

Wireless Networking Backgrounder

Things you wanted to know about wireless networking

THE CONSIDERATION OF USING WIRELESS SOLUTIONS FOR YOUR INTERNET CONNECTION MAY RAISE SOME QUESTIONS FOR THOSE UNFAMILIAR WITH THE TECHNOLOGY.

Does weather affect wireless connections? Should I worry about rain or fog?

Rain and fog typically have a negligible impact on system performance for wireless systems operating below 11 GHz. Since Covad Wireless' customer premises products operate at 5.3 and 5.8 GHz, such environmental factors typically have an insignificant effect on performance. Systems functioning above 11 GHz are referred to as millimeter wave systems and one does need to take weather into consideration when considering using such systems. Most satellite TV systems function above 11 GHz, and consequently are impacted by weather. The size of the RF signal carrying direct-to-home television happens to be about the size of the average raindrop. When the weather is clear, the RF signal can reach the satellite TV dish with a minimum of degradation. However, when it starts to rain, some of the signal gets absorbed by rain and, therefore, less of it reaches the dish on the roof. Very heavy rain can entirely eliminate the signal as you may have noticed on rare occasions. Wireless systems operating above 11 GHz are engineered with particular consideration to environments subject to rain and with added care taken when areas are subject to cloud cover and temperature variations or over-water links. For example microwave links operating at frequencies such as 18, 23 and 38 GHz can be impacted by very dense rainfall. There are mathematic prediction models that account for climate conditions at all frequencies, and the system can be designed to provide a very reliable link even in the face of adverse weather conditions. Covad Wireless products can reliably span distances of up to 8 miles, even in adverse weather conditions.

Do Covad Wireless' radios emit unsafe amounts of radiation?

The products that Covad Wireless uses adhere to all applicable Federal Communications Commission rules that pertain to radio frequency (RF)

exposure levels. Such rules are based on the scientific evidence presently available and incorporate significant margins of safety to ensure the health of the general public.

The risk of harmful exposure to any radiated energy is a function of the frequency of the radiation, the power of the energy, the proximity and the length of time of exposure. For example, solar radiation can cause sunburn and potentially lead to skin cancer if one spends enough time in direct sunlight. Similarly, medical X-Rays, in small exposures over long intervals, are shown to have minimal safety risk to patients. Covad Wireless radios with their antenna are typically installed on rooftops or up against a window with the bulk of the RF energy pointed away from where people are located. The energy remaining in the area is typically less than that of the use of a cell phone or a common indoor wireless access point or router.

Note that radio waves should not be confused with X-Rays, which are much more powerful and have different effects on the human body.

Does Covad Wireless' wireless technology offer intermittent availability similar to my cellular telephone?

While both Covad Wireless' communication devices and cellular telephones do use Radio Frequency (RF) technology, the Covad Wireless links are engineered to offer greater than 99.995% uptime, which translates into less than one hour of unplanned downtime per year. Cellular telephone technology is designed to function at "threshold" using the minimum necessary signal to maintain a connection. As a result of this design, cell phones are susceptible to lost connections. Covad Wireless connections provide 100 to 1000 times the minimum signal and have a considerable "fade margin" enabling the technology to provide connection even in adverse circumstances.

Does wireless breach security since anyone can listen to the network traffic?

Security is an area of concern for those considering the use of fixed wireless devices to transmit data. Because Covad Wireless' radios transmit signals into the "air," the perception can be that anyone could receive and possibly "steal" or "listen too" someone's data. The transceivers that Covad Wireless installs offer a very robust framework featuring a variety of security related countermeasures:

- 1) The Covad Wireless transmission signal is so unique that it requires another Covad Wireless radio to receive and decode the signal. The Ethernet traffic (along with associated control & monitoring information for the link) is assembled in a proprietary framing structure and sent to the receiving radio. The data remain encoded until they are received and disassembled by the radio at the customer's end. Data are scrambled in a nearly random pattern prior to transmission by adding specific bits of data to the information being transmitted: bits that are subsequently processed by the receiving bridge to ensure data integrity. For example, the base station maintains a user-configurable and password controlled table of authorized subscriber unit MAC (Media Access Control) addresses. Customer radio units cannot talk to the network unless they are authenticated in the Covad Wireless network.
- 2) The customer radios are configured to filter the downlink traffic stream to prevent another radio from outputting traffic that is destined to another radio other than the Covad Wireless base station. The filtering restrictions are based upon Ethernet addresses, VLAN addresses, or other IP addresses. Only the network operator can configure the filtering controls. This prevents unauthorized access of another user's data.
- 3) One basic tenet of the fixed wireless technology used by Covad Wireless is the requirement for "line of sight." The transmitting and receiving antennas on the radios communicate through a relatively narrow radio frequency (RF) beam. This directional point-to-point RF approach is in stark contrast some omni-directional antennas used on cellular telephones and wireless LAN products where anyone in the vicinity could receive the signal. With Covad Wireless, only an antenna firmly in the focused RF target area could receive information which, as noted above, is encrypted. By its very nature, Covad Wireless' wireless technology further minimizes the opportunity for intrusion.

Covad Wireless' wireless system and 802.11a/b/g: Apples & Oranges

The IEEE standard for wireless LAN communications, 802.11, was featured in the news when particular wireless protocols used by 802.11 were discovered to have the potential for improper access. These flaws left the 802.11 technology vulnerable to attacks that could decrypt traffic. The 802.11 technology is used predominately in point-to-multipoint applications such as wireless LAN connectivity for PCs and local LAN devices.

The technology that Covad Wireless uses is different from the 802.11 devices and adheres to 802.3 standards and uses a different proprietary security scheme than that used by 802.11 devices. The proprietary nature of Covad Wireless' technology precludes threats to data privacy that are encountered by 802.11 wireless LAN technologies.

Please refer to our FAQ for answers to other commonly asked questions about our service.
<http://www.covadwireless.com/support-servicefaq.htm>