Chapter 1 Review Question Answers

1. To establish an open, flexible and standard networking software architecture which would be used as a framework to guide the compatible implementation of protocols and technology

2. No functionality is missing. The TCP/IP stack incorporates the functions of the OSI Application, Presentation and Session layers in its Application layer. This is an example of the flexibility of the OSI architecture concept. Another example is the NetWare stack that does not have seven layers.

3. SNMP is part of the Application layer of the TCP/IP protocol stack

4. A NMS is set of applications and does not belong to any layer. It can be thought of as residing above the Applications layer and being serviced by that layer

5. The Protocol Data Unit (PDU) contains the data element provided by the application and an element consisting of the headers created by appropriate protocols in the stack. The header element encapsulates the data element.

6. An SNMP packet would contain the Application layer, Transport Layer and Network layer and Network Interface layer headers.

7. A Web Browser uses the Hypertext Transfer Protocol (HTTP) of the Application Layer

8. That switch may be configured not to accept packets from a specified hardware address because it is inappropriate for that address to be communicating with the device.

9. In a switched LAN one can configure Virtual Private Networks (VPNs). These are independent virtual circuits that can transmit and receive data simultaneously without the collisions that would occur in a 10BASE2 LAN under such circumstances.

10. No they are not always layer-2 devices these days. The architecture of some switches enables hardware, network and transport layer headers to be examined before switching the PDU to the destination device.

11. Hubs enable the devices on the LAN to be connected directly to a central location which provides easy access for network configuration.

12. The IEEE 802.3 implements the Carrier Sense Multiple Access with Collision Detection (CMSA/CD) specification. This specification takes into account signal loss and signal transit time between devices. To meet the criteria determined by values of these parameters, two devices can be no further than 200 meters apart. Thus no device can be connected to the hub with a 10BASET cable that is longer than 100 meters.

13. The bridge table maps the source address of a packet received by the bridge to the port from which the packet was received. This enables the bridge to drop packets that are addressed to

a device on the same segment. The result is the only packets whose destination is a device on the other segment are transmitted, greatly reducing unnecessary traffic.

14. Switch tables map destination addresses to the port to which the destination device is attached.

15. Routing tables map destination network addresses to port numbers

16. The Ethernet II frame contains a Type field that follows the Source Address field. This field specifies the first protocol header in the Data field. For TCP/IP, this is usually the network layer protocol IP. The IEEE 802.3 frame has two fields that follow the Source Address field before the Data field. The first is the Length field and the second is the LLC field. The LLC field contains the Logical Link Control header that enables reliable communication on a single network. The length field is the number of bytes in the LLC and Data fields.

17. The NDIS makes it possible for multiple media specifications (e.g. Ethernet II) to be compatible with the TCP/IP protocol stack. If the media driver is written to the NDIS standard, it will interface correctly with the Network Interface layer.

Chapter 1 Exercise Answers

1. The purpose of this exercise is to reduce the helplessness that some students feel when they walk into a computer lab or computer classroom and all they see is some computers connected together. They have no idea how these computers communicate, if this is an isolated network, if it is connected to other computer labs or if it is somehow connected to the Internet. For those who are interested in such, it can be a frustrating feeling that should be addressed first. It is like being dropped off in the middle of a jungle and being asked to find your way out without a compass. The exercise is not intended to provide details but only to give the student some perspective on network connectivity.

Chapter 2 Exercise Solutions

1. Examples [(a)] are:
    - Setting switches on modem cards to select IRQ number and COM port
    - Placing jumpers on a network card to select IRQ number and I/O address
    - Placing jumpers on a network card to select the media that will be attached
    - Setting switches on a network card to select IRQ number, I/O address and COM port
    - Using a cable tester to located broken cables
    - Creating and maintaining and inventory of cables types and cable runs
    - Installing software from CD-ROM or diskette

    (a) Fortunately, recent network cards do not require jumper placement or switch setting

2. Examples are:
    - Installation of a network card driver
    - Software configuration of a network card's IRQ number, I/O address and COM port
    - Selection and configuration of a protocol stack
        - Configuring network address selection (Permanent or by DHCP)
        - Configuring the subnet mask
        - Specifying the network address of the DNS server
        - Specifying the network address of the WINS server
        - Specifying the network address of the default Gateway
    - Selection and configuration of network services such as SNMP agent
    - Installation and configuration of dial-up software
    - Configuration of routers:
        - network address and subnet mask for each port
        - transport protocols accepted
        - routing protocols such as RIP or OSPF
        - routing table for static routing
        - configuration password
        - configuration of SNMP agent
    - Configuration of switches:
        - network address and subnet mask
        - default gateway address
        - virtual private network (VPN) partitions
        - DNS server address
        - SNMP Read, Write and Trap community strings
        - Port configuration such as "enabled" or "disabled."
        - Mapping of ports to Ethernet addresses; static, dynamic or restricted

3. The items of this list will depend on what software is installed on the device. Examples are:

    a. PCs
        - Memory allocated
        - Kernel usage
        - Network usage
        - Resources accessed by other users on the network
        - File backup
        - Received/transmitted packet monitoring
        - Discovery of network resources
        - NMS polling of network devices
        - Graphical presentation of network activity based on polling

    b. Switches and Routers
        - Packet filtering based on:
            - Ethernet address
            - Protocol
            - Network address
            - Community String
            - Authentication
            - User ID
            - Password

    c. Probes
        - Packet capture
        - Packet statistics by:
            - Source and/or Destination Ethernet address(es)
            - Source and/or Destination network address(es)
            - Protocol
            - Application

4. Examples are:
    - Configuration of :
        - Desktop Management Initiative (DMI) supported objects on PCs using RPC or SNMP set commands
        - Router, Switch and Hub objects using an embedded Telnet server and a Telnet client and password.
        - mib-2 objects on PCs, routers, switches and probes using SNMP set commands
        - RMON packet filters on probes

    - Monitoring of:
        - DMI objects on PCs
        - mib-2 and RMON objects on routers, switches and hubs
        - RMON objects on probes

- Control of:
  - Probe Monitoring start
  - Probe Monitoring stop

5. Examples are:
   - Alarm-based events detected by devices such as probes. For example, an alarm could be set to send a trap if the number of packets received by a router during a given interval exceeds a threshold.
   - Traps sent by remote devices to management stations
   - Denial-of-Access GetResponse message sent by a device to a management station if a GetRequest packet does not contain the correct password (SNMPv3)
   - Information in GetResponse packet Error Status fields about VarBind values that are not available (SNMPv2 and SNMPv3)

Chapter 2 Review Question Answers

1. The Simple Gateway Management Protocol (SGMP) was the precursor to the Simple Network Management Protocol (SNMP). It was designed to manage only objects of relevance to Gateways (Routers); for example the number of Gateway ports. This capability was considered sufficient at the time. Today, SNMP can manage objects relevant to any device that has an SNMP agent installed.

2. A MIB is a virtual Management Information Base for a device. Each object in a MIB has an Object Identifier that defines its location in the iso tree of objects. An object contains a configured value for a device such as an IP address. These values are accessed or changed by a Network Management System (NMS) in order to manage the device. The use of the adjective virtual means that the values of objects are not centralized but maintained by relevant software such as the network driver for the device.

3. The RMON 1 standard added network-based MIB objects. These objects contained values that specified network performance rather than device performance. An example is the number of packets on the network from a specific Ethernet address. A special device called a network monitor or probe was used to capture packets on a network segment and determine these values for the segment.

4. The agent process is a virtual Database Manager. It accesses requested values of device objects directly or uses the support of a specialized subagent to do so. These values are the delivered to the protocol SNMP for return to the NMS.

5. The degree of network management is a tradeoff between management information desired and the network traffic required to obtain that information. Too much network management will reduce network performance.

6. The OSI protocol stack uses the CMIP for network management. CMIP stands for Common Management Information Protocol. It is more comprehensive than SNMP.

7. CMIP is the management protocol of the OSI Application layer

8. Because device management reduces cycle time available to the device for performing its primary functions.

9. SNMP is a de facto Internet standard because its pervasiveness exists by agreement of the users that evolved by the use of RFCs rather than committee.