

Routers:

- Why may you need a router:
 - If you have more than one computer
 - If you want to use your computer around the home without wires.
 - Want internet protection provided by “hiding” behind a router. (Equivalent to having a hardware firewall)
- Types of routers:
 - 4, 8, 16... port — wired (no wireless)
 - 4 port wired + wireless
 - Type “b” — 2.4 Ghz—11 Mbit/s (4.3)
 - Type “g” — 2.4 Ghz—54 Mbit/s (19)
 - Type “b-g”— 2.4 Ghz—will support both of the above
 - Type “a” — 5 Ghz—54 Mbit/s (23)
 - Type “n”—2.4 & 5 Ghz — 600 Mbit/s (74)
 - Type “y”— 3.7 Ghz — 54 Mbit/s (23) coming in 2010
- If you have or purchase a wireless router, you will need to do the program your router for the following—
 - The broadcasted “name” of your router
 - The protocol the router will support—
 - “b” only
 - “b & g”
 - Security for the connection
 - WPA or WPA2 with a password
 - Recommend that you set the router to a channel other than channel 1,6 or 11
 - If you have the router at the time you hook up to DSL, Wydebeam will program your router during installation/setup.
 - If you purchase your router later, you can program it during installation via the setup wizard supplied by the manufacture.
 - If you need another way to setup your router, you can call (a fee is charged for the service)
 - Willie Muhlenberg
 - 480-600-8117
 - williem5@wmcomputing.net
 - The final way to setup your router would be at a “Router Workshop provided by the Computer Club. Yet to be setup.

Wired Equivalent Privacy (WEP)

From Wikipedia, the free encyclopedia

Wired Equivalent Privacy (WEP) is a flawed algorithm to secure [IEEE 802.11](#) wireless [networks](#). Wireless networks broadcast messages using [radio](#), so are more susceptible to [eavesdropping](#) than wired networks. When introduced in 1999, WEP was intended to provide [confidentiality](#) comparable to that of a traditional wired [network](#).

Beginning in 2001,^[1] several serious weaknesses were identified by [cryptanalysts](#) with the result that today a WEP connection can be cracked with readily available software within minutes. Within a few months the [IEEE](#) created a new [802.11i](#) task force to counteract the problems. By 2003, the [Wi-Fi Alliance](#) announced that WEP had been superseded by [Wi-Fi Protected Access](#) (WPA), which was a subset of then upcoming 802.11i amendment. Finally in 2004, the IEEE declared that both WEP-40 and WEP-104 " have been [deprecated](#) as they fail to meet their security goals".^[2] with the ratification of the full 802.11i standard (also known as WPA2). Despite its weaknesses, WEP is still widely in use as it provides a level of security that may appear to deter casual snooping or unintentional use of a private network.

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA and WPA2) is a class of systems to secure wireless ([Wi-Fi](#)) [computer](#) networks. It was created in response to several serious weaknesses researchers had found in the previous system, [Wired Equivalent Privacy](#) (WEP). WPA implements the majority of the [IEEE 802.11i](#) standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is designed to work with all [wireless network interface cards](#), but not necessarily with first generation [wireless access points](#). WPA2 implements the full standard, but will not work with some older network cards. Both provide good security, with two significant issues:

- Either WPA or WPA2 must be enabled and chosen in preference to WEP. WEP is usually presented as the first security choice in most installation instructions.

In the "Personal" mode, the most likely choice for homes and small offices, a [passphrase](#) is required that, for full security, must be longer than the typical 6 to 8 character [passwords](#) users often employ.

Radius

This stands for [Remote Authentication Dial In User Service](#). This is an [AAA \(authentication, authorization and accounting\) protocol](#) used for remote network access. This service provides an excellent weapon against crackers. RADIUS was originally proprietary but was later published under ISOC documents [RFC 2138](#) and [RFC 2139](#). The idea is to have an inside server act as a gatekeeper through the use of verifying identities through a username and password that is already pre-determined by the user. A RADIUS server can also be configured to enforce user policies and restrictions as well as recording accounting information such as time connected for billing purposes.

WPA2

WPA2 implements the mandatory elements of 802.11i. In particular, in addition to TKIP and the Michael algorithm, it introduces a new [AES](#)-based algorithm, [CCMP](#), that is **considered fully secure**. From [March 13, 2006](#), WPA2 certification is mandatory for all new devices wishing to be Wi-Fi certified.