line. Although the Internet is used, it is private because the link is encrypted and convenient to use. A medium sized business needing a secure way to connect several offices will find this a good choice.

9. Clear employee guidelines should be implemented for using the Internet, including access to non-work related websites, sending and receiving information.
10. Individual accounts to log on and access company intranet and Internet with monitoring for accountability.
11. Have a back-up policy to recover data in the event of a hardware failure or a security breach that changes, damages or deletes data.
12. Disable Messenger.
13. Assign several employees to monitor a group like CERT which studies Internet security vulnerabilities and develops training to help improve security.

Large businesses :

1. A strong firewall and proxy, or network Guard, to keep unwanted people out.
2. A strong Antivirus software package and Internet Security Software package.
3. For authentication, use strong passwords and change it on a weekly/bi-weekly basis.
4. When using a wireless connection, use a robust password.
5. Exercise physical security precautions to employees.
6. Prepare a network analyzer or network monitor and use it when needed.
7. Implement physical security management like closed circuit television for entry areas and restricted zones.
8. Security fencing to mark the company's perimeter.
9. Fire extinguishers for fire-sensitive areas like server rooms and security rooms.
10. Security guards can help to maximize physical security.

School :

1. An adjustable firewall and proxy to allow authorized users access from the outside and inside.
2. Strong Antivirus software and Internet Security Software packages.
3. Wireless connections that lead to firewalls.
4. Children's Internet Protection Act compliance. (Only schools in the USA)
5. Supervision of network to guarantee updates and changes based on popular site usage.
6. Constant supervision by teachers, librarians, and administrators to guarantee protection against attacks by both internet and sneakernet sources.
7. An enforceable and easy to understand acceptable use policy which differentiates between school owned and personally owned devices
8. FERPA compliance for institutes of higher education network

Large government :

1. A strong firewall and proxy to keep unwanted people out.
2. Strong antivirus software and Internet Security Software suites.
3. Strong encryption.
4. White list authorized wireless connection, block all else.
5. All network hardware is in secure zones.
6. All hosts should be on a private network that is invisible from the outside.
7. Host web servers in a DMZ, or a firewall from the outside and from the inside.
8. Security fencing to mark perimeter and set wireless range to this.
9. Inventory controls of government owned mobile.

Q24. Define different types of Security management.

Ans. Security management for networks is different for all kinds of situations. A home or small office may only require basic security while large businesses may require high-maintenance and advanced software and hardware to prevent malicious attacks from hacking and spamming. Different kinds of situations for security management network are as follows :

Homes & Small Businesses :

1. Basic firewall or a unified threat management system.
2. For Windows users, basic Antivirus software. An anti-spyware program would also be a good idea. There are many other types of antivirus or anti-spyware programs available.
3. When using a wireless connection, use a robust password. Also one could try to use the strongest security supported by their wireless devices, such as WPA2 with AES. TKIP may be more widely supported by their devices and should only be considered in cases where they are NOT compliant with AES.
4. If using Wireless: Change the default SSID network name, also disable SSID Broadcast; as this function is unnecessary for home use. (Security experts consider this to be easily bypassed with modern technology and some knowledge of how wireless traffic is detected by software).
5. Enable MAC Address filtering to keep track of all home network MAC devices connecting to one's router. (This is not a security feature per se; However it can be used to limit and strictly monitor one's DHCP address pool for unwanted intruders if not just by exclusion, but by AP association.)
6. Assign STATIC IP addresses to network devices. (This is not a security feature per se; However it may be used, in conjunction with other features, to make one's AP less desirable to would-be intruders.)
7. Disable ICMP ping on router.
8. Review router or firewall logs to help identify abnormal network connections or traffic to the Internet.
9. Use passwords for all accounts.
10. For Windows users, Have multiple accounts per family member and use non-administrative accounts for day-to-day activities.
11. Raise awareness about information security to children.

Medium businesses :

1. A fairly strong firewall or Unified Threat Management System
2. Strong Antivirus software and Internet Security Software.
3. For authentication, use strong passwords and change them on a bi-weekly/monthly basis.
4. When using a wireless connection, use a robust password.
5. Raise awareness about physical security to employees.
6. Use an optional network analyzer or network monitor.
7. An enlightened administrator or manager.
8. Use a VPN, or Virtual Private Network, to communicate between a main office and satellite offices using the Internet as a connectivity medium. A VPN offers a solution to the expense of leasing a data line while providing a secure network for the offices to communicate. A VPN provides the business with a way to communicate between two in a way mimics a private leased