DOWNLOAD PDF AS/400 WIRELESS LAN PRODUCTS FAMILY CONFIGURATION EXAMPLES,TIPS AND TECHNIQUES

Chapter 1 : Free Professional and Technical Research Library of White Papers, Magazines, Reports, and e

*As/ Wireless Lan Products Family Configuration Examples, Tips and Techniques [IBM Redbooks] on racedaydvl.com *FREE* shipping on qualifying offers.*

Disclaimer Due to increased demand for convenient networking and more flexible access to both the Internet and company resources via more geographically widespread coverage areas, wireless networking use has dramatically increased in recent years. Mobile access to data services previously unavailable is now common. The sales and penetration of wireless access have resulted in a recent projection by ABI Research that one billion Wi-Fi chipsets will ship in the year Not only has wireless data access achieved a great deal of market penetration in recent years, but the price of the related hardware has dropped dramatically, making it even more accessible. Wi-Fi seems to be everywhere; in laptops, desktops, PDAs, cell phones and routers, and there is such a large amount of wireless networks in many urban areas that complete overcrowding of the public radio spectrum in use can occur. This guide provides a high-level overview of the past, present, and future of IEEE Although the specific wireless technology based on IEEE Parts of this guide contain detailed information specific to Fedora Documentation and other Linux operating systems, however, many of the topics and concepts relate to all operating systems, vendors, and environments. Who should read this guide? You should read this guide if you are looking for an overview of wireless technologies and how they are implemented in Fedora Documentation or other Linux operating systems. Other readers will gain general information on how wireless works, the hardware involved, and other topics such as standards and security. What is a Wireless LAN? A wireless LAN referred to as WLAN in this guide is a wireless local area network that allows computers or other devices to communicate via radio frequency RF technology. It affords the user mobility to move around and stay connected to the network without using physical cables such as in a traditional Ethernet system. The IEEE Institute of Electrical and Electronics Engineers is a non-profit, global organization which implemented and continually develops a set of standards for wireless communication. This family of standards is known as IEEE Standards are discussed in more detail later. Although wireless networks are commonly referred to as Wi-Fi, this is only a marketing term chosen by the Wireless Ethernet Compatibility Alliance now known as the Wi-Fi Alliance. History of Wireless LANs Although wireless communications are nothing new, Norman Abramson, as a professor at the University of Hawaii, led the development of what is acknowledged as the first computer network using wireless communications, in With more available devices, higher data rates and cheaper hardware, wireless access has now become widespread. The IEEE recently ratified This amendment addresses several performance and security issues and is covered later in this guide. Also, the installation of a WLAN is in many cases easier than a wired network, because of the lack of a need to install actual cables in wall fittings and data centers. A properly designed WLAN can be installed relatively quickly and can also be transported to a new location more easily. Considerations Wireless LANs introduce several deployment and usability factors that should be considered. An Ethernet system generally has its electrical current traveling neatly bounded inside a wire. The performance and reliability of a wireless LAN is dependent on atmospheric conditions, physical obstructions, other WLANs, RF interference, RF propagation characteristics and the basic laws of physics. The use of a WLAN is therefore generally not as reliable or as fast as a wired system, however recent developments in the communications standards that actually use some of these atmospheric anomalies to their advantage have alleviated the problems to a degree. The reliability and performance of a WLAN depends on correct deployment which has all of these conditions taken into account. Security concerns are also a factor. A WLAN spreads to coverage areas outside that of a controlled wired system, and is much less predictable. For instance, many wireless networks used in the home can be detected from the street outside. A business may inadvertently make their network available to a competitor in an adjacent building. Hence, several security mechanisms exist for IEEE These are covered later. Linux Wireless Support Linux supports many wireless devices. Many of these adapters are supported by

default in the Linux kernel via open source drivers available in Fedora Documentation. Your device is most likely supported; however, to find an overview of devices and drivers currently supported in Linux and Fedora Documentation, refer to the following URL at Linuxwireless. Disclaimer Any products pictured or otherwise referred to in this guide are provided for reference purposes only, and no endorsement or guarantees of supportability are intended. These bodies develop and implement standards and regulations that include limits on factors such as power output, antenna height, hardware compatibility, frequency allocation and usage and general spectrum management. This chapter gives an overview of these bodies and their responsibilities. Note that local regulations may exist in your area that may differ from those listed here. When deploying a WLAN, the requirements of your local regulatory domain authority should always be adhered to. The ITU-R manages worldwide spectrum management and satellite orbits and keeps the interference-free operation of communications as its primary objective. More information can be found at the ITU-R homepage: Wi-Fi Alliance - A non-profit, worldwide association consisting of more than member companies from more than 20 countries. This is done by performing a series of certification testing on products. Details about Wi-Fi Alliance certifications and programs can be found at http: IEEE - The Institute of Electrical and Electronics Engineers is a global, non-profit organization, with more than , members from more than countries. The IEEE is a professional group working towards the advancement of technology, to "foster technological innovation and excellence for the benefit of humanity. More information about the IEEE and the Equipment that conforms to this standard is considered legacy and is no longer being manufactured. It is, however, considered the baseline for IEEE The most recent revision of the This standard sparked a huge increase of WLAN adoption, and is considered as one of the main catalysts for the popularity of Wi-Fi today. Equipment that operates under this standard is not compatible with The higher frequency in use by Equipment conforming to this As it uses the same 2. Devices operating under the This technology uses multiple antennas and multiple wireless connections to achieve these rates, and is much more resistant to interference without requiring a significant increase in power used to transmit the data. MIMO also presents the ability to use multipath an atmospheric anomaly where a single signal takes different paths and arrives at the receiver at slightly different times, causing a negative factor on performance when using older standards to its advantage. Many products existed on the market before the standard was fully ratified; often known as "Pre N" or "Draft N", these devices are not guaranteed to fully operate under, or be compatible with, specifications of the completed standard. These draft devices are also not guaranteed to be compatible across differing vendors. At the time of writing, there are concerns that

Chapter 2 : Practical Programming for AS/ FTP Automated Interfaces

AS/ Wireless LAN Products Family: Configuration Examples,Tips and Techniques ATM Configuration Examples An Industry Around the Tivoli Framework: Examples from the 10/Plus Association.

The WEP algorithm is intended to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network. WEP encrypts the payload of data packets. Management and control frames are always transmitted in the clear. WEP uses the RC4 encryption algorithm. The shared-secret key is either 40 or bits long. The key is chosen by the system administrator. In the ad hoc mode, each station is a peer to the other stations and communicates directly with other stations within the network. No AP is involved. All stations can send Beacon and Probe frames. A station in the infrastructure mode communicates only with an AP. Together they operate as a fully connected wireless network. This field uniquely identifies each BSS. Both the station and AP radiate and gather The format of frames is illustrated below. Most of the frames contain IP packets. The other frames are for the management and control of the wireless connection. The management frames establish and maintain communications. These are of Association request, Association response, Reassociation request, Reassociation response, Probe request, Probe response, Beacon, Announcement traffic indication message, Disassociation, Authentication, Deauthentication types. The SSID is part of several of the management frames. The control frames help in the delivery of data. The payload part of the datagram is WEP-encrypted. In the open system authentication, all stations are authenticated without any checking. A station A sends an Authentication management frame that contains the identity of A, to station B. Station B replies with a frame that indicates recognition, addressed to A. The shared key authentication uses a standard challenge and response along with a shared secret key. All the APs transmit Beacon frames a few times each second that contain the SSID, time, capabilities, supported rates, and other information. The association is a two-step process. A station that is currently unauthenticated and unassociated listens for Beacon frames. The station selects a BSS to join. The station and the AP mutually authenticate themselves by exchanging Authentication management frames. The client is now authenticated, but unassociated. In the second step, the station sends an Association Request frame, to which the AP responds with an Association Response frame that includes an Association ID to the station. The station is now authenticated and associated. A station can be authenticated with several APs at the same time, but associated with at most one AP at any time. There is no state where a station is associated but not authenticated. Sniffing is eavesdropping on the network. A packet sniffer is a program that intercepts and decodes network traffic broadcast through a medium. Sniffing is the act by a machine S of making copies of a network packet sent by machine A intended to be received by machine B. Sniffing has long been a reconnaissance technique used in wired networks. Attackers sniff the frames necessary to enable the exploits described in later sections. Sniffing is the underlying technique used in tools that monitor the health of a network. Sniffing can also help find the easy kill as in scanning for open access points that allow anyone to connect, or capturing the passwords used in a connection session that does not even use WEP, or in telnet, rlogin and ftp connections. It is easier to sniff wireless networks than wired ones. It is easy to sniff the wireless traffic of a building by setting shop in a car parked in a lot as far away as a mile, or while driving around the block. In a wired network, the attacker must find a way to install a sniffer on one or more of the hosts in the targeted subnet. Depending on the equipment used in a LAN, a sniffer needs to be run either on the victim machine whose traffic is of interest or on some other host in the same subnet as the victim. An attacker at large on the Internet has other techniques that make it possible to install a sniffer remotely on the victim machine. A passive network scanner instructs the wireless card to listen to each channel for a few messages. This does not reveal the presence of the scanner. An attacker can passively scan without transmitting at all. Several modes of a station permit this. This is analogous to placing a wired Ethernet card in promiscuous mode. This mode is not enabled by default. Some wireless cards on the market today have disabled this feature in the default

firmware. One can buy wireless cards whose firmware and corresponding driver software together permit reading of all raw A station in monitor mode can capture packets without associating with an AP or ad-hoc network. The so-called promiscuous mode allows the capture of all wireless packets of an associated network. In this mode, packets cannot be read until authentication and association are completed. An example sniffer is Kismet http: Recall that management frames are always in the clear, even when WEP is enabled. To such a request, there will be an Associate Response frame from the AP. Both frames will contain the SSID in the clear, and the attacker sniffs these. Normal association then begins. The attacker can also chose to actively probe by injecting frames that he constructs, and then sniffs the response as described in a later section. The source and destination MAC addresses are always in the clear in all the frames. There are two reasons why an attacker would collect MAC addresses of stations and APs participating in a wireless network. Often, the shared key can be discovered by guesswork based on a certain amount of social engineering regarding the administrator who configures the wireless LAN and all its users. Some client software stores the WEP keys in the operating system registry or initialization scripts. In the following, we assume that the attacker was unsuccessful in obtaining the key in this manner. The attacker then employs systematic procedures in cracking the WEP. For this purpose, a large number millions of frames need to be collected because of the way WEP works. The wireless device generates on the fly an Initialization Vector IV of bits. Adding these bits to the shared-secret key of either 40 or bits, we often speak of , or bit encryption. WEP generates a pseudo-random key stream from the shared secret key and the IV. It is then exclusive-ORed with the pseudo-random key stream to produce the cipher text. The IV is appended in the clear to the cipher text and transmitted. The receiver extracts the IV, uses the secret key to re-generate the random key stream, and exclusive-ORs the received cipher text to yield the original plaintext. Certain cards are so simplistic that they start their IV as 0 and increment it by 1 for each frame, resetting in between for some events. Even the better cards generate weak IVs from which the first few bytes of the shared key can be computed after statistical analyses. Some implementations generate fewer mathematically weak vectors than others do. The attacker sniffs a large number of frames from a single BSS. These frames all use the same key. The number of encrypted frames that were mathematically weak is a small percentage of all frames. In a collection of a million frames, there may only be a hundred mathematically weak frames. It is conceivable that the collection may take a few hours to several days depending on how busy the WLAN is. Given a sufficient number of mathematically weak frames, the systematic computation that exposes the bytes of the secret key is intensive. However, an attacker can employ powerful computers. On an average PC, this may take a few seconds to hours. The storage of the large numbers of frames is in the several hundred-mega bytes to a few giga bytes range.

Chapter 3 : HP ProDesk G4 Microtower Business PC Specifications | HPÂ® Customer Support

AS/ Wireless LAN Products Family: Configuration Examples,Tips and Techniques The OS/2 Debugging Handbook - Volume III System Trace Reference IBM TotalStorage Copy Services and System i5 Setup examples using DS CLI.

In this case, I have used a template that a program then changes. You can build it however you want, as long as the FTP syntax is correct. This way, when the job ends the customized file and member containing the user profile and password to the remote system disappear with the end of the job. Others may choose to create all the records at the last minute, not using a template. I have found it convenient to read it in a program and analyze the FTP responses to figure out if the transfer was successful. As it turns out, you will notice in an automated process, knowing if you are successful in your transfer is just as important as transferring the data itself. You can send a file for example from one library to another on the same system. This relationship goes both ways, i. Most times, having just the User Profile and the Password is enough. However, some operating systems and their FTP servers are more picky. If the system you are communicating with has a case-sensitive password, you could get frustrating experiences of not getting in even if you have the correct password however in incorrect case, e. The error message will not tell you anything too explicit. In this case, the transmission was successful. Here, the success message is , "File transfer completed successfully". The text in the code and other FTP return codes can vary depending on the system you are communicating with. Once saying "Now using naming format "0" and once saying "File transfer completed successfully". These are subtle differences, but basically you should check the message number rather than the text with your error checking program. When you write your error checking program it is a good idea to experiment first and check for the success messages that you can expect from what ever combination of systems you are transferring from and to. Note the differences in how the output can vary when communicating with one system or the other. TXT" 46 bytes Rather, we got a message, its equivalent. This is another illustration of how different systems can respond. Again, a reminder to test and try the communication manually to see what you get message-wise when you transmit data between any two systems. Of course, you can code an FTP result checking application that can check for and return codes. This is probably the best thing to do. Here is an example of a failed transmission. The easiest way to know that things went wrong is that you will not find in this OUTPUT member any successful completion message. Failing to find such a message, your program can notify you for failure.

Chapter 4 : Hacking Techniques in Wireless Networks

Listen with Audible. Sponsored. Genres.

Accordingly, a router is configured with a public access profile or profiles , which may be selectively enabled or disabled. When enabled, the router sends out an identifier that can be used to associate a client device with a public i. The router also sends out a conventional identifier that can be used to associate another client device with a secured i. WiFi has become very popular among businesses and consumers as an alternative to a wired network configuration. Depending on which Devices conforming to In one alternative aspect, the specifying specifies a plurality of public access profiles for the WAP; the adapting selectively enables or disables each of the public access profiles; and the transmitting of the public access identifier comprises transmitting a public access identifier representing a public access path through the WAP to the computer network for each of the public access profiles that is enabled. This aspect may further comprise: The public access path and the authenticated access path may be simultaneously provided by the WAP. In this and other aspects, the WAP may optionally restrict access to services provided by the WAP, for a guest client device that connects to the WAP using the public access identifier, and not restrict access to the services for an authenticated client device that connects to the WAP using the authenticated access identifier. In another aspect, an embodiment of the present invention provides public access to a network through a wireless router, comprising: In yet another aspect, an embodiment of the present invention provides public access to a network through a WAP, comprising: The foregoing is a summary and thus contains, by necessity, simplifications, generalizations, and omissions of detail; consequently, those skilled in the art will appreciate that the summary is illustrative only and is not intended to be in any way limiting. Other aspects, inventive features, and advantages of the present invention, as defined by the appended claims, will become apparent in the non-limiting detailed description set forth below. The present invention will be described with reference to the following drawings, in which like reference numbers denote the same element throughout. WiFi devices are being embraced by everyday people who love the convenience of being mobile. Mass production has made WiFi devices so inexpensive that WiFi is being widely used for networking in many places, replacing the high-cost special wiring of the past and allowing people to easily move their computing workspace on a moment-to-moment whim. In addition to its popularity in small offices and for in-home networks, public places where WiFi access is commonly available include hotels, airports, coffee shops, and so forth. As shown therein, devices , , access a wired network through various access points WiFi access points may be implemented using wireless routers, which typically also act as firewalls and switches. When a WiFi client i. First, the client searches for available routers Block In either case, the client receives information sent from each router within range of this client, where the received information identifies the router and enables the client to attempt a connection request to that router. A default SSID is commonly set by the router manufacturer, and this default value can then be changed e. Commonly, the SSID is changed to descriptive text that describes the network for which this router provides access. The SSID of each router detected by a client device is typically displayed on a user interface of the client device, enabling a user of the client device to make a selection from among these routers. In this example, user interface presents SSID values from 3 routers that are within range of a hypothetical client device; see reference numbers Once the user selects a router associated with a particular SSID, the client device attempts a connection to that router i. This is referred to in FIG. As part of the connection protocol, the client device may be authenticated to the router. WiFi networks generally use one of the following authentication methods: By default, routers are typically sold without an authentication key e. In this case, client devices that do not provide the proper authentication key value during authentication will be denied access to the network. In the shared-key authentication approach, the client may obtain the authentication key from the router during a challenge message exchange details of which are not deemed necessary to an understanding of the present invention. In the pre-shared-key

approach, the client already has the authentication key, and provides this to the router without requiring a challenge message exchange. Upon receiving the authentication key from the client device, the router performs an authentication process for that client. Block tests whether the authentication is successful. If so, then the client is allowed access Block ; as stated above, no actual authentication is performed for open-system authentication, and thus all client devices will successfully complete this open-system authentication process. If the test in Block has a negative result, however indicating that the client device did not supply the correct authentication key , access to the network through this router is denied Block When the authentication succeeds, the client proceeds to an association process which sets up a logical session over which higher-layer protocols and data may flow not shown in FIG. At any point thereafter, either the router or the client may terminate the association, shutting down further data communications. After the association is terminated, no further data communication can occur until the aforementioned synchronization protocol is repeated to join the network anew. The above-discussed authentication process is carried out by an authentication layer of the router. The channel ID is commonly used to prevent interference among routers that are located in close proximity to one another. As discussed above, the authentication mechanism â€”which comprises the open-system approach, the shared-key approach, or the pre-shared key approachâ€”indicates what type of authentication is used when authenticating a client device to the router, and the authentication key is used in this process. The routing mechanism within router consults its routing table to find a path to the destination of the incoming traffic, as represented generally at Traffic sent from the network to a client , then traverses a return path through the router to that client. Presently, routers come with capability for a single wireless access configuration. As has been described above, this access configuration can be set to open-system i. Using techniques disclosed herein, routers can provide multiple types of accessâ€”that is, unprotected access as well as protected accessâ€”simultaneously. Optionally, an embodiment of the present invention may come with the public access configuration already enabled, by default. In another embodiment, routers may come with multiple profiles, beyond a single public access profile and a single secured-access profile, and configuring and using a router having multiple profiles is discussed in more detail below with reference to FIG. In this manner, WiFi access can be widely supported by leveraging router devices that may be for example operating in households throughout a neighborhood, in businesses throughout a business district, and so forth. WiFi devices can therefore operate in any location where such routers are deployed with public access configuration enabled, even though the router may also be using authentication to provide secure access to a network. Using techniques disclosed herein that provide public access through secured-access routers, the public-access coverage can thus be extended without requiring an increase in the number of router devices that are deployed. Using existing techniques, users of VOIP phones therefore need to ensure that their phone is within range of a WiFi router or access point; otherwise, the phone cannot be used. These existing handoff protocols occur using techniques which are not deemed necessary to an understanding of the present invention. This configuration interface provides for changing the SSID see and channel see , and for selecting one of the authentication mechanisms see Any one of 4 authentication keys may be specified from this sample interface, as shown at ; a drop-down box allows the user to select the encoding in which the keys are specified. In this sample interface , a set of radio button graphics is depicted at , and these radio buttons are used to enable or disable a public WiFi access path provided by one embodiment of the present invention. When a public access path is enabled, the router can simultaneously support secured and unsecured access, thus providing one access path for clients that are authenticated and another access path for clients that are not authenticated respectively , as will now be discussed in more detail. As has been discussed above with reference to FIG. See Block , corresponding to a client that will use a public access path, and Block , corresponding to a client that will use a secured access path. Accordingly, one physical router may appear to a client as two or more distinct available access paths and will thus be represented by two or more distinct entries on user interface This is illustrated in FIG. Note, however, that in some scenarios, routers might not be represented by an SSID for an authenticated access path in this list Preferably, for those routers providing authenticated access paths, the

corresponding SSID values are shown in a conventional manner on user interface Techniques are known in the art for visually distinguishing those routers that provide an authenticated access path from those routers that provide an unauthenticated access path such as displaying a graphic representing a padlock for authenticated-access SSIDs. In one approach to guest access, as shown in FIG. For a client that will authenticate to the router, Block indicates that this client also searches for available routers. A user interface such as of FIG. Upon the user selecting one of the authenticated access paths represented by a particular SSID value, the client associates with that SSID and the corresponding authentication key which, as discussed above with reference to Block of FIG. As indicated by Block , the router verifies the authentication key, and if this verification is successful, control transfers to Block which indicates that the router grants secured access rights to this client. If the verification fails, on the other hand, Block indicates that the client is denied access rights. As shown in FIG. As discussed with reference to FIG. The authentication process for clients , is carried out by an authentication mechanism of an authentication layer , which is preferably analogous to the authentication layer discussed above with reference to FIG. See of FIG. Because router does not execute the authentication process for guest client , FIG. The routing mechanism within router is preferably similar to routing mechanism of FIG. Traffic sent from the network to a client , , then traverses a return path through the router to that client. In an optional aspect, services provided to guests clients may be restricted as compared to services provided to authenticated clients, as will now be described. In one approach, a bandwidth restriction feature may be implemented that restricts access to bandwidth for guest clients. As one example, available bandwidth may be divided between traffic pertaining to i. For example, guest clients might be limited to transmission at a rate of kilobits per second, whereas traffic pertaining to authenticated clients might be transmitted at a rate of several megabits per second, so that the guest clients are not able to take all of the available bandwidth to the disadvantage of the authenticated clients. Router may implement this bandwidth restriction feature in one approach by building a list of network addresses corresponding to guest clients, and using the restricted portion of the bandwidth for traffic that pertains to the network addresses on this list. In another approach, a router priority feature may be implemented whereby authenticated clients receive higher priority than guest clients. For example, traffic pertaining to guest clients may be buffered while the router processes traffic for authenticated clients. A router might use a round-robin scheduling approach to performing path lookups in its routing table, as one example, whereby it iteratively processes path lookups pertaining to 5 authenticated clients and then processes a path lookup for 1 guest client. A quality of service indicator associated with the packets processed by the router may be used, if desired, to determine how to prioritize among the packets to provide this priority handling, whereby the indicator is set higher for authenticated clients than for guest clients. In yet another approach, a port restriction feature may be implemented that restricts access to ports for guest clients. As another example, guest clients may be denied access to other port numbers. In another optional aspect, encryption may be handled differently for guests clients as compared to encryption for authenticated clients. In one approach, encryption of traffic to and from guest clients is not supported by router In another approach, encryption may be provided to and from the router, thereby providing privacy for traffic sent over this wireless link but for those client devices which access the router as guest clients, the router will route traffic to the public network but will not route traffic into the private portion of the network. Authentication keys might be used for differentiating between guest clients and authenticated clients. For example, a client device might be provided with one key that authorizes this client to access the internal or local network connected to that router, whereas a second client device might be provided with a different key that only authorizes this second client to use guest access privileges that is, to access a public network which is connected to the same router. In one approach, the key that authorizes the authenticated client to access the internal network may be distributed to the client device out of band i. In an alternate embodiment, link privacy could be established to the guest without prior key exchange, for example by using a well-known ad hoc key negotiation protocol such as a Diffie-Hellman key exchange details of which are not deemed necessary to an understanding of the present invention.

DOWNLOAD PDF AS/400 WIRELESS LAN PRODUCTS FAMILY CONFIGURATION EXAMPLES,TIPS AND TECHNIQUES

Chapter 5 : USA1 - Wireless Public Network Access - Google Patents

AS/ Wireless LAN Products Family: Configuration Examples,Tips and Techniques by Ibm ATM Configuration Examples by Ibm Build a Portal with Domino: A S/ Example by Ibm.

Click here for a sample chapter for this book: Chapters end with From Here and Notes. Types of Cable and Hardware. Copper, Fiber, or Wireless Media: Unshielded Twisted Pair Cabling. The Right Fiber Optic Cable. Fiber Optic Receiver Specifications. Fiber Optic Cable Connectors. Copper Versus Fiber Cable. The Public Domain Internet. A Cost-Effective and Timely Solution. Integrating Information Design with Business Planning. Network Cabling Standards Organizations. How Does it Work? DSL versus Cable Modems. DSL Progress is Thwarted. Planning Implications for the Enterprise Network Manager. Enterprise Network Management Capabilities. Enterprise Network Management Architecture. Lucent Technologies Cabling System Solutions. Gigabit Cabling System Solutions. Customer Sales and Service. Distributed and Mobile Workforce. Multimedia Messaging and Response. Power Sum Cables, Connectors, and Systems. Millennium Technologies of New Boston. Installation Planning and Practices. Main Types of Physical Topologies. Multiple Wiring Closets with Backbone Connection. Backbone Cabling Services Evaluation. Bridging the Ethernet Gap. Network Design Documentation Issues. Network Design Standards and Technology Issues. Cisco Systems Network Design Issues. Cost Justification and Consideration. The Fiber Cabling Cost Curve. The Good without the Bad and the Ugly. Designing Distributed Cabling System Standards. New Standards Design Issues. Category 6 or Category 7. Complexity of Information Technology. Distribution and Electrical Needs. Specialized Types of Circuits. Building or Structured Cabling Considerations. Equipment Rooms or Wiring Closets. Typical Floor Distribution Cabling Systems. Different Media for Physical Layer. Shielded versus Unshielded Cables. Data Link Layer Standard. Category 5 Cables are Created Equal. Wide Area Interconnection of Heterogeneous Networks. Reasons for Wireless ATM. Wireless Communications Hardware and Applications. Wireless Access to Enhanced Emergency Services. The Future of Wireless. Fiber Types and Materials. How Fibers Guide Light: Light Rays and Light Waves. How Single Mode and Multimode are Different. Trading Ease for Highest Performance. Planning and Investing for the Future. When Should Collisions Take Place? Microseconds, Bytes, and Bits. Loss and Attenuation of Fibers. Understanding How Loss is Measured: Sources for Loss Measurements. Using a Loss Test Set: Optical Power versus Attenuation: The Capacity for Information. The Effect on Measurements. When Bandwidth is an Issue. Physical Sizes of Fiber. Dealing with Manufacturing Tolerances: Choosing a Launch Cable for Testing. Using Fiber Optic Transmitters and Receivers. Light Sources Used in the Field. Detecting Light with Photodiodes. Choosing the Right Detector. What to Look for in Test Instrumentation. Connection, Identification, and Installation. Why Tight Buffer is Common. Testing Tips and Techniques. Handling and Cleaning Procedures. Examining Cable Plant Loss. Troubleshooting Fiber Optic Systems. Knowing When to Troubleshoot. Common Steps to Identify the Problem. Surviving with Fiber Optics. Optical Time Domain Reflectometer. Understanding the Physics and Errors of the Measurement. Special Consideration for Multimode Fiber. Measuring Fiber, Not Cable Distance. Relying on Your Own Interpretation. This Trick Can Help. Selecting Connectors and Splices. Identifying Different Types of Connectors. Widespread Fiber Optic Connectors. Fusion and Mechanical Splices. Pros and Cons of Mechanical Splicing.

DOWNLOAD PDF AS/400 WIRELESS LAN PRODUCTS FAMILY CONFIGURATION EXAMPLES,TIPS AND TECHNIQUES

Chapter 6 : Network Diagram Templates | Editable Online or Download for Free | Creately

Buy As/ Wireless Lan Products Family Configuration Examples, Tips and Techniques by IBM Redbooks (ISBN:) from Amazon's Book Store. Everyday low prices and free delivery on eligible orders.

Tweet It Introduction Networks carry all sorts of confidential data, so security is a highly important part of any wireless network structure. Security ensures that the same level of data integrity and confidentiality as a wired network are maintained. Without properly implemented security measures, any wireless network adapter coming within range of another network adapter or access point can join the network. I once did a little research of my own and found that 3 out of 5 of the public access points I checked had either no security at all or WEP - which allowed me to crack the key within 15 minutes using freely available tools on the Internet. So why is there such a high lack of security? To overlook wireless security is like leaving the front door to your house permanently open. With the introduction of push-button security for home user products, we can expect to see an increase in the implementation of wireless security among wireless router users. The main aim behind push-button security is to provide a simplified and enhanced method of setting up and building a home network. With so many people â€" particularly home users â€" failing to notice the importance of security as part of their wireless network building, push-button becomes a means of enabling some form of security with a click of the mouse or touch of a button. While one may begin to question the strength of such security, another will remind you that something is better than nothing at all! Wireless Security Threats What are the threats that we face today with regards to wireless networks? An informative list has been compiled by the National Institute of Standards and Technology as part of their documentation on Wireless Security. Hereunder is an extract from that document. To date, the list below includes some of the more salient threats and vulnerabilities of wireless systems: All the vulnerabilities that exist in a conventional wired network apply to wireless technologies. Sensitive information that is not encrypted or that is encrypted with poor cryptographic techniques and that is transmitted between two wireless devices may be intercepted and disclosed. Denial of service DoS attacks may be directed at wireless connections or devices. Sensitive data may be corrupted during improper synchronization. Malicious entities may be able to violate the privacy of legitimate users and be able to track their physical movements. Malicious entities may deploy unauthorized equipment e. Handheld devices are easily stolen and can reveal sensitive information. Data may be extracted without detection from improperly configured devices. Viruses or other malicious code may corrupt data on a wireless device and be subsequently introduced to a wired network connection. Malicious entities may, through wireless connections, connect to other agencies for the purposes of launching attacks and concealing their activity. Interlopers, from inside or out, may be able to gain connectivity to network management controls and thereby disable or disrupt operations. Internal attacks may be possible via ad hoc transmissions. As with wired networks, agency officials need to be aware of liability issues for the loss of sensitive information or for any attacks launched from a compromised network. One prime example would be, with reference to the above point about how handheld devices are easy stolen - we can take the simple preventative measures to combat such a threat. Leave other data on the corporate or home network, or on a removable storage media. Also, if available, enable the auto lock feature with a password and add a PIN number to the device; so that when you switch it on, you will have to enter a Personal Identification Number before it starts up. Wireless Security Considerations The following are a few things you need to ask yourself when implementing security for your wireless network. Do I have some form of logging enabled? Logging is important as it will help you to trace who is trying to gain unauthorized access to your network. It will also act as evidence when prosecuting a suspected intruder in court. Do I allow guest access? Where does my wireless signal end? Perform a site survey and find out exactly where the signal starts and ends; know your boundary. Document everything and when a new access point is attached to the current network make sure you know about it. In larger companies, departments implement their own WLAN by adding an access point to the

network and not informing the administration department, thus potentially opening up a hole in the network. Make sure you scan your network to identify known vulnerabilities, and if any are found, take action as soon as possible! Are the wireless clients safe? Introduce, or amend a current security policy that will require mobile users to keep their laptops protected with antivirus and firewall software. Tips for Securing your Wireless Network There are a numbers of things you can keep in mind which will help to lessen the likeliness of a breach of security in your wireless network. I have compiled a list of tips that I think will be of use to anyone who has a wireless network. As should be the case with a wired network, only share what is needed. Also, depending on the level of confidentiality, you should always password protect anything that is shared using an archive tool. Disable access point administration via wireless clients. This means that any changes to the access point configuration would have to be done from a machine attached to the wired network. On smaller networks, use MAC address filtering as an added means of security. Change the default SSID to something that is understandable to you but not to outsiders. This will make it slightly more difficult for people to connect to your network. This feature is meant to make it easier for clients to connect to the network because the network name can be automatically discovered by the client operating system. This means anyone in range of your access point will automatically know your network exists. This is fairly quick and easy to setup and has great benefits, as opposed to other means of security. Conclusion That concludes my overview of wireless security article. We took a look at why security is so important for wireless networks, I gave you some general tips for securing a network and showed you the different threats that one may face. Despite what most people think, a wireless network can be secure. However, there is a dire need for better education and stronger security implementations. If you are new to the wireless world then I hope you have learned how vital it is to implement security, whatever the network size. For information about the various security methods available, please see my Introduction to Wireless Networking Part 3 - Security, General Tips and Tricks.

DOWNLOAD PDF AS/400 WIRELESS LAN PRODUCTS FAMILY CONFIGURATION EXAMPLES,TIPS AND TECHNIQUES

Chapter 7 : Beasley, Networking | Pearson

/ / As/ Wireless Lan Products Family Configuration Examples,Tips and Techniques / IBM Redbooks / / DB2 V3 Performance Topics / IBM Redbooks / / Managing Ip Networks Using Netview Multisystem Manager R2 / IBM Redbooks.

Next page Wireless networking is a hot industry segment. Several wireless technologies have been targeted primarily for data transmission. Bluetooth is a standard used to build small networks between peripherals: Most people in the industry are familiar with the hype surrounding Bluetooth, though it seems to have died down as real devices have been brought to market. In the first edition, I wrote that I have not met many people who have used Bluetooth devices, but it is much more common these days. I use a Bluetooth headset on a regular basis. They promise data rates of megabits per cell, as well as the "always on" connections that have proven to be quite valuable to DSL and cable modem customers. After many years of hype and press from 3G equipment vendors, the rollout of commercial 3G services is finally underway. I recently subscribed to an unlimited GPRS service to get connected during my train trips between my office and my home. Many articles quote peak speeds for these technologies in the hundreds of kilobits per second or even megabits, but this capacity must be shared between all users in a cell. Real-world downstream speeds are roughly comparable to dial-up modem connections and cannot touch an This is a book about Some people call A second name which has grown dramatically in popularity since the first edition of this book is Wi-Fi, from the interoperability certification program run by the Wi-Fi Alliance, the major trade assocation of The Wonderful Thing About Standards Several standards groups are involved in Most of the effort remains concentrated in the IEEE, but important contributions to wireless LAN standards have come from several major locations. In addition to its activities as a professional society, the IEEE works on standardizing electrical equipment, including several types of communication technology. IEEE standardization efforts are organized by projects, each of which is assigned a number. Within a project, individual working groups develop standards to address a particular facet of the problem. Working groups are also given a number, which is written after the decimal point for the corresponding projects. Wireless LANs were the eleventh working group formed, hence the name Within a working group, task groups form to revise particular aspects of the standard or add on to the general area of functionality. Task groups are assigned a letter beneath the working group, and the document produced by a task group combines the project and working group number, followed by the letter from the task group. Some letters that are subject to easy confusion with letters, such as the lowercase "l," are not used. In wireless networking, the first task group to gain wide recognition was Task Group B TGb , which produced the Table is a basic listing of the different Interestingly enough, the case of the letter in a standards revision encodes information. Lowercase letters indicate dependent standards that cannot stand alone from their parent, while uppercase letters indicate full-fledged standalone specifications. In constrast, standards like At periodic intervals, the additions from dependent task groups will be "rolled up" into the main parent specification. The initial revision of Minor changes to the text were released as The most recent rollup is

Chapter 8 : An Overview of Wireless Network Security

Jim Geier offers practical methods, tips, and recommendations that draw on his decades of experience deploying wireless solutions and shaping wireless standards. He carefully introduces ac's fundamentally different design, site survey, implementation, and network configuration techniques, helping you maximize performance and avoid pitfalls.

Chapter 9 : Cabling Handbook, The, 2nd Edition | InformIT

Download designing and deploying 11n wireless networks or read online here in PDF or EPUB. Please click button to

DOWNLOAD PDF AS/400 WIRELESS LAN PRODUCTS FAMILY CONFIGURATION EXAMPLES,TIPS AND TECHNIQUES

get designing and deploying 11n wireless networks book now. All books are in clear copy here, and all files are secure so don't worry about it.