



Wireless Networking Q&A

Increased use of laptop computers within the enterprise, and increase in worker mobility have fuelled the demand for wireless networks. Up until recently, wireless technology was a patchwork of incompatible systems from a variety of vendors. The technology was slow, expensive and reserved for mobile situations or hostile environments where cabling was impractical or impossible. With the maturing of industry standards and the deployment of lightweight wireless networking hardware across a broad market section, wireless technology has come of age.

We are presenting this KnowledgeShare in a Q&A (Questions and Answers) format that we hope will be useful. We are dealing with the subject on a general basis and so the information offered here should apply to most wireless networking devices. We welcome feedback and comments from any readers on the usefulness or content.

We are providing the best information available to us as of date of writing and intend to update it at frequent intervals as things change and/or more information becomes available. However we intend this KnowledgeShare as a guide only and recommend that users obtain specific information to determine applicability to their specific requirements. (This is another way of saying that we can't be held liable or responsible for the content).

What is Vicomssoft's Interest in Wireless Networking?

Vicomssoft does not sell wireless (or wired) networking interface hardware (NICs). Accordingly we are neutral on which NICs are used and whether wired or wireless technologies are used. In the course of its business Vicomssoft has acquired considerable knowledge in the area of wireless networking and wishes to share it.

This KnowledgeShare document addresses the main types of wireless networking today based on the IEEE 802.11 standard.

Questions are split into two sections; the first section is on general wireless networking, and the second aimed at users wishing to use wireless technology to provide access to the Internet.

Questions

Section One - Wireless Networking

1. What is wireless networking?
2. What is a wireless network made up of?
3. What is IEEE 802.11?
4. Can I mix wireless equipment from different vendors?
5. If my computer is connected to a wireless LAN, can it communicate with computers on a wired LAN as well?

Content of this page in its entirety is protected by US & UK Copyright
© 2002 Vicomssoft Ltd

Reproduction in electronic and written form is expressly forbidden without written permission.



6. What is the range of a wireless network?
7. How many wireless networked computers can use a single access point?
8. Can I have more than one access point?
9. What is Roaming?
10. How can I use a wireless network to interconnect two LANs?
11. Is it true that wireless networking is only good for laptop computers?
12. What about security?

Section Two - Wireless Networking and the Internet

13. How can I use a wireless network to share an Internet connection?
14. If I have more than one hardware access point, how can I share a single Internet connection?
15. If I use a wireless network to connect to the Internet does my ISP need a wireless network too?
16. Can networking software identify a wireless computer in the same way it can identify an ethernet computer on the network?

Answers

Section One - Wireless Networking

1. What is wireless networking?

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. 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.

2. What is a wireless network made up of?

There are two kinds of wireless networks:

a.

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")



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

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

b.

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:

i.

Dedicated hardware access points (HAP) such as Lucent's WaveLAN, Apple's Airport Base Station or WebGear's AviatorPRO. (See Figure 2). Hardware access points offer comprehensive support of most wireless features, but check your requirements carefully.

ii.

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. (See Figure 3) The Vicomssoft InterGate 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. Vicomsoft's solutions support file sharing using TCP/IP.

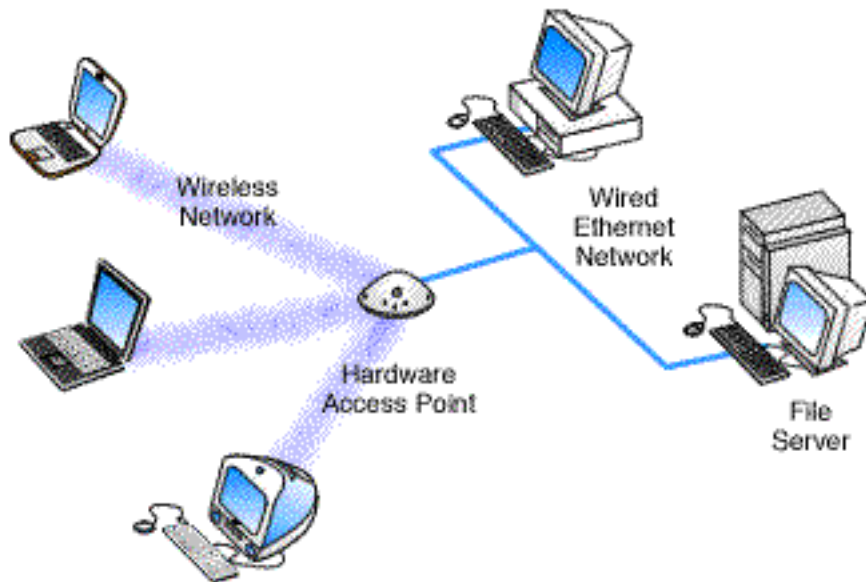


Figure 2: Hardware Access Point.

Wireless connected computers using a Hardware Access Point.

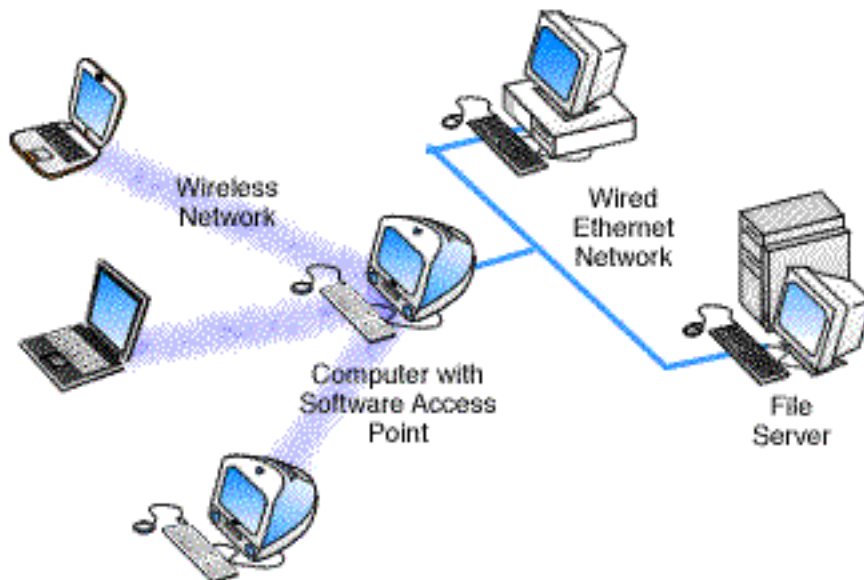


Figure 3: Software Access Point.

Wireless connected computers using a Software Access Point.



3.What is IEEE 802.11?

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). This is a standard defining all aspects of Radio Frequency Wireless networking.

4.Can I mix wireless equipment from different vendors?

Because most wireless networking hardware vendors support the 802.11 standard they can inter operate. However, we recommend verification as the standard is a fairly recent one, and does specify two different methods for wireless communications; Frequency Hopping (FH) and Direct Sequence Spread Spectrum (DSSS or DS), which are not interoperable.

When purchasing wireless networking hardware from separate vendors be sure to obtain guarantees from the vendors that the hardware will interoperate and follows the standards.

Within a short time we expect all new wireless cards, like ethernet cards, to become inexpensive, ubiquitous and totally interoperable.

Also of note is that the latest version of the standard defines 11mbps and 5.5mbps networking, with support for the older standard 1mbps and 2mbps speeds. This provides some compatibility with different or older equipment. Note that this new standard covers DS-type Networks, not FH types.

Software access points such as InterGate which uses the wireless interface of the host computer should have no compatibility issues with third party wireless hardware, as long as standards are followed. Typically wireless hardware is identified to the software as a network interface, and therefore can be used in the same way as any other network card.

5. If my computer is connected to a wireless LAN, can it communicate with computers on a wired LAN as well?

To do this you 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 your networking requirements change.

If networking requirements go beyond just interconnecting a wired network 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.



Further to this the software access point may include significant additional features such as shared Internet access, web caching or content filtering, providing significant benefits to users and administrators.

6. What is the range of a wireless network?

Each access point has a finite range within which a wireless connection can be maintained between the client computer and the access point. The actual distance varies depending upon the environment; manufacturers typically state both indoor and outdoor ranges to give a reasonable indication of reliable performance. Also it should be noted that when operating at the limits of range the performance may drop, as the quality of connection deteriorates and the system compensates.

Typical indoor ranges are 150-300 feet, but can be shorter if the building construction interferes with radio transmissions. Longer ranges are possible, but performance will degrade with distance.

Outdoor ranges are quoted up to 1000 feet, but again this depends upon the environment.

There are ways to extend the basic operating range of Wireless communications, by using more than a single access point or using a wireless relay /extension point. See Question 8 for further information.

7. How many wireless networked computers can use a single access point?

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.

8. Can I have more than one access point?

Yes, 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. (See Figure 4)

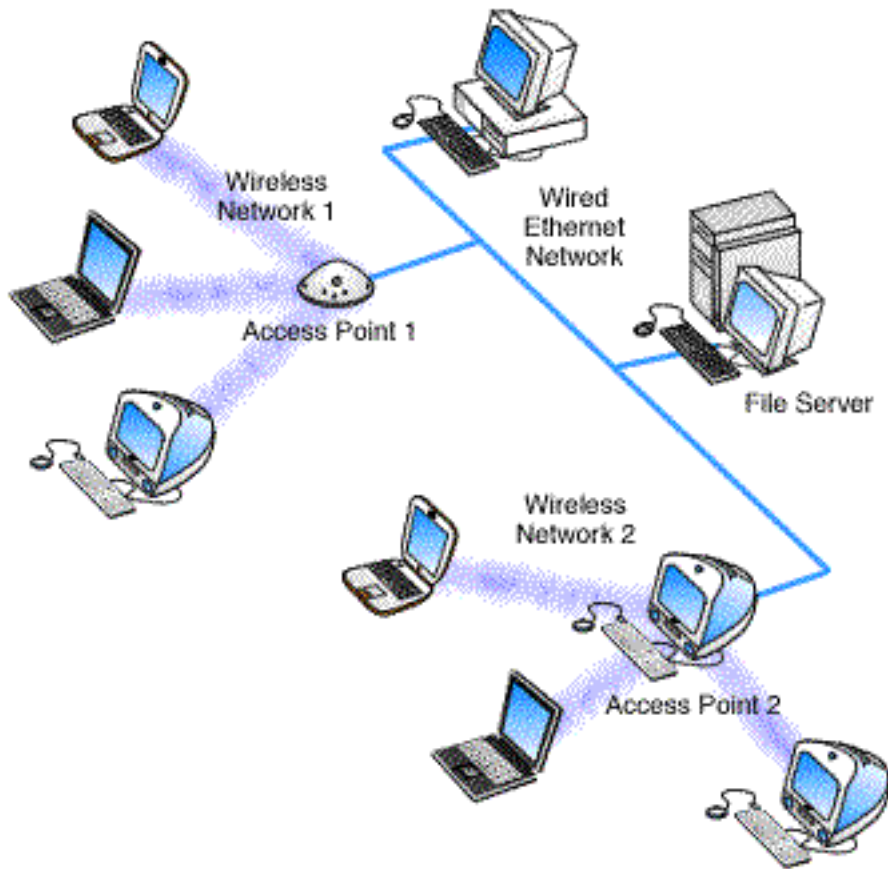


Figure 4: Multiple Access Points.

Wireless connected computers using 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. -- Note that an "extension point" is 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. " (See the next question for an explanation of 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. (See Figure 5)

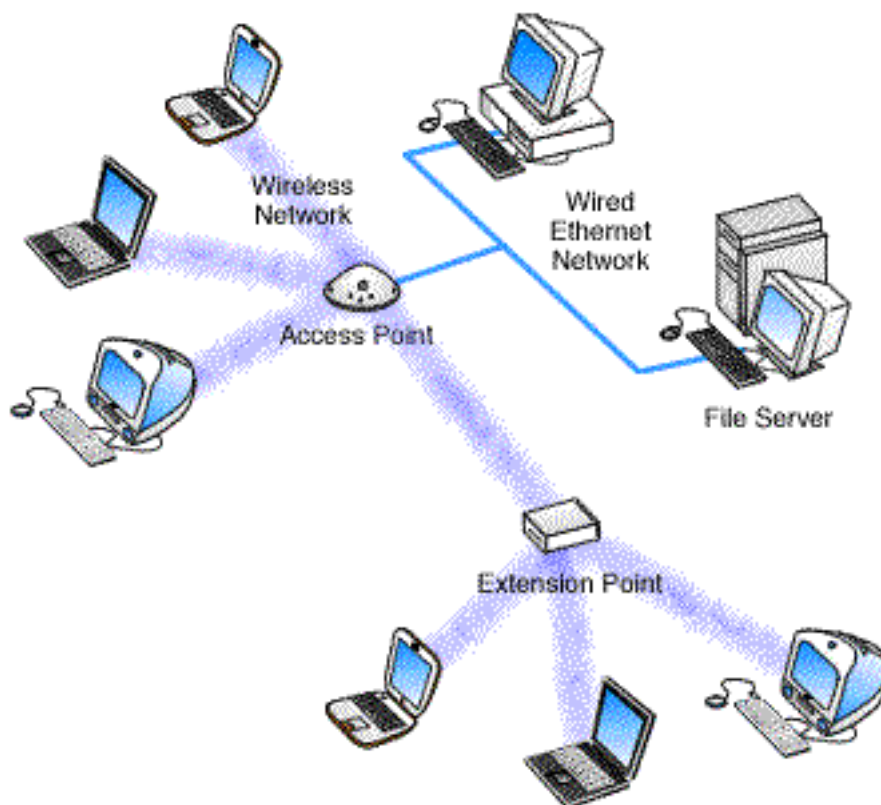


Figure 5: Extension Point.

Wireless connected computers using an Access Point with an Extension Point.

9. What is 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 best quality. 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:

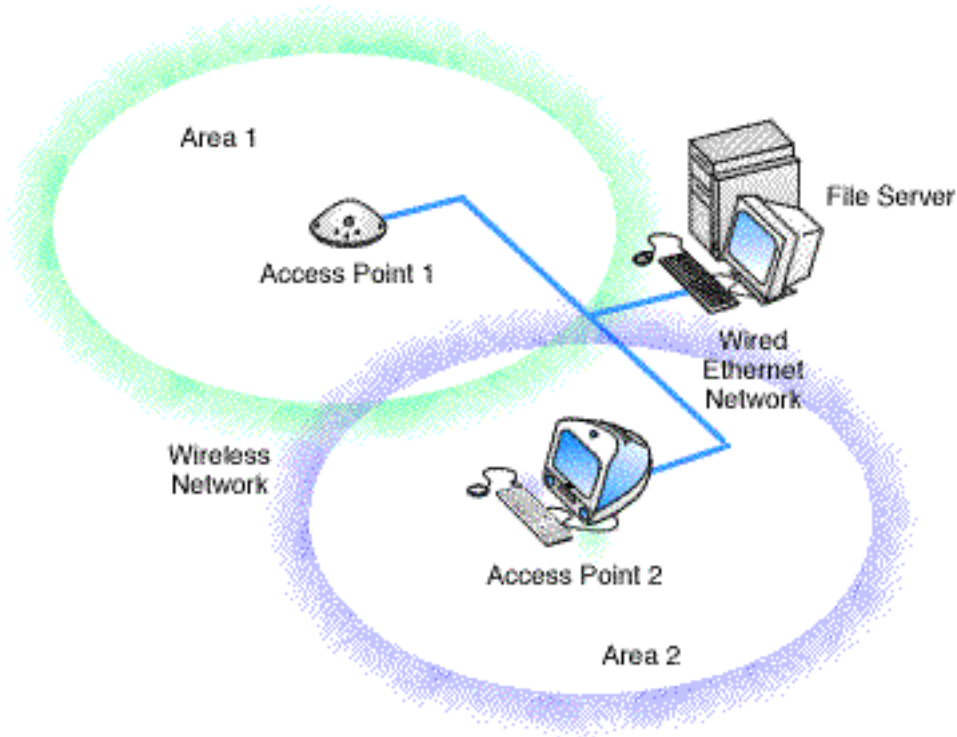


Figure 6: Roaming.

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

10. Can I use a wireless network to interconnect two LANs?

Yes. 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.

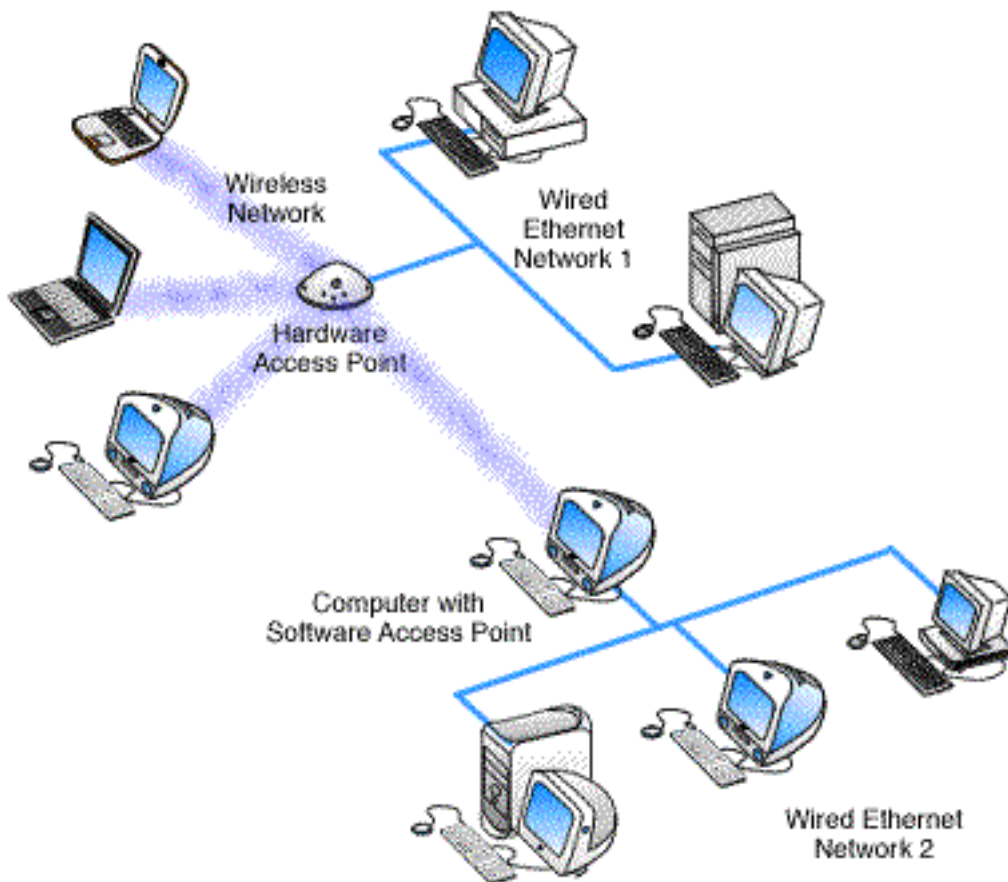


Figure 7: LAN to LAN Wireless Communications

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.

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, and is beyond the scope of this introduction. See the reference links at the end of this section if you require further information.

11. Is it true that wireless networking is only good for laptop computers?

Although wireless networking offers obvious benefits to users of laptops who move from location to location throughout the day, there are benefits for users of fixed position computers as well:

Many schools and businesses have unsuitable building layouts or walls that cannot be wired for various reasons making it difficult or impossible to build a wired network. Wireless networking in these environments is a very cost effective alternative also providing future flexibility.



In cases where a small number of computers are separated from a main network a wireless link may be more cost effective than network cabling although the latter is perfectly feasible.

Temporary wireless LANs can easily be created for exhibitions, school or business projects, all without any trailing cabling.

12. What about security?

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.

Section Two - Wireless Networking and the Internet

13. How can I use a wireless network to share an Internet connection?

Once you realise 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 a 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)

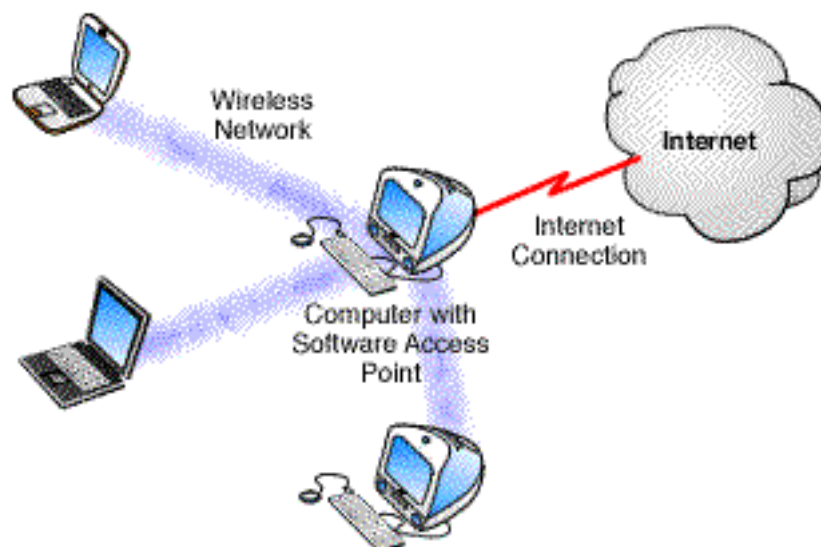


Figure 8: Software Access Point.

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

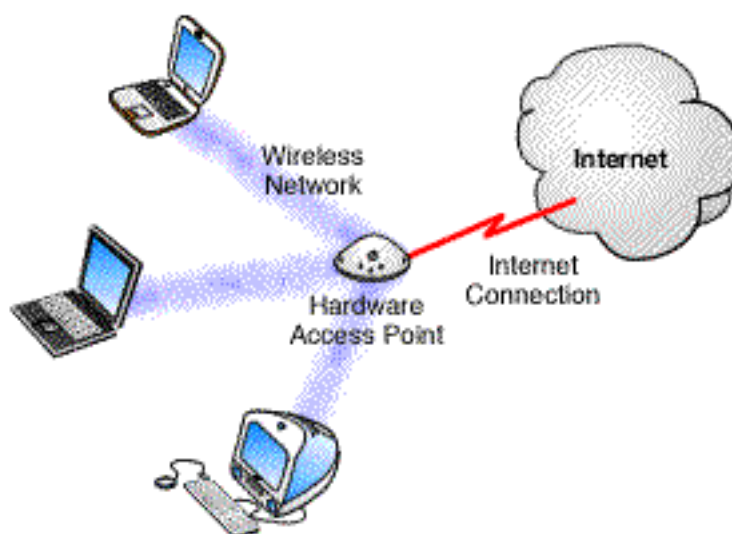


Figure 9: Hardware Access Point.

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

14. If I have more than one hardware access point, how can I share a single Internet connection?

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.

Content of this page in its entirety is protected by US & UK Copyright
© 2002 Vicomssoft Ltd

Reproduction in electronic and written form is expressly forbidden without written permission.

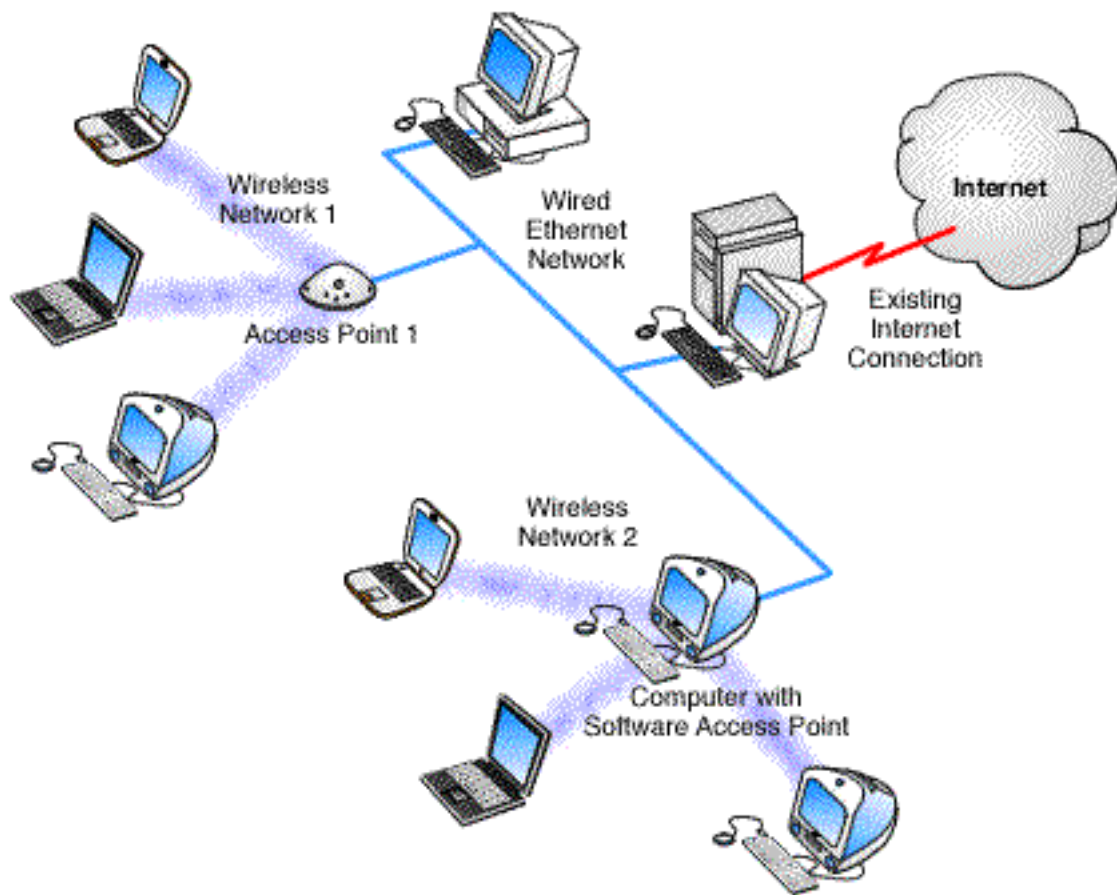


Figure 10: Multiple Access Points.

Wireless connected computers using Multiple Access Points.

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

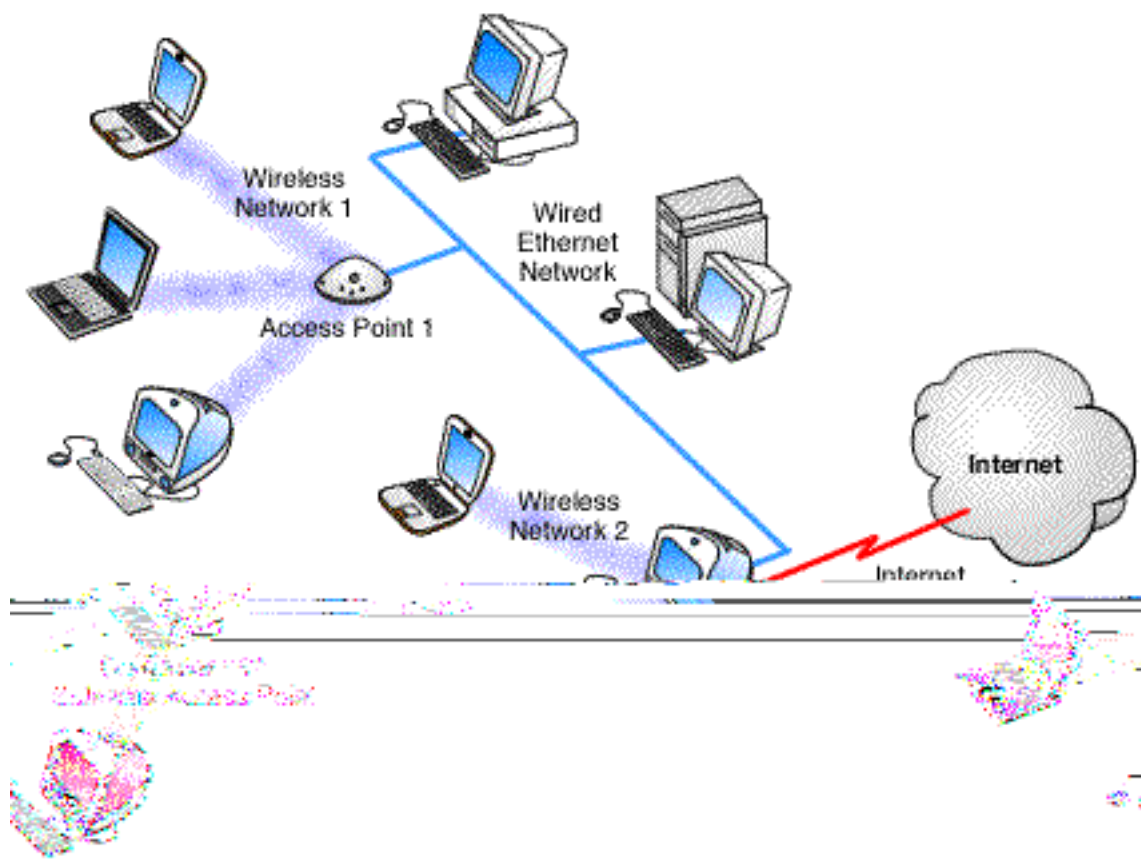


Figure 11: Software Access Point sharing one Internet connection.

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

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.

15. If I use a wireless network to connect to the Internet does my ISP need a wireless network too?

If you use a wireless network to connect to the Internet, the wireless part only concerns your LAN. The communications link from your LAN to your Internet service provider (ISP) would be identical whether or not you had a wireless network. For example, if you connected an ethernet network to the Internet via a 56K modem, when you upgraded your network to use wireless, you would still use the same 56K modem to connect to the Internet.

16. Can networking software identify a wireless computer in the same way it can identify an ethernet computer on the network?



Wireless cards look just like ethernet cards to your network drivers. In fact, wireless networking cards have unique MAC hardware addresses that are formatted like ethernet hardware addresses allocated from the same standards organization.