**Question 1**Discuss basic configurations you would do in the following LAN components:

1. **Proxy server**Proxy server is a machine which acts as an intermediary between the computers of local area network and the internet, e.g. squid  
   Basic configurations

* Install the package squid from the package group: Network/Server
* The configuration of squid is included in the file: /etc/squid/squid.conf
* To allow access from the client, change the entries at acl and http\_access.
* For security reasons, change the settings for http\_port.
* To enable access to the proxy server from the router, leave the entry http\_access allow localhost in the configuration.

1. **DHCP server**  
   Basic configurations

* Configure a DHCP database agent or disabling DHCP conflict logging
* Excluding IP addresses since the DHCP server assumes that all addresses in the address pool are available for assigning to clients
* Configure DHCP address pool
  + Configure the DHCP Address Pool Name and Entering DHCP Pool Configuration Mode
  + Configure the DHCP Address Pool Subnet and Mask
  + Configure the Domain Name for the Client
  + Configure the IP Domain Name System Servers for the Client
  + Configure the NetBIOS Windows Internet Naming Service Servers for the Client
  + Configure the NetBIOS Node Type for the Client
  + Configure the Default Router for the Client
  + Configure the Address Lease Time

1. **Web server**  
   A web server e.g. apache has three configuration files, that is, access.conf – specifies what hosts and users are allowed access to what documents and services, srm.conf – specifies how your server’s documents are organized and formatted, httpd.conf – specifies options that govern the operation of the httpd daemon

* Host name

1. **Router**  
   • Enable the router’s firewall.  
   • Set a Service Set Identifier*,* or SSID*,* for your wireless network.  
   • Set the encryption for the network, known as the WEP, or Wired Equivalent Privacy which is the password  
   • Configure the base station to allow connections only from known computers.  
   • Tell the wireless router to provide IP addresses dynamically for all computers on the network.
2. **WAP**

* Change the default admin password
* IP address: change the IP address to match your network.
* Radio channel:  set the radio channels in wireless access points within range of each other to different channels to prevent them from interfering with each other.
* Service set identifier (SSID): change the SSID to a non-default value to minimize unauthorized users from associating with the access point.
* Encryption: enable wired equivalent privacy (WEP), which encrypts the frame body of each data frame.
* Authentication: many wireless access points include 802.1x mechanisms that authenticate users with an external authentication server.
* Administrative interfaces: disable the console port of the access point to avoid an unauthorized person reconfiguring encryption and authentication functions.

**Question 2**  
Discuss the difference between IPv4 and IPv6 and explain ways currently implemented to smoothly transit from IPv4 to IPv6

|  |  |
| --- | --- |
| IPv4 | IPv6 |
| Broadcast messages are available | Broadcast messages are not available. |
| Fragmentation is done by sender and forwarding routers | Fragmentation is done only by sender |
| IPv4 addresses are 32 bit length | IPv6 addresses are 128 bit length |
| IPv4 addresses are binary numbers represented in decimals. | IPv6 addresses are binary numbers represented in hexadecimals. |
| IPSec support is only optional | Inbuilt IPSec support |
| Checksum field is available in IPv4 header | No checksum field in IPv6 header. |
| No packet flow identification. | Packet flow identification is available within the IPv6 using the flow label field |
| Address Resolution Protocol (ARP) is available to map IPv4 address to MAC addresses | Address Resolution Protocol (ARP) is replaced with a function of Neighbour Discovery Protocol (NDP) |
| Internet Group Management Protocol (IGMP) is used to manage multicast group membership. | IGMP is replaced with multicast Listener Discovery (MLD) messages |
| Manual configuration (static) of IPv4 addresses or DHCP (dynamic) is replied to configure IPv4 addresses. | Auto-configuration of addresses is available |

Ways currently used to smoothly transit from IPv4 to IPv6

**Dual stack routers**  
Routers can be installed with both IPv4 and IPv6 addresses configured on its interfaces pointing to the network of relevant IP scheme. A server having an ipv4 and ipv6 addresses configured for it can speak with all the hosts on both the ipv4 as well as the ipv6 networks with the help of a dual stack router.

**Tunnelling**   
Tunnelling enables users data pass through a non-supported IP version. This is achievable for instance when two remote IPv4 networks can communicate via a tunnel, where the transit network was on IPv6. Likewise, this is also possible where the transit network is on ipv6 and the remote sites that intend to communicate on IPv4.

**NAT Protocol Translation**  
This is facilitated by NAT-PT (Network Address Translation –Protocol Translation) enabled device. A host with IPv4 address sends a request to an IPv6 enabled server on internet that does not understand IPv4 addresses but with the help of NAT-PT device communication is achieved.

**Question 3**  
You have been employed as Network Administrator in a university. The university currently has five thousand users of the network. You are planning to use private IPs behind a proxy server.

1. State with reason the IPv4 address class recommended for the network.
2. Explain the role of a NAT device to be used in the network
3. State sample private IPs to be used in the network
4. Explain why you will need at least two public IPs
5. Using an appropriate program, design the University LAN showing all the relevant devices in the network and sample IPs recommended above