MCF3000 Series

Multi-channel Media Converters

MCF3300 Chassis

MCF3000/8LC Media Converter

MCF3000/8SP Media Converter

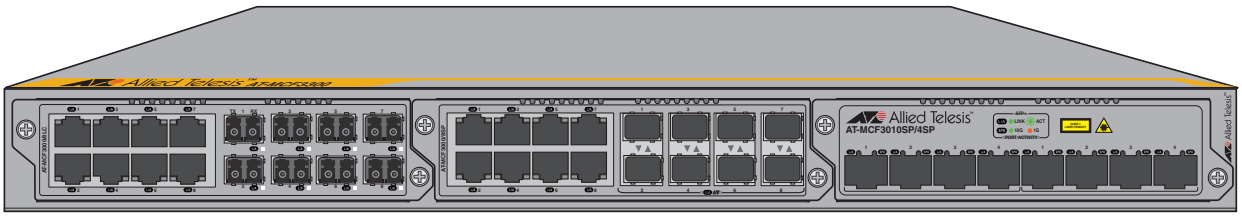
MCF3010SP/4SP Media Converter

MCF3010SPT/4SP Media Converter

MCF3000M Management Model

MCF3300AC Power Supply

MCF3300DC Power Supply



Software Release Notes

Version 2.0 (1027)

613-003370 Rev. A

Electrical Safety and Emissions Standards

This product meets the following standards.

US Federal Communications Commission

Radiated Energy

Note
This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Note
Modifications or changes not expressly approved of by the manufacturer or the FCC, can void your right to operate this equipment.

Industry Canada

Radiated Energy

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

RFI Emissions	FCC Class A, EN55032 Class A, EN61000-3-2, EN61000-3-3, VCCI Class A, ICES-003 Issue 6

Warning: In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

EMC Immunity	EN55024
Electrical Safety	EN62368-1 (CE), UL62368-1 ($_{C}UL_{US}$)

Warning
Laser Safety, EN 60825

Translated Safety Statements

Important: The ✍ indicates that translations of the safety statement are available in the PDF document **Translated Safety Statements** posted on the Allied Telesis website at **alliedtelesis.com/library/search**.

Übersetzte Sicherheitserklärungen

Wichtig: Das ✍ zeigt an, dass Übersetzungen der Sicherheitserklärung in den PDF-**Translated Safety Statements** auf der Allied Telesis-Website unter **alliedtelesis.com/us/en/library/search** verfügbar sind.

Declaraciones de seguridad traducidas

Importante: El ✍ indica que las traducciones de la declaración de seguridad están disponibles en las **Translated Safety Statements** en PDF publicadas en el sitio web de Allied Telesis en **alliedtelesis.com/us/en/library/search**.

Consignes de sécurité traduites

Important: Le symbole ✍ indique que les traductions de la déclaration de sécurité sont disponibles dans le PDF **Translated Safety Statements** publiées sur le site Web de Allied Telesis à l'adresse **alliedtelesis.com/us/en/library/search**.

Dichiarazioni di sicurezza tradotte

Importante: ✍ indica che le traduzioni della dichiarazione di sicurezza sono disponibili nelle **Translated Safety Statements** in PDF pubblicate sul sito Web di Allied Telesis all'indirizzo **alliedtelesis.com/us/en/library/search**.

Översatta säkerhetsförklaringar

Viktig: ✍ anger att översättningar av säkerhetsförklaringen finns tillgängliga i PDF-dokumentet **Translated Safety Statements** som publicerats på Allied Telesis webbplats på **alliedtelesis.com/us/en/library/search**.

Contents

Figures

Tables

Preface

The preface contains the following sections:

Software Update Version 2.0

Table 1 lists the new features in Software Update Version 2.0 for the MCF3000 Series.

Table 1: New Features **in** Software Update Version 2.0

Name	Description
SNMPv1, v2c, v3	This release adds SNMPv1, v2c, and v3 management to the media converter. Refer to Chapter 2, “SNMP Client” on page 27.
RADIUS client	This release adds a RADIUS client to the management software for authenticating the “manager” and “user1” accounts. When the RADIUS client is configured, managers who log on using either account are authentication by both an authenticated module and a RADIUS server on your network. Refer to Chapter 3, “RADIUS Client” on page 41.
TACACS+ client	This release also adds a TACACS+ client to the management software for authenticating the “manager” and “user1” accounts with a TACACS+ server on your network. Refer to Chapter 4, “TACACS+ Client” on page 49.
syslog client	This release adds a syslog client for transmitting event messages from the management module to a syslog server on your network. Refer to Chapter 5, “syslog Client” on page 57.

Installation and User Guides

The following product documents are available on the Allied Telesis web site:

- *MCF3000 Series Multi-Channel Media Converters Installation Guide* (PN: 613-002756)
- *MCF3000 Series Multi-channel Media Converters Web Browser Interface User Guide* (PN: 613-002809)
- *MCF3000 Series Multi-channel Media Converters Command Line Interface User Guide* (PN: 613-002808)

Safety Symbols Used in this Document

This document uses the following conventions.

Note
Notes provide additional information.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Warning
Laser warnings inform you that an eye or skin hazard exists due to the presence of a Class 1 laser device.

Chapter 1

MCF3300 Media Converter Hardware Components

This chapter briefly describes the hardware components of the MCF3300 multi-channel modular media converter. For further details, refer to the *MCF3000 Series Multi-channel Media Converter Installation Guide*:

Note
The MCF3010T/4SP media converter module described in rev. A of the *MCF3000 Series Multi-channel Media Converters Installation Guide* is not available for purchase at this time.

MCF3300 Chassis and Power Supplies

The front and rear panels of the MCF3300 chassis are shown in Figure 1.

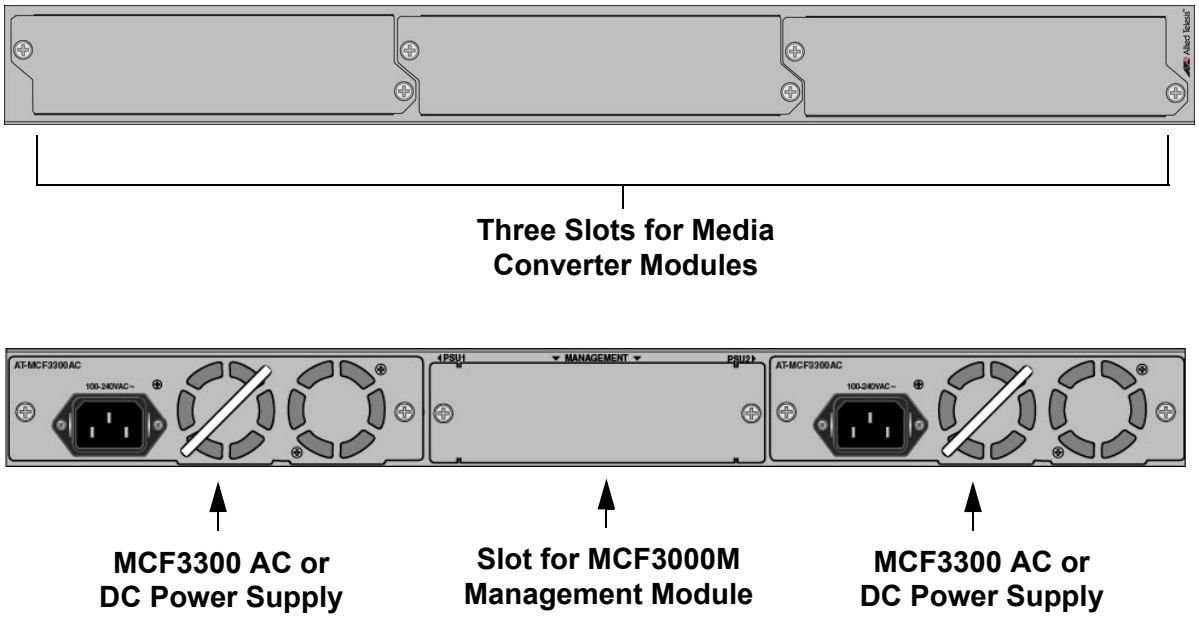


Figure 1. Front and Rear Panels of the MCF3300 Chassis

The power supplies for the chassis are the AC MCF3300AC and DC MCF3300DC modules. Refer to Figure 2.

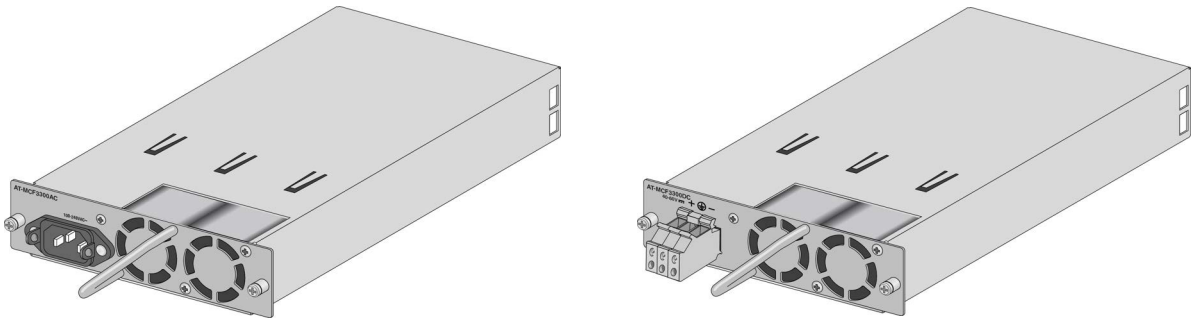


Figure 2. MCF3300AC and MCF3300DC Power Supplies

Here are power supply operational notes:

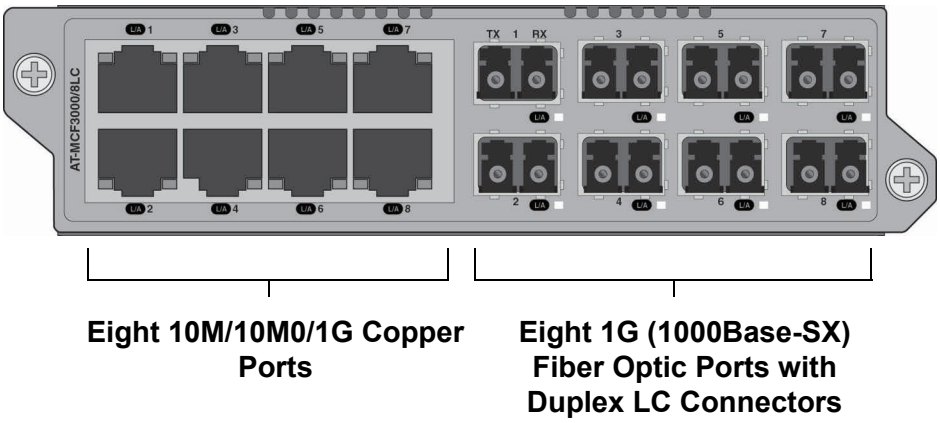
- The MCF3000/8LC and MCF3000/8SP media converter modules require only one power supply in the chassis. Installing a second power supply adds power redundancy.
- The MCF3010SPT/4SP and MCF3010SP/4SP media converter modules require two power supplies for adequate power and cooling in the chassis.

- If the chassis has the optional MCF3000M management module, the module will shut down the MCF3000/8LC and MCF3000/8SP media converter modules if the chassis has only one power supply.
- The media converter comes with one AC or DC power supply preinstalled. Additional power supplies are ordered separately.

MCF3000/8LC and MCF3000/8SP Media Converter Modules

The MCF3000/8LC and MCF3000/8SP media converter modules are illustrated in Figure 3.

MCF3000/8LC



MCF3000/8SP

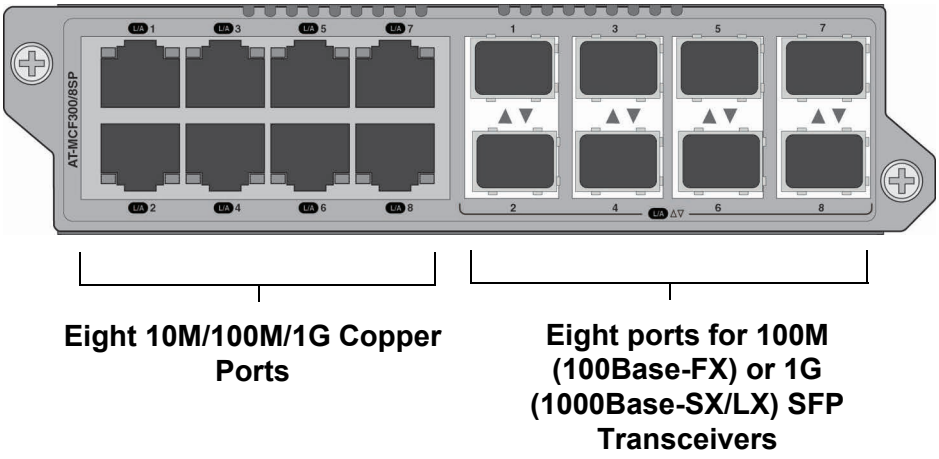


Figure 3. MCF3000/8LC and MCF3000/8SP Media Converter Modules

Media Converter Channels

The media converter channels are predefined. Channel 1 consists of copper port 1 and fiber optic port 1, channel 2 of copper port 2 and fiber optic port 2, and so forth. Refer to Figure 4 on page 19. You cannot change the port-to-channel assignments.

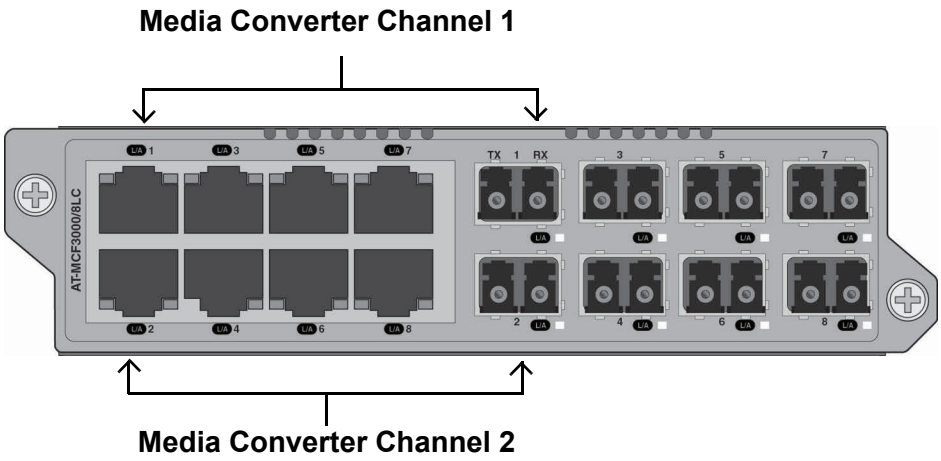


Figure 4. Media Converter Channels on the MCF3000/8LC and MCF3000/8SP Media Converter Modules

Copper Ports

Here are the properties of the copper ports:

- Standard RJ-45 8-pin connectors.
- Speeds of 10M/100M/1G.
- Half or full-duplex mode at 10M/100M. Full-duplex mode is recommended for best performance.
- Full-duplex mode only at 1G.
- Maximum operating distance of 100 meters (328 feet) at 10M/100M/1G.
- IEEE 802.3u. Auto-Negotiation that automatically sets speeds and duplex modes. You can manually adjust the ports with the optional management module.
- Auto-MDI/MDI-X that automatically adjusts the wiring configurations to MDI or MDI-X, depending on the wiring configuration of the local devices. This allows you to use standard UTP Ethernet copper cable regardless of the wiring configuration of the ports on network devices.

Auto-MDI/MDI-X is only available when the copper ports are using Auto-Negotiation, the default setting. If you disable Auto-Negotiation on a port and set the speed and duplex mode manually, this feature is also disabled and the port defaults to the MDI-X setting.

Copper Cable

The minimum cable requirements for the copper ports are given here.

- 10M/100M: Standard TIA/EIA 568-B-compliant Category 3 unshielded cabling.

- 1G: Standard TIA/EIA 568-A-compliant Category 5 or TIA/EIA 568-B-compliant Enhanced Category 5 (Cat 5e) unshielded cabling.

MCF3000/8LC Fiber Optic Ports

The fiber optic ports on the MCF3000/8LC media converter module have the following properties:

- Fixed speed of 1G (1000Base-SX)
- Full-duplex mode only
- Maximum operating distance of 500 meters (1640 ft.) with 50/125µm multimode fiber optic cable or 220 meters (722 ft.) with 62.5/125µm (core/cladding) multimode cable
- Duplex LC connectors

MCF3000/8SP Fiber Optic Ports

The fiber optic ports on the MCF3000/8SP media converter module support 100M 100Base-FX or 1G 1000Base-SX/LX SFP transceivers. They do not support 10G transceivers. Contact your Allied Telesis sales representative for a list of supported transceivers.

MCF3010SP/4SP Media Converter Module

The MCF3010SP/4SP media converter module is shown in Figure 5.

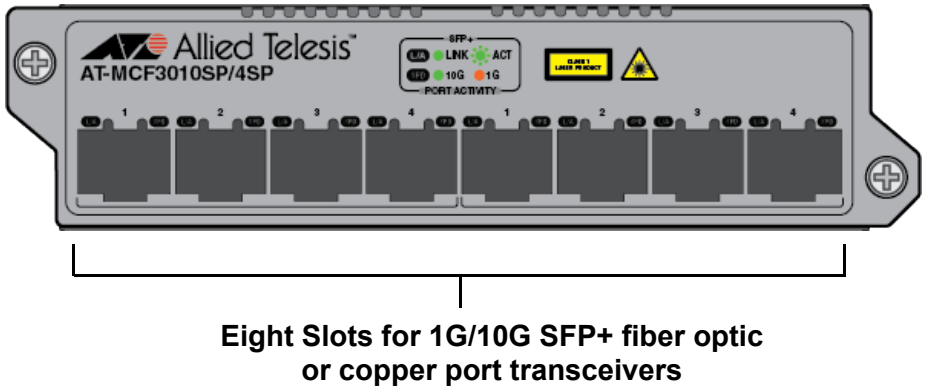


Figure 5. MCF3010SP/4SP Media Converter Module

Media Converter Channels

The MCF3010SP/4SP module has four independent media converter channels. Each channel consists of two slots for 1G/10G SFP+ fiber optic or copper port transceivers. The channels, which are predefined, are numbered 1 to 4. Channel 1 consists of slots 1 and 1, channel 2 consists of slots 2 and 2, and so on. Refer to Figure 6.

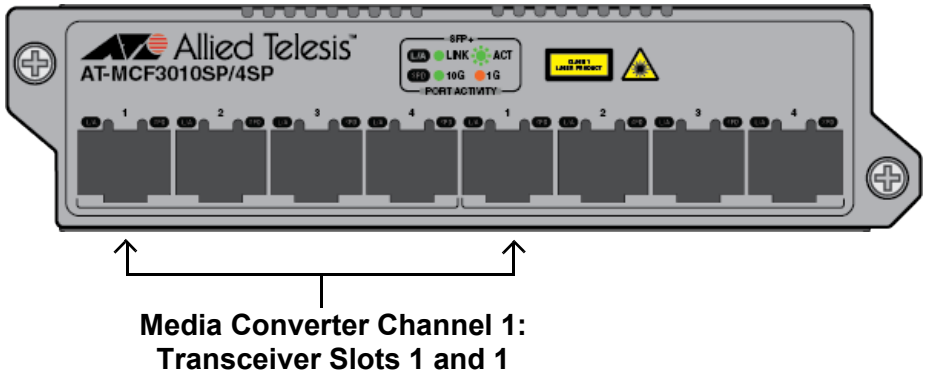


Figure 6. Media Converter Channel 1 on the MCF3010SP/4SP Module

Requirement

The MCF3010SP/4SP module has the following requirement:

- The MCF3010SP/4SP module requires two MCF3300AC or MCF3300DC power supplies in the chassis for adequate power and cooling.

Guidelines

Here are the guidelines to the media converter module:

- The channel slots support 1G and 10G SFP+ fiber optic or copper port transceivers. For a list of supported SFP+ and copper transceivers, contact an Allied Telesis sales representative.

- The channel assignments of the transceiver slots cannot be changed.
- The four media converter channels operate independently of each other. The network traffic of one channel cannot cross over to another channel.
- For two network devices to communicate with each other through the media converter module, they must be connected to SFP+ transceivers in slots of the same media converter channel, such as slots 1 and 1, or slots 2 and 2.
- The two network devices of a media converter channel can operate at different speeds. For example, one can be operating at 1G and the other at 10G.
- The ports of a channel use store and forward to forward traffic. Packets are forwarded to the egress port of a channel after they have been fully received and buffered on the ingress port and checked for cyclic redundancy check (CRC) errors. Packets without a CRC error are forwarded to the egress port where CRC is regenerated prior to retransmission, while packets with CRC errors are discarded to prevent their propagation on the network.
- You can use the media converter channels in any order.
- Changing channel and port settings requires the optional MCF3000M management module.
- The MCF3000M management module must have bootloader v1.3 and firmware v2.0 or later.
- The MCF3000M management module will shut down MCF3010SP/4SP Modules if the chassis has only one power supply.
- There are no adjustable switches on the media converter module.

MCF3010SPT/4SP Media Converter Module

The MCF3010SPT/4SP media converter module is a bundled product consisting of these products:

- One MCF3010SP/4SP media converter module.
- Four pre-installed 10/100M/1/2.5/5/10G AT-SP10TM copper port transceivers.

Refer to Figure 7.

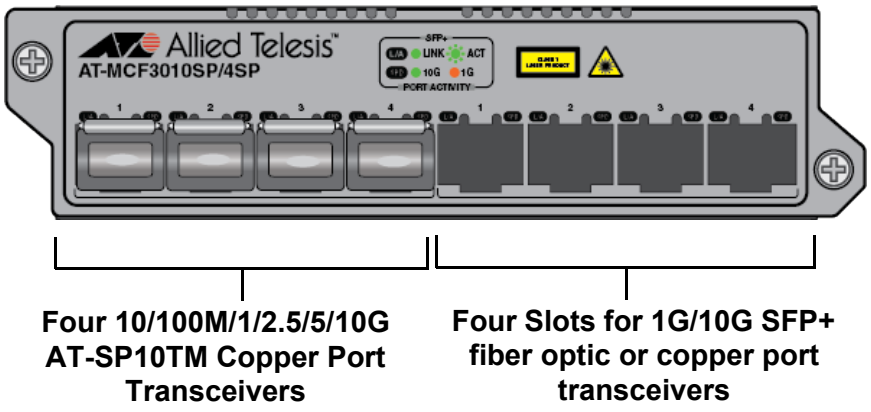


Figure 7. MCF3010SPT/4SP Media Converter Module

Media Converter Channels

The MCF3010SPT/4SP module has four independent media converter channels. Each channel consists of one copper port and one SFP+ transceiver slot. The copper ports are 10/100M/1/2.5/5/10G transceivers. The port and slot assignments of the channels are predefined. Media converter channel 1 consists of copper port 1 and transceiver slot 1, channel 2 consists of copper port 2 and transceiver slot 2, and so on. Refer to Figure 8.

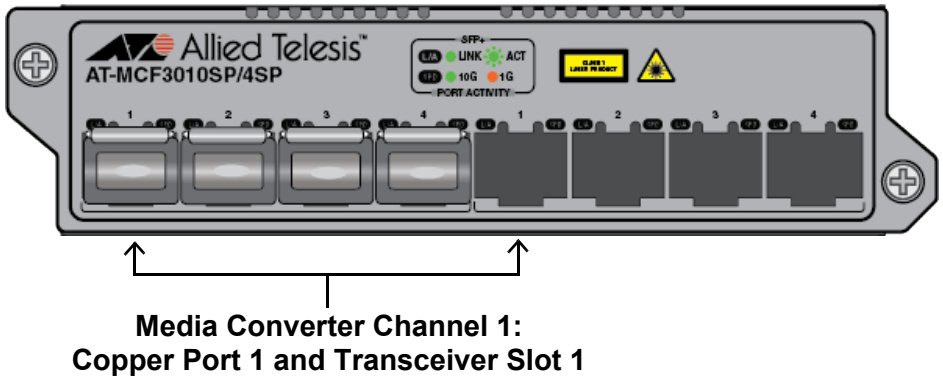


Figure 8. Media Converter Channel 1 on the MCF3010SPT/4SP Module

Requirement

The MCF3010SPT/4SP media converter module has the following requirement:

- The MCF3010SPT/4SP module requires two MCF3300AC or MCF3300DC power supplies in the chassis to maintain adequate power and cooling.

Guidelines

Here are the guidelines to the MCF3010SPT/4SP module:

- The four copper port transceivers support speeds of 10/100M/1/2.5/5/10G.
- The default speed setting for the copper ports is auto-negotiation. Setting the speed manually requires the MCF3000M management module.
- The SFP+ transceiver slots support 1G and 10G fiber optic, or copper port transceivers. For a list of supported SFP+ transceivers, contact an Allied Telesis sales representative.
- The channel assignments of the ports cannot be changed.
- The four media converter channels operate independently of each other. The network traffic of one channel cannot cross over to another channel.
- For two network devices to communicate with each other through the media converter module, they have to be connected to ports in slots of the same media converter channel, such as copper port 1 and SFP+ transceiver slot 1, copper port 2 and SFP+ transceiver slot 2, and so forth.
- The two network devices of a media converter channel can operate at different speeds. For example, the copper port in a channel can operate at 100M and the fiber optic transceiver at 1G.
- The ports of a channel use store and forward to forward traffic. Packets are forwarded to the egress port of a channel after they have been fully received and buffered on the ingress port and checked for cyclic redundancy check (CRC) errors. Packets without a CRC error are forwarded to the egress port where CRC is regenerated prior to retransmission, while packets with CRC errors are discarded to prevent their propagation on the network.
- You can use the media converter channels in any order.
- Changing channel and port settings requires the optional MCF3000M management module.
- The MCF3000M management module must have bootloader v1.3 and firmware v2.0 or later.
- The MCF3000M management module will shut down MCF3010SPT/4SP modules if the chassis has only one power supply.
- There are no adjustable switches on the media converter module.

MCF3000M Management Module

The optional MCF3000M management module is used to monitor and configure the ports and channels on the media converter modules. Refer to Figure 9. You can access the module locally through its CONSOLE port or remotely over your network through the MGMT 10/100/1000Base-T port, from Telnet or SSH clients.

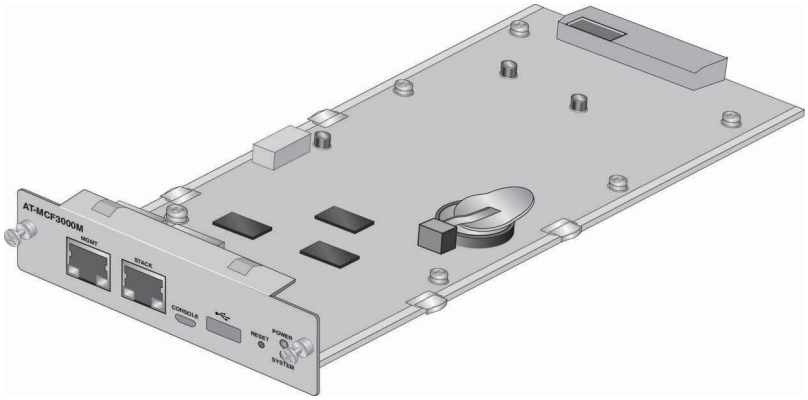


Figure 9. MCF3000M Management Module

Note
The MCF3000M management module is optional. The media converter modules can be used as unmanaged devices.

Here are examples of management functions:

- Configure the following operating parameters of the copper ports on the media converter channels:
  - Auto-Negotiation
  - Speed
  - Duplex mode
  - Flow control
- Set the operating modes of the media converter channels:
  - Regular
  - MissingLink
- Download new versions of the management software to the management module and the media converter modules.

Note
For the complete list of management features, refer to the *MCF3000 Series Command Line Interface User Guide* or *MCF3000 Series Web Browser Interface User Guide*, on the Allied Telesis web site.

Chapter 2

SNMP Client

Software Update Version 2.0 adds the capability of configuring selected SNMP MIB objects in the MCF3000M management module from the command line and web browser interfaces. The chapter contains the following sections:

SNMP Objects

The SNMP objects on the MCF3000M management module are divided into two groups. The first group consists of those SNMP objects that are common to SNMPv1, v2c, and v3. The second group consists of those objects that are restricted to SNMPv3. Table 1 lists the SNMP objects.

Table 1. Configurable SNMP Objects

SNMP Versions	MIB Objects
SNMPv1, v2c, v3	Manager name
	Physical location
	Read-only community string
	Read-write community string
	Trap community string
	Destination IPv4 address for device traps
SNMPv3	User-based Security Model name
	SNMPv3 security level (Unauthenticated, Authenticated, or Authenticated and Encrypted)
	Authentication algorithm (MD5 or SHA) for the Authenticated or Authenticated and Encrypted security level
	Authentication passphrase for the Authenticated or Authenticated and Encrypted security level
	Encryption method (DES or AES) for the Authenticated and Encrypted security level
	Encryption passphrase for the Authenticated and Encrypted security level

Configuring SNMP with the Command Line Interface

The SNMP objects on the MCF3000M management module are divided into two groups. The first group consists of those SNMP objects that are common to SNMPv1, v2c, and v3. The second group consists of those objects that are restricted to SNMPv3. Table 2 lists the commands in the command line interface that configure the common SNMP objects.

Table 2. Commands for Configuring the Common SNMP Objects

Command	Description
`configure snmp enabled 0|1`	Enables or disables SNMP v1, v2c, and v3 management on the media converter. Options are: - 0: Disables SNMP management. This is the default setting. - 1: Enables SNMP management.
`configure snmp contact` *`contact`*	Specifies the name or phone number of the manager responsible for maintaining the network device. Here are the requirements: - There is no default contact. - The maximum length of the contact is 31 characters. - The contact cannot have spaces. (MIB object: sysContact)
`configure snmp location` *`location`*	Specifies the physical location of the network device. Here are the requirements: - There is no default location. - The maximum length of the location is 31 characters. - The location cannot have spaces. (MIB object: sysLocation)

Table 2. Commands for Configuring the Common SNMP Objects (Continued)

Command	Description
`community snmp getstring` *community*	Specifies the read-only community string. Here are the guidelines: - The maximum length is 32 characters. - The string cannot contain spaces. - The default value is “public”.
`community snmp setstring` *community*	Specifies the read-write community string. Here are the guidelines: - The maximum length is 32 characters. - The string cannot contain spaces. - The default value is “private”.
`community snmp trapstring` *community*	Specifies the trap community string. Here are the guidelines: - The maximum length is 32 characters. - The string cannot contain spaces. - The default value is “public”.
`community snmp trapdest` *IPv4_address*	Specifies the IPv4 address of a network node to receive traps from the management module. Here are the guidelines: - You can specify only one trap receiver. - You cannot enter an IPv6 address.

Table 3 lists the SNMP commands in the command line interface that are specific to SNMPv3.

Table 3. Commands for Configuring the SNMPv3 Parameters

Command	Description
`configure snmp usev3 0|1`	Enables or disables the restriction of SNMP management to SNMPv3 only. Options are: - 0: Permits SNMP management of SNMPv1, SNMPv2c, and SNMPv3. This is the default setting. - 1: Restricts SNMP management to SNMPv3 only.

Table 3. Commands for Configuring the SNMPv3 Parameters (Continued)

Command	Description
`configure snmp username` *name*	Specifies the User-based Security Model (USM) name. Here are the guidelines - There is no default user name. - The name must be a minimum of eight characters. - The name cannot be more than 32 characters. - The name cannot contain spaces. - Only the USM name can manage the switch using SNMPv3. - You can change the name with this command only once. For additional changes, you have to use the Linux snmpuser utility.
`configure snmp securitylevel 0|1|2`	Sets the SNMPv3 security level. Options are: - 0: Unauthenticated: Managers are not required to send authentication or encryption passphrases. (MIB object: noAuthNoPriv) - 1: Authenticated: Managers are required to send authentication verification. This may include.MD5 or SHA and a passphrase. (MIB object: authNoPriv) - 2: Authenticated and Encrypted: Managers are required to send authentication verification. This may include.MD5 or SHA and a passphrase. Managers are also required to provide encryption information, which may include DES or AES and an encryption passphrase. (MIB object: authPriv) (MIB object: SecLevel)

Table 3. Commands for Configuring the SNMPv3 Parameters (Continued)

Command	Description
`configure snmp authtype 0|1`	If the security level is set to either Authenticated or Authenticated and Encrypted, select the authentication algorithm from the pull-down menu. Options are: - 0: MD5 - This is the default value. - 1: SHA (MIB object: AuthProtocol)
`configure snmp authphrase` *passphrase*	If the security level is set to either Authenticated or Authenticated and Encrypted, enter an authentication passphrase. Here are the guidelines: - The passphrase must be a minimum of eight characters. - The maximum length of the passphrase is 32 characters. - The passphrase cannot contain spaces. - The default is no passphrase. (MIB object: AuthPassword)
`configure snmp privtype 0|1`	If the security level is set to Authenticated and Encrypted, select the encryption method. Options are: - 0: DES (Data Encryption Standard) - This is the default setting. - 1: AES
`configure snmp privphrase` *passphrase*	If the security level is set to Authenticated and Encrypted, enter an encryption passphrase. Here are the guidelines: - The passphrase must be a minimum of eight characters. - The maximum length of the passphrase is 32 characters. - The passphrase cannot contain spaces. - The default is no passphrase.

Table 3. Commands for Configuring the SNMPv3 Parameters (Continued)

Command	Description
`configure snmp context` *`context`*	This parameter is not implemented in the current release. Do not change this parameter from its default setting. There is no default context.

Configuring SNMP with a Web Browser

To configure the SNMP objects from a web browser management session, perform the following procedure:

1. Select **Configuration** from the menu bar.
2. Select the **SNMP** tab.
3. To configure the common SNMPv1, v2c, and v3 objects, select the **V2** tab. This is the default tab. Refer to Figure 1.

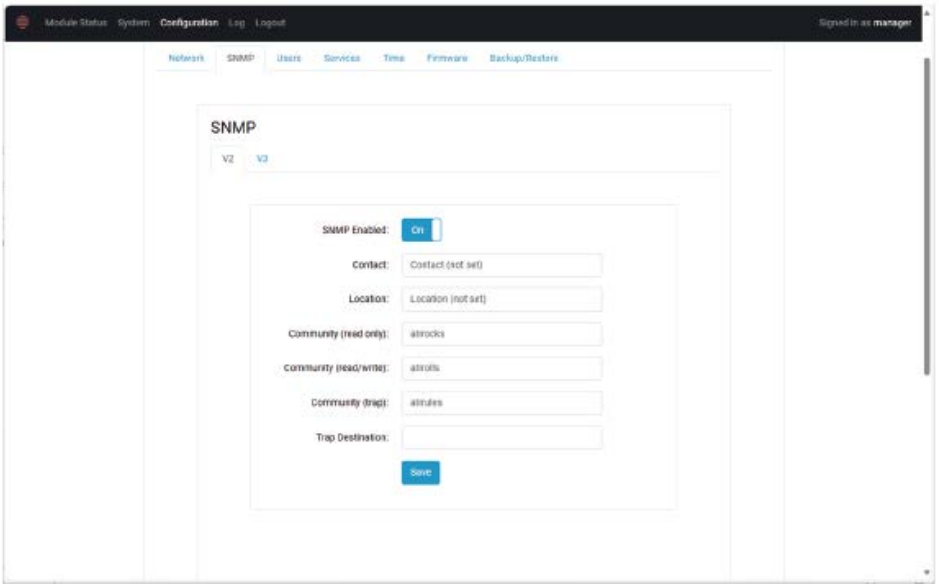


Figure 1. SNMP V2 Window

4. Configure the objects by referring to Table 4

Table 4. Parameters in the SNMP V2 Window

SNMP Parameter	Description
SNMP Enabled	Enables or disables SNMP v1, v2c, and v3 management on the media converter. Options are: - Off: Disables SNMP management. This is the default setting. - On: Enables SNMP management.

Table 4. Parameters in the SNMP V2 Window (Continued)

SNMP Parameter	Description
Contact	Specifies the name of the manager responsible for maintaining the network device. Here are the requirements: - There is no default contact. - The maximum length of the contact is 31 characters. - The contact cannot have spaces. (MIB object: sysContact)
Location	Specifies the physical location of the network device. Here are the requirements: - There is no default location. - The maximum length of the location is 31 characters. - The location cannot have spaces. (MIB object: sysLocation)
Community (read only)	Specifies the read-only community string. Here are the guidelines: - The maximum length is 32 characters. - The string cannot contain spaces.
Community read-write	Specifies the read-write community string. Here are the guidelines: - The maximum length is 32 characters. - The string cannot contain spaces.
Community (trap)	Specifies the community string for traps. Here are the guidelines: - The maximum length is 32 characters. - The string cannot contain spaces.

Table 4. Parameters in the SNMP V2 Window (Continued)

SNMP Parameter	Description
Trap Destination	Specifies the IPv4 address of a network node to receive traps from the management module. Here are the guidelines: - You can specify only one trap receiver. - You cannot enter an IPv6 address.

5. To configure SNMPv3 objects, select the **V3** tab. Refer to Figure 2.

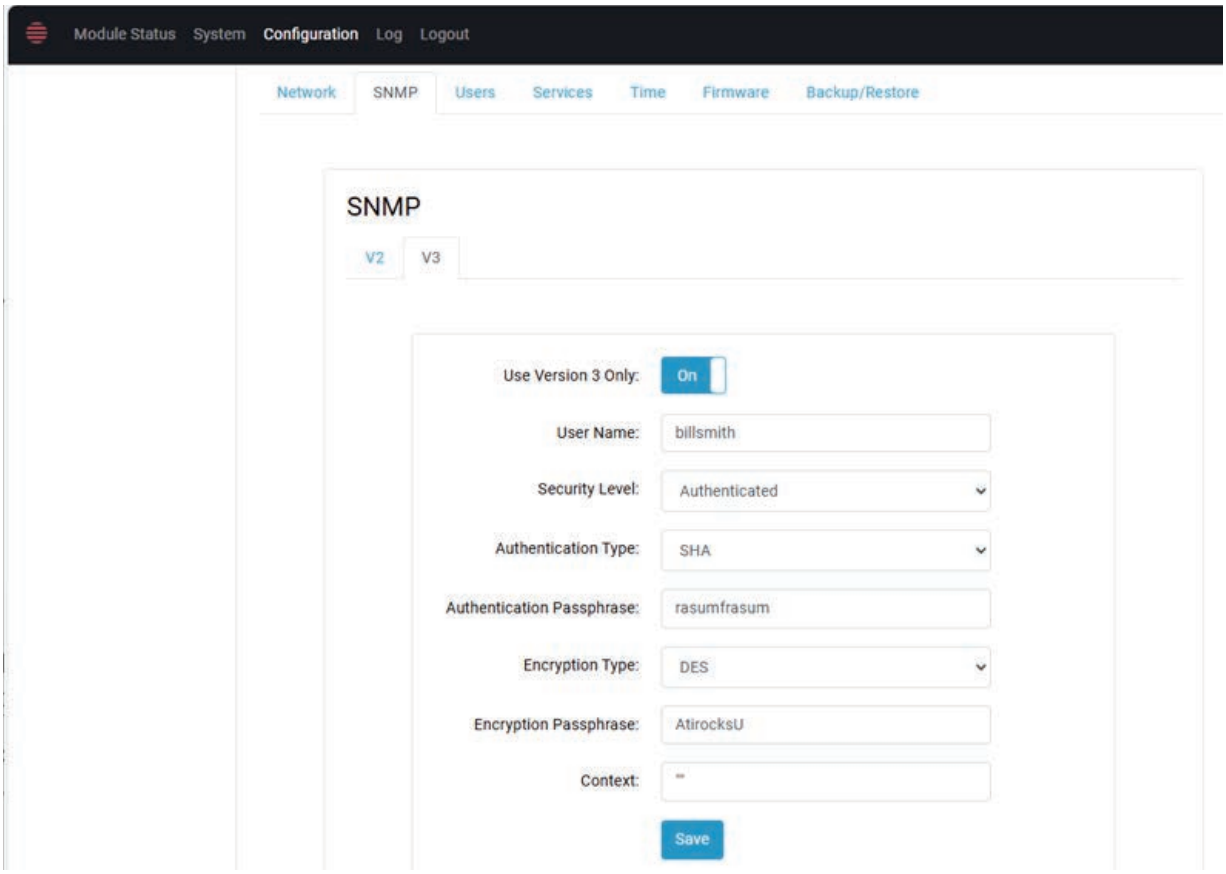


Figure 2. SNMP V3 Window

6. Configure the SNMP objects by referring to Table 5 on page 37.

Table 5. Parameters in the SNMPv3 V3 Window

Parameter	Description
Enabled	Enables or disables the restriction of SNMP management to SNMPv3 only. Options are: - Off: Permits SNMP management using SNMPv1, SNMPv2c, and SNMPv3. This is the default setting. - On: Restricts SNMP management to SNMPv3 only.
User Name	Specifies the User-based Security Model (USM) name. Here are the guidelines: - There is no a default user name. - The name must be a minimum of eight characters. - The name cannot be more than 32 characters. - The name cannot contain spaces. - Only the USM name can manage the switch using SNMPv3. - You can change the name with this command only once. For additional changes, you have to use the Linux snmpuser utility.

Table 5. Parameters in the SNMPv3 V3 Window (Continued)

Parameter	Description
Security Level	Sets the SNMPv3 security level. Options are: - Unauthenticated: Managers are not required to send authentication or encryption passphrases. (noAuthNoPriv) - Authenticated: Managers are required to send authentication verification. This may include.MD5 or SHA and a passphrase. (authNoPriv) - Authenticated and Encrypted: Managers are required to send authentication verification. This may include.MD5 or SHA and a passphrase. Managers are also required to provide encryption information, which may include DES or AES and an encryption passphrase. (authPriv) (MIB object: SecLevel)
Authentication Type	If the security level is set to either Authenticated or Authenticated and Encrypted, select the authentication algorithm from the pull-down menu. Options are: - MD5 - This is the default value. - SHA (MIB object: AuthProtocol)
Authentication Passphrase	If the security level is set to either Authenticated or Authenticated and Encrypted, enter an authentication passphrase. Here are the guidelines: - The passphrase must be a minimum of eight characters. - The passphrase cannot be longer than 32 characters. - The passphrase cannot contain spaces. - The default is no passphrase. (MIB object: AuthPassword)

Table 5. Parameters in the SNMPv3 V3 Window (Continued)

Parameter	Description
Encryption Type	If the security level is set to Authenticated and Encrypted, select the encryption method. Options are: - DES - This is the default setting. - AES
Encryption Passphrase	If the security level is set to Authenticated and Encrypted, enter an encryption passphrase. Here are the guidelines: - The passphrase must be a minimum of eight characters. - The passphrase cannot be longer than 32 characters. - The passphrase cannot contain spaces. - The default is no passphrase.
Context	This parameter is not implemented in the current release. Do not change this parameter from its default setting. There is no default context.

7. To save your changes, click the **Save** button.

   The following prompt is displayed at the bottom of the window:

   ```
   Changes saved. System restart required.
   ```

   Note
   To activate your changes now, reboot the MCF3000M management module by continuing with step 8:

8. Select **System** from the menu bar.
9. Scroll to the bottom of the window.
10. Click the **System Restart** button. Refer to Figure 3.

Figure 3. System Restart Button in System Window

The management module displays a confirmation prompt.

11. Click the **OK** button to boot the management module or the **Cancel** button to stop the procedure.

    If you click OK, the management module restarts and your management session ends.

12. To resume managing the media converter, wait one minute for the modules to initialize their software, and then start a new management session.

Chapter 3

RADIUS Client

The chapter contains the following sections:

Note
For instructions on configuring the TACACS+ client, refer to Chapter 4, “TACACS+ Client” on page 49.

RADIUS and TACACS+ Clients Overview

Management software version 2.0 adds RADIUS and TACACS+ clients to the MCF3000M management module. You may use the clients to authenticate the username and password credentials of managers who log on using the “manager” and “user1” accounts on the management module. When the RADIUS or TACACS+ client is activated, managers who log on are authenticated by both the management module and a RADIUS or TACACS+ server on your network.

Note
The “user1” account can only be used to view activity messages and the parameter settings on the media converters. To configure the parameter settings of the media converters, you must log on as the “manager” account.

Here are the guidelines to the RADIUS and TACACS+ clients:

- You should activate only one authentication client on the MCF3000M management module.
- The clients cannot be used to authenticate any traffic passing through the media converter modules.
- The clients authenticate the “manager” and “user1” accounts in web browser, Telnet, and SSH management sessions.
- The clients can also authenticate manager accounts on the micro-USB Console port.
- You cannot add manager accounts.
- You cannot change the “manager” and “user1” login names. You must enter the names on the RADIUS or TACACS+ server in lowercase letters.
- The account passwords on the MCF3000M management module and the RADIUS or TACACS+ authentication server must be identical. For instance, if the password for the “user1” account is “WindMill” on the management module, it must be the same on the RADIUS or TACACS+ server.
- The maximum length of the “manager” and “user1” passwords is sixteen characters. Passwords are case sensitive.
- The password can contain special characters, such as asterisks, question marks, and quote marks.
- The password cannot contain spaces or the percent character (%).
- The default password for the “manager” account is “friend”. The default password for the “user1” account is “user1”.

The RADIUS and TACACS+ clients have these requirements:

- The network must have a RADIUS or TACACS+ server that the MCF3000M management module can reach from its MGMT port or micro-USB Console port. The management module cannot communicate with the server through the media converter ports.
- You can specify the IP address of only one RADIUS or TACACS+ server on the MCF3000M management module.
- The RADIUS or TACACS+ server must have an IPv4 address. The MCF3000M management module does not support IPv6 addresses.
- If the RADIUS or TACACS+ server is on a different subnet from the MCF3000M management module, the module must have a default gateway address to communicate with the server via the gateway.

Note
This guide does not explain how to install or configure RADIUS or TACACS+ server software. Refer to the documentation that comes with the server software for instructions.

Note
RADIUS and TACACS+ server software are not available from Allied Telesis.

Configuring the RADIUS Client with the Command Line Interface

The following sections explain how to configure the RADIUS client using the commands in the command line interface of the MCF3000M management module:

- “Enabling or Disabling the RADIUS Client,” next
- “Specifying the IPv4 Address of a RADIUS Server” on page 44
- “Specifying the Shared Secret of a RADIUS Server” on page 45
- “Displaying the RADIUS Client Settings” on page 45
- “Example of Configuring the RADIUS Client” on page 46

Note
All changes to RADIUS client settings, including enabling and disabling the service, are immediately implemented by the management module on the client.

Enabling or Disabling the RADIUS Client

Here is the command for enabling or disabling the RADIUS client on the MCF3000M management module:

```
configure radius enable 0|1
```

The variables are defined here:

- 0 (zero) - Disables the RADIUS client. This is the default setting.
- 1 - Enables the RADIUS client.

This example enables the RADIUS client:

```
MCF3000M>>configure radius enable 1
```

This example disables the client:

```
MCF3000M>>configure radius enable 0
```

Specifying the IPv4 Address of a RADIUS Server

The command for adding the IPv4 address of a RADIUS server on the network to the MCF3000M management module is CONFIGURE RADIUS SERVER. Here is the format:

```
configure radius server IPV4_address
```

The variable is defined here:

- IPv4_address - Specifies the IPv4 address of the RADIUS server on the network.

Here are the command guidelines.

- The default is no server address (i.e., 0.0.0.0)
- You can specify only one IPv4 address.
- You cannot specify a subnet mask.
- You cannot enter an IPv6 address.

This example designates 132.67.189.43 as the IPv4 address of the RADIUS server:

```
MCF3000M>>configure radius server 132.67.189.43
```

Specifying the Shared Secret of a RADIUS Server

The command for adding the shared secret of a RADIUS server to the MCF3000M management module is CONFIGURE RADIUS SECRET. Here is the format:

```
configure radius secret shared_secret
```

The variable is defined here:

- shared_secret - Specifies the shared secret on the RADIUS server.

Here are the variable guidelines:

- The maximum length of the secret is 128 characters.
- The shared secret is case sensitive.
- The shared secret is required.
- You can specify only one shared secret.
- The shared secret can contain special characters, such as asterisks, question marks, and quote marks.
- The shared secret cannot contain spaces or the percent character (%).

This example of the command changes the shared secret on the RADIUS client to “45Petal98”:

```
MCF3000M>>configure radius secret 45Petal98
```

Displaying the RADIUS Client Settings

The command for displaying the RADIUS client settings on the MCF3000M management module is SHOW RADIUS. The command does not have any variables. Here is an example:

```
MCF3000M>>show radius
```

Figure 4 on page 46 is an example of the command output.

```
MCF3000M>> show radius
Enable/disable:    disable
Server:            192.168.1.10
Secret             45Petal98
```

Figure 4. Example of the SHOW RADIUS Command

Example of Configuring the RADIUS Client

This example configures the RADIUS client on the MCF3000M management module to these settings:

- RADIUS server IPv4 address: 143.102.22.17
- Shared secret: LTwCom92
- Status: Enabled

Here are the commands:

```
MCF3000M>>configure radius server 143.102.22.17
MCF3000M>>configure radius secret LTwCom92
MCF3000M>>configure radius enable 1
MCF3000M>>show radius
```

Note
The management module automatically activates all changes to the status and settings of the RADIUS client.

Configuring the RADIUS Client with a Web Browser

To configure the RADIUS client from a web browser management session, perform the following procedure:

1. Select **Configuration** from the menu bar.
2. Select the **Services** tab.

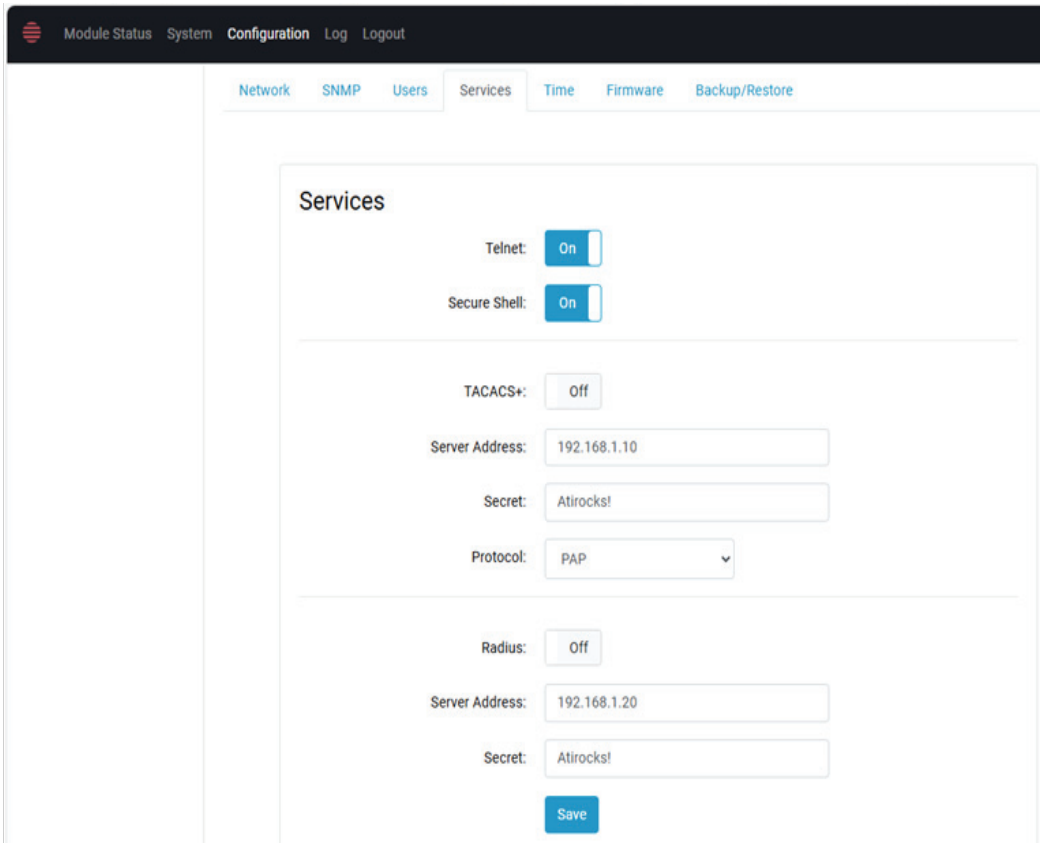


Figure 5. Services Window - Configuring the TACACS+ and RADIUS Clients

Note
For descriptions of the Telnet and Secure Shell options in the Services window, refer to the *MCF3000 Series Multi-channel Media Converters Web Browser Interface User Guide.*

3. To enable or disable the RADIUS client on the MCF3000M management module, select **ON** or **OFF**, respectively, for the RADIUS parameter. The default setting is OFF.

Note
If you disable the feature, go to step 6.

4. To specify the IPv4 address of a RADIUS server, enter its address in the **Server Address** field. The parameter has these guidelines.
   - ❒ The default is no server address (i.e., 0.0.0.0)
   - ❒ You can specify only one IPv4 address.
   - ❒ You cannot specify a subnet mask.
   - ❒ You cannot enter an IPv6 address.
5. To specify the shared secret on the RADIUS server, enter the secret in the **Secret** field. The parameter has these guidelines:
   - ❒ The maximum length of the secret is 128 characters.
   - ❒ The shared secret is required.
   - ❒ The shared secret is case sensitive.
   - ❒ You can specify only one shared secret.
   - ❒ The shared secret can contain special characters, such as asterisks, question marks, and quote marks.
   - ❒ The shared secret cannot contain spaces or the percent character (%).
6. Click the **Save** button to save your changes in the configuration file on the MCF3000M management module.

   The following prompt is displayed at the bottom of the window:

   ```
   Changes saved.
   ```

   Note
   The management module automatically activates changes to the status and settings of the RADIUS client.

Chapter 4

TACACS+ Client

The chapter contains the following sections:

Note
For guidelines and requirements of the TACACS+ client, refer to “RADIUS and TACACS+ Clients Overview” on page 42.

Configuring the TACACS+ Client with the Command Line Interface

The following sections explain how to configure the TACACS+ client using the commands in the command line interface of the MCF3000M management module:

- “Enabling or Disabling the TACACS+ Client,” next
- “Specifying the IPv4 Address of a TACACS+ Server” on page 50
- “Specifying the Shared Secret of a TACACS+ Server” on page 51
- “Setting the TACACS+ Protocol” on page 51
- “Displaying the TACACS+ Client Settings” on page 52

Note
All changes to TACACS+ client settings, including enabling and disabling the service, are immediately implemented by the management module on the client.

Enabling or Disabling the TACACS+ Client

Here is the command for enabling or disabling the TACACS+ client on the MCF3000M management module:

```
configure tacacs enable 0|1
```

The variables are defined here:

- 0 (zero) - Disables the TACACS+ client. This is the default setting.
- 1 - Enables the TACACS+ client.

This example enables the TACACS+ client:

```
MCF3000M>>configure tacacs enable 1
```

This example disables the client:

```
MCF3000M>>configure tacacs enable 0
```

Specifying the IPv4 Address of a TACACS+ Server

The command for adding the IPv4 address of a TACACS+ server to the MCF3000M management module is CONFIGURE TACACS SERVER. Here is its format:

```
configure tacacs server IPV4_address
```

The variable is defined here:

- IPv4_address - Specifies the IPv4 address of the TACACS+ server.

Here are the command guidelines.

- The default is no server address (i.e., 0.0.0.0
- You can specify only one address.
- You cannot specify a subnet mask.
- You cannot specify an IPv6 address.
- The TACACS+ server must be reachable from the MGMT port on the MCF3000M management module.

This example designates the IP address of the TACACS+ server as 151.101.45.78:

```
MCF3000M>>configure tacacs server 151.101.45.76
```

Specifying the Shared Secret of a TACACS+ Server

The command for adding the shared secret of a TACACS+ server to the MCF3000M management module is CONFIGURE TACACS SECRET. Here is the format:

```
configure tacacs secret shared_secret
```

The variable is defined here:

- shared_secret - Specifies the shared secret on the TACACS+ server.

Here are the command guidelines:

- The shared secret is case sensitive.
- You can specify only one shared secret.
- The shared secret can contain special characters, such as asterisks, question marks, and quote marks.
- The shared secret cannot contain spaces or the percent character (%).
- The maximum length of the secret is 63 characters.

This example changes the shared secret on the TACACS+ client to “45Petal98:”

```
MCF3000M>>configure tacacs secret 45Petal98
```

Setting the TACACS+ Protocol

The command for specifying the protocol of a TACACS+ server is CONFIGURE TACACS PROTOCOL. Here is the format:

```
configure tacacs protocol 0|1|2
```

The variables are defined here:

- 0 - PAP
- 1 - CHAP
- 2 - Login/ASCII

Here are the command guidelines:

- The protocol on the client and server must be the same.
- The client can have only one protocol.
- The default is PAP (0).

This example configure the TACACS+ protocol on the client to CHAP:

```
MCF3000M>>configure tacacs protocol 1
```

Displaying the TACACS+ Client Settings

The command for displaying the TACACS+ client settings on the MCF3000M management module is SHOW TACACS+. The command does not have any variables. Here is an example:

```
MCF3000M>>show tacacs
```

Figure 6 is an example of the command output.

```
MCF3000M>> show tacacs
Enable/disable:    disabled
Server:            192.168.1.10
Secret             45Petal98
Protocol:          PAP
```

Figure 6. Example of the SHOW TACACS+ Command

Example of Configuring the TACACS+ Client

This example of the commands configures the TACACS+ client on the MCF3000M management module to these settings:

- TACACS+ server IPv4 address: 189.156.14.9
- Shared secret: 981YPiwuq
- Protocol: Login/ASCII
- Status: Enabled

Here are the commands:

```
MCF3000M>>configure tacacs server 189.156.14.9
MCF3000M>>configure tacacs secret 981YPiwuq
MCF3000M>>configure tacacs protocol 2
MCF3000M>>configure tacacs enable 1
MCF3000M>>show tacacs
```

Note
The management module automatically activates all changes to the status and settings of the TACACS+ client.

Configuring the TACACS+ Client with a Web Browser

To configure the TACACS+ client from a web browser management session, perform the following procedure:

1. Select **Configuration** from the menu bar.
2. Select the **Services** tab. Refer to Figure 5 on page 47.
3. To enable or disable the TACACS+ client on the MCF3000M management module, select **ON** or **OFF**, respectively. The default setting is OFF.

   Note
   If you disable the feature, go to step 7.

4. To specify the IPv4 address of a TACACS+ server, enter the address in the **Server Address** field. Here are the guidelines.
   - ❒ The default is no server address (i.e., 0.0.0.0)
   - ❒ You can specify only one IPv4 address.
   - ❒ You cannot specify a subnet mask.
   - ❒ You cannot enter an IPv6 address.
5. To specify the shared secret on a TACACS+ server, enter the secret in the **Secret** field. Here are the guidelines:
   - ❒ The maximum length of the secret is 63 characters.
   - ❒ The shared secret is case sensitive.
   - ❒ You can specify only one shared secret.
   - ❒ The shared secret can contain special characters, such as asterisks, question marks, and quote marks.
   - ❒ The shared secret cannot contain spaces or the percent character (%).
6. To set the protocol of the client, select the **Protocol** pull-down menu. The parameter has these guidelines:
   - ❒ The protocol can be one of the following: 0 - PAP, 1 - CHAP, or 2 Login/ASCII.
   - ❒ The protocol on the client and server must be the same.
   - ❒ The client can have only one protocol.
   - ❒ The default is 0 - PAP.

7. Click the **Save** button to save your changes in the configuration file on the MCF3000M management module.

   The following prompt is displayed at the bottom of the window:

   ```
   Changes saved.
   ```

   Note
   The management module automatically activates changes to the status and settings of the TACACS+ client.

Chapter 5

syslog Client

The chapter contains the following sections:

syslog Client Overview

The MCF3000M management module with the Version 2.0 Software Update has a syslog client for transmitting the messages in its event log to a syslog server on your network. A syslog server can store event messages from many networks devices, thus simplifying the tasks of maintaining and troubleshooting network devices.

Here are the guidelines to the syslog client:

- You can define only one syslog server in the client.
- The MCF3000M management module must have an IPv4 address.
- The syslog server must have an IPv4 address. The MCF3000M management module does not support IPv6 addresses.
- The MCF3000M management module must be able to communicate with the syslog server through its MGMT port. The module cannot communicate with the server through the media converter ports.
- The MCF3000M management module and syslog server must be members of the same subnet or must be able to communicate via routers or other Layer 3 devices.
- The MCF3000M management module transmits event messages as they are generated. It does not transmit any event messages that already exist in the event log when the syslog client is enabled.
- The syslog client uses UDP port 514. You cannot change the UDP port.

Note
This guide does not explain how to install or configure syslog server software. Refer to the documentation provided with the server software for instructions.

Configuring the syslog Client from the Command Line Interface

This section contains the following procedures for configuring the syslog client on the management module from the command line interface:

Enabling or Disabling the Syslog Client

Here is the command for enabling or disabling the syslog client on the management module:

```
configure syslog enable 0|1
```

The variables are defined here:

- ❒ 0 (zero) - Disables the syslog client. This is the default setting.
- ❒ 1 - Enables the syslog client.

Here are the command guidelines:

- ❒ Enabling or disabling the client requires rebooting the media converter.
- ❒ Changes to all other with syslog client settings are immediately implemented after you enter a command.

This example enables the syslog client and reboots the media converter:

```
MCF3000M>>configure syslog enable 1
MCF3000M>>reboot system
```

This example disables the client:

```
MCF3000M>>configure syslog enable 0
MCF3000M>>reboot system
```

Warning
Booting the management and media converter modules is disruptive to network operations. The media converter modules stop forwarding traffic on their ports while they initialize their management software. E132

Warning
The REBOOT SYSTEM command does not display a confirmation prompt. The management and media converter modules immediately begin reinitializing their software as soon as you enter the command. E132

Specifying the IPv4 Address of a Syslog Server

Here is the command for adding the IPv4 address of a syslog server to the MCF3000M management module:

```
configure syslog server address IPv4_address
```

The variable is defined here:

- IPv4_address - Specifies the IPv4 address of a syslog server. You can specify only one address.

Here are the command guidelines.

- The default is no syslog server address (i.e., 0.0.0.0
- You can specify only one address.
- You cannot specify a subnet mask.
- You cannot specify an IPv6 address.

This example designates the IPv4 address of the syslog server as 132.67.189.43:

```
MCF3000M>>configure syslog server 132.67.189.43
```

Specifying the Priority Level of the Event Messages

You can specify a priority level for the event messages. The MCF3000M management module assigns the priority level to the event messages as it transmits them to the server. Assigning different priority levels to event messages from different devices on your network will make it easier to identify the source devices of the messages when you view them on the syslog server.

Here is the command for specifying a priority level for the event messages:

```
configure syslog priority 1-8
```

Note
The CONFIGURE SYSLOG PRIORITY command is nonfunctional in this release. All event messages transmitted by the management module are assigned the priority level 8.

The variable is defined here:

- 1-8 - Specifies the priority level to be assigned to the event messages. You can specify only one priority level.

This example of the command assigns the priority level 2 to the event messages as they are transmitted by the MCF3000M management module to the syslog server:

```
MCF3000M>>configure syslog priority 2
```

Displaying the Syslog Client Settings

The command for displaying the syslog client settings on the MCF3000M management module is shown here:

```
MCF3000M>>show syslog server settings
```

Figure 7 is an example of the command output.

```
MCF3000M>> show syslog server settings
Status:   disabled
Server:   192.168.1.50
Priority: 1
```

Figure 7. Example of the SHOW SYSLOG SERVER SETTINGS Command

Configuring the syslog Client with a Web Browser

To configure the syslog client from a web browser management session, perform the following procedure:

1. Select **Configuration** from the menu bar.
2. Select the **Network** tab.

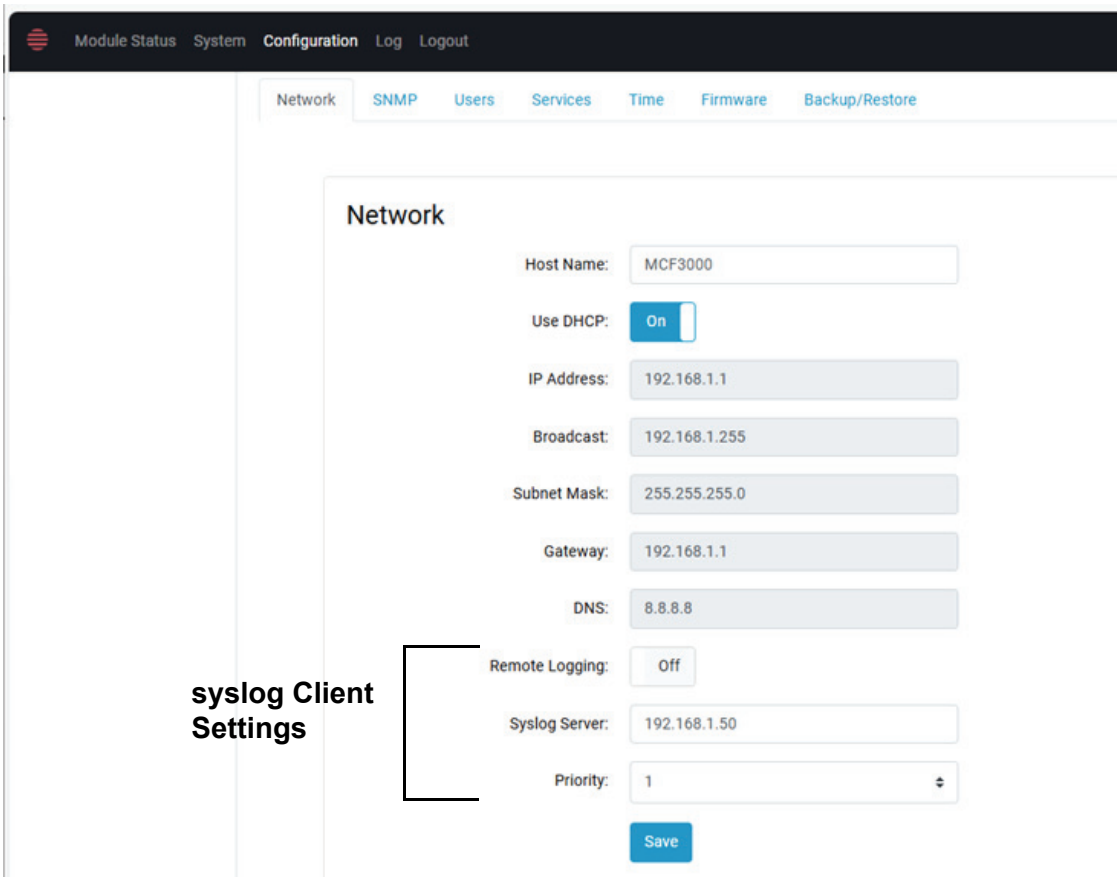


Figure 8. Network Window - Configuring the syslog Client

Note
For a description of the Network window, refer to the *MCF3000 Series Multi-channel Media Converters Web Browser Interface User Guide.*

3. To activate the syslog client so that the MCF3000M management module sends its event messages to a syslog server, select **ON** from the **Remote Logging** option. To disable the client, select **OFF**. This is the default setting.

Note
If you disable the feature, go to step 6.

4. To specify the IPv4 address of the syslog server to receive the event messages, enter the address in the **Syslog Server** field. The parameter has these guidelines.

   - ❒ The default is no server address (i.e., 0.0.0.0)
   - ❒ You can specify only one IPv4 address.
   - ❒ You cannot specify a subnet mask.
   - ❒ You cannot enter an IPv6 address.

   Note
   The **Priority** option is nonfunctional. All event messages sent by the management module are assigned the priority level 8.

5. Click the **Save** button to save your changes in the configuration file on the MCF3000M management module.

   The following prompt is displayed at the bottom of the window:

   ```
   Changes saved. System restart required.
   ```

6. Reboot the MCF3000M management module by selecting **System** from the menu bar and clicking the **System Restart** button at the bottom of the window.

   This step is required if you the enabled or disabled the syslog client. The management module has to be rebooted to implement a change to the status of the client.

Warning
Booting the management and media converter modules is disruptive to network operations. The media converter modules stop forwarding traffic on their ports while they initialize their management software. 🔗 E132

Appendix A
Updating the Management Firmware

The instructions in this appendix explain how to upload Version 2.0 management firmware to the MCF3000 management and media converter modules from a local management session, using the command line interface. The appendix has the following sections:

Introduction

Table 6 lists the upgrade procedures. They should be performed in the order presented here.

Table 6: Version 2.0 Upgrade Procedure

Procedure	Description
"1. Displaying Software and Bootloader Version Numbers" on page 68	This procedure displays the version numbers of the management software and bootloaders already installed on the MCF3000M management module. Depending on the version numbers, it may be necessary to upload a more recent version of the software before uploading Version 2.0 software.
"2. Removing MCF3000 Media Converter Modules" on page 70	This procedure removes the media converter modules from the chassis. Allied Telesis recommends updating the MCF3000M management module first, without the media converter modules in the chassis.
"3. Uploading Version 2.0 Software to the MCF3000M Management Module" on page 72	This procedure uploads Version 2.0 software from a USB drive to the MCF3000M management module.
"4. Reinstalling the Media Converter Modules" on page 75	This procedure reinstalls the media converter modules into the chassis, one at a time. The management module automatically uploads Version 2.0 software to the modules over the backplane in the chassis.
"5. Finishing the Upgrade" on page 78	In this procedure, you reattach the network cables to the ports on the media converter modules and perform SHOW commands to verify the configurations and status of the media converter ports.
"6. Creating a Backup Configuration File" on page 79	This procedure creates a backup copy of the configuration settings of the media converter chassis, with Version 2.0 software.

The procedures require the following items:

- Micro-USB Console port management cable (included with the MCF3000M management module)
- USB flash drive with a FAT directory
- Cross-head screwdriver

Review the following before beginning the upgrade procedure:

- Version 2.0 software is available from the Allied Telesis web site at www.alliedtelesis.com.
- The following procedures perform the upgrade from a local command line management session on the CONSOLE port on the management module.
- The upgrade procedure takes approximately 45 minutes.

Note
Allied Telesis recommends performing the upgrade procedures during non-business hours to minimize disruption to your network.

1. Displaying Software and Bootloader Version Numbers

This procedure explains how to display the version numbers of the current management software and bootloaders on the MCF3000M management module. Depending on the version numbers, it may be necessary to update the software to a more recent version before uploading Version 2.0 software.

To view the version numbers of the current management software and bootloaders on the MCF3000M management module, perform the following procedure:

1. Start a local command line management session on the MCF3000M management module. For instructions, refer to Appendix B, “Starting a Local Management Session” on page 81 or the *MCF3000 Series Command Line Interface User Guide*.

2. Enter the SHOW FIRMWARE INFO command. Here is an example of the command:

```
MCF3000M>>show firmware info
Management Card Firmware
   Bootloader: 1.2
   Software: 1.00

Available Linecard Firmware:
   Bootloader: 1.1
   Software: 1.00

.
.
.
```

> **Note**
> If the “Bootloader” for “Management Card Firmware” is 1.3 and the “Software’’ is 2.0, no upgrade is required. The MCF3000M management module already has Version 2.0 software.

3. Examine the “Management Card Firmware” section. It displays the version numbers of the bootloader and management software used by the MCF3000M management module. To upgrade the management software to Version 2,0, the following requirements must be met:

   - ❒ The “Bootloader” must be v1.2 or higher.
   - ❒ The “Software” must be v1.00 or higher.

Do one of the following:

- If both versions of the “Bootloader” and “Software” on your management module are the same or higher than the above values, go to the next step.
- If either version of the “Bootloader” or “Software” is earlier, do not continue. You must update the software to a more recent version before uploading Version 2.0. Released software for the product are available on from the Allied Telesis web site. For instructions, refer to the product’s user guide.

4. Examine the “Available Linecard Version” section of the command. It displays the version numbers of the bootloader and management software for the media converter modules stored on the MCF3000M management module. To upgrade the management software on the media converter modules to Version 2,0, the following requirements must be met:

   - The “Bootloader” must be v1.1 or higher.
   - The “Software” must be v1.00 or higher.

   Do one of the following:

   - If the versions of the “Bootloader” and “Software” for your media converter modules are the same or higher than the above values, go to the next step.
   - If either version of the “Bootloader” or “Software” is earlier, do not continue. You must update the software to a more recent version before uploading Version 2.0. Released software for the product are available from the Allied Telesis web site. For instructions, refer to the product’s user guide.

5. Go to “2. Removing MCF3000 Media Converter Modules” on page 70.

2. Removing MCF3000 Media Converter Modules

This procedure removes the media converter modules from the chassis. Allied Telesis recommends updating the MCF3000M management module first, without the media converter modules in the chassis.

Caution
Media converter modules are sensitive to and can be damaged by electrostatic discharge. Wear a grounding device and observe electrostatic discharge precautions when handling the modules.

To remove the media converter modules from the chassis, perform the following procedure:

1. Power off the MCF3000 chassis.
2. Label and disconnect all copper and fiber optic cables from the ports on all MCF3000 media converter modules in the chassis. Labeling the cables will make it easier to reconnect them at the conclusion of the upgrade procedure.
3. Install dust covers on the fiber optic ports.
4. Using a cross-head screwdriver, loosen the two captive screws that secure a media converter module to the chassis. Refer to Figure 9.

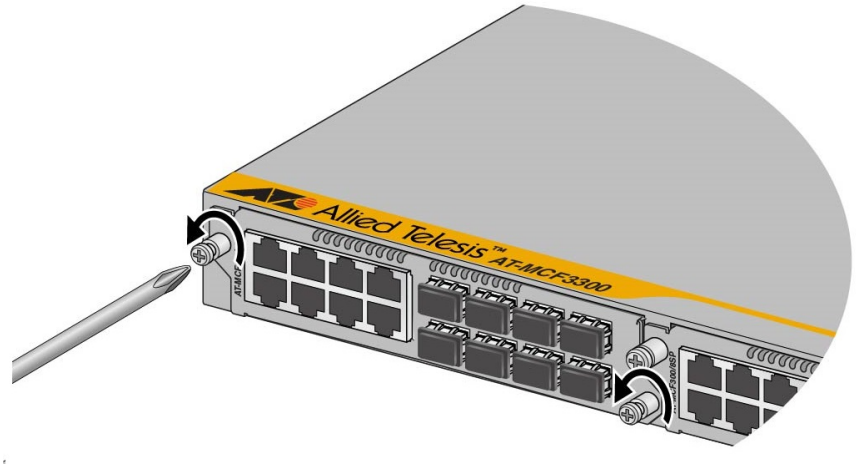


Figure 9. Loosening the Two Captive Screws on a Media Converter Module

5. Slide the module from the unit. Refer to Figure 10.

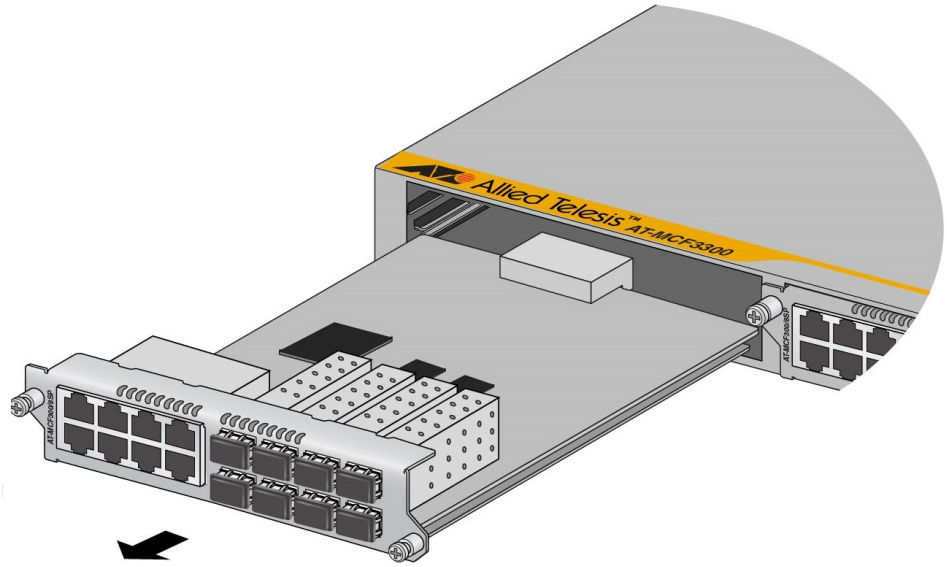


Figure 10. Sliding a Media Converter Module from the Chassis

6. Repeat this procedure to remove all media converter modules from the chassis.

7. Go to “3. Uploading Version 2.0 Software to the MCF3000M Management Module” on page 72

3. Uploading Version 2.0 Software to the MCF3000M Management Module

This section contains the procedure for uploading the Version 2.0 software to the MCF3000M management module from a USB flash drive.

There are two update files, one for the Version 1.3 bootloader and a second for the Version 2.0 management software. Here is the filename for Version 1.3 bootloader and its MD5 checksum:

- Bootloader filename: mcf3000m-u-boot-a38x-1.3.rel.
- MD5 checksum: 23497c448acfe12745bd6c89859ffeae

Here is the filename for the Version 2.0 management software and its MD5 checksum:

- mcf3000m-rootfs.ubifs-2.0-1027.rel
- 8203bd3d9acfce996994b409decfef00

Note
This procedure assumes that you have already obtained the Version 2.0 files from the Allied Telesis web site and stored them on a USB flash drive with a FAT format.

Note
This procedure can also be performed with a TFTP server. For instructions, refer to the *MCF3000 Series Multi-channel Media Converters Command Line Interface User Guide*.

To upload new MCF3000M management module firmware from a flash drive in the USB port, perform the following procedure:

1. Obtain the new Version 2.0 software files from the Allied Telesis web site and store the files on a USB flash drive that has a FAT format.
2. Power on the MCF3000 chassis.
3. Wait thirty seconds for the MCF3000M management module to initialize the management software.
4. Insert the USB drive with the Version 2.0 management software files into the USB port on the management module. The management module automatically connects to the flash drive.
5. Start a local command line management session. Refer to Appendix B, “Starting a Local Management Session” on page 81 for instructions.

6. Enter the SHOW FILES command to display the directory on the USB flash drive. This is to confirm that the management module can read the files on the flash drive.

```
MCF3000M>>show files
```

7. Enter the UPDATE MGMT USB command to upload the new Version 1.3 bootloader file to the MCF3000M management module. Here is the format of the command:

   update mgmt usb *filename md5_checksum*

   Here is the command:

```
MCF3000M>>update mgmt usb mcf3000m-u-boot-a38x-1.3.rel
23497c448acfe12745bd6c89859ffeae
```

   Note
   You must upload the bootloader first.

   Note
   The checksum is case sensitive. Letters must be lowercase.

8. Wait two minutes for the management module to upload the new bootloader, reboot once, and initialize its management software.

9. Start a new command line management session.

10. Enter the UPDATE MGMT USB command to upload Version 2.0 management software to the management module. Here is the command:

```
MCF3000M>>update mgmt usb mcf3000m-rootfs.ubifs-2.0-
1027.rel 8203bd3d9acfce996994b409decfef00
```

    Note
    The checksum is case sensitive. Letters must be lowercase.

11. Wait three minutes for the system to upload the management software, reboot twice, and initialize the management software.

12. Start a new command line management session.

13. Enter the SHOW FIRMWARE INFO command.

14. Examine the “Software” version numbers for both “Management Card Firmware” and “Available Linecard Firmware.” Both numbers should be 2.0. See below.

```
MCF3000M>> show firmware info
Management Card Firmware
   Software: 2.0
   Bootloader: 1.3

Available Linecard Firmware:
   Software: 2.00
   Bootloader:
       1G: 1.3
       10G: 1.0
.
.
.
```

15. Do one of the following:

    - ❒ If the version numbers are correct, continue with the next step.
    - ❒ If the version numbers are incorrect, repeat this procedure.

16. Enter the UNMOUNT USB command to disconnect the USB drive from the management module.

```
MCF3000M>>unmount usb
```

> **Note**
> You must issue the UNMOUNT USB command before removing a flash drive from the USB port. Otherwise, the USB port will be blocked and you will have to boot the chassis to unblock it.

17. Remove the flash drive from the USB port.

18. Go to “4. Reinstalling the Media Converter Modules” on page 75.

4. Reinstalling the Media Converter Modules

Now that the MCF3000M management module has the Version 2.0 management software, you can reinstall the media converter modules. The management module will automatically deliver the new software to the media converter modules over the backplane. Allied Telesis recommends installing and updating one media converter module at a time, as described below.

To install and update the MCF3000 media converter modules, perform the following procedure:

1. If the chassis is powered off, power it on and wait three minutes for it to initialize the management software.

2. Install a media converter module in the chassis by aligning its edges with the guides in the slot. Carefully slide it into the chassis until it makes contact with the backplane connector in the chassis. Refer to Figure 11.

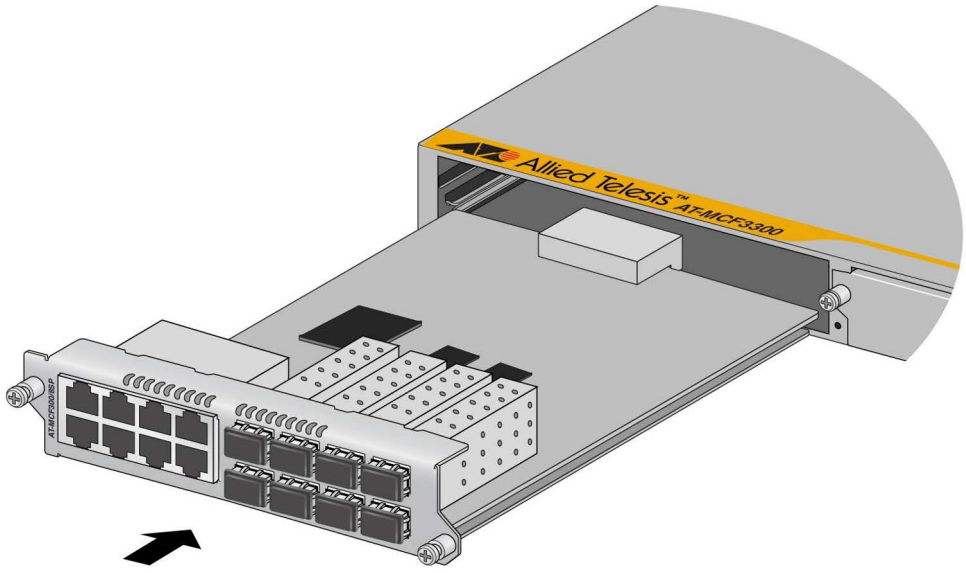


Figure 11. Sliding a Media Converter Module into the Chassis

Caution

Do not force the module into place. If there is resistance, remove the module, verify that the edges of the card are properly aligned in the guides in the chassis' module slot, and reinsert it.

3. Gently press on both sides of the faceplate to seat the module on the backplane connector in the chassis. Refer to Figure 12.

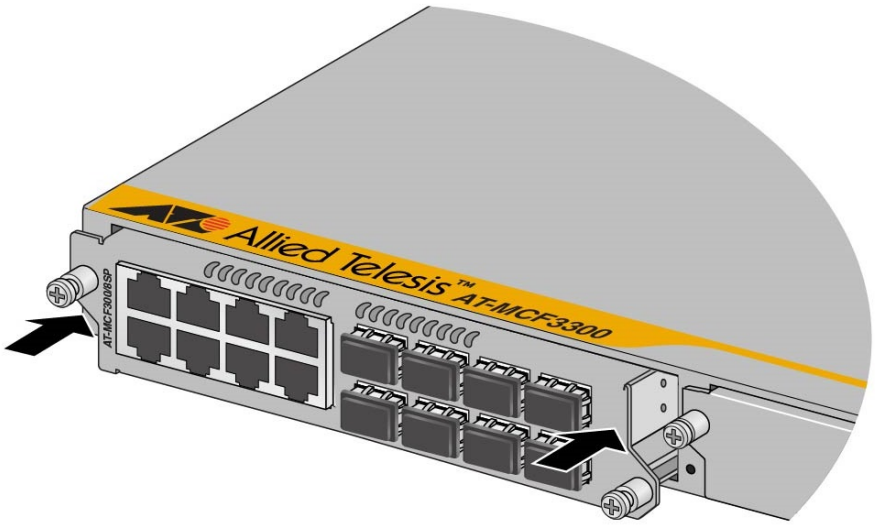


Figure 12. Seating a Media Converter Module on the Backplane Connector

4. Tighten the two captive screws on the media converter module with a cross-head screwdriver to secure it in the chassis. Refer to Figure 13.

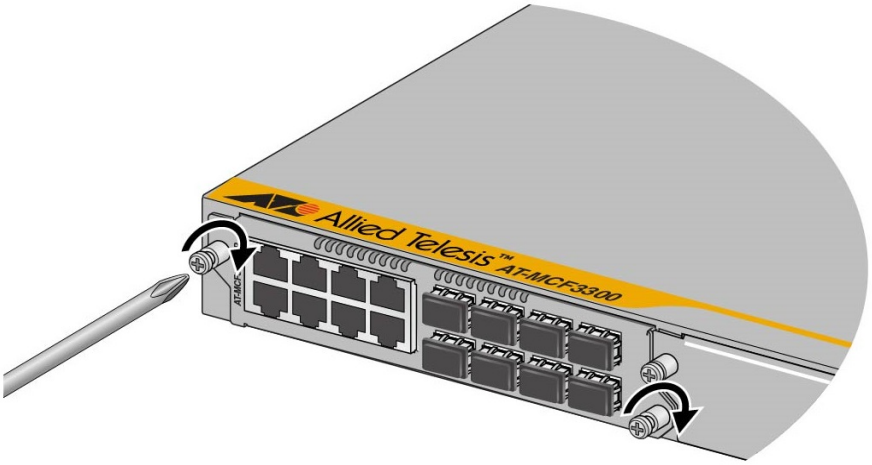


Figure 13. Securing a Media Converter Module

5. Wait three minutes for the media converter module to receive Version 2.0 management software and bootloader from the MCF3000M management module over the backplane in the chassis.

6. Start a new command line management session with the management module.

7. Enter the SHOW FIRMWARE INFO command.

8. Examine the “Software” version number for the “Linecard” that corresponds to the media converter module you installed. The software should be 2.0. In the example below, the MCF3000/8LC media converter module in slot 1 (Linecard 1) is now operating with Version 2.0 management software.

```
MCF3000M>>show firmware info
Management Card Firmware
   Bootloader: 1.3
   Software: 2.0
Available Linecard Firmware:
   Bootloader: 1.3
   Software: 2.00

Linecard 1: MCF3000/8LC
Bootloader: 1.3
   Software: 2.0
.
.
.
```

9. If there is a second media converter module, repeat steps 2 to 8 to install it and confirm that it received Version 2.0 software from the management module.

10. If there is a third media converter module, repeat steps 2 to 8 to install it and confirm that it received Version 2.0 software from the management module.

11. Go to “5. Finishing the Upgrade” on page 78.

5. Finishing the Upgrade

Now that the MCF3000M management module and media converter modules are operating with Version 2.0 software, perform the following procedure to complete the upgrade:

1. Reattach the network cables to the ports on the media converter modules. For instructions, refer to the *MCF3000 Series Multi-channel Media Converters Installation User Guide*

2. Start a new local command line management session. Refer to Appendix B, “Starting a Local Management Session” on page 81

3. Perform the following commands to verify that the chassis has retained its previous configuration and that the ports have established connections to active local or remote devices:

   - ❒ If the chassis previously had an IP address, perform the SHOW NETWORK to verify that it retains the address.
   - ❒ Perform the SHOW PORT SETTINGS command to verify the parameter settings of the ports on the media converter modules.
   - ❒ For ports connected to active network devices, perform the SHOW PORT STATISTICS command to verify that the ports have established links to the devices and are actively forwarding traffic. You can also view the Link/Activity LEDs on the front panels of the modules.

Caution

DO NOT restore the configuration settings by downloading a backup configuration file from an earlier version of the management software. The results may be unpredictable. Instead, if any of the configuration settings are incorrect, use the command line or web browser interface to correct them.

4. Enter the SHOW DATE command to verify that the date and time are set correctly. If they are not correct, reset them with the CONFIGURE TIMEZONE and CONFIGURE DATE commands.

5. Go to “6. Creating a Backup Configuration File” on page 79.

6. Creating a Backup Configuration File

Now that the chassis has Version 2.0 management software, Allied Telesis recommends creating a backup configuration file of the operational settings.

Caution
Do not restore a backup configuration file from an earlier version of the management software to the chassis. The results may be unpredictable.

To create a backup file of the configuration settings of the chassis, perform the following procedure:

1. Insert a flash USB drive into the USB port on the management module. The management module automatically connects to the drive.

   Note
   There is a MOUNT USB command for manually connecting the management module to the USB port. You should never need to use it. You may see an error message if you enter it.

2. Enter the SHOW FILES command to display the directory on the USB drive. This is to confirm that the management module is connected to the drive and can read its files.

   ```
   MCF3000M>>show files
   ```

3. Enter the BACKUP SETTINGS command.

   ```
   MCF3000M>>backup settings
   ```

   The management module stores a copy of its configuration file on the USB drive and displays a confirmation message. The filename is “mcf3000_backup.bin”. This takes only a few seconds. Here is an example of the confirmation message:

   ```
   System database successfully copied to USB drive.
   ```

   Note
   The confirmation message might include a checksum value. It can be ignored.

4. Issue the UNMOUNT USB command.

```
MCF3000M>>unmount usb
```

Note
You must issue the UNMOUNT USB command before removing a flash USB drive from the USB port. Otherwise, the USB port will be blocked and you will have to boot the chassis to unblock it.

5. Remove the flash drive from the USB port.

This completes the upgrade procedure.

Appendix B
Starting a Local Management Session

The procedure in this appendix explains how to start a local command line management session on the MCF3000M management module, using the micro-USB Console port and the provided management cable.

> **Note**
> Local management of the management module requires the CP210x USB to UART Bridge Virtual COM Port (VCP) driver from Silicon Labs. You have to install the driver on your management workstation or laptop computer. The driver is not available from Allied Telesis.

To start a local management session on the MCF3000M management module:

1. Connect the micro-USB connector on the management cable to the CONSOLE port on the management module. Refer to Figure 1.

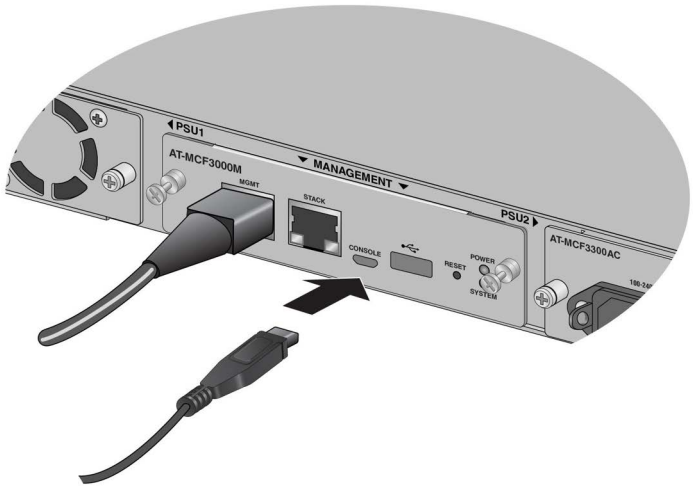


Figure 1. Connecting the Management Cable to the CONSOLE Port

2. Connect the USB Type A connector on the management cable to a USB port on your computer. Refer to Figure 2.

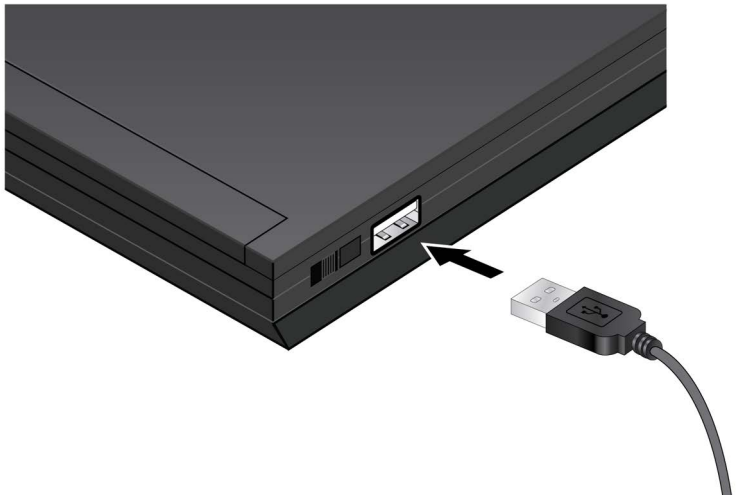


Figure 2. Connecting the USB Cable to Your Computer

3. Configure the terminal or terminal emulator program as follows:

   - ❒ Baud rate: 115200 bps (The baud rate of the RS-232 Terminal port is adjustable from 9600 to 115200 bps. The default is 115200 bps.)
   - ❒ Data bits: 8
   - ❒ Parity: None
   - ❒ Stop bits: 1
   - ❒ Flow control: None

   The terminal emulator also needs to know the COM number of the Silicon Labs driver. If your program does not automatically display COM numbers and you are using Microsoft Windows, open the Device Manager and display Ports (COM & LPT) to view the numbers.

Note
The port settings are for a DEC VT100 or ANSI terminal, or an equivalent terminal emulator program.

Note
If you reset or power cycle the chassis during a local management session and press any key while the system is initializing its operating system, the management module might not complete the initialization process and instead display the “MCF3000M>” prompt without the login prompt. If this happens, type “boot” to instruct the management module to perform the initialization process again.

4. Press Enter.

   The management module displays:

   ```
   Welcome...
   MCF3000 login:
   ```

5. Enter the user name of a manager account. The module comes with two on-board accounts. The login names are “manager” and “user1”. The manager account lets you view and change all system parameters, as well as view traffic statistics. The user1 account is only used to view the parameter settings and traffic statistics.

   After you enter the user name, the management module displays:

   ```
   Password:
   ```

6. Enter the password of the manager account you are using. The “manager” account has the default password “friend”. The “user1” account has the default password “user1”.

   The management session starts and the command line interface prompt is displayed:

   ```
   You are logged in as manager:
   MCF3000M>>
   ```

7. To display a list of commands, press the Return key.

8. To end a management session, enter **quit**.

Note
To protect the security of the media converter, you should always log out after completing your management sessions.

Appendix C

Version 1.0 Management Software Release Notes

This appendix contains the software release notes to version 1,0 of the management software for the MCF3000 Series of management and media converter modules. The appendix has the following sections:

Software and Bootloader Versions

This appendix applies to these previous software and bootloader releases:

- MCF3000M management module:
  - Software: v1.00
  - Bootloader: v1.2
- MCF3000 media converter modules:
  - Software: v1.00
  - Bootloader: v1.1

Supported Platforms

The releases support the following modules:

- MCF3300 chassis
- MCF3000/8LC media converter module
- MCF3000/8SP media converter module
- MCF3010SP/4SP media converter module
- MCF3000M management module
- MCF3300AC power supply
- MCF3300DC power supply

Operational Notes / Known Issues

- The BACKUP SETTINGS command in the command line interface might assign incorrect creation dates and times to backup configuration files that are saved on flash drives in the USB port.
- The BACKUP SETTINGS command does not display an error message if the management card cannot access the USB drive to save backup configuration files. To avoid this issue, always perform the SHOW FILES command before the BACKUP SETTINGS command to confirm that the management module can read the flash drive in the USB port.
- The media converter modules do not support Auto-Negotiation for flow control. Consequently, do not use Auto-Negotiation for flow control on network devices. Instead, set their flow control to either Enabled or Disabled to match the flow control settings on the media converter channel ports.
- The MCF3000/8SP media converter module might show valid links on 100Mb transceivers that are cabled to 1Gb network devices.
- Flow control might unexpectedly change from enabled to disabled on copper ports in half-duplex mode.
- The management module might set the states of the Telnet and SSH servers incorrectly when you restore the factory default settings or upload a backup configuration file. You should check the states of the servers with the management interfaces, and set them as desired, after performing either procedure. The default setting for the servers is enabled.
- The management module might not reset the date and time when the chassis is returned to the factory default settings.

Firmware Update Notes / Known Issues

- If the management module displays the bootloader version number v2020.06.09 in the management interfaces after you upload a newer bootloader, try booting the system again.
- When media converter modules are hot-swapped in a chassis where Allow Updates is set to enabled, they should automatically retrieve the available bootloader and software from the management module before forwarding traffic on their channel ports. You can confirm this by comparing the version numbers of the available firmware on the management module and the firmware on the media converter modules themselves. The command for this in the command line interface is SHOW FIRMWARE INFO.

  If a hot-swapped media converter modules does not retrieve the available firmware from the management module, you will have to update the media converter bootloader and software on the management module again and boot the system. The steps are listed here and explained in the MCF3000 user guides:

  1. Upload the latest bootloader and software for the media converter modules to the management module.
  2. Set Allow Updates to enabled.
  3. If you are using the web browser interface, save the configuration.
  4. Boot the system.
- If media converter modules do not resume normal operations two minutes after retrieving new bootloader and software from the management module, try booting the system.
- Media converter modules always retrieve both the bootloader and software from the management module when Allow Updates is set to enabled and the system is booted.
- The management module might return the system date and time to the default values when you update its software. This only occurs when the date and time are set manually. Setting the date and time again resolves the issue.