

ESTABLISHING CAMPUS AREA NETWORKING (CAN) USING A COMBINATION OF WIRELESS AND WIRED CONNECTIVITY – AN OPTIMUM SOLUTION

***R. Ganesan and C.R. Girija**

Rajiv Gandhi Institute of Veterinary Education and Research, Puducherry, India

Email: ashwinarvind@sify.com (**Corresponding Author*)

Abstract: Computer networking is undergoing drastic transformation in response to end users' need for mobility and connectivity while exchanging information among computers. There are two basic ways by which a computer network can be established - "wired" using Ethernet cables or "wireless" using radio waves, also known as "Wi-Fi" - Wireless Fidelity. The technology of wireless connectivity has come of age, and is now a viable, low cost alternative to the traditional wired technologies. Wireless technology gives users the mobility to move around within a reasonably broad coverage area and still be connected to the network. Most wireless local area networks (WLANs) today use the 2.4-gigahertz (GHz) or 5 GHz frequency band, the only portion of the radio frequency (RF) spectrum reserved around the world for unlicensed devices. The freedom and flexibility of wireless networking can be applied both within buildings and between buildings. In many places, combination of wired and wireless technology is used to meet all the networking needs. As the market for WLAN is continuously increasing, this paper discusses an overview of wireless technology and also how the Campus Area Network (CAN) has been optimally established using a combination of wired and wireless technology connecting computers located in nine buildings within the campus of 1 km radius.

Keywords: Wireless networking, Wi-Fi, Wired communication, RF, Campus area networking.

1. INTRODUCTION

In many offices today, computers communicate with each other and with printers and other devices in a Local Area Network (LAN) by sending information along wires. Wireless networking (Wi-Fi) allows computers and peripherals to communicate using radio frequency (RF) transmissions rather than over conventional network cabling. Using wireless network adaptors, any device capable of being used on a regular computer network can be accessed over a wireless connection for tasks ranging from file and printer sharing to multimedia and Internet access. Wireless technology utilizes the license-free radio frequency bands around the 2.4GHz and/or 5GHz ranges. The wireless LAN allows users to operate their computers

anywhere in the network area, such as an office building or University campus.

The popularity of wireless LAN is a testament primarily to their implementation convenience, mobility, productivity, cost efficiency, expandability and ease of integration with other networks. The majority of computers sold today come pre-equipped with all necessary wireless LAN technology. Applying wireless LAN technology to desktop systems provides an organization with flexibility impossible with a traditional LAN. Desktop client systems can be located in places where running cable is impractical or impossible. Desktop PCs can be redeployed anywhere within a facility as frequently as needed, making wireless networks ideal for temporary workgroups and fast-growing organizations.

2. TECHNOLOGY REVIEW

2.1 Wireless networking hardware

There are several kinds of hardware that may be used to implement a wireless network. However, primary components include Wireless Network card, Wireless Access Point, Wireless Antenna and Wireless Router.

A wireless network card is required on each device on a wireless network. A laptop usually has an expansion (PCMCIA) slot which the network card would fit in to. A desktop computer would need an internal PCI wireless network card or an USB wireless network card which will usually have a small antenna on it. The wireless card translates data into a radio signal and transmits it using an antenna as per the defined communication wireless standards and vice versa.

Access points (AP) are base stations for the wireless network. They transmit and receive (transceiver) radio frequencies for wireless enabled devices to communicate. A wireless access point can be used to join wireless devices to a wired network, or to extend the range of a wireless network.

Wireless antenna may be required to either extend the broadcast range of an access point or to increase the range from which a wireless network adapter can receive a signal. Different types of wireless antennas are available which can be used for different situations. An Omni-directional antenna radiates horizontally all around and the directional antenna radiates horizontally in a particular direction.

Wireless router connects networked devices to other networks or to the Internet.

2.2 Wi-Fi Mode

There are two modes in which Wi-Fi can be set up. In an *ad-hoc* mode, two or more PCs with wireless network cards can communicate among themselves. In the *infrastructure mode*, the wireless enabled devices communicate through an access point which acts like a hub. This mode is useful if the wireless enabled devices need to access some wired network resources.

The access point can be configured as a bridge in the *point to point mode* to establish wireless network for connecting two buildings. Here one AP communicates directly to another AP. No other wireless enabled device can access this transmission. If the AP's in the two buildings are set to Point to Point mode, and the Media Access Control (MAC) address of each access point is entered in the other access point and a directional antenna used in the two building tops, then the wireless connectivity can be established between the two buildings. Similarly, the access point can also be configured as a bridge in the *point to multi point mode* to establish wireless connectivity for connecting many buildings.

2.3 Wi-Fi Standards

The communication protocols for wireless networking are defined by the *Institute of Electrical and Electronics Engineers* (IEEE) as follows.

<u>Wireless Standard</u>	<u>Data Transfer Rate</u>	<u>Frequency Band</u>
802.11 b	Up to 11 Mbps	2.4 GHz
802.11 a	Up to 54 Mbps	5.0 GHz
802.11 g	Up to 54 Mbps	2.4 GHz
802.11 n	Up to 300 Mbps	2.4 & 5 GHz

All the wireless network hardware needed for establishing the connectivity has to be compatible with the wireless standard chosen to establish the network.

2.4 Security

The most widely deployed security solution for wireless networks is **WEP / WEP2** (Wired Equivalent Privacy), which encrypts data sent over the network. WEP is a form of encryption that is similar to SSL (secure socket layer), which is used to secure Web browser sessions. The cryptological algorithm used by WEP is a very strong 64 / 128 bit password key encryption. A more advanced form of protection is **WPA / WPA2** (Wi-Fi Protected Access), which provides individual user authentication as well as more secure 128 / 192 / 256 bit encryption. This also supports an 8 – 63 character long passphrase or Pre Shared Key (PSK). Some more additional safety measures can be implemented to secure the wireless

network like changing the admin passwords for access points, disabling SSID (Service Set Identifier) broadcast, turning on WEP / WPA encryption, using of a longer passphrase (PSK), enabling MAC address filtering, ensuring that access points are placed securely (e.g. in the center of a room / office to minimise its signal strength outside the office), disabling wireless access to the configuration page of the access point and avoiding interference by choosing non-overlapping channels 1, 6 or 11.

2.5 Other Wireless Technologies

Bluetooth is a wireless protocol designed to connect computers to gadgets such as mobile phones and PDAs. The range of Bluetooth is only about 10m and the data rate is a mere 723Kbps, making it virtually unusable except for small file transfers. **Infrared** is another wireless protocol known as IrDA (Infrared Data Association). Many notebook computers are equipped with IrDA wireless adaptors, and these allow simple file transfers between nearby computers as well as the downloading of photos from digital cameras. USB IrDA adaptors are also available. The IrDA protocol is rated at 4Mbps with a high-speed version called VFIR rated at 16Mbps. **WiMAX** (Worldwide Interoperability for Microwave Access) is designed for high data transfer rate and long-range wireless networking (spanning miles). It is based on IEEE 802.16 standard and has the potential to take wireless broadband internet to very far off places, even to remote villages.

3. OBJECTIVES

To establish a secure and flexible network of the entire systems located in the nine buildings (situated within a radius of 1 km) inside the campus in a cost effective manner for Internet Connection Sharing, File Sharing, Hardware Resource Sharing and Intranet applications.

4. BACKGROUND

There were 9 main buildings in the college campus which were to be networked namely “ADMIN”, “AHE”, “VBC”, “LPT”, “VAN”, “VMC”, “ECELL”, “LIB” & “FARM”. Each building was having several computers. Within each building, the PC’s were located in different floors with lot of obstruction (walls and other laboratory equipments). Also, between buildings, there were many trees, concrete and metal road crossings. The college computer center, located in the Admin building, was having a high speed internet connection and was shared by all the computers in the computer center.

5. CHOICE OF TECHNOLOGY FOR THE NETWORK

As wired connectivity using fiber optic cabling / UTP cabling connecting buildings would be very expensive and / or difficult / not possible to implement in the given situation and also since the line of sight from the building tops was very good for many buildings, it was decided to use **wireless technology to establish connectivity among buildings using IEEE 802.11 g standards at 54 Mbps**. And since, already a wired LAN existed in the main college computer center and the other PC's in the remaining 8 buildings are located in different floors in each building with lot of obstructions, it was decided to use **wired technology using Ethernet to establish connectivity within all buildings** instead of wireless connectivity as the later would be more expensive and less powerful than the former. It was also decided to use **point to multi point bridging** mode to establish wireless connectivity among the nine buildings. Thus a **combination of wired and wireless network plan** was our choice of technology for establishing the campus area networking.

As the distance between the buildings is more than the range of the access point, it was decided to use an omni directional antenna at the base station and directional antennas in the client stations. It was decided to position the access points indoors in the top floor of each building but as close as possible to the wireless antenna kept outdoors in each building to minimize the length of RF cable to be used connecting the antenna and the access point. As electric power outlets were not available for the access point because of its location in each building, Power over Ethernet (POE) was used to power the access points through the UTP cable connecting the switch and the access point. Appropriate pigtail cables, RF cables, Cat 5 UTP cables and connectors were used while establishing the network.

6. IMPLEMENTATION

The following hardware was procured to implement the solution.

Item	Quantity
1. Omni-directional antenna (13 dBi, 2.4 GHz)	2 nos.
2. Directional antenna (13 dBi, 2.4 GHz)	8 nos.
3. Access Points (128 bit encryption)	10 nos.
4. Power over Ethernet	10 nos.
5. RF Cable	50 mtrs.
6. CAT 5 UTP cable	900 mtrs.

7. Pig tail cables	20 cables (1 mtr.)
8. Switch (8 port)	8 nos.
9. RF connectors	20 nos.

A line of sight survey was done from the building tops. As it was difficult to get a very good line of sight of all buildings from the top of Admin Block, it was decided to implement the wireless connectivity of nine buildings in two segments and bridge the two segments to establish the full connectivity. So, based on this survey, it was decided that the **Admin block** would act as the **first base station** with AHE, VBC, LPT and VAN acting as the client stations of the first base station and the **VAN building** acting as the **second base station** with VMC, ECELL, LIB and FARM as the client stations of the second base station (Fig.1). In the Admin building one Omni antenna was used (Fig. 2). In the VAN building, two access points and two antennas' (one directional – which receives the signals from the Admin building and one Omni directional – which relays signals to its client stations have been bridged) (Fig. 3). In each building, UTP cable runs from the access point to a switch and from the switch, connection is established to all PC's located in various departments within that building. Directional antenna is used in all client locations (Fig. 4). All the access points were properly configured to establish the connectivity. While configuring the access points, the MAC address of the client access points were set in the base access point. Similarly, in the client access point, the MAC address of its base is set. This ensured that no roaming wireless device got connection to our wireless network. Also all the access points were disabled from broadcasting their network name or SSID. All other security settings were properly implemented. The speed of the network was tested by transferring huge files across departments which were found to be satisfactory. All the systems located in the various building have been configured to share the single broadband internet connection. Thus the network of connecting all computers located in the nine buildings was well established using wireless and wired connectivity.

7. CONCLUSION

In this paper, it is presented how the campus area network can be established optimally using wired and wireless technology. Both wired and wireless are great ways to network. When it comes to wired network, speed, reliability and security are its major strengths while implementation, maintenance and overall cost are its limitations. But when it

comes to wireless network, implementation, mobility and overall cost are its strengths while performance and security still needs some improvement. Wireless LAN has redefined what it means to be connected. It has stretched the boundaries of the local area computer network. It makes an infrastructure as dynamic as it needs to be. With standard and interoperable wireless networking products, LANs can reach scales unimaginable with a wired infrastructure. They can make high-speed interconnections for a fraction of the cost of traditional wide area technologies.

Finally, the best network plan is always based on the specific situation and needs and often it may be beneficial to combine both wireless and wired technology to establish a campus area networking.

ACKNOWLEDMENT

Authors are thankful to the Dean of the College for sanctioning financial support for executing this project. Authors are also thankful to the National Informatics Center, Puducherry, India for their technical inputs.

REFERENCES

- [1] Andrew Z.Tabona (2005). An Overview of Wireless Network Security.
http://www.windowsnetworking.com/articles_tutorials/Wireless-Networking-questions-answered.html
- [2] Andrew Z.Tabona (2004). An Introduction to Wireless Networking (Part 2) - Requirements and Setup.
http://www.windowsnetworking.com/articles_tutorials/Introduction-Wireless-Networking-Part2.html
- [3] Sylvia Chorp (2002). Wireless vs. Hard-Wired Network Use in Education
<http://www.thejournal.com/articles/16161>
- [4] http://en.wikipedia.org/wiki/Wireless_network

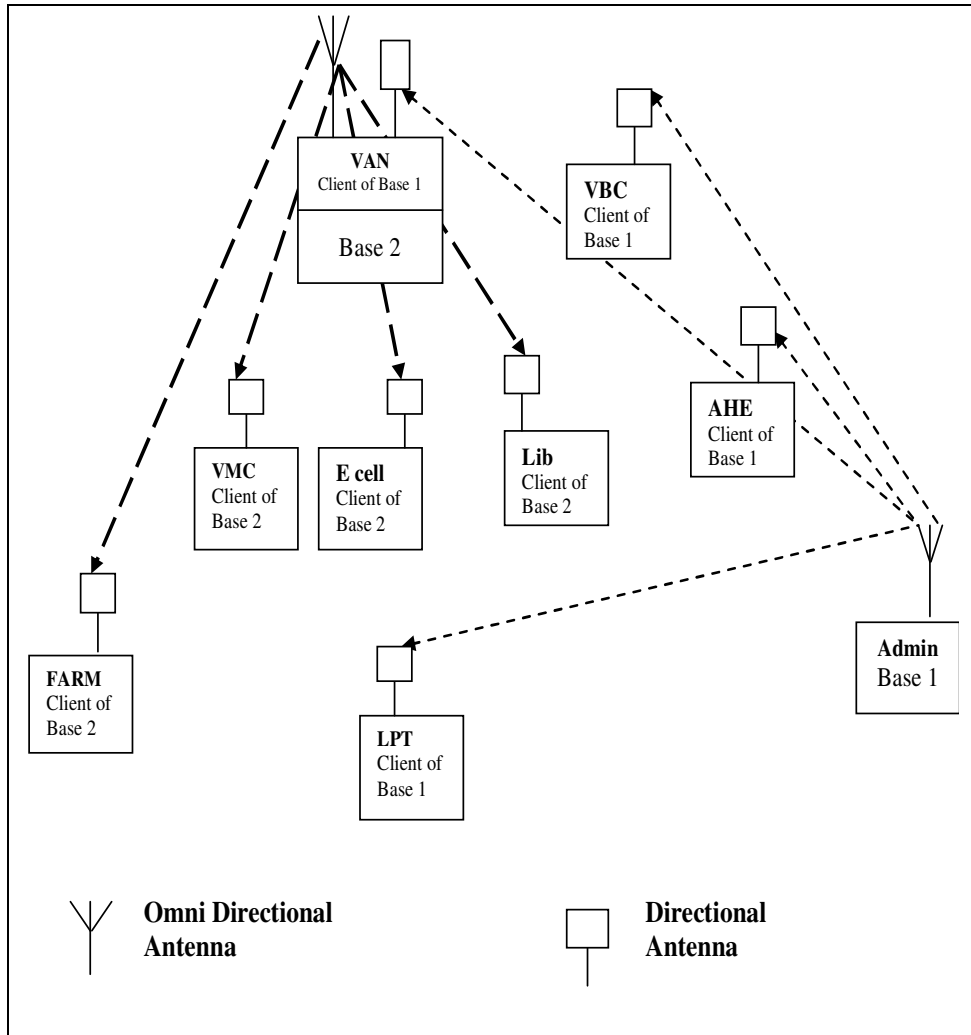


Fig. 1. Schematic diagram of the wireless connectivity among buildings

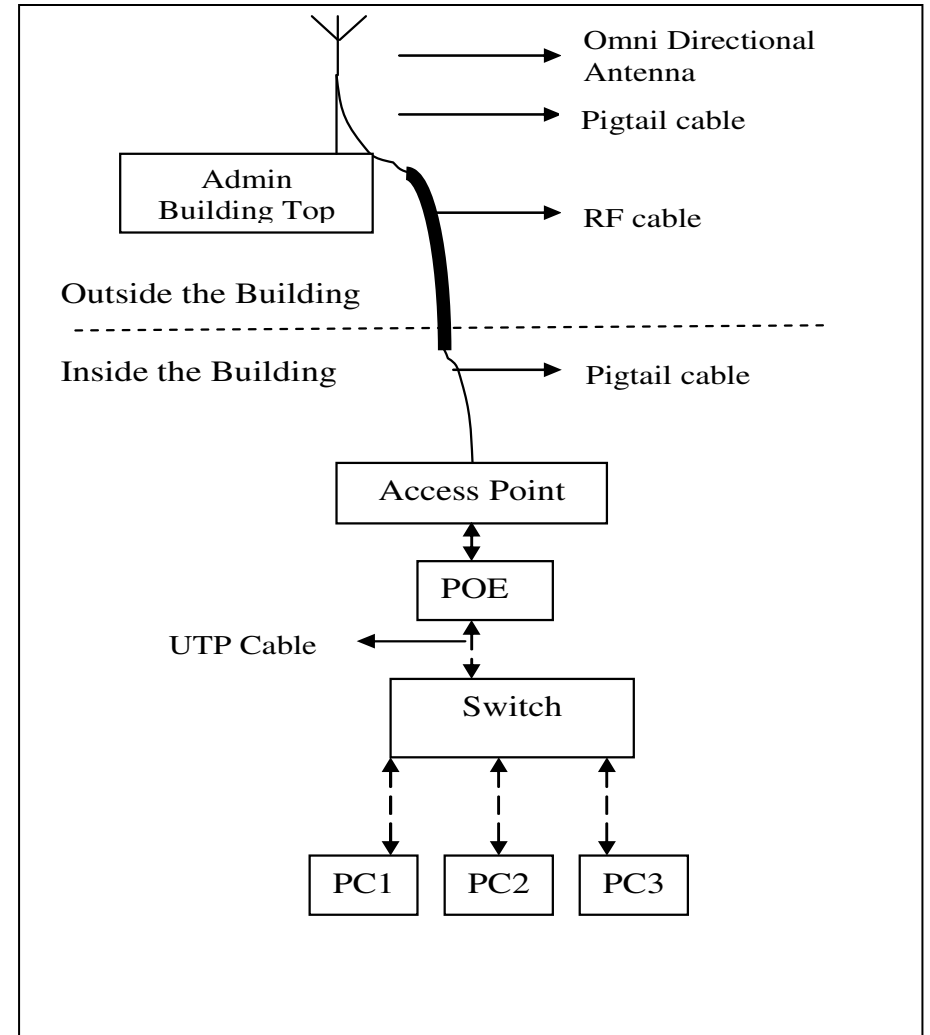


Fig. 2. Schematic diagram of the connectivity in the Admin building (First Base Station)

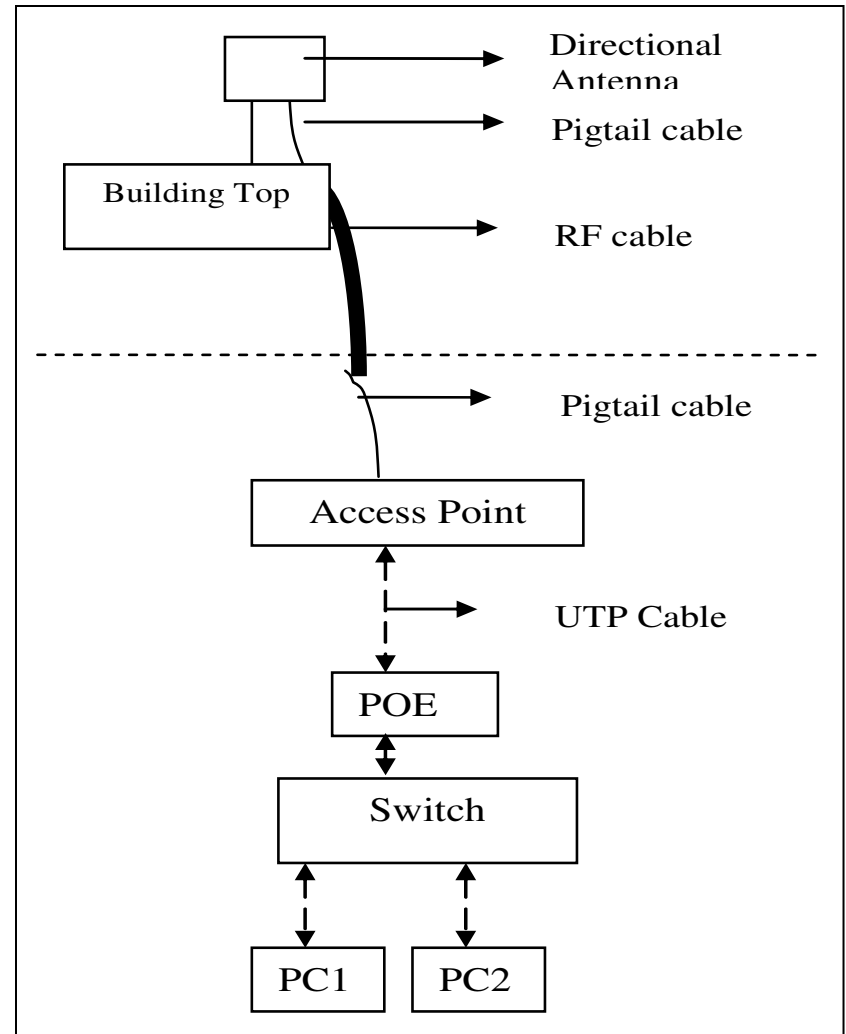
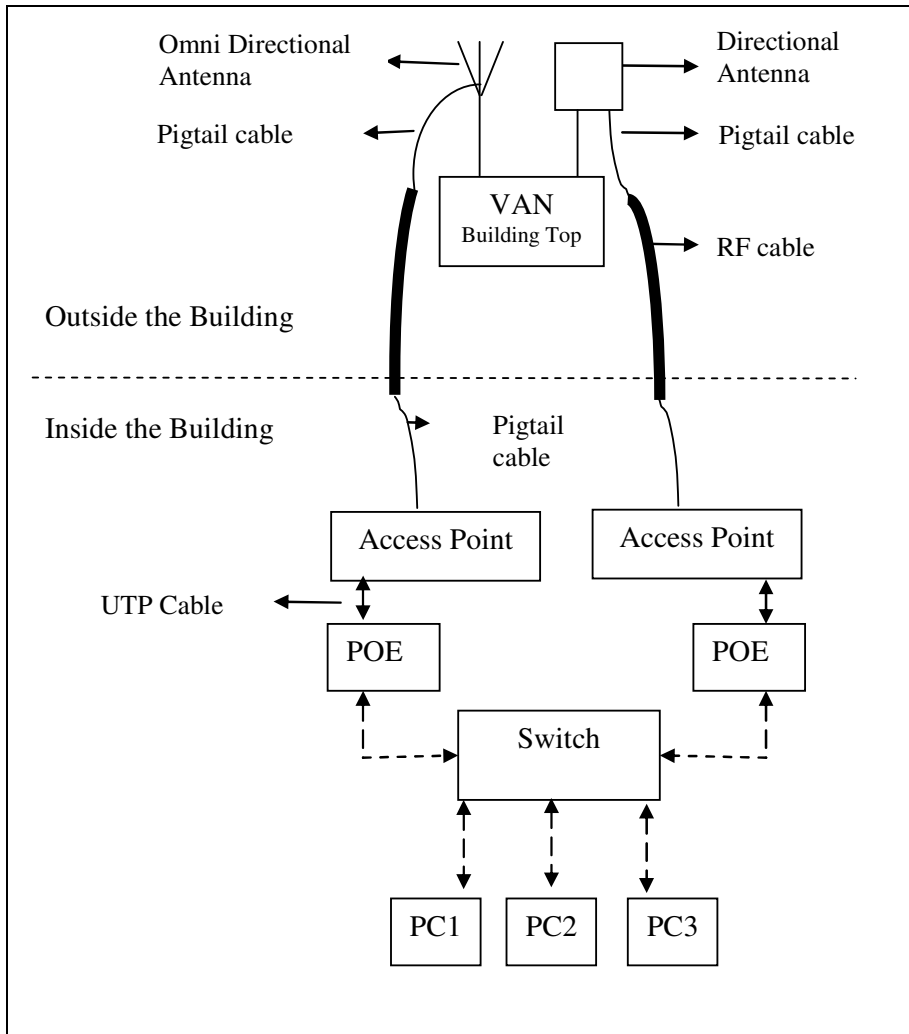


Fig. 3. Schematic diagram of the connectivity in the VAN building (Second Base Station)

Fig. 4. Schematic diagram of the connectivity in all client locations