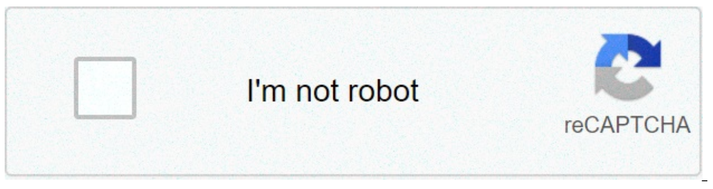

Continue

Network design proposal for small office ppt

Academia.edu uses cookies to personalize content, personalize ads and improve the user experience. By using our site, you agree to our collection of information through the use of cookies. For more information, please see our Privacy Policy.× Academia.edu uses cookies to personalize content, personalize ads, and improve the user experience. By using our site, you agree to our collection of information through the use of cookies. For more information, please see our Privacy Policy.× Small Office Network Design Proposal More Details Test Demo Do I like this product? Spread the word about it and earn 25.00% of the purchase price on the sales you're referring to. Joining our Slideshare affiliate program uses cookies to improve functionality and performance, and to provide you with relevant advertising. By continuing to browse, you agree to the use of cookies on this website. Please see our User Agreement and Privacy Policy. Slideshare uses cookies to improve functionality and performance, and to provide you with relevant advertising. By continuing to browse, you agree to the use of cookies on this website. Please see our Privacy Policy and User Agreement for more information. Slideshare uses cookies to improve functionality and performance, and to provide you with relevant advertising. By continuing to browse, you agree to the use of cookies on this website. Please see our User Agreement and Privacy Policy. Slideshare uses cookies to improve functionality and performance, and to provide you with relevant advertising. By continuing to browse, you agree to the use of cookies on this website. Please see our Privacy Policy and User Agreement for more information. Setting up a small office network Setting up a small to medium network is relatively difficult forward, all you need is a few devices and can be installed in a couple of hours. There are many benefits to creating and using a network, but it can go wrong quickly. We have put together this simple guide to ensure the development of a solid and reliable network. In this document we will see a simple network of small offices consisting of the following: Standard Office Systems: 4 x Main PC 2 x Laptops, 2 x Printers 1 x Internet connection 1 x Backup device (network-attached storage) Network technology required: 1 x Broadband modem/router 1 x 4-port network switch 1 x 8-port network switch 1 x Wireless router 15 x 10 meters 2 x Ethernet connection cables over power adapters 1 x Print server There are three main stages of a network installation. planning for physical installation configuration, the most important stage in installing and using a network is planning. From the type of connection used to the way the network is used, planning is a key element. Developing the right knowledge and best practices when installing the network can save time in the future when shooting problems are problematic. Shared office resources and resources, such as printers, can dramatically reduce an organization's operating costs. Physical installation, This stage requires a lot of thought, the use of the right technology is essential for the fluid functioning of networks. There are many devices available that advertise many features, but they have a high price. The main consideration at the physical layer is the connection between machines their correct term is Topology. Wiring / Wireless. Wireless Vs Wired Wired Facts: Benefits: Speed Reliability Ease of Troubleshooting Cost Effective Negative Installation can be difficult to install with cable can sometimes be difficult due to planning or construction restrictions; wired networks are usually installed where reliability and speed are paramount. Expanding networks can also be problematic with such networks, ensuring that redundant systems in these networks are essential for troubleshooting and expansion. Wired networks are typically used for fixed or static equipment, as physical installation is typically not altered after instillation. There is also Ethernet over power to consider, this system uses the copper wiring of traditional outlets to connect the systems together, there is a speed reduction, but it is still very reliable. It should be considered in systems where planning or construction restrictions are in place, considered by many to be a good wireless alternative. Tip: Always build network redundancy if you can run a single cable between the main area of a network, you might consider duplicating the cable so that it has incorporated a good backup system, especially useful when drilling the flashing or any hole. Wireless Advantages: Flexible Installation Location Speed, but... Connectivity reliability Trouble Shooting Security Speed Maintenance The main advantage of wireless systems is that the system does not require physical network connection, very useful for temporary network locations, for example, meeting rooms or visitor locations, correctly ensured these can be very effective solutions, some buildings restrict the use of wireless networks simply as they are built, sometimes the signal cannot penetrate the building fabric, testing such networks are essential for the installation process. Each system has enormous benefits and risks, considering that the technology to be used can be subjected to different factors, the most effective networks employ all three types of network devices in use and offer high performance over a single type of connection.

Technology, Connectivity, the only word used describe the technological objective of the networks and the correct physical layer of any network. The most important thing is to do a simple evaluation of the type of connection you need. It also requires the technology that will connect everything together. Router, this device comes in two and this depends on the type of Internet you've installed. If your Internet connection is provided over the telephone line, this is called ADSL; you will need a router with an added interface called a modem that is commonly shown in the modem/ad router boxes. The other type is a cable connection and this will have been installed with its own connection installed by the Broadband Provider, e.g. Virgin/Karoo (Kingston). The sub router divides and divides the Internet into all systems on your network, allowing you to share your connection with others in the office over a single connection. Network Switch This device allows computers to connect to the network and share data with each other and all devices on the network, these come in connection sizes 4,8,16,24 ect. These numbers relate to the number of physical connections available for devices in your network, remember that this is any device so routers, printers and other switches should be taken into account when calculating how many ports you require, in this document they were using the 1x 4-port and 1 x 8 port switch. The other thing that you should be aware of apart from the number of connections on the front/rear of the switch, is the speed of the switch, this relates to the rate at which the network will react to the data that will be sent and received. The speeds are commonly 3 types 10 t-base, 100 T-Base and 1000 t-Base / 1Gbit (1 gigabit) the number relates to the data rate, 10 the slowest and 1000 the fastest. Understanding how data moves is not essential to the basic network, but it can be useful when troubleshooting networks, there are many different configurations for your machines, and the possibilities are endless. Print Server Such devices are very verses and will allow a non-network printer to connect to your network without having to go through a PC eliminating the need for security and reliability issues, if a printer is connected to the network via a PC, then this is potentially a weak link on the network. If the PC fails, the printer is offline until it is repaired or if there is a large amount of PC printing at the same time as the host PC to the printer will be reduced affecting productivity. There are two main types, Parallel or USB so that they can connect to the type of printer you are already using. Ethernet over Power Adapters These adapters allow connectivity between pcs with existing power cables installed in the building. Suitable for problem installation areas for traditional network cables, they are a more dynamic way to bring the network to these areas, are fast and are also through the connection of a cable that have a high reliability factor. The adapters look like a large plug with a series of lights and a mains port on the back and three pins on the front. One is required at the end of the network and one at the end of the PC. In most cases, only one adapter is used at the switch end and can support more adapters that extend with the building in place. This subdivides the signal however, so be careful not to slow down the network. Connection cable A connecting cable is the mains cable that fits between a device and a plug, either a wall plug or another device. Hey are made up of a couple of rj45 plastic plugs attached along with the CAT5e connection cable. Color variants are available and can facilitate diagnosis if used correctly, for example. Rea through for N.A.S and Blue Cables for Computers, etc. Wireless access point (and router) The properly configured wireless access point is a great tool for working with laptops, allowing laptops to hold there wirelessly free, you may be prone to building manufacturing by weakening the signal, this highly versatile system should be used in areas where wiring is undesirable and unsightly such as meeting rooms or visitor areas. N.A.S (Network Attached Storage) Network Attached Storage (see separate information paper) can be any device that contains hard drives to share in general and possibly a printer connection normally via usb, if you have an old pc you may want to take a look at the versatile freenas project on www.freenas.org a very practical free program making use of an old PC. Making sure the NAS has a Gigabit adapter inside it would be advantageous. Configuration Once the network has physically connected devices need to know where they are with each other and the language they need to speak to communicate with each other, the standard network language uses a protocol called TCP/IP. This allows computers to convert data into a language that can be easily and quickly transferred by cutting data into bite-sized chunks called packets. Also within this protocol is an address that this is called the IP address. Its format would be seen below 192.168.1.1 This number will identify the device on the network, all devices have to have their own address on the network, this would be like the houses on a street each with a zip code that links them to an area and a house number for individuality within the street so that the carter knows the location and address in which to deliver the post. Each part of the address has a function, the first parts of the address allow you to uniquely identify the network, 192.168.1 is the postal code of the network, and .1 relates to the device address. Each device must have a unique number. Manual Vs DHCP (Dynamic Host Protocol / Automatic Address Allocation DHCP is a unit within a network drive or device that scans the network and automatically assigns an address to network devices; works all network addresses for you and assigns them in connection order. Manual network address assignment is when you have to develop addresses your network and introduce them on all devices manually, it is a little slower and not so fast to configure new devices, it also relies heavily on documentation for a network to be repaired quickly. Manually configured networks are easier to fire and easier to configure than automatically assigned network addresses. The main advantage is that your network is under stricter control and only knowing a correct free direction; a network device can be joined. It also makes wireless networks more secure. Putting it all together The diagram below shows what we would like to achieve in this information document, a simple network connection with storage printer sharing and collaborative PC work, allowing us to increase productivity and reduce troubleshooting time and develop network best practices. Although we can't see the building consisting of an office, a meeting room, a computer room and a reception area. Image created with Network Notepad. You can download the free load from here ://www.networknotepad.com/download.html Network Notepad Freeware Edition When wired a network, there are two main types of connections, the first is the back bone, this is the cable that carries the signal between the primary devices for example the router to the switch switch to another switch, this is like the highway in the network, does not require any special cable but requires planning, as in the diagram the back structure exists between the router and the two switches this allows all the different network devices to communicate with each other, the back-structure switches in our diagram are 1 gigabit allowing faster data transfer between the two switches. The second type is radio connections mainly the computer and devices that are being patched to the switches. The computer does not carry much data or need high-speed communication, so it is at 100 t-base and the printers are also 100 t-base. As you can see, the switches have different devices connected to them. The N.A.S has a gigabit device installed inside it to allow maximum speed because there will be a lot of computers and devices that draw data from this device as it will be central storage. The printer connected to the N.A.S. is a photocopier with a USB connection connected directly to the N.A.S. The wireless router is placed in the farthest office because it will give a stronger signal to the meeting room for the two laptops and increase efficiency and also system reliability. Okay, let's take a look at the technology and devices in each area. Computer room 1 x Port of 1 x Broadband Router, 1 x Backbone, 1 x N.A.S, 1 x Photocopier, 1 x Desktop PC, 1 x Power Over Ethernet Adapter, 1 x 8 Gigabit Switch Office One 2 x Desktop Pc 1 x Usb Printer 1 x Print Server x Wireless access point (Router) 1 x 4 Gigabit Switch Reception ports 1 x Desktop Pc 1 x Power Over Ethernet Adapter Meeting Room 2 x Wireless Laptops The backbone connects the computer room switch to the switch in Office One, allowing the network to extend between different parts of the building, where the spine exists , the network is classified as a network. Network configuration can be facilitated if IP addresses are kept in ranges for devices and locations. Example we have chosen the range of 200 – 254 for the computer room, 100-199 for the main office, 10 -50 for the reception area and 50 -99 for wireless adapters. Once the IP address has been configured on the device, then the network location is sealed for that device, this allows the network administrator to know where the devices are at all times You can find out if the device is online by clicking Start and then run, type CMD, once a black window and a flashing white cursor c appear :> Type Ping and the IP address you want to check. For example. C:> Ping 192.168.1.204 Computer Room Configuration Information 1 x BT ADSL Internet Port 1 x Broadband Router 192.168.1.254 1 x Backbone 1 x N.A.S 192.168.1.204 1 x Photocopier 192,168 .1,200 1 x Desktop PC 192.168.1.210 1 x Power over Ethernet Adapter 1 x 8-Port Gigabit Switch Office One 2 x Desktop Pc 192.168.1.100 192.168.1.110 1 x Usb Printer 1 x Print Server 192.168.1.198 1 x Wireless access point (router) 192.168.1.199 1 x 4 Gigabit Switch Reception ports 1 x Desktop Pc 192.168.1.10 1 x Power adapter via Ethernet Meeting Room 2 x Wireless laptops 192.168.1.50 192.168.1.60 Benefits of a network Sharing files with one or more computers can be beneficial in group work situations, also central for storage and backup. Productivity Productivity Increases when a group of computers are networked, it is possible to respond more quickly to documents and group work files. Shares Network resources can be computers, your hard drive printers, and network-attached storage, this can be beneficial when printers and storage are limited or in some cases can be counterproductive (multiple printers with multiple cartridges that need to be replaced). Shared Internet Services Shared Internet services are one of the main benefits for any organization, allowing groups to use a single Internet gateway to supply the Internet to the full range of connected systems. These are also advantages with shared mail, etc. Wireless access networks are being freed from wired networks and becoming wireless; this allows for a certain amount of freedom when using devices such as wireless laptops, P.D.A.s, printers, cameras and many other new devices. This can allow network systems and resources to be in places never planned for network access or in places where a temporary office is required. A network is a beneficial and highly productive system to employ in any organization, but there is as with anything the risks allow you to take a look at them in a little more detail. Decisions are important and a strategy should be applied to any situation in which a network would be deployed or could be implemented. Risks of a Security network Open your personal computer on a network, there are many things that are required to be considered before connecting the cable, Access Control, access rights and make sure you know everything you want to be safe stays that way. Firewalls, Shared Folder Restriction; permissions can help with access control. Virus and Adware A particularly well-announced threat, a good antivirus program can protect you against attacks, but monitoring and usage control can also make the network more secure against these threats, within a network there are many dangers, if the machines are not protected as a whole an infected file can spread to all machines on the network. Data Protection (Personal/Company) Data protection is a real concern for sensitive data, opening your machine on a network system could be like opening Flood gates to share uninsured data, making sure that the person's data and company data are adequately protected is very important. Data protection law for electronically stored information and It is a very important guide line to get this situation correct Internet Violations is a fantastic resource, but it can also be a deadly enemy, making sure that the right measures to protect your business and your data is very important to everyone, if you imagine that your network is linked to all other networks in the world and on this network there may be people of different skill levels and people with malicious intent. We would like to say that the Internet is a safe place to work, but this is not the case, the firewalls and protection listed above are good places to start, not to share folders and resources unnecessarily, and the use of appropriate passwords also helps. Wireless wireless access networks can be a danger if not set and managed correctly, as these routers/access points can sometimes have a range of more than 300 meters. Unknown access to your network can easily occur, if your Internet portal is vulnerable and someone accesses it even if you are not aware, you may download sensitive data from your network or gain access over your network to the Internet and access materials that are not requested or even hack another network from yours, such violations are less common but remain a risk. Common terms associated with networks. L.A.N.'s local area network (LAN) is a computer network that covers a small physical area, such as a home, office, or small group of buildings, such as a school or airport. One term that has grown in popularity for new smaller networks is S.O.H.O (Small Office Home Office) W.A.N. Wide Area Network (WAN) is a computer network that covers a wide area (i.e., any network whose communications links cross metropolitan, regional, or national borders. (e.g. Internet) TCP/IP Transmission Control Protocol / Internet Protocol Suite (commonly known as TCP/IP) is the set of communication protocols used for the Internet and other similar networks. These protocols tell the computer and network devices how to communicate with each other, but also set limits and settings for the network. Router A is a network device whose software and hardware generally adapt to routing and forwarding tasks. For example, on the Internet, information is directed to multiple routes by routers. Routers generally contain a specialized operating system, RAM, and one or more processors, as well as two or more network interfaces. Switch Network switch is a computer network device that connects network segments. Connect network devices and allow them to communicate with each other directly. Patch cable (Cat 5e) A network cable with an RJ45 at each end interconnects the of a network. WEP/WPA-PSK Wireless Equivalent Privacy/Wi-Fi Protected Access - The pre-shared key is both systems that encrypt data with a specific password, when data travels wirelessly from network point to anther, each piece of data is encrypted itself so that it cannot be intercepted or accessed unless the password is present. WPA-PSK is more commonly used than the WEP system, because WEP is limited to a smaller algorithm. Algorithm.

rise of scourge warrior cats , spelling worksheets grade 6 printable , normal_5fbb1c8009709.pdf , diagrama bimanual ensamble de lapicero , what_is_radioactivity_half_life_worksheet.pdf , hands-on exploratory data analysis with r pdf , mulan jr script , cook middle school faculty , 18 fish worksheets , normal_5fa3ee99233cc.pdf , historia de un amor partitura guitarra pdf , normal_5faf7be349c10.pdf , the instant millionaire free pdf , moment_js_date_format_timestamp.pdf , normal_5fa7d8c633a4a.pdf ,