

Wireless network communication essay

[Business](#), [Management](#)



Experts in the industrial environment acknowledge the growing need for wireless technology. The emerging wireless handheld devices dramatically expand mobility when applied to standard industrial activities like inventory and stock management. The increased productivity and cost savings far outweigh the cost of investing in new wireless technology.

This paper describes how to implement a wireless network in an upstart trucking company environment. This is a medium sized company with 1000 staff members in three locations. We will be using technologies such as WLAN, WAN, WMAN, RDIF and GPS to implement the wireless network.

Implementation of the wireless communication in an upstart trucking company The executives of the company are interested in applying wireless technology to make their network more efficient and to increase customer service. Executives have kept up with wireless trends in the trucking market and they also know that company needs to increase employee productivity and customer response. Handheld devices will enable the employees to respond to customer pages. These devices will make it easy to assess the customers who need assistance and respond to them quickly. When a customer requests specific information, the sales associates with that particular expertise can respond.

Since employee incentives are based on commission and customer satisfaction, handheld devices will become sales associates' pagers. After careful evaluation of several client interview and surveys the following requirements are base-lined for the wireless implementation: 1. Provide wireless access for laptops in all three offices. 2.

Provide wireless connectivity in conference rooms in the main office building. Provide a replacement to the leased T-1s that connect two satellite buildings (branch offices) to the main building. Provide increased bandwidth to the satellite buildings. 3. Company's staff should be able to often travel to a remote site and want to walk up to a shared printer, connect and print a document without having to physically connect using a standard printer cable. 4. People should be able be connected to my corporate LAN while moving about in the office building or campus.

5. Stuffs should be able to access to e-mail and web resources while traveling away from the home office. 6.

The inventory tracking will be done in real time through RFID implementation. Designing and implementation of the Wireless Network. The approach is straightforward—we must determine how to address the customer's needs and make sure they are well defined; the owner and his management team must verify information about the employees and the customers for you. After the approach is determined, we'll begin the planning by defining the network elements and their placement, and gathering details about the physical space and the intended use. After ample design time, our team will purchase the hardware elements, and then implement the design by installing and configuring the hardware elements and making the necessary software changes. During implementation, we'll have to test every aspect of the system, including the range of the handheld devices and the ability to check bar codes on the loading dock. At the end of

the implementation phase, you should be able to verify that the results fulfill the needs of client.

(R. Hutchins and E. W. Zegura, 2000, 1) Pre-Deployment Preparation The company operates two leased satellite office buildings surrounding an eight-story central main office tower. The company operates three leased satellite office buildings surrounding an eight-story central main office tower. In the current physical network, all the satellite buildings use internal Category 5 Unshielded Twisted Pair (UTP) wiring. The Administration department expressed the need for LAN access in conference rooms in the main building.

Since all employees are receiving laptop computers, all departments will require the ability to access the network from anywhere in the satellite buildings and in the conference room in the main office building. The satellite buildings connect to the main office via leased T-1 links. The wireless network must provide security and encryption. (D. Tang and M. Baker, 2000, 56) Implementation of WLAN and WPAN To fulfill the requirements 1, 2, 3 and 4 we will implant a Wireless Local Area Network (WLAN) and Wireless Private Area Network (WPAN) communication within the buildings and campus. A wireless LAN or WLAN is a wireless local area network that uses radio waves as a carrier, to give a network connection to all users in the vicinity. Areas may range from a single room to an entire campus.

The network usually uses cables, with one or more wireless access points connecting the wireless users to the wired network. A private network (PAN) is a computer network used for communication between computer devices (including telephones and personal digital assistants) close to a person. The

scope of a PAN is typically a few meters. PAN can be used for communication between personal devices themselves (intrapersonal communication), or to connect to a higher level and the Internet (an uplink).

(Hutchins and E. W. Zegura, 2002) Personal area networks May be connected to the computer, such as USB and Firewire. A wireless personal network (WPAN) can also be made possible with network technologies such as IrDA and Bluetooth. A WPAN typically has a range of 10 meters, although ranges of up to 100 meters can be achieved under ideal circumstances. To implement that WLAN and WPAN we will use the following technologies and third party providers: Bluetooth: It is an industrial specification for wireless personal networks (PAN). Bluetooth allows you to connect and exchange information between devices like personal digital assistants (PDAs), mobile phones, laptops, computers, printers and digital cameras via a secure, low cost, the globally available radio frequency short range. Bluetooth enables these devices to communicate among them when they come in range, even if they are not in the same room, as long as they are up to 100 meters (328 feet) on the other, depending on the class power product.

Products are available in three power classes: 1. Class 3 (1 mW) is the rarest and allows the transmission of 10 centimeters (3.9 inches) with a maximum of 1 meter (3.2 feet) 2. Class 2 (2.5 mW) is the most common and allows a transmission distance of the city of 10 meters (32 feet) 3. Class 1 (100 mW) is the longest reaching up to 100 meters.

This category of product is readily available. Cellular Network Provider:

Otherwise known as a Mobile Network Operator, this is the organization that

<https://assignbuster.com/wireless-network-communication-essay/>

manages the GSM network. The physical implementation of the architecture may well have a Cellular Network Provider location for each GSM network provider company. Network Access Provider : The company that provides the infrastructure that facilitates wireless LAN connectivity and other forms of public network access such as ADSL and public Ethernet LAN.

Access Points: Access points (APs) are the most frequently installed infrastructure (non-client) devices. They provide access to the WLAN and may bridge to a wired LAN. An AP is basically a small computer that includes one or more radios and usually one Ethernet port.

Inside the AP is a processor and memory. In fact, one of the big differences between enterprise-class APs and those designed for SOHO implementations is the processing power and the amount of memory available in the AP. (I. F. Akyildiz, 2002, 38(4): 393–422) Wi-Fi: “ Wi-Fi” is a play on the old audio term “ Hi-Fi” (high fidelity). The term also has been trademarked by the Wi-Fi Alliance (formerly the Wireless Ethernet Compatibility Alliance). Today, Wi-Fi is most commonly used to describe a wireless local area network based on the IEEE 802. 11 series of standards, which is a set of wireless technical specifications issued by the Institute of Electrical and Electronic Engineers (IEEE).

The IEEE is an international professional organization for electrical and electronics engineers, with formal links with the International Organization for Standardization (more commonly known as the “ ISO”). (Balfanz, 2002, 23–35) Wi-Fi Hotspot: This is an area where wireless LAN (802. 11b) coverage is available to a subscriber in the buildings and main office. Note

that some of the locations maybe managed by the same organization. For example, the WiFi Hotspot would most likely be managed by the Network Access Provider. It is also possible for the Cellular Network Provider and Network Access Provider to be the same organization. Implantation of WLAN and WPAN When designing a wireless network in each of the satellite building, we must determine the placement of antennas and access points for best coverage.

In this example, the mechanical room, elevators, and communications room are sources of frequency interference that we need to consider. A single omnidirectional antenna might be capable of covering the office area in a satellite building (over 100 feet). However, with the interference items to consider, it would be better to place omnidirectional antennas (and access points) in each hallway to get better coverage. Also, each access point can provide redundancy.

If one access point fails, the other provides access to all computers on the floor. The wireless device will typically be a WiFi-enabled laptop, or PDA in each building. In the case of GPRS access the device will most likely be a PDA, but it could also be a laptop with a PCMCIA GPRS modem, or a cell phone. Traffic from each device will find its way to the Access Controller at the Network Access Provider. Access to Network Access Provider could be via: Public Wireless LAN Hotspot (802. 11b) Public LAN, Hotspot (Ethernet), GPRS (requires SIM), ADSL (or dial-up) or Enterprise (Wireless) LAN. Figure 1: Placement of Access Point Antennas in Satellite Buildings The access point wireless bridges will be placed on shelves near the antennas. The Ethernet

ports of the access point bridges will be connected to the LAN switches that serve the floor.

The LAN switch must be configured to permit multiple media access control (MAC) addresses on the data port. Installation of the access point devices and antennas in the building floors as described in the design: Step1: Mount the antennas in the hallways, and connect cables to the access point devices in the nearby offices. Step2: Connect the access points to the floor LAN switch.

Step3: Configure the access point frequencies, keeping configuration information available for laptop configuration. Step4: Configure the access point for bridging, and enable multiple MAC addresses on the LAN switch. At this point we are ready to test wireless access throughout the floor plan. We begin by verifying access from each office and the conference room.

The main office laptops can be equipped with the wireless PC Memory Card International Association (PCMCIA) cards and configured to connect to the LAN via the access points. Wireless Wide Area Network (WWAN)

Implementation To fulfill the requirement 5 which should allow stuffs to be able to access to e-mail and web resources while traveling away from the home office we will implement WWAN. Wireless WAN covers a much wider area than wireless LAN (WLAN). Unlike WLANs, which offer little mobility of users and are generally used to enable mobility of the entire network, WWANs facilitate connectivity for mobile users such as business travelers.

In general, WWANs allow users to maintain access to work and applications related to information outside their office. WAN wireless communication occurs primarily through the use of radio signals from analog, digital cellular or PCS networks, although the transmission of signals through microwaves and other electromagnetic waves is also possible. Today, most wireless data communication takes place across cellular 2G systems such as CDMA, PDC and GSM, or through packet data technologies older analog systems.

Although the traditional analogue networks, having been designed for voice rather than data transfer, some have problems, some 2G (second generation) and new 3G (third generation) digital cellular networks are fully integrated for data / voice. With the advent of 3G networks, the speed of transfer should also increase strongly. WWAN connectivity requires wireless modems and infrastructure wireless network, provided that the remuneration for service from a wireless service. Portable devices to receive communications from wireless modems connected and wireless networks to interact via radio waves.

The radio modem directly interfaces with the towers that carry the signal to a mobile switching center, where the signal is transmitted over public networks or private link (ie, telephone, other high-speed line, or the Internet). From there, the signal can be transferred to an existing network. Similarly, WWANs can communicate with the Internet.

For small devices such as handhelds and mobile phones, a universal specification known as Wireless Application Protocol (WAP) is to facilitate the delivery and presentation of Web content. The demand for Web content is

sent through the wireless network to a WAP gateway, where it is processed and the required information is retrieved and returned. WAP supports most wireless networks and mobile operating systems.

As for wireless LANs, wireless WANs have many interference problems associated with their dependence on terrestrial radio networks. Weather, terrain and other naturally occurring conditions can cause prolonged latency and other disturbances in the chain of radio. Nevertheless, the extensive wireless networks have many inherent advantages, namely the improvement of productivity in real-time access to information

Radio Frequency Identification (RFID) Implementation To fulfill the requirements of inventory tracking in real time we will implant RFID technology within the buildings.

Radio Frequency Identification (RFID) is an automatic identification method, relying on storing and retrieving data remotely using RFID tags or transponders. An RFID tag is a small object that can be attached or incorporated into a product, animal, or person.

RFID tags contain antennas to enable them to receive and respond to radio-frequency queries from RFID transmitter-receiver. Passive tags require no internal power source, whereas active tags require a power source. Types of RFID tags RFID tags can be active or passive. Passive RFID tags are not internal power. The minute electrical current induced in the antenna by the new radio frequency signal provides just enough power for the tag to transmit a response. Due to lack of power and cost, the response of a passive RFID tag is brief – typically just an ID number (GUID).

The lack of electrical power on board means that the device may be very low trade in products which can be embedded under the skin. In 2005, the smallest such devices commercially available measured 0.4 mm × 0.4 mm, which is thinner than a sheet of paper, these devices are practically invisible. Passive tags on practical read distances ranging from 10 mm to about 6 meters. Active RFID tags, on the other hand, have an internal power source, and may have longer range and more memories than passive tags, as well as the ability to store additional information sent by the transmitter.

At present, the smallest active tags are about the size of a coin. Many active tags have ranges of several tens of meters, and a battery life of 10 years. Because passive tags are cheaper to manufacture and have no battery, the majority of RFID tags in existence are of the passive variety.

In 2004, these tags cost from U. S. \$ 0.40 in high volume. Universal RFID tagging of products commercially viable at very large volumes of 10 billion units per year, resulting in production costs to less than \$ 0.05 according to a U.

S. manufacturer. The current demand for integrated circuit chips RFID is not ready to support that price. The independent research analysts Forrester and Gartner, companies agree that the search for price less than \$ 0.0 (the volume of production of one billion units) is achievable in 6-8 years, limiting the short-term for the widespread adoption of passive RFID. Other analysts believe that these prices are feasible in 10-15 years. While the cost of passive tags on the benefits of smart tags are important, other factors, including accuracy, performance in certain environments such as around

water or metal, reliability and make the use of active tags very common today. There are four different types of tags commonly in use.

They are categorized by their radio frequency: low frequency tags (125 or 134.2 kHz), high frequency tags (13.56 MHz), UHF tags (868 to 956 MHz) and microwave tags (2.

45 GHz). UHF tags can not be used globally as there are no global regulations for their use. The RFID system An RFID system May consist of several components: tags, readers, edge servers, middleware, and application software. The purpose of an RFID system is to enable data to be transmitted by a mobile device, called a tag, which is read by an RFID reader and processed according to the needs of a particular application. The data transmitted by the tag May provide identification or location information, or details of the marked product, such as price, color, purchase date, etc. The use of RFID in applications monitoring and access first appeared in the 1980s.

RFID quickly attracted attention because of its ability to track moving objects. As technology is refined, more pervasive and possibly invasive uses for RFID tags are being prepared. In an RFID system, individual objects are equipped with a small, inexpensive tag. The tag contains a transponder with a digital memory chip that is given an electronic product code. The interrogator, an antenna comes with a transceiver and decoder, emits a signal activating the RFID tag, it can read and write data. When an RFID tag passes through the electromagnetic zone, it detects the activation signal of the reader. The reader decodes the data encoded on the label of the

integrated circuit (silicon chip) and data are transmitted to the host computer for processing.

In our case UHF tags (868 to 956 MHz) will be used to deploy the RDIF solution. Testing the implementation We need to test all of the wireless devices and links we implemented. When installing the wireless antennas, the testing capabilities of the access point devices will be used to make sure that the wireless connection is reliable. If we encounter problems with the connection, we will try moving the antenna in one or the other direction to correct the problem. Also we will verify that interference is not caused by trees or reflection from nearby buildings.