Question 1

Dig is a command for querying domain servers, so running dig on a domain name gives all the information that DNS has on a particular domain name. For example, it shows not only the associated IP but also information on the name servers associated with a particular domain name.

Ping shows sends an ICMP packet to a server. If the remote server is alive and up it responds with another ICMP packet, the ping command shows this response along with the amount of time it took to receive this response. Using this information one can determine the latency between the local server and a remote server.

Traceroute shows the routing between a local server and a remote server. It shows each server a packet travels through when attempting to reach a destination. It also shows how long it’s taking for a packet to reach each jump on its route to the remote host. Sometimes traceroute will return a ‘*’, this occurs when it hits a firewall that doesn’t allow the traceroute traffic through.

Question 2

The following screenshot shows the output of ‘dig www.cs.csub.edu’ and ‘dig soa www.cs.csub.edu’.
Using just dig without the soa flag will return the IP address of a given domain name and its name servers. The difference using the soa flag is it shows the Start of Authority record. This shows authoritative information about the DNS zone that the domain name is in. DNS is a hierarchical system so the SOA defines DNS information for all those within its zone. Running 'dig +trace www.cs.csub.edu' will show name servers that are further up the hierarchy.

**Question 3**

'dig soa 209.9.244.in-addr.arpa' is the correct command to find the SOA record for the network. 'in-addr.arpa' can be appended to a IP address to do a reverse domain name lookup. Performing a DNS lookup on a individual server's IP will return the domain name for that server. By appending 'in-addr.arpa' to a Class C network and running the dig command you can determine what SOA that network is in. Ping is wrong because it only shows...
whether a server is up and its latency.

**Question 4**

‘unknown host’ generally means that the domain name didn’t resolve to a valid IP address or there was a problem with looking up the IP address. If this message occurs when an IP address is the argument, it means that the IP address is not valid. I would try pinging nameservers to see if there was a problem with DNS. I would try to ping the same domain name or IP, which would likely result in the same message. Then I would use dig to attempt to see if it returned a valid IP. If it didn’t and I was reasonably sure it was a valid host name, I would try running dig from another machine or looking up the IP using a web-based service as there might be an issue with the local host’s DNS service.

**Question 5**

This differs from the previous error message in that it means that the host is valid, but the connection fails for some reason. This could be a failure of routing or a problem with the server itself. I would again first use ping which would likely fail. Then I would run traceroute to see if there was a problem reaching the server. If I was reaching the server ok I would check to make sure that the ftp service or whatever service I am trying to use is running on the remote server.