

This document defines the requirements for configuring a NetMAX™ Server for Linux to function as a wireless access point.

What is a Wireless Access Point?

Before defining specifically a wireless access point, let us review the wireless technology that is supported by this NetMAX server. This technology or standard is referred to as 802.11b. It specifies a method of communication between computers using a wireless connection. The advantage of using a wireless connection is that computers (and other devices on a typical network) do not need to be physically interconnected with wires and hubs. This “freedom” allows users to roam with their laptops within spaces ranging in size from a single room to entire cities and to remain connected to a computer network. The 802.11b standard specifies the frequency, power, and bandwidth available for communication. The simplest way to look at 802.11b is that it operates at 2.4GHz, at a power of less than 100mW, and at a maximum bandwidth of 11 Mbit/sec. In order for computers on an 802.11b network to communicate, they must follow certain protocols. These protocols dictate how data is transmitted and received.

Of these protocols, there are essentially two classes: *ad hoc* and managed connections.¹ These define how different nodes will communicate with one another. With an ad hoc wireless network, each computer will “talk” directly to every other computer in the network (see Figure 1). The advantage to this type of network is that it can be quick to set up a few computers and is particularly useful if one does not wish to deal with managing access to the wireless network.² **NetMAX Server does not support *ad hoc* wireless networking.**

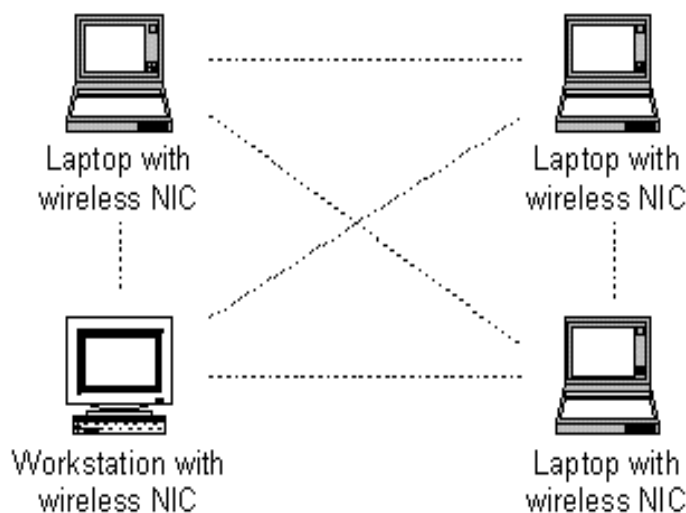


Figure 1 - Ad-hoc Wireless Network

¹Many Windows-based applications incorrectly use the term “peer to peer.”

²It should be noted that one cannot actually manage access to a wireless network. Because of the use of radio frequency, anyone within range has access; consider this to be the same as physical access to a wired network. One is truly managing how the computers are communicating logically. How the wirelessly connected computers decide how to do this is more complicated and is elaborated upon later in this document.

NetMAX Server provides that other communication protocol of “managed” mode. Unlike ad hoc, managed mode 802.11b requires that all participants in the wireless network communicate via a central hub, called the master (see Figure 2). In order for any two computers to communicate, they send/receive data to/from the master. The master acts as an arbitrator in the network, including announcing that there exists a network, controlled who has logical access, and often provide other network services such as DHCP, firewalls, and VPN.

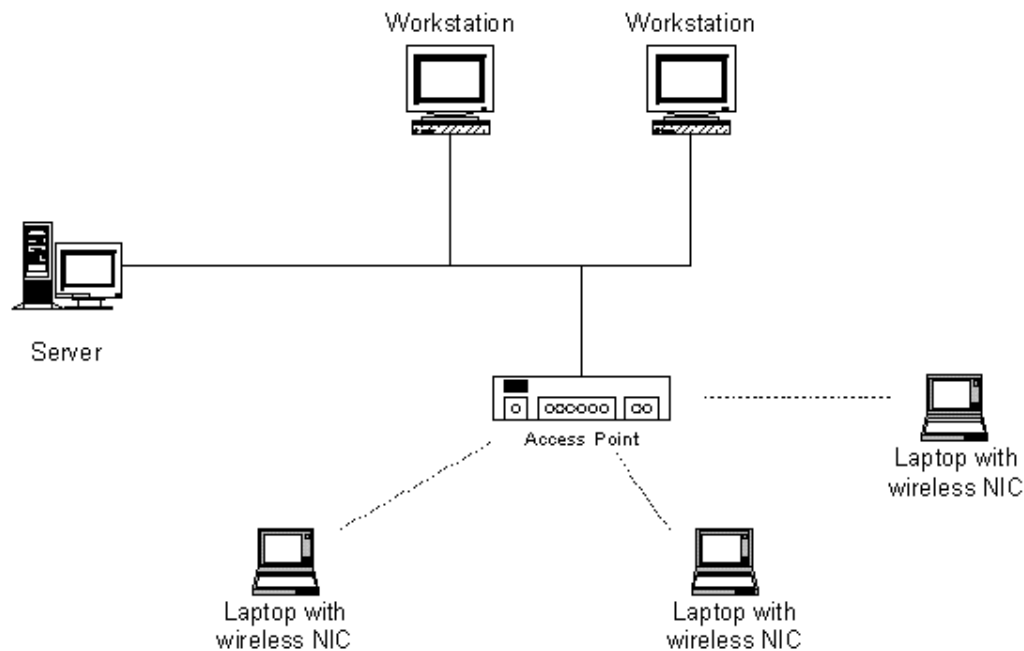


Figure 2 - Managed Wireless Network

Software Requirements

Your NetMAX Server must be operating at a least L2.4Pv4.03.

Hardware Requirements

The driver used by the NetMAX Server that provides managed wireless communications requires that use of a wireless card based on the Intersil PRISM2 chipset. For a partial list of compatible cards, please see Appendix A of this document. Your computer must have a i82365 compatible PCMCIA adapter (most are). As of NetMAX Server L2.4Pv4.03, PCI and PCX cards are **not** supported. You may purchase compatible PCMCIA adapters and PCMCIA wireless cards from the NetMAX Store (<http://buy.netmax.com>). If you have a Toshiba SG20 or Z-Series server, your PCMCIA adapter is supported.

For best performance, your wireless card should be flashed to include secondary firmware v1.4.9. For information on upgrading your card and for checking compatibility, we have found these URLs useful:

<http://www.netgate.com/>

http://www.netgate.com/support/prism_firmware/

If you have a compatible card but are not sure about your secondary firmware version, the NetMAX Server will automatically attempt to upload a RAM-only version of the v1.4.9 secondary firmware when it attempts to configure the PCMCIA wireless adapter. Check your NetMAX Alerts (from the Personal Page) as an administrator. These alerts will let you know if a wireless card was detected with a non-v1.4.9 secondary firmware and if the card was automatically upgraded.

Other issue you may wish to be aware of include:

- Ⓣ NetMAX Server does not support more than one (1) wireless card at a time.
- Ⓣ The wireless driver is compatible with WEP encryption 56- and 104-bit key length.³
- Ⓣ The wireless driver can provide Link-Level MAC address filter.

Configuring Your NetMAX Server

If you are required to install a PCMCIA adapter because your computer does not already have one, follow these steps:

1. Shut down your NetMAX Server by going to Home|System|Shutdown and click on IMMEDIATE SHUTDOWN.
2. Completely unplug the power and follow your manufacturer's instructions for hardware installation.
3. After the PCMCIA adapter is installed, insert the PCMCIA wireless card into the PCMCIA port of the PCMCIA adapter.

If you already have a PCMCIA port on your computer, follow these steps:

1. Insert your PCMCIA wireless adapter in your PCMCIA port.
2. Restart your NetMAX Server by going to Home|System|Shutdown and click on IMMEDIATE RESTART.

When your NetMAX Server reboots, you will hear an extra series of beeps (assuming your system has a PC speaker). Two high-tone beeps indicate that the wireless card was recognized and is ready to be configured. A high-tone beep followed by a low-tone beep indicates that the card are recognized but that it is incompatible with the NetMAX wireless driver. These beeps are produced before the standard NetMAX trio of beeps that indicate all services are configured.

Configuring the Ethernet Properties of your Wireless Card

Wireless cards are configured similarly to Ethernet cards.

³WEP encryption does NOT protect your network or make your data difficult to decrypt by unknown third parties. It has been shown that it is possible to break into a 56-bit encrypted network in less than 5 minutes, and a 104-bit network in as little as 5 hours. In spite of this, we do recommend using WEP encryption to eliminate the casual hacker from accessing your network and the transmissions across it. For better encryption, we recommend configuring your computers to communicate using a VPN connection.

- 1.[1]Select Home|Network|Interfaces.
- 2.The **Available Network Interfaces** table appears. The **Device Name** relates to the port that the device is plugged into. You will need to select an interface that appears in the list of devices with "Wireless" in its **Description**.[2]
- 3.[3]The **Configuration** column shows how the Ethernet card will be configured during the next commit. The **Running Configuration** is the currently operating configuration.
- 4.Click the pencil on the row of the Wireless interface to configure.[4]
- 5.[5]Enter the **ESSID**. The ESSID (Extended Service Set Identifier) identifies your access point to other 802.11b wireless devices. The ESSID is sometimes referred to by different names, such as Network Name, Preferred Network, SSID, or Wireless LAN Service Area. The ESSID is specific to your wireless network and should be unique, particularly if there are adjacent wireless networks within the vicinity of your access point.
- 6.Select the **Channel** for the wireless interface card. The Channel will be between 1 and 11 in the United States. Select a channel that is at least 2 channels (3 is preferred) different than adjacent access points.

Using VPN to Provide Secure Encryption

For Encryption:

- 1.To enable **Encryption** over the wireless network between, clients and the access point select the level of encryption desired here. Because Wireless LAN use radio waves instead of cables to transmit network traffic, the data transmission are susceptible to interception. **Low** encryption is 64 bit encryption, and **High** encryption is 128 bit encryption. Both levels of encryption use a WEP (Wired Equivalent Privacy) algorithm. When implemented correctly, it does provide an additional layer of protection for your network.
- 2.Enter an **Encryption Key** for the encrypted wireless network. Low encryption requires a key length of 5 characters. High encryption requires a key length of 13 characters.

For Added Security:

- 1.Check the box to **Enable MAC Address Filtering**. All Ethernet cards (NICs) have a unique 48-bit MAC address burned into the ROM chip on the card itself. When MAC address filtering is enabled, you are restricting the NICs that are allowed to connect to your access point. The MAC address is not easily changed. This filtering greatly enhances the security of your wireless network by only allowing machines within the selected group to access your access point.
- 2.If you have enabled filtering, then **Select Machine Group** to allow access to the wireless network. Only machines in that machine group are allowed to communicate with your access point.

Appendix A

This section is a copy of URL <http://www.personaltelco.net/index.cgi/Prism2Card> for quick reference to compatible hardware. Note, we are only listing the PCMCIA models; the actual pages also lists PCI hardware.

Make	Model	Connector	Rx	Tx
Addtron	AWP-100	.	-76 dBm	>13 dBm
Addtron	AWP-101	Unknown	.	.
Asanté	AL1011	.	?	13 dBm
Asus	wl110	none	.	12-15 dBm
Belkin	F5D6020	.	.	13-20 dBm (50mW max)
Compaq	WL100	None	?	20mW typ / 100mW max
Demarc	Relia-Wave	Diversity RP-MMCX	-91db	100mW or 20dBm
Demarc	Relia-Wave	Diversity RP-MMCX	-91dB	200mW or 23dBm
D-Link	DW-655H	yes, with nice switch	standard prism2.5?	standard prism2.5?
D-Link	DWL-650		-78 or -84 dBm	14 or 17 dBm
LinkSys	WPC11	.	.	14 dBm
LinkSys	WMP11	RP-SMA	.	+16dBm
Musenki	?	Reverse SMC	-87 dBm	18 dBm
Musenki	?	Dual MMCX	-89 dBm	23dBm (200mw)
Proxim	RangeLAN-DS 8434-05	Dual Reverse MMCX	-83 dBm	13dBm
Proxim	RangeLAN-DS 8433-05	Single unknown connector (SSMB?)	-83 dBm	13dBm
SMC	SMC2632W		-76 dBm	50mw Max (17 dBm)
Teletronics	WL-11000	Dual Reverse MMCX	-83 dBm	15 dBm
Zcomax	XI-300	Dual Reverse MMCX	-83 dBm	13 dBm
Zcomax	XI-300B	None	-83 dBm	13 dBm
Zcomax	ZFE-300	Dual MMCX (probably reverse)	.	.
Zcomax	XI-325	Dual Reverse MMCX	-85dBm	15dBm
Zcomax	[XI-325H]	Dual Reverse MMCX	-83	100mw
ZoomAir	4105	RP-SMA	.	14 dBm

Advanced Compatibility Testing

If you are having problems with the detection of your wireless network card, there are a few steps you can take to troubleshoot the problem. While there are a number of reasons you could be encountering problems, you should first verify that the card is compatible with NetMAX. To check compatibility, open a command prompt and enter the following command:

```
iwconfig wlan0
```

If the command returns, “no wireless connections”, then either the card is not compatible, it is not properly seated in the PCMCIA slot, or it is broken.

Another command that may shed more light on the problem is:

```
/sbin/hostap_diag -r wlan0
```

This command will return Host AP driver diagnostics information for 'wlan0'. If neither of these commands work, try a different wireless network card, or call Cybernet Technical Support.