DOWNLOAD PDF 7.2 WIRELESS COMPUTER NETWORKS AND INTERNET ACCESS

Chapter 1 : How to Set up a Wireless Network (WiFi) Connection: 12 Steps

Wireless Computer Networks and Internet Access Short-range wireless networks Medium-range wireless networks Wide-area wireless networks This preview has intentionally blurred sections. Sign up to view the full version.

Role of the Yellow nodes: Are there places or times in a social situation where you are in an Access Point or Client situation? Are there places or times when you are in an Ad-Hoc situation? What connects to what? From the roles above, you can see that Clients always need to connect to an Access Point, and Mesh nodes all connect to each other. It should also be noted that due to how Wi-Fi is designed, this also prevents different roles from connecting to each other as well. Access Points cannot connect to each other wirelessly: Clients cannot connect to each other wirelessly: Clients cannot connect to Ad-Hoc Mesh devices wirelessly: Access Points cannot connect to Ad-Hoc Mesh devices wirelessly: Wireless devices in networks Treat the three types of roles above - Clients, Access Points, and Ad-Hoc nodes - as the building blocks for large networks. Below are several examples that demonstrate how devices configured for different roles can be used. Access Point - Home or Office network Wireless networks used in your home or office are generally a combination of a router and a wireless Access Point AP. In the diagram above: In many home networks, or small office networks, the router and AP may be combined into a single device. This is usually just called a wireless router. In large office scenarios, there may be several AP devices spread throughout the building to provide more even wireless coverage, connected back to the router through long Ethernet cables. Point to Point link - Long Distance Connections Wireless networks can be used to connect distant buildings or areas. It usually requires very focused antennas - such as a dish antenna - that can send a narrow beam in a specific direction. This is discussed in Learn Wireless Basics - so go there for more details on how that works. The name describes the concept: This requires two wireless devices: In the example below, two wireless devices are configured to create a point-to-point link. Omnidirectional Access Point and Client Link 1 represents computers connected with Ethernet cables to the wireless devices. These computers are connected to each other over the Point-to-Point link. This could look like the building-to-building connection, as shown below: Long-distance directional Access Point and Client Link Here we have another example of a point-to-point link, but where the routers have dish antennas for greater link distance. This could look like the network below, where an AP mounted on a tower is able to connect with a Client device in a home very far away, since the dishes are facing one another. In both of these examples, there are just two wireless devices linked together - and the antennas determine the range at which they can connect. The more focused the signal, the further the point-to-point link can reach. As the distance between the devices grow, it is more an more important to focus the signal with antennas - at both ends of the connection. Otherwise one end may hear the other, but not be loud enough to be heard! Point to MultiPoint - Wireless Internet Service Provider model If we combine the two principles used in the networks above - many client devices connecting to an Access Point, and more powerful antennas used for outdoor devices to create longer links - we can create Point to Multipoint networks. Instead of running cables around a neighborhood or town, they put up one or more powerful Access Points on a tall building or tower. The diagram below demonstrates one model for how this works. There is a powerful Access Point mounted on a high building, and several nearby buildings with rooftop wireless Client devices: Connected to each of the Client devices is an indoor router or Access Point, which allows users to connect their computers, laptops, tablets, or smartphones to the WISP network. Mesh - Neighbor-to-neighbor Networks A mesh network takes the principle of Point-to-Multipoint, and extends it to the idea of every node connecting to every other node in range. For more information on how this principle works, see the Introduction to Mesh document. These nodes will share all resources connected to them such as local servers hosting applications and connections to the Internet. They can also be connected to computers, Access Points, or routers inside the buildings so users can access the resources anywhere on the network. These nodes are receiving Internet access from Mesh Node B. They may be connected to different devices inside the building. Hybrid Networks

DOWNLOAD PDF 7.2 WIRELESS COMPUTER NETWORKS AND INTERNET ACCESS

When designing and building town or community-sized networks, it may be difficult or impossible to use a single method to connect everyone. For instance, a single Point-to-Multipoint network may not cover an entire community. Mesh nodes can be used to extend client sites to nearby buildings. Point-to-point connections can bridge longer distances and join several disconnected networks together. In the diagram below, we can see an example of a hybrid network. There is no single example that can cover all of the possible uses for a network! In the activity that follows, you will explore the different ways to build a network by working through scenarios. One last note before we move on to the activity - in the examples above, and in the activity that follows, the diagrams focus on building networks across rooftops or from building to building. This is generally the best way to build networks that cover neighborhoods, towns, or communities. Keep in mind that these rooftop routers may not provide connections to users on the ground, or in buildings. A good way to provide these connections is by attaching Access Points to an Ethernet port on the rooftop router. This indoor Access Point can be set up to use the rooftop network as the source of connections to the Internet, or to provide access to applications and servers on the network. A detailed look at this is below: It could be a Mesh Node, or Client router. Group Activity Since there are so many ways to build wireless networks to cover your town or community, we recommend working through these pen-and-paper activities. Download the network worksheets and example solutions and try your hand at designing wireless networks. If you are working through the activity on your own, try printing out the worksheets first and draw in a possible solution to each of the scenarios. You can then review the example solutions and see how your networks compare with some others. We recommend you work through this activity with a group of your community members, especially when planning and designing a network. First print out a few sets of the network worksheets, and break into groups of two or three people depending on how many people are gathered. Draw solutions to each scenario, then meet back up and compare all of your solutions to the scenarios. You can also look through the example solutions and compare them to what your groups came up with. Discuss what solutions might be best for your community. There are a few basic rules to follow when working through the activity. There are three types of routers you will use: These can send and receive wireless signals in every direction. These send and receive wireless signals in a limited arc. Limit the connections these routers make to a wedge-shaped area. These send and receive wireless signals in a narrow beam. Limit the connections to a single thin line. You have a limited amount of equipment available for each network. Each worksheet has icons of the types and number of pieces of equipment. The example below provides three omnidirectional, one sector, and one focused router: You can assume that all of the wireless equipment in the examples are within range of each other - the signals will reach. Remember that Clients can only connect to Access Points. APs cannot connect to each other wirelessly, Clients cannot connect to each other wirelessly, and Mesh nodes cannot connect to APs or Clients wirelessly. Many Clients can connect to a single Access Point. Ad-hoc mesh devices can have connections to multiple other mesh devices at once. This way devices that normally cannot connect wirelessly can still be networked. Now download and print out the worksheets and example solutions , and try out some designs! These are networks that may be ad-hoc mesh networks or point to point links between computers for small file sharing. Antenna Converts electrical signals to radio waves. It is normally connected to a radio transmitter or radio receiver, and is the interface between the electrical signals in the radio, and the movement of the signals through the air. The device with a wifi radio that you use to connect to a wireless access point, e. Ethernet A type of networking protocol - it defines the types of cables and connections that are used to wire computers, switches, and routers together. Most often Ethernet cabling is Category 5 or 6, made up of twisted pair wiring similar to phone cables. PoE Power over Ethernet describes systems which pass electrical power along with data on Ethernet cabling. Node An individual device in a mesh network. It is a partner document to Wireless Challenges , and can be done before or after that activity.

DOWNLOAD PDF 7.2 WIRELESS COMPUTER NETWORKS AND INTERNET ACCESS

Chapter 2 : Windows 7 - Unidentified Network - [Solved] - Networking

Wireless computer networks offer several distinct advantages compared to wired networks but are not without a downside. The primary and most obvious, advantage of using wireless technology is the huge mobility it offers (portability and freedom of movement).

Protect Your Network during Mobile Access Understand How a Wireless Network Works Going wireless generally requires connecting an internet "access point" â€” like a cable or DSL modem â€” to a wireless router, which sends a signal through the air, sometimes as far as several hundred feet. Any device within range can pull the signal from the air and access the internet. Unless you take certain precautions, anyone nearby can use your network. That means your neighbors â€” or any hacker nearby â€” could "piggyback" on your network or access information on your device. If an unauthorized person uses your network to commit crime or send spam, the activity could be traced back to your account. Using encryption is the most effective way to secure your network from intruders. Two main types of encryption are available for this purpose: Your computer, router, and other equipment must use the same encryption. WPA2 is strongest; use it if you have a choice. It should protect you against most hackers. Consider buying a new router with WPA2 capability. Wireless routers often come with the encryption feature turned off. You must turn it on. The directions that come with your router should explain how. Limit Access to Your Network Allow only specific devices to access your wireless network. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses to access to the network. Your router directs traffic between your local network and the internet. Strangers also could seize control of your router, to direct you to fraudulent websites. Change the name of your router from the default. The name of your router often called the service set identifier or SSID is likely to be a standard, default ID assigned by the manufacturer. Change the name to something unique that only you know. Use long and complex passwords â€” think at least 12 characters, with a mix of numbers, symbols, and upper and lower case letters. Never leave this feature enabled. Hackers can use them to get into your home network. Log out as Administrator: Keep your router up-to-date: To be secure and effective, the software that comes with your router needs occasional updates. To make sure you hear about the latest version, register your router with the manufacturer and sign up to get updates. For example, use protections like antivirus, antispyware, and a firewall -- and keep these protections up-to-date. Protect Your Network during Mobile Access Apps now allow you to access your home network from a mobile device. Before you do, be sure that some security features are in place. Use a strong password on any app that accesses your network. That way, no one else can access the app if your phone is lost or stolen. Password protect your phone or other mobile device.

DOWNLOAD PDF 7.2 WIRELESS COMPUTER NETWORKS AND INTERNET ACCESS

Chapter 3 : Types of Wireless Networks

Chapter 7: Telecommunications, the Internet, and Wireless Technology This VPN is a private network of computers linked using a secure "tunnel" connection over the Internet. It.

A ruling by the U. This was updated in with In , the Wi-Fi Alliance formed as a trade association to hold the Wi-Fi trademark under which most products are sold. The yin-yang Wi-Fi logo indicates the certification of a product for interoperability. Wi-Fi ad-hoc mode[edit] Wi-Fi nodes operating in ad-hoc mode refers to devices talking directly to each other without the need to first talk to an access point also known as base station. As of [update] , the Wi-Fi Alliance consisted of more than companies from around the world. Manufacturers with membership in the Wi-Fi Alliance, whose products pass the certification process, gain the right to mark those products with the Wi-Fi logo. Specifically, the certification process requires conformance to the IEEE Certification may optionally include tests of IEEE The lack of Wi-Fi certification does not necessarily imply that a device is incompatible with other Wi-Fi devices. A dot with curved lines radiating from it is a common symbol for Wi-Fi, representing a point transmitting a signal. The combination of computer and interface controllers is called a station. For all stations that share a single radio frequency communication channel, transmissions on this channel are received by all stations within range. A carrier wave is used to transmit the data. The data is organised in packets on an Ethernet link, referred to as " Ethernet frames ". The service set can be local, independent, extended or mesh. The SSID is configured within the devices that are considered part of the network, and it is transmitted in the packets. Receivers ignore wireless packets from networks with a different SSID. Versions[edit] There are many different versions of Wi-Fi: Equipment frequently support multiple versions of Wi-Fi. To communicate, devices must use a common Wi-Fi version. The versions differ between the radio wavebands they operate on, the radio bandwidth they occupy, the maximum data rates they can support and other details. In general, lower frequencies have better range but have less capacity. Some versions permit the use of multiple antennas, which permits greater speeds as well as reduced interference. Historically, equipment has listed the versions of Wi-Fi that it supports, but the Wi-Fi alliance has now standardised generational numbering so that equipment can indicate that it supports Wi-Fi 4 if the equipment supports The alliance have stated that the generational level 4, 5, or 6 can be indicated in the user interface when connected, along with the signal strength. The coverage of one or more interconnected access points hotspots can extend from an area as small as a few rooms to as large as many square kilometres. Coverage in the larger area may require a group of access points with overlapping coverage. For example, public outdoor Wi-Fi technology has been used successfully in wireless mesh networks in London, UK. An international example is Fon. Wi-Fi provides service in private homes, businesses, as well as in public spaces at Wi-Fi hotspots set up either free-of-charge or commercially, often using a captive portal webpage for access. Organizations and businesses , such as airports, hotels, and restaurants, often provide free-use hotspots to attract customers. Enthusiasts or authorities who wish to provide services or even to promote business in selected areas sometimes provide free Wi-Fi access. Routers that incorporate a digital subscriber line modem or a cable modem and a Wi-Fi access point, often set up in homes and other buildings, provide Internet access and internetworking to all devices connected to them, wirelessly or via cable. Similarly, battery-powered routers may include a cellular Internet radio modem and Wi-Fi access point. When subscribed to a cellular data carrier, they allow nearby Wi-Fi stations to access the Internet over 2G, 3G, or 4G networks using the tethering technique. Many smartphones have a built-in capability of this sort, including those based on Android , BlackBerry , Bada , iOS iPhone , Windows Phone and Symbian , though carriers often disable the feature, or charge a separate fee to enable it, especially for customers with unlimited data plans. Some laptops that have a cellular modem card can also act as mobile Internet Wi-Fi access points. Google is intending to use the technology to allow rural areas to enjoy connectivity by utilizing a broad mix of projection and routing services. Google also intends to bring connectivity to Africa and some Asian lands by launching blimps that

will allow for internet connection with Wi-Fi technology. Municipal wireless network An outdoor Wi-Fi access point In the early s, many cities around the world announced plans to construct citywide Wi-Fi networks. A company called WiFiyNet has set up hotspots in Mysore, covering the complete city and a few nearby villages. Carnegie Mellon University built the first campus-wide wireless Internet network, called Wireless Andrew , at its Pittsburgh campus in before Wi-Fi branding originated. Many universities collaborate in providing Wi-Fi access to students and staff through the Eduroam international authentication infrastructure. Wi-Fi ad hoc versus Wi-Fi direct[edit] Wi-Fi also allows communications directly from one computer to another without an access point intermediary. This is called ad hoc Wi-Fi transmission. This wireless ad hoc network mode has proven popular with multiplayer handheld game consoles , such as the Nintendo DS , PlayStation Portable , digital cameras , and other consumer electronics devices. Some devices can also share their Internet connection using ad hoc, becoming hotspots or "virtual routers". Countries apply their own regulations to the allowable channels, allowed users and maximum power levels within these frequency ranges. The ISM band ranges are also often used. Because of this choice of frequency band, Spectrum assignments and operational limitations are not consistent worldwide: Australia and Europe allow for an additional two channels 12, 13 beyond the 11 permitted in the United States for the 2. In the US and other countries, A Wi-Fi signal occupies five channels in the 2. Any two channel numbers that differ by five or more, such as 2 and 7, do not overlap. The oft-repeated adage that channels 1, 6, and 11 are the only non-overlapping channels is, therefore, not accurate. Channels 1, 6, and 11 are the only group of three non-overlapping channels in North America and the United Kingdom. In Europe and Japan using Channels 1, 5, 9, and 13 for Electromagnetic interference at 2. Wi-Fi protocols are designed to share channels reasonably fairly, and will often work with little to no disruption. In addition interference can be caused by overlapping channels in the These issues can become a problem in high-density areas, such as large apartment complexes or office buildings with many Wi-Fi access points. Additionally, other devices use the 2. It is also an issue when municipalities [64] or other large entities such as universities seek to provide large area coverage. These bands are allowed to be used with low power transmitters, without requiring a license and with few restrictions. However, while unintended interference is common, users that have been found to knowingly cause deliberate interference to other users particularly for attempting to locally monopolise these bands for commercial purposes have been handed large fines.

DOWNLOAD PDF 7.2 WIRELESS COMPUTER NETWORKS AND INTERNET ACCESS

Chapter 4 : Connecting to Two Networks Simultaneously Solved - Windows 7 Help Forums

Multiple Networks and no Internet Connection I have a HP Pavilion mn and a HP Pavilion ax on a home network using an Actiontec DSL Modem and a Linksys Etherfast Cable/DSL Router. I have just upgraded the mn from Vista Home Premium to Windows 7 Home Premium.

Setting up a wireless network Content provided by Microsoft Applies to: Windows 10Windows 7Windows 8. This article describes the basic steps for setting up a wireless network and starting to use it. Broadband Internet connection and modem. A broadband Internet connection is a high-speed Internet connection. You can get a broadband connection by contacting an Internet service provider ISP. You can also find these at computer or electronics stores, and online. A router sends info between your network and the Internet. With a wireless router, you can connect PCs to your network using radio signals instead of wires. A wireless network adapter is a device that connects your PC to a wireless network. Positioning the wireless router Put your wireless router somewhere where it will receive the strongest signal with the least amount of interference. Place your wireless router in a central location. Place the router as close to the center of your home as possible to increase the strength of the wireless signal throughout your home. Position the wireless router off the floor and away from walls and metal objects, such as metal file cabinets. Some networking equipment uses a 2. This is the same frequency as most microwaves and many cordless phones. If you turn on the microwave or get a call on a cordless phone, your wireless signal might be temporarily interrupted. You can avoid most of these issues by using a cordless phone with a higher frequency, such as 5. To help make your network more secure: Change the default user name and password. This helps protect your router. Someone could use this info to access your router without you knowing it. To help avoid that, change the default user name and password for your router. Set up a security key password for your network. Wireless networks have a network security key to help protect them from unauthorized access. See the documentation for your router for more detailed info, including what type of security is supported and how to set it up. Do one of the following, depending on which version of Windows is running on your PC: In Windows 7 or Windows 8. Select Set up a new connection or network. The wizard will walk you through creating a network name and a security key. Write down your security key and keep it in a safe place. You can also save your security key on a USB flash drive by following the instructions in the wizard. Windows Firewall is included with this version of Windows.

DOWNLOAD PDF 7.2 WIRELESS COMPUTER NETWORKS AND INTERNET ACCESS

Chapter 5 : Computer Networks, Fourth Edition [Book]

Connecting to Two Networks Simultaneously So I need help being able to connect to a wireless network with internet access and a wired network with no internet access. Of course, being connected to both simultaneously results in no internet access.

WLANs Terrestrial microwave â€" Terrestrial microwave communication uses Earth-based transmitters and receivers resembling satellite dishes. Terrestrial microwaves are in the low gigahertz range, which limits all communications to line-of-sight. These Earth-orbiting systems are capable of receiving and relaying voice, data, and TV signals. Cellular and PCS systems use several radio communications technologies. The systems divide the region covered into multiple geographic areas. Each area has a low-power transmitter or radio relay antenna device to relay calls from one area to the next area. Radio and spread spectrum technologies â€" Wireless local area networks use a high-frequency radio technology similar to digital cellular and a low-frequency radio technology. Wireless LANs use spread spectrum technology to enable communication between multiple devices in a limited area. Free-space optical communication uses visible or invisible light for communications. In most cases, line-of-sight propagation is used, which limits the physical positioning of communicating devices. The use of spread-spectrum or OFDM technologies may allow users to move around within a local coverage area, and still remain connected to the network. Products using the IEEE Fixed wireless technology implements point-to-point links between computers or networks at two distant locations, often using dedicated microwave or modulated laser light beams over line of sight paths. It is often used in cities to connect networks in two or more buildings without installing a wired link. Wireless ad hoc network[edit] A wireless ad hoc network, also known as a wireless mesh network or mobile ad hoc network MANET , is a wireless network made up of radio nodes organized in a mesh topology. Each node forwards messages on behalf of the other nodes and each node performs routing. Ad hoc networks can "self-heal", automatically re-routing around a node that has lost power. Various network layer protocols are needed to realize ad hoc mobile networks, such as Distance Sequenced Distance Vector routing, Associativity-Based Routing , Ad hoc on-demand Distance Vector routing , and Dynamic source routing. These networks can be used to connect branch offices of business or as a public Internet access system. The wireless connections between access points are usually point to point microwave links using parabolic dishes on the 2. A typical system contains base station gateways, access points and wireless bridging relays. Other configurations are mesh systems where each access point acts as a relay also. When combined with renewable energy systems such as photovoltaic solar panels or wind systems they can be stand alone systems. In a cellular network, each cell characteristically uses a different set of radio frequencies from all their immediate neighbouring cells to avoid any interference. When joined together these cells provide radio coverage over a wide geographic area. This enables a large number of portable transceivers e. Although originally intended for cell phones, with the development of smartphones , cellular telephone networks routinely carry data in addition to telephone conversations: The GSM network is divided into three major systems: The cell phone connects to the base system station which then connects to the operation and support station; it then connects to the switching station where the call is transferred to where it needs to go. GSM is the most common standard and is used for a majority of cell phones. Sprint happened to be the first service to set up a PCS. The newer GSM networks are replacing the older system. Global area network[edit] A global area network GAN is a network used for supporting mobile across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications is handing off user communications from one local coverage area to the next. Different uses[edit] Some examples of usage include cellular phones which are part of everyday wireless networks, allowing easy personal communications. Another example, Intercontinental network systems, use radio satellites to communicate across the world. Emergency services such as the police utilize wireless networks to communicate effectively as well. Individuals and businesses use wireless networks to

send and share data rapidly, whether it be in a small office building or across the world. General[edit] In a general sense, wireless networks offer a vast variety of uses by both business and home users. Each wireless technology is defined by a standard that describes unique functions at both the Physical and the Data Link layers of the OSI model. These standards differ in their specified signaling methods, geographic ranges, and frequency usages, among other things. Such differences can make certain technologies better suited to home networks and others better suited to network larger organizations. The use of this technology also gives room for expansions, such as from 2G to 3G and, 4G and 5G technologies, which stand for the fourth and fifth generation of cell phone mobile communications standards. As wireless networking has become commonplace, sophistication increases through configuration of network hardware and software, and greater capacity to send and receive larger amounts of data, faster, is achieved. Now the wireless network has been running on LTE, which is a 4G mobile communication standard. Users of an LTE network should have data speeds that are 10x faster than a 3G network. Wireless networks offer many advantages when it comes to difficult-to-wire areas trying to communicate such as across a street or river, a warehouse on the other side of the premises or buildings that are physically separated but operate as one. Space is also created in homes as a result of eliminating clutters of wiring. Home[edit] For homeowners, wireless technology is an effective option compared to Ethernet for sharing printers, scanners, and high-speed Internet connections. WLANs help save the cost of installation of cable mediums, save time from physical installation, and also creates mobility for devices connected to the network. These NEs can be stand-alone systems or products that are either supplied by a single manufacturer or are assembled by the service provider user or system integrator with parts from several different manufacturers. Wireless NEs are the products and devices used by a wireless carrier to provide support for the backhaul network as well as a mobile switching center MSC. Reliable wireless service depends on the network elements at the physical layer to be protected against all operational environments and applications see GR, Generic Requirements for Network Elements Used in Wireless Networks â€" Physical Layer Criteria. The attachment hardware and the positioning of the antenna and associated closures and cables are required to have adequate strength, robustness, corrosion resistance, and resistance against wind, storms, icing, and other weather conditions. Requirements for individual components, such as hardware, cables, connectors, and closures, shall take into consideration the structure to which they are attached. Interferences[edit] Compared to wired systems, wireless networks are frequently subject to electromagnetic interference. This can be caused by other networks or other types of equipment that generate radio waves that are within, or close, to the radio bands used for communication. Interference can degrade the signal or cause the system to fail. This can cause dead zones where no reception is available. Multipath fading[edit] In multipath fading two or more different routes taken by the signal, due to reflections, can cause the signal to cancel out at certain locations, and to be stronger in other places upfade. Hidden node problem[edit] The hidden node problem occurs in some types of network when a node is visible from a wireless access point AP , but not from other nodes communicating with that AP. This leads to difficulties in media access control. Shared resource problem[edit] The wireless spectrum is a limited resource and shared by all nodes in the range of its transmitters. Bandwidth allocation becomes complex with multiple participating users. Often users are not aware that advertised numbers e. With increasing demand, the capacity crunch is more and more likely to happen. User-in-the-loop UIL may be an alternative solution to ever upgrading to newer technologies for over-provisioning.

Chapter 6 : How do I restrict or block Internet access on a home network? - Super User

3 WIRELESS NETWORK MODES WIRELESS SECURITY SETTINGS Computer/Notebook and Internet access. 2. (2) Ethernet cables. 3. (1) EnGenius ENH

Chapter 7 : Windows 7 No internet Access but network connected

DOWNLOAD PDF 7.2 WIRELESS COMPUTER NETWORKS AND INTERNET ACCESS

A wireless network is a computer network that uses wireless data connections between network nodes. [1] Wireless networking is a method by which homes, telecommunications networks and business installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations. [2].

Chapter 8 : Multiple Networks and no Internet Connection - Microsoft Community

The problem is that although in Network and Sharing center it shows that the wireless connection has internet, it also shows that the computer is not connected to the internet. If I only connect with the wireless, I have internet connection, but when connecting to the wired one it just can't access the internet anymore.

Chapter 9 : Wireless network - Wikipedia

a broadband Internet connection, network printers, data files, and even streaming audio 7 âˆšâˆš âˆš âˆš network is composed of a wireless access point(s).