Examples of free wlan essay

A wireless LAN or WLAN is a wireless local area network, which is the linking of two or more computers or devices without using wires. WLAN uses spread-spectrum or OFDM modulation technology based on radio waves to enable communication between devices in a limited area, also known as the basic service set. This gives users the mobility to move around within a broad coverage area and still be connected to the network. For the home user, wireless has become popular due to ease of installation, and location freedom with the gaining popularity of laptops.

Public businesses such as coffee shops or malls have begun to offer wireless access to their customers; some are even provided as a free service. Large wireless network projects are being put up in many major cities. Her are the major cities that have WLAN networking service to Mountain View, California, San Francisco and New York City boroughs of the city with wireless Internet access. Here is some of the History in the network of WLAN wireless. In 1970 University of Hawaii, under the leadership of Norman Abramson, developed the world’s first computer communication network using low-cost ham-like radios, named ALOHA net.

The bi-directional star topology of the system included seven computers deployed over four islands to communicate with the central computer on the Oahu Island without using phone lines. The first generation of wireless data modems was developed in the early 1980s by amateur radio operators, who commonly referred to this as packet radio. They added a voice band data communication modem, with data rates below 9600 bit/s, to an existing short distance radio system, typically in the two meter amateur band. The second generation of wireless modems was developed immediately after the

FCC announcement in the experimental bands for non-military use of the spread spectrum technology.

These modems provided data rates on the order of hundreds of kbit/s. The third generation of wireless modem then aimed at compatibility with the existing LANs with data rates on the order of Mbit/s. Several companies developed the third generation products with data rates above 1 Mbit/s and a couple of products had already been announced by the time of the first IEEE Workshop on Wireless LANs. “ The first of the IEEE Workshops on Wireless LAN was held in 1991. At that time early wireless LAN products had just appeared in the market and the committee had just started its activities to develop a standard for wireless LANs. The focus of that first workshop was evaluation of the alternative technologies.

By 1996, the technology was relatively mature, a variety of applications had been identified and addressed and technologies that enable these applications were well understood. Chip sets aimed at wireless LAN implementations and applications, a key enabling technology for rapid market growth, were emerging in the market. Wireless LANs were being used in hospitals, stock exchanges, and other in building and campus settings for nomadic access, point-to-point LAN bridges, ad-hoc networking, and even larger applications through internetworking. Applause quickly built as people realized there were no wires. This was the first time Wireless LAN became publicly available at consumer pricing and easily available for home use. Before the release of the Airport, Wireless LAN was too expensive for consumer use and used exclusively in large corporate settings.

Originally WLAN hardware was so expensive that it was only used as an alternative to cabled LAN in places where cabling was difficult or impossible. Early development included industry-specific solutions and proprietary protocols, but at the end of the 1990s these were replaced by standards, primarily the various versions of IEEE 802. 11 (Wi-Fi). An alternative ATM-like 5 GHz standardized technology, HiperLAN/2, has so far not succeeded in the market, and with the release of the faster 54 Mbit/s 802. 11a (5 GHz) and 802. 11g (2.

4 GHz) standards, almost certainly never will. Here are some of the Benefits in the network of WLAN wireless. Convenience: The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment (home or office). With the increasing saturation of laptop-style computers, this is particularly relevant. Mobility: With the emergence of public wireless networks, users can access the internet even outside their normal work environment.

Most chain coffee shops, for example, offer their customers a wireless connection to the internet at little or no cost. Productivity: Users connected to a wireless network can maintain a nearly constant affiliation with their desired network as they move from place to place. For a business, this implies that an employee can potentially be more productive as his or her work can be accomplished from any convenient location. Deployment: Initial setup of an infrastructure-based wireless network requires little more than a single access point.

Wired networks, on the other hand, have the additional cost and complexity of actual physical ables being run to numerous locations (which can even be impossible for hard-to-reach locations within a building). Expandability: Wireless networks can serve a suddenly-increased number of clients with the existing equipment. In a wired network, additional clients would require additional wiring. Cost: Wireless networking hardware is at worst a modest increase from wired counterparts.

This potentially increased cost is almost always more than outweighed by the savings in cost and labor associated to running physical cables. Here are some of the Disadvantages in the network of WLAN wireless. Security: Wireless LAN transceivers are designed to serve computers throughout a structure with uninterrupted service using radio frequencies. Because of space and cost, the antennas typically present on wireless networking cards in the end computers are generally relatively poor. In order to properly receive signals using such limited antennas throughout even a modest area, the wireless LAN transceiver utilizes a fairly considerable amount of power.

What this means is that not only can the wireless packets be intercepted by a nearby adversary’s poorly-equipped computer, but more importantly, a user willing to spend a small amount of money on a good quality antenna can pick up packets at a remarkable distance; perhaps hundreds of times the radius as the typical user. In fact, there are even computer users dedicated to locating and sometimes even cracking into wireless networks, known as war drivers. On a wired network, any adversary would first have to overcome the physical limitation of tapping into the actual wires, but this is not an issue with wireless packets. To combat this consideration, wireless networks

users usually choose to utilize various encryption technologies available such as Wi-Fi Protected Access (WPA). Some of the older encryption methods, such as WEP are known to have weaknesses that a dedicated adversary can compromise.

Range: The typical range of a common 802. 11g network with standard equipment is on the order of tens of meters. While sufficient for a typical home, it will be insufficient in a larger structure. To obtain additional range, repeaters or additional access points will have to be purchased. Costs for these items can add up quickly. Other technologies are in the development phase, however, which feature increased range, hoping to render this disadvantage irrelevant.

Reliability: Like any radio frequency transmission, wireless networking signals are subject to a wide variety of interference, as well as complex propagation effects (such as multipath, or especially in this case Ricans fading) that are beyond the control of the network administrator. One of the most insidious problems that can affect the stability and reliability of a wireless LAN is the microwave oven. In the case of typical networks, modulation is achieved by complicated forms of phase-shift keying (PSK) or quadrate amplitude modulation (QAM), making interference and propagation effects all the more disturbing. As a result, important network resources such as servers are rarely connected wirelessly. Speed: The speed on most wireless networks (typically 1-108 Mbit/s) is reasonably slow compared to the slowest common wired networks (100 Mbit/s up to several Gbit/s).

There are also performance issues caused by TCP and its built-in congestion avoidance. For most users, however, this observation is irrelevant since the speed bottleneck is not in the wireless routing but rather in the outside network connectivity itself. For example, the maximum ADSL throughput (usually 8 Mbit/s or less) offered by telecommunications companies to general-purpose customers is already far slower than the slowest wireless network to which it is typically connected. That is to say, in most environments, a wireless network running at its slowest speed is still faster than the internet connection serving it in the first place. However, in specialized environments, higher throughput through a wired network might be necessary.

Newer standards such as 802. 11n are addressing this limitation and will support peak throughputs in the range of 100-200 Mbit/s. Here is some of the Architecture in the network of WLAN wireless. Stations All components that can connect into a wireless medium in a network are referred to as stations.

All stations are equipped with wireless network interface cards (WNICs). Wireless stations fall into one of two categories: access points, and clients. Access points (APs) are base stations for the wireless network. They transmit and receive radio frequencies for wireless enabled devices to communicate with. Wireless clients can be mobile devices such as laptops, personal digital assistants, IP phones, or fixed devices such as desktops and workstations that are equipped with a wireless network interface. Basic service set The basic service set (BSS) is a set of all stations that can communicate with each other.

There are two types of BSS: Independent BSS (also referred to as IBSS), and infrastructure BSS. Every BSS has an identification (ID) called the BSSID, which is the MAC address of the access point servicing the BSS. An independent BSS (IBSS) is an ad-hoc network that contains no access points, which means they can not connect to any other basic service set. An infrastructure BSS can communicate with other stations not in the same basic service set by communicating through access points.