Avaya M12-100T/M12-100F Ver. 3.1 Release Notes

Introduction

This document contains information relating to the M12-100T/M12-100F module, with DomainX OBA (On-Board Agent) S/W Version 3.1.1.
This document also describes compatibility issues.

Contents

These Release Notes contain the following Sections:

- Important Notes
- New Functionality
  - Port Auto Negotiation support (M12-100T only)
  - Port priority support
- Functionality introduced in previous releases
- Problems Fixed
- Known Problems
- Where to Get the Software
- How to Download Software to the Module.

Important Notes

Avaya M770 and Avaya P580

When you have an Avaya M770 and an Avaya P580 switch in the same network, do not assign any ports to VLAN #255. This is because the Global VLAN (#255) concept is not supported on the Avaya P580.

Module Software Version

- All modules must have software version 3.1 in order to support the functionality of this version
- Modules running version 1.*x* are not supported in this version.

Upgrading Module Software

Software upgrade must be performed as follows:

- Download the new code (3.0.9) using the Download Application or Terminal to the M-SPV/M-SPX Supervisor module
- Download the new code (3.1.1) using the Download Application or Terminal to all DomainX modules
- Reset the hub or reset all modules to activate the new S/W version on all modules.

Sideband Management Connection

Connectivity from a DomainX port to the M-SPV/M-SPX Supervisor module is achieved by using the Sideband connection. Once the connection is established, the speed of the 10/100 Mbps port should not be changed.

Changing the speed from 10 Mbps to 100 Mbps or visa-versa may result in loss of connection.

To regain connection perform one of the following:

- Disconnect the Sideband connection, and then reconnect it
- Reset the M-SPV/M-SPX Supervisor module.

New Functionality

Port Auto Negotiation support (M12-100T only)

You can enable/disable the Autonegotiation mode using the Port Configuration window, in the CajunView™ management platform.

The default Autonegotiation mode is *enabled*.

When Autonegotiation is enabled, the module should automatically identify the speed and the duplex mode for the port. If Autonegotiation mode is not enabled at the other end, then the M12-100T module will use its Autosensing capability to set the speed of the connection as configured at the other end. In this case, the duplex mode will be set to half-duplex.

Port Priority Support

You can configure a port to be in High or Regular priority mode. Packets entering the switch via a High priority port will have preference over packets entering the switch through a Regular priority port.

The default port priority is Regular priority.

Functionality Introduced in Previous Releases

Secure Telnet - Agent Security

Configuring Authorized Managers

This section describes how to view and set up a list of IP addresses of authorized managers. An authorized manager is any station that is listed in the Secure Allowed Table and has the permission to manage the module using SNMP and/or Telnet.

Once you enable the management security feature, then only authorized managers that have been specified in the security tables will be able to manage the module.

A maximum of 20 concurrent stations that can manage a single module when management security is enabled, otherwise the number is unlimited.

Listing all authorized managers

You can list all stations that are set up as authorized managers in the M-SPV/M-SPX. For each station in the table the index entry number and IP address are displayed.

To display a list of authorized managers, choose Option 12 from the Setup Main Menu and then Option 2, List.

```
Agent Security Menu
S/W Version: 3.0.9 Slot #: 15

<CR> Refresh the screen
 0.  Return to Previous Menu
 1.  Enable/Disable
 2.  List
-----------------------------
 3.  Add[]
 4.  Delete[]
>>>Enter your choice: 2
Agent Security is enabled

1 ) 150.67.88.24
 : :
20) Not Used

>>>Enter CR to continue:
```

Setting up an authorized manager entry

You can add up to 20 authorized managers into the Secure Allowed Table. Only these authorized managers will be able to access this module.

To add an authorized manager, choose Option 3, “Add” from the Agent Security Menu.

```
>>>Enter your choice: 3
Agent Security is enabled

1 ) 150.67.88.24
 : :
20) Not Used

>>>Enter ip address (nnn.nnn.nnn.nnn):149.49.36.200

>>>Enter CR to continue:
```

Deleting an authorized destination station

To delete an authorized manager station from the Allowed Table, choose Option 4, “Delete” from the Agent Security Menu.

```
>>>Enter your choice: 4
Agent Security is enabled

1 ) 150.67.88.24
 : :
20) Not Used

>>>Enter ip address (nnn.nnn.nnn.nnn):149.49.36.200

>>>Enter CR to continue:
```

Enabling/Disabling the authorized managers table

Before enabling/disabling management security, ensure that you have set up your station in advance, as an authorized manager in the Allowed Secure Table, otherwise you will not be able to manage the module via SNMP or Telnet.

To enable/disable the secure mode, choose Option 1, “Enable/Disable” from the Agent Security Menu.

```
>>>Enter your choice: 1
Agent Security Disabled

 *** Do You wish to Enable it?
 ***, Confirm [y/n]? y
Done

   >>>Enter CR to continue:
```

Secure Telnet - Passwords and Security

Software Version 2.5 and higher provides Secured Telnet. This means that in order to access the Main Menu of the module's Command Line Interface (CLI) via Telnet you must enter a User Name and Password.

There are four security access levels – configuration, privileged, technical support and super-user. The levels are defined as follows:

The “conf” user is used for minimal management and includes the current agent menus.

The “priv” user has full management access but currently this access level is the same as the previous level, “conf”.

The “tech” (technical support) user is for technical support personnel and includes access to basic debugging and log information.

The “super” (super-user) user has the right to change the passwords for all levels except for the hidden static password.

To access the Change Authentication menu select **Users and Passwords** from the Setup Main Menu.

Note:

1. Connecting by a direct connection to the console port of the Avaya M770 chassis can terminate a current Telnet connection.
2. If a user has forgotten the Telnet password, it can be reconfigured via a direct connection to the Console port.
3. Only one Telnet connection is possible at one time.

Default VLAN 1

So far the Default VLAN was 0. Software Version 2.5 and higher allows you to define the default VLAN to the value 1, as specified by IEEE 802.1Q standard.

You can change the default VLAN from the M-SPV/M-SPX Setup Menu. Once you have changed it to 1. Assuming that all modules in the chassis have S/W Ver. 2.5 or higher, after the reset all modules should have default VLAN 1. All switch ports assigned to VLAN #0 will be automatically reassigned to VLAN #1.

Warning: If you use VLANs in your network do not use VLAN0.

Software Redundancy

Version 2.5 of the software introduced a speed-up in the switchover from the Main to the Redundant link in case the Main link fails.

Note:

1. All modules must have S/W Ver 2.5 or higher installed including the M-SPV/M-SPX.
2. Ensure that the software redundancy option is enabled in the Device Configuration window.

You cannot manually enable a dormant port when software redundancy is active on that port. First disable redundancy on the dormant port and then enable the port.

VLAN Information Distribution Protocol (VIDP)

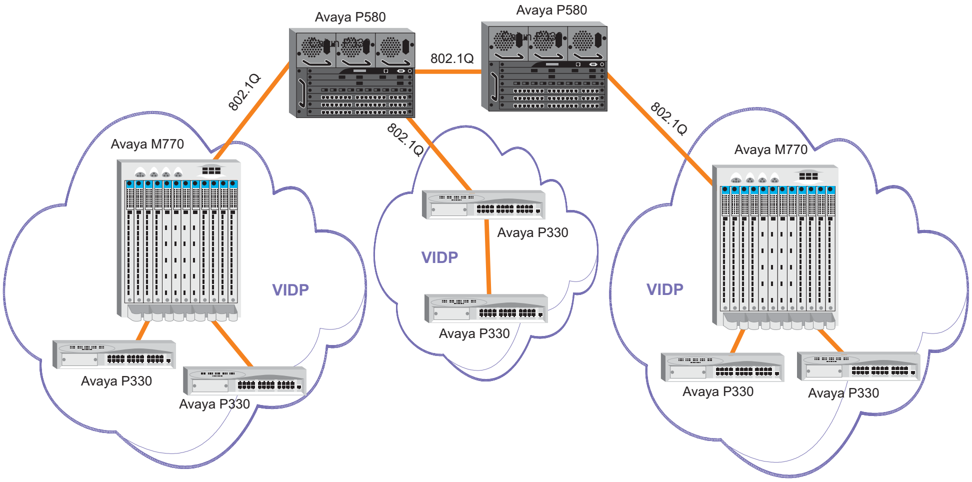
Description

VIDP is a VLAN per-MAC Distribution Protocol, which is used to propagate VLAN-to-MAC information between M770 and P330 switches over regular non-tagging Ethernet backbone ports. Each switch distributes that information for all its local stations to all other M770/P330 switches in the network. It allows an implicit VLAN mapping of incoming packets according to their source MAC address.

Although the VIDP protocol was created to allow VLAN connectivity between Avaya P330 and M770 switch through non-tagging ports, the introduction of the standard 802.1Q tagging in current networks created a situation of mixed configurations of standard 802.1Q tagging and VIDP.

802.1Q's VLAN per-packet mechanism is interoperable with VIDP's VLAN per-MAC mechanism. A typical network is comprised of one or more Avaya P580s (LANswitch or other) switches in the backbone of the network, connected through standard 802.1Q tagging links to Avaya P330/M770-based sub-networks that use the VIDP protocol to share MAC-VLAN mapping information between them.

The following Figure shows a typical application.



802.1Q VLAN Tagging to VIDP Preparations

Before you can use VIDP you must ensure that:

- VIDP is enabled on all connected switches (see below, Using VIDP).
- All Avaya M770 modules including the M-SPV/M-SPX have S/W Ver. 2.5 or higher.
- All Avaya P110 NMA agents must have S/W Ver. 8.7 or higher.
- You have CajunView 2.2 and downloaded and installed the latest CajunView update from the Web site: http://avayanetwork.com/site/software/index.htm

Note: The default VLAN in the system should be 1 (not 0).

Using VIDP

You can enable or disable VIDP (factory default is disabled) using the Avaya M770 Device Manager (Zoom view) within the CajunView Suite. In the Zoom View select Configuration → Device Information. The Device Information window opens. Here you can enable/disable VIDP.

Note: A non-tagging VIDP backbone port cannot manually be assigned to a specific VLAN. In this case it is automatically assigned to the Global VLAN (255).

Interoperability

You can use VIDP with Avaya M440 and Avaya M770 in the network under the following conditions:

If you are using Avaya M770 with VIDP and there is an Avaya M440 Gate Switch in the network (connected via LGE-2000 in IEEE 802.1Q tagging mode), you should use the Avaya M770 M-MLS Multilayer module, not the Avaya M440 3LS as your router.

Warning: Special VIDP Cases

1. You cannot use VIDP and VLAN Bridging at the same time. figure VIDP cannot coexist with tagged stations using the same MAC address over different VLANs since VIDP uses VLAN per MAC addressing mechanism.
2. After you connect a station for the first time to a switch running VIDP, you should reboot the station.
3. Before you change mode from VIDP enabled to disabled or vice versa you should wait at least 30 seconds.
4. After changing VLAN tagging mode to VLAN per port mode, while VIDP is enabled, requires a module reset.
5. You cannot run VIDP on a mixed network with both Avaya M770 and P110 switches if you have more than: 1,500 connected stations for P110 version **8.7** or 5,000 connected stations for P110 version **8.9**.
6. You cannot insert an M32-100T into a Domain where VIDP is running.

Spanning Tree Protocol (STP)

Description

The Avaya M770 now implements the IEEE 802.1D Spanning Tree (STP) which allows backup paths and prevents loops throughout the Physical LAN. The Avaya M770 uses a single STP for Bridged LAN according to IEEE 802.1D.

Preparations

Before you can use STP you must ensure that:

- STP is enabled on all connected switches (see below, Using STP).
- All Avaya M770 modules including the M-SPV/M-SPX have S/W Ver. 2.5 or higher (modules with S/W version less than 2.5 can coexist in the same switch but they will not be able to implement STP on their port).
- You have CajunView 2.2 and have downloaded and installed the latest CajunView update from the Web site: http://avayanetwork.com/site/software/index.htm.

Using STP

You can enable or disable STP (factory default is disabled) using the Avaya M770 Device Manager (Zoom view) within the CajunView Suite. In the Zoom View select Configuration ▶ Device Information. The Device Information window opens. Here you can enable/disable STP.

When you insert a new module (S/W Ver. 2.5 or higher), into an Avaya M770 chassis in which STP is enabled, then STP will automatically configure all new ports to blocking state until STP recalculates.

Note:

1. A single STP (802.1D) is supported in the Avaya M770. STP per VLAN or Dual Layer STP (Avaya P580 modes) are not supported.
2. We recommend that you do not use Spanning Tree together with Software Redundancy.

Interoperability between Avaya M770 and P580

You must use the single STP mode on the P580 when working with the Single STP of the M770.

When using VLANs, all backbone connections should be in 802.1Q VLAN Tagging Mode.

Ensure that VLAN 255 on the Avaya P580 has been created (this limitation will be fixed in a future version). Do not assign any ports to this VLAN.

Special Spanning Tree Cases

Before you change mode from STP enabled to disabled or vice versa you should wait at least 30 seconds.

VLAN Bridging Mode

Inter-VLAN Bridging allows non-IP/IPX communication to cross VLANs, which were originally formed according to IP or IPX criteria (VLAN=IPsubnet, etc.).

In order to support Inter-VLAN Bridging in M770-based networks, you should do *all* of the following:

Configure a single M-MLS to perform VLAN Bridging

1. Enable VLAN Bridging mode in all M770 switches
2. Use Gigabit backbones with “Plus Tagging” mode between the switches.

The M-MLS is able to bridge broadcast/multicast packets of protocols, that are not routed (i.e. not IP or IPX), between a group of VLANs which are defined by the user. When bridging is active, non-IP/IPX packets, received on a VLAN, will be bridged to the other VLANs in the same group.

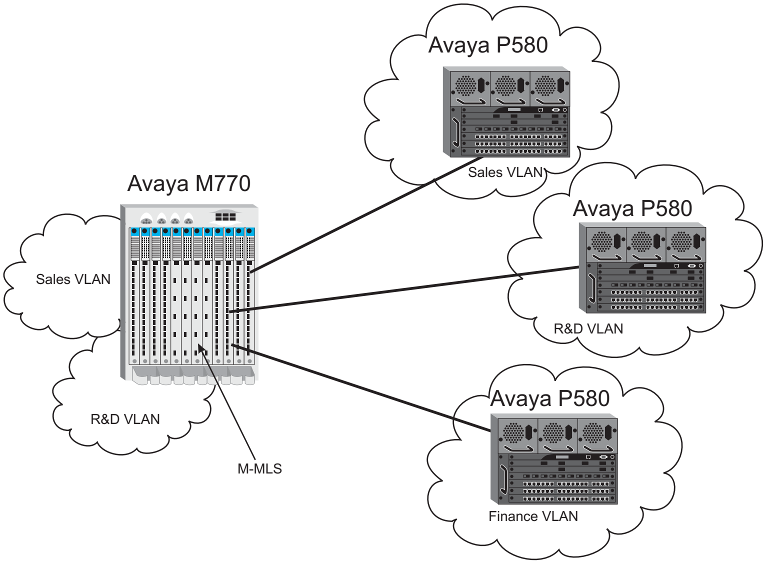
The user can define a list of VLANs to the following protocols:

- DEC
- NETBIOS
- APPLETALK
- OTHER (all other protocols will be bridged according to the group of VLANs defined by the user).

Warning: You cannot use both VLAN bridging and VIDP at the same time.
The backbone ports should use Plus Tagging (not VIDP).

Note:

1. In order to forward bridging unicast packets, the Avaya M770 chassis must be in VLAN bridging mode. To enable this mode in the CajunView Suite's Avaya M770 Device Manager, select, from the menu, Configuration ▶ Device Information Window and change the VLAN Bridging field to "enabled".
   To allow the transfer of bridged packets between different chassis, the backbone port must be in plusTagging mode. Select the port in the Zoom view and then select, from the Menu, Configuration ▶ Element ▶ Port Window and change the Tagging field to "plusTagging" .
2. When you move a station from one VLAN to another while in Bridging mode, it may take up to 20 seconds for the changes to take effect.
3. Versions of the Avaya P110 prior to 8.9 and P580 switches do not support VLAN Bridging, so Inter-VLAN Bridging mode cannot be used in mixed networks with M770. See the following figure for valid Bridging options within mixed networks.



How to connect an Avaya M770 to another switch family in bridging mode

Each switch (except another Avaya M770) connected to the Avaya M770 should be in a single VLAN. The ports on the Avaya M770 connected to the switch as well as all ports connected to that switch should be configured to the same VLAN. The Avaya M770 performs bridging between VLANs from one switch to another.

The backbone between the Avaya M770 and other switches should be in VLAN-per-port mode (not Tagging mode).

In the above figure:

- The port of the Avaya M770 connected to the topmost Avaya P580 should be assigned the "Sales VLAN".
- The port of the Avaya M770 connected to the middle Avaya P580 stack should be assigned the "R&D VLAN".
- The port of the Avaya M770 connected to the bottommost Avaya P580 stack should be assigned the "Finance VLAN".

Port Mirroring

General

- The Port Mirroring feature supports the standard Switch Monitoring MIB (ftp://ftp.isi.edu/in-notes/rfc2613.txt), as well as Avaya Proprietary MIB.
- The Port Mirroring feature allows you to copy all transmitted and received traffic from a source port to a destination port.
- In every DomainX the Port Mirroring works with a single source and a single destination.

- You can configure Port Mirroring, per DomainX, using the M770 CajunView Manager.

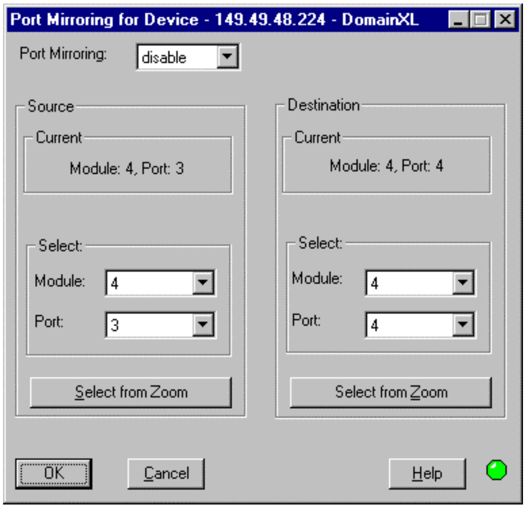
Using the Port Mirroring Application

In order to launch the Port Mirroring function, you should use the CajunView Suite's Avaya M770 Zoom application (see Important Notes on Page 16 regarding CajunView versions):

From the Avaya M770 Zoom view pull down the Configuration Menu, choose **Port Mirroring** and select DomainXL or DomainXR:

Configuration ▶ Port Mirroring ▶ DomainXL *or* **▶ DomainXR**

The following window opens:



Port Mirroring for Device - 149.49.48.224 - DomainXL

Port Mirroring: disable

Source

Current: Module: 4, Port: 3

Select: Module: 4 Port: 3

Destination

Current: Module: 4, Port: 4

Select: Module: 4 Port: 4

Within the Port Mirroring for Device application, select the Source port (left hand column) and the Destination port numbers (right hand column), from the list of available modules/ports (or from the Zoom selection). Then confirm the configuration by clicking OK.

Interoperability and Limitations

- Under heavy network traffic do not use 100 Mbps Ethernet as a source port to a 10 Mbps Ethernet destination port.
- Before you can use the Port Mirroring feature, the M-SPV/M-SPX Supervisor module must have S/W Ver. 3.0.5 or higher and DomainX modules must have S/W Ver. 2.6 (or higher).
- Destination port is assigned automatically to the same VLAN as the Source port.
- Do not change the VLANs of the Source and the Destination ports while Port Mirroring is enabled.

- If a port is disabled or its link is down, then it cannot be used in Port Mirroring (this is an SMON MIB Standard requirement).
- You cannot use a 1000BaseX port as a Source/Destination port.
- A Destination port cannot be a member in S/W Redundancy application.
- Do not change the Port Administration status of the Source and the Destination ports while Port Mirroring is enabled.
- If either the Source or Destination port enters Blocking mode because of STP, then Port Mirroring becomes disabled
- You cannot activate Port Mirroring on ports (source or destination) that are in blocked STP state.
- If an M32-100T port is configured as a Destination port, you must use another M32-100T port as the Source port. However if the source port is the M32-100T, you can use any other 10/100 Mbit/s port as a Destination port

MIB-II Interface Tables

S/W Version 2.6 and higher supports the `ifTable` and the `ifXTable` counters for every switched Ethernet port.

ifIndex, *ifName* and *ifAlias* Parameters

The ***ifIndex*** parameter is calculated using the formula 1024*S+P, where S is the slot number and P is the port number. For example the ***ifIndex*** used for port number 3 in slot number 4 is: (1024 * 4 + 3) = **4099**.

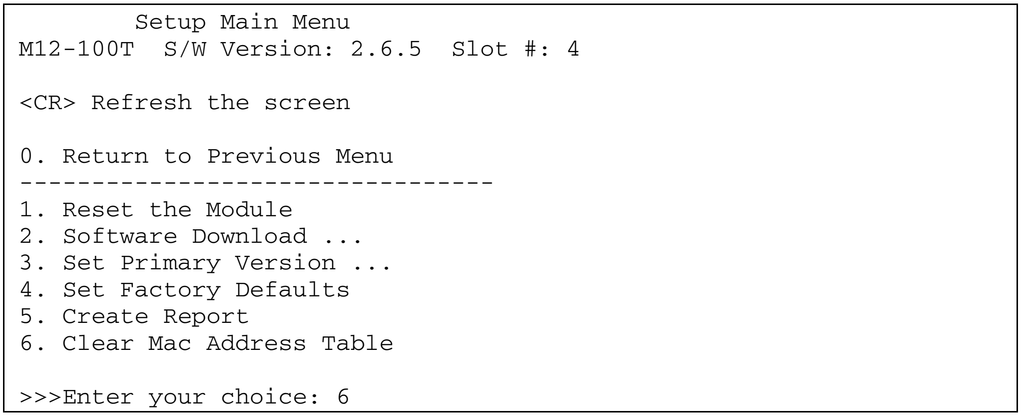
The ***ifName*** parameter shows the mapping to the module name, slot number, port number and VLAN defined on this port for each interface. For example if interface number 4099 is on module M12-100T/M12-100F and this interface is assigned to VLAN number 125, the resulting ***ifName*** is: **M12-100T/M12-100F.4.3.V125**.

Use the ***ifAlias*** Parameter to assign an alphanumeric string (up to 63 bytes long) to a port for identification purposes.

Clear Mac Address Table

Option 6 from the Main Menu 'Clear Mac Address Table', allows you to clear the MAC address table of the entire Avaya M770 domain from a single point.

Module Setup Main Menu



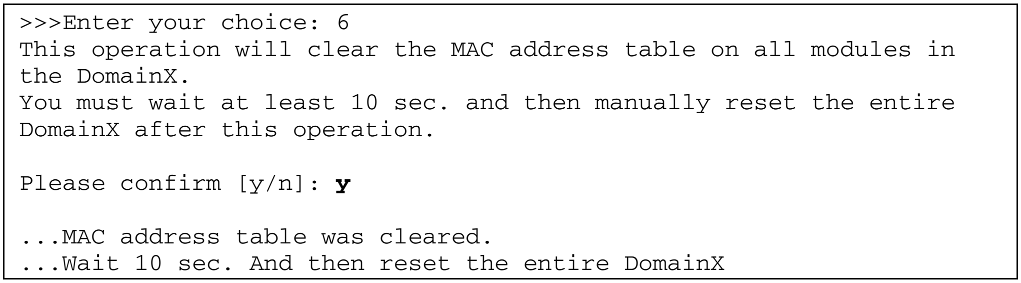
```
        Setup Main Menu
M12-100T  S/W Version: 2.6.5  Slot #: 4

<CR> Refresh the screen

0. Return to Previous Menu
---------------------------------
1. Reset the Module
2. Software Download ...
3. Set Primary Version ...
4. Set Factory Defaults
5. Create Report
6. Clear Mac Address Table

>>>Enter your choice: 6
```

When you choose Option 6, the following menu appears. Select **`y`** to confirm or **`n`** to cancel:



```
>>>Enter your choice: 6
This operation will clear the MAC address table on all modules in
the DomainX.
You must wait at least 10 sec. and then manually reset the entire
DomainX after this operation.

Please confirm [y/n]: y

...MAC address table was cleared.
...Wait 10 sec. And then reset the entire DomainX
```

After system reset, the MAC address table on all modules in the DomainX is cleared.

Note: The above command takes effect only after you perform a reset (wait at least 10 seconds before resetting, in order to complete this operation).

Note: The 'Clear MAC Address Table' command can be executed from one of the modules in a DomainX only.

CajunView Management

You can download and install the latest update of CajunView at the following Web Site: http://www.avayanetwork.com/site/software/index.htm.

Problems Fixed

Note: The fixed problems listed below only occurred sometimes.

- Avaya M770 modules no longer freeze when generating packets with a multicast source address.
- Creating a report no longer leads to an Avaya M770 module freezing or automatically resetting.

Known Problems

DRU Overload

Warning: Always verify that the DRU calculation *never* exceeds 100 DRUs.

A DRU overload can be identified by:

- Blinking OPR LED of each module (can also indicate a module fault).
- Via the CajunView Avaya M770 Manager, check the DRU report window (in the Configuration drop-down Menu).
- Using the “Set Show” command in the Zoom view of the CajunView Avaya M770 Manager NMS application.

Setup Session

Error messages may appear during an Open Setup Terminal session. These messages should be ignored.

VIDP modules

After inserting a module from a domain with VIDP OFF into a domain with VIDP ON, the module must be restarted.

Where to Get the Software

In order to benefit from the latest features, the module must use the latest software version. Modules loaded with earlier versions should be upgraded by performing a software download.

To check what software version you have, view the main setup menu of the module or the module configuration screen in the management console.

World-Wide Web

You can download the latest agent software from the Avaya Network Web Site.

1. Go to the Avaya Network Software Download Site using your WWW browser: http://www.avayanetwork.com/site/software/index.htm.
2. Click on the Avaya M770 icon (Avaya M770).
3. Click on "Avaya M770 Switch" in the list of Latest Software Download Versions.
4. Under "M12-100T" or "M12-100F", click on the Codes icon ( ) to download the file. Details of the file size and accompanying documentation are given for each software version.

How To Download Software to the Module

Software can be downloaded in one of the following methods:

- Using CajunView.
- Using TFTP.

Using CajunView

Software download is most easily performed via SNMP using a CajunView network management station. Instructions can be found in the in the UpdateMaster User Guide.

Using TFTP

Software download can also be performed via TFTP using a terminal connected to the serial port of the M-SPV/M-SPX Superfisor module. Full download instructions can be found in the module's Installation Guide.

To perform the download, the station containing the source file (the CajunView or TFTP Server PC) should be able to reach the M-SPV/M-SPX through the network. The simplest way to test this is to check if you can ping the agent (M-SPX/M-SPV).

AVAYA

Attention: Technical Support

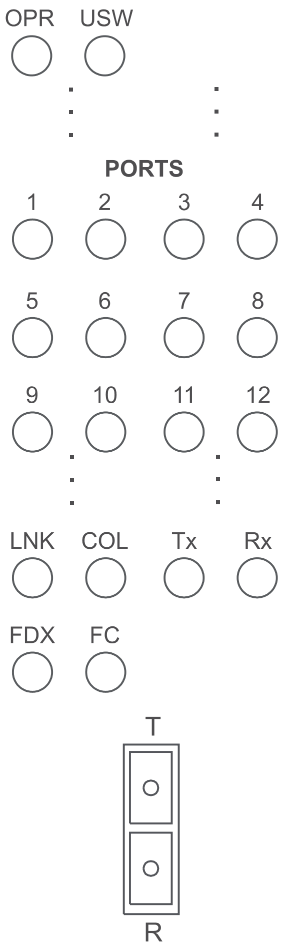
M12-100F Diagnostic Worksheet

1. C/S: ____________________

S/N: ____________________

Manu. Date: ______________

Slot Position: ____________



2. Please Indicate the Status of Each LED
Mark the LEDs on the picture in the following manner:

● If the LED is on

⦶ If the LED is blinking

⊗ If the LED is off

3. Please indicate the DIP switch settings on your module (only if the USW LED is ON).

4. Please include any additional information, such as your network configuration, network protocols and other Avaya M770 modules in the hub.

5. Prepared By: ____________________

Customer: ____________________

Phone: ____________________

Fax: ____________________

Date: ____________________

Please Fax Back to Your Local Avaya Representive

Attention: Technical Support

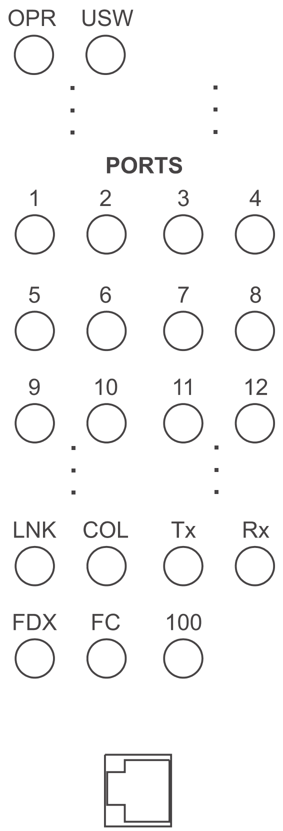
M12-100T Diagnostic Worksheet

1. C/S: ____________________

S/N: ____________________

Manu. Date: ______________

Slot Position: ____________



2. Please Indicate the Status of Each LED Mark the LEDs on the picture in the following manner:

   ● If the LED is on

   ① If the LED is blinking

   ⊗ If the LED is off

3. Please indicate the DIP switch settings on your module (only if the USW LED is ON).

4. Please include any additional information, such as your network configuration, network protocols and other Avaya M770 modules in the hub.

5. Prepared By: ____________________________

   Customer: ____________________________

   Phone: ____________________________

   Fax: ____________________________

   Date: ____________________________

Please Fax Back to Your Local Avaya Representative

avaya.com