TCM SECTOR
SYSTEM AND INSTALLATION GUIDE

Overview

This document includes the system information and installation guide for the TCM Sector.

Please be sure to read the system information and installation warnings carefully before installing the product!

The TCM Sector is a flexible platform with the capability of access point, bridge, and workgroup bridge functionality.

The TCM Sector Provides high speed and cost effective wireless connectivity.

Building a metropolitan area wireless infrastructure with the TCM Sector provides deployment personnel with a flexible, easy to use solution that meets the security requirements of wide area networking professionals.

System information

Cisco Router – Cisco851 is integrated into the TCM Sector. This system supports the 802.11b/g standard – providing 54 Mbps data rates with a proven, secure technology.

Installation:

The multi-function mount provides a method for mounting the TCM Sector on a mast, tower, or a roof mount and consists of two parts:

TCM Sector bracket—attaches to the back of the unit.
Mast bracket—attaches to the mast, tower, or roof mount.

The basic mounting procedure is shown below:

1. Mount the TCM Sector bracket to the mounting lugs on the Sector.
2. Mount the mast bracket to the tower or mast using the supplied U-bolts or appropriately sized user-supplied U-bolts.
3. Suspend the TCM Sector on to the mast bracket using the support pins.
4. Secure the TCM Sector bracket to the mast bracket using the supplied nuts, bolts, and washers (hand tighten).
5. Connect the ground wire to the outdoor mounted TCM Sector using the supplied ground lug.
6. Connect the power cable to the power
7. Connect the data cable.
8. Tighten the nuts and bolts.

OUTDOOR INSTALLATION WARNING

IMPORTANT SAFETY PRECAUTIONS:

LIVES MAY BE AT RISK!

Carefully observe these instructions and any special instructions that are included with the equipment you are installing.

IMPORTANT

Look over the site before beginning any installation, and anticipate possible hazards, especially the following:

CONTACTING POWER LINES CAN BE LETHAL. Make sure no power lines are anywhere where possible contact can be made. Antennas, masts, towers, guy wires or cables may lean or fall and contact these lines.

People may be injured or killed if they are touching or holding any part of equipment when it contacts electric lines.

Make sure there is NO possibility that equipment or personnel can come in contact directly or indirectly with power lines.

Assume all overhead lines are power lines.

The horizontal distance from a tower, mast or antenna to the nearest power line should be at least twice the total length of the mast/antenna combination.

This will ensure that the mast will not contact power if it falls either during installation or later.

TO AVOID FALLING,
USE SAFE PROCEDURES WHEN WORKING AT HEIGHTS ABOVE GROUND.

Select equipment locations that will allow safe, simple equipment installation.

Don't work alone. A friend or co-worker can save your life if an accident happens.

Use approved non-conducting ladders and other safety equipment. Make sure all equipment is in good repair.

If a tower or mast begins falling, don't attempt to catch it. Stand back and let it fall.

If anything such as a wire or mast does come in contact with a power line,
DON'T TOUCH IT OR ATTEMPT TO MOVE IT.
Instead, save your life by calling the power company.

Don't attempt to erect antennas or towers on windy days.

MAKE SURE ALL TOWERS AND MASTS ARE SECURELY GROUNDED, AND ELECTRICAL CABLES CONNECTED TO ANTENNAS HAVE LIGHTNING ARRESTORS.

This will help prevent fire damage or human injury in case of lightning, static build-up, or short circuit within equipment connected to the antenna.

The base of the antenna mast or tower must be connected directly to the building protective Ground or to one or more approved grounding rods, using 1 OAWG ground wire and corrosion- Resistant connectors.
Refer to the National Electrical Code for grounding details.

IF A PERSON COMES IN CONTACT WITH ELECTRICAL POWER, AND CANNOT MOVE DON'T TOUCH THAT PERSON, OR YOU MAY BE ELECTROCUTED.

Use a non-conductive dry board, stick or rope to push or drag them so they no longer are in contact with electrical power.

Once they are no longer contacting electrical power, administer CPR if you are certified, and make sure that emergency medical aid has been requested.

Interference Statement

This device complies with Part 15 of the FCC Rules and with RSS-210 of Industry Canada.

Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Warning: Changes or modifications not expressively approved by the Party responsible for compliance could void the user's authority to operate the equipment

Information to the user

NOTE:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instructions, it may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.
Increase the distance between the equipment and the receiver.
Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
Consult the dealer or an experienced radio/TV technician for help.

Any changes or modifications of equipment not expressly approved by the manufacturer could void the user's authority to operate the equipment and the company's warranty.

The device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

When this device is installed either as a fixed-mount or mobile application there is a minimum required separation distance of 21 cm from users.

Initial Configuration

Installing “Cisco Router and Security” Device Manager

Once you have completed the cable connections and powered up the TCM Sector, we recommend that you use the Cisco Router and Security Device Manager (SDM) web-based application to configure the initial TCM Sector settings.

To install the SDM for configuring the router, follow these steps:

Step 1 Connect a PC to the TCM Sector console port.

Step 2 Insert the SDM software CD into the CD drive of the PC to launch an installation wizard. Install the SDM by following the instructions on the installation wizard user Interface.

Step 3 Use the SDM to configure the TCM Sector.

Initial Configuration Using the SDM

If the following messages appear at the end of the startup sequence, the SDM is installed on the TCM Sector router:

```
Yourname con0 is now available
Press RETURN to get started.
```

Initial Configuration Using the Setup Command Facility

This section describes how to use the setup command facility to configure a hostname for the router, set passwords, and configure an interface for communication with the management network.

If the following messages appear at the end of the startup sequence, the setup command facility has been invoked automatically:

```
--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help. Use ctrl-c to abort
configuration dialog at any prompt. Default settings are in square brackets '[]'.

Would you like to enter the initial configuration dialog? [yes/no]:
```

The setup command facility prompts you for basic information about your router and network, and it creates an initial configuration file. After the configuration file is created, you can use the CLI or Security Device Manager to perform additional configuration.

The prompts in the setup command facility vary, depending on your router model, the installed interface modules, and the software image. The following example and the user entries (in **bold**) are shown as examples only.

Note If you make a mistake while using the setup command facility, you can exit and run the setup command facility again. Press **Ctrl-C**, and enter the **setup** command at the privileged EXEC mode prompt (Router#).

Step 1 To proceed using the setup command facility, enter **yes**:

Would you like to enter the initial configuration dialog? [yes/no]: **yes**

Step 2 When the following messages appear, enter **yes** to enter basic management setup:

At any point you may enter a question mark '?' for help. Use ctrl-c to abort configuration dialog at any prompt.

Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity for management of the system, extended setup will ask you to configure each interface on the system

Would you like to enter basic management setup? [yes/no]: **yes**

Step 3 Enter a hostname for the router (this example uses Router):

Configuring global parameters: Enter host name [Router]: **Router**

Step 4 Enter an enable secret password. This password is encrypted (more secure) and cannot be seen when viewing the configuration:

The enable secret is a password used to protect access to privileged EXEC and configuration modes. This password, after entered, becomes encrypted in the configuration.

Enter enable secret: **xxxxxx**

Step 5 Enter an enable password that is different from the enable secret password. This password is *not* encrypted (less secure) and can be seen when viewing the configuration:

The enable password is used when you do not specify an enable secret password, with some older software versions, and some boot images.

Enter enable password: **xxxxxx**

Step 6 Enter the virtual terminal password, which prevents unauthenticated access to the router through ports other than the console port:

The virtual terminal password is used to protect access to the router over a network interface. Enter virtual terminal password: **xxxxxx**

Step 7 Respond to the following prompts as appropriate for your network:

Configure SNMP Network management? [yes]:
Community string [public]:

A summary of the available interfaces is displayed.

Step 8 Choose one of the available interfaces for connecting the router to the management network:

Enter interface name used to connect to the
management network from the above interface summary: **fastethernet0**

Step 9 Respond to the following prompts as appropriate for your network:

Configuring interface FastEthernet0:
Use the 100 Base-TX (RJ-45) connector? [yes]: **yes**
Operate in full-duplex mode? [no]: **no**
Configure IP on this interface? [yes]: **yes**
IP address for this interface: **172.1.2.3**
Subnet mask for this interface [255.255.0.0] : **255.255.0.0**
Class B network is 172.1.0.0, 26 subnet bits; mask is /16

Step 10 The configuration is displayed:

The following configuration command script was created:

hostname Router
enable secret 5 1D5P6$PYx41/lQIASK.HcSbfO5q1
enable password xxxxxx
line vty 0 4
password xxxxxx
snmp-server community public
!
no ip routing
!
interface FastEthernet0
no shutdown speed 100
half-duplex
ip address 172.1.2.3 255.255.0.0
!

Step 11 Respond to the following prompts. Enter **2** to save the initial configuration.

[0] Go to the IOS command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration to nvram and exit.

Enter your selection [2]: **2**
Building configuration...
Use the enabled mode 'configure' command to modify this configuration.

Press RETURN to get started! **RETURN**

The user prompt is displayed.

Router>

Verifying the Initial Configuration

To verify that the new interfaces are operating correctly, perform the following tests:

- To verify that the interfaces are operating correctly and that the interfaces and line protocol are in the correct state—up or down—enter the **show interfaces** command.
- To display a summary status of the interfaces configured for IP, enter the **show IP interface brief** command.
- To verify that you configured the correct hostname and password, enter the **show configuration** command.

After you have completed and verified the initial configuration, you can configure the TCM Sector for specific functions.

For further information contact:

TCM Ltd.

Address 11 Amal Street, Park Afeq, Rosh Ha'ain, Israel

Phone +972-77-786-6617