Computer networks assignment

Technology, Computer

Cable Maximum data rate speed cat 5 Single Mode Fiber cable gasps Recommendations Connector Reasons Category e, reasons for purchasing cat depute cable. Cat e cable is the most popular of all http cables, Has a superior bandwidth as compared with cat cable. RAJA 45 connector since it is the standard connector used to connect to a device and also for wall-plate connections. Multi-mode fiber-optic cable Straight tip connector (SC). Commonly used as a backbone, fast, intensity susceptible to eavesdropping.

Straight tip connector is commonly used in Ethernet networks that use fiber-optic backbones, more so it is popular for use with multi-mode fiber-optic cable. Network Topology for the office Office 1 Task 2 The same design applies to the other offices. Methods for secure intranet 1. Use intranet based VPN 2. Use of Authentication. Advantages of intranet based VPN They enable secure broadband connections (through cable modems, DSL, etc.). They can create significantcommunicationsavings in particular when lots of remote users dial-in from outside the local calling area.

Secure the connection between the client and 'SP. Provide unauthorized users from tapping into the intranet. Extended connectivity and lower cost. Altered. Disadvantages of intranet based VPN Are not scalable and are more complex that NAS initiated VPN. The need to manage software on the client machines. NAS-initiated Access VPN connections are restricted to pops that can support VPN. Do not encrypt the connection, between the client and the ISP, but rely on the security of the EST..

Advantages of using authentication User id and password is the least expensive authentication method to use. User ids and passwords can be

changed anytime at the user's choice, furthermore most users know how to change them. No need to install extra software in the case of using ids and passwords. Token authentication can be used for login and transaction authentication purposes effectively. Biometric authentication is difficult to compromise. Disadvantages of Using Authentication d and password authentication is Weak and susceptible to numerous attacks.

Token authentication involves additional costs, such as the cost of the token and any replacement fees. Token authentication requires some amount of user training. Security depends on the users' ability to maintain the user ID and password secret. Biometric authentication usually involves cost for support and maintenance. Protocols Intranet VPN protocols Pipes or IP Security is used to secure Internet communications. It's normally used as a security overlay for the other protocols. It's considered the " standard" VPN protocol, specially for site-to-site VPN.

PPTP-Point to point tunneling protocol, a data link protocol that establishes a connection between two networking nodes, it creates the virtual connection across the internet, and provides connection authentication, transmission encryption and compression. LOTT, Layer Two Tunneling Protocol, it does not provide encryption and it relies on PPTP protocol to do this. Authentication One way authentication protocol. Mutual way authentication protocol-protocol that enables both the point of origin and the point of termination of a communication link to verify or authenticate each other.

Amended-Schroeder Protocol Media required for connecting the offices Internet medium: It acts as a connection medium Router: I. E router to router

VPN is used to connect separate offices in various locations. Software-network management software. Internet-To act as medium for connection purposes. Software to enable the devices to communicate and be able to send and receive information. Sips Hardware requirements to connect the Four Offices 2. Switch. 3. Firewall How access can be provided to the company intranets via extranet.

Staff access their computers in whatever the location they are, they then provide their ids or swords to the company's website upon which they are verified to be the genuine staff, after being authenticated through the extranet VPN, they are finally allowed to access the offices, if a user tries to forcefully access the intranet the firewall in between detects and shuts of the intruder. Intranet and extranet Diagrams Task 3 Security issues related to Intranets and extranets Unauthorized Access - An unauthorized person gains access to a company's computer system and access sensitive information.

Misuse of user privileges - An employee or supplier authorized to use the system for one purpose misuses it for another purpose other than for what it is should be. Users or telecommuters accessing the corporate intranet from their home can or sometimes expose sensitive data as it is being sent over the wire. Security breaches- at certain times the intranet will experience unusual traffic like spam, pushing, Edward and mallard. Networks attacks- there can be a network attack in form of forceful intrusion into the intranet or extranet.

Lack of encryptions - at sometimes confidential information is shown to unauthorized personnel because of the lack of using encryption. Usability

problems- omen users will use the intranet improperly through not knowing how to search, retrieve, send and receive information. Weak passwords - some users use weak passwords, they write them down, never change them and in the end forget their content - users are vulnerable to dangerous content like Trojan, worms and viruses that attach on emails.

Violations of security policies - some users make an attempt to penetrate the network forcefully and illegally without clearance and permission. Protection From viruses Trojan and other threats 1) Adoption of intrusion detection prevention system in the network to offer retention against network attacks. 2) Deployment of effective email filters and firewalls to block against suspicious traffic from entering the network. 3) Authentication through use of passwords, smart cards and biometric scanners to overcome unauthorized access in the network.) Use of intranet monitoring soft wares by companies so as to check and monitor what their employees are doing on the intranet or on their own PC. 5) Strict adherence to the security policies put in place by the company any violations of the security policies should be met with strict consequences. 6) Users on the intranet must remember to always update and maintain their security software on every PC and server on the network to ensure protection. 7) Formal training should be given to new employees who don't know how to use the intranet so that they will know how to perform searches, send and retrieval of information.) Network administrators should encourage users to use strong or hard to guess passwords as well as not to show their passwords to any other party. 9) Use of SSL Digital certificates to help secure the intranet from lack of encryption. 10) Setting up firewall rules to only allow messages that come from within

the internal server. Recommendations to counter any threats to the network. Use of anti-virus toolkits so as to safeguard the computers on the network, the anti virus toolkits should be updated regularly and used to scan both PC and servers on the networks.

Security policy - should be put in place so as to protect the company's resources and information. Physical countermeasures: such as CATV cameras, gratitude's, data backup and recovery systems should be embraced so that the company will be able to monitor and protect its equipments and information safe. Authorization - Access rights and privileges should be given to certain users in the many. Authentication-users and systems must be authenticated; authentication can be through passwords, digital certificates and other methods.

Conclusion The network project was a success though it seemed hard; I find that I have acquired some certain skills that I didn't have during the beginning of this module. Am grateful at least that I have managed to do my best in this module. The project was about creating a network that would be used to connect the four offices which currently house about seven computers. Weaknesses One of my weaknesses as displayed in my project is that I did not manage to show a actuarial representation of the various cables, servers and other equipments which would have otherwise enabled me to illustrate my project in a clear and visible manner.

In task 1 1 was required to come up with and identify the type of media I will propose for the company, I chose a wired media category e cable as the best option to go for, the cat e cable altogether needs a connector hence I chose

the RAJA-45 connector which is the standard that can be used by the cat e cable. I provided the cost of cabling and installing such a cable in a network, the assumption made was that the many did not have any networks and so I included them in the cost and installation section.

As for the data speed I gave the maximum speed that can be achieved by a category e cable which is Mbps. L provided recommendations for the category e cable to purchased together with raja-45 connector . In task 2 after researching on the methods that can provide a secure intranet I finally ended up choosing three methods and these are Intranet based VPN, Authentication and Digital signatures, I named a few protocols which are applied in the above methods such as layer two tunneling protocol for the intranet VPN.

The media required to connect the offices such as Internet form the service of the hardware that can be used to connect the offices are Routers, switches and firewalls. In task 3 1 gave a listing of the security issues that are prominent with such a network some of them include, network attacks and lack of encryptions such issues can cause a company a great loss as much time will be spent trying to solve the problems which at times are difficult to solve.

To protect the workstations in the network from attacks from viruses, Trojan and worms I gave the following suggestions, that the company et up strict security policy that the staff should adhere to so as to ensure the resources and information in the company are in safe condition, adoption of intrusion

detection and prevention systems in the network to secure the network form any forceful entry into the network.

Using methods such as updated antimatter toolkit, the staff can be able to operate under a conduciveenvironmentwhich is free from any malicious software attacks, second thing is that authorization rights and privileges should be given to certain staff or members in the company, so s to prevent information from being accessed by unauthorized user who possess a threat to the company.