Testout chapter 6

Which of the following is the best definition for a LAN? A network in a small geographic area, like in an office.

Explanation

A LAN is a network in a small geographic area, like in an office.

A WAN is a network whose computers and servers are geographically far apart but still connected. A PAN (personal area network) is the interconnection of components, such as laptops, mobile devices, printers, mice, keyboards, and other Bluetooth equipped devices, using some form of wireless technology within a personal range (typically 10 meters or less). A VPN is the extension of a private network over a shared or public network such as the Internet.

Which of the following terms refers to a network resource sharing model that uses access control lists saved on each computer? Workgroup

Peer-to-peer

Explanation

Access to shared resources are controlled separately on each computer in the workgroup or peer-to-peer models. For example, each computer in a peer-to-peer network maintains its own set of user accounts.

A domain is a collection of computers that share a common security database. Access is controlled by maintaining access control lists in a centralized directory. The client/server model places shared resources on a server. Resources are accessed by clients.

Which of the following is a rating of the amount of data that can be sent over a network in a period of time? Bandwidth

Explanation

The network bandwidth is a rating of how much data can be sent over a network.

Broadband is a signaling scheme that divides a single network media into multiple transmission channels. Latency measures the delay between transmission and reception of network data. Jitter measures how much variation occurs in a network” s latency measurement over time.

Which of the following terms describes a group of computers and users that utilize centralized resources, administration, and security settings? Domain

Directory

ExplanationA domain and a directory both identify a group of computers that utilize centralized resources, administration, and security settings. For example, Active Directory is a service that provides a centralized database of resources for a domain.

A Local Area Network (LAN) is a network in a small geographic area, like in an office. A peer-to-peer network is a decentralize network where each host has its own user accounts and shared network resources. A peer-to-peer network does not utilize centralized resources, administration, and security settings. A workgroup is an example of a peer-to-peer network. In a workgroup, each computer controls access to its own resources. Security

controls on each computer identify who can have access to the computer’s resources.

Which of the following are advantages of using a domain to manage a network? Scalability

Centralized administration.

ExplanationA domain is an example of client/server networking where shared resources reside on special computers called servers. Other computers, called clients, connect to the server to access resources. Security controls on the server identify which clients can have resource access. Advantages of client/server networks include:

– Scalability– Centralized administration.– Centralized network services and resources.

Setup with little or no configuration is a characteristic of a peer-to-peer network as is decentralized administration.–

You have a network that uses a logical ring topology. How do messages travel through the network? Messages travel from one device to the next until they reach the destination device.

ExplanationIn a logical ring topology, messages travel to each device in turn. If the message is not intended for that device, the message is forwarded to the next device on the network.

You have a network that uses a logical bus topology. How do messages travel through the network? Messages are broadcast to all devices connected to the network.

ExplanationMessages sent using a physical bus topology are broadcast to all devices in the network. The device in the middle of the star (typically a hub), receives the message and forwards it on to all other devices.

Which of the following topologies connects each network device to a central hub? Star

ExplanationStar topologies connect each device on the network to a central hub.

You have implemented an ad-hoc wireless network that doesn’t employ a wireless access pint. Every wireless network card can communicate directly with any other wireless network card on the network. What type of physical network topology has been implemented in this type of networks? Mesh

Explanation

This type of network uses a physical mesh topology. There’s no central connecting point. any host can communicate directly with any other host on the network. A mesh network, such as this one, is usually impractical on a wired network. Each host would have to have a separate, dedicated network interface and cable for each host on the network. However, a mesh topology can be implemented with relative ease on a wireless network due to the lack of wires.

A network in a small geographic area that typically uses wires to connect systems together. Local Area Network (LAN)

A small network used for connecting devices, such as a notebook computer, a wireless headset, a wireless-printer, and a smartphone. Personal Area Network (PAN).

A network that is typically owned and managed by a city as a public utility. Metropolitan Area Network (MAN)

A group of networks that are geographically isolated, but are connected to form a large internetwork. Wide Area Network (WAN)

Similar to a standard LAN, but uses radio signals instead of wires to connect systems together. Wireless Local Area Network (WLAN)

A network that covers an area as small as a few city blocks to as large as an entire city. Metropolitan Area Network (MAN).

A set of subnets connected to each other, typically by wires, using at least one router. Local Area Network (LAN)

ExplanationThe following network types are defined by the geographical area they cover:

Personal Area Network (PAN): A very small network used for communicating between personal devices. For example, a PAN may include a notebook computer, a wireless headset, a wireless printer, and a smartphone. A PAN is limited in range to only a few feet.

Local Area Network (LAN): A network in a small geographic area, like an office. A LAN typically uses wires to connect systems together. For example, a LAN is usually a set of subnets connected to each other using routers to connect the subnets.

Wireless Local Area Network (WLAN): A network that covers an area that is roughly the same size as a standard LAN. However, it uses radio signals instead of wires to connect systems together.

Metropolitan Area Network (MAN): A network that covers an area as small as a few city blocks to as large as an entire metropolitan city. MANs are typically owned and managed by a city as a public utility.

Wide Area Network (WAN): A group of LANs that are geographically isolated, but are connected to form a large internetwork.

A user on your network has been moved to another office down the hall. After the move she calls you, complaining that she has only occasional network access through her wireless connection. Which of the following is most likely the cause of the problem? The client system has moved too far away for the access point.

ExplanationIn this case, the wireless client system has had no problems accessing the wireless access point until the move to the new office. In some cases moving a system will cause signal loss either from the increased distance away from the WAP or from unexpected interference by such things as concrete wall or steel doors. There are several ways to correct the problem including reducing the physical distance to the client, using a

wireless amplifier, upgrading the antennas on the wireless devices or adding another WAP to the infrastructure. Because the client could previously access the WAP and still has occasional access, it is likely that the move was the cause of the problem rather than any configuration setting on the client system.

A user calls to report that she is experiencing intermittent problems while accessing the wireless network from her laptop computer. While talking to her, you discover that she is trying to work from the break room two floors above the floor where she normally works. What is the most likely cause of her connectivity problem? The user is out of the effective range of the wireless access point on her floor.

Explanation

Because the user is only experiencing intermittent problems, the most likely cause is that she is out of the effective range of the wireless network access point. All of the other answers listed may be appropriate if the user was unable to connect to the network at all. However, as the user is experiencing only intermittent problems, none of the other answers is likely to be the cause of the problem.

You’re trying to access your office network with your Windows workstation from home using your organization’s virtual private network (VPN). Your DSL modem has connected to your ISP, but you cannot connect to your office network. You issue the ipconfig command from the command prompt and learn that your system has been assigned an IP address of 169. 254. 1. 12. What’s causing the problem? Your ISP’S DHCP server isn’t working properly.

ExplanationAnytime you see a network interface assigned an IP address in the 169. 254. 0. 1 to 169. 254. 255. 254 range, you know that it was unable to acquire an IP address from a DHCP server. Automatic Private IP Addressing (APIPA) on the workstation automatically took over and assigned an IP address in the range listed above. Because of this, the workstation isn’t configured with the correct router and DNS server addresses, and can’t access the company’s VPN.

Your workstation is unable to communicate with any other computer on the network. Which of the following tools should you use to test the ability of the network card to send and receive signals? Loopback plug

ExplanationUse a loopback plug to test the network card’s ability to send and receive signals. Pinging the local host (ping 127. 0. 0. 1) tests the TCP/IP protocol stack, but does not actually send signals out the network card. A cable tester tests continuity of all wires in a cable and ensures that wires are connected appropriately in the plugs. Use a multimeter and an ohmmeter to test the electrical properties of cables and signals.

You are troubleshooting connectivity between your computer and the www. widgets. com server, whose IP address is 192. 168. 1. 1. Which of the following commands tests connectivity to the device as well as name resolution? ping www. widgets. com

Explanation

To test both name resolution and communication with the server, use the ping command with the host name. The first step in the ping test is to find

the IP address of the specified host. Using ping with just the IP address will not test name resolution. Using nslookup only tests name resolution, it does not test communication with the end device.

A user reports that he can’t browse to a specific website on the Internet. From his computer, you find that a ping test to the Web server succeeds. A trace route test shows 17 hops to the destination Web server. What is the most likely cause of the problem? Incorrect DNS server address.

Explanation

In this scenario, a ping test to the Web site succeeds while accessing the Web site through the browser does not work. Users type host names in the browser to go to Web sites, and host names must be translated to IP addresses by a DNS server. Either the workstation is using the wrong address for the DNS server, the DNS server is not available, or the DNS server does not have an entry for the Web site. Because the ping and trace route tests works, you know that the IP address, subnet mask, and default gateway values are correct.

You manage a network that has multiple internal subnets. You connect a workstation to the 192, 168. 1. 0 subnt, which uses the default subnet mask. This workstation can communicate with some hosts on the private network, but not with other hosts. You run ipconfig /all and see the following:

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix: mydomain. local

Description: Broadcom network adapter.

Physical Address: 00-AA-BB-CC-74-EF.

DHCP Enabled: No

Autoconfiguration Enabled: Yes

IPv4 Address: 192. 168. 1. 102 (Preferred)

Subnet Mask: 255. 255. 0. 0

Default Gateway: 192. 168. 1. 1

DNS Servers: 192. 168. 1. 20 192. 168. 1. 27.

What is the most likely cause of the problem?

Incorrect subnet mask

Explanation

In this example, the network us using a mask of 255. 255. 255. 0 (24-bits), but the workstation is configured to use a mask of 255. 255. 0. 0.

You manage a network that has multiple internal subnets. You connect a workstation to the 192. 168. 1. 0 subnet using the default subnet mask. This workstation can communicate with some hosts on the private network, but not with other hosts. You run ipconfig /all and see the following:

Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix: mydomain. local.

Description: Broadcom network adapter.

Physical Address: 00-AA-BB-CC-74-EF

DHCP Enabled: No

Autoconfiguration Enabled: Yes

IPv4 Address: 192. 168. 1. 102 (Preferred).

Subnet Mask: 255. 255. 255. 0

Default Gateway: 192. 168. 2. 1.

DNS Servers: 192. 168. 2. 20

What is the most likely cause of the problem?

Incorrect default gateway.

Explanation

In this example, the default gateway address is incorrect. The default gateway address must be on the same subnet as the IP address for the host. The host address is on the 192. 168. 1. 0/24 subnet, but the default gateway address is on the 192. 168. 2. 0 subnet.

A user is having problems connecting to other computers using host names. Which of the following commands will help you troubleshoot this problem?

nslookup

Explanation

Use Nslookup to troubleshoot DnS name resolution problems. Use Arp to view information about MAC addresses and their corresponding IP addresses. Netstat 9network statistics is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. Use Nbtstat to help troubleshoot NetBIOS name resolution problems.

You work in an office that uses Linux and Windows servers. The network uses the IP protocol. You are sitting at a Windows workstation and an application you are using is unable to connect to a Windows server named FiledSrv2. Which commands can you use to test network connectivity between your workstation and the server? Tracert

Ping

Explanation

On an IP based network, you can use the ping command to check connectivity between a source and destination computer.. You can also use tracert on a Windows system to check the routing path between two hosts. The tracert command performs the same function as ping, but includes the path information. Use nslookup and dig on Windows and Linux to resolve the IP addresses of host names using DNS lookups. Use Arp to view information about MAC addresses and their corresponding IP addresses.

Which command would you use to have a workstation stop using an IP address that it obtained from a DHCP server? ipconfig /release

ExplanationUse ipconfig /release to release the IP configuration information obtained from the DHCP server. Use ipconfig /renew to request new IP configuration information from the DHCP server. Use net stop to stop a network service. Use net logoff to break the connection between your computer and a shared resource.

You suspect large packets are being dropped on your network because of their large size. Which utility can you use to confirm your suspicion? ping -l

Explanation

Use ping -l to configure the payload size to identify when packets above a certain size are being lost. Ping -t continuously sends pings to a specific device. Tracert tests connectivity between devices while showing the path between the two devices. Nslookup resolves (looks up) the IP address of a host name. Netstat shows IP-related statistics.

Examine the following output:

Reply from 64. 78. 193. 84: bytes= 32 time= 86ms TTL= 115. Reply from 64. 78. 193. 84: bytes= 32 time= 86ms TTL= 115. Reply from 64. 78. 193. 84: bytes= 32 time= 86ms TTL= 115. Reply from 64. 78. 193. 84: bytes= 32 time= 86ms TTL= 115.

Which utility produced this?

Ping

Explanation

The output shown was produced by the ping utility. Specifically, the information output was created using the ping -t command. The -t switch causes packets to be sent to the remote hots continuously until stopped manually. Ping is a useful tool for testing connectivity between devices on a network. Using the -t switch with ping can be useful in determining whether the network is congested, as such a condition will cause sporadic failures in the ping stream.

Tracert is similar to ping in that it tests connectivity between two hosts on the network. The difference is the tracert reports information on all intermediate devices between the host system and the target system. Ping, on the other hand, does not report information on intermediate devices. Nslookup is a tool provided on Linux, Unix, and Windows systems that allows manual name resolution requests to be made to a DNS server. This can be useful when troubleshooting name resolution problems. Ifconfig is a tool used on Unix, Linux, and Macintosh systems to view the configuration of network interfaces, including TCP/IP network settings.

Examine the following output:

4 22 ms 21 ms 22 ms 22 ms sttlwa01gr02. bb. ispxy. com [154. 11. 10. 62]5 39 ms 39 ms 65 ms plalca01gr00. bb. ispxy. com [154. 11. 12. 11]6 39 ms 39 ms 39 ms Rwestplalca01gr00. bb. ispxy. net [205. 171. 205. 29]8 75 ms 117 ms 63 dia-core-01. inet. ispxy. net [205. 171. 142. 1]

Which command produced this output?

Tracert

Explanation

The output is from a tracert command run on a Windows Server system. The tracert command provides information on each step in the route a packet takes to reach a remote host. Responses from each hop on the route are measured three times to provides an accurate representation of how long the packet takes to reach, and be returned by that host. This information can be useful in locating congestion points on a network, or when verifying that network routing is operating as expected. The ping command is used to test connectivity between devices on a network. Like tracert, ping sends three packets to the target host, but it does not report information on any intermediate devices it traverses to reach the target. Nslookup is a tool provided on Linux, Unix, and Windows systems that allows manual name resolution requests to be made to a DNS server. This can be useful when troubleshooting name resolution problems.

Which of the following are antenna types that are commonly used in wireless networks? Directional antenna

Omnidirectional antenna

Explanation

Directional and omnidirectional are two type of antennae commonly used in wireless networks.

A directional antenna:

– Creates a narrow, focused signal in a particular direction, which increases the signal strength and transmission distance.

– Provides a stronger point-to-point connection; is better equipped to handle obstacles.

An omnidirectional antenna:

– Disperses the RF wave in an equal 360-degree pattern.– Provides access to many clients in a radius.

You have a small network. All computers are running Windows 7. You have created a HomeGroup for your network. You have a laptop that you use at work that runs Windows 7 Professional. You connect the laptop to the network. You are unable to see shared files on other computers. What should you do? Join the laptop to the HomeGroup.

ExplanationTo access resources in a HomeGroup, the computer must join the HomeGroup. Setting the network type to Home and enabling Network Discovery are all necessary, but by themselves will not allow resource access until the HomeGroup is joined. You can only create a single HomeGroup on a LAN segment; because one already exists, you will not be able to create a new one on the laptop.

You have a Windows 7 computer connected to a small network that is not part of a domain. You want to see the computers and printers on the network. Which feature would you use? HomeGroup

ExplanationHomeGroups are a simple way of sharing resources and managing authentication to resources on a home network. You can use the Home Group option in the Control Panel or Explorer to see computers. Shared files, and printers that are part of the HomeGroup. My Network Places is a feature of Windows XP that you would use to browse network devices. Use Devices and Printers or Device Manager to manage hardware devices connected to the local computer.

You want to join your computer to a homegroup but you don’t see any homegroups on your home network. You know they have been set up on other computers at home, so what might be preventing you from seeing the homegroups that have been created? The network location is not set to Home Network.

Network Discovery has been disabled on your computer.

ExplanationYour network location must be set to Home Network before you can see homegroups that have been set up on your home network. Network Discovery is enabled by default on your computer, but it’s one of the settings you should check if you cannot see homegroups when you know they have been created. It could have been disabled inadvertently.

You will not have the option to share resources until find the homegroup can click the Join Now link. The next step will be to enter the homegroup password. There is no homegroup administrator.

Because of how simple they are to set up, you want to create a homegroup at the office. What is most likely to prevent you from setting up a homegroup

at work? Your computer belongs to a domain. Your network location is not set to Home Network.

ExplanationYou are going to have trouble creating a homegroup at work, where there is likely to be a work network set up and running because.

Your network location must be set to Home Network, but Work Network is selected as the default network location. You cannot create a homegroup on a computer that belongs to a domain.

Home groups are designed to be an easy way to share resources on a home network. You are not likely to need a homegroup at work because all the resources you need for sharing are part of a typical work network.

Network Discovery is enabled by default so that is not likely to prevent from creating a homegroup. There is no homegroup administrator role that could be used to prevent you from creating a homegroup. Libraries are needed for homegroups but they cannot be disabled.

Your home computer belongs to a homegroup so that resources can be shared between other computers you have in your home. Where would you find the resources that are being shared from other computers? In the Libraries container in Windows Explorer

ExplanationEach homegroup is displayed as a separate node in the Libraries container in Windows Explorer. Just open the homegroup node to see the resources, which are displayed by username and computer name within the homegroup node.

Which of the following tools allow for remote management of servers? SSH

Telnet

Explanation

Both Telnet and SSH are tools for remote management of servers. However, you should avoid using Telnet as it sends all data, including authentication information, clear text on the network. POP3 is for retrieving e-mail from a remote server, and FTP is for transferring files. LDAP is a protocol used to access information about network resources from a directory service.

Which utility would you use to view current connections and active sessions and ports on a computer? Netstat

Explanation

Netstat shows IP-related statistics including:

– Incoming and outgoing connections.– Active sessions, ports, and sockets.– The local routing table.

Ipconfig displays IP configuration information for network adapters. Use ipconfig to view IP address, subnet mask, and default gateway configuration. Nslookup resolves (looks up) the IP address of a host name. Ping sends an ICMP echo request/reply packet to a remote host. A response from the remote host indicates that both hosts are correctly configured and a connection exists between them.

Which of the following utilities can you use from the command line on a Linux system to see a list of the installed network interfaces, along with their current status and configuration? ifconfig

Explanation

ifconfig is used on Linux (and Mac OS) systems to display the installed network interfaces, their current status, and the current configuration settings for each interface, including the MAC address, IP address, broadcast address, and subnet address.

Ipconfig is used on Windows systems to view the installed network interfaces and their IP address, subnet mask, and default gatewar configuration. Netstat is used on a Windows. system to display IP-related statistics, netconfig, if lookup and netinfo are not the names of real networking utilities.

You need to view detailed IP configuration information on Windows workstation. In addition to the IP address, subnet mask, and default gateway configuration, you need to now see the network card’s MAC address and the addresses of the DHCP and DNS servers the workstation is communicating with.

What command would you enter at the command line to see this detailed information?

ipconfig /all

Use ipconfig /all to view detailed configuration information including the MAC address and the DHCP and DNS servers the workstation is communicating with.

When you see the address of the DNS server, you realize that this information needs to be updated. Earlier in the day, you implemented a new DNS server with a new IP address. The workstation will update this information in 24 hours. What command can you enter at the command line to update the DNS server information right away? ipconfig /flushdns

Explanation

Use ipconfig /flushdns to flush (or remove) all the entries in the workstations' current DNS cache. If the IP address of a network server is changed, your local cache will contain the old IP address until the cache is updated (every 24 hours) or the flushdns option is used.

Resolves (look ups) the IP address of the specified hostname. Nslookup

Tests connectivity between devices and shows the routers in the path between the two devices. Tracert

Sends an ICMP echo request/reply packet to a remote host. Ping

Displays current connecitons and incoming and outgoing connections. Netstat

A few simple replies to this reques from the remote host indicates that a connection exists between sender and receiver. Ping

Displays active sessions, ports, and sockets, and the local routing table.

Netstat

When used with the -t option, performs a continues connection test. Ping

ExplanationPing sends an ICMP echo request/reply packet to a remote host. A response from the remote host indicates that both hosts are correctly configured and a connection exists between them. Using ping -t performs a continuous connection test (press Ctrl+C to stop sending the ping requests).

Tracert is similar to the ping utility in that it tests connectivity between devices; however, tracert also shows the routers in the path between the two devices. Responses from each hop on the route are measured three times to provide an accurate representation of how long the packet takes to reach, and be returned by the specific host.

Nslookup resolves (looks up) the IP address of the specified hostname. It also displays additional name resolution information, such as the DNS server used for the lookup request.

Netstat displays the following IP-related statistics:

– Current connections.– Incoming and outgoing connections.– Active sessions, ports, and sockets.– The local routing table.

Ipconfig displays IP configuration information for network adapters.

Which of the following utilities would you use to do the following?

– Establish a remote server management session.– Send unencrypted (clear text) transmissions to the remote server.– Use mostly to manage specialized industrial and scientific devices.

Telnet

Explanation

The Telnet utilities is used to do the following:

– Establish a remote server management session.– Send unencrypted (clear text) transmission to the remote server.– Use mostly to manage specialized industrial and scientific devices.

SSH is similar to Telnet. It is used for remote server management, however, SSH encrypts all communications and is much more secure. PuTTY, xterm, and RUMBA are all terminal emulators.

What is name of the utility which is similar to Telnet, that you can use to establish a secure remote server management session? SSH

Explanation

Similar to Telnet, the SSH utility is used for remote server management; however, SSH encrypts all communications and is much more secure.

Which of the following are good reasons to enable NAT? To translate between Internet IP addresses and the IP address on your private network.

Explanation

NAT translates the Internet IP addresses and the IP addresses on your private network. This allows for multiple computers to share the single IP address used on the Internet. Firewalls prevent unauthorized users from accessing private networks connected to the Internet, including the DHCP server. A proxy server caches web pages.

Which of the following is not one of the ranges of IP addresses defined in RFC 1918 that are commonly used behind a NAT router? 169. 254. 0. 1 – 169. 255. 254

Explanation

169. 254. 0. 1 – 169. 254. 255. 254 is the range of IP addresses assigned to Windows DHCP clients if a DHCP server does not assign the client an IP address. This range is known as the Automatic Private IP Addressing (APIPA) range. The other three ranges listed in this question are defined as the private IP addresses from RFC 1918 which are commonly used behind a NAT server.

You have a computer that is connected to the Internet through a NAT router. You want to use a private addressing scheme for your computer. Which of the following IP addresses could you assign to the computer? 172. 18. 188. 67192. 168. 12. 25310. 0. 12. 15

ExplanationOf the addresses listed here, the following are in the private IP address ranges: 10. 0. 12. 15 (private range = 10. 0. 0. 0 to 10. 255. 255. 255) 172. 18. 188. 67 (private range = 172. 16. 0. 0 to 172. 31. 255.

255)192. 168. 12. 253 (private range = 192. 168. 0. 0 to 192. 168. 255. 255).

You recently installed a small office home office wireless router. To avoid security holes and bugs, what should you do to the router? Update the firmware.

ExplanationYou should update the firmware on the router to fix bugs or security holes. You will typically download the firmware and use a Web browser to update the firmware. Enable the DHCP service to assign IP addresses to hosts on the private network. Enable NAT so multiple computers can share the single IP address used on the Internet. Configure port triggering to dynamically open incoming ports based on outgoing traffic from a specific private IP address and port.

You need to add security for your wireless network. You would like to use the most secure method. Which method should you implement? WPA2

Explanation

Wi-Fi Protected Access 2 (WPA2) is currently the most secure wireless security specification. WPA2 includes specifications for both encryption and authentication. WPA was an earlier implementation of security specified by the 802. 11i committee. WEP was the original security method for wireless networks. WPA is more secure than WEP, but less secure than WPA2. Kerberos is an authentication method, not a wireless security method.

A customer has called and indicated that he thinks his neighbour is connecting to his wireless access point (WAP) to use his high-speed Internet

connection. Which of the following will help resolve this issue? Disable SSID broadcast on the WAP. Implement WPA2

ExplanationYou should disable SSID broadcast. Disabling SSID broadcast will make the WAP not appear when the unauthorized user is looking for available wireless networks. Implementing WPA2 will enable encryption and authentication on the WAP. Without the correct passphrase, the neighbour will not be able to connect to the wireless access point. Changing the signal channel sometimes helps eliminate interference problems with neighbouring wireless systems. however, network cards automatically detect the channel, so changing the channel offers no security benefits. By itself, 802. 11g is no more secure than any other wireless networking standard.

You have a small wireless network that uses multiple access points. The network uses WPA and broadcasts the SSID. WPA2 is not supported by the wireless access points. You want to connect a laptop computer to the wireless network. Which of the following parameters will you need to configure on the laptop? TKIP encryption. Preshared key.

ExplanationTo connect to the wireless network using WPA, you will need to use a preshared key and TKIP encryption. When using a preshared key with WPA, it is known as WPA-PSK or WPA Personal. AES encryption is used by WPA2. The channel is automatically detected by the client. The Basic Service Set Identifier (BSSID) is a 48-bit value that identifies an AP in an infrastructure network or a STP in an ad hoc network. The client automatically reads this and uses it to keep track of APs when roaming between cells.

You have a small wireless network with less than 50 client computers. You upgraded the hardware on two wireless devices so you can use a better security standard than WEP. Now you need to implement the new security standard. You need the greatest amount of security with the least amount of effort, and without replacing any of the wireless infrastructure. What should you do? Configure each client with the same key. Implement WPA2-AES.

Explanation

In this case, implementing WPA2 with AES and using the same pre-shared key on each client provides the greatest amount of security with the least amount of effort, and does not require the replacement of any of the wireless infrastructure. WPA-2 Enterprise uses 802. 1x for authentication and requires the configuration of an authentication server. WPA2 is more secure than WPA-PSK.

Which of the following is the primary device needed to set up a SOHO network? Wireless router

ExplanationA wireless router, or wireless access point is the primary device that is needed to set up a SOHO network. The router is the device that provides the connection that computers, printers, and mobile devices use to communicate with each other. (A wireless router can be a multi functioning device that also function as a modem, 4 port switch, NAT router, DHCP server, and a firewall.).

A cable or DSL modem provides the needed Internet connection, but a modem only gives one device access to the Internet. A SOHO network isn’t

possible unless the device you connect to the modem is a wireless router. A NAT router, a DHCP server, and a firewall are all very useful SOHO network services; wireless routers are available that include these functions.

List the general steps that are used to configure a SOHO router and set up the network. (Assume that the wireless router does not also function as a modem.). Configure the Internet connection.

Configure the wireless router.

Enable NAT.

Configure DHCP

Secure the SOHO network.

ExplanationThe general steps you would use to configure a SOHO router and set up the network are as follows:

– Configure the Internet connection- Begin by connecting the wireless router to the DSL or cable modem that provides the Internet connection, using the router’s WAN port. If the router does not automatically detect and configure the Internet connection follow the configuration instructions provided by the Internet Service Provider.

– Configure the wireless router- Before setting up the network, the default administrator username and password should be changed and the firmware on the router should be updated to fix bugs or security vulnerabilities.

– Enable NAT- Before the network host devices (computers, mobile devices, and printers) can receive IP addresses, NAT must be enabled on the router. NAT allows multiple computers to share a single public IP address used on the Internet. The host devices will communicate with each other using private network addresses from of the private address ranges.

– Configure DHCP- After NAT is configured to use a range of private network addresses, DHCP can be configured to assign IP addresses from that range to the host devices.

– Secure the SOHO network- Secure the SOHO network by; configuring the firewall on the router, configuring content filtering and parental controls, and physically securing the router.

There are other wireless communication technologies, but Wi-Fi based on the 802. 11 standard is the only practical option for the typical SOHO environment. A SOHO network does not need a server so you will generally not configure a network server. A SOHO network only uses one subnet, so there is no need to design a subnetting scheme. Using a wireless router means the physical network star topology is already determined.

When you enable quality of service (QoS) on a SOHO network, which of the following is an example of a network feature that could be implemented? Give VoIP network traffic higher priority and more bandwidth than HTTP (web browser) traffic.

ExplanationEnable quality of service (QoS) on a SOHO network allows you to prioritize certain network communications over others. For example, you

could give VoIP network traffic higher priority and more bandwidth than HTTP (web browser) traffic.

Enabling and configuring a demilitarized zone (DMZ) would allow you to cause all incoming port traffic to be forwarded to a specified DMZ host. Enabling the Universal Plug and Play (UPnP) and media content. Configuring content filtering and parental controls allows you to prevent hosts from accessing specific websites or using a specific Internet service, such as chat, torrent, or gaming applications.

You are installing a satellite connection so your home office can connect to the Internet. Which of the following statements is true? The satellite disk must be pointed in the correct direction for communicating with the satellite.

ExplanationDuring the installation, the satellite dish must be pointed in the correct direction for communicating with the satellite. With a single line satellite installation, the satellite connection is used for downloads and a phone line with a modem is used for uploads. Connect a satellite modem/router to the satellite disk using coaxial cable (RG-6) and a F-type connector. Connect the modem/router to your computer using a USB or Ethernet connection.

Which of the following are used to connect a cable modem the Internet connection? RG-6 coaxial cable. F-Type connectors

ExplanationCable modems connect to the service provider using coaxial cable (RG-6) and an F-Type connector. DSL routers and dial-up modems use

RJ-11 connectors. Ethernet uses Cat5 and Cat6 UTP cables and RJ-45 connectors.

To access the Internet through the Publicly Switched Telephone Network (PSTN), what kind of connectivity device must you use? Modem

Explanation

To establish a connection to Internet through the PSTN/POTS you must use a modem (modulator/demodulator) which converts digital PC data into analogue signals that can be transmitted through standard telephone lines. A CSU/DSU (Channel Service Unit/Data SErvice line. Data terminal equipment (DTE) is an end instrument that converts user information into signals for transmission or reconverts received signals into user information. Time-Division Multiplexing (TDM) is a type of digital or (rarely) analogue multiplexing in which two or more signals or bit streams are transferred apparently simultaneously as sub-channels in one communication channel, but physically are taking turns on the channel. A switch is a device for changing the course (or flow) of a circuit.

You are talking with a customer support technician on the telephone. The technician recommends downloading a particular driver from Internet. When you try to connect to the Internet using your modem, you can’t. What is the problem? You need to hang up.

ExplanationYou cannot talk on the telephone over the same line that the modem needs to use. When you try to connect with the modem, the line will be in use and the connection will fail because the modem can’t dial the

destination device. When troubleshooting a modem connection: Verify that the modem gets a dial tone. Verify that the modem dials the correct number. Verify that the receiving device answers the call. Verify network connection parameters (such as TCP/IP settings or connection settings). Verify any authentication or logon parameters.

Which type of network medium is used by an Integrated Services Digital Network (ISDN)? Copper telephone wire.

ExplanationISDN is a set of standard that allow digital data to be sent and received over copper wiring.

Which of the following network technologies is packaged as part of a BRI plan? ISDN

ExplanationISDN is a digital service operating over standard telephone company copper wiring offered in a variety of configurations. ISDN consists of multiple 64 Kbps channels. Basic Rate Interface (BRI) is a standard ISDN offering for household service.

Which of the following are features of Basic Rate ISDN (BRI)? Two data Channels.

One control channel.

Dial-up connection.

ExplanationBasic Rate ISDN service is a dial-up service consisting of two 64 Kbps data (bearer) channels and a single control (delta) channel. the two data channels can be used independently of each other or bonded together

to provide a total bandwidth of 128 Kbps. Primary Rate ISDN (PRI) shares many of the features of BRI, but includes up to 24 data channels.

When configuring an ADSL installation, where should you install the DSL filters? On connections leading to an analogue phone.

ExplanationFor ADSL installations, place filters (splitters) on the line everywhere that an analogue phone is used. Do not install a filter on the line connected to the DSL router or DSL card. An F-type connector is used in cable Internet and TV connections.

Which actions allow you to access the Internet on your laptop via a cellular network? Install a cellular USB adapter in an open port on the laptop.

ExplanationTo access content on your computer (laptop):

– Install a cellular adapter in a PCMCIA, ExpressCard, or USB slot.

– Install and configure the software to use the card.

An RJ-11 connection is typically for analogue phones, and is used for DSL, ISDN, and Dial-up Internet connections. Dial-up Internet connections use two ports on the modem:

– The LINE port connects the modem to the wall jack.

– The PHONE port connect the modem to the anlogue phone.

You can’t typically connect a USB device, such as a cellular adapter, to a wireless access point.

You are configuring an ADSL connection. Which of the following will be part of the configuration? RJ-11 connectors.

Filters or splitters.

Explanation

To connect to the internet through a DSL connection:

– Install an Internal DSL card in a single computer, or connect a DSL router to the phone line.

– Use a phone cable with an RJ-11 connector to connect the DSL or router to the phone line. For ADSL, place filters (splitters) on the line everywhere that an analogue phone is used.

– Do not install a filter on the line connected to the DSL router.

Analogue modems are used for dial-up Internet access. F-type connectors and RG-6 cables are used for cable Internet access.

A healthcare organization provides mobile clinics throughout the world and needs to transfer patient statistical data to a central database via the Internet. Which network technology should you select to ensure network connectivity for any clinic located anywhere in the world, even remote areas? Satellite

ExplanationSatellite capability is available even in areas that do not have a local network infrastructure. Satellite requires a local portable transmitter with an antenna directed skywards to a satellite. Satellite service providers

offer nearly 100% global network coverage by maintaining a series of satellites circling the earth in geosynchronous orbit. Dial-up, ISDN and cable modem, require a local network infrastructure provided by either the telephone company or cable television company.

Which of the following types of Internet connection services can allow you to be truly mobile while maintaining your Internet connection? Cellular

ExplanationCellular networking uses the cellular phone infrastructure for Internet access. The computing device, such as a notebook or table, must have a cellular antennae to connect directly to the cellular network. You can travel anywhere and stay connected to the network, as long as you are within the coverage are of the cellular service provider. You can also connect a computing device to a cellular network by tethering it to a smartphone or by using a smartphone as a Wi-Fi hot-spot.

Mobile hot-spots are devices that can be used to connect to a cellular network. Wi-Fi is a technology that provides wireless access to a computer network but is limited to the range of the wireless access point. Satellite networking requires a satellite dish, which is not truly mobile. ISDN is a land line based technology.

Which of the following are options for connecting a computing device, such as a notebook computer or a tablet, to a cellular network? Use a USB cable to connect the device to the network through a smartphone.

Use the device’s Wi-Fi to connect to the network through a cellular Wi-Fi hot spot.

Use an integrated cellular antennae to connect the device directly to the cellular network.

Use a USB cellular antennae to connect the device directly to the cellular network.

Explanation

You can connect a computing device, such as notebook computer or a tablet, to a cellular network by using any of these four options:

– Use a USB cable to connect the device to the network through the smartphone.

– Use the device’s Wi-Fi to connect to the network through a cellular Wi-Fi hot spot.

– Use a USB cellular antennae to connect the device directly to the cellular network.

– Use an integrated cellular antennae to connect the device directly to the cellular network.

A transmitter antennae, or a dish, to communicate with a satellite will connect you to a satellite network, not a cellular network. Connecting to the cable service will also not connect you to a cellular network. Cable is a separate type of networking service.

A portable computer connected to a printer with an infrared interface works fine inside your office. However, when you go outside it works sporadically. How can you fix this? Move the printer closer to the computer.

Block any direct and reflected sunlight from the pathway between the PC and the printer.

Explanation

Infrared light is light that is near visible in the electromagnetic spectrum. Therefore very bright lights and in particular sunlight may cause interference with infrared interfaces. The best way to manage this interference is to minimize the distance between the connected devices and minimize interfering sunlight.

You want to use a wireless keyboard and mouse with your laptop computer. Which method you choose? Bluetooth

Explanation

Bluetooth would be the best choice because it has a high transfer rate and because it automatically detects other Bluetooth devices in the area and creates an encrypted PAN between them. 802. 11g is a wireless networking standard for communicating between computers, not for connecting wireless devices to a computer. PS/2, IEEE 1394 (FireWire), and USB are all wired connections standards.

What is the maximum range of the Bluetooth 2. 0 specification for Class 1 devices? 100 M

Explanation

Bluetooth version 2. 0 class 1 devices have a maximum range of about 100 meters. Earlier versions had a maximum range of only about 10 meters.

Which of the following are characteristics of Bluetooth? 2. 4 GHz radio wireless.

Ad hoc connecitons.

Explanation

Bluetooth is a wireless networking standard that uses 2. 4 GHz radio waves. These are the same type of radio waves used with 802. 11 wireless networking, so radio transmission can go through walls (not limited to line-of-sight connections). Bluetooth uses ad hoc connections between devices. Infrared uses red spectrum light waves and is limited to line-of-sight transmissions.

What is the maximum transmission speed for Bluetooth v3 and v4 devices? 24 Mbps

Explanation

Bluetooth v3 and v4 devices have a maximum transmission speed of up to 24 Mbps.

Bluetooth v1. 2 devices have a maximum transmission speed of up to 1 Mbps. Bluetooth v2 devices have a maximum transmission speed of up to 3

Mbps. The wireless standard 802. 11b transmits data at a rate of up to 11 Mbps.

You need a type of wireless connection that can transfer data between your phone, PDA, and laptop. You are transferring sensitive information. Which would be the best choice? Bluetooth

Explanation

A Bluetooth connection would be the best choice because it automatically detects Bluetooth-enabled devices and creates a wireless PAN between them. It can be used for both voice and data signals, and it also provides 128-bit encryption to protect sensitive information in transit. Infrared is a line-of-sight medium so it may be difficult to maintain connectivity, it also doesn’t provide encryption. Cellular WAN provides very little security for information in transit and requires a cellular connection for each device. Wireless Ethernet is used for transferring data, not connecting devices.

You want to use a wireless printer at home. The printer will be used by two computers in two different rooms. Which interfaces could be used to do this? Wireless Ethernet

Explanation

You could use an 801. 11 wireless Ethernet connection for the printer. 802. 11 wireless Ethernet has a greater range than infrared, and will go through walls. The other interfaces are wired interfaces. IEEE 1394 is Firewire. IEEE 1284 is parallel.

Which of the following wireless communication technologies can be described as follows?

– Has a very limited transmission range, of less than two inches.

– Used with credit cards and passports.

– Slower than other wireless technologies.

– Constantly emitting a signal.

NFC

Explanation

Near Field Communication, or NFC, uses the 13. 56 MHz frequency and has a very short range- in order for devices to communicate, they have to be within two inches of each other. NFC chips are being used for such applications as passports and credit cards to contain all the information about the passport holder or the credit card account. NFC chips use encryption algorithms to secure the connection but are constantly emitting a signal and use a much slower transmission speed than other wireless technologies.

Up to 100 meters for Class 1 devices. Bluetooth

Up to 30 meters in areas without interference. Infrared

Up to 10 meters for Class 2 devices. Bluetooth

ExplanationRadio frequency wireless transmissions can reach up to 356 meters, depending upon the 802. 11 standard used and interference present in the environment.

Infrared wireless transmission work best for devices within 1 meter, but can operate up to 30 meters in areas without ambient light interference.

The maximum Bluetooth transmission distance depends on the device class:

– Class 3 devices transmit up to 1 meter.

– Class 2 devices transmit up to 10 meters.

– Class 1 devices transmit up to 100 meters.

ScenarioRecently, you implemented a wireless network at your home. However, without additional configuration, the wireless access point will allow connections from any laptop or mobile device. You need to secure the wireless network from unauthorized connections.

In addition, you suspect that wireless access points used by your neighbours are interfering with your access point. You’ve discovered that they are using channels 2 and 5 for their wireless networks.

Your task in this lab is to secure the wireless network as follows:

– Use PoliceSurveillanceVan for the SSID. Note: The SSID name is case sensitive.– Disable SSID broadcasts.– Set the channel such that it doesn’t conflict with access points in neighbouring homes.– Use WPA2-PSK authentication, with AES for encryption. Configure S3CuR31! as the security

key. Note: The security key is case sensitive.– Only allow devices with following hardware addresses to connect to the wireless network:– 00: 87: FC: E2: E5: D2.– 00: 50: 56: C0: 00: 08.– 00: 87: FC: E2: E5: F2– Change the administrator authentication credentials on the wireless access point to:– Username: @dm1n– Password: @Rd.

Explanation

Complete the following steps:

1. In the Windows Security pop-up dialogue, click OK.

2. Click Wireless > Basic on the left of the web page.

3. Change the SSID name.

4. Disable SSID broadcasts.

5. Set the wireless channel to 7 or higher.

6. Scroll down and click Apply.

7. In the pop-up dialogue, Click OK.

8. Click Wireless > Security on the left of the web page.

9. Change the authentication (Security Mode) for the PoliceSurveillanceVan SSID.

10. Enter the security key (Pass Phrase), and click Apply.

11. Click Wireless > MAC Filer on the left of the web page.

12. Set the policy to Allow all, then click Apply.

13. In the pop-up dialogue, click OK.

14. In the MAC Address field, enter the first allowed MAC address, then click Apply.

15. Add the remaining allowed MAC addresses in the same manner.

16. Click Administrator > Management on the left of the web page.

17. Change the administrator authentication credentials, and click Apply.

Which of the following features on a wireless network allows or rejects client connections based on the hardware address? MAC address filtering

Explanation

MAC address filtering allows or rejects client connections based on the hardware address. Wi-Fi Protected Access (WPA2) provides encryption and user authentication for wireless networks. Wired Equivalent Privacy (WEP) also provides security, but WPA2 is considered more secure than WEP. The SSID is the network name or identifier.

Which of the following is used on a wireless network to identify the network name? SSID

Explanation

Wireless devices use the SSID (Service Set Identification) to identify the network name. All devices on a wireless network use the same SSID. The

MAC address is a unique physical device address. The WPA2 Personal passphrase and the WEP key are both mechanisms used to secure wireless communications.

Which type of configuration would you use if you wanted to deploy 802. 11n technology to communicate directly between two computers using a wireless connection? Ad hoc

Explanation

Configure an ad hoc connection to connect one computer directly to another using a wireless connection. An infrastructure configuration users a Wireless Access Point (WAP) to create a network. Devices communicate with each other through the WAP. WEP is a security mechanism used for authentication.

You are designing a wireless network for a client. Your client needs the network to support a data rate of at least 150 Mbps. In addition, the client already has a wireless telephone system installed that operates 2. 4 GHz. Which 802. 11 standard will work best in this situation? 802. 11n

Explanation

802. 11n is the best choice for this client. 802. 11b and 802. 11g both operate in the 2. 4 GHz to 2. 4835 GHz range, which will cause interference with the client’s wireless phone system. 802. 11a operates in the 5. 725 GHz to 5. 850 GHz frequency range, which won’t interfere with the phone system. However, its maximum speed is limited to 54 Mbps.

Which of the following are characteristics of the 802. 11g wireless standard?- Backwards compatible with 802. 11b devices.

– Have a maximum bandwidth of 54 Mbps.

– Are backwards compatible with 802. 11b networks.

Explanation

802. 11b provides 11 Mbps bandwidth. 802. 11a operates in the 5. 75 GHz range. For this reason, 802. 11a is not compatible with 802. 11b or 802. 11g.

Which of the following locations will contribute the greatest amount of interference for a wireless access point. Near backup generators.

Near cordless phones.

Explanation

Other wireless transmitting devices (such as cordless phones or microwaves) and generators cause interference for wireless access points. In general, place access points higher up to avoid interference problems caused by going through building foundations. DHCP servers provide IP information for clients and will not cause interference.

Which of the following recommendations should you follow when placing wireless access points (WAPs) to provide wireless access for users within your company building? Place WAPs above where most clients are.

Explanation

Devices often get better reception from WAPs that are above or below. If possible, place WAPs higher up to avoid interference problems caused by going through building foundations. For security reasons, do not place WAPs near outside walls. The signal will extend outside beyond the walls. Placing the WAP in the centre of the building decreases the range of the signals available outside of the building. When using multiple WAPs, place access points evenly through the area, taking care to minimize the overlap of the broadcast area while ensuring adequate coverage for all areas.

You have been contacted by OsCorp to recommend a wireless Internet solution. The wireless strategy must support a transmission range of 150 feet, use a frequency range of 2. 4 GHz, and provide the highest possible transmission speeds. Which of the following wireless solutions would you recommend? 802. 11n

Explanation

Of the technologies listed, only the IEEE 802. 11n wireless standard addresses the desired requirements. The 802. 11a wireless standard offers maximum speeds of 54 Mbps and uses the 5 GHz frequency range. The 802. 11g wireless standard offers maximum speeds of 54 Mbps. 802. 11b uses he 2. 4 GHz frequency range but supports only 11 Mbps transfer speeds.

Which wireless standard has the highest data transfer rates? 802. 11n

Explanation

802. 11n has the highest data transfer rates, up to (theoretically) 600 Mbps. 802. 11a and g have speeds up to 54 Mbps or 108 Mbps when using channel bonding. 802. 11b has speeds up to 11 Mbps.

You are designing a wireless network for a client. Your client needs the network to support a data rate of at least 54 Mbps. In addition, the client already has a wireless telephone system installed that operates 2. 4 GHz. Which 802. 11 standards will work best in this situation? 802. 11a

802. 11n

Explanation802. 11a or 802. 11n are the best choices for this client. While both 802. 11a and 802. 11g each operate at 54 Mbps, 802. 11g operates in the 2. 4 GHz to 2. 4835 GHz range, which will cause interference with the client’s wireless phone system. 802. 11a and 802. 11n, on the other hand, operate in the 5. 725 GHz to 5. 850 GHz frequency range, which won’t interfere with the phone system. 802. 11n can operate at speeds up to 300 Mbps.

You are designing an update to your client’s wireless network. The existing wireless network uses 802. 11b equipment, which your client complains runs too slowly. She want to upgrade the network to run at 150 Mbps. Due to budget constraints, your client wants to upgrade only the wireless access points in the network this year.

Next year, she will upgrade the wireless network boards in her users’ workstations. She has also indicated that the system must continue to function during the transition period.

Which 802. 11 standard will work best in this situation?

802. 11n

Explanation802. 11n is the best choice for this client. Both 802. 11a and 802. 11g each operate at a maximum speed of 54 Mbps. 802. 11a isn’t compatible with 802. 11b network boards. 802. 11n access points, on the other hand, are backwards-compatible with 802. 11b equipment and run at speeds of up to 300 Mbps. using this type of access will allow the wireless network to continue to function during the transition.

Which of the following wireless networking standards uses a frequency of 5 GHz and supports transmission speeds up to 1. 3 Gbps. 802. 11ac

Explanation

The 802. 11ac standard uses the 5 GHz frequency and supports data tra