DOWNLOAD PDF ESSENTIAL GUIDE TO HOME NETWORKING TECHNOLOGIES, THE

Chapter 1 : How to set up your small business computer network - Essential Guide

Only one book covers all you need to know: The Essential Guide to Home Networking Technologies. This book starts where other home networking guides leave off, with thorough, expert coverage of every issue and technology driving home networking.

Radio waves burning holes in your brain as packets of data containing a Netflix movie fly through the air over to your TV; what could be better? Neighbors using up your bandwidth watching cat videos on YouTube. Signal dropping every time you take your iPad into the bathroom and try to download a new app you know you do it. Agonizingly slow speeds every time your other family members jump on the network. Setting up a wireless network properly can alleviate all of these problems. Resolving these issues is actually pretty easy. This guide takes you through the basic set up and configuration of a wireless router, and points you to a few extra resources to help optimize the system. You could skip this part of the tutorial if you want, but it provides a fundamental understanding of how a wireless network works that will help frame the rest of the guide and allow you to troubleshoots problems more easily. Modem â€" The modem is the first link in this chain. It allows your home to connect to the Internet. Power is for, well, power. If you have cable Internet then the modem will have a coax cable jack on the back. If you have DSL, you will see a phone jack instead of a cable connection. The last jack is Ethernet, which looks like a wide phone jack. If you find that your modem has multiple Ethernet jacks, then is it what is referred to as a gateway, and likely also has built-in wireless. Think of a gateway as a wireless router and modem combined into one box. You can still follow this tutorial for setting up a gateway. Simply ignore steps 2 and 4 about physically hooking up a router, all of the wireless configuration is the same. First, it takes the Internet signal from the modem and transmits it wirelessly in your home. Somewhere on the box of your router, it will tell you what types of wireless protocols it broadcasts. As wireless technology has developed, new wireless protocols have emerged. Over the past 6 years or so, wireless g has slowly been phased out by a newer protocol, wireless n. Over the past 2 years, the newest wireless protocol, wireless ac has started to come into prominence. Luckily, all wireless routers are backwards compatible, so a brand new wireless ac router will work with older wireless g devices. There are two older protocols called wireless a and wireless b, but those where largely phased out years ago. The same goes for any wireless protocol, like Nearly all modern computers, tablets, phones, and game consoles have built-in wireless. The reason I specified a computer is because in this tutorial the best device to use to configure the wireless network is a computer. All of the setup procedures can be completed using a wireless computer, but it will make the process a pain. Seriously, use a hardwired computer for this tutorial; it will make your life much easier. First, connect the coax cable or phone cable for DSL modems from the wall to the modem. Remember that if you have a wireless gateway i. In fact, you should not try to use a separate router combined with a gateway without advanced knowledge of home networks, particularly the functions of DHCP. If you have a gateway, simply connect the coax or phone line to it and power it on, wait a few minutes, and skip to step 5. The modem will take a few minutes to fully start up. Next, connect the power cable for the router. Again, wait a minute or two for it to start up completely. As always, you can consult the product manuals to find out what the various lights mean. Most routers have 4 LAN connections, any one of them will work fine. Give the computer a minute or two to connect to the Internet. At this point, we can test that everything is working. Simply click this link: Did an Internet browser pop up and take you to Google figure 1 below. If, instead, your browser was not able to load Google, there are two possibilities. Some routers will take you to a sort of intro page the first time you go online. Disconnect power from both devices For good measure, turn off your computer as well. If at this point you are still not able to connect, I would call your Internet provider for help. Figure 2 â€" Bad: As of right now, you are done making physical connections. Now we need to login to the router using the computer and start changing some internal settings. After that, we will update the firmware Step 6 , set the wireless name Step 7 and security step 8. If so, you could leave everything as is. However, I

would highly recommend following the rest of this tutorial to customize the network so it works best for you. If your router can with a setup disk, you could use it at this time and jump to the last step in the tutorial. Feel free to try it, but proceed at your own risk. I would recommend setting it aside and following the rest of this tutorial. Before we can adjust any settings in the router, we need to actually login to it. We have a separate tutorial to show you how to login to a router. Once you are logged into the router, you can continue to the next step. It should always been done when setting up a router. Additionally, If you ever experience weird issues in the future, you should check to see if the firmware is the most current version. Good manufacturers continue to update the firmware for their routers for a long time after the router is no longer in production. D-Link DIR Firmware Upgrade Screen The firmware setting is buried in a slightly different spot in the menu of each router, so you will just have to poke around a bit. After locating the firmware section, you will need to determine if it already has the most recent version installed. Linksys , Netgear , Belkin , D-Link. Once the firmware update process starts, do not do anything! Let it run its course. The router will likely take a few minutes to reboot. If you interrupt this process you can ruin the router. Once the firmware is updated, you may have to log back into the router. You can just move on to the next step. In the image below, you can see a list of available networks as displayed on Windows 7. You need to decide on a network name that is different than any other networks in your area, but remember that this information is public. This is not a password. Avoid using a last name or any other information that could identify you, like your address. Try something generic, like a sports team or hobby. Avoid using any special characters, and stick to letters or numbers. Also avoid making it unnecessarily long. Do not use the exact same name. Once you have decided on a name, save the network settings. Your router might take a few moments to update. First, to keep unwanted guests from logging on and using up your bandwidth. Second, to keep people from eavesdropping on your network activity and stealing important data. Just like there are different wireless protocols remember WEP used to be used most often, but it is easily hacked and should be avoided. However, WPA2 is the newest and preferred security option. Simply select it as the security type. It allows you to connect equipment to the network without actually knowing the password, a cool feature designed for convenience. Yes, it is, but unfortunately it has well document security flaws as well. Next, you need to choose a password. It can be between 8 and 63 characters. You can use a combination of uppercase and lowercase letters, numbers, and special characters. While a longer, more complex or random password is better for security than a short, simple password, it can also be more difficult to remember. It can also be a pain to enter in. I would recommend at least using one uppercase letter and one number in your password. No matter what you choose as a password, write it on a scrap of paper and tape it to the router. I would recommend upgrading the wireless card in that device or hard-wiring it to the network. I would NOT recommend compromising the security of the entire network just for one outdated device. Wireless Security Selection 9 Optimize performance Technically, step 9 is optional, but we highly recommend following it.

Chapter 2 : How to Set Up a Home Network - Equipment & Networking Basics Guide

Essential Guide to Home Networking Technologies, The by GERARD O'DRISCOLL Stay ahead with the world's most comprehensive technology and business learning platform. With Safari, you learn the way you learn best.

Today computer networks are everywhere. You will find them in homes, offices, factories, hospitals leisure centres etc. But how are they created? What technologies do they use? In this tutorial you will learn the basic networking technologies, terms and concepts used in all types of networks both wired and wireless, home and office. Home and Office Networks The network you have at home uses the same networking technologies, protocols and services that are used in large corporate networks and on the Internet. The only real difference between an home network and a large corporate network is the size. A home network will have between 1 and 20 devices and a corporate network will have many thousands. Setting Up and building a Home Network will introduce some basic networking component and show you how to build a home network and connect it to the Internet. Networking Types and Structures Networks can be wired or wireless with most networks being a mixture of both. Wired vs Wireless Networks Early pre networks were predominately wired. Today however most networks will use a mixture of wired and wireless network. Wired networks use Ethernet as the data link protocol. Wired networks are faster than Wireless. Data rates were periodically increased from the original 10 megabits per second, to 1gigabits per second. Most home networks use Mbps. More secure than Wireless Need to Use cable which can be unsightly, difficult to run and expensive. Note a new technology that uses mains cable overcomes many of these disadvantages. Wireless Networks â€" Advantages and Disadvantages Wireless networks use Wi-fi as the data link protocol. However other wireless options are being developed for the IOT Internet of things. Advantages Generally easier to set up. Can be used both on home and public networks No cables required. Can be used with mobile phones and tablets. Wireless Networks Disadvantages Generally Slower than wired networks. Not as secure depending on set up. Networking Topologies and Layout There are many different ways network nodes can be connected together. There are many different ways network nodes can be connected together. Common connection technologies like Wi-Fi, Bluetooth etc are designed to work using a particular network topology. When designing networks and choosing connection protocols having an understanding of these topologies is important.

Chapter 3 : Basic Networking Concepts-Beginners Guide

Networking-for-beginners-tutorial 1-Introduction-to-Computer-Networks-basics-lecture NEW Space Documentary HD Future Space Travel technologies NEW Science & technology.

Justin Ellingwood Introduction A basic understanding of networking is important for anyone managing a server. Not only is it essential for getting your services online and running smoothly, it also gives you the insight to diagnose problems. This document will provide a basic overview of some common networking concepts. We will discuss basic terminology, common protocols, and the responsibilities and characteristics of the different layers of networking. This guide is operating system agnostic, but should be very helpful when implementing features and services that utilize networking on your server. Networking Glossary Before we begin discussing networking with any depth, we must define some common terms that you will see throughout this guide, and in other guides and documentation regarding networking. These terms will be expanded upon in the appropriate sections that follow: In networking, a connection refers to pieces of related information that are transfered through a network. This generally infers that a connection is built before the data transfer by following the procedures laid out in a protocol and then is deconstructed at the at the end of the data transfer. A packet is, generally speaking, the most basic unit that is transfered over a network. When communicating over a network, packets are the envelopes that carry your data in pieces from one end point to the other. Packets have a header portion that contains information about the packet including the source and destination, timestamps, network hops, etc. The main portion of a packet contains the actual data being transfered. It is sometimes called the body or the payload. A network interface can refer to any kind of software interface to networking hardware. For instance, if you have two network cards in your computer, you can control and configure each network interface associated with them individually. A network interface may be associated with a physical device, or it may be a representation of a virtual interface. The "loopback" device, which is a virtual interface to the local machine, is an example of this. LAN stands for "local area network". It refers to a network or a portion of a network that is not publicly accessible to the greater internet. A home or office network is an example of a LAN. WAN stands for "wide area network". It means a network that is much more extensive than a LAN. While WAN is the relevant term to use to describe large, dispersed networks in general, it is usually meant to mean the internet, as a whole. If an interface is said to be connected to the WAN, it is generally assumed that it is reachable through the internet. A protocol is a set of rules and standards that basically define a language that devices can use to communicate. There are a great number of protocols in use extensively in networking, and they are often implemented in different layers. A port is an address on a single machine that can be tied to a specific piece of software. It is not a physical interface or location, but it allows your server to be able to communicate using more than one application. A firewall is a program that decides whether traffic coming into a server or going out should be allowed. A firewall usually works by creating rules for which type of traffic is acceptable on which ports. Generally, firewalls block ports that are not used by a specific application on a server. NAT stands for network address translation. It is a way to translate requests that are incoming into a routing server to the relevant devices or servers that it knows about in the LAN. This is usually implemented in physical LANs as a way to route requests through one IP address to the necessary backend servers. VPN stands for virtual private network. It is a means of connecting separate LANs through the internet, while maintaining privacy. This is used as a means of connecting remote systems as if they were on a local network, often for security reasons. There are many other terms that you may come across, and this list cannot afford to be exhaustive. We will explain other terms as we need them. At this point, you should understand some basic, high-level concepts that will enable us to better discuss the topics to come. Network Layers While networking is often discussed in terms of topology in a horizontal way, between hosts, its implementation is layered in a vertical fashion throughout a computer or network. What this means is that there are multiple technologies and protocols that are built on top of each other in order for communication to

function more easily. Each successive, higher layer abstracts the raw data a little bit more, and makes it simpler to use for applications and users. It also allows you to leverage lower layers in new ways without having to invest the time and energy to develop the protocols and applications that handle those types of traffic. The language that we use to talk about each of the layering scheme varies significantly depending on which model you use. Regardless of the model used to discuss the layers, the path of data is the same. As data is sent out of one machine, it begins at the top of the stack and filters downwards. At the lowest level, actual transmission to another machine takes place. At this point, the data travels back up through the layers of the other computer. Each layer has the ability to add its own "wrapper" around the data that it receives from the adjacent layer, which will help the layers that come after decide what to do with the data when it is passed off. This model defines seven separate layers. The layers in this model are: The application layer is the layer that the users and user-applications most often interact with. Network communication is discussed in terms of availability of resources, partners to communicate with, and data synchronization. The presentation layer is responsible for mapping resources and creating context. It is used to translate lower level networking data into data that applications expect to see. The session layer is a connection handler. It creates, maintains, and destroys connections between nodes in a persistent way. The transport layer is responsible for handing the layers above it a reliable connection. In this context, reliable refers to the ability to verify that a piece of data was received intact at the other end of the connection. This layer can resend information that has been dropped or corrupted and can acknowledge the receipt of data to remote computers. The network layer is used to route data between different nodes on the network. It uses addresses to be able to tell which computer to send information to. This layer can also break apart larger messages into smaller chunks to be reassembled on the opposite end. This layer is implemented as a method of establishing and maintaining reliable links between different nodes or devices on a network using existing physical connections. The physical layer is responsible for handling the actual physical devices that are used to make a connection. This layer involves the bare software that manages physical connections as well as the hardware itself like Ethernet. As you can see, there are many different layers that can be discussed based on their proximity to bare hardware and the functionality that they provide. It defines the four separate layers, some of which overlap with the OSI model: In this model, the application layer is responsible for creating and transmitting user data between applications. The applications can be on remote systems, and should appear to operate as if locally to the end user. The communication is said to take place between peers. The transport layer is responsible for communication between processes. This level of networking utilizes ports to address different services. It can build up unreliable or reliable connections depending on the type of protocol used. The internet layer is used to transport data from node to node in a network. This layer is aware of the endpoints of the connections, but does not worry about the actual connection needed to get from one place to another. IP addresses are defined in this layer as a way of reaching remote systems in an addressable manner. The link layer implements the actual topology of the local network that allows the internet layer to present an addressable interface. It establishes connections between neighboring nodes to send data. This made it easier to implement and allowed it to become the dominant way that networking layers are categorized. Interfaces Interfaces are networking communication points for your computer. Each interface is associated with a physical or virtual networking device. Typically, your server will have one configurable network interface for each Ethernet or wireless internet card you have. In addition, it will define a virtual network interface called the "loopback" or localhost interface. This is used as an interface to connect applications and processes on a single computer to other applications and processes. You can see this referenced as the "lo" interface in many tools. Many times, administrators configure one interface to service traffic to the internet and another interface for a LAN or private network. In DigitalOcean, in datacenters with private networking enabled, your VPS will have two networking interfaces in addition to the local interface. The "eth0" interface will be configured to handle traffic from the internet, while the "eth1" interface will operate to communicate with the private network. Protocols Networking works by piggybacking a number of different protocols on top of each other. In this

way, one piece of data can be transmitted using multiple protocols encapsulated within one another. We will talk about some of the more common protocols that you may come across and attempt to explain the difference, as well as give context as to what part of the process they are involved with. We will start with protocols implemented on the lower networking layers and work our way up to protocols with higher abstraction. Media Access Control Media access control is a communications protocol that is used to distinguish specific devices. Each device is supposed to get a unique MAC address during the manufacturing process that differentiates it from every other device on the internet. Addressing hardware by the MAC address allows you to reference a device by a unique value even when the software on top may change the name for that specific device during operation. Media access control is one of the only protocols from the link layer that you are likely to interact with on a regular basis.

Chapter 4 : Feeling clueless about Wi-Fi and home networking? Here's where you start. - CNET

If you are looking for quick summaries of the various standards and technologies pertinent to home networking, this is a useful book. As mentioned by the other reviewers, it covers almost everything developed or under development.

Securing your network Rule of thumb: The speed of a single network connection is determined by the slowest speed of any party involved. For example, in order to have a wired Gigabit Ethernet connection between two computers, both computers, the router they are connected to and the cables used to link them together all need to support Gigabit Ethernet or a faster standard. If you plug a Gigabit Ethernet device and an regular Ethernet device into a router, the connection between the two will be capped at the speed of Ethernet, which is Mbps. In short, LAN ports on a router allow Ethernet-ready devices to connect to one another and share data. On many routers, this port may also be labeled the internet port. A typical CAT5e network cable. A hub and a switch both add more LAN ports to an existing network. They help increase the number of Ethernet-ready clients that a network can host. The main difference between hubs and switches is a hub uses one shared channel for all of its ports, while a switch has a dedicated channel for each one. For this reason, hubs are much cheaper than switches with the same number of ports. However, hubs are largely obsolete now, since the cost of switches has come down significantly. The price of a switch generally varies based on its standard regular Ethernet or Gigabit Ethernet, with the latter being more expensive , and the number of ports the more ports, the higher the price. You can find a switch with just four or up to 48 ports or even more. For example, a four-port switch will add another three clients to the network. This is because you need to use one of the ports to connect the switch itself to the network, which, by the way, also uses another port of the existing network. With this in mind, make sure you buy a switch with significantly more ports than the number of clients you intend to add to the network. Wide-area network WAN port: Also known as the internet port. Generally, a router has just one WAN port. Some business routers come with dual WAN ports, so one can use two separate internet services at a time. On any router, the WAN port will be separated from the LAN ports, and is often distinguished by being a different color. A WAN port is used to connect to an internet source, such as a broadband modem. The WAN allows the router to connect to the internet and share that connection with all the Ethernet-ready devices connected to it. Often called a DSL modem or cable modem, a broadband modem is a device that bridges the internet connection from a service provider to a computer or to a router, making the internet available to consumers. To hook up more than one device to the internet, you will need a router. These are the cables used to connect network devices to a router or a switch. They are also known as Category 5 cables, or CAT5 cables. The latest network cabling standard currently in use is CAT6, which is designed to be faster and more reliable than CAT5e. The difference between the two is the wiring inside the cable and at both ends of it. CAT5e and CAT6 cables can be used interchangeably, and in my personal experience their performance is essentially the same. For most home usage, what CAT5e has to offer is more than enough. Also, network cables are the same, no matter how they shape, round or flat. Wireless networking A wireless network is very similar to a wired network with one big difference: Instead, they use radio wireless connections called Wi-Fi Wireless Fidelity , which is a friendly name for the In a typical home network, there are generally both wired and wireless devices, and they can all talk to one another. In order to have a Wi-Fi connection, there needs to be an access point and a Wi-Fi client. Basic terms Each of the Wi-Fi networks that a client, such as an iPhone, detects generally belongs to one access point. You can buy an AP separately and connect it to a router or a switch to add Wi-Fi support to a wired network, but generally, you want to buy a wireless router, which is a regular router one WAN port, multiple LAN ports and so on with a built-in access point. Some routers even come with more than one access point see discussion of dual-band and tri-band routers below. A Wi-Fi client or WLAN client is a device that can detect the signal broadcast by an access point, connect to it and maintain the connection. All recent laptops, phones and tablets on the market come with built-in Wi-Fi capability. Think of a Wi-Fi client as a device that has an invisible network port and an invisible network cable. This metaphorical

cable is as long as the range of a Wi-Fi signal broadcast by an access point. The type of Wi-Fi connection mentioned above is established in the Infrastructure mode, which is the most popular mode in real-life usage. Technically, you can skip an access point and make two Wi-Fi clients connect directly to each other, in the Adhoc mode. However, as with using a crossover network cable, this is rather complicated and inefficient. Typically, a good Wi-Fi network is most viable within about feet from the access point. This distance, however, changes based on the power of the devices involved, the environment and most importantly the Wi-Fi standard. The Wi-Fi standard also determines how fast a wireless connection can be and is the reason Wi-Fi gets complicated and confusing, especially when considering the fact there are multiple Wi-Fi frequency bands. These bands are the radio frequencies used by the Wi-Fi standards: Generally, the 5 Ghz band delivers faster data rates but a little less range than the 2. Note that a 60 GHz band is also used but only by the Depending on the standard, some Wi-Fi devices use either the 2. Generally later standards are backward compatible with earlier ones. This was the first commercialized wireless standard. It offers a top speed of 11 Mbps and operates only on the 2. The standard was first available in and is now totally obsolete; Introduced in , the The standard offers the top speed of 54 Mbps but operates on the 2. This standard is supported by access points of later standards. Available since , The standard operates on both 2. There are two types of dual-band routers: On each band, the Wireless-N standard is available in three setups, depending on the number of spatial streams being used: This in turns creates three types of true dual-band routers: N each of the two bands offers a Mbps speed cap , N one band has a Mbps speed cap while the other caps at Mbps and N each of the two bands allows up to Mbps cap speed. In order to create a Wi-Fi connection, both the access point router and the client need to operate on the same frequency band. For example, a 2. Also, a Wi-Fi connection takes place on just one band at a time. If you have a dual-band capable client such as the iPhone 6 with a dual-band router, the two will connect on just one band, likely the 5 Ghz. Sometimes referred to as 5G Wi-Fi, this latest Wi-Fi standard operates only on the 5 GHz frequency band and currently offers Wi-Fi speeds of up to 2, Mbps or even faster with latest chip when used in the quad-stream 4x4 setup. The standard also comes with the 3x3, 2x2, 1x1 setups that cap at 1, Mbps, Mbps and Mbps, respectively. Technically, each spatial stream of the Note that the real-world sustained speeds of wireless standards are always much lower than the theoretical speed cap. This is partly because the cap speed is determined in controlled, interference-free environments. The fastest peak real-world speed of an On the same 5 GHz band, That said, all First introduced in , the Prior to that, it was considered a different type of wireless networking. Operating in the 60 Ghz frequency band, the For this reason, the new standard is a supplement to the existing This is the next generation of Wi-Fi, set to supersede In other words, Ultimately, this means it allows for higher ratio of real-world speed versus theoretical ceiling speed. That said, consumer devices that support Wi-Fi designations Wi-Fi designations are the way networking vendors market their Wi-Fi routers in an effort to differentiate between them. As mentioned above, the top commercial speed of However, in June , Broadcom introduced a new And also for this reason, With more and more advanced Wi-Fi chips being developed, That said, let me state the rule of thumb one more time: The speed of a single network connection one pair is determined by the slowest speed of any of the parties involved. That means if you use an In order to get the top Also right now, the fastest This means getting routers of higher designations are unlikely to bring you benefits in Wi-Fi speeds. This means that, unlike a dual-band AC router that has one 2.

DOWNLOAD PDF ESSENTIAL GUIDE TO HOME NETWORKING TECHNOLOGIES, THE

Chapter 5 : [PDF] Essential Guide to Home Networking Technologies The [Read] Online - Video Dailymoti

Home Networking Technologies The that you could be safe this for free on calendrierdelascience.com Disclaimer, this site dont put ebook downloadable Essential Guide To Home Networking Technologies The on calendrierdelascience.com, this is just book generator result for the preview.

Enjoy this article as well as all of our content, including E-Guides, news, tips and more. Step 2 of 2: You forgot to provide an Email Address. This email address is already registered. You have exceeded the maximum character limit. Please provide a Corporate E-mail Address. Please check the box if you want to proceed. I agree to my information being processed by TechTarget and its Partners to contact me via phone, email, or other means regarding information relevant to my professional interests. I may unsubscribe at any time. Networks allow you to share a single broadband internet connection among multiple computers and PC users, and they are able to share files among computers more easily and share software resources such as diaries. Wireless networking allows you to have a more attractive and arguably safer office environment with fewer cables around. It gives you more flexibility about where you locate your IT kit, and you can use your laptop from anywhere in your office. It also allows you to offer visitors wireless internet access or hot-desk facilities. However, Ethernet-based wired networking can still have the edge over wireless equipment in being more reliable, lower cost and offering faster connection speeds. Wireless signals, on the other hand, can vary depending on the layout of an office, the thickness of the walls and sometimes even the weather. What equipment do I need to set up a basic network? This means that if you have a relatively up-to-date laptop or desktop PC, it should be fairly straightforward to network machines together. Apart from the computers, you will also need some networking equipment, which may be as basic as having a single cable to connect two computers together. This will then allow other PCs and notebooks, which have wireless networking equipment integrated or attached, to pick up the wireless signals and join the local area network LAN. How do I secure the network? You may also choose to use hardware security such as fingerprint recognition, security and password keys, and full disk encryption to further protect the network. You can add additional security packages to protect and maintain the network perimeters, checking for attacks from both the outside and the inside. What else can I use my network for? Apart from file and print operations, you can use your network to share other peripherals such as scanners and copiers. Wireless networks will also allow you to use wide variety of devices such as wireless cameras, and wireless digital multi-media receivers. One challenge in managing wireless networks is that the tools and tech are changing rapidly. This was last published in July Read more on Networking hardware.

Chapter 6 : An Introduction to Networking Terminology, Interfaces, and Protocols | DigitalOcean

Note: Citations are based on reference standards. However, formatting rules can vary widely between applications and fields of interest or study. The specific requirements or preferences of your reviewing publisher, classroom teacher, institution or organization should be applied.

A central hub of operators would sit in one room, and a person would use their home phone to call up the central hub and tell them who they would like to be connected to. The operator would then patch the call through. This hub is known as a network, and you can create one to link together all of your electronic gadgets at home in a few simple steps. What Is a Home Computer Network? A home data network is an electronic communications system linking all of your devices to the Internet and to each other. A home data network can utilize both wired and wireless technologies, connecting all devices to a central point called a hub or a switch. In this way, the devices can communicate with each other. For example, computers can access files and printers on other computers, televisions can play movies or other media stored on your computers, and Internet-enabled devices can connect to programs and services outside of your home. Benefits of Setting Up a Home Network A home network provides you with time efficiency, organization, accessibility, and cost savings. It allows you to utilize a single Internet connection to power a variety of devices while also allowing those devices to effectively interact with each other. And in what is a surprise to many people, beyond computers, there are all sorts of devices that can utilize a home network. Other products that can utilize a home data network include digital video recorders DVRs , Internet-enabled Blu-ray players, video gaming consoles, home automation systems, and networked printers. And even better, unlike your plumbing or electrical systems, creating a home data network will not require professional help. The essential components are readily available and inexpensive, and can be configured by people with modest computer skills. Essential Networking Components of a Home Network 1. With service from your cable company, their coaxial cable connects to your cable modem. In the case of DSL service, their Internet modem connects to your phone line. Keep in mind that you do not have to rent your Internet modem from your provider. You are free to buy one of your own. Ethernet Hub or Switch The Ethernet hub or switch is the heart of a network with numerous Ethernet ports so that wired components can gain access to the Internet via the hub or switch. Think of this device like the power strip you use to connect all of your electrical devices; you will need one port for each device you wish to connect. Once you have acquired a hub or a switch, you merely need to plug it in to the electrical socket and connect the Ethernet cables from the devices on the network. Virtually every computer sold in the past 10 years comes equipped with an Ethernet connection and the cables are so ubiquitous that you can even buy them at The Home Depot. I would highly recommend a switch as traditional hubs are now obsolete with very little difference in cost. When purchasing a switch for home use, look for an unmanaged switch. While many of your network components will be able to connect wirelessly, there are still some that require the traditional Ethernet connection to your hub or switch. Wireless Router Unlike your plumbing and electrical systems, a home data network can be extended to places without a physical connection. To connect your network to devices without running cables, a wireless router is a popular addition to any home network. In fact, a wireless router may have multiple Ethernet ports as well, combining the functionality with that of an Ethernet hub or switch. Once you plug the wireless router into an electrical socket, you must then configure it though your computer. Configuration is a simple task where you give the router a name and enable password authentication. Wireless connections do have some disadvantages. A wireless signal may not penetrate all of the areas of your home, and you therefore may need to deal with weak signals in different parts of the house. Also, older wireless systems will not have the capacity to transmit large streams of data such as high-definition television. Finally, wireless networks need to be secured, which requires some additional setup. When evaluating routers, the wireless signal will be shown as The higher the letter, the higher the bandwidth e. A VoIP device connects from your home telephone system, through your home network, to the

Internet. The result is that your telephone calls are routed through the Internet by one of the many affordable VoIP providers that can offer service for far less than your telephone company. Like the router from your Internet service provider, your VoIP router may need to be configured through your computer with the assistance of your VoIP provider. Media Extenders A media extender is a device that connects to your home network and allows audio and video content to be displayed on your television. The source of this content can be an Internet streaming site, a home media server, or both. Some new Blu-ray players and televisions are pre-equipped to stream content from the Internet. Media extenders should need little or no configuration once they are connected to your media server through your home data network. For more information, check out this guide on how to set up a home media center. A home network is the ideal way to allow your video game console to access the Internet. Alternatively, wireless adapters can be purchased. Home Security Systems Traditional alarm systems contact a central dispatch station through your telephone when your alarm system goes off. Since this is probably the worst possible time to tie up your telephone line, most systems can also route data though the Internet by way of your home network. Some systems will even allow you to monitor and control your home security system through the Internet or through a mobile device. Your home security monitoring service should assist you in configuring your connection to their system. If you want to install video surveillance cameras, these too would transmit their images through a home network that can be viewed on the Internet. This is a standalone unit that contains several inexpensive, internal hard drives. It offers the advantages of greater capacity and redundancy over the hard drive in my computer. Each drive contains a small copy of the data on the other hard drives in such a way that the failure of any single hard drive does not result in the loss of data. Combined, this device can hold far more data than any one hard drive can. I use it to securely store all my movies, music, and photographs. I can also use it to back up files from my computer automatically. It connects to my home network just like any other device and the files can be accessed by my computer or my media extenders. As a separate device, I can also locate it in a more secure part of my house than my computer. A well-designed NAS device should be easily configurable by computers though a simple interface. Networked Printers Traditionally, home printers have attached directly to computers, but many new home printers are network enabled. Both wired and wireless networked printers can be accessed by any computer on the network. Final Word Fifteen years ago, my roommate and I ran Ethernet wires between the bedrooms of our house. By following the simple steps above, you too can inexpensively build a home network that will help you be more efficient â€” and more technologically advanced than your neighbors. Do you have a home network in place? What were some of the biggest challenges in getting it set up, and what are your favorite uses for the network?

Chapter 7 : How Home Networking Works | HowStuffWorks

READ The Essential Guide to Home Networking Technologies by Gerard O Driscoll READ The Essential Guide to Home Networking Technologies Epub READ The Essen Slideshare uses cookies to improve functionality and performance, and to provide you with relevant advertising.

Chapter 8 : How to Set Up a Wireless Network From Start to Finish | Audioholics

The essential guide to home networking technologies. By Gerard O'Driscoll. Topics: Computing and Computers. Publisher: Prentice Hall PTR. Year: OAI identifier.

Chapter 9 : FITPAL for Healthy Networks - CA Technologies

A beginner's guide to network and data plans. Here Are the Key VPN Security Technologies. Article. Essential Settings for Your Home Network Routers.