Solutions to Assignment 3

Question 1

The answer will be different for each name. In this example I'll use the generic name "John Doe".

(a) "John Doe" has 8 characters.

(b) The SHA-1 cryptographic hash of "John Doe" is:

```
ae6e4d1209f17b460503904fad297b31e9cf6362
```

(c) The length of the SHA-1 hash value is 160 bits. In hexadecimal notation this requires 40 characters.

(d) The SHA-1 cryptographic hash of "John doe" is:

```
7f4ab9b2bf9680bd2237e633adb88bdef11060be
```

only one bit in the string changed (upper-case 'D' is 0x44 and a lower-case 'd' is 0x64).

(e)
```
ae6e4d1209f17b460503904fad297b31e9cf6362
7f4ab9b2bf9680bd2237e633adb88bdef11060be
----------------------------------------
       *                 **    *       *
```

As indicated by the positions of the asterisks above, five of the characters in the hexadecimal representation did not change, while the other 35 changed.

(f) Each character represents four bits. Consider the two characters in one position. The probability that the second hash value has the same character (the same four bits) is $\frac{1}{16}$ (once the first number is determined, the probability that the second matches it is 1/16).

The number of matches has a binomial probability distribution with a mean $\frac{40}{16} = 2.5$.

Question 2

(a) An IPv6 address has 128 bits. The most-significant 64 bits are used for routing while the least-significant 64 bits are used to identify a host in a network.

(b) The answer will depend on your ISP. As of December 2017, the Vancouver area, Telus supports IPv6 but Shaw does not. All widely-used operating systems (Windows, Mac OS, Linux) support IPv6.

(c) The DNS query `nslookup -type=AAAA www.bcit.ca` does not return an IPv6 address while the same query for netflix.ca returns a series of addresses in the network `2620:108:700f::`.

Question 3

(a) According to the Cisco documentation, the command:

`Router(config)#` **ip dhcp ping packets** *number*

sets *"The number of ping packets that are sent before the address is assigned to a requesting client."*

(b) A DHCP server can be manually configured with IP addresses for specific hosts (via a MAC address to IP address mapping). This is useful when the host's IP address must be set to a specific value. For example if that host provides services and other devices must be configured with the server address (instead of the name).

Question 4

There are various ways to write the BIND records, but the simplest is probably:

```
www.schoolbuds.ca.  A   104.238.64.106
schoolbuds.ca.      MX  10 www.schoolbuds.ca.
```

which would add an 'A' (address) resource record for the domain name `www.schoolbuds.ca` with the value 104.238.64.106 and an MX record with priority 10 that points to the same host.