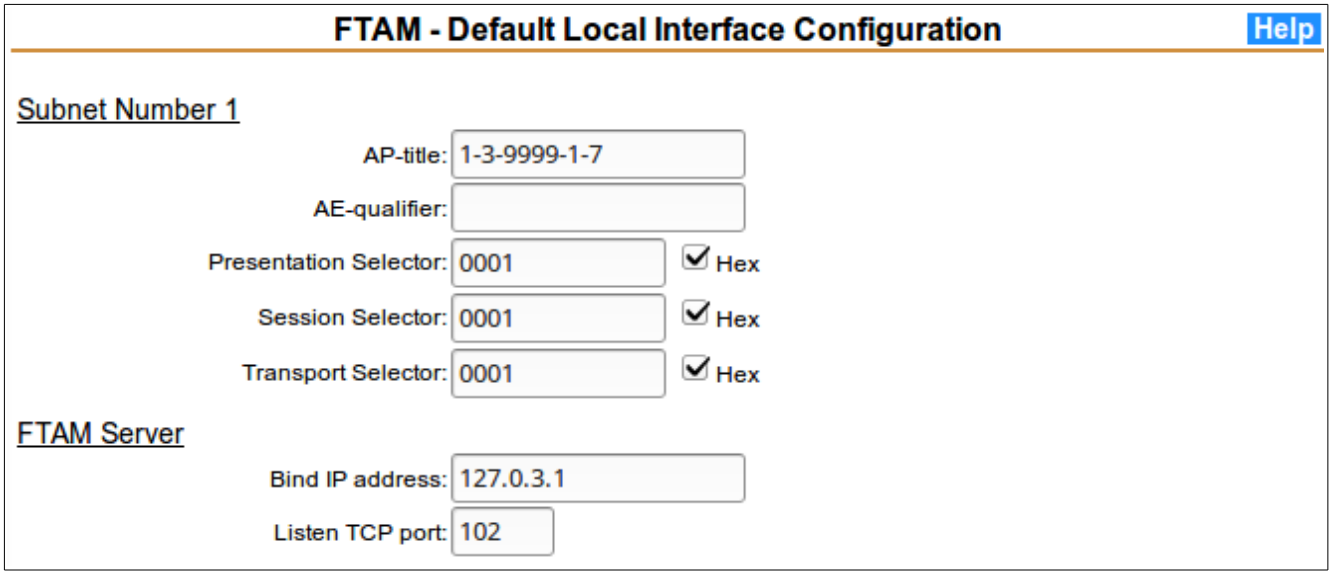
If the X.25 gateway is external, enter it's external IP address. In the example below, the listening TCP port is bound to the unit's own IP address, 10.1.1.240, and the external gateway's IP address is

192.168.1.35.


X.25/TCP Gateway Connected to Switch
Remote IP address
192.168.1.35

3.2.10 FTAM Local Configuration

The **FTAM Local Configuration** page provides the common parameters of the FTAM file server. The **FTAM Server** section defines the listening TCP port number for connections from an X.25 gateway connected to the switch's x.25 interface, or directly from a switch with an IP interface.



If connections are from the local XOT or X.25 gateway only, then set the **Bind IP Address** to a local IP address as in the example. If connections are from an external gateway, then leave the field blank, or set to the unit's own external IP address.

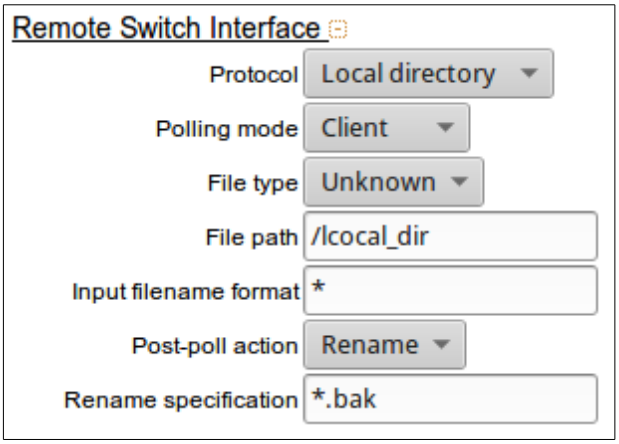
3.2.11 LOCAL Directory Configuration

This configuration is for pulling files from a local directory for forwarding to a remote file server. Typically used for forwarding to a second server for another NE configuration.

If **Polling Mode** is set to **Client**, the **File path** must be configured with a valid local directory. If the **File path** is that of another collector to provide a second forwarding destination for its files, then the backup directory of the other collector must be entered. For example, if the other collector name is “Switch2”:

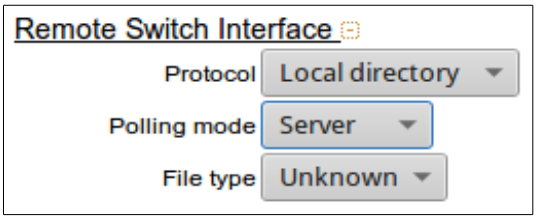
`/var/lib/acm/collector/Switch2/databackup/`

The **File name** must be specified; wildcards permitted.



Once a file is pulled from the other local directory, it may be deleted or renamed to prevent being pulled again by selecting the appropriate **Post-poll action**.

If **Polling Mode** is set to **Server**, the collector will take no polling action at a scheduled interval.



It is assumed that some process has pushed the files to this collectors working directory:

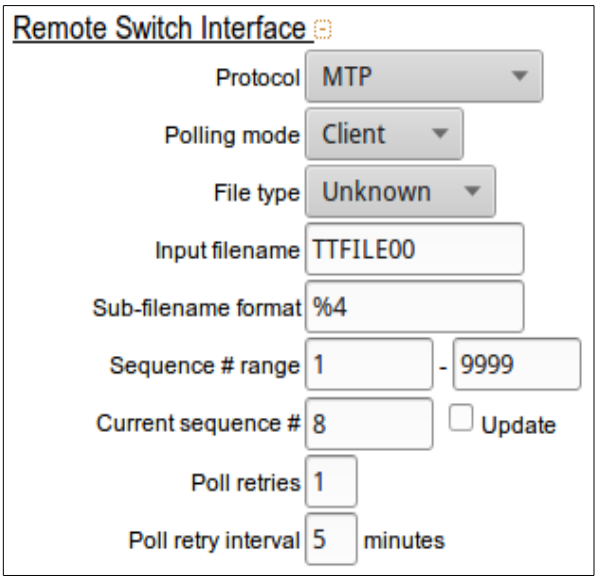
`/var/lib/acm/collector/MY-NAME/`

If a remote FTP or SFTP client is pushing files to the collector, then use polling protocol FTP/SFTP in server mode, and define a local user.

At the scheduled poll events, any new files are processed and put into the file forwarding subdirectory for transfer to the billing/mediation server.

3.2.12 MTP Client (SFI) Configuration

Configuration for active collection from the AXE switch consists of creating an SFI client (Session File Input) for pulling files from the switch's MTP server. Select **Protocol** MTP and **Polling mode** Client.



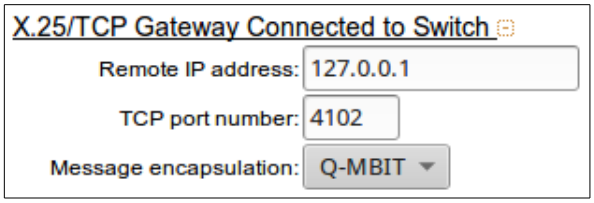
Select **Polling Mode = Client** if the Collection Manager initiates the polling connection. The collector will poll for files defined in the **Input file name** + **Subfile name** fields. The file name must be defined for polling to occur. A **sequence number** is included for unique file retrieval by adding a sequence # variable to the Subfile name. The range of sequence numbers can be defined, and the next to collect can be set by entering the **Current seq #** and selecting **Update**.

The collected file name will be <File Name>-<Subfile>, for example: “TTFILE00-0008”.

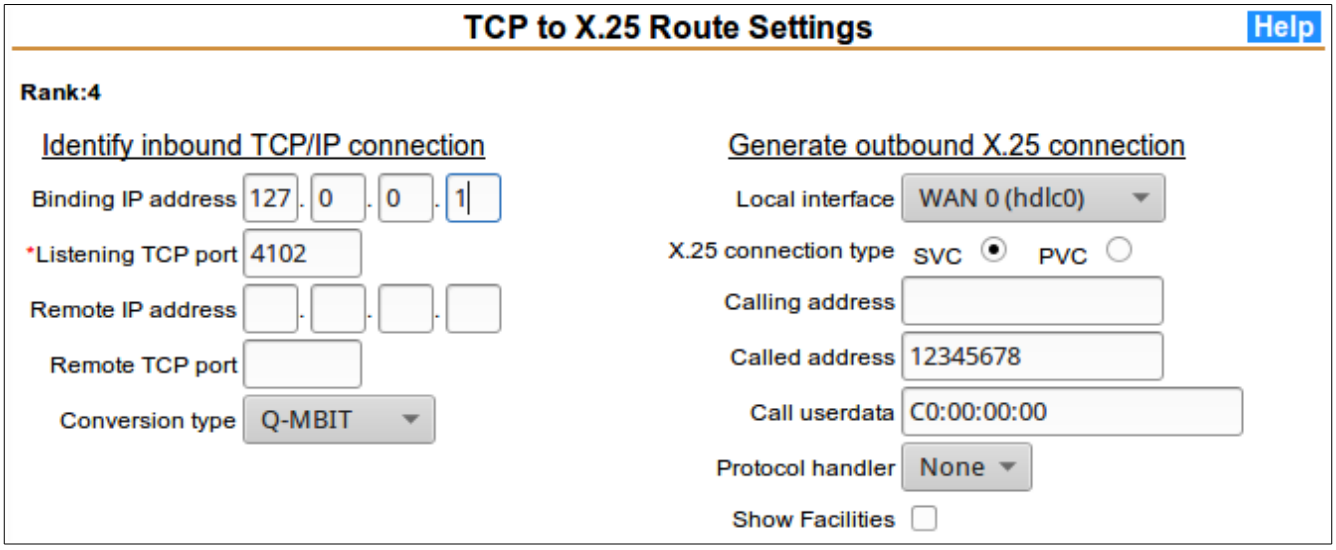
The **X.25/TCP Gateway** parameters are used by the collector to connect to the switch's X.25 interface via the local or a remote X.25/TCP gateway. The **Message Encapsulation** must be set for a type that supports X.25 Q-bit packets like Q-MBIT, QRBP, or AEPN.

3.2.12.1 Local (internal) X.25/TCP gateway

The collector connects via local TCP/IP to the internal X.25/TCP Gateway application.

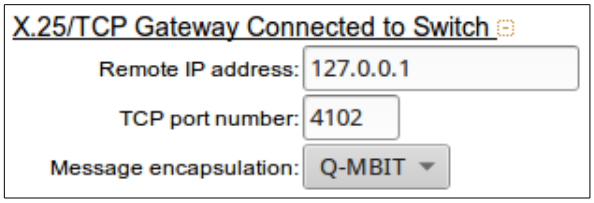


The **Remote IP Address** is set to the local IP network interface to address the local gateway which connects directly to the X.25 interface of the switch via a WAN interface. The **TCP to X.25 Routes** section of the internal gateway must listen on the **TCP Port Number** (and bind to the same local IP address).

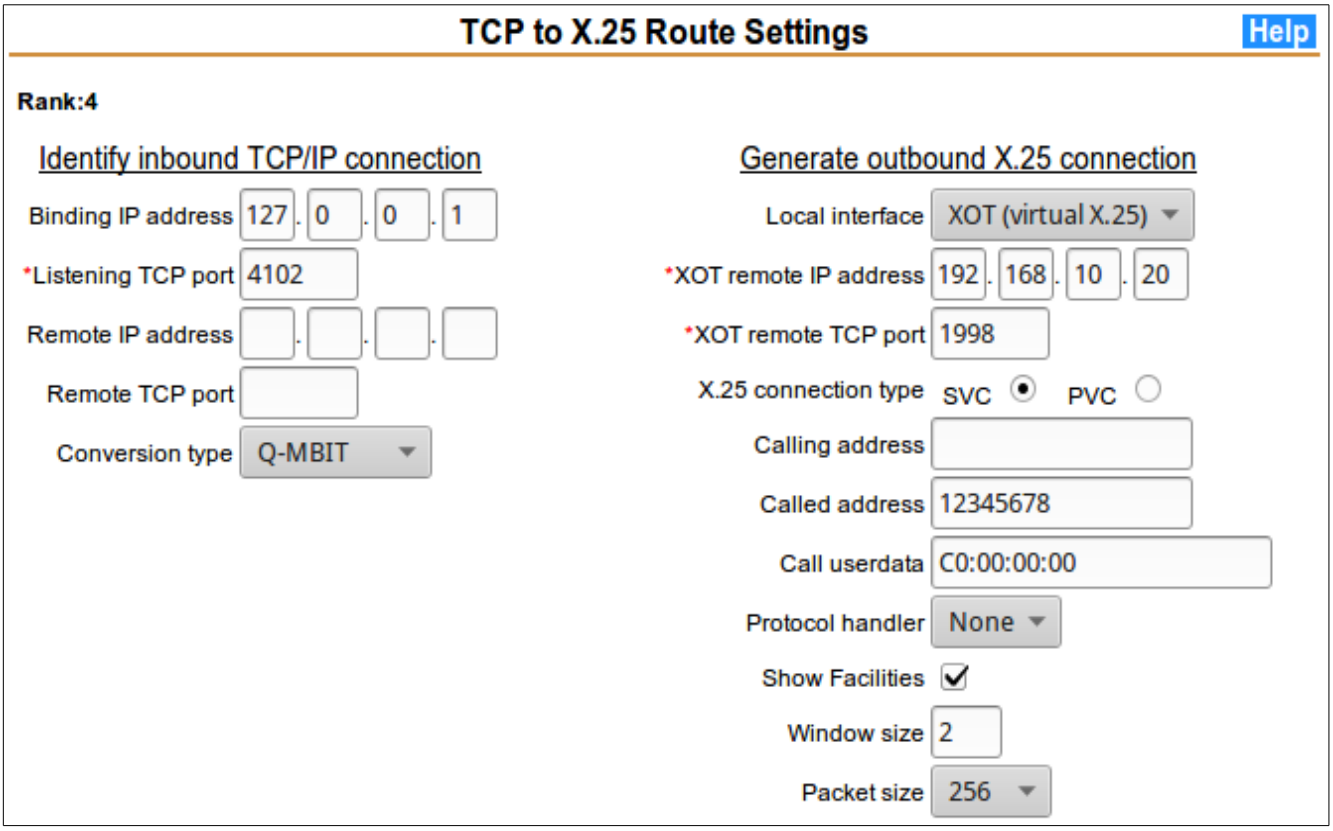


3.2.12.2 Local (internal) XOT gateway

The collector connects via local TCP/IP to the internal XOT Gateway application.



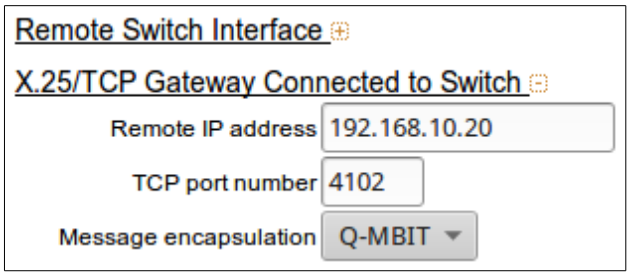
The **Remote IP Address** is set to the local IP network interface to address the local XOT gateway which connects indirectly to the X.25 interface of the switch via a remote XOT Gateway. The **TCP to X.25 Routes** section of the internal gateway must listen on the **TCP Port Number** (and bind to the same local IP address).



The **XOT remote IP address** and **TCP port** are set to connect to the external XOT router connected to the switch X.25 interface. The X.25 call parameters are used for the virtual X.25 connection.

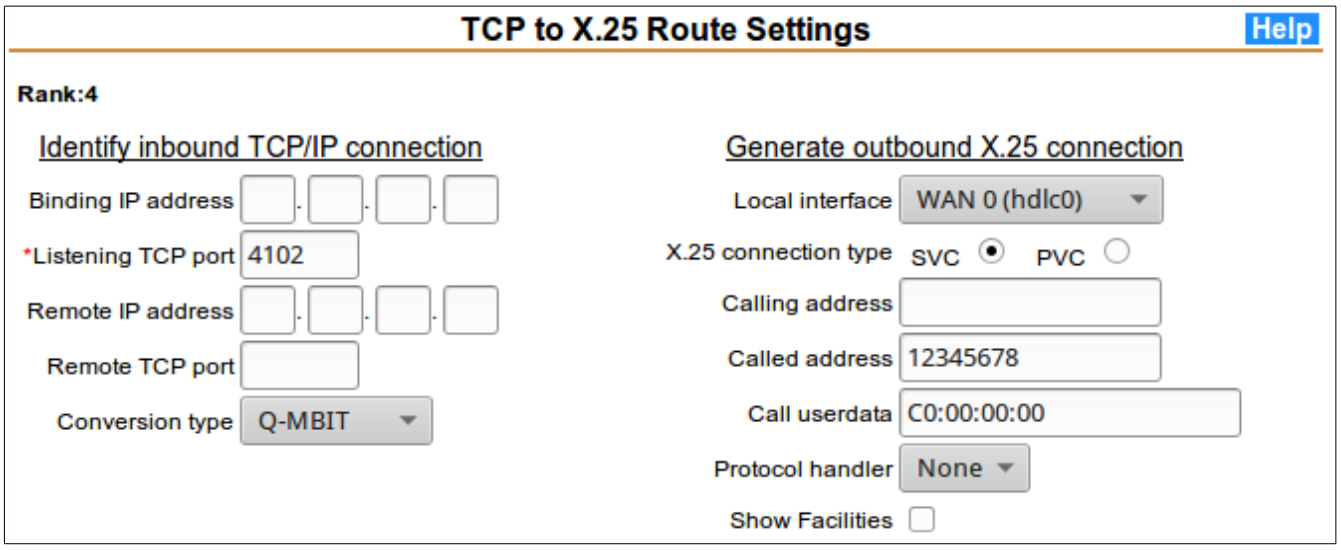
3.2.12.3 Remote (external) X.25/TCP gateway

The collector connects via external TCP/IP to the remote X.25/TCP Gateway unit.



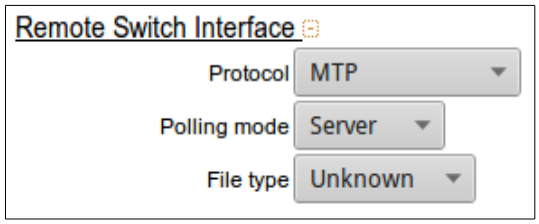
The **Remote IP Address** is set to the external IP network interface to address the remote gateway which connects to the X.25 interface of the switch. The TCP to X.25 route/map of the remote gateway must listen on the **TCP Port Number**.

If the remote X.25 gateway is a Microtronix X.25/TCP gateway, then the configuration would be similar to this example:



3.2.13 MTP Server (SFO) Configuration

Configuration for passive collection from the AXE switch consists of creating an SFO server (Session File Output) for accepting files from the switch's MTP client. Select **Protocol** MTP and **Polling mode** Server.



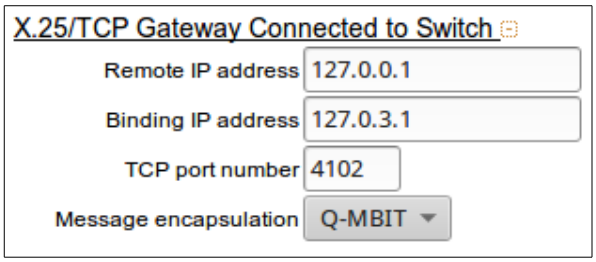
The **File type** may be used to scan files for format errors.

At the scheduled poll events, any new files are processed and put into the file forwarding subdirectory for transfer to the billing/mediation server.

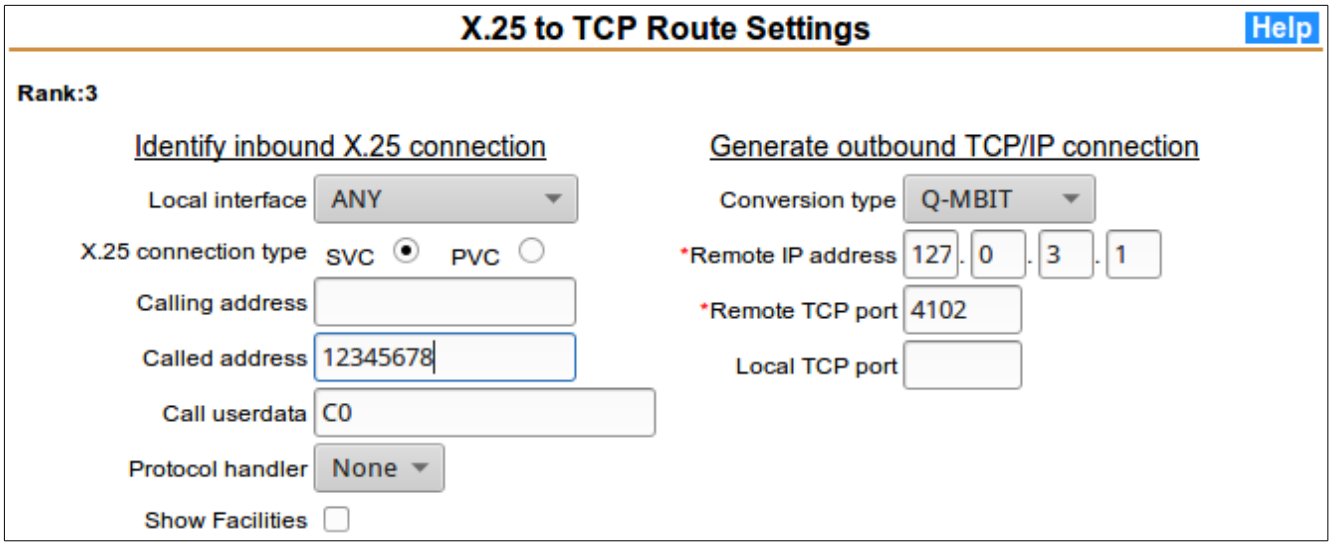
3.2.13.1 Local (internal) X.25/TCP gateway

The switch connects via the local X.25/TCP Gateway to the MTP collection server.

Enter the local listening TCP port number in the **TCP Port Number** field of the **X.25/TCP Gateway** section. The TCP port may be bound to the local IP interface to restrict access or avoid TCP conflict. For monitoring purposes, the Remote IP address is set to 127.0.0.1.



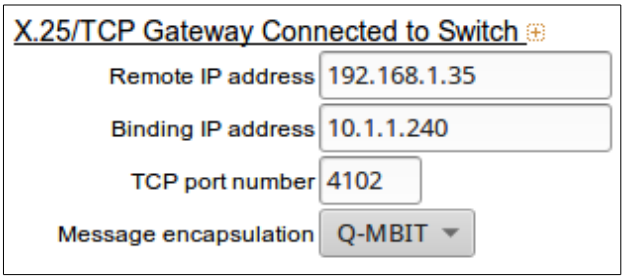
The X.25 to TCP route's TCP/IP destination, and the encapsulation/conversion (Q-MBIT) must match.



3.2.13.2 Remote (external) X.25/TCP gateway

The switch connects via an external X.25/TCP Gateway to the MTP collection server.

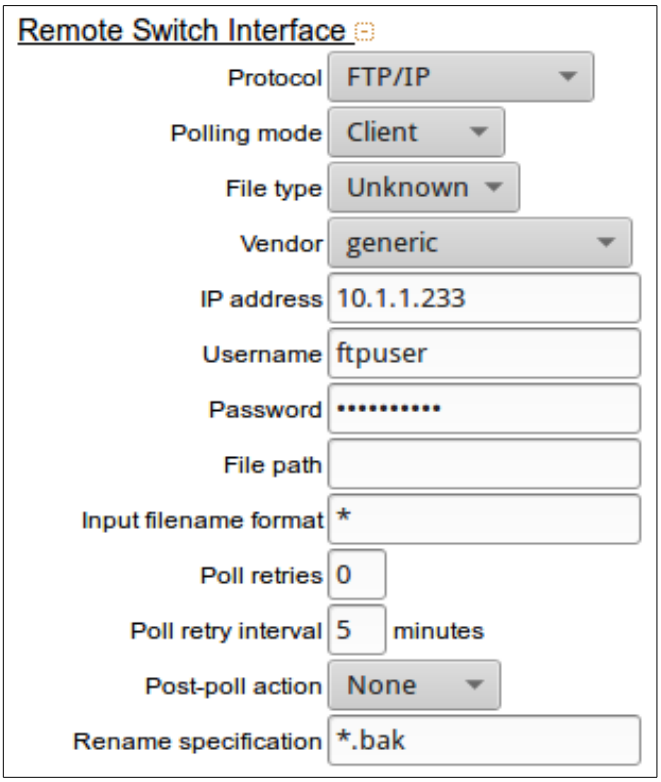
Enter the local listening TCP port number in the **TCP Port Number** field of the **X.25/TCP Gateway** section. The listening TCP port number may be bound to the local IP interface to restrict access or avoid TCP conflict.



The **Message Encapsulation** must be set for a type that supports X.25 Q-bit packets like Q-MBIT, QRBP, or AEPN. These must agree with the setting in the X.25 to TCP Routing table corresponding to the incoming X.25 connection. The **Remote IP address** of the external X.25 gateway may be entered for monitoring purposes.

3.2.14 FTP/IP Client Configuration

Configuring for collection from a legacy CO or soft switch consists of creating a client for pulling files from the switch's FTP server. Select **Protocol** FTP/IP and **Polling mode** Client. The X.25/TCP Gateway parameters are not used.



Fill in the **IP Address, Username,** and **Password** fields for logging into the remote switch.

Vendor identifies the manufacturer of the switch or the system type to choose the specific FTP client behavior required.

File type may be used to identify the type of file pulled from the switch, for example AMATPS. This may be used for scanning the file content or converting to other formats.

The **File Path** field consists of a specific path if the files are not in the user's home directory.

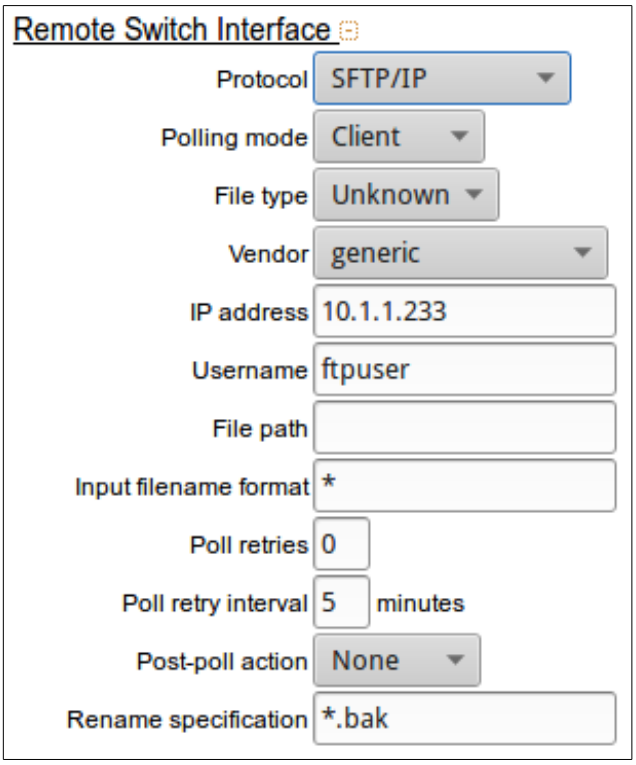
The **Input filename format** field consists of a file name, and can include a wildcard (* or ?), or sequence number specification (%#) for file lookup.

The **Poll Retries** field defines how many additional times an FTP pull operation is attempted after a failure.

The **Post-poll Action** parameter may be configured for **Delete** or **Rename** to cause the collection cycle to delete the file from the switch, or rename it using the **Rename Specification** parameter so that the file is no longer available for collection. If Rename is selected, the rename specification is used to rename the file, with the "*****" replaced with the original filename, and any date variables substituted accordingly (%Y, %y, %m, %d, %H, %M, %S). Setting to **None** allows the switch to leave the file available or perform an automatic rotation operation.

3.2.15 SFTP/IP Client Configuration

Configuring for collection from a legacy CO or soft switch consists of creating a client for pulling files from the switch's SFTP server. Select **Protocol** SFTP/IP and **Polling mode** Client. The X.25/TCP Gateway parameters are not used.



Fill in the **IP Address** and **Username** fields for logging into the remote server.

Password-less login is used, so the ***CM***'s SSH public authentication key must be installed on the remote server. This can be done by logging into the ***CM***'s command line interface and issuing one of these commands as a root user:

```
# ssh-copy-id -i /.ssh/id_rsa.pub username@IPaddress
# ssh-copy-id -i /root/.ssh/id_rsa.pub username@IPaddress
```

Enter the remote user password when prompted.

Check the key by logging into the remote server with the command:

```
# ssh username@IPaddress
```

It should successfully login with asking for password.

Vendor identifies the manufacturer of the switch or the system type to choose the specific SFTP client behavior required.

File type may be used to identify the type of file pulled from the switch, for example AMATPS. This may be used for scanning the file content or converting to other formats.

The **File Path** field consists of a specific path if the files are not in the user's home directory.

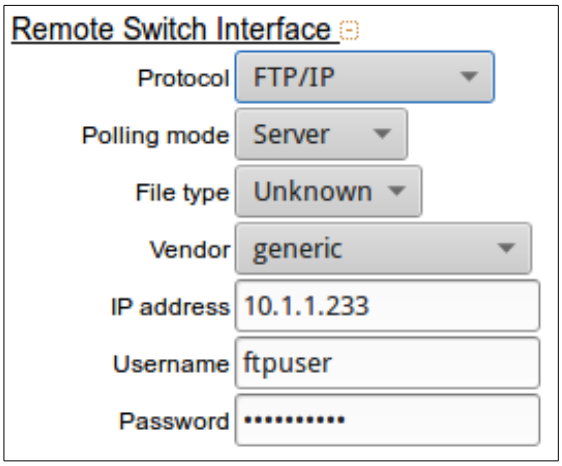
The **Input filename format** field consists of a file name, and can include a wildcard (* or ?), or sequence number specification (%#) for file lookup.

The **Poll Retries** field defines how many additional times an SFTP pull operation is attempted after a failure.

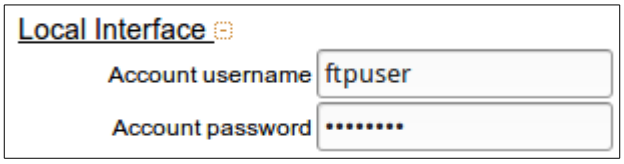
The **Post-poll Action** parameter may be configured for **Delete** or **Rename** to cause the collection cycle to delete the file from the switch, or rename it using the **Rename Specification** parameter so that the file is no longer available for collection. If Rename is selected, the rename specification is used to rename the file, with the "*****" replaced with the original filename, and any date variables substituted accordingly (%Y, %y, %m, %d, %H, %M, %S). Setting to **None** allows the switch to leave the file available or perform an automatic rotation operation.

3.2.16 FTP/IP & SFTP/IP Server Configuration

Configuring for collection from a legacy CO or soft switch consists of creating a server for receiving files from the switch FTP or SFTP client. Select **Protocol** FTP/IP or SFTP/IP and **Polling mode** Server. The X.25/TCP Gateway parameters are not used.



Fill in the **Account Username** and **Password** (FTP only) fields in the **Local Interface** section to match the remote switch's FTP/SFTP client so it can login and push files.



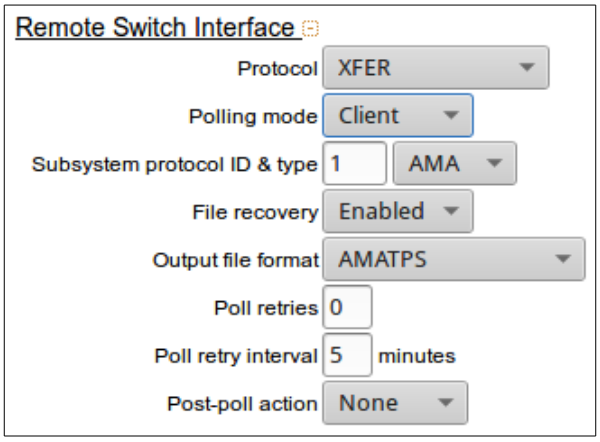
The **Remote IP address** of the switch is provided it can be used for status monitoring or manual client operations.

File type may be used to identify the type of file pulled from the switch, for example AMATPS. This may be used during file processing for scanning the file content or converting to other formats.

At the scheduled poll events, any new files pushed by the switch are processed and put into the file forwarding subdirectory for transfer to the billing/mediation server.

3.2.17 XFER Client Configuration

Configuring for collection from the switch consists of creating a client for pulling files from the switch's XFER file server. Select **Protocol** XFER and **Polling mode** Client.



The **Protocol ID** field must be set to a non-zero value to collect files and must correspond with the subsystem value expected by the switch for the type of file collected. The **Protocol Type** field must be set to the type of file. This should correspond with the subsystem ID type on the switch..

A collector configuration may be added for each of the file types: AMA, CDR, SMDR, OM, JF, ICMA, and DLOG.

Recovery of partial file retrieval due to connection problems is configured using the **File Recovery** parameter. Normally set to **Enabled**, but may be set to **Disabled** to always delete partial files and collect files from the start.

The **Output File Format** parameter specifies the output format or conversion of collected files. For example, blocked files may be converted to unblocked/streamlined, and AMA records may be converted to BAF.

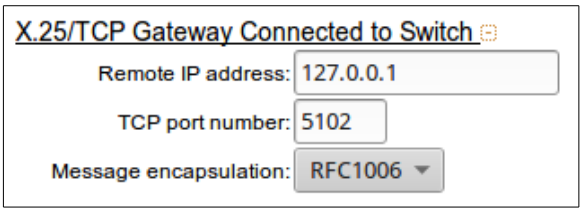
The **Poll Retries** parameter specifies the number of retries attempted after a first failure.

The **Post-poll Action** parameter should be configured for **Confirm** to cause the collector to confirm successfully collected files. The switch will automatically rotate the file so it is no longer available for collection. Setting to **None** causes the collector to not confirm the file so that the switch will leave the file available. This will cause the file to be retrieved at every poll interval, so should only be used for testing purposes.

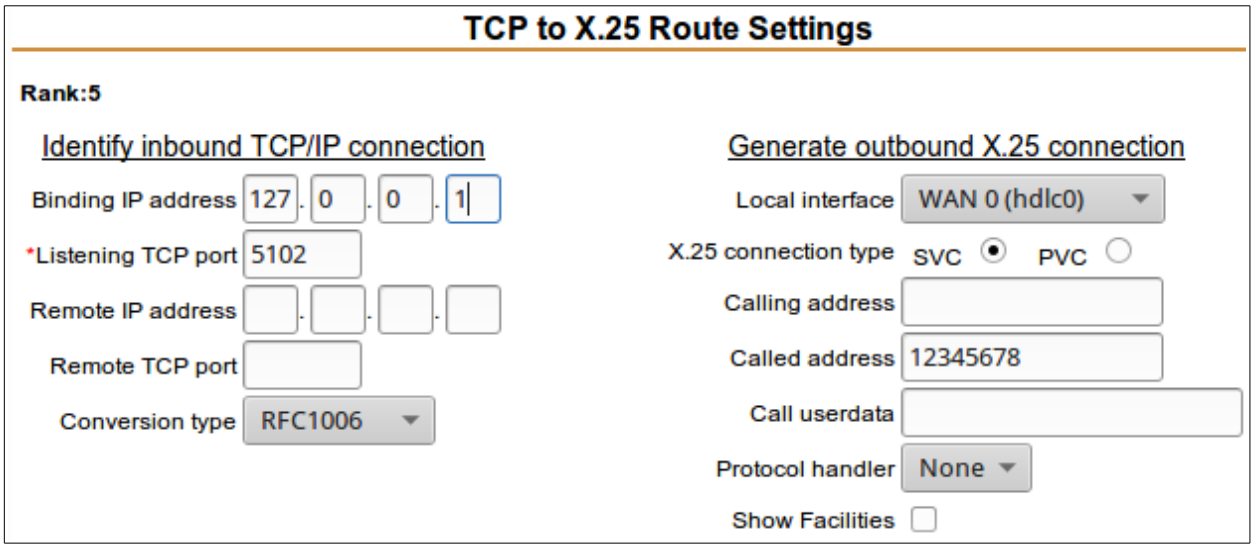
The **X.25/TCP Gateway** parameters are used by the collector to connect to the switch's X.25 interface via the local or a remote X.25/TCP gateway.

3.2.17.1 Local (internal) X.25/TCP gateway

The collector connects via local TCP/IP to the internal X.25/TCP Gateway application.

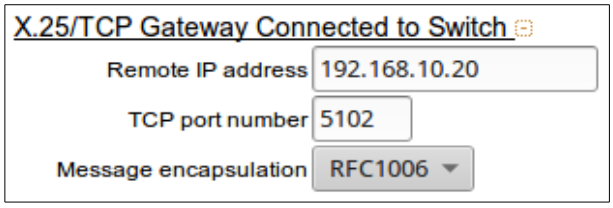


The **Remote IP Address** is set to the local IP network interface to address the local gateway which connects directly to the X.25 interface of the switch via a WAN interface. The **TCP to X.25 Routes** section of the internal gateway must listen on the **TCP Port Number** (and bind to the same local IP address).

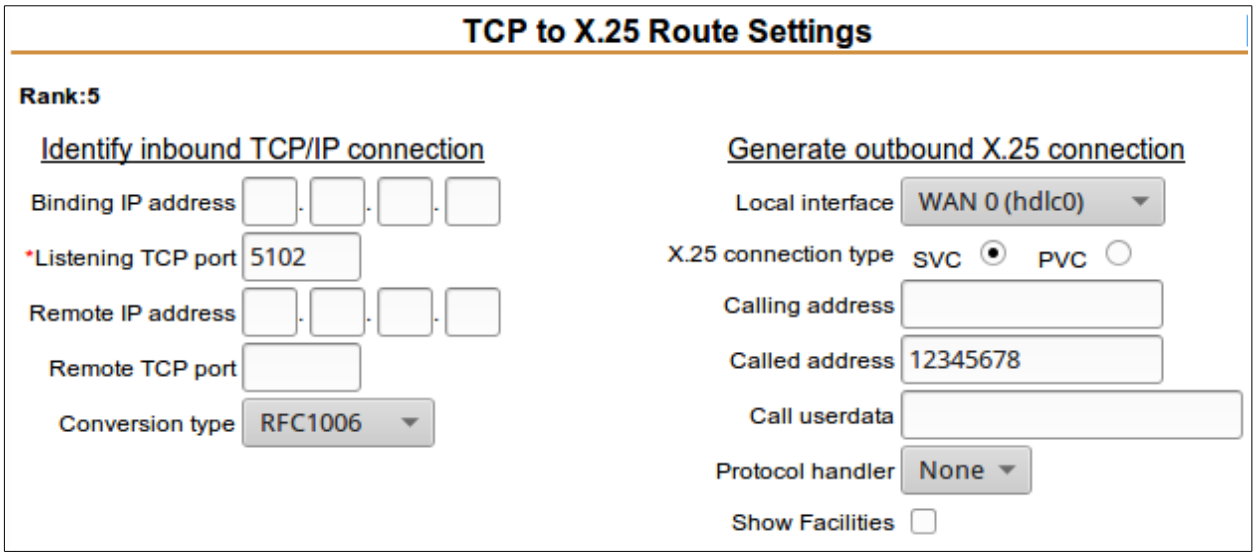


3.2.17.2 Remote (external) X.25/TCP gateway

The collector connects via external TCP/IP to the external X.25/TCP Gateway unit.



The **Remote IP Address** is set to the external IP network interface to address the remote gateway which connects to the X.25 interface of the switch via it's local interface. The TCP to X.25 route of the external gateway must listen promiscuously on the **TCP Port Number** (or bound to an external IP interface).



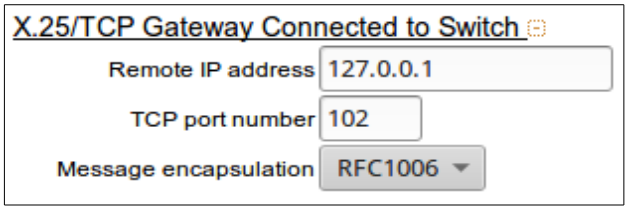
3.3 X.25/TCP Gateway Connected to Switch

The collector uses a TCP/IP socket to make a connection towards the switch via an X.25/TCP gateway that is connected to the switch's X.25 interface. The gateway may be an external X.25/TCP gateway unit, the internal X.25/TCP Gateway application, or the internal XOT Gateway application.

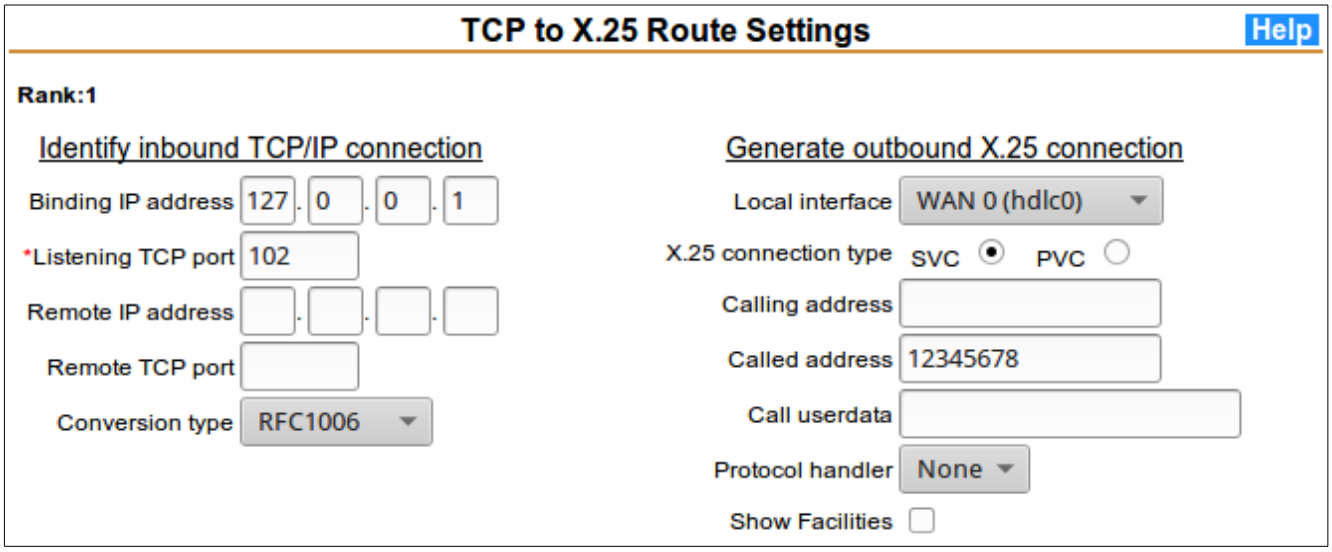
Message encapsulation methods specify how X.25 messages are preserved (encapsulated) over the TCP socket in order to delineate message boundaries. This method must be the same between the collector configuration and it's destination X.25 gateway.

3.3.1 Internal Access 1000/4000 X.25/TCP Gateway application

If the internal Access 1000/4000 X.25/TCP Gateway is used, the local X.25 interface(s) will be connected to the switch directly and must be configured accordingly (see the **X.25 WAN** sections).



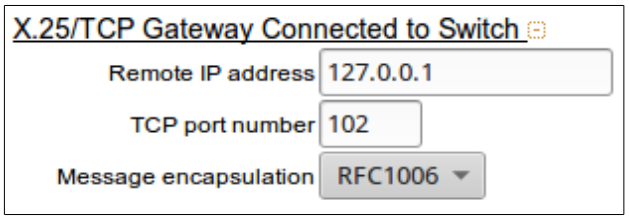
The **Remote IP Address** is set the local (loopback) address, and the **TCP Port Number** set to match the corresponding listening entry in the TCP to X.25 Routes. **Message encapsulation** must match **Conversion type**.



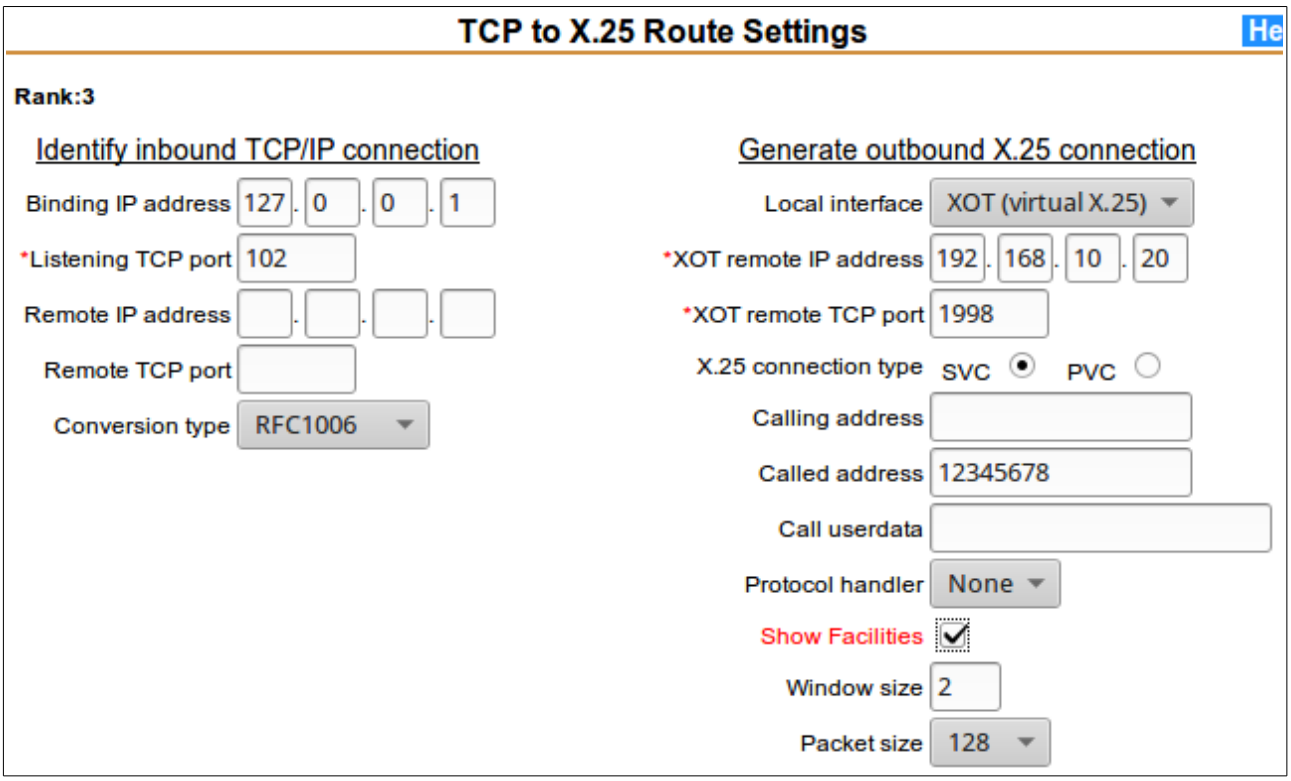
Message Encapsulation should match Conversion type. RAW should be used for BUFFER protocol. Q-MBIT should be used for AFT and MTP. Other protocols should use RFC1006.

3.3.2 Internal XOT Gateway application

If the internal XOT Gateway is used, it will use a virtual X.25 connections to a remote XOT gateway/router that connects to the switch's X.25 interface.

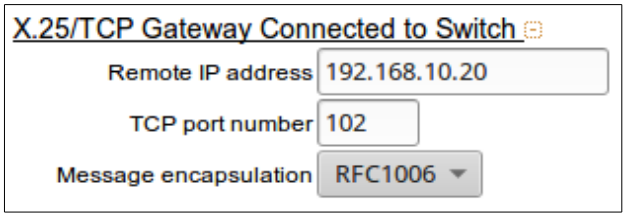


The **Remote IP Address** is set the local (loopback) address, and the **TCP Port Number** set to match the corresponding listening entry in the TCP to X.25 Routes. **Message encapsulation** must match **Conversion type**.



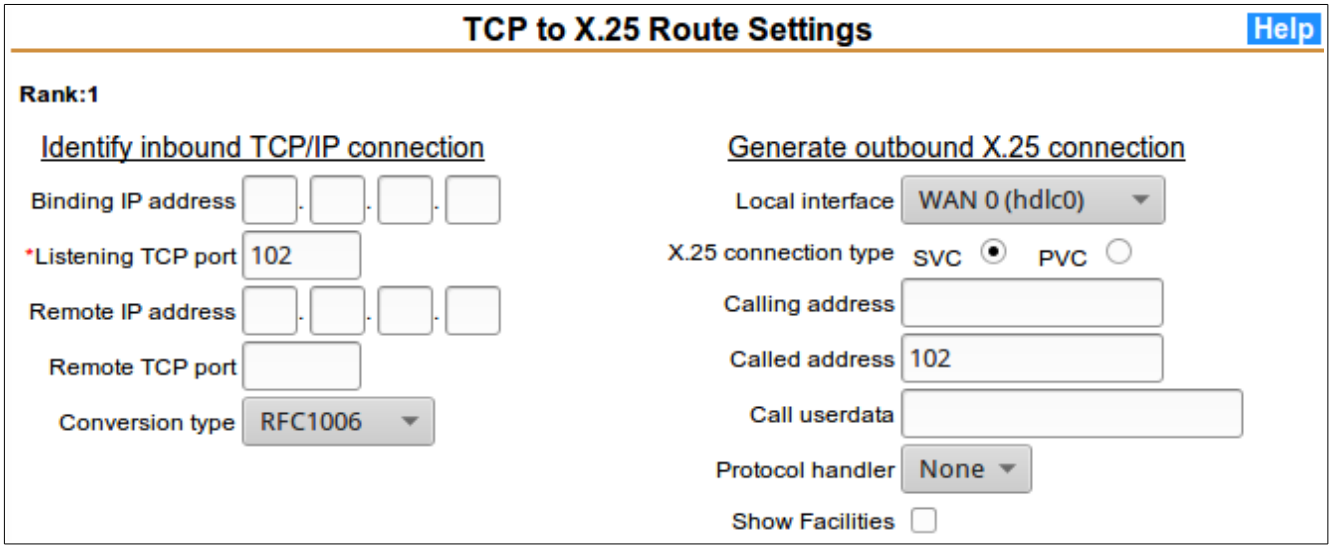
3.3.3 External X.25/TCP gateway unit

If an external gateway is connected to the switch's X.25 interface, then it's IP address must be used, for example 192.168.10.20.



The **Remote IP Address** is set the external address, and the **TCP Port Number** set to match the corresponding listening entry in the external gateway routing/mapping table. **Message encapsulation** must match the method supported by the remote gateway and specified in the route. Common methods include RBP, QRBP, and AEPN.

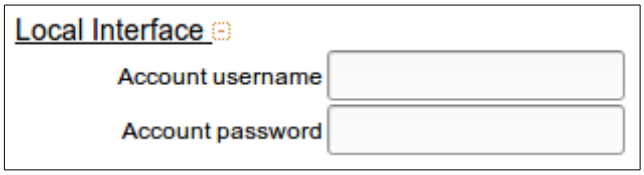
If the external X.25/TCP gateway is an Access 1000/4000, the TCP to X.25 route entry will be:



The **Binding IP address** should be blank to allow external requests on the listening TCP port. It could be bound to the external IP interface (example 192.168.10.20).

3.4 Local Interface

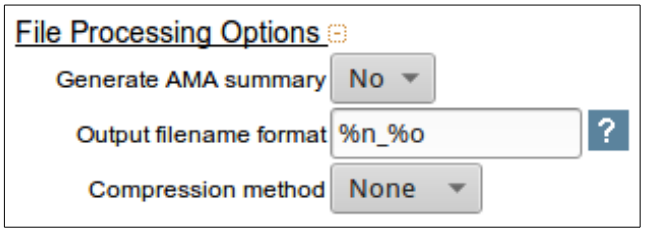
When creating a collector configuration, a local Linux user account will be created for remote clients to push files, or operators to login and manually poll or test the switch interface.



The **Account Username** and **Password** parameters are used to create a local Linux user account for this collector. This account will be used when the collector is configured as a **server** (FTAM, FTP/IP, or SFTP/IP) for the remote switch client to login and push files to the collector. If the Username field is left blank when adding a new collector, an account using the Network Element Name will be created. If not specified, the default Password will be the same as the Username. The account name and/or password may be subsequently changed by entering values into the fields.

3.5 File Processing Options

This section configures parameters for the collector side of the interface, and general polling parameters. Only fields and options relevant to the collector's protocol will be displayed.

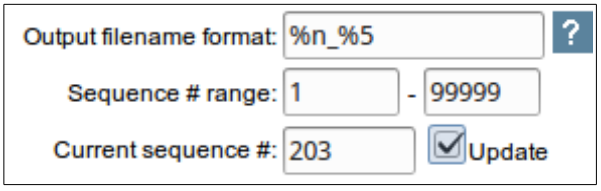


The **Generate AMA Summary** parameter will cause a summary file of AMA format files to be generated at a poll cycle.

The **Output Filename Format** parameter specifies how collected files can be renamed for local storage and forwarding. The parameter consists of a string containing text and replacement variables (%*V*) for adding sequence number and/or date/time components to the file name. This is mandatory if the collected filename is not unique.

If this field is left blank, the collected file will not be renamed. This is not recommended especially where the collected file name is not unique.

The **File Sequence Number** parameter allows the definition of the starting point for the sequence number replacement variable in **Output Filename Format**.



This is done during installation to set the sequence to match a prior collector, or any time that it needs to be changed. Remember to click the update button for the new number to take effect when the form is applied with the Add/Update button at the bottom. The **Sequence # range** parameters define the upper limit of the number, and the wrap to number (usually 0 or 1).

The **Compression Method** parameter specifies the compression or encryption method to be applied to collected files when stored.

3.6 File Forwarding Service

This section configures the parameters for forwarding/transferring the collected files to the mediation, billing, or other application client/server; or making the files available for external client applications.

If collected files are to be automatically forwarded to a remote application server, then a **client** (FTP or SFTP), or **Local** destination method must be chosen.

If the remote application server pulls files, then **Server** option should be chosen, but the **Passive** option may also be chosen.

The **Disabled** option has no automatic action, and assumes no external action. It will cause a poll to fail.

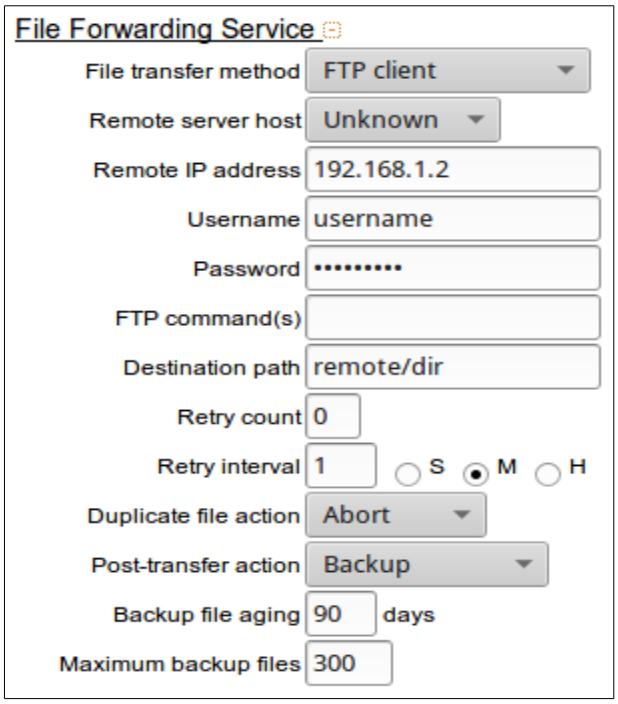
The **Backup file extension** parameter specifies the extension used by a remote client to rename files it retrieves. These renamed files will by moved daily into the backup directory where they will be subject to automatic aging according to the following paramaters.

The **Backup file aging** parameter specifies how many days files that have been moved into the backup archive (after successful forwarding) before they are removed from storage. Aging still occurs even when forwarding is disabled.

The **Maximum backup files** parameter specifies a limit on the number files stored in the backup directory. Aging and pruning occur during the daily log rotation scheduled event.

3.6.1 FTP Client

Choose FTP client to automatically forward files to a mediation/billing server.



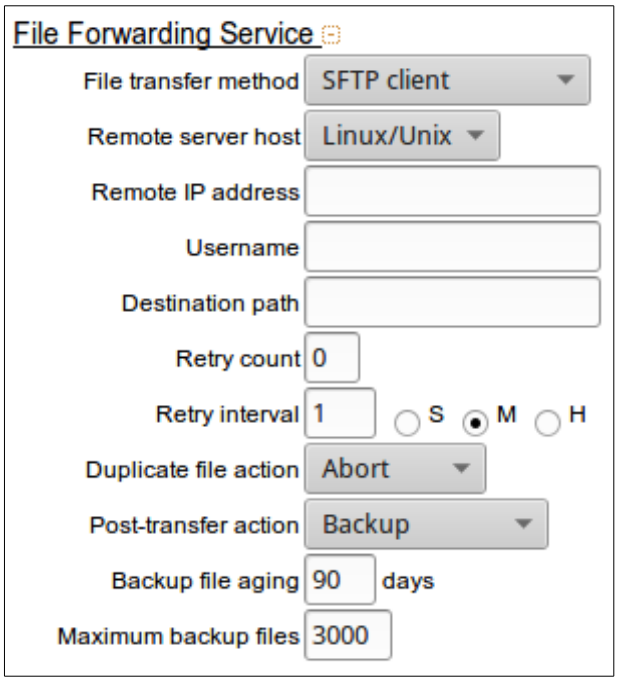
The **Remote server host** parameter specifies the O/S of the remote server in order that system-specific operation may be carried out. If Linux/Unix or Windows is chosen, then file size verification will be performed.

The **Duplicate File Action** parameter affects the action taken by the collector in case there is a file of the same name on the server. If set to **Abort**, the collector will not transfer the file, and leave it ready for transfer. If set to **Overwrite**, the collector will replace the file on the server with the new file. If set to **Rename**, a data/time stamp is added to the file before being transferred. If set to **Backup**, the collector will not transfer the file, but move it to backup in case it is needed later. If set to **Delete**, The collected file is deleted (NOT RECOMMENDED).

The **Post-transfer Action** parameter may be configured for **Delete** to delete the file, or **Backup** to save the file in the collector's `databackup` subdirectory. The **Gzip** and **GnuPG** backup options specify that the backup files are Gzip compressed or GnuPG encrypted.

3.6.2 SFTP Client

Choose SFTP client to automatically forward files to a secure mediation/billing server.



The **Remote server host** parameter specifies the O/S of the remote server in order that system-specific operation may be carried out. If Linux/Unix or Windows is chosen, then file size verification will be performed.

The **Duplicate File Action** parameter affects the action taken by the collector in case there is a file of the same name on the server. If set to **Abort**, the collector will not transfer the file, and leave it ready for transfer. If set to **Overwrite**, the collector will replace the file on the server with the new file. If set to **Rename**, a data/time stamp is added to the file before being transferred. If set to **Backup**, the collector will not transfer the file, but move it to backup in case it is needed later. If set to **Delete**, The collected file is deleted (NOT RECOMMENDED).

The **Post-transfer Action** parameter may be configured for **Delete** to delete the file, or **Backup** to save the file in the collector's `databackup` subdirectory. The **Gzip** and **GnuPG** backup options specify that the backup files are Gzip compressed or GnuPG encrypted.

When configured for SFTP client, the **Password** field is not used. Instead, the ***CM***'s SSH public key must be installed in the authorized keys file in the user home directory on the server.

The SSH public key may be retrieved from the ***CM*** at the path:

```
/.ssh/id_rsa.pub
```

and the content added to the server file:

```
<home directory>/.ssh/authorized_keys2
```

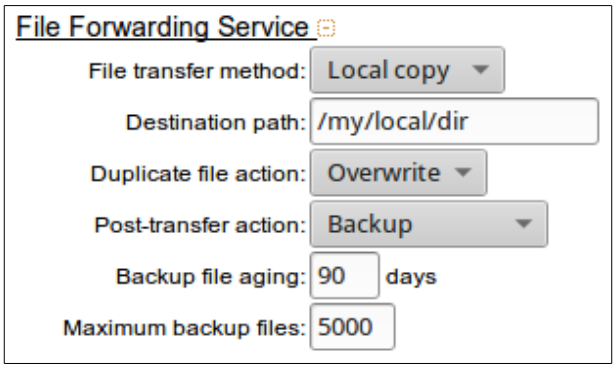
Once copied, the authentication needs to be completed by connecting from the ***CM*** to the server using the ssh command:

```
ssh <user>@<serverIP>
```

answer “yes” if and when prompted to continue.

3.6.3 Local Copy

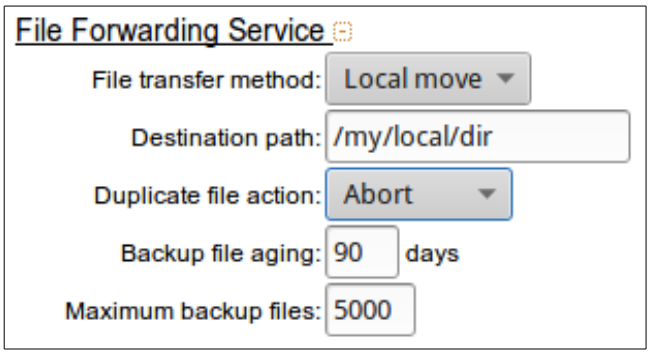
If collected files are to be automatically copied to a local directory of the user's choice, then select **Local copy** and enter the local directory to which collected files are to be copied.



The user is responsible for creating the local directory, and any further action on the files once they are moved. On the Access 1000/4000 platform, the local directory must be on the mounted USB 2.0 flash drive located at "`/mnt/usb1/`" or via soft link "`/var/lib/acm/`".

3.6.4 Local Move

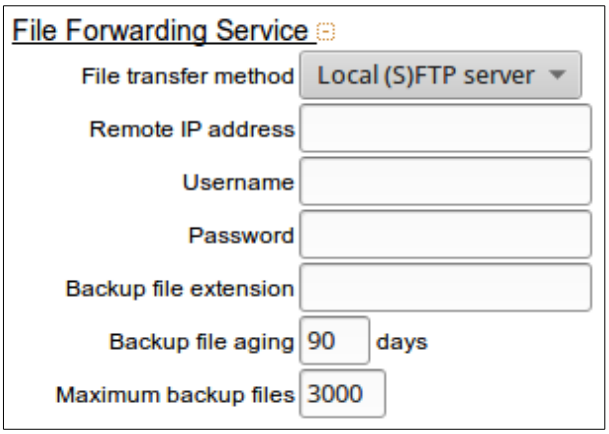
If collected files are to be automatically moved to a local directory of the user's choice, then select **Local move** and enter the local directory to which collected files are to be moved. The file is removed from the collector's directory so is no longer subject to backup



The user is responsible for creating the local directory, and any further action on the files once they are moved. On the Access 1000/4000 platform, the local directory must be on the mounted USB 2.0 flash drive located at "`/mnt/usb1/`" or via soft link "`/var/lib/acm/`".

3.6.5 Local (S)FTP Server

If files are to be pulled by a remote client, the **Server** method should be chosen.



For **Server** operation, fill in the **Username** and **Password** fields to create a local user account into which the remote FTP/SFTP client can login and pull files. The **Remote IP address** of the remote client may be entered for monitoring purposes.

The remote client has the responsibility to manage the files, and prevent file duplication by renaming, moving, or deleting the files from the collector's data directory. Successfully retrieved files should be backed up to the directory:

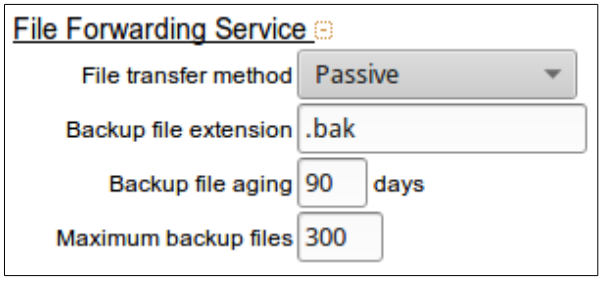
```
../databackup/
```

If the remote FTP client renames the files with a backup extension or suffix in the current directory, then the **Backup file extension** should be configured with that extension. Once a day (midnight), the file aging script runs and will move files matching the extension into the `../databackup/` directory.

Files moved to the `../databackup/` directory will be stored until deleted according to the aging and/or maximum files parameters.

3.6.6 Passive

Collected files made available for forwarding to a remote application will not be automatically forwarded, but remain in the collector's data directory until manually pushed to or pulled from a remote server. Poll events will NOT report a failure, and will exit with a normal condition.



It is entirely the user's responsibility to retrieve and dispense with the files so that the local storage drive does not fill up. The files may be deleted, moved to the backup directory for automatic aging, or renamed with an extension that matches the **Backup file extension** parameter for automatic aging.

3.6.7 Disabled (Not recommended)

Collected files made available for forwarding to a remote application will not be automatically forwarded, but remain in the collector's data directory. It is also assumed that no remote application is available for retrieving the files. Poll events WILL report and exit with a failure condition.

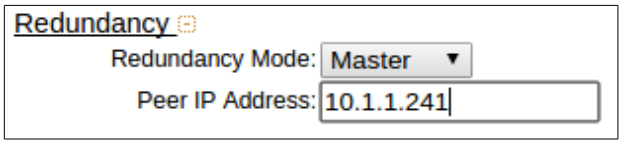
It is entirely the user's responsibility to retrieve and dispense with the files so that the local storage drive does not fill up. See Passive method above.

NOTE: This setting should only be used temporarily to prevent forwarding.

3.7 Redundancy

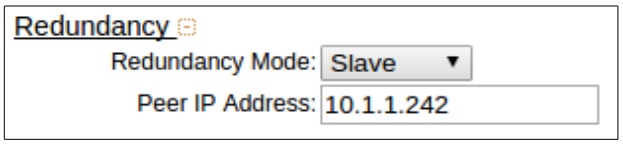
Each collector configuration can have a redundancy peer in case of failure. One collector is configured as the master and the other is configured as the slave. The master normally does the collection on one X.25 interface to the switch, and the slave connects to another X.25 interface to the switch but waits idly. If the master fails to collect for any reason, the slave takes over the collection.

Master configuration:



When Redundancy Mode is set for Master, the Peer IP Address is that of the slave unit backing it up.

Slave configuration:



When Redundancy Mode is set for Slave, the Peer IP Address is that of the master unit that it backs up.

The redundancy process uses a secure SCP connection to exchange status and any sequence number files used during collection. The public key of each unit must be installed in the authorized keys file of it's peer for password-less login. To locate each others files, both the slave and the master must have the same Network Element name, so that the underlying directory tree is the same.

Redundancy is only relevant for client configurations. A pair of units with server configurations can both be active at the same time. The switch itself would select one or the other of it's 2 interfaces.

3.8 Poll Schedules

When a collector is first added, a default polling schedule is created for midnight of the configured timezone. This schedule can be changed in the **Poll Schedules** page. If a collector configuration is deleted, the schedule is also deleted.

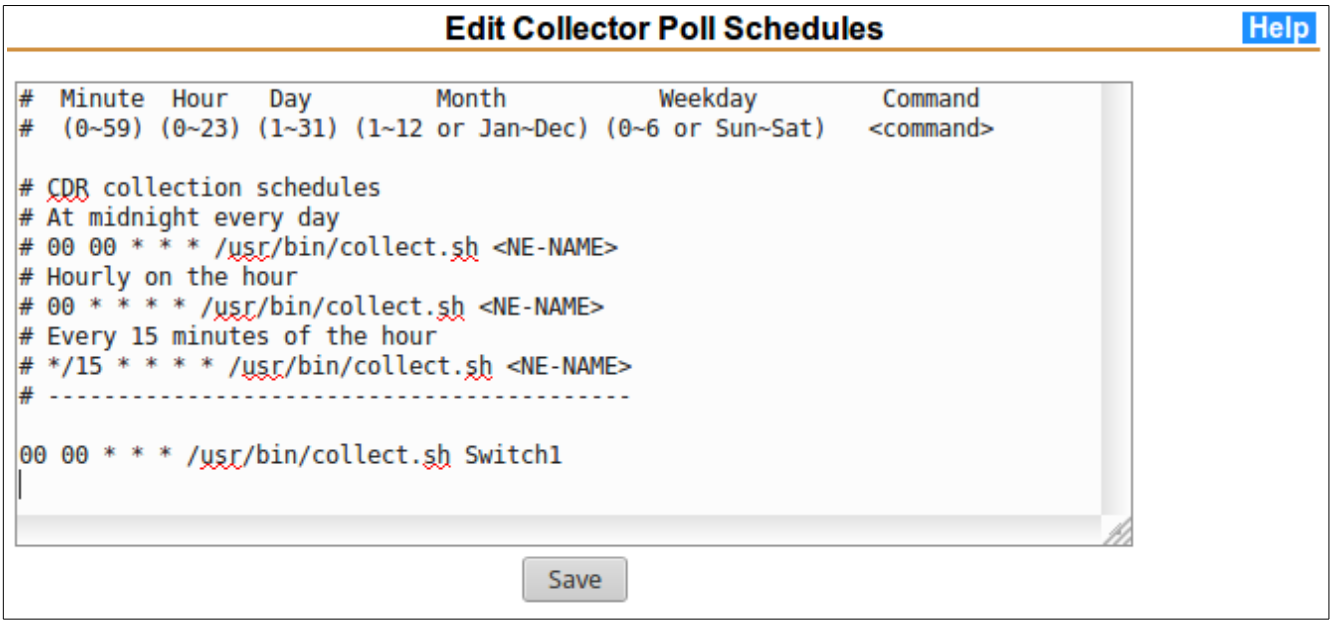
The Linux cron scheduler is used, and the **crontab** can be edited using this page.

3.8.1 Access 1000/4000 Collection Manager

The name and path of the polling script is: **`/usr/bin/collect.sh`**

It takes the collector name as it's single argument.

Note: It is recommended that an NTP server be defined in the **Date and Time** page to keep the collector's time coordinated.



In addition to collector schedules, file sequence number files used to sequence daily files may be reset by entering a midnight schedule to reset them. These files are in the collector's working directory. These should be placed BEFORE any midnight poll schedule. For example:

1) Reset output file sequence letter to A at midnight:

```
00 00 * * * printf A > /var/lib/acm/collector/Switch1/.seqltr 2>/dev/null
00 00 * * * /opt/acm/bin/collect.sh Switch1
```

2) Reset output file sequence number to 0 at midnight:

```
00 00 * * * printf 0 > /var/lib/acm/collector/Switch1/.sequencenumber 2>/dev/null
```

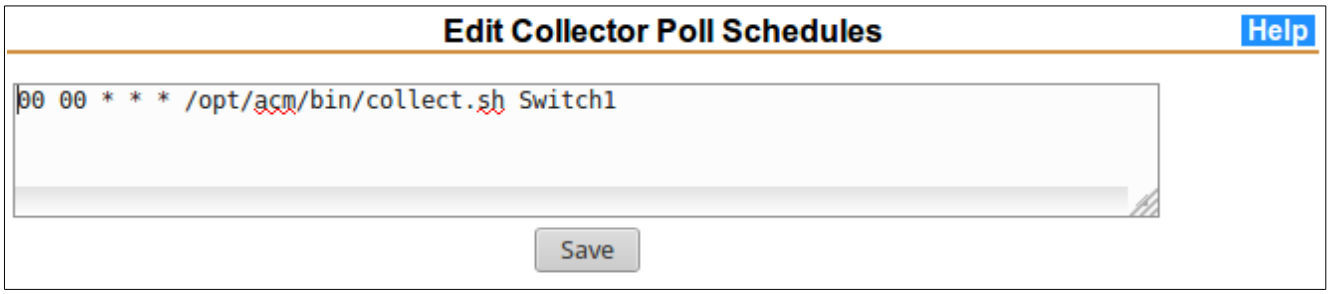
3) Reset input file sequence number 1 to 1 at midnight:

```
00 00 * * * printf 1 > /var/lib/acm/collector/Switch1/.sequencenumber1 2>/dev/null
```

3.8.2 x86 Collection Manager Server

The name and path of the polling script is: **`/opt/acm/bin/collect.sh`**

It takes the collector name as it's single argument.



The default collector working directory is:

`/var/lib/acm/collector/NENAME/`

Depending on the initial installation, this could be a different base directory:

`/`*`USERS`*`/`*`CHOICE`*`/acm/collector/NENAME`

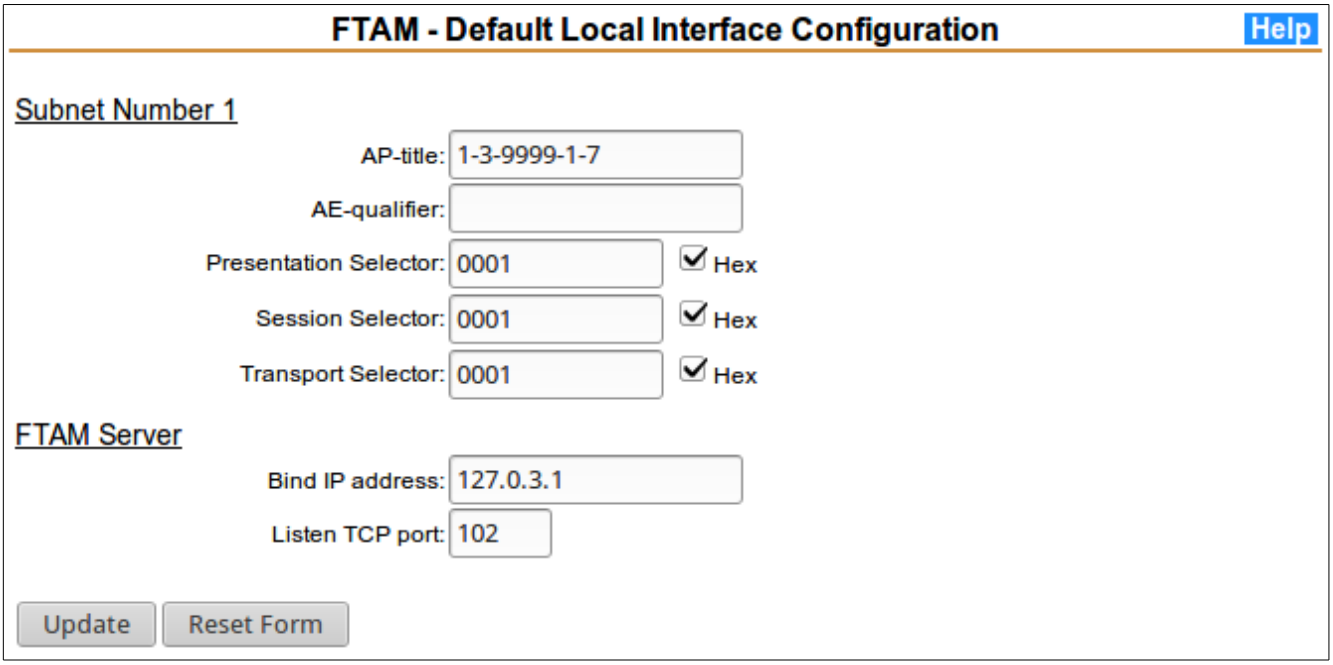
If sequence number resets are used, then the proper base directory must be used.

4 FTAM System Configuration (Access 1000/4000)

When the FTAM support package is installed, there are some local common OSI settings required for interfacing with remote FTAM switches.

4.1 FTAM Local Collector Interface

This section configures parameters for the collector side of the FTAM interface. These parameters will be sent to the switch as the source values.

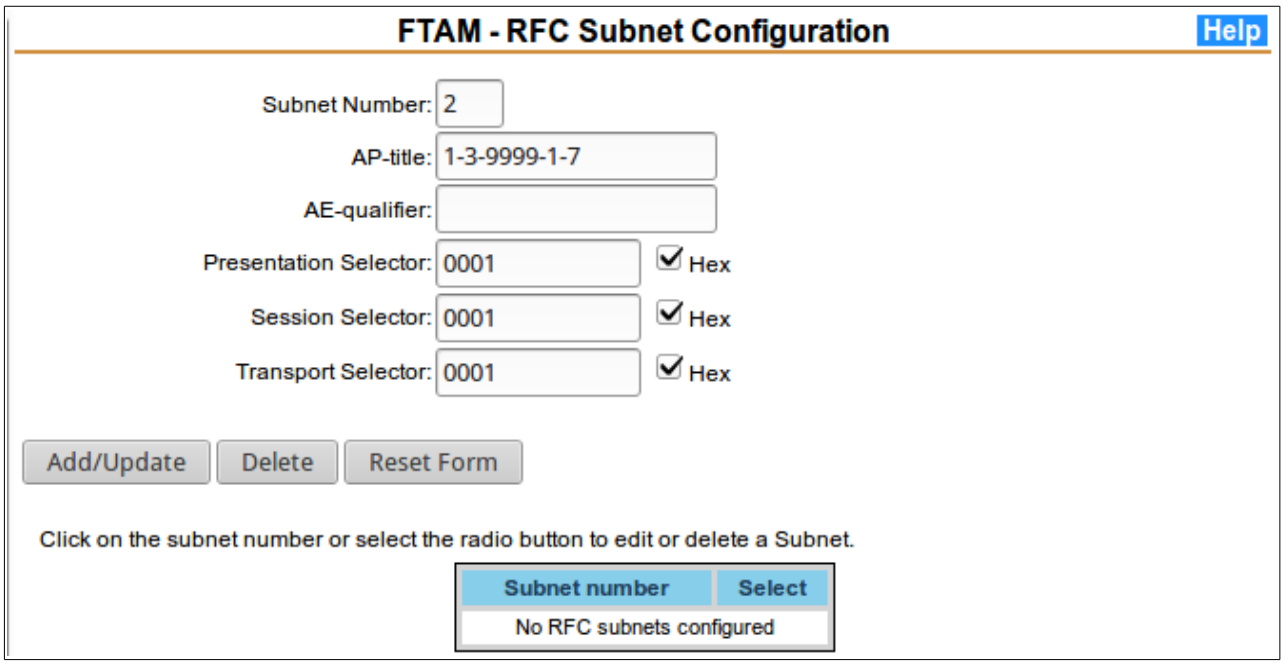


Fill in the **AP-title**, **AE-qualifier**, **Presentation** / **Session** / **Transport Selector** fields as expected by the switch. FTAM collectors will use this set of common parameters if their Subnet Address Index is set to 1. If an additional set of these parameters is required, then these can be defined in the following section, FTAM Subnets Configuration.

The **FTAM Server** section defines a common FTAM server using the **Bind IP address** and the **Listen TCP port** parameters. The initial values allow internal RFC1006/TCP connections from the X.25 Gateway. Remote FTAM switches can login and push files using a collector configured for FTAM Server polling mode.

4.2 FTAM Subnets Configuration

This section configures additional FTAM parameter sets for the collector side of the FTAM interface.



When the page is first displayed or Reset, the **Subnet Number** field contains the next available subnet number.

Fill in the **AP-title**, **AE-qualifier**, **Presentation** / **Session** / **Transport Selector** fields as expected by the switch. Click the **Add/Update** button to save these parameters under the Subnet Number displayed. FTAM collectors may use this set of common parameters if their Subnet Address Index is set to this Subnet Number.

To modify an existing subnet, select the desired subnet number in the table at the bottom of the form. The selected subnet will be displayed for editing. Click on the **Add/Update** button when changes are complete.

To delete an existing subnet, select the desired subnet number in the table at the bottom of the form. The selected subnet will be displayed. Click on the **Delete** button to remove the subnet.

5 TCP to X.25 Routing Configuration

If the CDR Collection Manager is polling the switch for CDR/AMA files, then it initiates the X.25 connection by issuing a localhost (127.x.x.x) TCP connection to the internal X.25 gateway. The parameters for the X.25 connection to the switch are specified in the TCP to X.25 Route section. There is a pre-defined route that can be edited for some X.25 specifics like called/calling addresses

To add or modify a TCP to X.25 mapping entry to the routing table, select **TCP to X.25 Routes** in the **X.25 Gateway** section of the main menu to display the configuration form and current TCP to X.25 routes. If modifying an existing route, select the Edit button to the right or the entry in the table below the form.

A backup X.25 link may be configured by adding a second entry with the same listening TCP port, and a different destination interface. The other outbound connection information may be the same or different. For example, the primary X.25 link may be WAN 0 (hdlc0), and the backup link may be WAN 1 (hdlc1), or a link on a remote X.25 gateway by selecting the XOT interface.

5.1 Identify inbound TCP/IP connection

Identify the TCP/IP parameter(s) that will be used to match the incoming connection from the collector(s). These MUST match the value in the X.25 Gateway CDR Collector configuration page.. Fill in the left side of the form:

1) Specify the TCP port configured in the X.25 Gateway section of the CDR Collector configuration page in the Listening TCP Port field. Usually port 102.
2) In the Remote IP Address field, enter the localhost address, 127.0.0.1, for connection to WAN 0.

5.2 Conversion or Encapsulation Method

Choose from the drop-down list in the Conversion Type field, the method for this connection. This method MUST match the value in the X.25 Gateway CDR Collector configuration page.

1) Q-MBIT/QRBP/AEPN when the polling protocol is AFT or MTP.
2) RFC1006 when the polling protocol is AMATPS, EADAS, FTAM, or XFER

5.3 Generate outbound X.25 connection

Specify the X.25 parameters used to connect to the switch. Fill in the right side of the form:

1) Select the interface connected to the X.25 interface of the switch (WAN 0 or 1). If the switch is connected to a remote router providing X.25 Over TCP encapsulation, select XOT and specify the IP address of the remote router.
2) Choose the connection type (usually SVC, but AMATPS and EADAS use PVCs)
3) Specify the called and calling X.25 addresses to be used in the outbound call request or the PVC logical channel number to be assigned (AMATPS uses PVC 1, EADAS uses PVC 2,3, ...).
4) If SVC, specify user data and facilities as required. FTAM may require Called/Calling Address extension DTE facilities.

Add the new entry to the displayed table at the bottom by clicking **Add Entry**.

Update the existing entry in the displayed table at the bottom by clicking **Update Entry**.

Click on **Save and Apply Changes** button for the entry to be saved and become active.

For additional information, click the **Help** button on the page.

5.4 Default TCP to X.25 Routes

TCP to X.25 route defaults by switch polling protocol						
	AMATPS	**DCO**	**EADAS**	**FTAM**	**MTP**	**XFER**
Listening TCP	1102	7102	2102	102	4102	5102
Binding IP	127.0.0.1	127.0.0.1	127.0.0.2	127.0.0.1	127.0.0.1	127.0.0.1
Conversion	RFC1006	RFC1006	RFC1006	RFC1006	Q-MBIT	RFC1006
WAN interface	WAN 0	WAN 0	WAN 1	WAN 0	WAN 0	WAN 0
Connection type	PVC	SVC	PVC	SVC	SVC	SVC
Local LCN (PVC)	1	n/a	2,3,...	n/a	n/a	n/a
Called address	n/a		n/a	102	4102	5102
Calling address	n/a		n/a			
Call User Data	n/a		n/a	03:01:01:00	C0:00:00:00	

6 X.25 to TCP Routing Configuration

If the switch initiates a CDR/AMA file transfer (supported features of AFT, FTAM, and MTP), then an X.25 to TCP routing must be configured to connect the inbound X.25 connection to the collection application via the localhost IP address.

To add an X.25 to TCP mapping entry to the routing table, select **X.25 to TCP Routes** in the **X.25 Gateway** section of the main menu to display the configuration form, and current X.25 to TCP route entries. An entry can be added to the X.25 to TCP Routing table, or an existing entry modified. If modifying an existing entry, click on the Edit button beside the entry in the table below the form.

6.1 Identify inbound X.25 connection

Specify the call request parameter(s) that will be used to identify the incoming X.25 call request. This is usually the local physical interface), and the X.25 called address. Fill in the left side of the form:

1) Select the interface on which the call request is going to be received (usually WAN 0)
2) Choose connection type: Switched Virtual Circuit
3) Enter destination X.25 address in the Called Address field

6.2 Generate outbound TCP/IP connection

Specify the TCP/IP host to which the call will be connected. Fill in the right side of the form:

1) Specify the loopback IP address (127.0.0.1) in the Remote IP Address field.
2) Specify the TCP port number on which the collector is listening in the Remote TCP Port field (usually 4102 – must match the Collector application configuration).

6.3 Conversion or Encapsulation Method

Choose from the drop-down list in the Conversion Type field, the method for this connection. This method MUST match the value in the X.25 Gateway CDR Collector configuration page.

1) Q-MBIT (for AFT and MTP protocols only)
2) RAW for (BUFFER protocol)
3) RFC1006 (recommended for all other collection protocols)

Add the new entry to the displayed table at the bottom by clicking **Add Entry**.

Update the existing entry in the displayed table at the bottom by clicking **Update Entry**.

Click on **Save and Apply Changes** button for the entry to be saved and become active.

For additional information, click the **Help** button on the page.

6.4 Default X.25 to TCP Routes

X.25 to TCP route defaults by switch polling protocol					
	AFT		**FTAM**	**MTP**	
WAN interface	ANY		ANY	ANY	
Connection type	SVC		SVC	SVC	
Called address	n/a		102		
Calling address	n/a				
Call User Data	C0		03	C0	
Conversion	Q-MBIT		RFC1006	Q-MBIT	
Remote IP address	127.0.3.1		127.0.3.1	127.0.3.1	
Remote TCP port	5102		102	4102	

7 Operation Guide

The web page menu contains options for manually operating the Collection Manager. The options include:

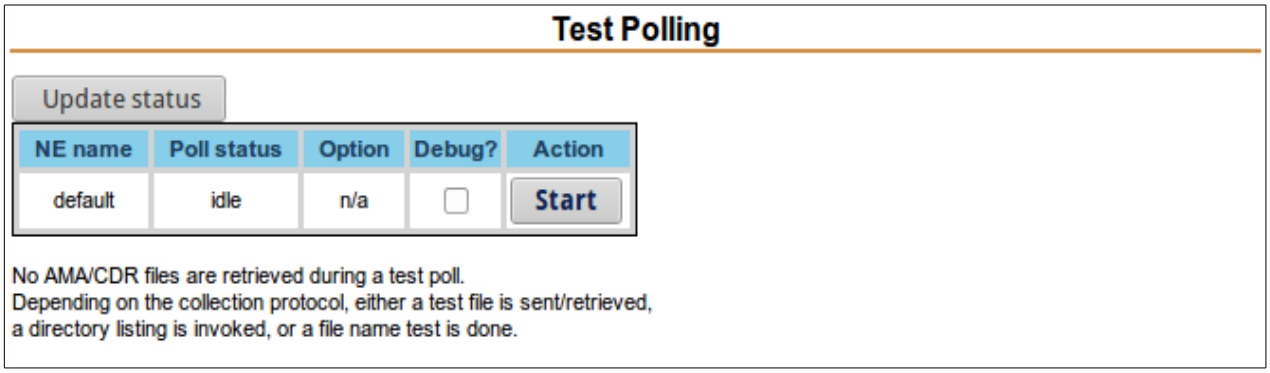
- manual testing and polling of switches
- testing of and forwarding files to file forwarding destinations
- managing backup files
- push/pull files from switches
- stating and stopping collection servers
- viewing logs
- starting the Collection Manager Monitor

7.1 Connect Test

A connection test may be done at any time after installation and configuration is complete. Connect tests retrieve special files or directory listings of the switch directory without actual file retrieval.

Before starting, make sure that the X.25 cable is connected and that the X.25 is operational by checking the X.25 status. Correct any issues before proceeding.

Open the **Connect Test** page and click on the Start button of the desired collector in the displayed table. Connection test are usually very quick (a few seconds), so if there is long delay, there may be a problem with the X.25 or CDR/switch configuration. If the test succeeds, a primary poll should work and can be done now, or can wait for the next scheduled poll event.



If the connection test fails, there is probably an issue with the X.25 configuration, the X.25 gateway routing, or the NE switch configuration. Check the system log for possible cause of failure. If the cause cannot be readily identified, it may be necessary to monitor the X.25 exchange between the switch and the collector.

To monitor the X.25 traffic, open a Telnet or SSH session to the ***CM***. It is best to log the session with the appropriate option when invoking Telnet. When prompted, login using “root” and password “f0adA”. Enter the following command at the “#” prompt:

```
# x25trace hdlc0
```

Start the connect test again, and observe the trace output. It is beyond the scope of this document to provide protocol analysis, so if required, the output can be captured and sent to Microtronix support for analysis. For the second X.25 link, use **hdlc1**.

To monitor the internal TCP/IP localhost (loopback) connection, enter the following commands:

```
# cd /tmp

# tcpdump -i lo -w cm.pcap tcp port 102
```

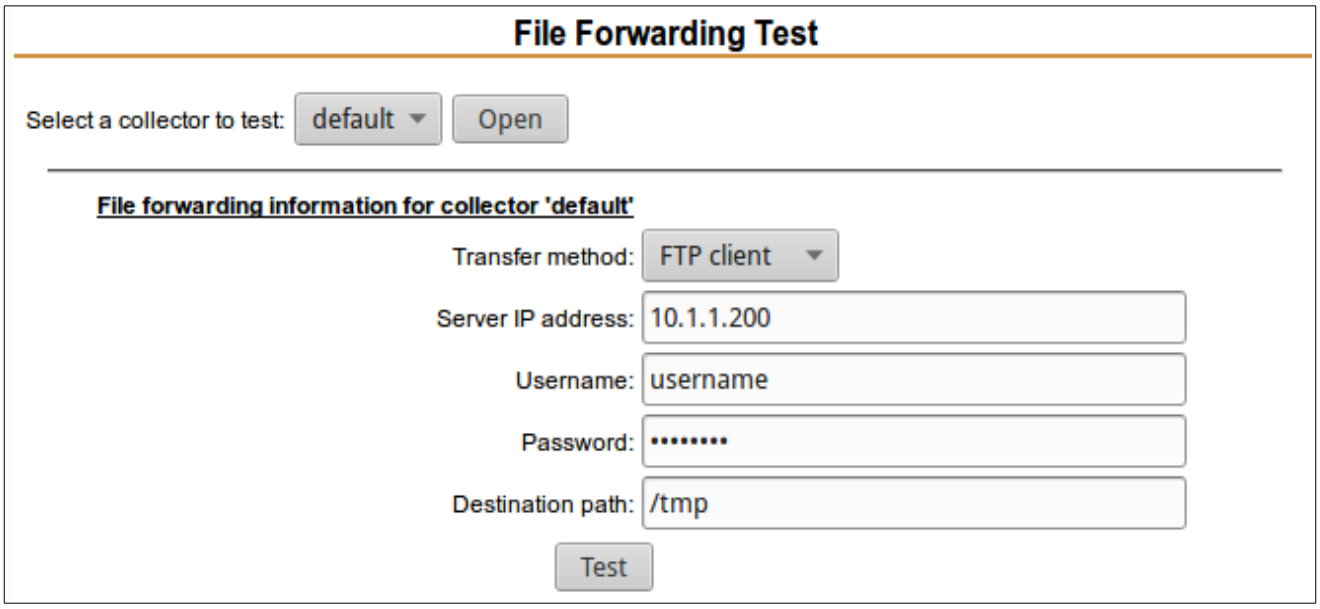
Type CTRL-C to stop the trace. Only run the trace for a short time as the “tmp” file system may fill. The file may be pulled from the ***CM*** using FTP, SFTP, or SCP. The file may also be pushed to a PC or file server using SFTP or SCP:

```
# scp cm.pcap USER@IP-ADDRESS:[DIRECTORY]
  <enter password>
```

Run Wireshark on the PC to view the capture. Especially useful for viewing interpreted FTAM messages.

7.2 File Forwarding Test

Once the File forwarding parameters are configured, the FTP/SFTP client or Local copy service can be tested by opening the **File Forwarding Test** page. Select the collector by it's name and click **Open**. A form with the defined parameters will be displayed and may be edited for temporary values.



Click the **Test** button to start the file transfer test. A test file will be pushed to the server, then pulled back for comparison.