Fedora 12

Wireless Guide

Wireless and mobile networking overview for Fedora Linux

Scott Radvan

Fedora 12 Wireless Guide
Wireless and mobile networking overview for Fedora Linux
Edition 1.2

Author	Scott Radvan	*sradvan@redhat.com*

Copyright © 2009 Red Hat, Inc.

An overview of IEEE 802.11-based and other mobile networking technologies and their implementation in Fedora Linux.

Preface

1. Document Conventions

This manual uses several conventions to highlight certain words and phrases and draw attention to specific pieces of information.

In PDF and paper editions, this manual uses typefaces drawn from the *Liberation Fonts*[1] set. The Liberation Fonts set is also used in HTML editions if the set is installed on your system. If not, alternative but equivalent typefaces are displayed. Note: Red Hat Enterprise Linux 5 and later includes the Liberation Fonts set by default.

1.1. Typographic Conventions

Four typographic conventions are used to call attention to specific words and phrases. These conventions, and the circumstances they apply to, are as follows.

`Mono-spaced Bold`

Used to highlight system input, including shell commands, file names and paths. Also used to highlight keycaps and key combinations. For example:

> To see the contents of the file `my_next_bestselling_novel` in your current working directory, enter the `cat my_next_bestselling_novel` command at the shell prompt and press `Enter` to execute the command.

The above includes a file name, a shell command and a keycap, all presented in mono-spaced bold and all distinguishable thanks to context.

Key combinations can be distinguished from keycaps by the hyphen connecting each part of a key combination. For example:

> Press `Enter` to execute the command.

> Press `Ctrl`+`Alt`+`F1` to switch to the first virtual terminal. Press `Ctrl`+`Alt`+`F7` to return to your X-Windows session.

The first paragraph highlights the particular keycap to press. The second highlights two key combinations (each a set of three keycaps with each set pressed simultaneously).

If source code is discussed, class names, methods, functions, variable names and returned values mentioned within a paragraph will be presented as above, in `mono-spaced bold`. For example:

> File-related classes include `filesystem` for file systems, `file` for files, and `dir` for directories. Each class has its own associated set of permissions.

Proportional Bold

This denotes words or phrases encountered on a system, including application names; dialog box text; labeled buttons; check-box and radio button labels; menu titles and sub-menu titles. For example:

---

[1] https://fedorahosted.org/liberation-fonts/

> Choose **System > Preferences > Mouse** from the main menu bar to launch **Mouse Preferences**. In the **Buttons** tab, click the **Left-handed mouse** check box and click **Close** to switch the primary mouse button from the left to the right (making the mouse suitable for use in the left hand).

> To insert a special character into a **gedit** file, choose **Applications > Accessories > Character Map** from the main menu bar. Next, choose **Search > Find…** from the **Character Map** menu bar, type the name of the character in the **Search** field and click **Next**. The character you sought will be highlighted in the **Character Table**. Double-click this highlighted character to place it in the **Text to copy** field and then click the **Copy** button. Now switch back to your document and choose **Edit > Paste** from the **gedit** menu bar.

The above text includes application names; system-wide menu names and items; application-specific menu names; and buttons and text found within a GUI interface, all presented in proportional bold and all distinguishable by context.

Note the **>** shorthand used to indicate traversal through a menu and its sub-menus. This avoids difficult-to-follow phrasing such as 'Select **Mouse** from the **Preferences** sub-menu in the **System** menu of the main menu bar'.

`Mono-spaced Bold Italic` or **`Proportional Bold Italic`**

Whether mono-spaced bold or proportional bold, the addition of italics indicates replaceable or variable text. Italics denotes text you do not input literally or displayed text that changes depending on circumstance. For example:

> To connect to a remote machine using ssh, type **`ssh username@domain.name`** at a shell prompt. If the remote machine is **`example.com`** and your username on that machine is john, type **`ssh john@example.com`**.

> The **`mount -o remount file-system`** command remounts the named file system. For example, to remount the **`/home`** file system, the command is **`mount -o remount /home`**.

> To see the version of a currently installed package, use the **`rpm -q package`** command. It will return a result as follows: **`package-version-release`**.

Note the words in bold italics above — username, domain.name, file-system, package, version and release. Each word is a placeholder, either for text you enter when issuing a command or for text displayed by the system.

Aside from standard usage for presenting the title of a work, italics denotes the first use of a new and important term. For example:

> When the Apache HTTP Server accepts requests, it dispatches child processes or threads to handle them. This group of child processes or threads is known as a *server-pool*. Under Apache HTTP Server 2.0, the responsibility for creating and maintaining these server-pools has been abstracted to a group of modules called *Multi-Processing Modules* (*MPMs*). Unlike other modules, only one module from the MPM group can be loaded by the Apache HTTP Server.

1.2. Pull-quote Conventions

Terminal output and source code listings are set off visually from the surrounding text.

Output sent to a terminal is set in `mono-spaced roman` and presented thus:

```
books        Desktop   documentation  drafts  mss     photos   stuff  svn
books_tests  Desktop1  downloads       images  notes  scripts  svgs
```

Source-code listings are also set in `mono-spaced roman` but add syntax highlighting as follows:

```java
package org.jboss.book.jca.ex1;

import javax.naming.InitialContext;

public class ExClient
{
   public static void main(String args[])
      throws Exception
   {
      InitialContext iniCtx = new InitialContext();
      Object         ref    = iniCtx.lookup("EchoBean");
      EchoHome       home   = (EchoHome) ref;
      Echo           echo   = home.create();

      System.out.println("Created Echo");

      System.out.println("Echo.echo('Hello') = " + echo.echo("Hello"));
   }
}
```

1.3. Notes and Warnings

Finally, we use three visual styles to draw attention to information that might otherwise be overlooked.

Note

Notes are tips, shortcuts or alternative approaches to the task at hand. Ignoring a note should have no negative consequences, but you might miss out on a trick that makes your life easier.

Important

Important boxes detail things that are easily missed: configuration changes that only apply to the current session, or services that need restarting before an update will apply. Ignoring a box labeled 'Important' won't cause data loss but may cause irritation and frustration.

Warning

Warnings should not be ignored. Ignoring warnings will most likely cause data loss.

2. We Need Feedback!

To provide feedback for this guide, contact the author or file a bug in *https://bugzilla.redhat.com/*. Please select the proper component for this guide.

Introduction

Due to increased demand for convenient networking and more flexible access to both the Internet and company resources via more geographically widespread coverage areas, wireless networking use has flourished in recent years. Mobile access to data services previously unavailable is now common. The sales and penetration of wireless access have resulted in a recent projection by *ABI Research*[1] that one billion Wi-Fi chipsets *will ship in the year 2011*[2].

Not only has wireless data access achieved a great deal of market penetration in recent years, but the price of the related hardware has dropped dramatically, making it even more accessible. Wi-Fi seems to be everywhere; in laptops, desktops, PDAs, cell phones and routers, and there is such a large amount of wireless networks in many urban areas that complete overcrowding of the public wireless radio spectrum in use can occur.

This guide provides a high-level overview of the past, present, and future of IEEE 802.11 wireless networking standards, concepts, hardware components, security concerns, and their relation to Fedora Linux. Although the specific wireless technology based on IEEE 802.11 is the primary focus of this guide, other mobile technologies and their relation to Fedora and Linux are also mentioned. Parts of this guide contain detailed information specific to Fedora and other Linux operating systems, however, many of the topics and concepts relate to all operating systems, vendors, and environments.

1.1. Who should read this guide?

You should read this guide if you are looking for an overview of wireless technologies and how they are implemented in Fedora or other Linux operating systems. Other readers will gain general information on how wireless works, the hardware involved, and other topics such as standards and security.

1.2. What is a Wireless LAN?

A wireless LAN (referred to as WLAN in this guide) is a wireless local area network that allows computers or other devices to communicate via radio frequency (RF) technology. It affords the user mobility to move around and stay connected to the network without using physical cables such as in a traditional Ethernet system.

The IEEE (Institute of Electrical and Electronics Engineers) is a non-profit, global organization which implemented and continually develops a set of standards for wireless communication. This family of standards is known as IEEE 802.11 and consists of the actual standards and protocols defining how computers communicate via a WLAN. Standards are discussed in more detail later. Although wireless networks are commonly referred to as Wi-Fi, this is only a marketing term chosen by the Wireless Ethernet Compatibility Alliance (now known as the Wi-Fi Alliance). When referring to Wi-Fi, the underlying technology is typically a WLAN or device operating within the standards of the IEEE within the 802.11 family.

1.3. History of Wireless LANs

Although wireless communications are nothing new, Norman Abramson, as a professor at the University of Hawaii, developed what is acknowledged as the first computer network using wireless communications in 1970. Known as ALOHAnet, it enabled wireless communication between a small

---

[1] http://www.abiresearch.com/
[2] http://www.infoworld.com/d/networking/one-billion-wi-fi-chipsets-in-2011-216

set of islands and pioneered today's wireless networks, as well as lending concepts to Ethernet development. More information can be found at the *ALOHAnet page at Wikipedia*[3].

Wireless LANs under the IEEE 802.11 specifications did not become widely used until the introduction of the 802.11b standard in 1999. With more available devices, higher data rates and cheaper hardware, wireless access has now become widespread. The IEEE recently ratified the 802.11n standard. This standard addresses several performance and security issues and is discussed later in this guide.

1.4. Benefits of Wireless LANs

Wireless LANs offer mobility and convenience, allowing connections from nearly any location within the coverage area. Also, the installation of a WLAN is in many cases easier than a wired network, because of the lack of a need to install actual cables in wall fittings and data centers. A properly designed WLAN can be installed relatively quickly and can also be transported to a new location more easily.

1.5. Considerations

Wireless LANs introduce several deployment and usability factors that should be considered. An Ethernet system generally has its electrical current traveling neatly *bounded* inside a wire. As the elements that make up a WLAN depend heavily on communication via RF through the air, the fact that a WLAN is an *unbounded* medium introduces many factors. The performance and reliability of a wireless LAN is dependent on atmospheric conditions, physical obstructions, other WLANs, RF interference, RF propagation characteristics and the basic laws of physics. The use of a WLAN is therefore generally not as reliable or as fast as a wired system, however recent developments in the communications standards that actually use some of these atmospheric anomalies *to their advantage* have alleviated the problems to a degree. The reliability and performance of a WLAN depends on correct deployment which has all of these conditions taken into account.

Security concerns are also a factor. A WLAN spreads to coverage areas outside that of a controlled wired system, and is much less predictable. For instance, many wireless networks used in the home can be detected from the street outside. A business may inadvertently make their network available to a competitor in an adjacent building. Hence, several security mechanisms exist for IEEE 802.11 technologies. These are discussed later.

1.6. Linux Wireless Support

Linux supports many wireless devices. Client adapters are typically available in PCI, PCI Express, Mini-PCI, USB, ExpressCard, Cardbus and PCMCIA form. Many of these adapters are supported by default in the Linux kernel via open source drivers available in Fedora. Your device is most likely supported; however, to find an overview of devices and drivers currently supported in Linux and Fedora, refer to the following URL at Linuxwireless.org: *http://linuxwireless.org/en/users/Devices*. Specific information on configuring and activating a WLAN in Fedora is discussed later.

1.7. Disclaimer

Any products pictured or otherwise referred to in this guide are provided for reference purposes only, and no endorsement or guarantees of supportability are intended.

---

[3] http://en.wikipedia.org/wiki/ALOHAnet

Standards

The WLAN and radio communications industries are regulated by several different organizations. These bodies develop and implement standards and regulations that include limits on factors such as power output, antenna height, hardware compatibility, frequency allocation and usage and general spectrum management. This chapter gives an overview of these bodies and their responsibilities. Note that local regulations may exist in your area that may differ from those listed here. When deploying a WLAN, the requirements of your local regulatory domain authority should be adhered to.

2.1. Standards and Regulatory Bodies

- *ITU-R* - The Radio communications sector of the International Telecommunications Union.

  The ITU-R manages worldwide spectrum management and satellite orbits and keeps the interference-free operation of communications as its primary objective. More information can be found at the ITU-R homepage: *http://www.itu.int/ITU-R/index.asp*.

- *Wi-Fi Alliance* - A non-profit, worldwide association consisting of more than 300 member companies from more than 20 countries.

  The Wi-Fi Alliance, previously known as the *Wireless Ethernet Compatibility Alliance* (WECA), ensures that the actual WLAN products maintain a level of interoperability. This is done by performing a series of certification testing on products. Details about Wi-Fi Alliance certifications and programs can be found at *http://www.wi-fi.org/certified_products.php*.

- *IEEE* - The Institute of Electrical and Electronics Engineers is a global, non-profit organization, with more than 375,000 members from more than 160 countries.

  The IEEE is a professional group working towards the advancement of technology, to "foster technological innovation and excellence for the benefit of humanity." In terms of this guide, the IEEE 802.11 *working group* within the IEEE 802 *project* is the main focus, although the IEEE has many other projects and standards. The 802.11 working group sets the standards for Wireless LANs. More information about the IEEE and the 802.11 working group can be found here: *http://www.ieee802.org/11/*.

2.2. Standards Defined

- 802.11 - The first 802.11 standard (often referred to as 802.11 Prime), initially published in 1997 by the IEEE. The 802.11 standard only supports speeds up to 2 Mbps (megabits per second) in the unlicensed 2.4 GHz ISM (Industrial, Scientific and Medical) frequency band. Equipment that conforms to this standard is considered legacy and is no longer being manufactured. It is, however, considered the baseline for IEEE 802.11 WLANs and defined many of the communication concepts still in use today under the newest standards. The newest revision of the 802.11 Prime standard was published as IEEE Std. 802.11-2007.

- 802.11b - Created in 1999 as an expansion to the original standard, 802.11b supports a theoretical maximum data rate of 11 Mbps. Published as IEEE Std. 802.11b-1999, the 802.11b standard defines use of the same 2.4 GHz band as defined in 802.11 Prime, and the main focus behind the development of 802.11b was to increase data rates. This standard sparked a huge increase of WLAN adoption, and is considered as one of the main catalysts for the popularity of Wi-Fi today.

- 802.11a - The 802.11a standard, also created in 1999 as another extension to the 802.11 Prime standard, defines a different modulation technique for communications and operates at a higher frequency than 802.11 Prime or 802.11b. Published as IEEE Std. 802.11a-1999, the 802.11a standard operates in the 5 GHz UNII (Unlicensed National Information Infrastructure) band. Equipment that operates under this standard is not compatible with 802.11b equipment, as they use different frequencies and communication techniques. The higher frequency in use by 802.11a typically shortens the communication range and its ability to penetrate through obstructions, however it has the advantages of higher data rates (up to 54 Mbps) and also does not interfere with the comparatively larger amounts of 2.4 GHz equipment on the market, as the 5 GHz band is much less crowded. Equipment conforming to this 802.11a standard is considered more obscure however can still be found in use today.

- 802.11g - Published in 2003 as IEEE Std. 802.11g-2003, this standard is backward compatible with 802.11b, and higher data rates up to 54 Mbps are possible. As it uses the same 2.4 GHz band, devices conforming to 802.11g are susceptible to the same interference and can suffer from overcrowding in the frequency spectrum. Devices operating under the 802.11g standard can be configured to communicate directly with 802.11b devices in what is known as *mixed mode*.

- 802.11n - This recent amendment (ratified in September 2009 as IEEE Std. 802.11n-2009), introduces many features such as much higher communication ranges and data rates (up to 100 Mbps or more of typical throughput) and a new technology known as *multiple-input and multiple-output*, or *MIMO*. This technology uses multiple antennas and multiple wireless connections to achieve these rates, and is much more resistant to interference without requiring a significant increase in power used to transmit the data. MIMO also presents the ability to use multipath (an atmospheric anomaly where a single signal takes different paths and arrives at the receiver at slightly different times, causing a negative factor on performance when using older standards) to its *advantage*. Many products existed on the market before the standard was fully ratified; often known as "Pre N" or "Draft N", these devices are not guaranteed to fully operate under, or be compatible with, specifications of the completed standard. These draft devices are also not guaranteed to be compatible across differing vendors. At the time of writing, there are concerns that 802.11n devices may greatly interfere with the operation of nearby 802.11b and 802.11g devices and networks; however, there is little doubt that 802.11n represents the next generation of wireless equipment and provides many new features which overcome the problems and limitations of older equipment.

Hardware

This chapter gives an overview of some of the hardware available for wireless LANs, the role they play, and further details about their operation.

3.1. Components of a Wireless LAN

In order for successful communications to take place in a WLAN, certain hardware is needed. The hardware can be generally categorized as being a *transmitter*, *antenna*, a *receiver*, or a combination of these.

- Transmitter - A transmitter, as an *active* device, initiates an electromagnetic signal, which is where the communication used in a WLAN begins. Usually, a transmitter sends this signal to an antenna after the data has been received by the originating station (ie. computer).

- Antenna - An antenna acts as an intermediary device in a WLAN. Specifically, it can propagate a signal after it has been received from a transmitter as an AC signal and then *passively* creates the waveform for it to travel through the air. The actual shape and path that the electromagnetic waves take depends on the type of antenna, its intended purpose and its desired coverage area. An antenna also performs the reverse of this operation by receiving signals and passing them along to a receiver.

- Receiver - A receiver completes the electromagnetic communications in a WLAN by taking a signal (usually from an antenna) and passing it to the computer in a way it can understand (such as binary 1s and 0s).

3.2. Types of Cards

Wireless client adapters allow desktop and mobile computers to join and communicate on a WLAN. Adapters are typically available in PCI, PCI Express, Mini-PCI, USB, ExpressCard, Cardbus and PCMCIA form. This chapter provides details and sample images of three of the most commonly used adapter types: USB, PCMCIA/Cardbus, and PCI.

- USB - These adapters are particularly useful for mobile users, allowing quick access for any machine with a USB port. They can be quickly set up and transferred between machines. The antenna is built into an integrated unit and the adapters are approximately the same size as a USB flash memory adapter:

- PCMCIA/Cardbus - Designed for laptops, these adapters can have an integrated antenna; however, some models provide support for connecting an external antenna to modify signal requirements, or increase signal strength capabilities:
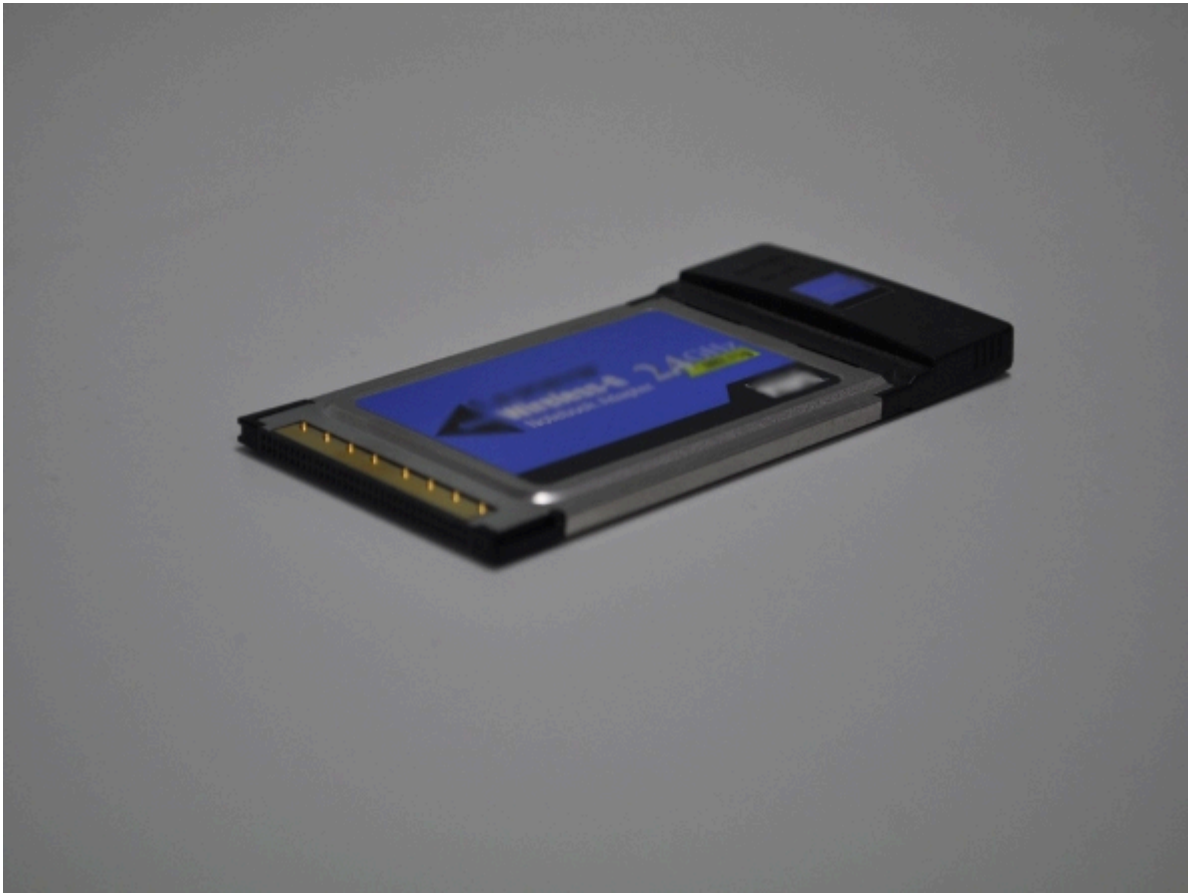
- PCI - These adapters are available for desktop machines with a standard PCI slot. They typically have an external antenna attached, and provide support for connecting antennas for specific signal requirements, or for increased signal strength:
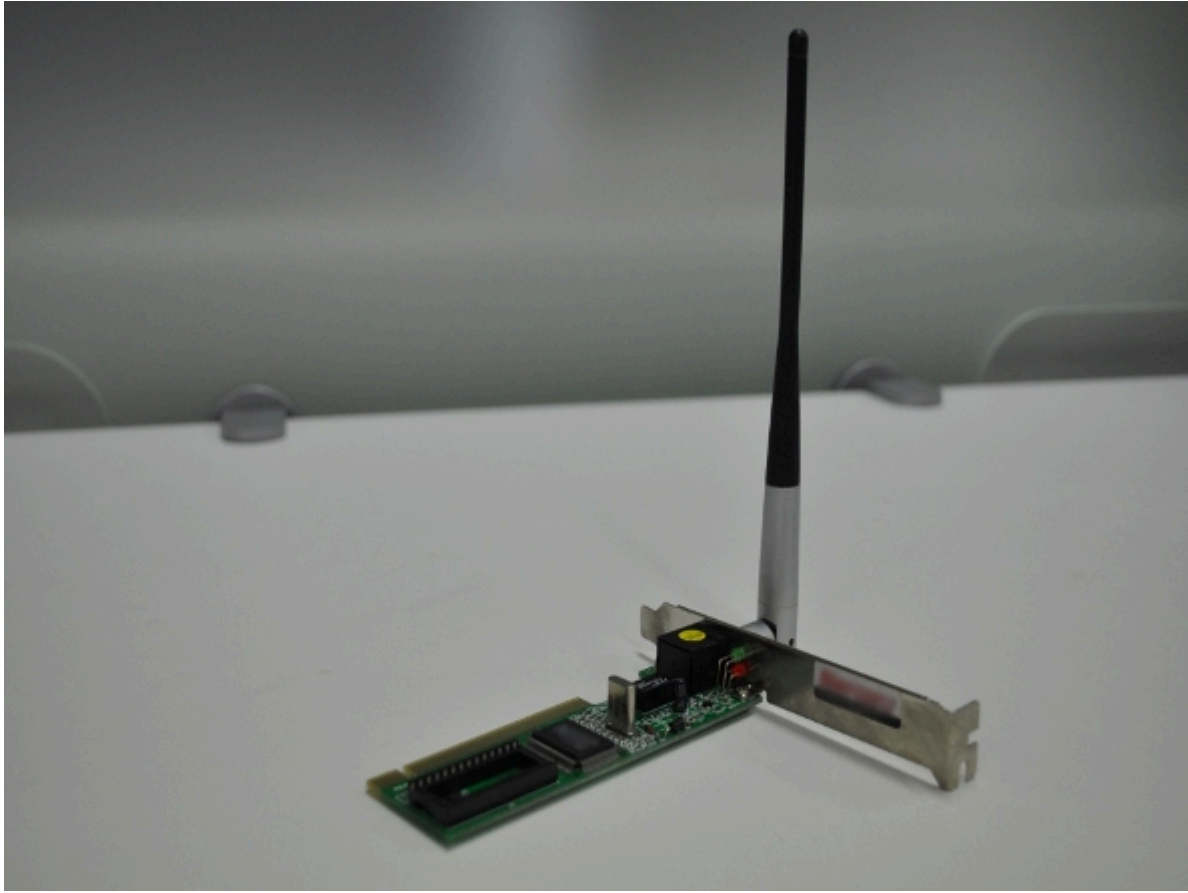
3.3. Types of Antennas

There are three main antenna categories available for wireless LANs: *Omnidirectional*, *Semidirectional* and *Highly directional*.

- Omnidirectional - *Omnidirectional antennas* are designed to radiate a signal in all directions. Although it is impossible under the basic laws of physics for an antenna to perfectly radiate a signal in all directions at equal strength, an antenna of this type is an attempt to provide general coverage in all directions. This is the most common type found for client adapters and access points, as in these situations, good coverage in a general spherical area around the antenna is desirable.

- Semidirectional - *Semidirectional antennas* are designed to provide specific, directed signal coverage over large areas. An example of a semidirectional antenna is a *Yagi antenna*.

- Highly-directional - *Highly directional* antennas are used for point-to-point links; for example, between two buildings. They radiate a very narrow beam over a long distance, and are often used for dedicated links.

3.4. Connection Modes

Clients typically connect in one of two modes: *adhoc* or *infrastructure*. Adhoc mode involves stations communicating directly with each other without the need for a central point to manage communications. This is also known as peer-to-peer mode. The default and most common mode is known as Infrastructure mode. Infrastructure mode uses a Wireless Access Point (WAP), which is a

central device that manages transmissions between clients. Refer to the following for more details on Access Points:

From *Wikipedia.org*[1]: *In computer networking, a wireless access point (WAP) is a device that allows wireless communication devices to connect to a wireless network using Wi-Fi, Bluetooth or related standards. The WAP usually connects to a wired network, and can relay data between the wireless devices (such as computers or printers) and wired devices on the network.*

Access points commonly found in home environments provide different features from those found in business or corporate settings. Consumer-level WAPs are often integrated into broadband gateways, and multiple functions can be served from a single device. These functions typically include a switch for wired access, routing functionality, a broadband modem, and a network firewall. Usually an omnidirectional antenna is used, or multiple antennas, a scheme known as *antenna diversity*. WAPs often have a built-in web interface for their configuration which can be accessed by a web browser.

---

[1] http://en.wikipedia.org/wiki/Wireless_access_point

Security

This chapter covers the security concerns and features of IEEE 802.11 WLANs, including the unique challenges presented by using a wireless access medium; the encryption mechanisms; wireless security myths; best practices when configuring and using a WLAN; and several resources for further reading.

4.1. Unique Challenges

As described in *Section 1.5, "Considerations"*, a WLAN uses an *unbounded* medium. This introduces several challenges to effective security. The standard security model known as CIA, or *Confidentiality*, *Integrity* and *Availability* can be applied to the unique elements of wireless data transmission. This three-tiered model is a general framework for assessing risks to sensitive information and establishing security policy. The following describes the CIA model as it applies to WLANs:

- *Confidentiality* - This part of the CIA model states that sensitive information must be available only to a set of pre-defined individuals, and unauthorized transmission and usage of information should be restricted. This element of the CIA model is worthy of attention when using a WLAN simply because the radiated signal can easily travel beyond the traditional borders of the network, through walls and other fixtures, and can become available to unauthorized users much more easily. This is especially true when using no encryption, weak encryption or if the network has other design flaws.

- *Integrity* - This part of the model states that information should not be altered in ways that render it incomplete or incorrect, and unauthorized users should be restricted from the ability to modify or destroy sensitive information. Much like the *confidentiality* element, affording unauthorized users a greater opportunity to intrude on the network can compromise the level of integrity of data. Data integrity checks are also integrated into the communication and encryption mechanisms used.

- *Availability* - This part of the CIA model states that information should be accessible to authorized users any time that it is needed. Availability is a warranty that information can be obtained with an agreed-upon frequency and timeliness. This element applies to all networking equipment - that a network service is available when needed, and it is no different for wireless equipment. Sufficient knowledge of the hardware and how a wireless LAN operates at a low level is important in order to provide reliable, timely network capabilities, especially in a complicated environment and where reliability is crucial.

4.2. Wired Equivalent Privacy (WEP)

From *Wikipedia.org*[1]: *Wired Equivalent Privacy (WEP) is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio and are thus more susceptible to eavesdropping than wired networks. When introduced in 1997,[1] WEP was intended to provide confidentiality comparable to that of a traditional wired network. Beginning in 2001, several serious weaknesses were identified by cryptanalysts with the result that today a WEP connection can be cracked with readily available software within minutes.*

The WEP protocol does not provide any support for key management mechanisms, and in most environments the same key is shared by many clients. In an environment where keys are not changed regularly, this can compound the problem of using WEP as a flawed protocol. WEP uses keys that must be shared by both the client and the access point as all stations that want to send or receive must know the key. These keys are commonly referred to as being 64 or 128 bits long. In fact, the

---

[1] http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

actual keys are either 40 or 104 bits long, and the remaining 24 bits in either configuration represent what is called the Initialization Vector (IV). This IV is used in combination with the key to encrypt the actual data. The implementation of the mechanisms used to combine the IV and the secret key in the WEP protocol has several flaws which can make the recovery of the keys by a malicious user simple:

- Short IV length - The 24 bits reserved for the IV do not allow for sufficient cryptographic complexity.

- IV is sent in cleartext - The IV is sent in cleartext (unencrypted) over the network. Once sufficient IVs are acquired in an attack, freely available tools exist to quickly analyze the IVs and extract the WEP key.

- Weak IVs - Some of the generated IVs do not provide enough randomness and these can be used to extract the key.

- The IV is part of the encryption key - As an attacker can see 24 bits of every key in cleartext without any effort, it becomes a basic mathematical process to deduce the rest of the key.

WEP is now considered an outdated algorithm and is not recommended for use; however, it should be noted that many of its shortcomings arise from it simply being a poor *implementation* of its underlying mechanisms, and does not necessarily indicate that the actual mechanisms are inherently flawed.

4.3. Wi-Fi Protected Access (WPA)

WPA (Wi-Fi Protected Access) is a certification program created by the Wi-Fi Alliance to address some of the security problems of WEP, namely the weaknesses in its IV headers, as mentioned earlier. WPA2, the newest encryption technology for wireless LANS, is the recommended method for securing wireless networks, although older hardware may not support WPA or WPA2. These technologies are often referred to as WPA-PSK and WPA2-PSK for most home users as they employ the use of a *Pre-Shared Key* so that dedicated authentication mechanisms, as might be used in a business or corporate environment, are not required.

WPA-PSK works as an improvement on WEP by using the following mechanisms:

- IV Length - WPA includes a 48 bit Initialization Vector, increasing the cryptographic complexity of encrypted data.

- Dedicated authentication methods - WPA introduced the ability to use 802.1x servers. These operate as a dedicated authentication mechanisms for users, ie. RADIUS.

WPA2 goes further by supporting the Cipher Block Chaining Message Authentication Code Protocol (CCMP) however it requires greater processing power as it uses the Advanced Encryption Standard (AES) algorithm.

With the growth of wireless networks worldwide, enabling secure communications is of utmost importance. Using WPA (preferably WPA2 with the AES algorithm) is the recommended way to encrypt your wireless network, and although some brute force attacks on WPA using the TKIP algorithm are becoming available, using a randomized, strong key, following a layered approach to security and employing secondary techniques to securing your wireless LAN beyond relying solely on encryption will alleviate these risks to a large degree.

4.4. Wireless Security Myths

- "WEP is sufficient for encryption." - WEP (Wired Equivalent Privacy) is a legacy encryption technique and is not recommended for use. WEP is a poorly implemented encryption solution for

securing wireless networks, and while it may deter the most novice of attackers, simple tools exist today to remotely acquire the encryption key and gain access to all transmissions within minutes.

- "MAC address filtering stops attackers." - MAC (Media Access Control) addresses are identifiers attached to every wireless network adapter and AP, and are designed to be unique to each client adapter in the world and every AP. Many believe that entering these MAC addresses into their wireless configuration to only allow access from the specified addresses affords them a high level of security. While this also may deter the most novice of attackers, the allowed MAC addresses can easily be discovered by an attacker and then "spoofed", impersonating a legitimate user and fooling the AP into thinking the attacker is an allowed user. This is one of the simplest wireless attacks; also, maintaining a list of allowed MAC addresses is a cumbersome approach for large environments.

- "Disabling ESSID broadcasts stops attackers." - Many access points offer the ability to hide, disable or cloak the broadcasting of the network's ESSID (Extended Service Set IDentifier), similar to a network name. Not only are there freely available tools which expose any hidden ESSID by sending special probes to the access point, but disabling ESSID broadcasts can actually open a security vulnerability: If an attacker were to discover the hidden ESSID, he could set up his own access point with the same ESSID, effectively creating a "honeypot" AP, to which clients would attempt to associate with, exposing further network details.

- "WPA alone is sufficient for security." - Although WPA and WPA2 represent the cutting edge in wireless encryption, relying on either of them alone is never a good idea. Weak WPA keys can be recovered using dictionary attacks, and your wireless network can still be open to a host of other vulnerabilities.

Remember that computer security is a *process*, not a product. Wireless networks are no different, regardless of their size - there is no "silver bullet" security solution, despite what some vendors would have you believe.

While implementing some of the above methods are considered as mostly ineffective and are treated here as myths, using them as a supplement might offer some sort of peace of mind, depending on your environment. The important thing to remember is that problems arise when a single solution is relied upon, and the *layered* approach to security methodology is abandoned.

4.5. Best Practices

- *Change passwords on routers/AP* - Wireless routers and access points ship with a default password (such as "admin", or "password") for their configuration interface. Attackers have access to the default usernames and passwords for most models on the market today. Change this default password to a complicated one so that an attacker can not gain access to the configuration pages and change settings, simply by knowing the default password of your particular model.

- *Change the default SSID* - The SSID represents the network name. Attackers also know the default SSID of most wireless devices, and leaving the SSID at the default value reveals information about your network and could give an attacker the opportunity to perform exploits on the device, or otherwise use the knowledge of the model/make of the device to their advantage. It is also a good idea to change the SSID on a regular basis.

- *Use WPA or WPA2* - As described in *Section 4.2, "Wired Equivalent Privacy (WEP)"*, WEP is considered a poor solution for wireless encryption. Using WPA or WPA2 with a strong, complicated key, using the AES algorithm is recommended.

- *Change keys regularly* - Keys should be changed regularly. Re-generate your encryption key from within the configuration interface of the access point if possible, or use online generators like the one available here: *http://www.yellowpipe.com/yis/tools/WPA_key/generator.php*

- *Disable DHCP* - Many routers and access points include a DHCP (Dynamic Host Configuration Protocol) server, which distributes IP addresses to wireless stations - an IP address is essential for a computer to communicate on the Internet. If your router or access point supports it, consider disabling the internal DHCP server and manually assigning IP addresses to allowed clients. This may deter some attackers who might not be able to otherwise discover the IP address range or types in use.

- *Enable the router's firewall* - As with any connection to the Internet, a firewall will help filter and block unwanted connections, and you should enable it if available.

- *Client-side security* - Continue to follow good system security practices; use updated anti-virus and anti-spyware/malware software, use firewalls, disable unnecessary services, and install the latest patches and updates from your operating system vendor.

Some of the recommended practices when configuring a wireless network may not stop an experienced attacker on their own, however using several security methods as part of a *layered* approach will help maintain the security of your network and protect your data. Again, security is a *process*, not a single product.

Fedora And Wireless

This chapter covers details specific to Fedora and the support for wireless hardware in the Linux kernel. Also included are instructions showing how to use the graphical and command-line interface (CLI) utilities when configuring a simple wireless connection.

5.1. Hardware

Before purchasing wireless hardware for Fedora it is a good idea to do some research first to make sure support for the hardware exists. The make and model of a particular client adapter may not be the most important factor when deciding on hardware; what is important in terms of Linux is which underlying *chipset* is used, as wireless hardware is rarely advertised based on its chipset.

The chipset is what the Linux driver usually recognises, and although the overall features are important (for instance 802.11g or 802.11n support, power output levels), the brand name is not always important to the Fedora infrastructure. For instance, a wireless card branded as a Netgear product might actually use an Atheros chipset for its internal mechanisms.

5.2. Drivers, Chipsets, Devices

Refer to *http://linuxwireless.org/en/users/Drivers* for an updated list of available Linux drivers. Click on each driver to find lists of supported devices if available.

5.3. Using NetworkManager

This section demonstrates setting up a wireless connection in Fedora using NetworkManager. You can configure a wired or wireless connection with NetworkManager, and roaming between different connections is possible, as the service can choose the best available connection. NetworkManager will only work once the appropriate drivers for the underlying hardware are installed and configured properly. This section provides screenshots for configuring a simple wireless connection via the graphical interface provided by Fedora. This is an example only and demonstrates how simple wireless connections are configured in Fedora using NetworkManager.

1. First, make sure that the relevant wireless interface (usually *eth0* or *eth1*) is controlled by NetworkManager. Click on `System>Administration>Network`:
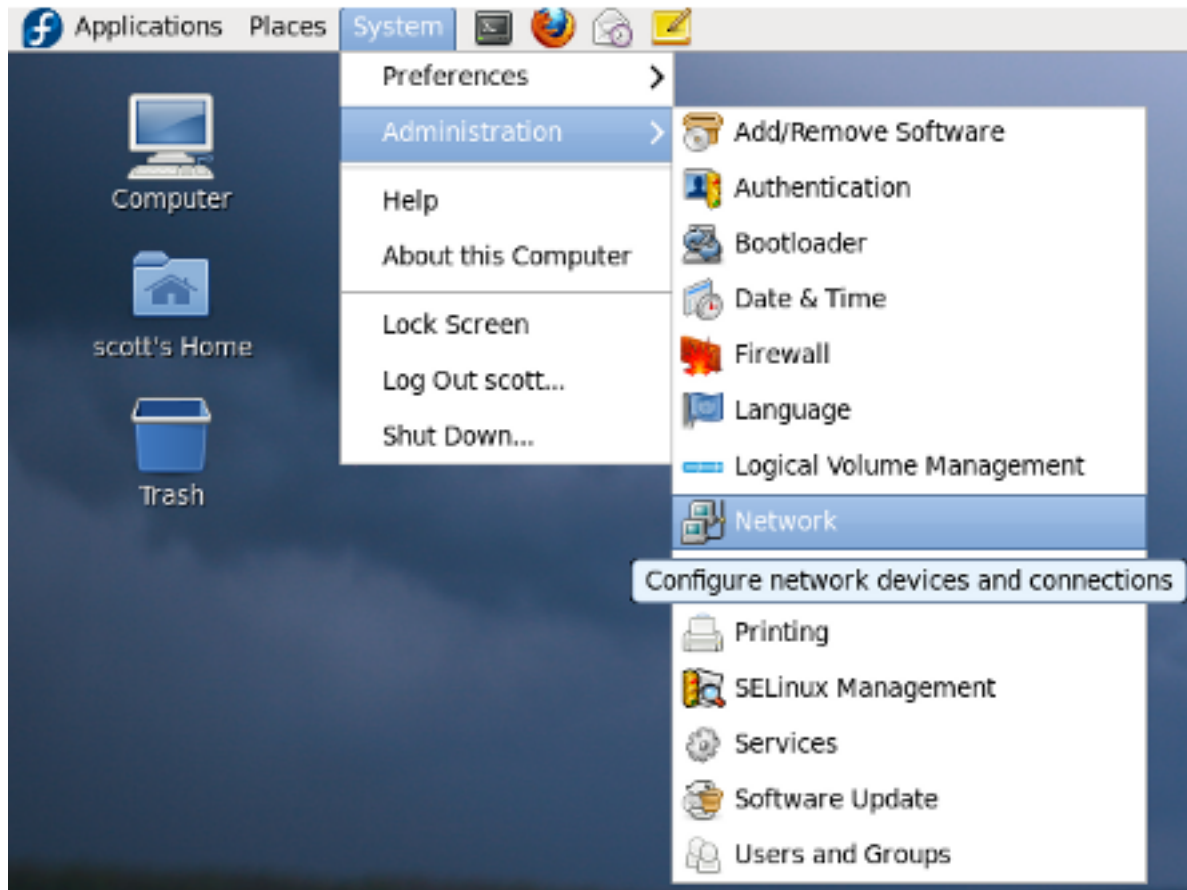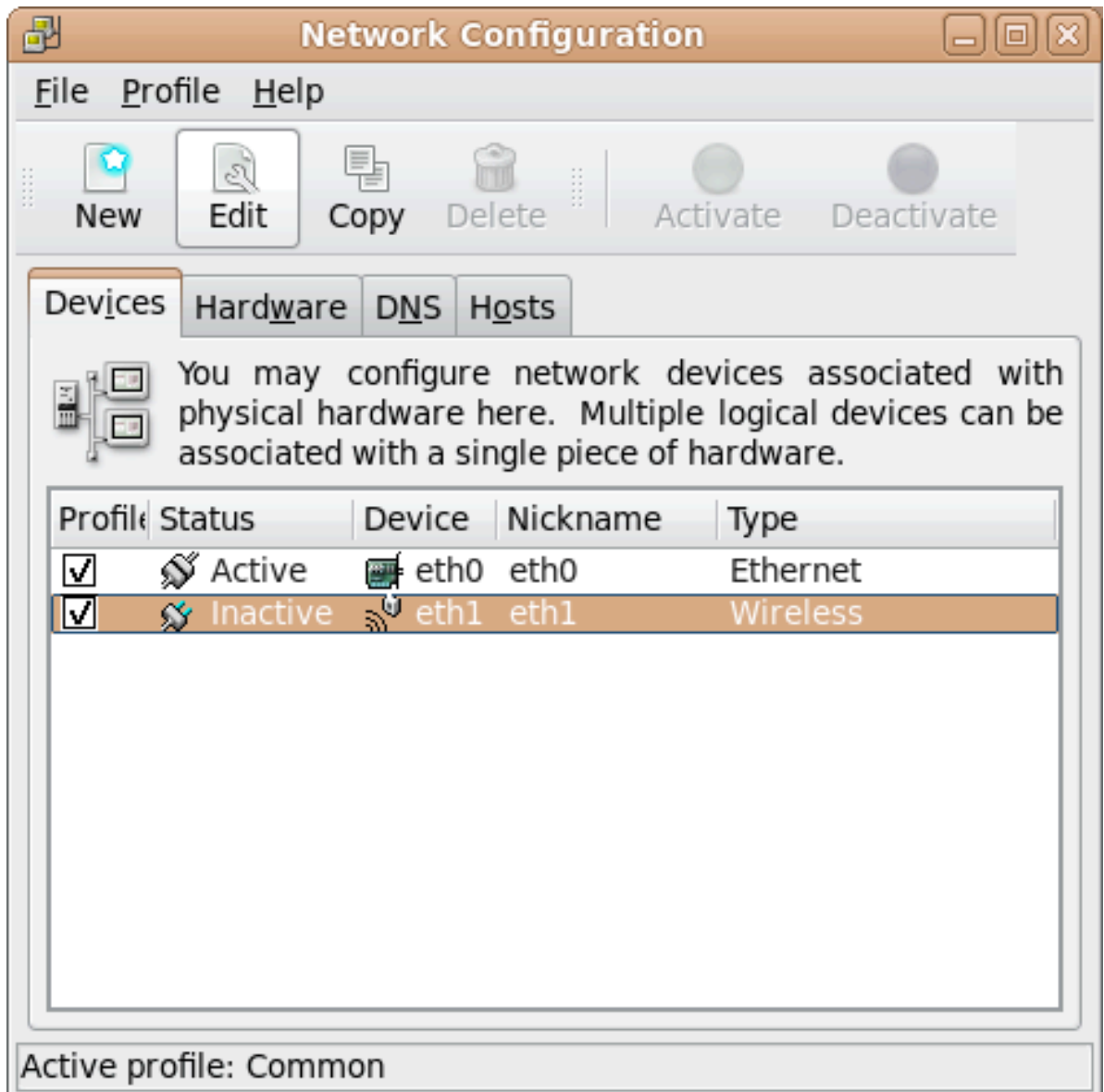
2. Enter your root (administrative) password to gain the privilige required to launch NetworkManager and click OK:
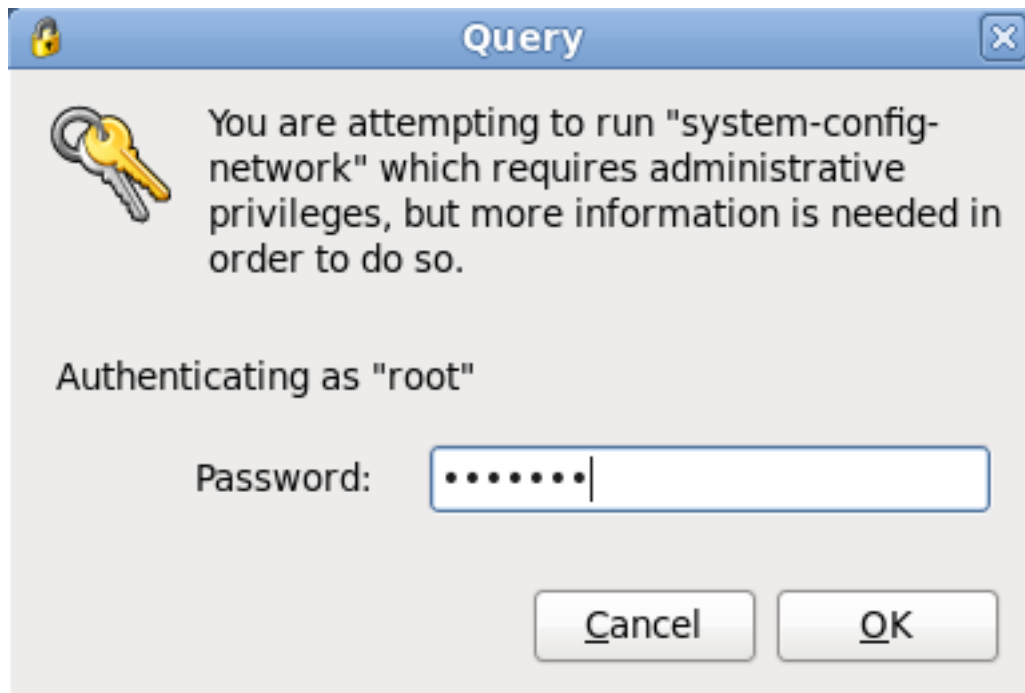
3. On the `Devices` tab, select the wireless interface and click `Edit`:

If you do not see a wireless interface in this window, it means that your wireless interface is not supported or configured properly. Make sure you have a supported card and that it is properly inserted and enabled. Many laptops have a physical hardware switch somewhere on the chassis - if present, make sure it is turned on.

4. On the `General` tab, make sure that `Controlled by NetworkManager` is enabled and click `OK`:
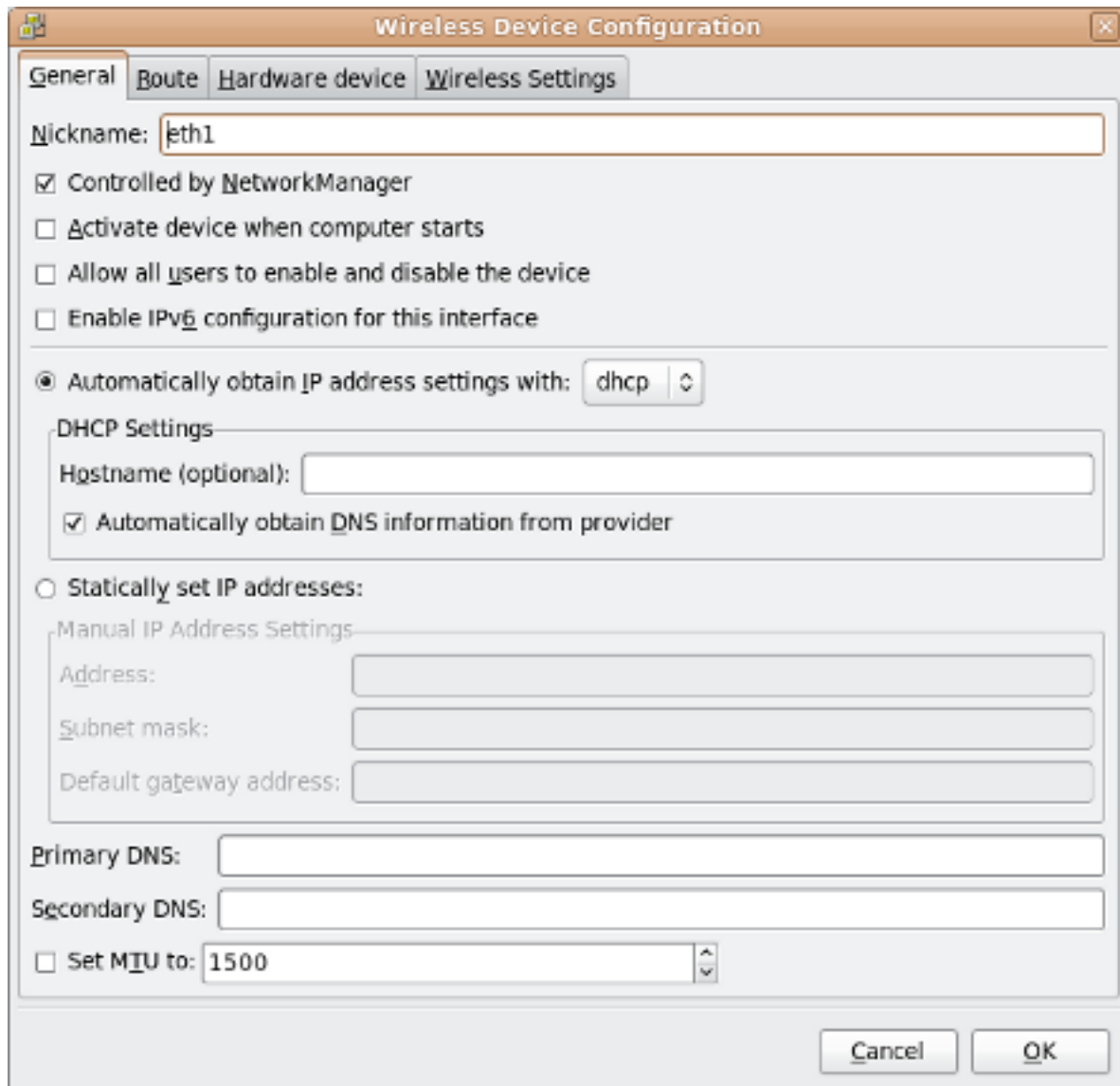
Close the `Network Configuration` window and save changes if any were made. Now that the interface is controlled by NetworkManager, the following steps will demonstrate how to connect to a wireless network using it.

5. Click on the wireless icon on the panel. As shown in the following image, a list of nearby available wireless networks will appear. The name that appears will be the same as your SSID or network name as configured in your access point. The names of the available networks in this image have been blurred:
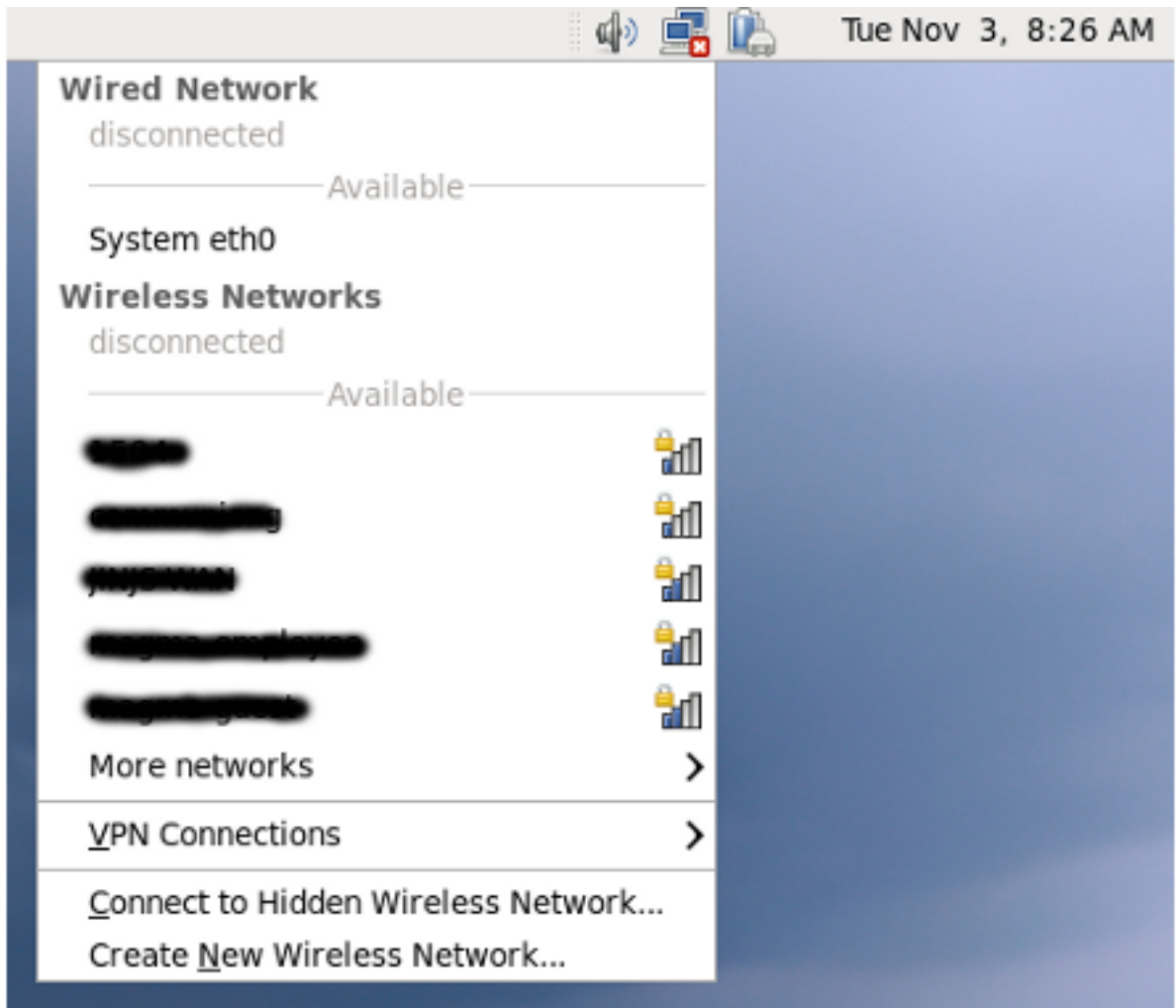
Simply click on your network. Depending on what encryption type is used, one of the following dialog boxes will appear.
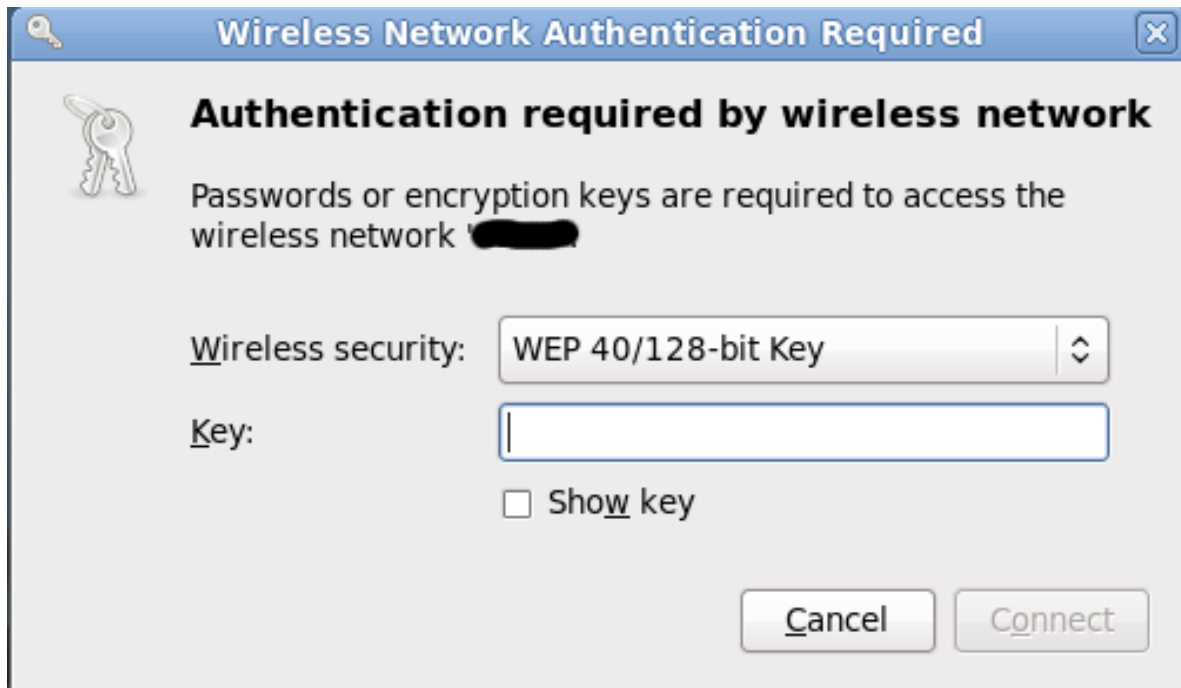
Note the different type of `Wireless security` options in the images. This represents the different types of encryption that the network uses. Fedora will detect which type is in use and present the correct option for you to enter your network key.

6. Enter your network key/password (WEP or WPA) into the available field and click `Connect`. If the access point is using DHCP and configured properly, Fedora will connect and network access should be functional.

5.4. Using the command line interface

The following steps demonstrate how to configure a wireless connection in Fedora using the command-line interface (CLI) using the **iwconfig** command. This is an example only and demonstrates how simple wireless connections are configured in Fedora using the **iwconfig** command. Using NetworkManager is the recommended method to configure a wireless network, and knowing how to use **iwconfig** is usually not required.

1. First make sure NetworkManager is not controlling the interface. Deselect the `Controlled by NetworkManager` option that is shown in the image available here: *Section 5.3, "Using NetworkManager"* at Step 4, then click `OK` and save changes.

2. Reboot the machine to make sure NetworkManager is not controlling the interface.

iwconfig is a command-line utility that sets the parameters of a network interface that connects to a wireless network. Open a terminal and run **su -** and enter the root/administrative password to switch to the root user. Run **iwconfig** without any arguments to show which interface has wireless capabilities:

```
[scott@localhost ~]$ su -
Password:
[root@localhost ~]# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

eth1      unassociated  Mode:Managed  Frequency=2.427 GHz
          Access Point: Not-Associated   Bit Rate:0 kb/s   Tx-Power=20 dBm
          Sensitivity=8/0
          Retry limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0

[root@localhost ~]#
```

Note that `eth1` is a working wireless interface, and is currently not associated to any network.

The following output shows the use of **iwconfig** to connect to a simple wireless network with an ESSID of `mynet` with a WEP key of `16a12bd649ced7ce42ee3f383f`:

```
[root@localhost ~]# iwconfig eth1 essid mynet key 16a12bd649ced7ce42ee3f383f
[root@localhost ~]# ifconfig eth1 up
[root@localhost ~]# dhclient eth1
```

Once these commands are entered, run **iwconfig eth1** to show the connection details:

```
[root@localhost ~]# iwconfig eth1
eth1      IEEE 802.11g  ESSID:"mynet"
          Mode:Managed  Frequency:2.427 GHz  Access Point: 00:1D:A2:88:A9:41
          Bit Rate:54 Mb/s   Tx-Power=20 dBm   Sensitivity=8/0
          Retry limit:7   RTS thr:off   Fragment thr:off
          Encryption key:16A1-2BD6-49CE-D7CE-42EE-3F38-3F   Security mode:open
```

```
        Power Management:off
        Link Quality=84/100  Signal level=-43 dBm  Noise level=-85 dBm
        Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
        Tx excessive retries:0  Invalid misc:7   Missed beacon:12
```

Other Wireless Technologies

IEEE 802.11 is not the only available mobile data access method. Many of the following mobile technologies are popular for Internet access from cell phones and other mobile devices, offering connectivity within the cell phone coverage areas. With the introduction of video calls and more bandwidth-intensive applications, higher speeds and more capability is in high demand for mobile devices.

6.1. CDMA

Code Division Multiple Access is a channel access method used by several radio technologies for cellular access. Originally a military technology, used as a way to transmit over several different frequencies instead of one single frequency, CDMA is the platform on which modern 3G services are built. CDMA uses spread-spectrum to communicate, using very low power levels, which makes it less likely for CDMA to cause interference with other systems.

6.2. GPRS

GPRS (General Packet Radio Service) is a mobile data service, available for both 2G and 3G cellular systems. Typical data rates are 56-114 kbit/s.

Linux provides support for several GPRS devices and connection methods (Serial, USB, Bluetooth). Refer to the following URL for a detailed guide on using GPRS with Linux: *http://www.xs4all.nl/~ernstagn/GPRS-HOWTO/*.

6.3. DECT

Digital Enhanced Cordless Telecommunications is a standard for cordless telephones. Features of a DECT system include extended battery life, multiple handsets that can make internal calls, extended range, and improved operation and call clarity in congested environments. More information about DECT can be found at the following URL: *http://en.wikipedia.org/wiki/Digital_Enhanced_Cordless_Telecommunications*.

6.4. EV-DO

Evolution-Data Optimized is a standard for wireless communications, often used for wireless broadband that provides up to 3Mbps of throughput. A user can seamlessly roam between cells, and can use the same cells as regular cell phones. It provides the capability for users that live outside the distance limitation of DSL services to access high-speed Internet connections. The following URL provides further details on EVDO - news, tips and product reviews: *http://www.evdoinfo.com/*.

6.5. HSDPA

High-Speed Downlink Packet Access is considered a 3.5G mobile service, and provides theoretical download speeds of up to 14.4Mbps. It is a protocol used by cell phones and is designed to increase speeds and coverage. Refer to the following URL for further information on HSDPA: *http://www.tech-faq.com/hsdpa.shtml*.

Other Resources

IEEE Resources

- *IEEE home page*[1]

- *About the IEEE*[2]

- *802.11 Working Group home page*[3]

- *IEEE at Wikipedia.org*[4]

General Wireless Resources

- *How WiFi works (Howstuffworks.com)*[5]

- *WiFi details and resources (About.com)*[6]

- *The ABCs of securing your wireless network (Arstechnica.com)*[7]

- *Wireless Security - How WEP works (Plynt.com)*[8]

- *Wi-Fi Protected Access (WPA) (Wikipedia.org)*[9]

- *http://www.home-wlan.com, general details on wireless in the home/office*[10]

Appendix A. Revision History

Revision 1.0   12 Nov 2009   Scott Radvan *sradvan@redhat.com*

Initial commit to SVN, add resources/URLs (chap7), attribute images

Revision 1.1   16 Nov 2009   Scott Radvan *sradvan@redhat.com*

Major review, remove draft status, prepare for publishing

Index