	NETWORK INFRASTRUCTURE MANAGEMENT (6135) - Rev 2015 ANSWER KEY		
Q no	**Scoring Indicators**	**Split score**	**Total score**
I	**PART A**		
1	Management of hardware and software resources and operations of an enterprise network to enable network connectivity and communication.	2 marks	2
2	IP version 4 (IPv4) and IP version 6 (IPv6).	2 marks	2
3	**DHCP (Dynamic Host Configuration Protocol)** is a network management protocol used to dynamically assign an Internet Protocol (IP) address to any device, or node, on a network so they can communicate using IP.	2 marks	2
4	A router is a device that forwards data packets along networks.	2 marks	2
5	Hop count, Bandwidth, Load, Delay, Reliability, Cost	Any two, 2 marks	2
II	**PART B**		
1	**Bluetooth** is a **wireless *technology*** standard for exchanging data over short distances. • A Bluetooth technology is a high speed low powered wireless technology, that is designed to connect phones or other portable equipment together. • Due to its low cost, manufacturers are willing to implement this technology in most devices. • It is designed for short range communications with a **range of about 10m**. Data can be exchanged at a **rate of 1 megabit per second -- up to 2 Mbps** • Consumes less power and are suited for very small battery powered devices and portable devices. • Problems associated when devices communicate via infrared or cables are removed. Infrared requires a line of sight (LOS), Bluetooth only needs to be in reasonable vicinity. • As cables are not required, it is less cumbersome carrying a personal Bluetooth device and space would be less cluttered.	Any 4 points x ½ marks	6

	• As Bluetooth devices automatically communicate with each other, it requires very little from the user.		
2	**Coaxial cable** looks essentially like community antenna television (CATV) cable. • It is a type of electrical cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. • It varies from thin and flexible 50 ohm cable to thick, rigid, low-loss 70 ohm cable. • Transmission signals are sent **using direct current (DC)** across cable length. • CC has a single solid copper core and a braided or foil shield. Core and shield are separated by a plastic insulator. • Thin CC is used with connectors known as ***British Naval Connectors***. • Thick CC is used with coax or vampire taps. Installing taps requires that cable have a small hole drilled into the casing and through shielding. Then, tap is inserted in hole and tightened down so tap pierces firmly into copper core.	Any 4 points x ½ marks	6
3	concept of domain and workgroup **domain** • In a Windows network, a domain is a **group of server computers that share a central directory** database. • The **central database contains user accounts and security information** for resources in that domain. • Each domain must have **at least one server computer designated as the domain controller**, which is ultimately in charge of the domain. **workgroup** • Windows Workgroups, by contrast, are other model for grouping computers running Windows in a networking environment. • Workgroup computers are 'standalone' - i.e. there is no formal membership or authentication process formed by workgroup. • A workgroup does not have servers and clients, and as such, it represents Peer-to-Peer (or Client-to-Client) networking paradigm, rather than centralized architecture constituted by Server-Client. • Workgroups are more suitable for small or home-	3marks x 2	6

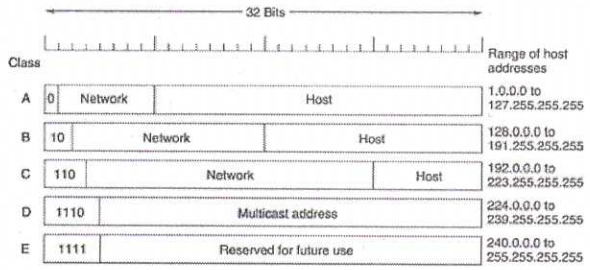
	office networks		
4	**Windows firewall** • Windows Firewall can provide computer or device with protection against attacks from local network or the internet. • Because Windows Firewall filters the traffic that goes on computer, it can also stop types of malicious software that use network traffic to spread themselves, like Trojan horse attacks and worms. • Another useful capability is that it can filter both outgoing and incoming connections to the Windows computer and block those which are unwanted. • The firewall uses a predefined set of rules for both types of network traffic, but its rules can be edited and changed both by the user and the software that the user installs **IP Security** • Internet protocol security (IPsec) is a set of protocols that provides security for Internet Protocol • It can use cryptography to provide security. • IPsec can be used for the setting up of virtual private networks (VPNs) in a secure manner. • IPsec involves two security services: ◦ Authentication Header (AH): authenticates the sender and it discovers any changes in data during transmission. ◦ Encapsulating Security Payload (ESP): This not only performs authentication for the sender but also encrypts the data being sent.	Windows firewall- any 3 points, 3 marks Ip sec- 3points, 3 marks	6
5	upgrading router IOS. • TFTP is easiest way to upgrade our router's IOS. • It is recommended that we have TFTP server on same local segment, if possible. • To perform an IOS upgrade, we need to configure router to load its IOS off TFTP server instead of using flash stored image. • IOS can be upgraded while router is in operation.	6marks	6

	There is an element of risk to this approach. If IOS image is corrupt, or if there are incompatibilities between our configuration and new IOS, we could have some problems. • To play it safe on both RFR and RFF router models, use TFTP to boot IOS image we plan to upgrade on our router. Then, upgrade it.		
6	IOS Message logging • *Logging* helps keeping up with what is going on with our router • In most cases, log information is simply status data, such as changes in router's interface status, modifications to running configuration, and debugging output. • When things are operating smoothly, this data is nice to have. When a problem comes up, however, this data can be quite valuable. • IOS uses UNIX's syslog logging system to generate IOS logging messages. • IOS provides four methods for viewing logging information: • Console—router's console port • Monitor—router's system monitor, a VTY "console" message display • Trap—Syslog output to a remote syslog server running on UNIX or NT • Buffer—A place to store a list of logging events in router's DRAM By default, all console and monitor methods are enabled, buffer is disabled, and trap (while set up) needs to be configured to know where to send its messages.	Any 4 points x ½ marks	6
7	Static routing TCP/IP Static Routing An administrator can build a master route table for network and distribute it to end stations so routes are added to local table when system boots up. If a change is needed, file is copied over network to end-stations, is rebooted, and new route is added.. merits of static routing: • Ease of use	Expln 3 Merits 3	6

	• Reliability • Control • Security • Efficiency		
	PART C		
III a	Explain any four networking devices 1. **Repeater** – A repeater operates at physical layer. It is a 2 port device • Its job is **to regenerate signal over the same network before signal becomes too weak or corrupted** so as to extend length to which signal can be transmitted over same network. 2. **Hub** – A hub is basically a multiport repeater. • A hub **connects multiple wires coming from different branches**, for example, the connector in star topology which connects different stations. Hubs **cannot filter data**, **so data packets are sent to all connected devices.** Collision domain of all hosts connected through Hub remains one. 3. **Bridge** – A bridge operates at data link layer. • A bridge is a repeater with add on functionality of **filtering content** by reading MAC addresses of source and destination. It is also **used for interconnecting two LANs** working on the same protocol. 4. **Switch** – A switch is a multi port bridge with a buffer and a design that can boost its efficiency (large number of ports implies less traffic) and performance. - Switch is a data link layer device. **Switch can perform error checking before forwarding data** 5. **Routers** – A router is a device like a switch that routes data packets based on their IP addresses. • Router is mainly a Network Layer device. Routers normally **connect LANs and WANs together** and have a dynamically updating routing table 6. **Gateway** – A gateway is a **passage to connect two networks together that may work upon different networking models.**	Any 4 x 2marks	8

b	**wi-fi networks.** • Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. • WiFi or Wireless Fidelity has a range of about 100m and allows **for faster data transfer rate between 10 - 54Mbps.** • There are **three different wireless standards under WiFi, 802.11a, 802.11b and 802.11g**. • The most widely used standard **is 802.11b and 802.11g** is expected to grow rapidly. • **The main difference between the two is the speed.** 802.11b has data transfer rate of upto 11Mbps and 802.11g has a rate of upto 54Mbps. • The cornerstone of any wireless network is an **access point (AP).** The primary job of an access point is to broadcast a wireless signal that computers can detect and "tune" into. • In order to connect to an access point and join a wireless network, computers and devices must be **equipped with wireless network adapters.**	Any 5 points, 7 marks	7
IV a	Straight-through cables are primarily used for connecting unlike devices **Straight-Through Wired Cables** Straight-Through refers to cables that have the pin assignments on each end of the cable. In other words Pin 1 connector A goes to Pin 1 on connector B, Pin 2 to Pin 2 ect. Straight-Through wired cables are most commonly used to connect a host to client. When we talk about cat5e patch cables, the Straight-Through wired cat5e patch cable is used to connect computers, printers and other network client devices to the router switch or hub (the host device in this instance). Straight Through Wiring Guide 568-B Connector A: Pin 1, Pin 2, Pin 3, Pin 4, Pin 5, Pin 6, Pin 7, Pin 8 Connector B: Pin 1, Pin 2, Pin 3, Pin 4, Pin 5, Pin 6, Pin 7, Pin 8	4marks each	8

	Crossover Wired Cables Crossover wired cables (commonly called crossover cables) are very much like Straight-Through cables with the exception that TX and RX lines are crossed (they are at oposite positions on either end of the cable. Using the 568-B standard as an example below you will see that Pin 1 on connector A goes to Pin 3 on connector B. Pin 2 on connector A goes to Pin 6 on connector B ect. Crossover cables are most commonly used to connect two hosts directly. Examples would be connecting a computer directly to another computer, connecting a switch directly to another switch, or connecting a router to a router. *Note: While in the past when connecting two host devices directly a crossover cable was required. Now days most devices have auto sensing technology that detects the cable and device and crosses pairs when needed.* Crossover Wiring Guide 568-B Connector A: Pin 1, Pin 2, Pin 3, Pin 4, Pin 5, Pin 6, Pin 7, Pin 8 Connector B: Pin 3, Pin 6, Pin 1, Pin 7, Pin 8, Pin 2, Pin 4, Pin 5 Connecting <u>like devices</u>		
b	Fibre optic cables **Optical fiber** cable is the preferred choice for high bandwidth, high speed, and long distance signal transmission. • Transmission signals are sent using **light emitting diodes (LEDs) or laser diodes** (LDs), and they are received using a pin field effect transistor (pinFET). • Signals are sent across an insulated glass core using modulated (mixing a data signal and an electromagnetic waveform) lightwaves. • These lightwaves travel across cable using *pulse amplitude* (lightwaves of varying intensity) or *pulse frequency* (lightwaves sent at a controlled frequency) to represent data signals. • <u>The biggest advantage associated with using OFC is its immunity to external noise and its extremely low attenuation.</u>	7 marks.	6
V a	various classes of IP address **Class A.** Few networks, each with many hosts. All class A network addresses begin with a binary 0. **Class B.** Medium number of networks, each with a medium number of hosts. class B addresses begin with a binary 10. **Class C.** Many networks, each with a few hosts. All class C addresses begin with a binary 110.	Explanation with necessary points 8marks	8

	Class D. Supports multicast, in which a datagram is directed to multiple hosts. All class D addresses begin with a binary 1110. **Figure 5-55. IP address formats.**  		
b	Remote desktop • With Remote Desktop Connection, we can connect to a computer running Windows from another computer running Windows that's connected to same network or to Internet. • For example, we can use all of our work computer's programs, files, and network resources from our home computer, and it's just like we're sitting in front of our computer at work. • To connect to a remote computer, that computer must be turned on, it must have a network connection, Remote Desktop must be enabled, we must have network access to remote computer (this could be through Internet), and we must have permission to connect. • For permission to connect, we must be on list of users. If the user account doesn't require a password to sign in, we'll need to add a password before we're allowed to start a connection with a remote computer.	7marks	7
VI a	steps for installation of active directory 1. Log in as an administrator to the Windows 2000 or 2003 server host. 2. From the Start menu, go to Administrative Tools > Manage Your Server. ... 3. In the Server Manager window, select the **Roles** directory. 4. In the **Roles Summary** section, click **Add Roles**. 5. On the Before You Begin page of the Add Roles Wizard, click **Next**. 6. On the Select Server Roles page, select the **Active**	8marks	8

	Directory Domain Services check box, and then click **Next**. 7. On the Confirmation page, click **Next**. 8. On the Installation Progress page, click **Install**. 9. On the Results page, after the role is successfully added, click **Close.**		
b	Domain Controller • **Defn:** A server running Active Directory Domain Services (AD DS) is called a domain controller. • Responsible of authenticating all users within the domain and applying group policies on the machines. • *Domain Controller* is essentially a Microsoft Windows Server that stores a copy of domain information and provides access and mechanisms to protect and use that data. • **It authenticates and authorizes all users** and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. • For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines **whether the user is a system administrator or normal user.** • Also, it allows management and storage of information, provides authentication and authorization mechanisms, and establishes a framework to deploy other related services:	4points 7marks	7
VII a	Memory on Routers. 1. Read-only memory (ROM) 2. Flash memory 3. Non-volatile random access memory (NVRAM) 4. Dynamic random access memory (DRAM) **ROM** is used on 1600, 2500, 2600, and 3x00 series routers to handle router's bootstrap process, and it has just enough headroom to load OS. In the case of 2500, ROM set also contains a limited version of router's operating system, called *Internetwork Operating System (IOS).* ***Flash memory*** is rewritable nonvolatile memory. Flash is either mounted on router's motherboard or installed in a router's PCMCIA slot(s). Flash memory is used on all routers to store IOS. On 4x00 and 7x00 routers, along with IOS flash, an additional flash chip known as *bootflash* contains bootstrap OS. By using bootflash,	2marks x 4	8

	bootstrap application can be upgraded without a hardware change. ***NVRAM*** is similar to flash in that it does not lose its contents when power is lost. It is used to store router's configuration information. ***DRAM*** is used for packet processing and IOS operation. On all router platforms (except 7x00 series), DRAM is partitioned into primary and shared memory.		
b	**Disaster recovery in routers** In most of the cases, if you powered on the router and the router is entering into rommon mode. The problem is 1) IOS is missing 2) IOS is corrupted Disaster recovery on routers using rommon and conf-reg settings is straight- forward because all routers use same basic boot sequence: 1. The router is powered up. 2. It checks its conf-reg settings. 3. It checks NVRAM for boot loader information. 4. It loads IOS. 5. It loads NVRAM config. Because conf-reg is the first boot element checked, it is possible to configure router to do a number of different things just by changing its conf-reg settings. conf-reg information is listed as final system variable in output of show version or show hardware privileged EXEC command.	7marks	7
VIII a	**Router IOS** • IOS is the standard operating system for all routers. • It is a deeply feature-rich, yet efficient, routing-centric OS. • Aside from creating router industry, what has made so popular among network managers and administrators is its solid implementation of standard and proprietary routing protocols and its reliability and security enhancements. • IOS is the standard by which other routing implementations are measured in terms of protocol implementation stability, IETF (RFCs), IEEE, and ANSI hardware and software standards implementations.	4points x 2 marks	8

	• IOS interface was based on TOPS-20 command shell interface, which was a user centric, help-oriented shell. IOS command interface is widely emulated on a variety of hardware vendors' configuration interfaces. • IOS is platform hardware-centric, and each hardware platform has its own specific version. IOS essentially comes in three flavors: 1. IP only—Comes in several variations (IP, IP Plus, IP 40, IP 40 Plus, to name a few). These variations provide additional services such as data encryption, firewalls, and Network Address Translation (NAT). 2. IP/IPX/AT/DEC—Provides multiprotocol support. 3. ENTERPRISE—Provides support for all the IOS enhanced features.		
b	**Talking to Router -Through the Console** • Access to router's console is required for access to operating system for initial setup and configuration. • After router is online, **Telnet** can be used to access a virtual router terminal port. • After router is online, ***Simple Network Management Protocol*** *(SNMP)* can be an alternative to router's Command-Line Interface (CLI) to make changes and gather information about router. • Like Telnet, SNMP is dependent on TCP/IP for transport. It requires TCP/IP to be enabled, in addition to its own protocol configuration. Once SNMP is configured and running on router, an SNMP manager is used to send and receive commands. • Router also has a Windows-based tool called **configMaker** which is often shipped with its low end routers. This tool provides a GUI configuration interface to perform initial router configurations on 1600, 2500, 2600, 3600, and 4000 series routers (it also works with Catalyst switches).	7marks	7
IX a	TCP /IP Interior Gateway Protocols • Protocols that perform intranetwork routing are known as *interior gateway protocols (IGPs).* Examples are RIP, IGRP, EIGRP, and OSPF • Routing Information Protocol (RIP) and Open	Defn and eg:2 marks Expln any 2, 3 marks each	8

	Shortest Path First (OSPF) are popular IGPs. Routing Information Protocol, v1 and v2: • RIP has largest support base of any of dynamic routing protocols. Almost every Layer 3 network device on market supports at least one version or both versions of RIP. RIP is also available on most of popular operating systems (UNIX and Windows NT), giving end-stations capability to support multiple network gateways. • RIP's universal support and easy setup make it very common in small, static point-to-point and redundant path LAN networks. • IGRP and EIGRP: *Interior Gateway Routing Protocol (IGRP)* and *Enhanced Interior Gateway Routing Protocol (EIGRP)* are Cisco Systems' proprietary protocols, which means they are only supported on Cisco routers. This is a severely limiting factor because interoperability with other non-Cisco routers would require running an additional routing protocol and redistributing it into IGRP or EIGRP process. OSPF: *Open Shortest Path First (OSPF)* is a link state protocol. • Routers running link state protocols exchange link state information about network in which they are directly connected. Each then uses this information to construct a map of entire network topology from its perspective.		
b	network management fundamentals. 1 Before computer networks emerged, there were mainframe time-sharing systems. These systems were standalone supercomputers that shared memory, processing, and storage resources between a certain number of users. Users would access mainframe through dumb terminals that were connected to server via serial controllers or modems. 2 But, large mainframe time-sharing systems required more attention and management	Expln 4 points, 7marks	7

	than most UNIX systems today. systems administrators would monitor mainframe's processor and memory utilization, I/O controllers, line terminals and modems, multiplexers, channel banks, dedicated circuits, disk, tape, and card reading systems. To managing these complex systems , separate management and configuration systems were required to manage all different system resources. These systems were comprised of custom tools to extract data from all of the subsystems, and this complexity was expensive in terms of development and personnel costs. 3 When LAN and WAN networks began to emerge in 1980s with introduction of the personal computer, similar configuration, management, and monitoring began to appear for computer networks. 4 In 1980s, there were no Internet service providers (ISPs). Instead, "Internet" was a collection of regional networks managed by government and research entities.		
X a	distinctions between EGP and IGP protocols are three Cs: 1 Context—IGPs and EGPs both operate in different routing contexts. IGP protocols are interested in building and exchanging routing information. EGPs are interested in network reachability information. 2 Connectivity—IGP networks are connected physically to one another. Routing tables are built on direct connectivity and local adjacency, using hop-to-hop routing paradigm common to IP. EGPs exchange network reachability information. Information is exchanged by designated peers. Routes are based on AS paths that need to be traversed in order to reach destination network. 3 Choice—IGP protocols support route metrics that enable router to choose best	4points, 2 marks each	8

	route path. EGPs do not support routing metrics. EGPs use policy routing to manage traffic behavior. 4 IGPs are designed to provide a dynamic means of constructing routing tables that enable datagram forwarding to occur in most efficient and reliable manner. EGPs provide capability to route IP datagrams between distinct open internetworks in a dynamic and manageable fashion.		
b	purpose of network analysis is twofold. • Through use of network analysis techniques, we have an understanding of how our network functions and we can establish a set of network performance baselines. Network baseline data is used for a variety of network management related tasks • The second purpose of network analysis is to resolve network fault conditions and to improve overall network performance through performance tuning. ▪ Performance tuning is making configuration and design adjustments to network to improve its performance based on the results of management and analysis data.	7marks	7