Wireless Network Connections Policies & Standards

Atul M. Gonsai

Nilesh N Soni

N N Jani

Abstract

This paper presents wireless networking scenario with standards & policies for its implementation. Wireless LAN is needed requirement for the organizations & institutions for unlimited access to their wired LAN. This WLAN set up provides Internet access too. Internet & WLAN access needs security to protect data. The paper also discusses security aspect of WLAN; cost consideration, different types of network setup for different need. The paper's focus is WLAN & Internet connectivity & its implementation. The benefited group for this paper is network administrators & management people of any organization.

Keyword : Wireless Network, Access Point, Wireless Security, Wireless Adapter Card, Network

0. Introduction

The term wireless networking refers to technology that enables two or more computers to communicate using standard network protocols, but without network cabling. Strictly speaking, any technology that does this could be called wireless networking. The current buzzword however generally refers to wireless LANs.[1] This technology, fuelled by the emergence of cross-vendor industry standards such as IEEE 802.11, has produced a number of affordable wireless solutions that are growing in popularity with business and schools as well as sophisticated applications where network wiring is impossible, such as in warehousing or point-of-sale handheld equipment.

1. Components of Wireless Network

There are two kinds of wireless networks:

1. An ad-hoc or peer-to-peer wireless network consists of a number of computers each equipped with a wireless networking interface card. Each computer can communicate directly with all of the other wireless enabled computers. They can share files and printers this way, but may not be able to access wired LAN resources, unless one of the computers acts as a bridge to the wired LAN using special software. This is called "bridging". [2]

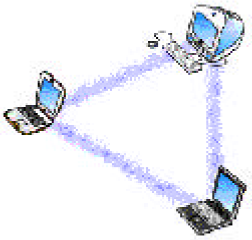


Figure 1: Ad-Hoc or Peer-to Peer Networking.

Each computer with a wireless interface can communicate directly with all of the others.

2. A wireless network can also use an access point, or base station. In this type of network the access point acts like a hub, providing connectivity for the wireless computers. It can connect (or “bridge”) the wireless LAN to a wired LAN, allowing wireless computer access to LAN resources, such as file servers or existing Internet Connectivity.

There are two types of access points:

✍ Dedicated hardware access points (HAP) such as Lucent’s Wave LAN, Apple’s Airport Base Station or Web Gear’s Aviator PRO. The Figure 2 shows Hardware access points offer comprehensive support of most wireless features.

Wireless connected computers using a Hardware Access Point.

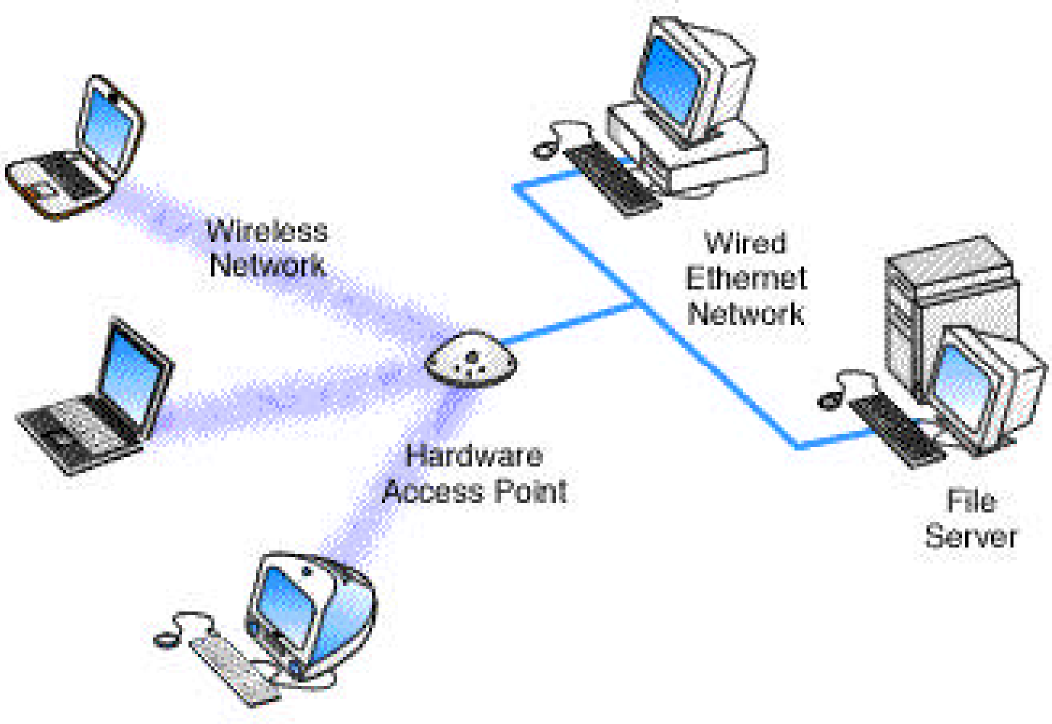


Figure 2: Hardware Access Point.

- ✍ Software Access Points which run on a computer equipped with a wireless network interface card as used in an ad-hoc or peer-to-peer wireless network which is shown in Figure 3. The Vicomsoft Internet Gateway suites are software routers that can be used as a basic Software Access Point, and include features not commonly found in hardware solutions, such as Direct PPPoE support and extensive configuration flexibility, but may not offer the full range of wireless features defined in the 802.11 standard. With appropriate networking software support, users on the wireless LAN can share files and printers located on the wired LAN and vice versa.

Wireless connected computers using a Software Access Point.

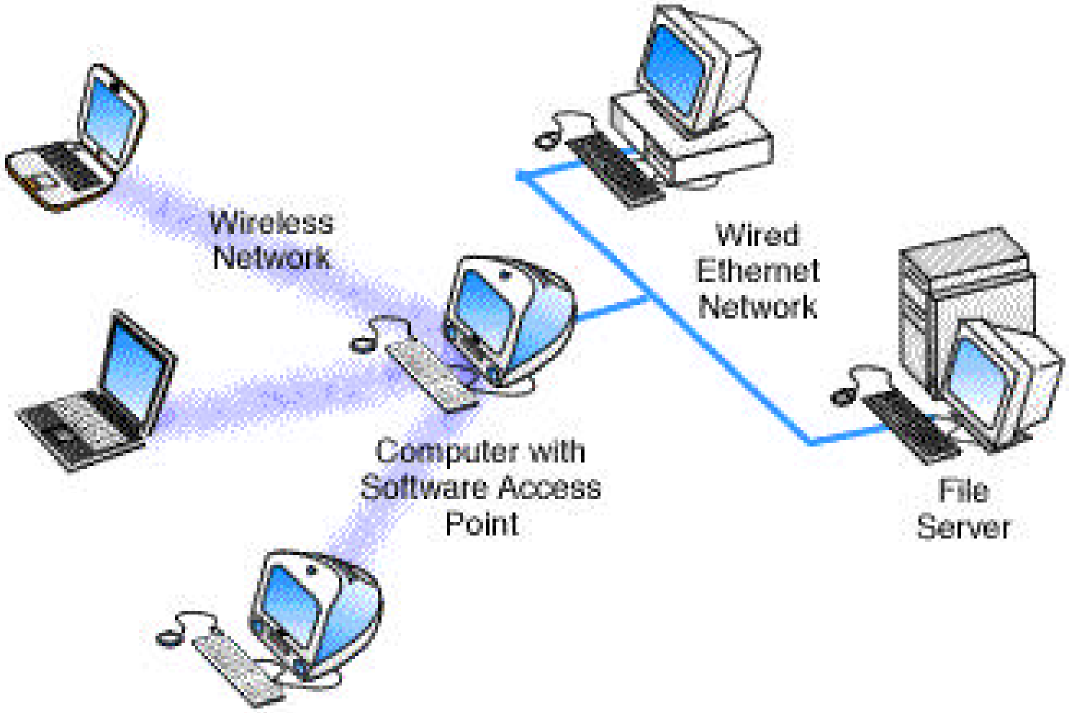
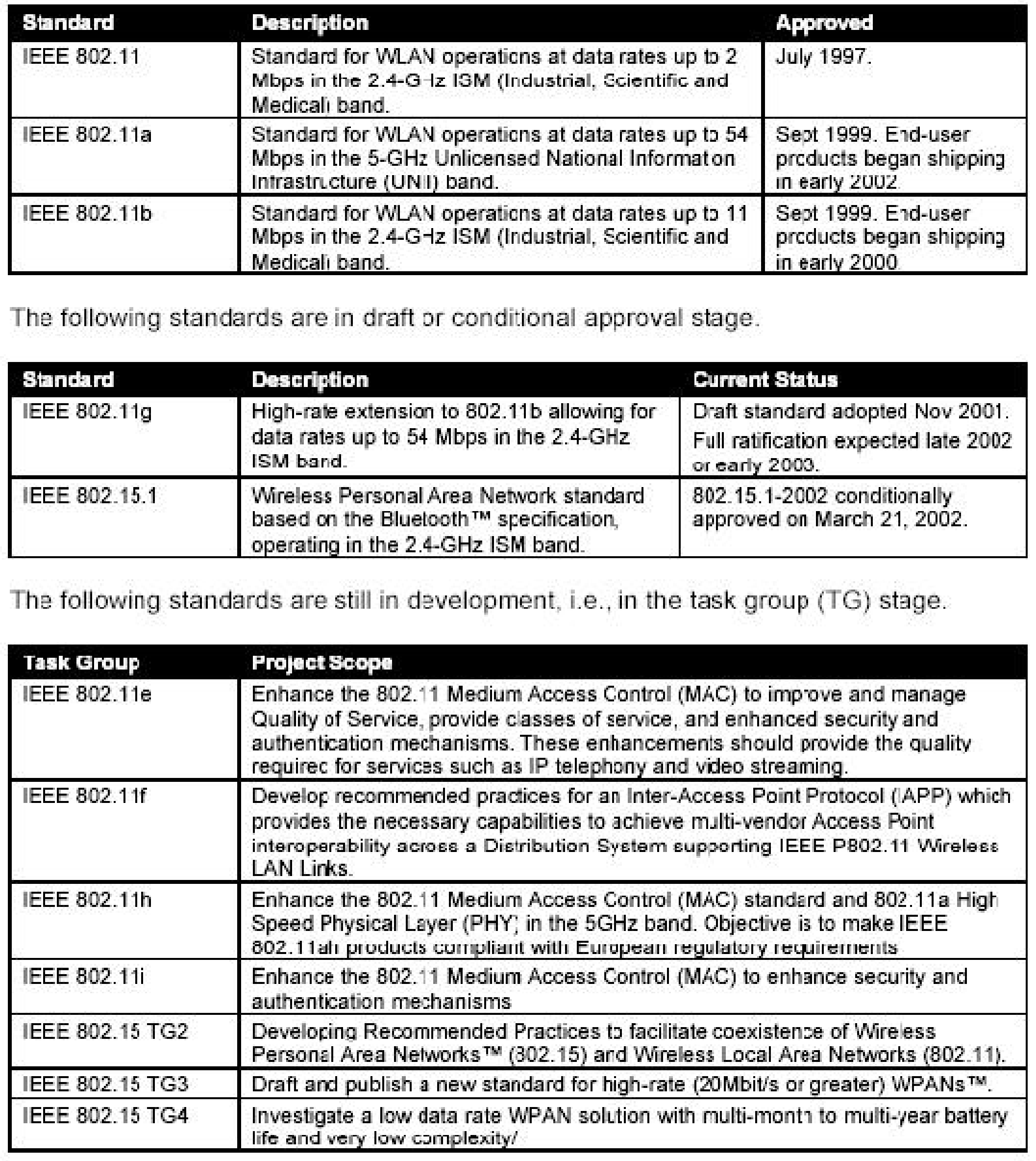


Figure 3: Software Access Point.

2. IEEE 802.11 Wireless standards

Wireless networking hardware requires the use of underlying technology that deals with radio frequencies as well as data transmission. The most widely used standard is 802.11 produced by the Institute of Electrical and Electronic Engineers (IEEE). [5] This is a standard defining all aspects of Radio Frequency Wireless networking. [6]

The following standards are approved:



Standard	Description	Approved
IEEE 802.11	Standard for WLAN operations at data rates up to 2 Mbps in the 2.4-GHz ISM (Industrial, Scientific and Medical) band.	July 1997.
IEEE 802.11a	Standard for WLAN operations at data rates up to 54 Mbps in the 5-GHz Unlicensed National Information Infrastructure (UNII) band.	Sept 1999. End-user products began shipping in early 2002.
IEEE 802.11b	Standard for WLAN operations at data rates up to 11 Mbps in the 2.4-GHz ISM (Industrial, Scientific and Medical) band.	Sept 1999. End-user products began shipping in early 2000.

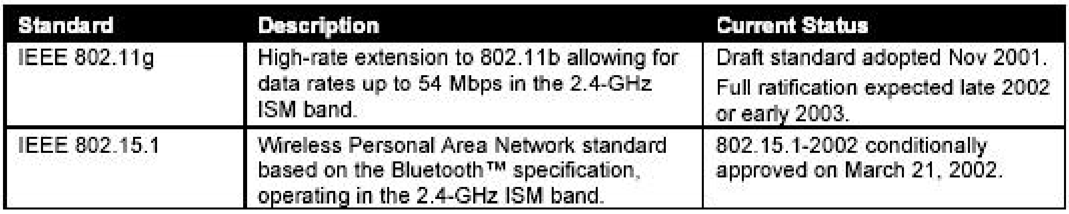
The following standards are in draft or conditional approval stage.

Standard	Description	Current Status
IEEE 802.11g	High-rate extension to 802.11b allowing for data rates up to 54 Mbps in the 2.4-GHz ISM band.	Draft standard adopted Nov 2001. Full ratification expected late 2002 or early 2003.
IEEE 802.15.1	Wireless Personal Area Network standard based on the Bluetooth™ specification, operating in the 2.4-GHz ISM band.	802.15.1-2002 conditionally approved on March 21, 2002.

The following standards are still in development, i.e., in the task group (TG) stage.

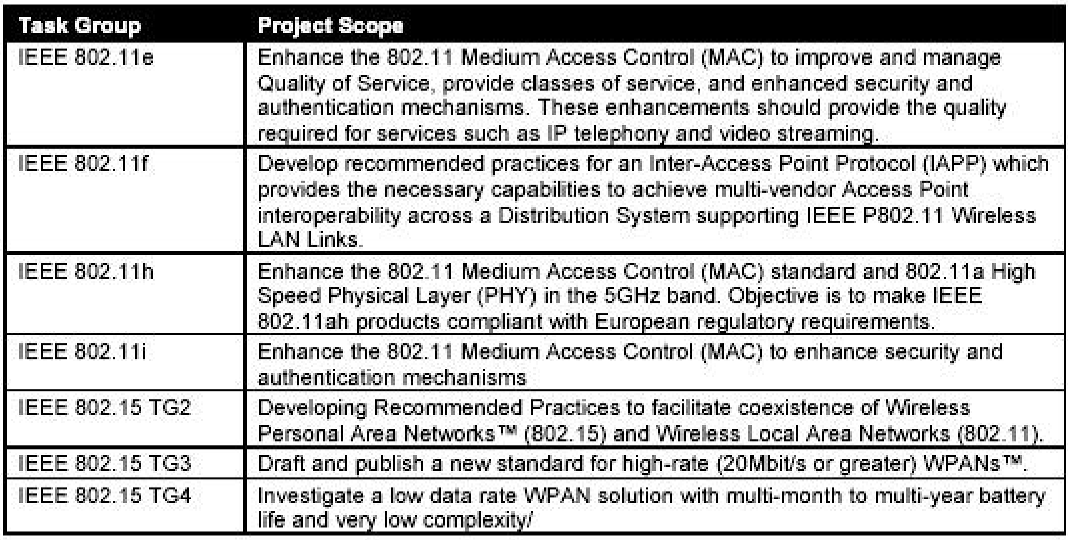
Task Group	Project Scope
IEEE 802.11e	Enhance the 802.11 Medium Access Control (MAC) to improve and manage Quality of Service, provide classes of service, and enhanced security and authentication mechanisms. These enhancements should provide the quality required for services such as IP telephony and video streaming.
IEEE 802.11f	Develop recommended practices for an Inter-Access Point Protocol (IAPP) which provides the necessary capabilities to achieve multi-vendor Access Point interoperability across a Distribution System supporting IEEE P802.11 Wireless LAN Links.
IEEE 802.11h	Enhance the 802.11 Medium Access Control (MAC) standard and 802.11a High Speed Physical Layer (PHY) in the 5GHz band. Objective is to make IEEE 802.11ah products compliant with European regulatory requirements
IEEE 802.11i	Enhance the 802.11 Medium Access Control (MAC) to enhance security and authentication mechanisms
IEEE 802.15 TG2	Developing Recommended Practices to facilitate coexistence of Wireless Personal Area Networks™ (802.15) and Wireless Local Area Networks (802.11).
IEEE 802.15 TG3	Draft and publish a new standard for high-rate (20Mbit/s or greater) WPANs™.
IEEE 802.15 TG4	Investigate a low data rate WPAN solution with multi-month to multi-year battery life and very low complexity/

The following standards are in draft or conditional approval stage.



Standard	Description	Current Status
IEEE 802.11g	High-rate extension to 802.11b allowing for data rates up to 54 Mbps in the 2.4-GHz ISM band.	Draft standard adopted Nov 2001. Full ratification expected late 2002 or early 2003.
IEEE 802.15.1	Wireless Personal Area Network standard based on the Bluetooth™ specification, operating in the 2.4-GHz ISM band.	802.15.1-2002 conditionally approved on March 21, 2002.

The following standards are in still development, i.e. in the task group (tg) stage.



Task Group	Project Scope
IEEE 802.11e	Enhance the 802.11 Medium Access Control (MAC) to improve and manage Quality of Service, provide classes of service, and enhanced security and authentication mechanisms. These enhancements should provide the quality required for services such as IP telephony and video streaming.
IEEE 802.11f	Develop recommended practices for an Inter-Access Point Protocol (IAPP) which provides the necessary capabilities to achieve multi-vendor Access Point interoperability across a Distribution System supporting IEEE P802.11 Wireless LAN Links.
IEEE 802.11h	Enhance the 802.11 Medium Access Control (MAC) standard and 802.11a High Speed Physical Layer (PHY) in the 5GHz band. Objective is to make IEEE 802.11ah products compliant with European regulatory requirements.
IEEE 802.11i	Enhance the 802.11 Medium Access Control (MAC) to enhance security and authentication mechanisms
IEEE 802.15 TG2	Developing Recommended Practices to facilitate coexistence of Wireless Personal Area Networks™ (802.15) and Wireless Local Area Networks (802.11).
IEEE 802.15 TG3	Draft and publish a new standard for high-rate (20Mbit/s or greater) WPANs™.
IEEE 802.15 TG4	Investigate a low data rate WPAN solution with multi-month to multi-year battery life and very low complexity/

3. Interconnecting Wireless LAN with wired LAN

To do this we will need some sort of bridge between the wireless and wired network. This can be accomplished either with a hardware access point or a software access point. Hardware access points are available with various types of network interfaces, such as Ethernet or Token Ring, but typically require extra hardware to be purchased if our networking requirements change.

If networking requirements go beyond just interconnecting a wired network to a small wireless network, a software access point may be the best solution. A software access point does not limit the type or number of network interfaces you use. It may also allow considerable flexibility in providing access to different network types, such as different types of Ethernet, Wireless and Token Ring networks. Such connections are only limited by the number of slots or interfaces in the computer used for this task. [4]

4. Access points in wireless network

This depends upon the manufacturer. Some hardware access points have a recommended limit of 10, with other more expensive access points supporting up to 100 wireless connections. Using more computers than recommended will cause performance and reliability to suffer.

Software access points may also impose user limitations, but this depends upon the specific software, and the host computer's ability to process the required information.

4.1 More than one access point

Multiple access points can be connected to a wired LAN, or sometimes even to a second wireless LAN if the access point supports this. In most cases, separate access points are interconnected via a wired LAN, providing wireless connectivity in specific areas such as offices or classrooms, but connected to a main wired LAN for access to network resources, such as file servers as shown in Figure 4.

Wireless connected computers using Multiple Access Points.

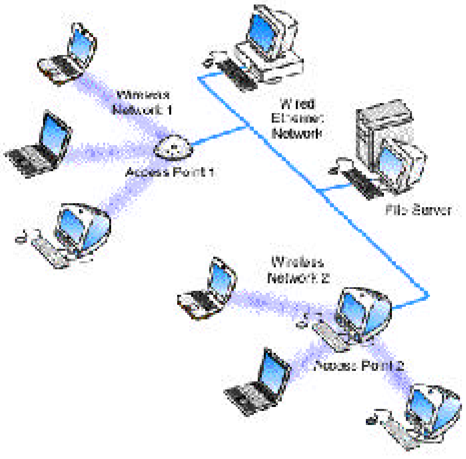


Figure 4: Multiple Access Points.

If a single area is too large to be covered by a single access point, then multiple access points or extension points can be used. The extension points are not defined in the wireless standard, but have been developed by some manufacturers. When using multiple access points, each access point wireless area should overlap its neighbors. This provides a seamless area for users to move around in using a feature called "roaming." Some manufacturers produce extension points, which act as wireless relays, extending the range of a single access point. Multiple extension points can be strung together to provide wireless access to far away locations from the central access point which is shown in Figure 5.Wireless connected computers using an Access Point with an Extension Point.

Wireless Connected Computers using an Access Point with an Extension Point

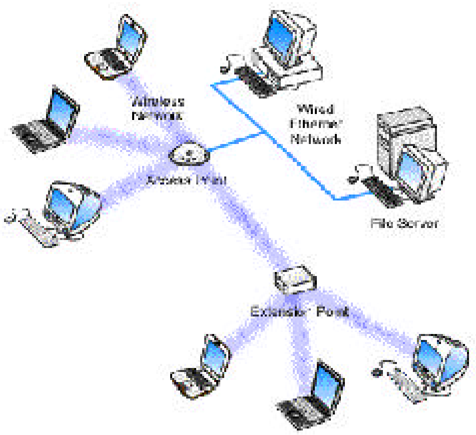


Figure 5: Extension Point.

4.1 Roaming

A wireless computer can “roam” from one access point to another, with the software and hardware maintaining a steady network connection by monitoring the signal strength from in-range access points and locking on to the one with the superior quality. [9] Usually this is completely transparent to the user; they are not aware that a different access point is being used from area to area. Some access point configurations require security authentication when swapping access points, usually in the form of a password dialog box. Access points are required to have overlapping wireless areas to achieve this as can be seen in the following diagram:

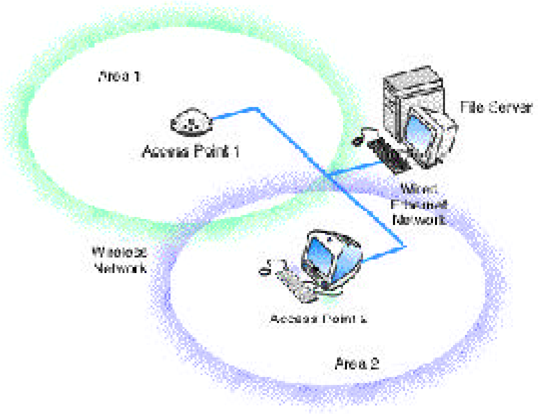


Figure 6: Roaming.

A user can move from Area 1 to Area 2 transparently. The Wireless networking hardware automatically swaps to the Access Point with the superior signal.

Not all access points are capable of being configured to support roaming. Also of note is that any access points for a single vendor should be used when implementing roaming, as there is no official standard for this feature.

5. Wireless Network to Interconnect Two LANs

Wireless networking offers a cost-effective solution to users with difficult physical installations such as campuses, hospitals or businesses with more than one location in immediate proximity but separated by public thoroughfare. This type of installation requires two access points. Each access point acts as a bridge or router connecting its own LAN to the wireless connection. The wireless connection allows the two access points to communicate with each other, and therefore interconnect the two LAN's.

A Hardware Access Point providing wireless connectivity to local computers and a software access point. The software access point provides Wired Ethernet network 2 computers access to Wired Network 1.

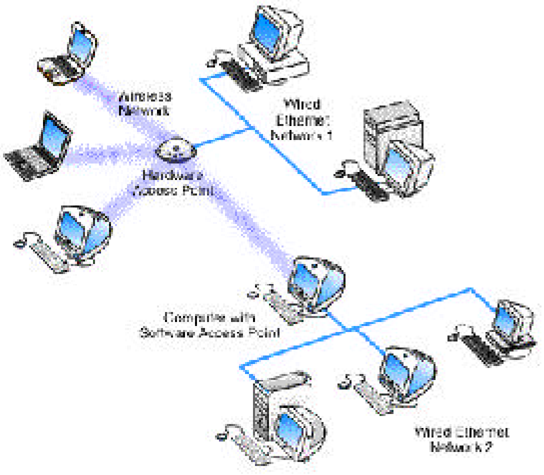


Figure 7: LAN to LAN Wireless Communications

Note that not all hardware access points have the ability to directly interconnect to another hardware access point, and that the subject of interconnecting LAN's over wireless connections is a large and complex one.

6. Security Scenario

Wireless communications obviously provide potential security issues, as an intruder does not need physical access to the traditional wired network in order to gain access to data communications. However, 802.11 wireless communications cannot be received —much less decoded— by simple scanners, short wave receivers etc. This has led to the common misconception that wireless communications cannot be eavesdropped at all. However, eavesdropping is possible using specialist equipment.

To protect against any potential security issues, 802.11 wireless communications have a function called WEP (Wired Equivalent Privacy), a form of encryption which provides privacy comparable to that of a traditional wired network. If the wireless network has information that should be secure then WEP should be used, ensuring the data is protected at traditional wired network levels. Also it should be noted that traditional Virtual Private Networking (VPN) techniques will work over wireless networks in the same way as traditional wired networks. [3]

A recent survey highlighted that 25% of organizations not using wireless LANs were held back by security concerns. No organization wishes a user to walk into the building and gain access to the private staff network or any module of the management system. Restrictions need to be made on who can access the network and from what access point or building. However, security provisions can be built into wireless LANs making them as secure as most standard LANs. [8]

6.1 Unauthorized access

Unauthorized users accessing network through the WLAN/LAN are a major security concern. We have to provide some mechanism, which will, denies unauthorized users access or limits their access to public network segments such as the Internet.

6.2 Unauthorized devices

Some devices, such as unauthorized laptops or PDAs, can leave you wide open to attack. It is needed to provide some mechanism to automatically discover any new devices on your network and immediately alerts to administrator.

7. Costing

Although running costs can be comparable to traditional wired networks, wireless transmission and reception equipment is generally much more expensive than the cost of comparable wired components. For Example the cost for DWL-520+ PCI Adapter and DWL 1000AP+ Access point of D-Link product is approximately Rs. 11500 and Rs. 18000 respectivelywhile many other wireless instruments are available in the market but the cost differs depending on the requirements and manufacturing company.[7]

7.1 Wireless Networking and the Internet

Once you realize that wireless cards are analogous to Ethernet cards and that empty space is analogous to Ethernet cabling, the answer to this question becomes clear. To share an Internet connection across a LAN you need two things:

- An Internet sharing hardware device or software program
- A LAN

If your LAN is wireless, the same criteria apply. You need hardware or software access point and a wireless LAN. Any computer equipped with a wireless network card running suitable Internet sharing software can be used as a software access point. (See Figure 8) A number of vendors offer hardware access points.

A hardware access point may provide Internet Sharing capabilities to Wired LAN computers, but does not usually provide much flexibility beyond very simple configurations. (See Figure 9)

Wireless connected computers using a Software Access Point for shared Internet access.

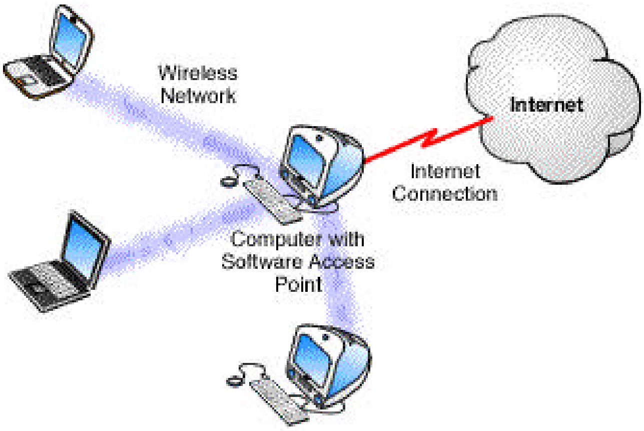


Figure 8: Software Access Point.

Wireless connected computers using a Hardware Access Point for shared Internet access.

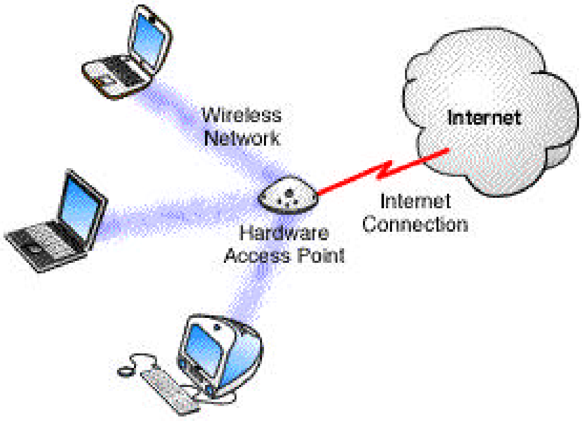


Figure 9: Hardware Access Point

If an existing wired LAN already has an Internet connection, then the hardware access points simply connect to your LAN and allow wireless computers to access the existing Internet connection in the same way as wired LAN computers.

Wireless connected computers using Multiple Access Points.

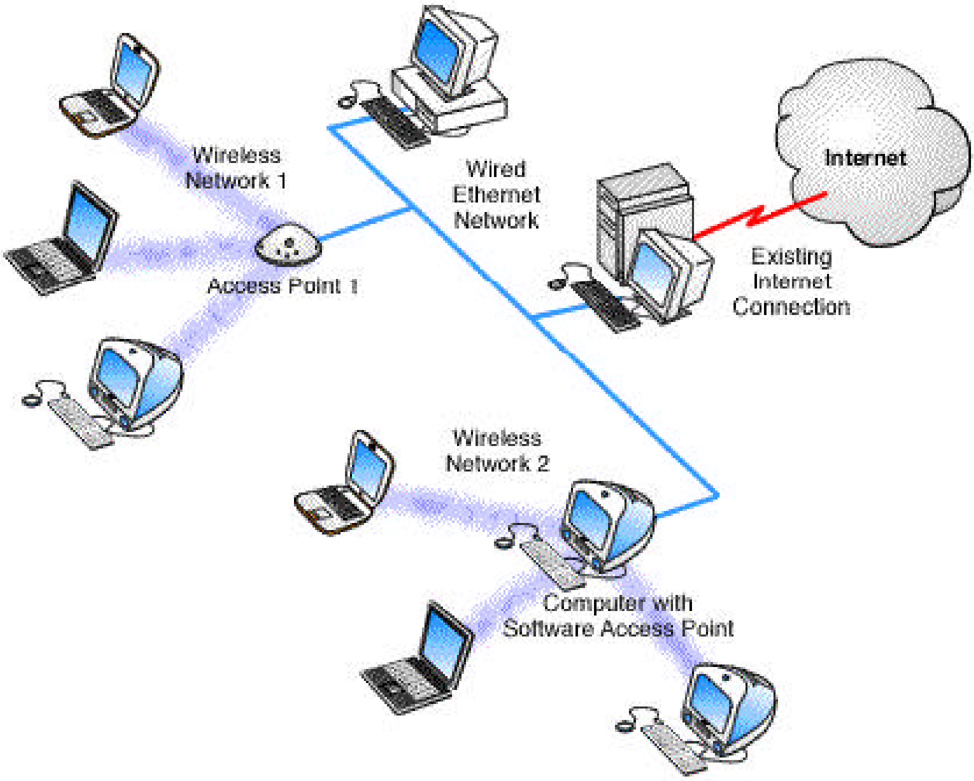


Figure 10: Multiple Access Points.

If there is no existing Internet connection, then this depends on the access point

Wireless connected computers using Multiple Access Points. All wired and wireless computers access the Internet through a single software access point.

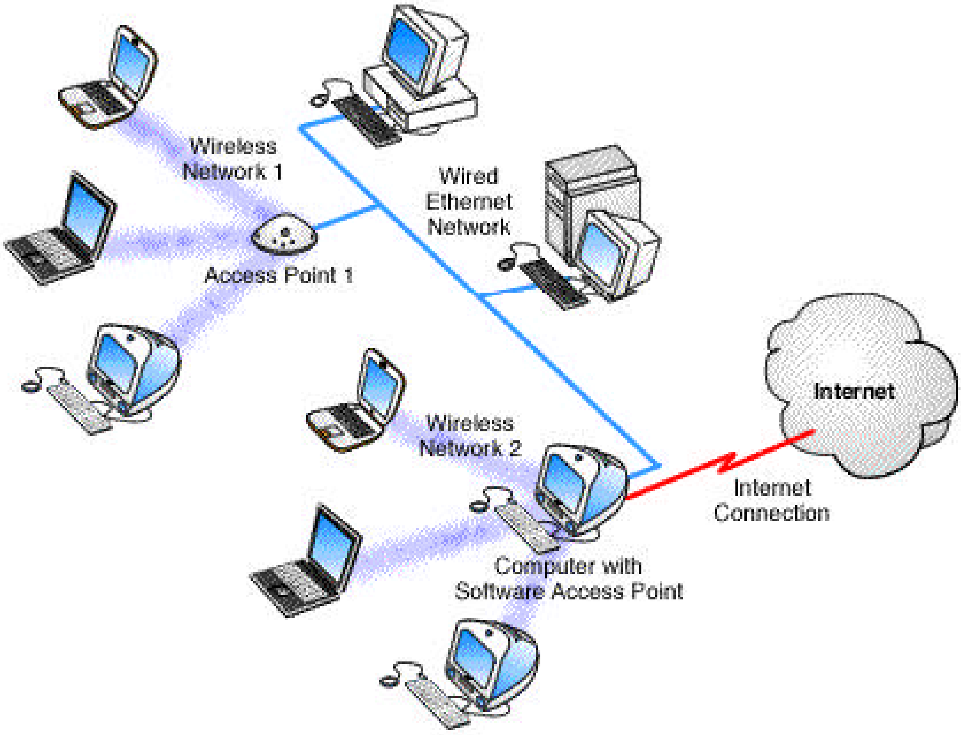


Figure 11: Software Access Point sharing one Internet connection.

If an access point provides some form of Internet sharing itself, then having multiple such access points connected to a wired LAN may require some special configuration, or possibly may require an additional Internet sharing device or software program.

8. Conclusion

The extension of the domain of the LAN and its integration with another network makes it convenient to adopt the technology of wireless LAN. This extension open ups an easy connectivity path towards hand held devices. Which is infecting the tomorrows need? Whatever is invested in network technology remains fruitful but an additional investment on wireless connectivity for internetworking and global connectivity creates an environment unconstraint information access even when an individual is on the move. A futuristic extension of sensors network willl also brings comparative ease. The modeled implementation is first step towards WLAN / LAN and Internet connectivity with considerable implementation of needed information security.

9. References

1. CSI Communications ISSN 0970-647x January-2004 page No.10-12
2. Wireless products and its applications www.winncom.com accessed on (15-5-2004)

3. IEEE 802.11b Wireless LANs http://www.wlana.com , www.3com.com Accessed on (20-5-2004)
4. Wirelesslan.com answer page, 2000. What is a Wireless LAN?http://www.wireless.com accessed on (19-4-2004)
5. IEEE standards. www.ieee.org accessed on (23-6-2004)
6. Stewart S. Miller (2003) Wi-Fi Security McGraw-Hill Companies, Inc.USA pp-75-80
7. For wireless products www.dlink-india.com Accessed on (18-11-2004)
8. Still secures A Guide to Wireless Network Security http://www.stillsecure.com Accessed on (21-1-2004)
9. Eric Ouellet, Robert Padjen (2002) Building a Cisco Wireless LAN Syngress Publishing, Inc. USA pp- 69-81, 183-185

About Authors

Mr. Atul Gonsaihas completed his Graduation in Bachelor of Business Administration (BBA) and Master degree in Master of Computer Applications (MCA) then recently in completed his Ph.D thesis work in Computer Networking. He is working as Assistant Professor in Department of Computer Science Saurashtra University Rajkot after completing his MCA from the same Institute in April 2000. He has written 13 research paper and 3 paper submitted for conference for acceptance. His research interest encompasses performance tuning of computer networks, wireless networks, High performance networking etc. He has taken part in 9 national and 3 international conferences and seminars. He is DCNI D – link Certified Network Integrator from D-link India Goa. He has published one book and is also writing one book on Computer Networking, which is not yet published. He is maintaining and handling MCA computer Labs and Saurashtra University Library Networking. He is life Member of ISTE New Delhi.
Email : atulgosai@yahoo.com or amgosai@sauuni.ernet.in

Dr. N N Jani is currently acting as Prof. & Head, Department of Computer science, Saurashtra university Rajkot. He obtained his masters degree of MSc then Ph.D in the area of material science. He has 60+ research contributions to his credit along with 10 books. He is currently guiding research scholar leading to Ph.D degree in the area of High performance networking, High performance, Biometric technology, data ware housing, data mining application and web services applications. His current research is on Embedded systems, MEMS and in near future in the area of nanotechnology.
Email : nnjani@sauuni.ernet.in

Mr. Nilesh N Soni has completed his Graduation in Bachelor of Commerce and also Library & Information Sc. with Master degree in 1992. He is working as I/c University Librarian, Saurashtra University Library Rajkot. He has written 7-research paper and 1 paper submitted for international conference for acceptance. His research interest encompasses computerization of Library, Digitization of Library Collection, networks, wireless networks etc. he has already computerized Nirma and Saurashtra university library. He has taken part in 5 national and international conference and seminars. He is life member of ISTE – New Delhi, ILA- New Delhi, Gandhralaya Sewa Sangh- Gujarat. He is engaged in the project to create a database of Rajkot Library Networking**.**
Email : sulnilesh@yahoo.co.uk