CE155 Assignment 1 – Cisco CCNA1 Skills Test

John Woods – January 2016 v1.6

**Note:** The assignment brief consists of two parts:

1. This document – a generic document describing the assignment.

2. An individual set of parameters for each student, (available from where you obtained this document) with each student page indexed via registration number. This is your “unique parameter web page”.

**Where you will submit the assignment:** Electronic submission server.

**When you will submit it:** Please check entry on Faser for the deadline date and time

**What you will submit:** A single document. The contents are summarised below, but see the individual parts for full details:

Part 1: Tables 1 and 2 completed according to the specification.

Part 2: A description of the efficiency of the address assignment and how to improve it.

Part 3: A description of the two application layers protocols that you have been allocated.

**Marking schedule:**

Part 1: 38% spread equally across the table elements.

Part 2: 22% broken down as:

15% for the technical content.

7% for presentation and English usage.

Part 3: 40% broken down as:

20% for the technical description of the protocols.

10% for presentation and English usage.

10% for including a reference for each protocol and citing it with correct context.

**1. Address assignment**

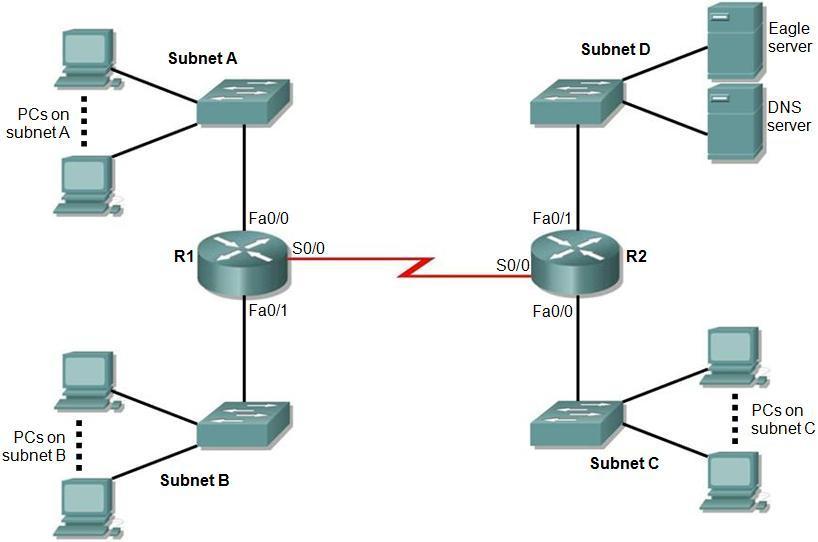


Figure 1. Topology diagram.

Figure 1 shows a network topology with five IP subnets. By referring to your unique parameter web page you will find you have been allocated:

* The number of PCs on subnets A, B and C.
* An address range for you to use.
* A subnet mask length to use for ALL the five subnets.

Your task is to assign IP addresses to the devices in the network. You will fill in Table 1 and Table 2 with appropriate information bearing in mind the values on your unique parameter web page and the following facts:

* In addition to the PCs, each router interface needs a “host” IP address and it is part of the subnet.
* Only the DNS server and Eagle server are on Subnet D.
* Switches are not allocated IP addresses in this network.
* PCs and servers are to be allocated the lowest IP addresses in each subnet.
* Router interfaces are to be allocated the highest IP addresses in each subnet.
* The subnets are to be allocated in the order A, B, C, D and E, (i.e. A is the lowest address and E is the highest).

In Table 2, it is only necessary to indicate the first and last address of the PCs in each subnet using the lowest block of addresses.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subnet | Network address | Mask in dotted decimal form  (e.g. 255.255.0.0) | Number of hosts, including PCs and router interfaces | Number of unused addresses |
| A | 192.168.77.0 | 255.255.255.192 | 17 | 45 |
| B | 192.168.77.64 | 255.255.255.192 | 9 | 53 |
| C | 192.168.77.128 | 255.255.255.192 | 20 | 42 |
| D | 192.168.77.192 | 255.255.255.192 | 3 | 59 |
| E | 192.168.78.0 | 255.255.255.192 | 2 | 60 |

Table 1. Subnet details.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Device | Interface | IP address | Mask in dotted decimal form  (e.g. 255.255.0.0 for /16) | Default Gateway |
| R1 | Fa0/0 | 192.168.77.62 | 255.255.255.192 | N/A |
| Fa0/1 | 192.168.77.126 | 255.255.255.192 | N/A |
| S0/0 | 192.168.78.62 | 255.255.255.192 | N/A |
| R2 | Fa0/0 | 192.168.77.190 | 255.255.255.192 | N/A |
| Fa0/1 | 192.168.77.254 | 255.255.255.192 | N/A |
| S0/0 | 192.168.78.61 | 255.255.255.192 | N/A |
| 1st PC subnet A | NIC | 192.168.77.1 | 255.255.255.192 | 192.168.77.62 |
| Last PC subnet A | NIC | 192.168.77.16 | 255.255.255.192 | 192.168.77.62 |
| 1st PC subnet B | NIC | 192.168.77.65 | 255.255.255.192 | 192.168.77.126 |
| Last PC subnet B | NIC | 192.168.77.73 | 255.255.255.192 | 192.168.77.126 |
| 1st PC subnet C | NIC | 192.168.77.129 | 255.255.255.192 | 192.168.77.190 |
| Last PC subnet C | NIC | 192.168.77.148 | 255.255.255.192 | 192.168.77.190 |
| 1st PC subnet D | NIC | 192.168.77.193 | 255.255.255.192 | 192.168.77.254 |
| Last PC subnet D | NIC | 192.168.77.194 | 255.255.255.192 | 192.168.77.254 |
| DNS server | NIC | 192.168.77.193 | 255.255.255.192 | 192.168.77.254 |
| Eagle server | NIC | 192.168.77.194 | 255.255.255.192 | 192.168.77.254 |

Table 2. Addressing table.

**2. Analysis of address space usage**

You will submit an explanation encompassing:

* A statement on how many further subnets are available using the address range and mask that you have been allocated.
* A comment on how efficiently the address space you have been allocated has been used.
* A brief description of how the address space you have been allocated could be utilised more efficiently to leave a maximum number of addresses free for future expansion. You should not state any actual addresses but rather provide a general description of the process used.

My range of subnets was 8 total subnets, 5 subnets were used, with 3 not being utilized at all, (all from my last address range 192.168.78.255) and each subnet consists of 64 blocks. The address range has been used very poorly; my minimum number of unused addresses was 42, and the addition of 3 subnets from my last address range (192.168.78.255) were not used at all. VLSM could have been used to reduce redundancy and assign host positions within the network. VSLM divides an IP into subnets of different sized without wasting the IP addresses, making it easy to create subnets with different host counts without wasting IP addresses.

**3. Application layer services**

In your unique parameter web page you have been allocated two application layer services. In most cases the name is given as an abbreviation.

For each one, provide:

* The full title of the protocol if it is given in abbreviated form (e.g. HTTP is hypertext transfer protocol)
* A brief description of the purpose of the application
* The transport layer protocol (or protocols) usually used to transport the application protocol
* The normal (well known) transport layer port(s) that the protocol uses (some may use more than one)
* A very brief description of how the protocol works, for example the key messages sent by the protocol
* A full reference to either: a book, published article, or standards document that describes the protocol. The reference should be included at a suitable point in your description of the protocol. A web reference (except to a standards document) is unacceptable. For example HTTP is defined in RFC 2626 [1], described in a journal paper by Janssen [2] and also described by Tanenbaum [3]. Note how a recognised reference standard is used here as an example to a standards document, a scholarly article and finally a well-known text book.

Telnet

A TELNET or Transmission Control Protocol [1] defined in RFC854 is a connection used to transmit data with interspersed TELNET control information.

TELNET protocol allows you to set up TCP/IP connections to a host (it accepts both IP addresses or a domain name is a remote access point). The TELNET protocol allows a user to interface terminal devices and terminal-oriented processes to each other.

A user will be on a local system and invoke a TELNET program by typing “telnet xxx.xxx.xxx” where x = host or IP address. The program will then establish a connection. Now the client program accepts keystrokes from the user and relays them to the TELNET server, which are then passed to a terminal server. TELNET then determines a Network Virtual Terminal. When a user TELNETS to a site that isn’t on the server, its deemed to be on an NVT, the client program translates the keystrokes from the terminal into NTV format. This is then translated back into the format needed by the destination host. [2]

The NTV format defines all characters as 8 bits long, 1 for common sequences and 7 bits for ASCII encoded data. The ASCII characters are divided into 95 printable characters and 33 control codes, for example: decimal 67 = “C” decimal 99 = “c”.

Useful TELNET options commands are IP- Interrupt process, AO – Abort output, EC- Erase character, SYNCH- Synchronize and QUIT for quitting the program.

Useful basic TELNET commands are:

IP - Interrupt Process

AO - Abort Output

AYT - Are You There

EC - Erase Character

EL - Erase Line

SYNCH - Synchronize

QUIT - Quit session

NNTP

NNTP or Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer system over packet switched variable latency data networks defined by NNTP Wikipedia article [1] and D. Mills, U. Delaware, J. Martin in “Network Time Protocol”.

NTP is widely used to synchronize system clocks among a set of distributed time servers and clients. It describes the core architecture, protocol, state machines, data structures, and algorithms. [2] D. Mills, U. Delaware, J. Martin in “Network Time Protocol”.

NTPv4 includes fundamental improvements in the mitigation and discipline algorithms that extend the potential accuracy to the tens of microseconds with modern workstations and fast LANs. It includes a dynamic server discovery scheme, so that in many cases, specific server configuration is not required. It corrects certain errors in the NTPv3 design and implementation and includes an optional extension mechanism.

This program assumes the integer data type is 32 bits and the long data type is 64 bits. The native data type used in most calculations is floating double. The data types used in some packet header fields require conversion to and from int and double representation. Some header fields involve partitioning into 8 bits, otherwise known as an octet. [2] D. Mills, U. Delaware, J. Martin “Network Time Protocol”.

The IPv4 address is 32 bits, while the IPv6 address is 128 bits.

**4. References**

[1] R. Fielding et al., Hypertext Transfer Protocol -- HTTP/1.1, IETF RFC 2626, June 1999. Available from: http://www.ietf.org/rfc/rfc2616.txt

[2] W. C. Janssen, “A next generation architecture for HTTP,” IEEE Internet Computing, Volume 3, Issue 1, Jan.-Feb. 1999, pp 69-73.

[3] A. S. Tanenbaum, *Computer Networks*, Pearson Education, 4th ed., 2007.

Telnet:

[1] J. Poster and J. Reynolds “Telnet protocol specification”, F

RFC 854, May 1983. Available from: <https://tools.ietf.org/html/rfc854>

[2] J. Davidson, J.Postel, N.Mimno, R.Thomas, D.Walden Telnet protocol: Its purpose, principles, implementation and operating system design, September 1977. Available from: <http://dl.acm.org/citation.cfm?doid=800103.803338>

NNTP:

[1] Wikipedia, 43 references on site. Available from: <https://en.wikipedia.org/wiki/Network_Time_Protocol>

[2] D. Mills, U. Delaware, J. Martin “Network Time Protocol”, IETF Internet Engineering Task Force, June 2010. Available from: https://tools.ietf.org/html/rfc5905