Microtronix
Collection Manager
Application Notes 0.10.4

File Transfer Options

AMATPS • AFT • DCO • XFER

FTAM • FTP • MTP • RAW

Local storage

FTP • SCP • SFTP • NFS
HTTP(S) up/download

X.25 • sync • serial • IP

Legacy Switch

Access 4000
Collection Manager

IP

Client/Server
Application
Processor
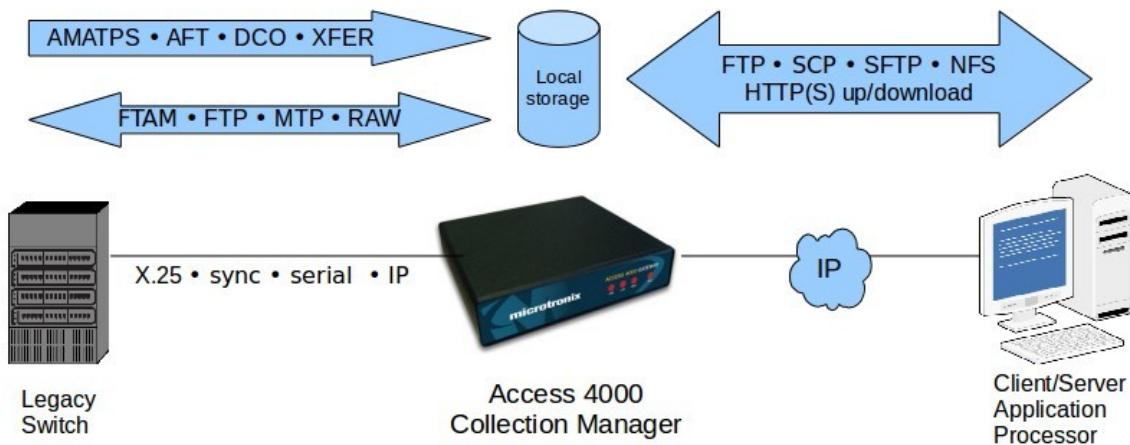
Microtronix Datacom Ltd.
4056 Meadowbrook Drive, Unit 126
London ON N6L 1E3
CANADA

www.microtronix.com

Tel: +1 519 690-0091
Fax: +1 519 690-0092

General Inquiries: info@microtronix.com
Sales Inquiries: sales@microtronix.com
Customer Support: support@microtronix.com

Table of Contents

1 Overview

The **Microtronix Collection Manager (CM)** polls legacy Central Office (CO) voice switches for files containing CDR, AMA, EADAS, SMDR, and other system data over X.25, serial, using the polling or file transfer protocol supported by the switch. Collected files are then forwarded to an IP-based host using FTP or SCP/SFTP. This process is automated via timed scheduling. Manual procedures are also available.

2 System Resources

The CM platform is based on the Linux operating system. Most basic system commands are implemented.

2.1 Command Line Interface

The *busybox* shell provides the command line interface and scripting language. It is compatible with bash and other shells with some restrictions and variations.

2.2 Legacy switch protocols

The CM includes legacy file transfer protocols that are used for connecting to the switch over X.25 (or IP) interfaces:

AMATPS – client collection of AMA files from Bellcore-compatible switches

AFT – server collection of AMA files from Nortel DMS switches

FTAM – generic client/server protocol for transferring files over X.25 or RFC1006/TCP

FTP – generic client/server protocol for transferring files with IP-based softswitches

MTP – generic Ericsson AXE client/server protocol for transferring files and establishing CLI

XFER – client collection of AMA files from Nortel DMS switches

FTP, FTAM, and MTP are generic protocols that support bi-directional file transfer of both billing (CDR) and system files. The CM supports both client and server modes of these protocols.

2.3 SSH/IP protocols

The CM supports the full suite of SSH protocols:

SSH client/server remote access

The SSH server allows remote clients to login and access the command line interface of the CM, or issue commands to be run on the CM command shell. The client allow that capability for a CM user.

SCP client/server file transfer

The SCP and SFTP server allows remote clients to provide user credentials to push/pull user files. The client is used by the CM to push/pull user files.

File transfers initiated by a script on the CM require public key authentication. This requires that it's public key be shared appropriately. On a command line of the CM, issue the following commands:

```
ssh-copy-id remoteUser@remoteIP
```

where:

remoteUser is the user name on the remote system whose home directory contains the shared files

remoteIP is the IP address of the remote system with an ssh daemon running

Enter the remote user's password and answer "yes" to the prompt to continue. Exit the session, and login again to verify.

For file transfers initiated by remote ssh clients, it is at the discretion of the user to decide if login or public key authentication is used.

2.4 Synchronous and X.25 interface tracing

There are command line utilities for tracing the CM's WAN interfaces. WAN port 0 is referred to as "hdlc0", and WAN 1 is referred to as "hdlc1".

For non-interpreted, tracing use:

```
hdlctrace hdlc0
```

which will trace and display the data of all frames in hexadecimal encoding.

For interpreted LAPB (layer 2) tracing, use:

```
hdlctrace -l hdlc0
```

and for interpreted X.25 (layer 3), use:

hdlctrace -x hdlc0.

For X.25 tracing without the lower level LAPB control frames, use:

```
x25trace hdlc0
```

To display the X.25 data packet contents in ASCII, use:

```
x25trace -a
```

2.5 tcpdump

The standard, open source, tcpdump utility can be used to do raw, filtered capture of either the external Ethernet or internal loopback interface. External man pages describe it's usage.

In general, tcpdump is used for capturing a problem with an application on the CM which usually involves a TCP port like an interconnection between an X.25 interface and a TCP port.

Once the TCP port number (and/or IP address) has been determined as the trace target, run the tcpdump utility to do a capture or display:

```
tcpdump -i dev [-w /mnt/usb1/tmp/mydump.pcap] tcp port <TCP#>
```

where dev=lo for the loopback/internal IP interface, and dev=eth0 for the external Ethernet/IP interface.

3 Application Notes

There are any number of ways that system resources can be utilized to realize an application on the CM. The command line interface provides most of the primitives to build simple to complex procedures and applications. Some common examples follow.

3.1 Manual file transfers between SCP/SFTP client and legacy switch

The CM acts as a store&forward intermediary for transferring files between a legacy switch and an SSH client, not as a protocol translator. So, it is necessary to perform 2-step file transfers when initiated by an SSH (SCP/SFTP) client using commands.

Pulling a file from the switch:

From a command line interface or script on the client, enter the following command on one line:

```
ssh NEuser@CMip "fileget.sh NEname filename"

        && scp NEuser@CMIP:filename [localname]
```

The first part will run a remote command on the CM to do a file retrieval from the legacy switch into the NEuser's home directory, and if successful, the second part will transfer the file from local storage to the initiating client system.

Pushing a file to the switch

From a command line interface or script on the client, enter the following command on one line:

```
scp filename NEuser@CMip:newname

        && ssh user@CMip "fileput.sh NEname newname"
```

The first part will copy the file from the client's system to the CM user's home directory, and if successful, the second part will transfer the file from that directory to the legacy switch.

3.2 Tapping sync/X.25 interface for parameter & procedure discovery

The CM's X.25 interfaces may be used for "tapping" an existing interconnection between a legacy switch and application processor. The "tap" is created by connecting the switch to one WAN interface of the CM, and the application processor into the other WAN interface. The X.25 interfaces are configured for Sync Server operation, where one of the Sync Servers initiates a TCP connection to other. Data is then transferred between the 2 interfaces transparently, so that the legacy operation is unaffected.

The TCP interconnection between the 2 WAN interfaces can be traced using *tcpdump* during legacy operations. This capture can be reviewed later to determine parameters used for protocol setup, and the procedures used for conducting a legacy operation.

Setup:

For each WAN port, disable any other process (X.25, Terminal Server), and enable it's Sync Server with parameters to match the attached device. One Sync Server will be set for listen on a particular TCP port, and the other to initiate a connection towards that TCP.

Run the tcpdump with filter on the above TCP port and an output file to the USB-mounted flash drive.

```
tcpdump -i lo -w //mnt/usb1/tmp/mydump.pcap tcp port <TCP#>
```

Type ctrl-C to stop the trace, and transfer the file to a PC using WinSCP or FileZilla. Wireshark provides excellent display options for analyzing the dump file.

Once the parameters of the interface and the protocol procedures have been determined, the CM can be configured to replicate.

3.3 Shared X.25 interface for application migration

Sometimes it is desirable during a proof of concept mission, to allow the legacy processors to continue to function uninterrupted while providing access to the new system. This is accomplished in the same manner as the "tapping" above, except that the higher X.25 protocols are used instead of the low level sync driver. The X.25/TCP mapping of the X.25 gateway application is configured to route the original connections appropriately, but allowing the the CM to also route it's TCP connections. This allows the CM to stay connected while the POC is conducted from a remote location accessible via remote IP.