UNDERSTANDING WIRELESS pdf

1: How do Wireless Networks Work? Webopedia Reference

Pursue a verified certificate for a chance to share your final project and receive $5, USD to implement your wireless idea to improve your community!

Read on to get a clearer picture of what you need to optimize your home network. When do you need a switch? What exactly does a router do? Do you need a router if you have a single computer? Network technology can be quite an arcane area of study but armed with the right terms and a general overview of how devices function on your home network you can deploy your network with confidence. Here is the simplest network configuration available: This user cannot access the internet with a Wi-Fi device thus no access for smart phones, tablets, or other wireless devices and they lose out on the benefits of having a router between their computer and the greater internet. When should you use a router? Given the low cost of home routers and the benefits gained from installing one on your network you should always use a router which almost always includes a firewall feature. Home routers are actually a a combination of three networking components: In a commercial setting the three pieces of hardware are kept separate but consumer routers are almost always a combination of both the routing and switching components with a firewall added in for good measure. At the most basic level a router links two networks together, the network within your home however big or small and the network outside your home in this case, the Internet. The broadband modem provided to you by your ISP is only suited to linking a single computer to the internet and usually does not include any sort of routing or switch functionality. A router performs the following functions: A router manages those multiple connections and ensures that the right packets of information go to the right places. Related to the IP sharing function, NAT modifies the headers in packets of information coming into and out of your network so that they get routed to the proper device. Without DHCP you would have to manually configure and add all the hosts to your network. This means every time a new computer entered the network you would have to manually assign it an address on the network. DHCP does that for you automatically so that when you plug your XBOX into your router, your friend gets on your wireless network, or you add a new computer, an address is assigned with no human interaction required. Routers act as basic firewalls in a variety of ways including automatically rejecting incoming data that is not part of an ongoing exchange between a computer within your network and the outside world. On the other hand, if a sudden burst of port probing comes in from an unknown address your router acts as a bouncer and rejects the requests, effectively cloaking your computers. In addition to the inside-to-outside network functionality outlined above, home routers also act as a network switch. A network switch is a piece of hardware that facilitates communication between computers on an internal network. Without the switching function the devices could talk through the router to the greater internet but not to each otherâ€”something as simple as copying an MP3 from your laptop to your desktop over the network would be impossible. Although the four-port limit on the super majority of home routers was more than enough for most home users, the last 10 years have brought a significant increase in the number of networkable devices within the home. As a side note, historically people often relied on hubs because they were so much cheaper than pricey switches. Because hubs have no management component there are frequent collisions between packets which leads to an overall decrease in performance. Hubs suffer from a number of technical shortcomings which you can read about here. Consumer grade networks switches have fallen in price so steeply over the last 10 years that very few hubs are even manufactured anymore Netgear, one of the largest manufacturers of consumer hubs, no longer even makes them. Because of the shortcomings of network hubs and the low prices of quality consumer-grade network switches we cannot recommend using a hub. Returning to the topic of switches: Unplug the devices from your router, plug all the devices into the switch, and then plug the switch into the router. Your router likely has a four-port switch built into it but that does not mean your new eight-port dedicated switch can replace your routerâ€”you still need the router to mediate between your modem and switch. There are two primary designations we are interested in: Ethernet connection speeds are designated in 10BASE. In order to take full advantage of the maximum speeds all the devices in the transfer chain need to be at or above the speed rating you want. In this situation upgrading the switch would boost your

network performance considerably. Outside of transferring large files and streaming HD video content across your home network there is little need to go out and upgrade all your equipment to Gigabit. Unlike the easy to translate number-as-network-speed designation we find with Ethernet the Wi-Fi designations actually refer to the draft versions of the IEEE Like Ethernet, Wi-Fi speeds are limited by the weakest link in the direct network. If you have an In addition to the speed limitations there is a very pressing reason for abandoning the oldest popular Wi-Fi protocol You must use the same level of encryption on every device in your network and the encryption schemes available to Upgrading your Wi-Fi router and wireless equipment allows you to upgrade your wireless encryption as well as enjoy faster speeds. Also like Ethernet, upgrading to the maximum speedâ€”in this case

UNDERSTANDING WIRELESS pdf

2: Understanding Wireless Scanning - Technical Documentation - Support - Juniper Networks

Understanding wireless adapters A wireless adapter is device that adds wireless connectivity to a laptop or desktop computer. Learn more about some popular wireless adapters here.

The areas outlined with dotted lines indicate the radiation pattern of each of the WAPs, also known as their footprint. In the organization depicted in the figure, these WAPs would typically not be wireless routers, but instead just plain WAPs. They would provide connectivity for the wireless clients to the wired network. The two buildings are far enough away from each other and the organization chose to connect the networks using two WAPs with directional Yagi antennas. Because the Yagi antennas provide high gain and a narrow radiation pattern, it reduces the possibility of someone intercepting the signal unless they are directly between the buildings. Remember this Most WAPs use an omnidirectional antenna. In some situations, administrators use a high-gain directional Yagi antenna to connect two WAPs together. For example, you can connect two buildings with two WAPs using Yagi antennas. Notice that the wireless coverage of WAPs 1, 3, 5, and 6 are all uniform. This indicates they have uniform power levels. However, WAP 2 has a smaller footprint, indicating it has a lower power level. In contrast, WAP 4 has a larger footprint, indicating it has a stronger power level. If you want to reduce the footprint of any WAP, you can reduce the power output because the amount of power used by the WAP determines how far it transmits. Of course, the trade-off is reduced performance for authorized users. If the signal is weak, the negotiated speed is slower. Some users farther away from the WAP may not be able to connect at all. It would be possible to increase the power of all the WAPs to eliminate them. However, this increases the footprint and causes the wireless signal to transmit well beyond the boundaries of the building, which increases the overall risk associated with the wireless network. Another method of changing the footprint is by modifying the position of the antennas. For example, if you position the antennas vertically straight up and down , the signals radiate outward, increasing the footprint. However, if you position the antennas horizontally parallel with the horizon or the floor , the signal radiates up and down more than it radiates outward. This is useful when transmitting a signal between floors of a building, and it also reduces the footprint outside the building. Administrators have competing goals with the footprint. Users want easy access to the WAP, so users prefer a large footprint with strong signals. However, the stronger the signal is, the easier it is for an attacker to eavesdrop and capture network traffic. From a security perspective, the goal is to limit the footprint to prevent attackers from accessing the wireless network from external locations such as a parking lot, while also ensuring that users have adequate access to the WAP. Get Certified Get Ahead: SY Study Guide is an update to the top-selling SY, SY, and SY study guides, which have helped thousands of readers pass the exam the first time they took it. It includes the same elements readers raved about in the previous three versions. Each of the eleven chapters presents topics in an easy to understand manner and includes real-world examples of security principles in action. Over realistic practice test questions with in-depth explanations will help you test your comprehension and readiness for the exam. A 75 question pre-test A 75 question post-test Practice test questions at the end of every chapter. Each practice test question includes a detailed explanation to help you understand the content and the reasoning behind the question. If you plan to pursue any of the advanced security certifications, this guide will also help you lay a solid foundation of security knowledge. This SY study guide is for any IT or security professional interested in advancing in their field, and a must-read for anyone striving to master the basics of IT security. Kindle edition also available. Most common wireless devices use omnidirectional antennas to receive a wireless signal from any direction. However, an attacker can create a directional antenna that can receive wireless traffic from a specific direction. For example, attackers create simple cantennas antennas using a can to capture signals from a specific direction. They connect the wireless receiver to one end of an empty can and simply point the can toward a wireless network. By pointing the cantenna in different directions, they can home in on the exact location of a wireless network. Additionally, they can eavesdrop on wireless conversations even though they are well outside the normal footprint.

UNDERSTANDING WIRELESS pdf

3: Understanding Your WiFi Network | HowStuffWorks

Wireless devices connect using what's known as Wi-Fi, the wireless networking protocol, which is defined in the series of standards. These standards are continually being improved. With the early a, b, and g, being superseded by n and ac, and speeds are continually increasing.

Send We respect your privacy. All email addresses you provide will be used just for sending this story. Oops, we messed up. Everyone from state and local governments to the wireless provider itself. How can you tell which is which? Some of those are expected; some are not. Mobile bills, as pieces of paperwork, tend to be sprawling; this sample from Verizon is nine pages long. If any line on the account had gone over its allotment of talk minutes, text messages, or data use, overage fees would also appear here in a quick-to-view grid. RED numbers 1, 2 are Verizon-originated charges or credits. Account Charges and Credits 1. The data pool is shared among all devices on the plan. On its website, Verizon describes the plan like so: Taxes and fees apply. Many large corporate employers provide some similar mobile plan discount as an employee benefit, usually with the wireless provider that the company uses for its own business needs. Any other applicable credits or refunds to your account, for specific service or billing issues, would appear in this general portion of the bill. This is not a charge for data usage, nor is it any kind of device payment plan. It has nothing whatsoever to do with any usage. Those charges would appear under a different part of the bill or, more likely, would be charged up front at the point of sale. Device Payment Agreement [number] 4b. Device Payment Agreement [different number] When Verizon changed its billing structure in , they did away with the traditional two-year contract and heavily subsidized phone purchase. In our case, one of the phones being paid off over time is an iPhone 6S and the other is a Samsung Galaxy S6. From a consumer perspective, it works out about the same: While Verizon customers who purchase phones through this installment plan are ultimately paying full-price for their devices, they are also paying lower monthly access fees. Usage and Purchase Charges 5. Voice This is where Verizon lists charges for voice minutes used. Most of its available new plans include unlimited voice, but some plans still meter minutes. Verizon confirms that only grandfathered, legacy plans still have metered talk or text. A full breakdown of what numbers each line called or were called by, where those calls originated, when the calls happened, and how long each call lasted appears on subsequent pages of the bill. Most of its available new plans include unlimited texting, but some plans still meter messages. Data This is where Verizon lists how much data each individual line on the account used. If the sum across all phone lines is greater than the monthly plan, you win an overage fee. Both users on this particular account mainly use their phones on WiFi, though, and so their data usage is well within the 3 GB allotment they subscribe to from Verizon. Other purchase and usage charges, like roaming fees, international calling, international travel plans, or charitable donations or purchases made by text message, appear under this section of the bill when incurred. The Universal Service Fund is paid into by telecom operators, who are permitted â€” but not obligated â€” to recoup that cost from consumers. That said, basically all carriers pass through their USF contributions as line-item fees to their subscribers. Just like with the USF fee above, the FCC rules permit â€” but do not require â€” operators to recover regulatory fees from subscribers in monthly installments. But everyone consistently passes this fee through to customers. Verizon uses these charges to pay for costs including property taxes, facility fees, regulatory obligations, and related costs of doing business. The company also says that this is a Verizon fee, not a tax, and that is subject to change. Local BUS Lic Surchg The municipal area where this subscriber lives imposes a Business License Tax on most commercial enterprises with revenue exceeding a certain threshold. Two phone lines on one bill means two fees on one bill. The vast majority of states impose some similar kind of fee. Communication Sales Tax The state where this subscriber lives imposes a sales tax on all wireless phone service, same as they do on landline, cable, and satellite service. Rates may also vary based on county or municipality. Verizon Wireless not your mobile phone provider? This article has been updated to clarify that the author is also on the account of the family whose bill is shown here. This article originally appeared on Consumerist. Try again later Consumer Support.

UNDERSTANDING WIRELESS pdf

4: Understanding Wireless QoS â€“ Part 3 | mrn-cciew

Join Martin Guidry for an in-depth discussion in this video Understanding wireless networks, part of Setting Up a Small-Office Network.

During passive scans, the radio listens for beacons and probe responses. If you use only passive mode, the radio scans once per second, and audits packets on the wireless network. Passive scans are always enabled and cannot be disabled because this capability is also used to connect clients to access points. Active scans are enabled by default but can be disabled in a Radio profile. During active scans, the radio sends probe-any requests probe requests with a null SSID name to solicit probe responses from other devices. In other words, access points actively look for other devices, in addition to listening for them. What Channels Are Scanned? RF scanning can be performed on a variety of different sets of channel ranges or frequencies. The scan can be configured in the Radio profile to scan either operating channels, regulatory channels, or all channels. An access point will never transmit on channels that are not authorized for transmission. In a Radio profile, you can change the channels a radio actively scans. These are the three options for active scanning: Only the current channel is scanned and audited. Only regulatory channels are scanned and audited. If the radio is configured for All channels are scanned and audited. How Does Scanning Work? To scan outside of the operating range, the access point must change channels. These off-channel scans are performed once per second, and a different channel in the range is scanned each second until it cycles through all in-scope channels. Scans are scheduled to avoid interfering with beacon transmission. Radio transmit queues are drained prior to channel change. Then the probes are sent once channel change is completed. Note that the scan frequency is reduced if voice, video traffic, or heavy load is detected. Also, the CTS-to-self feature can be configured to silence clients on the operating channel while access point goes off channel. The active-scan algorithm is sensitive to high-priority voice or video traffic or heavy data traffic. Active-scan scans for 30 milliseconds once every second, unless either of the following conditions is true: High-priority traffic voice or video is present at 64 Kbps or higher. In this case, active-scan scans for 30 milliseconds every 60 seconds. Heavy data traffic is present at 4 Mbps or higher. In this case, active-scan scans for 30 milliseconds every 5 seconds. Active scanning is more thorough and provides more information than passive scanning. If you select active mode, the radio actively sends probes on other channels and then audits the packets on the wireless network. What Happens to Scanned Information? Scanned information is stored and used by the:

UNDERSTANDING WIRELESS pdf

5: Understanding wireless speeds - [Solved] - Networking

Understanding Wireless 1 is a comprehensive course on the world of cellular radio. It is completely up to date, including explanation of the "latest" broadband wireless technology 1XEV-DO. We start with basic radio concepts, understanding "analog radio" and "digital radio", then cover fundamentals of mobile communication networks: base stations.

By comparison, creating a network by pulling wires throughout the walls and ceilings of an office can be labor-intensive and thus expensive. But even when you have a wired network already in place, a wireless network can be a cost-effective way to expand or augment it. The Basics Wireless networks operate using radio frequency RF technology, a frequency within the electromagnetic spectrum associated with radio wave propagation. When an RF current is supplied to an antenna, an electromagnetic field is created that then is able to propagate through space. The cornerstone of a wireless network is a device known as an access point AP. The primary job of an access point is to broadcast a wireless signal that computers can detect and "tune" into. Since wireless networks are usually connected to wired ones, an access point also often serves as a link to the resources available on the a wired network, such as an Internet connection. In order to connect to an access point and join a wireless network, computers must be equipped with wireless network adapters. These are often built right into the computer, but if not, just about any computer or notebook can be made wireless-capable through the use of an add-on adapter plugged into an empty expansion slot, USB port, or in the case of notebooks, a PC Card slot. Wireless Technology Standards Because there are multiple technology standards for wireless networking, it pays to do your homework before buying any equipment. The most common wireless technology standards include the following: The first widely used wireless networking technology, known as In , a follow-on version called Another improved standard called But even though the All of the Wi-Fi variants The catch is that doing so often requires special configuration to accommodate the earlier devices, which in turn can reduce the overall performance of the network. In truth, these performance figures are almost always wildly optimistic. While the official speeds of As a general rule, you should assume that in a best-case scenario you. As you might expect, the closer you are to an access point, the stronger the signal and the faster the connection speed. The range and speed you get out of wireless network will also depend on the kind of environment in which it operates. And that brings us to the subject of interference. Wireless Interference Interference is an issue with any form of radio communication, and a wireless network is no exception. Similarly, devices like microwave ovens and some cordless phones can cause interference because they operate in the same 2. When it does, you can usually minimize the interference by relocating wireless networking hardware or using specialized antennas. Data Security on Wireless Networks In the same way that all you need to pick up a local radio station is a radio, all anyone needs to detect a wireless network within nearby range is a wireless-equipped computer. WEP is the oldest and least secure method and should be avoided. WPA and WPA2 are good choices, but provide better protection when you use longer and more complex passwords all devices on a wireless network must use the same kind of encryption and be configured with the same password. Unless you intend to provide public access to your wireless network â€” and put your business data or your own personal data at risk â€” you should consider encryption mandatory. Adapted article courtesy of SmallBusinessComputing.

UNDERSTANDING WIRELESS pdf

6: Wireless Security Alarms | Home Security Systems by ADT

+ Mbps wireless is only a theory figure and its likely your actual connection will be lower than despite your best efforts. But like the above post says your internet will never achieve.

One factor that people may consider is whether to install a wired or wireless security system. Both a wired and a wireless home security system can be monitored by a professional security company. Both can be installed as a DIY project or by a professional, although an experienced security professional, such as ADT, is often recommended if you want to add sensors, remote arm and disarm, etc. Wired security systems and wireless security systems can be equally effective, but each has its own advantages and disadvantages. Wireless home security systems use radio waves, rather than wires or cables, to communicate between the control panel, sensors and cameras. Disadvantages of Wired Systems Wired systems can be time consuming and more expensive to install. It can be difficult or impossible to hide all the wiring when installed in an existing home. Once installed, it can be difficult to remove and take with you if you should move. Since wireless systems do not have to be hard-wired and have their own batteries, they can be installed in locations in a home where there are no wires or electrical access. The system can be expanded wirelessly as needed. Disadvantages of Wireless Systems Wireless sensors will need batteries to operate, so while battery life can be several years, the batteries will die if they are not checked. Wireless sensors need to be within a certain distance of the central control panel. This can limit where some sensors are placed. Radio frequency signals sent to and from wireless sensors may be susceptible to incidental interference, including interference from other devices that communicate using radio waves, such as baby monitors. ADT can offer an additional component that has been primarily used to address range issues but may be able to lessen the risk of any compromising of the wireless communication with peripherals, but it is not compatible with all security systems. Please talk to your ADT sales representative for more information and for a quote. Installation When it comes to installation, a wireless security system can be less time consuming when compared to hard-wired systems. In the hard-wired setup, wires must be run through the home to every device and sensor, which includes all door, window, motion and glass-break sensors. Wireless home security systems tend to be easier to install, and wireless DIY systems are portable, so in the event of a move, you can easily take the wireless DIY system with you. The Winner You are.

7: Understanding wireless adapters | CenturyLink Internet Help

Understanding Wireless Encryption and Ciphers Wireless network security relies on a combination of encryption, authentication, and authorization to provide maximum protection for a WLAN. Encryption is focused on protecting the information within a session, reading information in a data stream and altering it to make it unreadable to users.

8: Understanding Wireless Performance and Coverage - Cisco Meraki

Understanding Network Roaming Roaming occurs when you access the network of a different wireless service provider. If your phone signal or the nearest cell site's signal is too weak, roaming can occur automatically, even within your calling plan's area.

9: Solved: Understanding Wireless Mac Address - Cisco Community

For a more in-depth understanding of IP addresses, read What is an IP address? There are also a couple of important terms related to WiFi that you should know. A service set identifier (SSID) is the name that identifies a wireless network.

UNDERSTANDING WIRELESS pdf

The gate unlocked Living with Killer Bees Fat a cultural history of obesity American Mercury Magazine, May to August 1927 The Race Against Dry Grass Wide Slumber for Lepidopterists English-Russian glossary of selected terms in preventive toxicology Toni Morrison (SparkNotes Library of Great Authors (SparkNotes Library of Great Authors) My dad wished he had one of those Sanitized History The Adventures of Matt, Crowbar and Shane in the Lost City by the Bay Paradise Lost: John Milton Types of decision making in management A vindication of the character and condition of the females employed in the Lowell mills Iti machinist resume Tourette Syndrome A Medical Dictionary, Bibliography, and Annotated Research Guide to Internet References Spanish 8 Lessons (Basic) The Holy Warrior/The Reluctant Bridegroom/The Last Confederate/The Dixie Widow/The Wounded Yankee (The Ho Alien objects, human subjects Corporatism and the myth of consensus Columbia point peninsula: a proposal for the revitalization of columbia point peninsula. Lewis Henry Morgan and the Invention of Kinship, New Edition The Fibromyalgia Solution Learning impairment vs learning disability In vitro fertilization and other assisted reproduction Cam Jansen and the Ghostly Mystery (Cam Jansen) Point of power 30: God will grant me rest when I guard my heart Invigorating Defense Department governance Helluva town : my New York 1943 to 1976 by Alan Rich The beginning through pre-divestiture The Caedmon Poetry Collection Joel H. Johnsons Mormon sawmill Nier automata world guide art collection Centers for medicare for medicaid services cms report A tale of a hero and the song of her sword Burnt Cork and Tambourines Modern Painters Part Two Time for a revolution Kevin Y.L. Tan World war ii soviet armed forces 3 Mexican Blackletter