Point-M
Corporate Wireless LAN

Owner's Manual

NEC Laboratories America, Inc.
4 Independence Way
Princeton, NJ 08540, U.S.A.
(point-m@nec-labs.com)

Release: December 2002

Content

1 Installation

The initial Point-M installation should preferably be completed in the following order:

1. Install Point-M server.
2. Configure (existing) corporate DHCP server.
3. Install Point-M access points.
4. Install end-user equipment and create end-user accounts.

1.1 Installing the Point-M Server

Most Point-M customers receive the Point-M server hardware custom-build, with the software already pre-installed and pre-configured. Those customers can skip ahead to section 1.1.2.
Customers who received a Point-M installation-CD have to obtain their own PC-based hardware platform and install and configure the server software themselves, as described in section 1.1.1 below.

1.1.1 Installing the Point-M Server Software from CD

1. Select a computer platform that satisfies the following minimum requirements:

CPU:	Intel Pentium, 500 MHz
Memory:	128 MB RAM
Disk:	20 GB hard disk
Network:	1 Ethernet port, 100 Mbps
CD/DVD:	required only during installation; can be removed afterwards.

   Note: If you intend to offer services to more than 30 users simultaneously, we recommend that you upgrade to a 1GHz CPU, and to an 1000 Mbps Ethernet card (provided your corporation's central Ethernet HUB/Switch supports this rate). Memory and Disk requirements will not increase for larger user numbers.

2. Prepare the computer hardware for the software installation:
   - Make sure the CD/DVD drive is attached properly.
   - Insert the Point-M installation CD into the CD/DVD drive.
   - Use the BIOS setup to allow for booting from CD-ROM.

3. Consult with your systems administrator for the following information regarding your existing network:
   - IP address of the corporate DNS server
   - IP address for the corporate RADIUS server (including the access "secret")

- IP Netmask and Gateway for the LAN segment to which the Point-M server will later be attached.

4. Consult with your systems administrator to allocate the following new resources that are required for the Point-M installation:
    - IP address for the Point-M server (globally unique and globally routable IP address, i.e. no local/private IP addresses)
    - A machine name for the Point-M server. If you have only one Point-M server in your administrative domain, we recommend that you name it 'point-m'. Although not required, we recommend further that you configure your DNS service to associate this machine name with the Point-M server's IP address from above.
    - A root password for the Point-M server.

5. Boot your machine from the Point-M CD
    - Press ENTER to start the software installation and follow the instructions on the screen.
    - Choose 'Fresh Installation' when asked for the installation type.
    - We recommend to accept the default recommendations for the hard disk partitioning.
    - The entire installation may take up to 10 minutes. When completed, press ENTER and the machine will reboot. At this time, please remove the Point-M installation CD. If you prefer, you can also remove the CD/DVD drive at this time (Point-M does not require a CD/DVD drive for its operation).

1.1.2 Installing the Point-M Server in a Secured Machine Room

The Point-M server should be placed at a secure location, preferably in a machine room with restricted access, because it contains sensitive data, such as user accounts and WEP encryption keys.

The Ethernet port of the Point-M server needs to be connected to the corporate Ethernet/LAN. If your corporate LAN provides different speeds, ensure that you select a socket with supports at least 100 Mbps.

We recommend that you connect the Point-M server to a reliable power source. However, this is not mandatory, as the Point-M system was designed to recover from power outages without requiring manual interaction.

The Point-M server will be administered remotely through a WEB-based management interface. It is therefore not necessary to place the server at a easily accessible location. Furthermore, it is not necessary to equip the Point-M server with a keyboard or monitor.

1.2 Configuring the Corporate DHCP Server

Most corporations have a DHCP server installed as part of their regular corporate network infrastructure. DHCP is commonly used to dynamically assign IP addresses to DHCP clients, such as end-user workstations of user laptops. In addition, DHCP can also provide configuration information, such as DNS settings or TFTP coordinates to clients.

Point-M uses DHCP for the following purposes:

1. Assigning IP addresses to Point-M access points.
2. Providing the Point-M access point with the coordinates of the TFTP boot server. Note: Normally, the Point-M server assumes the role of TFTP boot server for the Point-M access points.
3. When a wireless client issues a DHCP request, the Point-M server will replay it to the corporate DHCP server. This makes it possible that wireless clients can obtain IP addresses and other configuration information from the corporate DHCP server as if they where connected to the wired network.

It is necessary to modify your existing DHCP server configuration to include information about the TFTP boot server and the boot image file name. This information will be made available in the replies that this DHCP server provides to its clients. Clients other than the Point-M access points will ignore this information. Note: Restart the DHCP service after your modifications are complete – to ensure that they take effect immediately.

Assuming that the Point-M server has the IP address 138.15.109.2, a DHCP server configuration on a Linux system may look as follows:

```
# /etc/dhcpd.conf  --- example

subnet 138.15.109.0 netmask 255.255.255.0
{
    option routers              138.15.109.254;
    option subnet-mask          255.255.255.0;
    option time-offset          -5;   # Eastern Standard Time

    range dynamic-bootp         138.15.109.10  138.15.109.99;
    default-lease-time          21600;
    max-lease-time              43200;
    option domain-name          "nec-labs.com";
    option domain-name-servers  138.15.100.4, 138.15.101.93;

    next-server       138.15.109.2;
    filename          "pm-linux";
}
```

If you use a different DHCP server product, please consult the manual of that product for details. A description of the Linux DHCP server and its configuration file is part of the standard Linux documentation.

Special attention should be given to the last two entries (shown in red). For the ‘next-server’ option, enter the IP address of your Point-M server (instead of 138.15.109.2). The line for the ‘filename’ option should be copied unchanged.
The ‘next-server’ option specifies the TFTP server from which the Point-M access points can download their software when they reboot. Normally, the Point-M server assumes the role of the TFTP server (i.e. enter the IP address if the Point-M server here). The ‘filename’ option specifies the filename where the software for the Point-M access points is stored on the TFTP server. The default Point-M server installation will place the access point software into a file named ‘pm-linux’ . Unless you have specific installation requirements, it is not advised to change this filename, or, to use a TFTP server different from the Point-M server.

A mistake at the DHCP server configuration can be easily discovered by looking at the “NETWORK” LED of a Point-M access point when it boots. Under normal circumstances, the “NETWORK” LED will flash 2 or 3 times and then move into a fast flickering when the software is downloaded via TFTP. It the LED shows only low activity after rebooting the access point, then one of the following could have happened:

Troubleshooting: Possible Errors:

1. The Point-M access point is not connected to the corporate LAN.
2. The access point can not obtain an IP address from the corporate DHCP server. Please check the log of the DHCP server to verify that a request was received from the access point and that this request was properly answered.
4. The access point receives an IP address from the DHCP server, but the DHCP request does not specify the TFTP server.
5. The Point-M server is not providing the TFTP service. To verify that the TFTP service works correctly, open a command shell and type:

   % tftp point-m
   > get pm-linux

   If the TFTP service works correctly, it will download the access point software image to your local disk within 2-3 seconds.

1.3 Installing the Point-M access points

1.3.1 What is a Point-M access point and what is it good for?

The access point is a small blue box with two black antennas, a 5V power connector and a 10/100Mbps Ethernet socket.

A user' s laptop, equipped with a WLAN card (also known as 802.11 card or WiFi card), exchanges radio signals with the access point in order to send digital data to the network, or, to receive digital data from the network.

1.3.2 Where to place the Access Point?

- Place the access points close to areas of high user concentration, such as office areas or conference rooms. Ensure that no user is more than 300 feet away from the nearest access point.
- Choose a location, where the access point does not disturb other users. Make sure that users do not have to move the access point in order to get access to other devices.
- For best RF propagation, place the access point as high as possible. Using the two holes on the back of the access point, the device can be mounted on a wall, preferably close to the ceiling. Alternatively, it can simply be placed on top of furniture.
- The access point needs to be connected to Ethernet LAN and to power.

1.3.3 How to install the Point-M access point?

- Choose a location with access to Ethernet and electric power.
- Remove the access point from its packaging.
- Connect the Ethernet (use a "straight" Ethernet cable).
- Connect the power supply (included in the packaging) to the access point. The access point will boot immediately. You can monitor the LED activity to verify its correct functioning (see section 2.1 for LED activity).

1.3.4 How to configure the Point-M access point?

- The Point-M access point does not require any configuration.
- However, make sure that your Point-M server is up and running, and that your DHCP server is configured to provide the correct TFTP boot option (see section 1.2).

1.4 Installing end-user devices (laptop,etc)

Point-M has no specific requirements regarding the end-user hardwareor software. The end-user can purchase any WiFi compatible hardware and device driver and install it according to the installation instructions of that particular product.
Please note that it should be standard practice to only admit users to the Point-M system that have a Point-M accounts. See section 2.2 for information how to create a user account.

2 Running the System (first time users)

2.1 Verifying that the access point boots correctly

2.1.1 The Access Point Status LEDs

The access point has 3 green LEDs for monitoring its status, see Figure 1. After successfully booting the access point, it is advisable to use the WEB-based monitoring tool of the Point-M server for monitoring the access point activity (see section **錯誤! 找不到參照來源**。).

Figure 1: The Point-M access point has 3 LEDs that provide status information.

POWER … is on as soon as the device is connected to electrical power. If this LED is off, check the power cables and the fuse of the main electric circuit.

NETWORK … usually flickers. It is on when the access point communicates with the network and it is off when the access point is not currently interacting with the network. Because network activity is quick, frequent and sporadic, this LED often appears to be flickering.

ONLINE … indicates that the access point is actually able to serve users. When the access point is booting, this LED is off (no users supported during this time). Right after booting, and whenever the RF quality drops below a certain level, the access point scans for another/better RF channel. During this process, which may take up to 4 seconds, ONLINE blinks. During that time, communication between the user and the access point may be interrupted.

Note: When the access point is already running, simply unplug the power cable and plug it in again to start initialization of the device. The boot process should then commence as described below.

2.1.2 Normal LED activity during access point booting

When the access point is connected to power, it automatically obtains an IP address via DHCP and downloads its software from the Point-M TFTP server.

The downloaded software then selects an RF channel based on local RF conditions. Below is the activity of the LEDs that can be observed during this process:

1. access point is connected to power and starts boot process.
   - ONLINE = off
   - NETWORK = off
   - POWER = on
2. access point sends out DHCP request to obtain IP address from local DHCP server.
   - ONLINE = off
   - NETWORK = slowly blinking, for 2-3 seconds
   - POWER = on
3. access point downloads software from TFTP server
   - ONLINE = off
   - NETWORK = high activity, for 30 seconds
   - POWER = on
4. access point initializes and scans for RF channel
   - ONLINE = blinking, for 4 seconds
   - NETWORK = low activity
   - POWER = on
5. access point is fully usable
   - ONLINE = on
   - NETWORK = current activity (on=activity, off=no activity)
   - POWER = on

2.2 Creating a user account (system administrator)

Use the WEB-based management tool to create new user accounts. The server will generate a respective number of account letters which contain 128-bit WEP keys. Please print these letters and seal them so that the WEP keys are not visible. Ideally, not even the system administrator should know the WEP key.

2.3 Connecting a user to the Point-M network

Give one of the account letters (see section 2.2) to the new user. Only the new user should see the WEP key that is printed on that letter.

In order to obtain access to the Point-M system, the user has to configure his client device (e.g. laptop) to encrypt its traffic with the provided key. The Point-M system will automatically recognize the new user and record its MAC address and user identification later on.

When configuring his client device (laptop), the user has to specify an SSID. For Point-M systems this SSID should be set to:

SSID: point-m

2.3.1 Physical connectivity

To verify that a user has physical access to the Point-M system, open a shell and type:

arp –n

This command exists on both, Linux and Windows. If the user already has connectivity to the Point-M network, the MAC address of the Point-M's WLAN card will be shown. If no MAC address is shown, then connectivity is not available. Check the following:

1. The SSID should be specified as 'point-m'
2. Make sure that the WEP key is entered correctly. Some systems support the use of up to 4 different WEP keys; make sure that you use the same KEY that you used when the account was created (for simplicity, we recommend to always use KEY 0).
3. On Windows: Make sure that your client I not set to ' WEP key will be provided by network' . You (the user) have to provide the WEP key (the initial WEP key is printed on the account letter that you received from your system administrator).

2.3.2 2nd stage login (in Web browser)

Optionally, a system administrator can request that a user passes an additional authentication test before he will be given access to the network. If enabled, this process is called ' 2 nd stage authentication' .

Normally, 2nd stage authentication is completed by opening a web browser (any browser is fine). The Point-M server will automatically redirect the user to a page that prompts the user for his user-name and password. This information is then verified against the corporate RADIUS service or against the NT-domain user account database. Before 2nd stage authentication is successfully completed, the user can only browse restricted pages on the Point-M server. Usually, those pages are configured to provide help information or general information about the visited organization (corporate black board)

3 Additional Information

3.1 Security

The Point-M access point will at no time have access to secret information, such as administrator passwords of encryption keys. In fact, the access point will not perform any encryption, nor will it make or enforce any access decision. This means, that an attacker can not retrieve any information from the access point (because there is none), nor can it trick the access point into admitting unauthorized users (because the access point is not making/enforcing this decision anyway). It is therefore safe to install Point-M access points in areas

where physical security is hard to guaranty (like open public spaces, e.g. lobbies, where potential attackers may have physical access to the access point device). The Point-M access point dynamically downloads its software from a central Point-M server. This makes it extremely easy to update the software from a central location: Simply put the net access point software on the Point-M server and all access points will automatically get the net software version from there – no further action by the systems administrator required. This feature is extremely important, because WLAN technology is still evolving, leading to periodic software upgrades.

3.2 Recovery from Power Outages

After a power outage, all access points will automatically reboot. It is therefore not necessary to connect the access points to a UPS. If the access point reboots before the Point-M servers have completed their boot process the access point will continue its boot attempt until the Point-M servers are available. In short: In case of a power outage there is nothing to worry about; the system will come online again automatically.

3.3 Access Point Replacement

Access points are durable devices. If, however, an access point becomes defect, it is sufficient to simply replace the box. The new box will automatically reboot and obtain the same software for the Point-M server that all other access points have, i.e. there is no danger that the new access point might be running a different software version. Also, there is no configuration required for the new access point. Simply replace the box – that' s all.

4 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. This equipment generates, uses and can radiated radio frequency energy and, if not installed and used in accordance with the instructions, 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 to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.
-Increase the separation between the equipment and receiver.

-Connect the equipment into 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.

Changes or modifications not expressly approved by the party responsible for compliance could void the user‘ s authority to operate the equipment.

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