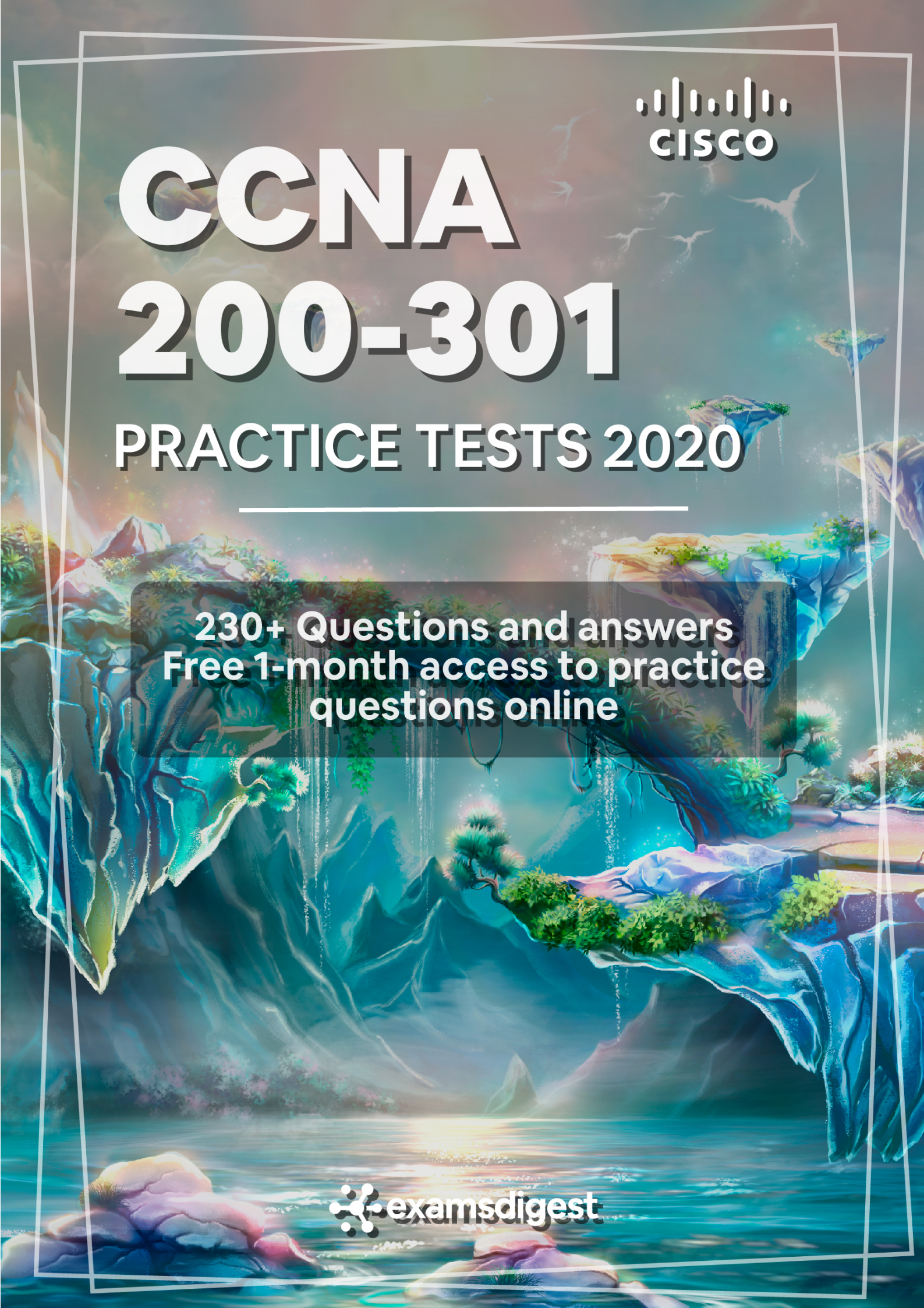

CISCO
CCNA
200-301
PRACTICE TESTS 2020
230+ Questions and answers
Free 1-month access to practice questions online
examsdigest

230+ CISCO CCNA 200-301

PRACTICE QUESTIONS

examsdigest

by Examsdigest®

examsdigest

Cisco CCNA 200-301 Practice Tests 2020®

Published by: Examsdigest LLC., Holzmarktstraße 73, Berlin, Germany, www.examsdigest.com Copyright © 2020 by Examsdigest LLC.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, Examsdigest, LLC., Holzmarktstraße 73, Berlin, Germany or online at https://www.examsdigest.com/contact.

Trademarks: Examsdigest, examsdigest.com and related trade dress are trademarks or registered trademarks of Examsdigest LLC. and may not be used without written permission. Amazon is a registered trademark of Amazon, Inc. All other trademarks are the property of their respective owners. Examsdigest, LLC. is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE.

Examsdigest publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may find this material at https://examsdigest.com

CONTENTS AT A GLANCE

Contents at a glance.....5

Introduction 8

Chapter 1 The intro to networking Questions 1-20 14

Chapter 2 Ethernet LANs 39

Questions 21-40 ----------39

Answers 21-40 ----------49

Chapter 3 IPv4 addressing.....62

Questions 41-63 ----------62

Answers 41-63----------70

Chapter 4 Advanced IPv4 Addressing.....90

Questions 64-90 ----------90

Answers 64-90----------100

Chapter 5 IPv4 Routing 131

Questions 91-105----------131

Chapter 5 OSPF Routing PROTOCOL.....157

Questions 106-120 ----------157

Answers 106-120 ----------165

Chapter 6 IP version 6 179

Questions 121-136 ----------179

Answers 121-136----------186

Chapter 7 Security Fundamentals..... 200

Questions 137-153 ----------200

Answers 137-153----------209

Chapter 8 IP ACCESS CONTROL LIST 227

Questions 154-178 ----------227

Answers 154-178----------239

Chapter 9 Wireless Networks 267

Questions 179-193 ----------267

Answers 179-193----------272

Chapter 10 IP SERVICES..... 287

Questions 194-203 ----------287

Answers 194-203----------293

Chapter 11 Network Design Architecture 310

Questions 204-217----------310

Answers 204-217 ----------315

Chapter 12 Network Automation 331

Questions 218-230----------331

Answers 218-230----------336

THE END 349

INTRODUCTION

The Cisco CCNA 200-301 examination is intended for individuals who perform a network engineer role and have one or more years of hands-on experience in the IT field.

About This Book

Cisco CCNA 200-301 Practice Tests 2020 by Examsdigest is designed to be a practical practice exam guide that will help you prepare for the CCNA 200-301 exams. As the book title says, it includes 200 questions, organized by exam so that you can prepare for the final exam.

This book has been designed to help you prepare for the style of questions you will receive on the CCNA 200-301 exams. It also helps you understand the topics you can expect to be tested on for each exam.

In order to properly prepare for the Cisco CCNA 200-301, I recommend that you:

✓ **Review a reference book:** Cisco CCNA 200-301 Practice Tests 2020 by Examsdigest is designed to give you sample

questions to help you prepare for the style of questions you will receive on the real certification exam. However, it is not a reference book that teaches the concepts in detail. That said, I recommend that you review a reference book before attacking these questions so that the theory is fresh in your mind.

✓ **Get some practical, hands-on experience:** After you review the theory, I highly recommend getting your hands on some routers and switches, or using a simulator; practice configuring the router with each topic you are studying. The CCNA certification is a practical, hands-on certification: The more hands-on experience you have, the easier the exams will be.

✓ **Do practice test questions:** After you review a reference book and perform some hands-on work, attack the questions in this book to get you "exam ready"! Also claim your free 1-month access on our platform to dive into to more questions, flashcards and much much more.

Beyond The Book

This book gives you plenty of CCNA 200-301 questions to work on, but maybe you want to track your progress as you tackle the questions, or maybe you're having trouble with certain types of questions and wish they were all presented in one

place where you could methodically make your way through them. You're in luck. Your book purchase comes with a free one-month subscription to all practice questions online and more. You get on-the-go access any way you want it — from your computer, smartphone, or tablet. Track your progress and view personalized reports that show where you need to study the most. Study what, where, when, and how you want!

What you'll find online

The online practice that comes free with this book offers you the same questions and answers that are available here and more.

The beauty of the online questions is that you can customize your online practice to focus on the topic areas that give you the most trouble.

So if you need help with IP Addressing, then select questions related to this topic online and start practicing.

Whether you practice a few hundred problems in one sitting or a couple dozen, and whether you focus on a few types of problems or practice every type, the online program keeps track of the questions you get right and wrong so that you can monitor

your progress and spend time studying exactly what you need.

You can access these online tools by sending an email to the info@examsdigest.com to claim access on our platform. Once we confirm the purchase you can enjoy your free access.

Cisco CCNA 200-301 Exam Details

The online practice that comes free with this book offers you the same questions and answers that are available here and more.

✓ **Format -** Multiple choice, multiple answer & Drag and Drop
✓ **Type -** Associate
✓ **Delivery Method -** Testing center or online proctored exam
✓ **Time -** 120 minutes to complete the exam
✓ **Cost -** Varies
✓ **Language -** Available in English, Japanese

Exam Content

Content Outline

The Cisco Certified Network Associate v1.0 (CCNA 200-301) exam is a 120-minute exam associated with the CCNA certification. This exam tests a candidate's knowledge and skills re-

lated to network fundamentals, network access, IP connectivity, IP services, security fundamentals, and automation and programmability. The course, Implementing and Administering Cisco Solutions (CCNA), helps candidates prepare for this exam.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

1.0: Network Fundamentals

2.0: Network Access

3.0: IP Connectivity

4.0: IP Services

5.0: Security Fundamentals

6.0: Automation and Programmability

CHAPTER 1
THE INTRO TO NETWORKING

QUESTIONS 1-20

Question 1. Which of the following terms describe Ethernet addresses that can send one frame and is delivered to multiple devices on the LAN? (Choose two answers.)

(A) Broadcast address

(B) Multicast address

(C) IP address

(D) MAC address

(E) Unicast address

Question 2. Which of the following address check a router when making a decision about routing TCP/IP packets?

(A) Destination MAC address

(B) Source IP address

(C) Source MAC address

(D) Destination IP address

Question 3. _____ is a set of rules determining how network devices respond when two devices attempt to use a data

channel simultaneously and encounter a data collision.

(A) CSMA/CD

(B) CSMA/CA

(C) TCP/IP

(D) TCP/UDP

Question 4. Ethernet standard _____ BASE-T defines Gigabit Ethernet over UTP cabling.

(A) 100

(B) 10

(C) 1000

(D) 1

Question 5. Which of the following IEEE 802.3 Ethernet Header and Trailer Fields allows devices on the network to easily synchronize their receiver clocks?

(A) Frame Check Sequence

(B) Data and Pad

(C) Start Frame Delimiter

(D) Preamble

Question 6. The host sends packets to its default gateway if the _____ IP address is in a different subnet than the host.

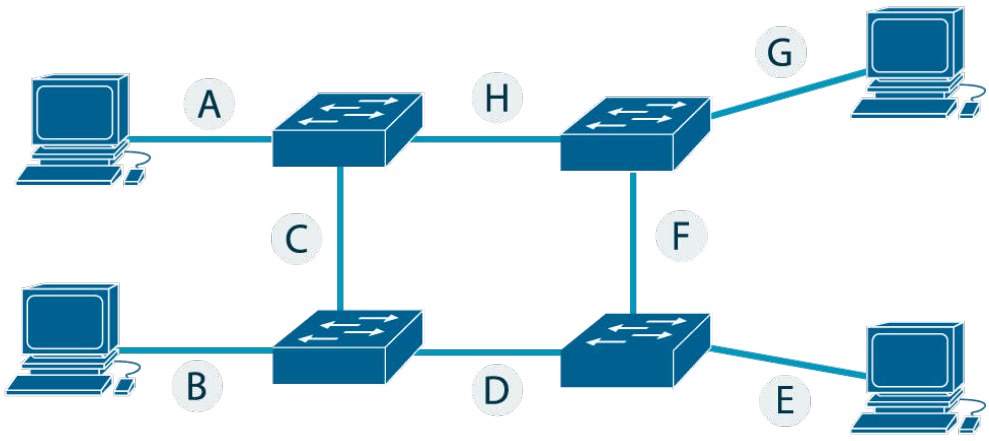
(A) Source

(B) Destination

(C) Unicast

(D) Broadcast

Question 7. The diagram below shows a campus LAN in a single building. Which of the following connections uses crossover Ethernet cables? (Choose all that apply)



(A) A

(B) C

(C) D

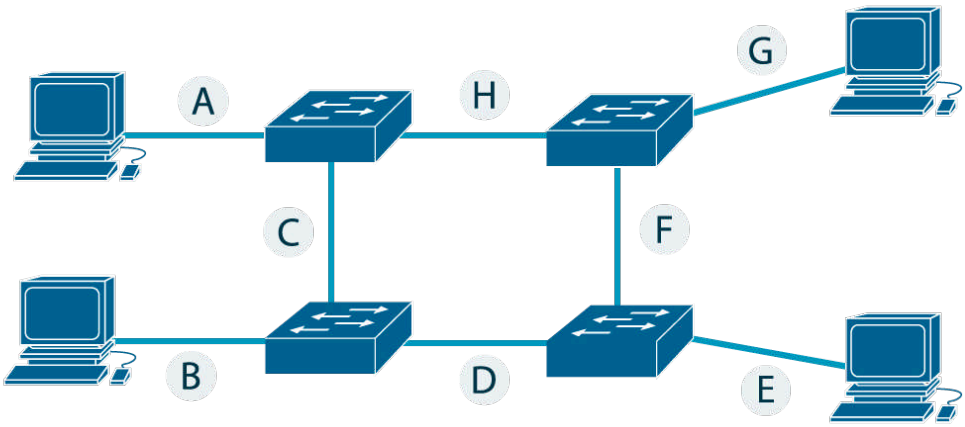
(D) E

(E) F

(F) G

Question 8. The diagram below shows a campus LAN in a single building. Which of the following connections uses straight-

through cables? (Choose all that apply)



(A) A

(B) C

(C) D

(D) E

(E) F

(F) G

Question 9. Which of the following protocols resides in the Application TCP/IP Architecture layer?

(A) SMTP

(B) TCP

(C) Ethernet

(D) IP

Question 10. Which of the following protocols resides in the Transport TCP/IP Architecture layer?

(A) SMTP

(B) TCP

(C) Ethernet

(D) IP

Question 11. Which of the following protocols resides in the Internet TCP/IP Architecture layer?

(A) SMTP

(B) TCP

(C) Ethernet

(D) IP

Question 12. Which of the following protocols resides in the Data Link & Physical TCP/IP Architecture layer?

(A) SMTP

(B) TCP

(C) Ethernet

(D) IP

Question 13. Which of the following protocols is used from PC1 to learn information from some other device on the same network?

(A) ping

(B) ARP

(C) DHCP

(D) DNS

Question 14. If the devices below were connected with UTP Ethernet cables, which pairs of devices would require a straight-through cable? (Choose two answers.)

(A) Router and PC

(B) Switch and PC

(C) Hub and switch

(D) Router and hub

Question 15. Which of the following protocols are examples of TCP/IP data-link layer protocols? (Choose two answers.)

(A) TCP

(B) HTTP

(C) Ethernet

(D) PPP

(E) SMTP

(F) HTTPS

Question 16. Which of the following statements are functions of a routing protocol? (Choose two answers.)

(A) Learning routes and putting those routes into the routing table for routes advertised to the router by its neighboring routers

(B) Advertising known routes to neighboring routers

(C) Learning routes for subnets directly connected to the router

(D) Forwarding IP packets based on a packet's destination IP address

Question 17. When you open a web browser and type in the hostname www.examsdigest.com, your computer does not send an IP packet with a destination IP address www.examsdigest.com; it sends an IP packet to an IP address used by the web server for Examsdigest. TCP/IP needs a way to let a computer find the IP address used by the listed hostname. That method uses the Domain Name System (DNS).

(A) TRUE

(B) FALSE

Question 18. A _____ address is an address that enables transmission to every node in a local network.

(A) Broadcast

(B) Multicast

(C) Unicast

(D) MAC

Question 19. TCP and _____ are the two most commonly used TCP/IP transport layer protocols.

(A) UDP

(B) HTTP

(C) DNS

(D) SMTP

Question 20. Which of the following IEEE 802.3 Ethernet Header and Trailer Fields provides a method for the receiving NIC to determine whether the frame experienced transmission errors?

(A) Frame Check Sequence

(B) Data and Pad

(C) Start Frame Delimiter

(D) Preamble

Answers 1-20

Question 1. Which of the following terms describe Ethernet addresses that can send one frame and is delivered to multiple devices on the LAN? (Choose two answers.)

(A) Broadcast address

(B) Multicast address

(C) IP address

(D) MAC address

(E) Unicast address

Explanation 1. **A and B are the correct answers.** **Broadcast address** and **multicast address** are the only type of addresses that can send frames to multiple devices on the Local Area Network (LAN).

Question 2. Which of the following address check a router when making a decision about routing TCP/IP packets?

(A) Destination MAC address

(B) Source IP address

(C) Source MAC address

(D) Destination IP address

Explanation 2. **Destination MAC address is the correct answer.** **Broadcast address** and **multicast address** are the only type of addresses that can send frames to multiple devices on the Local Area Network (LAN).

Question 3. _____ is a set of rules determining how network devices respond when two devices attempt to use a data channel simultaneously and encounter a data collision.

(A) CSMA/CD

(B) CSMA/CA

(C) TCP/IP

(D) TCP/UDP

Explanation 3. **CSMA/CD address is the correct answer.** **CSMA/CD** is a set of rules determining how network devices respond when two devices attempt to use a data channel simultaneously and encounter a data collision. The rules define how long the device should wait if a collision occurs.

If no transmission is taking place at the time, the particular station can transmit but If two stations attempt to transmit simultaneously, this causes a data collision, which is detected by all participating stations. After a random time interval, the stations that collided attempt to transmit again.

Question 4. Ethernet standard _____ BASE-T defines Gigabit Ethernet over UTP cabling.

(A) 100

(B) 10

(C) 1000

(D) 1

Explanation 4. **1000 address is the correct answer.** Ethernet standard 1000BASE-T defines Gigabit Ethernet over UTP cabling. The number before the word BASE defines the speed, in megabits per second (Mbps). 1000 Mbps equals 1 gigabit per second (1 Gbps). The T in the suffix implies twisted-pair or UTP cabling, so 1000BASE-T is the UTP-based Gigabit Ethernet standard name.

Question 5. Which of the following IEEE 802.3 Ethernet Header and Trailer Fields allows devices on the network to easily synchronize their receiver clocks?

(A) Frame Check Sequence

(B) Data and Pad

(C) Start Frame Delimiter

(D) Preamble

Explanation 5. **Preamble is the correct answer.**

Preamble: Allow devices on the network to easily synchronize

their receiver clocks.

Frame Check Sequence (FCS): Provides a method for the receiving NIC to determine whether the frame experienced transmission errors.

Data and Pad: Holds data from a higher layer, typically an L3PDU (usually an IPv4 or IPv6 packet). The sender adds padding to meet the minimum length requirement for this field.

Start Frame Delimiter (SFD): Signifies that the next byte begins the Destination MAC Address field.

Question 6. The host sends packets to its default gateway if the _____ IP address is in a different subnet than the host.

(A) Source

(B) Destination

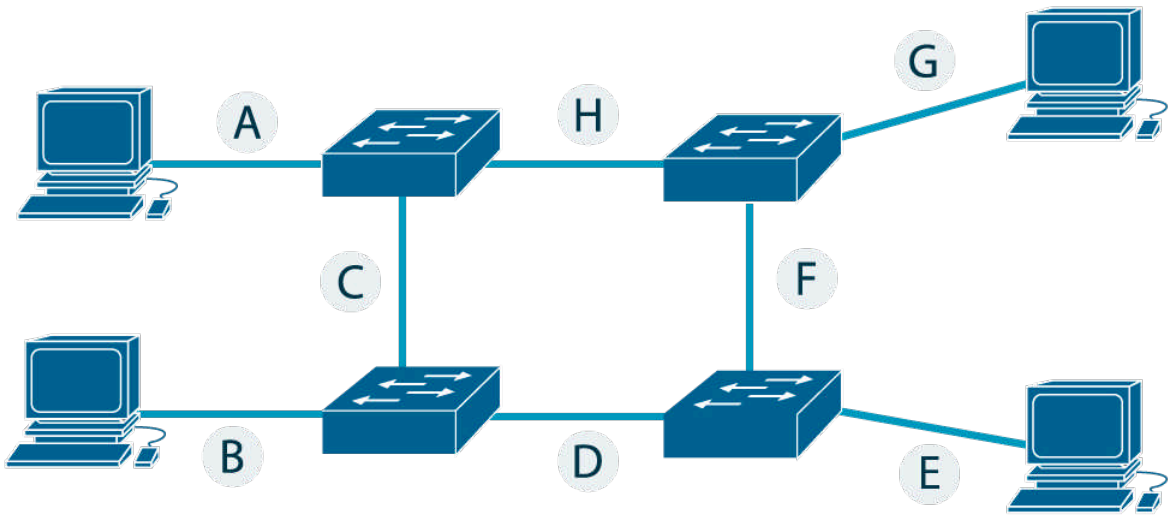
(C) Unicast

(D) Broadcast

Explanation 6. **Destination is the correct answer.** If the **destination** IP address is in a different subnet than the host, then the host sends packets to its default gateway.

If IPv4 hosts send an IP packet to another host on the same IP network or subnet that is on the same LAN, then the sender sends the IP packet directly to that host.

Question 7. The diagram below shows a campus LAN in a single building. Which of the following connections uses crossover Ethernet cables? (Choose all that apply)



(A) A

(B) C

(C) D

(D) E

(E) F

(F) G

Explanation 7. **B, C, E are the correct answers.** **Connections (C, D, F, H)** use Crossover Ethernet Cables.

A **crossover cable** is a type of twisted-pair copper wire cable for LANs (local area network) in which the wires on the cable are crossed over so that the receive signal pins on the RJ-45 connector on one end are connected to the transmit signal pins on the RJ-45 connector on the other end.

Wires 1 and 3 and wires 2 and 6 are crossed.
Crossover cables are used to connect two devices of the same type, e.g. two computers or two switches to each other.

Question 8. The diagram from the **Question 7** shows a campus LAN in a single building. Which of the following connections uses straight-through cables? (Choose all that apply)

(A) A
(B) C
(C) D
(D) E
(E) F
(F) G

Explanation 8. **A, D, E are the correct answers.** **Connections (A, B, E, G):** Straight-Through Cable.

Straight-through cable is a type of twisted-pair copper wire

cable for local area network (LAN) use for which the RJ-45 connectors at each end have the same pinout.
Straight-through cables are used to connect computers and other end-user devices e.g. printers to networking devices such as hubs and switches.

Question 9. Which of the following protocols resides in the Application TCP/IP Architecture layer?

(A) SMTP

(B) TCP

(C) Ethernet

(D) IP

Explanation 9. **SMTP is the correct answer.** The **TCP/IP application layer** protocol provides services to the application software running on a computer.

The application layer does not define the application itself, but it defines services that applications need. In short, the application layer provides an interface between software running on a computer and the network itself.

Question 10. Which of the following protocols resides in the Transport TCP/IP Architecture layer?

(A) SMTP

(B) TCP

(C) Ethernet

(D) IP

Explanation 10. **TCP is the correct answer.** The **Transport layer determines** how much data should be sent where and at what rate. This layer builds on the messages which are received from the application layer. It helps ensure that data units are delivered error-free and in sequence.

The transport layer helps you to control the reliability of a link through flow control, error control, and segmentation, or desegmentation.

Question 11. Which of the following protocols resides in the Internet TCP/IP Architecture layer?

(A) SMTP

(B) TCP

(C) Ethernet

(D) IP

Explanation 11. **IP is the correct answer.** The **TCP/IP Internet layer** includes a small number of protocols, but only one major protocol: the Internet Protocol (IP) and the Internet Control Message Protocol (ICMP). IP provides several features, most

importantly, addressing and routing.

Question 12. Which of the following protocols resides in the Data Link & Physical TCP/IP Architecture layer?

(A) SMTP

(B) TCP

(C) Ethernet

(D) IP

Explanation 12. **Ethernet is the correct answer.** The **data-link and physical layers** define the protocols and hardware required to deliver data across the physical network.

The two layers work together; in fact, some standards define both the data-link and physical layer functions. The physical layer defines the cabling and energy (for example, electrical signals) that flow over the cables.

Question 13. Which of the following protocols is used from PC1 to learn information from some other device on the same network?

(A) ping

(B) ARP

(C) DHCP

(D) DNS

Explanation 13. **ARP is the correct answer.** The **Address Resolution Protocol (ARP)** is a communication protocol used for discovering the link-layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.

This mapping is a critical function in the Internet protocol suite. The job of the ARP is essentially to translate 32-bit addresses to 48-bit addresses and vice-versa.

When a new computer joins a LAN, it is assigned a unique IP address to use for identification and communication. When an incoming packet destined for a host machine on a particular LAN arrives at a gateway, the gateway asks the ARP program to find a MAC address that matches the IP address.

Question 14. If the devices below were connected with UTP Ethernet cables, which pairs of devices would require a straight-through cable? (Choose two answers.)

(A) Router and PC

(B) Switch and PC

(C) Hub and switch

(D) Router and hub

Explanation 14. **B and D are the correct answers.** **Straight-through cable** is a type of twisted-pair copper wire cable for local area network (LAN) use for which the RJ-45 connectors at each end have the same pinout.

Straight-through cables are used to connect computers and other end-user devices e.g. printers to networking devices such as hubs and switches.

Routers, wireless access point Ethernet ports, and **PC NICs** all send using pins 1 and 2, whereas hubs and LAN switches transmit on pins 3 and 6. Straight-through cables connect devices that use opposite pin pairs for sending because the cable does not need to cross the pairs.

Question 15. Which of the following protocols are examples of TCP/IP data-link layer protocols? (Choose two answers.)

(A) TCP

(B) HTTP

(C) Ethernet

(D) PPP

(E) SMTP

(F) HTTPS

Explanation 15. **C and D are the correct answers.** The **Eth-**

ernet defines both physical and data-link protocols, **PPP** is a data-link protocol.

Question 16. Which of the following statements are functions of a routing protocol? (Choose two answers.)

(A) Learning routes and putting those routes into the routing table for routes advertised to the router by its neighboring routers

(B) Advertising known routes to neighboring routers

(C) Learning routes for subnets directly connected to the router

(D) Forwarding IP packets based on a packet's destination IP address

Explanation 16. A and B are the correct answers.

Routers do all the actions listed in all four answers; however, the **routing protocol** does the functions in the two listed answers.

Independent of the routing protocol, a router learns routes for IP subnets and IP networks directly connected to its interfaces. Routers also forward (route) IP packets, but that process is called IP routing, or IP forwarding, and is an independent process compared to the work of a routing protocol.

The functions of a routing protocol are:

1. Learning routes and putting those routes into the routing table for routes advertised to the router by its neighboring routers.
2. Advertising known routes to neighboring routers.

Question 17. When you open a web browser and type in the hostname www.examsdigest.com, your computer does not send an IP packet with a destination IP address www.examsdigest.com; it sends an IP packet to an IP address used by the web server for Examsdigest. TCP/IP needs a way to let a computer find the IP address used by the listed hostname. That method uses the Domain Name System (DNS).

(A) TRUE

(B) FALSE

Explanation 17. **TRUE is the correct answer.** The **Domain Name System (DNS)** is the phonebook of the Internet. Humans access information online through domain names, like examsdigest.com or youtube.com. Web browsers interact through Internet Protocol (IP) addresses. DNS translates domain names to IP addresses so browsers can load Internet resources.

Each device connected to the Internet has a unique IP address that other machines use to find the device. DNS servers eliminate the need for humans to memorize IP addresses such as

192.168.1.1 (in IPv4), or more complex newer alphanumeric IP addresses such as 2100:bb22:3272:1::2133:b1a4 (in IPv6).
DNS records are instructions that live in authoritative DNS servers and provide information about a domain including what IP address is associated with that domain and how to handle requests for that domain. These records consist of a series of text files written in what is known as DNS syntax. DNS syntax is just a string of characters used as commands which tell the DNS server what to do.

The most common types of DNS are:
A is used to map hostnames to an IPv4 address of the host.
AAAA is used to map hostnames to an IPv6 address of the host.
CNAME is used to point a domain or subdomain to another hostname.
SRV is used to identify computers that host specific services.
MX is used to help route emails.
TXT is used to provide the ability to associate text with a zone.
NS indicates which DNS server is authoritative for that domain.
PTR is used for the Reverse DNS (Domain Name System) lookup.

Question 18. A _____ address is an address that enables transmission to every node in a local network.

(A) Broadcast

(B) Multicast

(C) Unicast

(D) MAC

Explanation 18. **Broadcast is the correct answer.**

A **broadcast** address is a network address at which all devices connected to a multiple-access communications network are enabled to receive datagrams, which comprise UDP and TCP/IP packets, for instance. A message sent to a broadcast address may be received by all network-attached hosts.

Question 19. TCP and _____ are the two most commonly used TCP/IP transport layer protocols.

(A) UDP

(B) HTTP

(C) DNS

(D) SMTP

Explanation 19. **UDP is the correct answer.**

Transmission Control Protocol (TCP) and **User Datagram Protocol (UDP)** are two most commonly used TCP/IP transport layer protocols.

Each TCP/IP application typically chooses to use either TCP or UDP based on the application's requirements.

For example, **TCP provides error recovery**, but to do so, it consumes more bandwidth and uses more processing cycles. **UDP does not perform error recovery**, but it takes less bandwidth and uses fewer processing cycles.

TCP/IP Transport Layer Features are Multiplexing using ports, Error recovery (reliability), Flow control using windowing, Connection establishment, and termination, and Ordered data transfer and data segmentation.

Question 20. Which of the following IEEE 802.3 Ethernet Header and Trailer Fields provides a method for the receiving NIC to determine whether the frame experienced transmission errors?

(A) Frame Check Sequence

(B) Data and Pad

(C) Start Frame Delimiter

(D) Preamble

Explanation 20. Frame Check Sequence is the correct answer.

Preamble: Allow devices on the network to easily synchronize their receiver clocks.

Frame Check Sequence (FCS): Provides a method for the re-

ceiving NIC to determine whether the frame experienced transmission errors.

Data and Pad: Holds data from a higher layer, typically an L3PDU (usually an IPv4 or IPv6 packet). The sender adds padding to meet the minimum length requirement for this field.

Start Frame Delimiter (SFD): Signifies that the next byte begins the Destination MAC Address field.

CHAPTER 2
ETHERNET LANS

Questions 21-40

Question 21. Which of the following commands checks the status of the interfaces?

(A) show interface

(B) show status

(C) show interface status

(D) show status interface

Question 22. You are in console line configuration mode. Which of the following commands would place you in enable mode?

(A) end

(B) back

(C) enable

(D) change

Question 23. Which of the following commands copies the configuration from RAM into NVRAM

(A) copy running-config startup-config

(B) copy startup-config running-config

(C) copy ram nvram

(D) copy nvram ram

Question 24. The command that configures the switch as a DHCP client to discover its IPv4 address, mask, and default gateway is **ip address dhcp.**

(A) TRUE

(B) FALSE

Question 25. In which of the following modes of the CLI could you configure the duplex setting for interface Fast Ethernet 0/2?

(A) Global configuration mode

(B) Enable mode

(C) Interface configuration mode

(D) VLAN mode

Question 26. Which of the following commands administratively enables an interface

(A) shutdown

(B) no shutdown

(C) enable interface

(D) interface enable

Question 27. Switches use STP to prevent loops by causing

some interfaces to block, meaning that they do not send or receive frames.

(A) TRUE

(B) FALSE

Question 28. A Layer 2 switch configuration places all its physical ports into VLAN 2. The IP addressing plan shows that address 175.28.1.150 (with mask 255.255.255.0) is reserved for use by this new LAN switch and that 175.28.1.254 is already configured on the router connected to that same VLAN. The switch needs to support SSH connections into the switch from any subnet in the network. Which of the following commands are part of the required configuration in this case? (Choose two answers.)

(A) The switch cannot support SSH because all its ports connect to VLAN 2, and the IP address must be configured on interface VLAN 1.

(B) The ip address 175.28.1.150 255.255.255.0 command in interface vlan 2 configuration mode.

(C) The ip default-gateway 175.28.1.254 command in global configuration mode.

(D) The ip address 172.16.2.250 255.255.255.0 command in interface vlan 1 configuration mode.

(E) The ip default-gateway 175.28.1.150 command in global configuration mode.

Question 29. Which of the following commands lists the content of the startup-config (initial config) file.

(A) show startup-config

(B) show initial-config

(C) show content-config

(D) show file-config

Question 30. You want to configure the console password with password examsdigest. Which of the following commands will you type to meet the requirement?

(A) Examsdigest#(config)# line console 0
Examsdigest#(config-line)# password examsdigest
Examsdigest#(config-line)# login
Examsdigest#(config-line)# exit

(B) Examsdigest#(config)# enable secret examsdigest

(C) Examsdigest#(config)# enable console examsdigest

(D) Examsdigest#(config)# live vty 0 15
Examsdigest#(config-line)# password examsdigest
Examsdigest#(config-line)# login
Examsdigest#(config-line)# end

Question 31. You want to configure the telnet password for all vty lines with password examsdigest. Which of the following commands will you type to meet the requirement?

(A) Examsdigest#(config)# line console 0
Examsdigest#(config-line)# password examsdigest
Examsdigest#(config-line)# login
Examsdigest#(config-line)# exit

(B) Examsdigest#(config)# enable secret examsdigest

(C) Examsdigest#(config)# enable console examsdigest

(D) Examsdigest#(config)# live vty 0 15
Examsdigest#(config-line)# password examsdigest
Examsdigest#(config-line)# login
Examsdigest#(config-line)# end

Question 32. Which of the following type of memory is used to store the configuration used by the switch when it is up and running?

(A) ROM

(B) RAM

(C) NVRAM

(D) Flash

Question 33. You have been tasked to configure the IPv4 address on the switch only on the VLAN 1 following the details below.

Configuration details:

IP address: 199.255.240.100

Subnet mask: 255.255.255.0

Default gateway: 199.255.240.1

Which of the following commands will you type to complete the task?

(A) Examsdigest#(config)# interface vlan 1
Examsdigest#(config-line)# ip address 199.255.240.100 255.255.255.0
Examsdigest#(config-line)# no shutdown
Examsdigest#(config-line)# end
Examsdigest#(config)# ip default-gateway 199.255.240.1

(B) Examsdigest#(config)# interface vlan 1
Examsdigest#(config-line)# ip address 199.255.241.100 255.255.255.0
Examsdigest#(config-line)# no shutdown
Examsdigest#(config-line)# end
Examsdigest#(config)# ip default-gateway 199.255.240.1

(C) Examsdigest#(config)# interface vlan 1
Examsdigest#(config-line)# ip address 199.255.240.100 255.255.0.0
Examsdigest#(config-line)# no shutdown
Examsdigest#(config-line)# end
Examsdigest#(config)# ip default-gateway 199.255.240.1

(D) Examsdigest#(config)# interface vlan 11
Examsdigest#(config-line)# ip address 199.255.240.100 255.255.255.0
Examsdigest#(config-line)# no shutdown
Examsdigest#(config-line)# end
Examsdigest#(config)# ip default-gateway 199.255.240.1

Question 34. Which of the following configuration commands defines the password that all users must use to reach enable mode?

(A) enable secret "type password"
(B) enable "type password"
(C) secret "type password"
(D) secret enable "type password"

Question 35. Which of the following command will you type to produce the output below?

```
Vlan1 is up, line protocol is up
Hardware is EtherSVI, address is 0023.e21b.4cc0 (bia
0023.e21b.4cc0)
Internet address is 192.168.1.101/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
```

(A) show interfaces vlans

(B) show interfaces

(C) show interfaces vlan 1

(D) show vlan 1

Question 36. NVRAM stores the initial or startup configuration file that is used when the switch is first powered on and when the switch is reloaded.

(A) TRUE

(B) FALSE

Question 37. Which of the following commands will you type to configure the interface VLAN 5 of the switch to learn the IP address with DHCP?

(A) configure terminal

interface vlan 5
no shutdown

(B) configure terminal
interface vlan 5
ip address dhcp
no shutdown

(C) configure terminal
native vlan dhcp
ip address dhcp

(D) configure terminal
interface vlan 5
ip address dhcp

Question 38. The running (active) configuration file is stored in the Flash Memory.

(A) TRUE

(B) FALSE

Question 39. Which of the following Cisco IOS Software Command Help lists commands that start with **int**?

(A) int<Tab>

(B) int ?

(C) ?

(D) int?

Question 40. Type the configuration command that produce the given output.

```
            Mac Address Table
------------------------------------------

Vlan    Mac Address         Type          Ports
----    -----------         --------      -----
   1    02AA.AAAA.AAAA      DYNAMIC       Gi0/1
   1    02BB.BBBB.BBBB      DYNAMIC       Gi0/2
   1    02CC.CCCC.CCCC      DYNAMIC       Gi0/3
Total Mac Addresses for this criterion: 3
```

(A) show mac address-table dynamic

(B) show address-table

(C) show mac

(D) show dynamic address-table

Answers 21-40

Question 21. Which of the following commands checks the status of the interfaces?

(A) show interface

(B) show status

(C) show interface status

(D) show status interface

Explanation 21. **show interface status is the correct answers.**

Question 22. You are in console line configuration mode. Which of the following commands would place you in enable mode?

(A) end

(B) back

(C) enable

(D) change

Explanation 22. **end is the correct answer.** The end command and the Ctrl+Z key sequence both move the user to enable mode regardless of the current configuration submode.

Question 23. Which of the following commands copies the configuration from RAM into NVRAM

(A) copy running-config startup-config

(B) copy startup-config running-config

(C) copy ram nvram

(D) copy nvram ram

Explanation 23. copy running-config startup-config is the correct answer. The running-config file is in RAM, and the startup-config file is in NVRAM so the command is: **copy running-config startup-config**

Question 24. The command that configures the switch as a DHCP client to discover its IPv4 address, mask, and default gateway is **ip address dhcp.**

(A) TRUE

(B) FALSE

Explanation 24. TRUE is the correct answer. The command **ip address dhcp** configures the switch as a DHCP client to discover its IPv4 address, mask, and default gateway

Question 25. In which of the following modes of the CLI could you configure the duplex setting for interface Fast Ethernet 0/2?

(A) Global configuration mode

(B) Enable mode

(C) Interface configuration mode

(D) VLAN mode

Explanation 25. Interface configuration mode is the correct answer. The speed and the duplex settings for Fast Ethernet 0/2 can be configured in the **interface configuration mode**.

Question 26. Which of the following commands administratively enables an interface

(A) shutdown

(B) no shutdown

(C) enable interface

(D) interface enable

Explanation 26. no shutdown is the correct answer. Cisco uses two interface subcommands to configure the idea of administratively enabling and disabling an interface: the **shutdown** command (to disable) and the **no shutdown** command (to enable).

Question 27. Switches use STP to prevent loops by causing some interfaces to block, meaning that they do not send or receive frames.

(A) TRUE

(B) FALSE

Explanation 27. **TRUE is the correct answer.** A primary feature of LAN switches is loop prevention, as implemented by **Spanning Tree Protocol (STP)**. Without STP, any flooded frames would loop for an indefinite period of time in Ethernet networks with physically redundant links.

To prevent looping frames, STP blocks some ports from forwarding frames so that only one active path exists between any pair of LAN segments.

The result of STP is good: frames do not loop infinitely, which makes the LAN usable. However, STP has negative features as well, including the fact that it takes some work to balance traffic across the redundant alternate links.

Question 28. A Layer 2 switch configuration places all its physical ports into VLAN 2. The IP addressing plan shows that address 175.28.1.150 (with mask 255.255.255.0) is reserved for use by this new LAN switch and that 175.28.1.254 is already configured on the router connected to that same VLAN.

The switch needs to support SSH connections into the switch

from any subnet in the network. Which of the following commands are part of the required configuration in this case? (Choose two answers.)

(A) The switch cannot support SSH because all its ports connect to VLAN 2, and the IP address must be configured on interface VLAN 1.

(B) The ip address 175.28.1.150 255.255.255.0 command in interface vlan 2 configuration mode.

(C) The ip default-gateway 175.28.1.254 command in global configuration mode.

(D) The ip address 172.16.2.250 255.255.255.0 command in interface vlan 1 configuration mode.

(E) The ip default-gateway 175.28.1.150 command in global configuration mode.

Explanation 26. **B and C are the correct answers.** To allow SSH or Telnet access, a switch must have a correct IP configuration. That includes the configuration of a correct IP address and mask on a VLAN interface. That VLAN interface must have a path out of the switch via ports assigned to that VLAN. In this case, with all ports assigned to VLAN 2, the switch must use interface VLAN 2 (using the interface vlan 2 configuration command).

Question 29. Which of the following commands lists the con-

tent of the startup-config (initial config) file.

(A) show startup-config

(B) show initial-config

(C) show content-config

(D) show file-config

Explanation 29. **show startup-config is the correct answer.**

Question 30. You want to configure the console password with password examsdigest. Which of the following commands will you type to meet the requirement?

(A) Examsdigest#(config)# line console 0
Examsdigest#(config-line)# password examsdigest
Examsdigest#(config-line)# login
Examsdigest#(config-line)# exit

(B) Examsdigest#(config)# enable secret examsdigest

(C) Examsdigest#(config)# enable console examsdigest

(D) Examsdigest#(config)# live vty 0 15
Examsdigest#(config-line)# password examsdigest
Examsdigest#(config-line)# login
Examsdigest#(config-line)# end

Explanation 30. **A is the correct answer.**

Question 31. You want to configure the telnet password for all vty lines with password examsdigest. Which of the following commands will you type to meet the requirement?

(A) Examsdigest#(config)# line console 0
Examsdigest#(config-line)# password examsdigest
Examsdigest#(config-line)# login
Examsdigest#(config-line)# exit

(B) Examsdigest#(config)# enable secret examsdigest

(C) Examsdigest#(config)# enable console examsdigest

(D) Examsdigest#(config)# live vty 0 15
Examsdigest#(config-line)# password examsdigest
Examsdigest#(config-line)# login
Examsdigest#(config-line)# end

Explanation 31. **D is the correct answer.**

Question 32. Which of the following type of memory is used to store the configuration used by the switch when it is up and running?

(A) ROM

(B) RAM

(C) NVRAM

(D) Flash

Explanation 32. **RAM is the correct answer.** Switches (and routers) keep the currently used configuration in **RAM**.

RAM: Sometimes called DRAM, for dynamic random-access memory, RAM is used by the switch just as it is used by any other computer: for working storage. The running configuration file is stored here.

Question 33. You have been tasked to configure the IPv4 address on the switch only on the VLAN 1 following the details below.

Configuration details:

IP address: 199.255.240.100

Subnet mask: 255.255.255.0

Default gateway: 199.255.240.1

Which of the following commands will you type to complete the task?

(A) **Examsdigest#(config)# interface vlan 1**
Examsdigest#(config-line)# ip address 199.255.240.100 255.255.255.0
Examsdigest#(config-line)# no shutdown
Examsdigest#(config-line)# end
Examsdigest#(config)# ip default-gateway 199.255.240.1

(B) Examsdigest#(config)# interface vlan 1

Examsdigest#(config-line)# ip address 199.255.241.100 255.255.255.0

Examsdigest#(config-line)# no shutdown

Examsdigest#(config-line)# end

Examsdigest#(config)# ip default-gateway 199.255.240.1

(C) Examsdigest#(config)# interface vlan 1

Examsdigest#(config-line)# ip address 199.255.240.100 255.255.0.0

Examsdigest#(config-line)# no shutdown

Examsdigest#(config-line)# end

Examsdigest#(config)# ip default-gateway 199.255.240.1

(D) Examsdigest#(config)# interface vlan 11

Examsdigest#(config-line)# ip address 199.255.240.100 255.255.255.0

Examsdigest#(config-line)# no shutdown

Examsdigest#(config-line)# end

Examsdigest#(config)# ip default-gateway 199.255.240.1

Explanation 33. **A is the correct answer.**

Question 34. Which of the following configuration commands defines the password that all users must use to reach enable mode?

(A) enable secret "type password"

(B) enable "type password"

(C) secret "type password"

(D) secret enable "type password"

Explanation 34. A is the correct answer.

Question 35. Which of the following command will you type to produce the output below?

```
Vlan1 is up, line protocol is up
Hardware is EtherSVI, address is 0023.e21b.4cc0 (bia
0023.e21b.4cc0)
Internet address is 192.168.1.101/24
MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
```

(A) show interfaces vlans

(B) show interfaces

(C) show interfaces vlan 1

(D) show vlan 1

Explanation 35. **C is the correct answer.**

Question 36. NVRAM stores the initial or startup configuration file that is used when the switch is first powered on and when the switch is reloaded.

(A) TRUE

(B) FALSE

Explanation 36. **TRUE is the correct answer.**

Question 37. Which of the following commands will you type to configure the interface VLAN 5 of the switch to learn the IP address with DHCP?

(A) configure terminal
interface vlan 5
no shutdown

(B) configure terminal
interface vlan 5
ip address dhcp
no shutdown

(C) configure terminal
native vlan dhcp
ip address dhcp

(D) configure terminal
interface vlan 5
ip address dhcp

Explanation 37. **B is the correct answer.**

Question 38. The running (active) configuration file is stored in the Flash Memory.

(A) TRUE

(B) FALSE

Explanation 38. **FALSE is the correct answer.** **RAM** is used by the switch for working storage. The running (active) configuration file is stored here.

Flash memory stores fully functional Cisco IOS images and is the default location where the switch gets its Cisco IOS at boot time. It also can be used to store any other files, including backup copies of configuration files.

Question 39. Which of the following Cisco IOS Software Command Help lists commands that start with **int**?

(A) int<Tab>

(B) int ?

(C) ?

(D) int?

Explanation 39. **Int? is the correct answer.** **int?**: Lists commands that start with int.

Question 40. Type the configuration command that produce the given output.

```
            Mac Address Table
-------------------------------------------

Vlan    Mac Address        Type          Ports
----    -----------        --------     -----
   1    02AA.AAAA.AAAA     DYNAMIC      Gi0/1
   1    02BB.BBBB.BBBB     DYNAMIC      Gi0/2
   1    02CC.CCCC.CCCC     DYNAMIC      Gi0/3
Total Mac Addresses for this criterion: 3
```

(A) show mac address-table dynamic

(B) show address-table

(C) show mac

(D) show dynamic address-table

Explanation 40. **show mac address-table dynamic is the correct answer.**

CHAPTER 3
IPv4 ADDRESSING

Questions 41-63

Question 41. Which of the following addresses are not valid Class A network IDs? (Choose all that apply)

(A) 1.0.0.0

(B) 5.0.0.0

(C) 140.0.0.0

(D) 127.0.0.0

(E) 9.0.0.0

(F) 195.0.0.0

Question 42. Why does the formula for the number of hosts per subnet ($2^H - 2$) require the subtraction of two hosts?

(A) To reserve two addresses for redundant default gateways (routers)

(B) To reserve the two addresses required for DHCP operation

(C) To reserve addresses for the subnet broadcast address and subnet ID

(D) To reserve addresses for the subnet ID and default

gateway (router)

Question 43. Which of the following addresses are valid Class C network IDs? (Choose two answers)

(A) 195.0.0.0

(B) 22.22.3.0

(C) 222.0.0.0

(D) 191.255.255.0

(E) 127.0.0.0

Question 44. A network designer asked you how many subnet (S) bits does he need to create 200 subnets?

(A) 2

(B) 5

(C) 8

(D) 11

Question 45. The addresses in the same network have different values in the network part.

(A) TRUE

(B) FALSE

Question 46. Which of the following IPv4 addresses has a subnet mask 255.255.0.0?

(A) 188.187.186.185

(B) 204.203.202.201

(C) 55.44.22.11

(D) 10.0.0.56

Question 47. Which of the following IPv4 addresses has a subnet mask 255.255.255.0?

(A) 188.187.186.185

(B) 204.203.202.201

(C) 55.44.22.11

(D) 10.0.0.56

Question 48. The first octet range from the Class A IP networks is 1 - 126.

(A) TRUE

(B) FALSE

Question 49. Which of the following IPv4 addresses has a subnet mask 255.0.0.0? (Choose all that apply)

(A) 188.187.186.185

(B) 204.203.202.201

(C) 55.44.22.11

(D) 10.0.0.56

(E) 100.24.5.56

(F) 192.168.178.6

Question 50. Which of the following ranges is a valid class B network numbers?

(A) 128.0.0.0 - 191.255.0.0

(B) 1.0.0.0 - 126.0.0.0

(C) 192.0.0.0 - 223.255.255.0

(D) 224.0.0.0 - 254.255.255.0

Question 51. Which of the following ranges is a valid class C network numbers?

(A) 128.0.0.0 - 191.255.0.0

(B) 1.0.0.0 - 126.0.0.0

(C) 192.0.0.0 - 223.255.255.0

(D) 224.0.0.0 - 254.255.255.0

Question 52. Which of the following is the default mask of the IP 10.2.0.0?

(A) 255.0.0.0

(B) 255.255.0.0

(C) 255.255.255.0

(D) 255.255.255.255

Question 53. What information can you extract having the IP address 172.16.99.45? (Choose two answers.)

(A) The network ID is 172.0.0.0.

(B) The default mask for the network is 255.255.255.0.

(C) The network is a Class B network.

(D) The number of host bits in the unsubnetted network is 16.

(E) The broadcast address of the network is 172.255.255.255

Question 54. A network designer asked you how many subnets (S) bits does he need to create 100 subnets? (Type only the number)

(A) 4

(B) 5

(C) 6

(D) 7

Question 55. The senior network engineer asked you to choose the broadcast address from the last subnet according to the following details:

Network 172.28.0.0 (Class B)
Mask 255.255.0.0 (for all subnets)

(A) 172.28.255.254

(B) 172.255.255.255

(C) 172.28.200.255

(D) 172.28.255.255

Question 56. The address 130.0.0.0 is a Class _____ network ID

(A) A

(B) B

(C) C

(D) D

Question 57. Which of the following is the default mask of the IP 178.25.3.0?

(A) 255.0.0.0

(B) 255.255.0.0

(C) 255.255.255.0

(D) 255.255.255.255

Question 58. The address 200.0.0.0 is a Class _____ network ID

(A) A

(B) B

(C) C

(D) D

Question 59. The range of the Class C public IP Networks is _____ - _____

(A) 10.0.0.0 - 140.255.255.0

(B) 192.0.0.0 - 223.255.255.0

(C) 200.0.0.0 - 223.255.255.0

(D) 224.0.0.0 - 254.255.255.0

Question 60. The senior network engineer asked you to choose the last usable address for a host from the last subnet according to the following details:

Network 9.0.0.0 (Class A)
Mask 255.255.0.0 (for all subnets)

(A) 9.255.255.254

(B) 10.255.255.254

(C) 11.255.255.254

(D) 12.255.255.254

Question 61. The first octet range from the Class B IP networks is 1 - 126.

(A) TRUE

(B) FALSE

Question 62. A network designer asked you how many subnet (S) bits does he need to create 5 subnets?

(A) 2

(B) 3

(C) 4

(D) 5

Question 63. Which of the following are private IP networks? (Choose all that apply)

(A) 172.31.100.0

(B) 164.16.2.0

(C) 192.166.255.0

(D) 192.168.1.0

(E) 11.11.11.0

(F) 172.24.0.0

Answers 41-63

Question 41. Which of the following addresses are not valid Class A network IDs? (Choose all that apply)

(A) 1.0.0.0

(B) 5.0.0.0

(C) 140.0.0.0

(D) 127.0.0.0

(E) 9.0.0.0

(F) 195.0.0.0

Explanation 41. **C, D and F are the correct answers.** Class A networks have the first octet in the range of 1–126, inclusive, and their network IDs have a 0 in the last three octets.

Invalid Class A network IDs are:

140.0.0.0

127.0.0.0

195.0.0.0

Question 42. Why does the formula for the number of hosts per subnet ($2^H - 2$) require the subtraction of two hosts?

(A) To reserve two addresses for redundant default gateways (routers)

(B) To reserve the two addresses required for DHCP opera-

tion

(C) To reserve addresses for the subnet broadcast address and subnet ID

(D) To reserve addresses for the subnet ID and default gateway (router)

Explanation 42. To reserve addresses for the subnet broadcast address and subnet ID is the correct answer. By definition, two address values in every IPv4 subnet cannot be used as host IPv4 addresses:

1. The first (lowest) numeric value in the subnet for the **subnet ID**.
2. The last (highest) numeric value in the subnet for the subnet **broadcast address**.

Question 43. Which of the following addresses are valid Class C network IDs? (Choose two answers)

(A) 195.0.0.0

(B) 22.22.3.0

(C) 222.0.0.0

(D) 191.255.255.0

(E) 127.0.0.0

Explanation 43. A and C are the correct answers. Class C networks have the first octet in the range of 192–223, inclusive,

and their network IDs have a 0 in the last three octets.

Question 44. A network designer asked you how many subnet (S) bits does he need to create 200 subnets?

(A) 2

(B) 5

(C) 8

(D) 11

Explanation 44. **8 is the correct answer.** 8 bits are enough to create 200 subnets.

You need to follow the formula of **2^S > number of subnets** to find out the required number of subnet bits to create 200 subnets.

*S = number of subnet bits

For example:

2^6 = 64 < 200 is not large enough

2^7 = 128 < 200 is not large enough

2^8 = 256 > 200 is enough

Description	Class A	Class B	Class C
First octet range	**1 – 126**	**128 – 191**	**192 – 223**
Valid network numbers	1.0.0.0 – 126.0.0.0	128.0.0.0 – 191.255.0.0	192.0.0.0 – 223.255.255.0
Default mask	**255.0.0.0**	**255.255.0.0**	**255.255.255.0**

Question 45. The addresses in the same network have different values in the network part.

(A) TRUE

(B) FALSE

Explanation 45. **FALSE is the correct answer.** The addresses in the classful network have a structure with two parts: the network part and the host part.

Then, comparing any two IP addresses in one network, the following observations can be made:

1. The addresses in the same network have the same values in the network part.

2. The addresses in the same network have different values in the host part.

Question 46. Which of the following IPv4 addresses has a subnet mask 255.255.0.0?

(A) 188.187.186.185

(B) 204.203.202.201

(C) 55.44.22.11

(D) 10.0.0.56

Explanation 46. **188.187.186.185 is the correct answer.** Class B networks have the first octet in the range of 128–191. The default subnet mask for the Class B networks is 255.255.0.0

Question 47. Which of the following IPv4 addresses has a subnet mask 255.255.255.0?

(A) 188.187.186.185

(B) 204.203.202.201

(C) 55.44.22.11

(D) 10.0.0.56

Explanation 47. 204.203.202.201 is the correct answer.

Class C networks have the first octet in the range of 192–223. The default subnet mask for the Class C networks is 255.255.255.0

Description	Class A	Class B	Class C
First octet range	**1 – 126**	**128 – 191**	**192 – 223**
Valid network numbers	1.0.0.0 – 126.0.0.0	128.0.0.0 – 191.255.0.0	192.0.0.0 – 223.255.255.0
Default mask	**255.0.0.0**	**255.255.0.0**	**255.255.255.0**

Question 48. The first octet range from the Class A IP networks is 1 - 126.

(A) TRUE

(B) FALSE

Explanation 48. **TRUE is the correct answer.**

Class A networks have the first octet in the range of 1–126.

Question 49. Which of the following IPv4 addresses has a subnet mask 255.0.0.0? (Choose all that apply)

(A) 188.187.186.185

(B) 204.203.202.201

(C) 55.44.22.11

(D) 10.0.0.56

(E) 100.24.5.56

(F) 192.168.178.6

Explanation 49. **C, D, and E are the correct answers.**

Description	Class A	Class B	Class C
First octet range	1 – 126	128 – 191	192 – 223

Valid net-work num-bers	1.0.0.0 – 126.0.0.0	128.0.0.0 – 191.255.0.0	192.0.0.0 – 223.255.255.0
Default mask	255.0.0.0	255.255.0.0	255.255.255.0

Question 50. Which of the following ranges is a valid class B network numbers?

(A) 128.0.0.0 - 191.255.0.0

(B) 1.0.0.0 - 126.0.0.0

(C) 192.0.0.0 - 223.255.255.0

(D) 224.0.0.0 - 254.255.255.0

Explanation 50. **A is the correct answer.**

De-scrip-tion	Class A	Class B	Class C
First octet range	1 – 126	128 – 191	192 – 223

Valid net-work num-bers	1.0.0.0 – 126.0.0.0	128.0.0.0 – 191.255.0.0	192.0.0.0 – 223.255.255.0
De-fault mask	**255.0.0.0**	**255.255.0.0**	**255.255.255.0**

Question 51. Which of the following ranges is a valid class C network numbers?

(A) 128.0.0.0 - 191.255.0.0

(B) 1.0.0.0 - 126.0.0.0

(C) 192.0.0.0 - 223.255.255.0

(D) 224.0.0.0 - 254.255.255.0

Explanation 51. **192.0.0.0 - 223.255.255.0 is the correct answer.**

Question 52. Which of the following is the default mask of the IP 10.2.0.0?

(A) 255.0.0.0

(B) 255.255.0.0

(C) 255.255.255.0

(D) 255.255.255.255

Explanation 52. **255.0.0.0 is the correct answer.**

Class A networks have the first octet in the range of 1–126.The default subnet mask for the Class A networks is 255.0.0.0.

Question 53. What information can you extract having the IP address 172.16.99.45? (Choose two answers.)

(A) The network ID is 172.0.0.0.

(B) The default mask for the network is 255.255.255.0.

(C) The network is a Class B network.

(D) The number of host bits in the unsubnetted network is 16.

(E) The broadcast address of the network is 172.255.255.255.

Explanation 52. **C and D are the correct answers.**

The first octet (172) is in the range of values for **Class B addresses (128–191)**.

As a result, the **network ID** can be formed by copying the first two octets (172.16) and writing 0s for the last two octets (172.16.0.0).

The default mask for all Class B networks is 255.255.0.0, and the number of host bits in all unsubnetted Class B networks is

16.

The **broadcast address** of this network is **172.16.255.255**.

Question 54. A network designer asked you how many subnets (S) bits does he need to create 100 subnets? (Type only the number)

(A) 4

(B) 5

(C) 6

(D) 7

Explanation 54. **C and D are the correct answers.**

7 bits are enough to create 100 subnets. You need to follow the formula of **2^S > number of subnets** to find out the required number of subnet bits to create 200 subnets.

*S = number of subnet bits

For example:

2^5 = 32 < 100 is not large enough

2^6 = 64 < 100 is not large enough

2^7 = 128 > 100 is enough

Question 55. The senior network engineer asked you to choose the broadcast address from the last subnet according

to the following details:

Network 172.28.0.0 (Class B)

Mask 255.255.0.0 (for all subnets)

(A) 172.28.255.254

(B) 172.255.255.255

(C) 172.28.200.255

(D) 172.28.255.255

Explanation 55. 172.28.255.255 is the correct answer.

First subnet

Subnet Network: 172.28.0.0

IP Addresses: 172.28.0.1 – 172.28.0.254

Broadcast Address: 172.28.0.255

Second subnet

Subnet Network: 172.28.1.0

IP Addresses: 172.28.1.1 – 172.28.1.254

Broadcast Address: 172.28.1.255

Third subnet

Subnet Network: 172.28.3.0

IP Addresses: 172.28.3.1 – 172.28.3.254

Broadcast Address: 172.28.3.255

Skipping many subnets...

Last subnet

Subnet Network: 172.28.255.0

IP Addresses: 172.28.255.1 – 172.28.255.254

Broadcast Address: 172.28.255.255

Question 56. The address 130.0.0.0 is a Class _____ network ID

(A) A

(B) B

(C) C

(D) D

Explanation 56. **B is the correct answer.**

The address 130.0.0.0 is Class B network ID.

All Class B networks begin with values between 128 and 191, inclusive, in their first octets.

The network ID has any value in the 128–191 range in the first octet, and any value from 0 to 255 inclusive in the second octet, with decimal 0s in the final two octets.

Question 57. Which of the following is the default mask of the IP 178.25.3.0?

(A) 255.0.0.0

(B) 255.255.0.0

(C) 255.255.255.0

(D) 255.255.255.255

Explanation 57. **255.255.0.0 is the correct answer.**

First, you have to identify the Class of the given IP address.

In this case, the address **178.25.3.0** is a Class B.

Class B networks have 128-191 as their first octet and use a default subnet mask of 255.255.0.0.

De-scrip-tion	Class A	Class B	Class C
First octet range	1 – 126	128 – 191	192 – 223

Valid net-work num-bers	1.0.0.0 – 126.0.0.0	128.0.0.0 – 191.255.0.0	192.0.0.0 – 223.255.255.0
De-fault mask	**255.0.0.0**	**255.255.0.0**	**255.255.255.0**

Question 58. The address 200.0.0.0 is a Class _____ network ID

(A) A

(B) B

(C) C

(D) D

Explanation 58. **C is the correct answer.**

The address 200.0.0.0 is Class C network ID.

All Class C networks begin with values between 192 and 223, inclusive, in their first octets.

The network ID has any value in the 192–223 range in the first octet, and any value from 0 to 255 inclusive in the second octet, with decimal 0s in the final two octets.

Question 59. The range of the Class C public IP Networks is _____ - _____

(A) 10.0.0.0 - 140.255.255.0

(B) 192.0.0.0 - 223.255.255.0

(C) 200.0.0.0 - 223.255.255.0

(D) 224.0.0.0 - 254.255.255.0

Explanation 59. **192.0.0.0 - 223.255.255.0 is the correct answer.**

Question 60. The senior network engineer asked you to choose the last usable address for a host from the last subnet according to the following details:

Network 9.0.0.0 (Class A)
Mask 255.255.0.0 (for all subnets)

(A) 9.255.255.254

(B) 10.255.255.254

(C) 11.255.255.254

(D) 12.255.255.254

Explanation 60. **9.255.255.254 is the correct answer.**

First subnet

Subnet Network: 9.0.0.0

First IP Address: 9.0.0.1

Last IP Address: 9.0.255.254

Broadcast Address: 9.0.255.255

Second subnet

Subnet Network: 9.1.0.0

First IP Address: 9.1.0.1

Last IP Address: 9.1.0.254

Broadcast Address: 9.1.255.255

Third subnet

Subnet Network: 9.2.0.0

First IP Address: 9.2.0.1

Last IP Address: 9.2.0.254

Broadcast Address: 9.2.255.255

Forth subnet

Subnet Network: 9.3.0.0

First IP Address: 9.3.0.1

Last IP Address: 9.3.0.254

Broadcast Address: 9.3.255.255

Skipping many subnets...

Last subnet

Subnet Network: 9.255.0.0

First IP Address: 9.255.0.1

Last IP Address: **9.255.255.254**

Broadcast Address: 9.255.255.255

Question 61. The first octet range from the Class B IP networks is 1 - 126.

(A) TRUE

(B) FALSE

Explanation 61. **FALSE is the correct answer.**

De-scrip-tion	Class A	Class B	Class C
First octet range	**1 – 126**	**128 – 191**	**192 – 223**
Valid net-work num-bers	1.0.0.0 – 126.0.0.0	128.0.0.0 – 191.255.0.0	192.0.0.0 – 223.255.255.0

De-fault mask	**255.0.0.0**	**255.255.0.0**	**255.255.255.0**

Question 62. A network designer asked you how many subnet (S) bits does he need to create 5 subnets?

(A) 2

(B) 3

(C) 4

(D) 5

Explanation 62. **3 is the correct answer.** 3 bits are enough to create 5 subnets. You need to follow the formula of **2^S > number of subnets** to find out the required number of subnet bits to create 5 subnets.

*S = number of subnet bits

For example:

2^1 = 2 < 5 is not large enough

2^2 = 4 < 5 is not large enough

2^3 = 8 > 5 is enough

Question 63. Which of the following are private IP networks? (Choose all that apply)

(A) 172.31.100.0

(B) 164.16.2.0

(C) 192.166.255.0

(D) 192.168.1.0

(E) 11.11.11.0

(F) 172.24.0.0

Explanation 63. **A, D and F are the correct answers.** The range of private IP Networks are:

Class A 10.0.0.0 – 10.255.255.255

Class B 172.16.0.0 – 172.31.255.255

Class C 192.168.0.0 – 192.168.255.255

CHAPTER 4
ADVANCED IPv4 ADDRESSING

Questions 64-90

Question 64. Given the following IP address - 20.54.23.3 and subnet mask - 255.255.255.0 choose the subnet ID and the broadcast address from that particular IP.

(A) Subnet ID: 20.54.23.0
Broadcast Address: 20.54.23.255

(B) Subnet ID: 20.54.0.0
Broadcast Address: 20.54.0.255

(C) Subnet ID: 20.54.0.0
Broadcast Address: 20.54.255.255

(D) Subnet ID: 20.54.23.1
Broadcast Address: 20.54.23.255

Question 65. The converted binary mask 11111111.11111111.11000000.00000000 to decimal is _____.

(A) 255.255.192.0

(B) 255.255.64.0

(C) 255.192.0.0

(D) 255.255.255.192

Question 66. The converted binary mask 11111111.11100000.00000000.00000000 to decimal is _____.

(A) 255.255.255.224

(B) 255.255.224.0

(C) 255.224.0.0

(D) 255.64.0.0

Question 67. The converted binary mask 11111110.00000000.00000000.00000000 to decimal is _____.

(A) 255.255.255.254

(B) 254.0.0.0

(C) 255.254.0.0

(D) 255.255.254.0

Question 68. You are working with a network engineer to design a network for the new Campus. He provided the following details:

The IP address is 195.240.37.43

The subnet mask is 255.255.255.224

You have been tasked to:

1. Find the Prefix length

2. Find the Class of the address

(A) Prefix length = 24 | Class = C

(B) Prefix length = 20 | Class = B

(C) Prefix length = 15 | Class = C

(D) Prefix length = 30 | Class = A

Question 69. Your senior network engineer tells you to configure the DHCP server to lease the last 100 usable IP addresses in subnet 12.5.4.0/23. Which of the following IP addresses could be leased as a result of your new configuration?

(A) 12.5.1.156

(B) 12.5.5.200

(C) 12.5.4.254

(D) 12.5.255.200

Question 70. You are working with a network engineer to design a network for the new Campus. He provided the following details:

The IP address is 195.240.37.43

The subnet mask is 255.255.255.224

You have been tasked to find the:

1. Network (N) bits

2. Subnet bits (S)

3. Host (H) bits.

(A) Network Bits = 15 | Subnet Bits = 2 | Host Bits = 1

(B) Network Bits = 20 | Subnet Bits = 3 | Host Bits = 1

(C) Network Bits = 24 | Subnet Bits = 3 | Host Bits = 5

(D) Network Bits = 28 | Subnet Bits = 1 | Host Bits = 2

Question 71. Which of the following binary masks is equivalent to the 255.255.255.240 dotted-decimal notation (DDN)?

(A) 11111111.11111111.11111111.11111100

(B) 11111111.11111111.11111111.11110000

(C) 11111111.11111111.11111111.10000000

(D) 11111111.11111111.11111111.11111110

Question 72. Which of the following binary masks is equivalent to the 255.192.0.0 dotted-decimal notation (DDN)?

(A) 11111111.11000000.00000000.00000000

(B) 11111111.11111111.11111111.00000000

(C) 11111111.11111111.11111111.10000000

(D) 11111111.11111111.11111111.11111110

Question 73. Find the subnet ID from the IP address 10.75.20.3/24

(A) 10.75.5.0

(B) 10.75.0.0

(C) 10.75.20.0

(D) 10.0.0.0

Question 74. Find the subnet ID from the IP address 10.75.20.4/17

(A) 10.75.5.0

(B) 10.75.0.0

(C) 10.75.20.0

(D) 10.0.0.0

Question 75. Which of the following dotted-decimal notation (DDN) is equivalent of /17.

(A) 255.255.192.0

(B) 255.128.0.0

(C) 255.255.128.0

(D) 255.255.224.0

Question 76. Which of the following dotted-decimal notation (DDN) is equivalent of /28.

(A) 255.255.255.240

(B) 255.128.224.0

(C) 255.255.255.224

(D) 255.255.255.248

Question 77. The broadcast address from the IP address

67.68.67.68/12 is 67.79.255.255.

(A) TRUE

(B) FALSE

Question 78. Subnet masks can be written as 32-bit binary numbers, but not just any binary number. In particular, the binary subnet mask must follow these rules:

1. The value must not interleave 1s and 0s.

2. If 0s exist, they are on the left.

3. If 1s exist, they are on the right.

(A) TRUE

(B) FALSE

Question 79. Which of the following answers lists the prefix (CIDR) format equivalent of 255.255.254.0?

(A) /20

(B) /21

(C) /22

(D) /23

Question 80. Which of the following answers lists the prefix (CIDR) format equivalent of 255.192.0.0?

(A) /10

(B) /11

(C) /12

(D) /13

Question 81. Your task is to troubleshoot a user's PC with IP 192.168.100.1/28. Based on the given details choose the number of the network (N), subnet (S), and host (H) bits.

(A) Network Bits = 28 | Subnet Bits = 1 | Host Bits = 2

(B) Network Bits = 20 | Subnet Bits = 5 | Host Bits = 7

(C) Network Bits = 24 | Subnet Bits = 4 | Host Bits = 4

(D) Network Bits = 30 | Subnet Bits = 1 | Host Bits = 1

Question 82. Your task is to find the broadcast address from the IP address 10.75.20.3 with subnet mask 255.248.0.0

(A) Broadcast address: 10.75.255.255

(B) Broadcast address: 10.75.20.255

(C) Broadcast address: 10.79.255.255

(D) Broadcast address: 10.80.255.255

Question 83. Your task is to find the broadcast address from the IP address 172.30.70.26 with subnet mask 255.255.192.0

(A) Broadcast address: 172.30.127.255

(B) Broadcast address: 172.30.70.255

(C) Broadcast address: 172.30.100.255

(D) Broadcast address: 172.30.87.255

Question 84. Which of the following answers lists the dotted-

decimal notation (DDN) equivalent of /30?

(A) 255.255.255.240

(B) 255.255.255.252

(C) 255.255.192.0

(D) 255.255.252.0

Question 85. Which of the following answers lists the dotted-decimal notation (DDN) equivalent of /18?

(A) 255.255.255.192

(B) 255.255.224.0

(C) 255.255.128.0

(D) 255.255.192.0

Question 86. Which of the following masks, when used within a Class B network, would supply enough subnet bits to support 90 subnets? (Choose two)

(A) /24

(B) /21

(C) /19

(D) 255.255.255.252

(E) 255.255.240.0

(F) 255.255.224.0

Question 87. Which of the following masks, when used within a Class A network, would supply enough subnet bits to support

8 subnets? (Choose two)

(A) /10

(B) /11

(C) /9

(D) /8

Question 88. Your task is to troubleshoot a user's PC with IP 10.20.30.5 and mask 255.255.255.0. Based on the given details type the number of the network (N), subnet (S), and host (H) bits.

(A) Network Bits = 16 | Subnet Bits = 15 | Host Bits = 1

(B) Network Bits = 16 | Subnet Bits = 1 | Host Bits = 15

(C) Network Bits = 8 | Subnet Bits = 8 | Host Bits = 16

(D) Network Bits = 8 | Subnet Bits = 16 | Host Bits = 8

Question 89. The converted binary mask 11111111.11111111.11111110.00000000 to decimal is _____.

(A) 255.255.255.192

(B) 255.255.254.0

(C) 255.255.252.0

(D) 255.255.255.224

Question 90. Which of the following binary masks is equivalent to the 255.192.0.0 dotted-decimal notation (DDN)?

(A) 11111111.11000000.00000000.00000000

(B) 11111111.11100000.00000000.00000000

(C) 11111111.11110000.00000000.00000000

(D) 11111111.11111000.00000000.00000000

Answers 64-90

Question 64. Given the following IP address - 20.54.23.3 and subnet mask - 255.255.255.0 choose the subnet ID and the broadcast address from that particular IP.

(A) Subnet ID: 20.54.23.0
Broadcast Address: 20.54.23.255

(B) Subnet ID: 20.54.0.0
Broadcast Address: 20.54.0.255

(C) Subnet ID: 20.54.0.0
Broadcast Address: 20.54.255.255

(D) Subnet ID: 20.54.23.1
Broadcast Address: 20.54.23.255

Explanation 64. **A is the correct answer.** If the mask has only 255 and 0 then the process of finding the subnet ID and the broadcast address is straightforward.

Use the following steps for each of the four octets to find the subnet ID:

Step 1) If the mask octet = 255, copy the decimal IP address.

Step 2) If the mask octet = 0, write a decimal 0.

Use the following steps for each of the four octets to find the

subnet broadcast address:

Step 1) If the mask octet = 255, copy the decimal IP address.

Step 2) If the mask octet = 0, write a decimal 255.

Question 65. The converted binary mask 11111111.11111111.11000000.00000000 to decimal is _____.

(A) 255.255.192.0

(B) 255.255.64.0

(C) 255.192.0.0

(D) 255.255.255.192

Explanation 65. 255.255.192.0 is the correct answer.

There are only nine possible values in one octet of a subnet mask as shown in the table below.

Binary Mask Octet	Decimal Equivalent	Number of Binary 1s
0	0	0
10000000	128	1
11000000	192	2
11100000	224	3

11110000	240	4
11111000	248	5
11111100	252	6
11111110	254	7
11111111	255	8

Question 66. The converted binary mask 11111111.11100000.00000000.00000000 to decimal is _____.

(A) 255.255.255.224

(B) 255.255.224.0

(C) 255.224.0.0

(D) 255.64.0.0

Explanation 66. **255.224.0.0 is the correct answer.**

There are only nine possible values in one octet of a subnet mask as shown in the table below.

Binary Mask Octet	Decimal Equivalent	Number of Binary 1s
0	0	0

10000000	128	1
11000000	192	2
11100000	224	3
11110000	240	4
11111000	248	5
11111100	252	6
11111110	254	7
11111111	255	8

Question 67. The converted binary mask 11111110.00000000.00000000.00000000 to decimal is _____.

(A) 255.255.255.254

(B) 254.0.0.0

(C) 255.254.0.0

(D) 255.255.254.0

Explanation 67. **254.0.0.0 is the correct answer.**

There are only nine possible values in one octet of a subnet mask as shown in the table below.

Binary Mask Octet	Decimal Equivalent	Number of Binary 1s
0	0	0
10000000	128	1
11000000	192	2
11100000	224	3
11110000	240	4
11111000	248	5
11111100	252	6
11111110	254	7
11111111	255	8

Question 68. You are working with a network engineer to design a network for the new Campus. He provided the following details:

The IP address is 195.240.37.43

The subnet mask is 255.255.255.224

You have been tasked to:

1. Find the Prefix length

2. Find the Class of the address

(A) Prefix length = 24 | Class = C

(B) Prefix length = 20 | Class = B

(C) Prefix length = 15 | Class = C

(D) Prefix length = 30 | Class = A

Explanation 68. Prefix length = 24 | Class = C is the correct answer. The **Prefix Length** can be found once you convert the mask to binary and count the 1s.

In this case, the subnet mask 255.255.255.224 in binary is 11111111.11111111.11111111.11100000.

Count the number of the 1s to find the prefix length.

Prefix Length: /27.

The address 195.240.37.43 is a **Class C**.

The range of Class C public IP Networks is: 192.0.0.0 – 223.255.255.0

The number Network bits for Class C address is **24 bits**.

Question 69. Your senior network engineer tells you to configure the DHCP server to lease the last 100 usable IP addresses

in subnet 12.5.4.0/23. Which of the following IP addresses could be leased as a result of your new configuration?

(A) 12.5.1.156

(B) 12.5.5.200

(C) 12.5.4.254

(D) 12.5.255.200

Explanation 69. 12.5.5.200 is the correct answer. To answer this question, you need to find the range of addresses in the subnet, which typically then means you need to calculate the subnet ID and subnet broadcast address. With a subnet ID/mask of 12.5.4.0/23, the mask converts to 255.255.254.0.

The subnet mask is 255.255.254.0, so the network ID multiplier is 256 – 254 = 2.
The possible subnet IDs are 12.5.0.0, 12.5.2.0, 12.5.4.0, 12.5.6.0, 12.5.8.0, 12.5.10.0 and so on. In this case, the network **12.5.4.0** is the winner.

The IP address range of the network is **12.5.4.0 – 12.5.5.255** (the next address 12.5.6.0 is the next subnet ID)

The broadcast address is the last address of the network so, the broadcast address is 12.5.5.255. The usable addresses of that network are 12.5.4.1 – 12.5.5.254 we exclude the network

ID (12.5.4.0) and the broadcast address (12.5.5.255).

Now you need to find the last **100 usable addresses** to configure the DHCP. The range of the last 100 usable IP addresses is **12.5.5.155 – 12.5.5.254**

Question 70. You are working with a network engineer to design a network for the new Campus. He provided the following details:
The IP address is 195.240.37.43
The subnet mask is 255.255.255.224
You have been tasked to find the:
1. Network (N) bits
2. Subnet bits (S)
3. Host (H) bits.

(A) Network Bits = 15 | Subnet Bits = 2 | Host Bits = 1
(B) Network Bits = 20 | Subnet Bits = 3 | Host Bits = 1
(C) Network Bits = 24 | Subnet Bits = 3 | Host Bits = 5
(D) Network Bits = 28 | Subnet Bits = 1 | Host Bits = 2

Explanation 70. **Network Bits = 24 | Subnet Bits = 3 | Host Bits = 5 is the correct answer.** The **Prefix Length** can be found once you convert the mask to binary and count the 1s. In this case, the subnet mask 255.255.255.224 in binary is

11111111.11111111.11111111.11100000.

Count the number of the 1s to find the prefix length.
Prefix Length: /27.

The address 195.240.37.43 is a **Class C**.
The range of Class C public IP Networks is: 192.0.0.0 – 223.255.255.0
The number Network bits for Class C address is **24 bits**.
So, the Network bits are 24.

The number of Subnet bits is Prefix length (27) – Network bits (24).
So, the Subnet bits are 27 – 24 = 3.

The number of Host bits is the number of total address bits (32) – Prefix length (27).
So, the host bits are 32 – 27 = 5.

Question 71. Which of the following binary masks is equivalent to the 255.255.255.240 dotted-decimal notation (DDN)?

(A) 11111111.11111111.11111111.11111100
(B) 11111111.11111111.11111111.11110000
(C) 11111111.11111111.11111111.10000000
(D) 11111111.11111111.11111111.11111110

Explanation 71. **11111111.11111111.11111111.11110000 is the correct answer.** There are only nine possible values in one octet of a subnet mask as shown in the table below. So start converting each octet one by one to get the final result.

1. First octet = 255 | **First octet in binary** = 11111111
2. Second octet = 255 | **Second octet in binary** = 11111111
3. Third octet = 255 | **Third octet in binary** = 11111111
4. Forth octet = 240 | **Forth octet in binary** = 11110000

Final result: 11111111.11111111.11111111.11110000

Binary Mask Octet	Decimal Equivalent	Number of Binary 1s
0	0	0
10000000	128	1
11000000	192	2
11100000	224	3
11110000	240	4
11111000	248	5

11111100	252	6
11111110	254	7
11111111	255	8

Question 72. Which of the following binary masks is equivalent to the 255.192.0.0 dotted-decimal notation (DDN)?

(A) 11111111.11000000.00000000.00000000

(B) 11111111.11111111.11111111.00000000

(C) 11111111.11111111.11111111.10000000

(D) 11111111.11111111.11111111.11111110

Explanation 72. 11111111.11000000.00000000.00000000 is the correct answer. There are only nine possible values in one octet of a subnet mask as shown in the table below.

So start converting each octet one by one to get the final result.

1. First octet = 255 | **First octet in binary** = 11111111

2. Second octet = 192 | **Second octet in binary** = 11000000

3. Third octet = 0 | **Third octet in binary** = 00000000

4. Forth octet = 0 | **Forth octet in binary** = 00000000

Final result: 11111111.11000000.00000000.00000000

Question 73. Find the subnet ID from the IP address 10.75.20.3/24

(A) 10.75.5.0

(B) 10.75.0.0

(C) 10.75.20.0

(D) 10.0.0.0

Explanation 73. **10.75.20.0 is the correct answer.**

IP address = 10.75.20.3/24

Subnet mask = 255.255.255.0

The subnet mask can be found from the prefix length /24.

To find the subnet ID follow the steps for each of the four octets.

Step 1) If the mask octet = 255, copy the decimal IP address.

Step 2) If the mask octet = 0, write a decimal 0.

The subnet ID for 10.75.20.3/24 is **10.75.20.0**

Question 74. Find the subnet ID from the IP address 10.75.20.4/17

(A) 10.75.5.0

(B) 10.75.0.0

(C) 10.75.20.0

(D) 10.0.0.0

Explanation 74. **10.75.0.0 is the correct answer.**

IP address = 10.75.20.4/17

Subnet mask = 255.255.128.0

The subnet mask can be found from the prefix length /17.

The subnet mask is 255.255.128.0, so the network ID multiplier is 256 – 128 = 128

The possible subnet IDs are 10.75.0.0 and 10.75.128.0.

As you can see the network 10.75.0.0 is the winner as the IP address of 10.75.20.4 belongs to that network IP range.

The IP address range of the network is 10.75.0.0 – 10.75.127.255 (the next address 10.75.128.0 is the next subnet ID). The subnet ID for 10.75.20.4/17 is **10.75.0.0**

Question 75. Which of the following dotted-decimal notation (DDN) is equivalent of /17.

(A) 255.255.192.0

(B) 255.128.0.0

(C) 255.255.128.0

(D) 255.255.224.0

Explanation 75. **255.255.128.0 is the correct answer.**
The **/17** is the equivalent of the mask that in binary has 17 binary 1s.

To convert that to DDN format, write down all the binary 1s (17 in this case), followed by binary 0s for the remainder of the 32-bit mask.

Then take 8 bits at a time and convert from binary to decimal.

Using the /17 mask in this question, the binary mask is **11111111.11111111.10000000.00000000**. Each of the first two octets is all binary 1s, so each converts to 255.

The third octet, 10000000, converts to 128, for a DDN mask of **255.255.128.0.**

Question 76. Which of the following dotted-decimal notation (DDN) is equivalent of /28.

(A) 255.255.255.240

(B) 255.128.224.0

(C) 255.255.255.224

(D) 255.255.255.248

Explanation 76. **255.255.128.0 is the correct answer.**

The **/28** is the equivalent of the mask that in binary has 17 binary 1s.

To convert that to DDN format, write down all the binary 1s (17 in this case), followed by binary 0s for the remainder of the 32-bit mask.

Then take 8 bits at a time and convert from binary to decimal.

Using the /28 mask in this question, the binary mask is **11111111.11111111.11111111.11110000**. Each of the first three octets is all binary 1s, so each converts to 255.

The forth octet, 11110000, converts to 240, for a DDN mask of **255.255.255.240.**

Question 77. The broadcast address from the IP address 67.68.67.68/12 is 67.79.255.255.

(A) TRUE

(B) FALSE

Explanation 77. **TRUE is the correct answer.**

First, you have to find the subnet mask for the prefix **/12**. The

prefix length means that the subnet mask in binary is: **11111111.11110000.00000000.00000000**

Now, convert the subnet mask from binary to decimal.
The subnet mask in decimal is **255.240.0.0**, so the network ID multiplier is 256 – 240 = 16

So, the possible subnet IDs are:
67.0.0.0
67.16.0.0
67.32.0.0
67.48.0.0
67.64.0.0
67.80.0.0 and so on...

As you can see the network 67.64.0.0 **is the winner** as the IP address of 67.68.67.68 belongs to that particular network IP range.
The IP address range of the network is 67.64.0.0 – 67.79.255.255 (the next address 67.80.0.0 is the next subnet ID)

The broadcast address is the last address of the network so, the broadcast address is **67.79.255.255**

Question 78. Subnet masks can be written as 32-bit binary numbers, but not just any binary number. In particular, the binary subnet mask must follow these rules:

1. The value must not interleave 1s and 0s.

2. If 0s exist, they are on the left.

3. If 1s exist, they are on the right.

(A) TRUE

(B) FALSE

Explanation 78. **FALSE is the correct answer.**

Subnet masks can be written as 32-bit binary numbers, but not just any binary number. In particular, the binary subnet mask must follow these rules:

1. The value must not interleave 1s and 0s.

2. If 1s exist, they are on the left.

3. If 0s exist, they are on the right.

Question 79. Which of the following answers lists the prefix (CIDR) format equivalent of 255.255.254.0?

(A) /20

(B) /21

(C) /22

(D) /23

Explanation 79. **/23 is the correct answer.**

Convert one octet at a time:

The first octet (255) convert to an 8-bit binary **11111111** total 8.

The second octet (255) convert to an 8-bit binary **11111111** total 8.

The third octet (254) convert to an 8-bit binary **11111110** total 7.

The fourth octet (0) convert to an 8-bit binary **00000000** total 0.

The equivalent of 255.255.254.0 is 11111111.11111111.11111110.00000000

So, the total number of binary 1s (which defines the prefix length) is 8 + 8 + 7 + 0 = /23.

Question 80. Which of the following answers lists the prefix (CIDR) format equivalent of 255.192.0.0?

(A) /10

(B) /11

(C) /12

(D) /13

Explanation 80. **/10 is the correct answer.**

Convert one octet at a time:

The first octet (255) convert to an 8-bit binary **11111111** total 8.
The second octet (192) convert to an 8-bit
binary **11000000** total 2.
The third octet (0) convert to an 8-bit binary **00000000** total 0.
The fourth octet (0) convert to an 8-bit binary **00000000** total 0.

The equivalent of 255.192.0.0 is
11111111.11000000.00000000.00000000

So, the total number of binary 1s (which defines the prefix length) is 8 + 2 + 0 + 0 = /10.

Question 81. Your task is to troubleshoot a user's PC with IP 192.168.100.1/28. Based on the given details choose the number of the network (N), subnet (S), and host (H) bits.

(A) Network Bits = 28 | Subnet Bits = 1 | Host Bits = 2
(B) Network Bits = 20 | Subnet Bits = 5 | Host Bits = 7
(C) Network Bits = 24 | Subnet Bits = 4 | Host Bits = 4
(D) Network Bits = 30 | Subnet Bits = 1 | Host Bits = 1

Explanation 81. **Network Bits = 24 | Subnet Bits = 4 | Host Bits = 4 is the correct answer.**
The size of the **network part** is always either 8, 16, or 24 bits,

based on whether it is Class A, B, or C, respectively.

In this case, we have a Class C address, so the network part is 24bits.

N = 24

The prefix format is /28 so the mask is 255.255.255.240.
The number of subnet bits is the difference between the prefix length(28) and N(24).

S = prefix – N

S = 28 – 4 bits

S = 4

The number of the host bits is the total number of IP address bits(32) which is always 32bits minus the prefix length(28).

H = Address bits – prefix

H = 32 – 28

H = 4

Question 82. Your task is to find the broadcast address from the IP address 10.75.20.3 with subnet mask 255.248.0.0

(A) Broadcast address: 10.75.255.255

(B) Broadcast address: 10.75.20.255

(C) Broadcast address: 10.79.255.255

(D) Broadcast address: 10.80.255.255

Explanation 82. **Broadcast address: 10.79.255.255 is the correct answer.** The process of finding the broadcast ID when the mask is neither 255 nor 0 is more complicated. In order to find the broadcast ID you have to find the **network ID multiplier**.

The network ID multiplier can be found once you subtract the 256 – last octet from the mask that is neither 255 nor 0.

The subnet mask is 255.248.0.0, so the network ID multiplier is 256 – 248 = 8

The possible subnet IDs are:
10.0.0.0
10.8.0.0
10.16.0.0
10.24.0.0
....
....
10.64.0.0
10.72.0.0
10.80.0.0
10.88.0.0
10.96.0.0 and so on...

As you can see the network 10.72.0.0 is the winner as the IP address of 10.75.20.3 belongs to that particular network IP range.

The IP address range of the network is 10.72.0.0 – 10.79.255.255 (the next address 10.80.0.0 is the next subnet ID)
The broadcast address is the last address of the network so, the broadcast address is **10.79.255.255.**

Question 83. Your task is to find the broadcast address from the IP address 172.30.70.26 with subnet mask 255.255.192.0

(A) Broadcast address: 172.30.127.255

(B) Broadcast address: 172.30.70.255

(C) Broadcast address: 172.30.100.255

(D) Broadcast address: 172.30.87.255

Explanation 83. Broadcast address: 172.30.127.255 is the correct answer. The process of finding the broadcast ID when the mask is neither 255 nor 0 is more complicated. In order to find the broadcast ID you have to find the **network ID multiplier**.

The network ID multiplier can be found once you subtract the

256 – last octet from the mask that is neither 255 nor 0.

The subnet mask is 255.255.192.0, so the network ID multiplier is 256 – 192 = 64

The possible subnet IDs are:
172.30.0.0
172.30.64.0
172.30.128.0
172.30.192.0

In this case, the network 172.30.64.0 is the winner as the IP address of 172.30.70.26 belongs to that particular network IP range.

The IP address range of the network is 172.30.64.0 – 172.30.127.255 (the next address 172.30.128.0 is the next sub-net ID)

The broadcast address is the last address of the network so, the broadcast address is **172.30.127.255**

Question 84. Which of the following answers lists the dotted-decimal notation (DDN) equivalent of /30?
(A) 255.255.255.240

(B) 255.255.255.252

(C) 255.255.192.0

(D) 255.255.252.0

Explanation 84. 255.255.255.252 is the correct answer. /30 is the equivalent of the mask that in binary has 30 binary 1s. To convert that to DDN format, write down all the binary 1s (30 in this case), followed by binary 0s for the remainder of the 32-bit mask. Then take 8 bits at a time and convert from binary to decimal.

Using the /30 mask in this question, the binary mask is **11111111.11111111.11111111.11111100**. Each of the first three octets is all binary 1s, so each converts to 255.

The last octet, 11111100, converts to 252, for a DDN mask of 255.255.255.252.

Question 85. Which of the following answers lists the dotted-decimal notation (DDN) equivalent of /18?

(A) 255.255.255.192

(B) 255.255.224.0

(C) 255.255.128.0

(D) 255.255.192.0

Explanation 85. **255.255.192.0 is the correct answer.** **/18 is the equivalent of the mask that in binary has 18 binary 1s.** To convert that to DDN format, write down all the binary 1s (18 in this case), followed by binary 0s for the remainder of the 32-bit mask. Then take 8 bits at a time and convert from binary to decimal.

Using the /18 mask in this question, the binary mask is **11111111.11111111.11000000.00000000**. Each of the first two octets is all binary 1s, so each converts to 255.

The third octet, 11000000, converts to 252, for a DDN mask of 255.255.192.0.

Question 86. Which of the following masks, when used within a Class B network, would supply enough subnet bits to support 90 subnets? (Choose two)

(A) /24

(B) /21

(C) /19

(D) 255.255.255.252

(E) 255.255.240.0

(F) 255.255.224.0

Explanation 86. **A and D are the correct answers.**

The masks in binary define a number of binary 1s, and the number of binary 1s defines the length of the prefix (network + subnet) part. With a Class B network, the network part is 16 bits.

To support 90 subnets, the subnet part must be at least 7 bits long. Six subnet bits would supply only $2^6 = 64$ subnets, while 7 subnet bits supply $2^7 = 128$ subnets.

The **/24** answer supplies 8 subnet bits, and the **255.255.255.252** answer supplies 14 subnet bits.

Question 87. Which of the following masks, when used within a Class A network, would supply enough subnet bits to support 8 subnets? (Choose two)

(A) /10

(B) /11

(C) /9

(D) /8

Explanation 87. /11 is the correct answer.

The mask in binary define a number of binary 1s, and the number of binary 1s defines the length of the prefix (network + subnet) part.

With a Class A network, the network part is 8 bits.

To support 8 subnets, the subnet part must be at least 3 bits long. Two subnet bits would supply only $2^2 = 4$ subnets, while 3 subnet bits supply $2^3 = 8$ subnets.

The **/11** answer supplies 3 subnet bits.

Question 88. Your task is to troubleshoot a user's PC with IP 10.20.30.5 and mask 255.255.255.0. Based on the given details type the number of the network (N), subnet (S), and host (H) bits.

(A) Network Bits = 16 | Subnet Bits = 15 | Host Bits = 1

(B) Network Bits = 16 | Subnet Bits = 1 | Host Bits = 15

(C) Network Bits = 8 | Subnet Bits = 8 | Host Bits = 16

(D) Network Bits = 8 | Subnet Bits = 16 | Host Bits = 8

Explanation 88. **Network Bits = 8 | Subnet Bits = 16 | Host Bits = 8 is the correct answer.**

The size of the **network part** is always either 8, 16, or 24 bits, based on whether it is Class A, B, or C, respectively.

In this case, we have a Class A address, so the network part is 8bits.

N = 8

The mask 255.255.255.0, converted to prefix format is /24.

The number of subnet bits is the difference between the prefix length(24) and N(8).

S = prefix – N

S = 24 – 8 bits

S = 16

The number of the host bits is the total number of IP address bits(32) which is always 32bits minus the prefix length(28).

H = Adddres bits – prefix

H = 32 – 24

H = 8

Question 89. The converted binary mask 11111111.11111111.11111110.00000000 to decimal is _____.

(A) 255.255.255.192

(B) 255.255.254.0

(C) 255.255.252.0

(D) 255.255.255.224

Explanation 89. 255.255.254.0 is the correct answer.

There are only nine possible values in one octet of a subnet mask as shown in the table below.

Binary Mask Octet	Decimal Equivalent	Number of Binary 1s
0	0	0
10000000	128	1
11000000	192	2
11100000	224	3
11110000	240	4
11111000	248	5
11111100	252	6
11111110	254	7
11111111	255	8

Question 90. Which of the following binary masks is equivalent to the 255.192.0.0 dotted-decimal notation (DDN)?

(A) 11111111.11000000.00000000.00000000

(B) 11111111.11100000.00000000.00000000

(C) 11111111.11110000.00000000.00000000

(D) 11111111.11111000.00000000.00000000

Explanation 90. **11111111.11000000.00000000.00000000 is the correct answer.** There are only nine possible values in one octet of a subnet mask as shown in the table below. So start converting each octet one by one to get the final result.

1. First octet = 255 | **First octet in binary** = 11111111
2. Second octet = 192 | **Second octet in binary** = 11100000
3. Third octet = 0 | **Third octet in binary** = 00000000
4. Forth octet = 0 | **Forth octet in binary** = 00000000

Final result: 11111111. 11100000.00000000.00000000

Binary Mask Octet	Decimal Equivalent	Number of Binary 1s
0	0	0
10000000	128	1
11000000	192	2
11100000	224	3
11110000	240	4
11111000	248	5
11111100	252	6

11111110	254	7
11111111	255	8

CHAPTER 5
IPv4 ROUTING

Questions 91-105

Question 91. You have noticed that a server with IP 145.45.3.2 doesn't respond to requests. What command will you type first in order to test connectivity between your device and the server?

(A) request 145.45.3.2

(B) check 145.45.3.2

(C) ping 145.45.3.2

(D) ping 145.45.3.2

Question 92. A LAN design uses a Layer 3 EtherChannel between two switches SW1 and SW2, with port-channel interface 1 used on both switches. SW1 uses ports G0/1 and G0/2 in the channel. However, only interface G0/1 is bundled into the channel and working. Think about the configuration settings on port G0/2 that could have existed before adding G0/2 to the EtherChannel. Which answers identify a setting that could prevent IOS from adding G0/2 to the Layer 3 EtherChannel? (Choose two answers.)

(A) A different STP cost (spanning-tree cost value)

(B) A different access VLAN (switchport access vlan vlan-id)

(C) A different speed (speed value)

(D) A default setting for switchport (switchport)

Question 93. A network engineer has configured a Layer 3 switch with SVIs for VLANs 4 and 5. Hosts in the subnets using VLANs 4 and 5 can ping each other with the Layer 3 switch routing the packets. The next week, the network engineer receives a call that those same users can no longer ping each other. If the problem is with the Layer 3 switching function, which of the following could have caused the problem? (Choose two answers.)

(A) A shutdown command issued from VLAN 4 configuration mode

(B) VTP on the switch removing VLAN 5 from the switch's VLAN list

(C) 1 out of 10 working VLAN 4 access ports failing due to physical problems

(D) A shutdown command issued from VLAN 6 configuration mode

Question 94. Which of the given commands produces the following output?

Output:

Global values:
Internet Protocol routing is enabled
Embedded-Service-Engine0/0 is administratively down, line protocol is down
GigabitEthernet0/0 is up, line protocol is up
Internet address is 158.16.1.1/24
GigabitEthernet0/1 is administratively down, line protocol is down
Serial0/0/0 is up, line protocol is up
Internet address is 158.16.4.1/24
Serial0/0/1 is administratively down, line protocol is down
GigabitEthernet0/1/0 is up, line protocol is up
Internet address is 158.16.1.1/24

(A) show interfaces
(B) show protocols
(C) show values
(D) show routing

Question 95. Which of the following commands lists the router's entire routing table?

(A) show route
(B) show routing table
(C) show ip route
(D) show route table

Question 96. Which of the following commands lists detailed information about the route 156.10.2.0.

(A) show route 156.10.2.0

(B) show routing table 156.10.2.0

(C) show ip route 156.10.2.0

(D) show route table 156.10.2.0

Question 97. The commands **ping** and **traceroute** send messages in the network to test connectivity and rely on other devices to send back a reply

(A) TRUE

(B) FALSE

Question 98. A router lists the following partial output from the **show ip route** command. Out which interface will the router route packets destined to IP address 180.5.38.122?

10.0.0.0/8 is variably subnetted, 8 subnets, 5 masks

O 180.5.38.100/32 [110/50] via 172.16.25.2, 00:00:04, GigabitEthernet0/0/0

O 180.5.38.64/26 [110/100] via 172.16.25.129, 00:00:09, GigabitEthernet0/1/0

O 180.5.37.0/23 [110/65] via 172.16.24.2, 00:00:04, GigabitEthernet0/2/0

O 180.5.38.96/27 [110/65] via 172.16.24.129, 00:00:09, GigabitEthernet0/3/0
O 0.0.0.0/0 [110/129] via 172.16.25.129, 00:00:09, GigabitEthernet0/0/0

(A) G0/3/0

(B) G0/2/0

(C) G0/1/0

(D) G0/0/0

Question 99. You are connected on a router R1, Which command will you type the command to connect to R2 using SSH.

Login credentials in order to get access to R2.
R2's IP address: 145.167.2.1
username: userexamsdigest
password: passexamsdigest

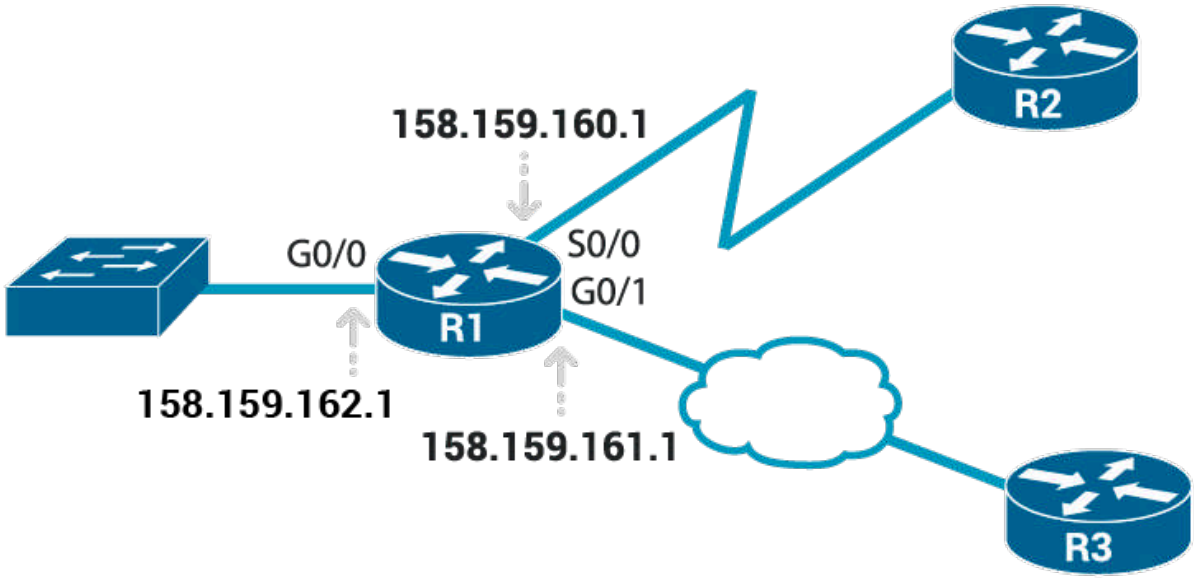
(A) ssh -l userexamsdigest 145.167.2.1 passexamsdigest

(B) ssh -l userexamsdigest 145.167.2.2 passexamsdigest

(C) ssh -l userexams 145.167.2.1 passexamsdigest

(D) ssh -l userexamsdigest 145.167.2.1
examsdigest

Question 100. The senior network engineer of your company, tells you to configure the interfaces of the R1 based on the diagram below. The subnet mask is 255.255.255.0.



(A) R1# configure terminal
R1(config)# interface G0/0
R1(config-if)# ip address 158.159.162.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface G0/1
R1(config-if)# ip address 158.159.161.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface S0/0

R1(config-if)# ip address 158.159.160.1 255.255.255.0
R1(config-if)# no shutdown

(B) R1# configure terminal
R1(config)# interface G0/1
R1(config-if)# ip address 158.159.162.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface G0/0
R1(config-if)# ip address 158.159.161.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface S0/0
R1(config-if)# ip address 158.159.160.1 255.255.255.0
R1(config-if)# no shutdown

(C) R1# configure terminal
R1(config)# interface G0/0
R1(config-if)# ip address 158.159.162.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface G0/1
R1(config-if)# ip address 158.159.161.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface S0/1
R1(config-if)# ip address 158.159.160.1 255.255.255.0
R1(config-if)# no shutdown

(D) R1# configure terminal
R1(config)# interface G0/0
R1(config-if)# ip address 158.159.162.1 255.255.0.0
R1(config-if)# no shutdown
R1(config-if)# interface G0/1
R1(config-if)# ip address 158.159.161.1 255.255.0.0
R1(config-if)# no shutdown
R1(config-if)# interface S0/0
R1(config-if)# ip address 158.159.160.1 255.255.0.0
R1(config-if)# no shutdown

Question 101. You have been tasked to set the router's IPv4 address and mask. What command will you type to complete the task?

(A) ip address [address mask]

(B) interface [address mask]

(C) set ip [address mask]

(D) add address [address mask]

Question 102. You have been tasked to list a single line of information about each interface, including the IP address, line and protocol status, and the method with which the address was configured. What command will you type to complete the task?

(A) show ip protocol brief

(B) show ip addresses brief

(C) show ip interface brief

(D) show ip status brief

Question 103. After configuring a working router interface with IP address/mask 10.1.1.100/26, which of the following routes would you expect to see in the output of the **show ip route** command? (Choose two answers.)

(A) A connected route for subnet 10.1.1.64 255.255.255.192

(B) A local route for host 10.1.1.64 255.255.255.255

(C) A local route for host 10.1.1.100 255.255.255.255

(D) A local route for host 10.1.1.100 255.255.255.192

(E) A connected route for subnet 10.1.1.0 255.255.255.0

Question 104. What command will you type to enable a switch's interface to be a routed interface instead of a switched interface

(A) routed interface

(B) enable interface

(C) no switch interface

(D) no switchport

Question 105. You are responsible to configure a static route for the network 156.187.45.0/24 using the IP address 156.187.80.45 as the next-hop IP. Which command will you

type to meet the requirement?

(A) ip route 156.187.45.0 255.255.0.0 156.187.80.45

(B) ip route 156.187.45.0 255.255.255.0 156.187.80.46

(C) ip route 156.187.0.0 255.255.255.0 156.187.80.45

(D) ip route 156.187.45.0 255.255.255.0 156.187.80.45

Answers 91-105

Question 91. You have noticed that a server with IP 145.45.3.2 doesn't respond to requests. What command will you type first in order to test connectivity between your device and the server?

(A) request 145.45.3.2

(B) check 145.45.3.2

(C) ping 145.45.3.2

(D) ping 145.45.3.2

Explanation 91. **ping 145.45.3.2 is the correct answer.** The command you will type first to test the connectivity between your device and the server is:

The **ping** command tests connectivity by sending packets to an IP address, expecting the device at that address to send packets back.

The **ping** command uses the Internet Control Message Protocol (ICMP), specifically the ICMP echo request and ICMP echo reply messages.

Question 92. A LAN design uses a Layer 3 EtherChannel between two switches SW1 and SW2, with port-channel interface

1 used on both switches. SW1 uses ports G0/1 and G0/2 in the channel. However, only interface G0/1 is bundled into the channel and working. Think about the configuration settings on port G0/2 that could have existed before adding G0/2 to the EtherChannel. Which answers identify a setting that could prevent IOS from adding G0/2 to the Layer 3 EtherChannel? (Choose two answers.)

(A) A different STP cost (spanning-tree cost value)

(B) A different access VLAN (switchport access vlan vlan-id)

(C) A different speed (speed value)

(D) A default setting for switchport (switchport)

Explanation 92. **C and D are the correct answers.** With a Layer 3 EtherChannel, two configuration settings must be the same on all the physical ports, specifically the **speed** and **duplex** as set with the speed and duplex commands. Additionally, the physical ports and port-channel port must all have the **no switchport** command configured to make each act as a routed port.

So, having a different speed setting, or being configured with switchport rather than no switchport, would prevent IOS from adding interface G0/2 to the Layer 3 EtherChannel.

Question 93. A network engineer has configured a Layer 3

switch with SVIs for VLANs 4 and 5. Hosts in the subnets using VLANs 4 and 5 can ping each other with the Layer 3 switch routing the packets. The next week, the network engineer receives a call that those same users can no longer ping each other. If the problem is with the Layer 3 switching function, which of the following could have caused the problem? (Choose two answers.)

(A) A shutdown command issued from VLAN 4 configuration mode

(B) VTP on the switch removing VLAN 5 from the switch's VLAN list

(C) 1 out of 10 working VLAN 4 access ports failing due to physical problems

(D) A shutdown command issued from VLAN 6 configuration mode

Explanation 93. **A and B are the correct answers.** A Layer 3 switch will not route packets on a VLAN interface unless it is in an up/up state.

A VLAN interface will only be up/up if the matching VLAN (with the same VLAN number) **exists on the switch**. If VTP deletes the VLAN, then the VLAN interface moves to a down/down state, and the routing on that interface stop.

Also, disabling VLAN 4 with the **shutdown** command in VLAN

configuration mode also causes the matching VLAN 4 interface to fail, which makes routing on interface VLAN 4 stop as well.

A Layer 3 switch needs only one access port or trunk port forwarding for a VLAN to enable routing for that VLAN, so nine of the ten access ports in VLAN 4 could fail, leaving one working port, and the switch would keep routing for VLAN 4.

A shutdown of VLAN 6 can't affect the VLANs 4 and 5.

Question 94. Which of the given commands produces the following output?

Output:

```
Global values:
Internet Protocol routing is enabled
Embedded-Service-Engine0/0 is administratively down, line protocol is down
GigabitEthernet0/0 is up, line protocol is up
Internet address is 158.16.1.1/24
GigabitEthernet0/1 is administratively down, line protocol is down
Serial0/0/0 is up, line protocol is up
Internet address is 158.16.4.1/24
Serial0/0/1 is administratively down, line protocol is down
```

GigabitEthernet0/1/0 is up, line protocol is up
Internet address is 158.16.1.1/24

(A) show interfaces
(B) show protocols
(C) show values
(D) show routing

Explanation 94. **show protocols is the correct answer.**

Question 95. Which of the following commands lists the router's entire routing table?
(A) show route
(B) show routing table
(C) show ip route
(D) show route table

Explanation 95. **show ip route is the correct answer.**

Question 96. Which of the following commands lists detailed information about the route 156.10.2.0.
(A) show route 156.10.2.0
(B) show routing table 156.10.2.0
(C) show ip route 156.10.2.0
(D) show route table 156.10.2.0

Explanation 96. **show ip route 156.10.2.0 is the correct answer.**

Question 97. The commands **ping** and **traceroute** send messages in the network to test connectivity and rely on other devices to send back a reply

(A) TRUE

(B) FALSE

Explanation 97. **TRUE is the correct answer.** **ping** and **traceroute** commands help network engineers isolate problems. Here is a comparison of the two:

1. Both send messages in the network to test connectivity.
2. Both rely on other devices to send back a reply.
3. Both have wide support on many different operating systems.
4. Both can use a hostname or an IP address to identify the destination.
5. On routers, both have a standard and extended version, allowing better testing of the reverse route.

Question 98. A router lists the following partial output from the **show ip route** command. Out which interface will the router

route packets destined to IP address 180.5.38.122?

10.0.0.0/8 is variably subnetted, 8 subnets, 5 masks

O 180.5.38.100/32 [110/50] via 172.16.25.2, 00:00:04, GigabitEthernet0/0/0
O 180.5.38.64/26 [110/100] via 172.16.25.129, 00:00:09, GigabitEthernet0/1/0
O 180.5.37.0/23 [110/65] via 172.16.24.2, 00:00:04, GigabitEthernet0/2/0
O 180.5.38.96/27 [110/65] via 172.16.24.129, 00:00:09, GigabitEthernet0/3/0
O 0.0.0.0/0 [110/129] via 172.16.25.129, 00:00:09, GigabitEthernet0/0/0

(A) G0/3/0

(B) G0/2/0

(C) G0/1/0

(D) G0/0/0

Explanation 98. G0/3/0 is the correct answer. Destination address 180.5.38.122 matches all the routes listed except the host route to 180.5.38.100/32.

The router will choose the matching route that has the longest prefix length, that is, the prefix-style mask with the highest

number. In this case, that route lists subnet 180.5.38.96 and mask /27, which lists **interface G0/3/0** as the outgoing interface.

Question 99. You are connected on a router R1, Which command will you type the command to connect to R2 using SSH.

Use the following login credentials in order to get access to R2.
R2's IP address: 145.167.2.1
username: userexamsdigest
password: passexamsdigest

(A) ssh -l userexamsdigest 145.167.2.1 passexamsdigest

(B) ssh -l userexamsdigest 145.167.2.2 passexamsdigest

(C) ssh -l userexams 145.167.2.1 passexamsdigest

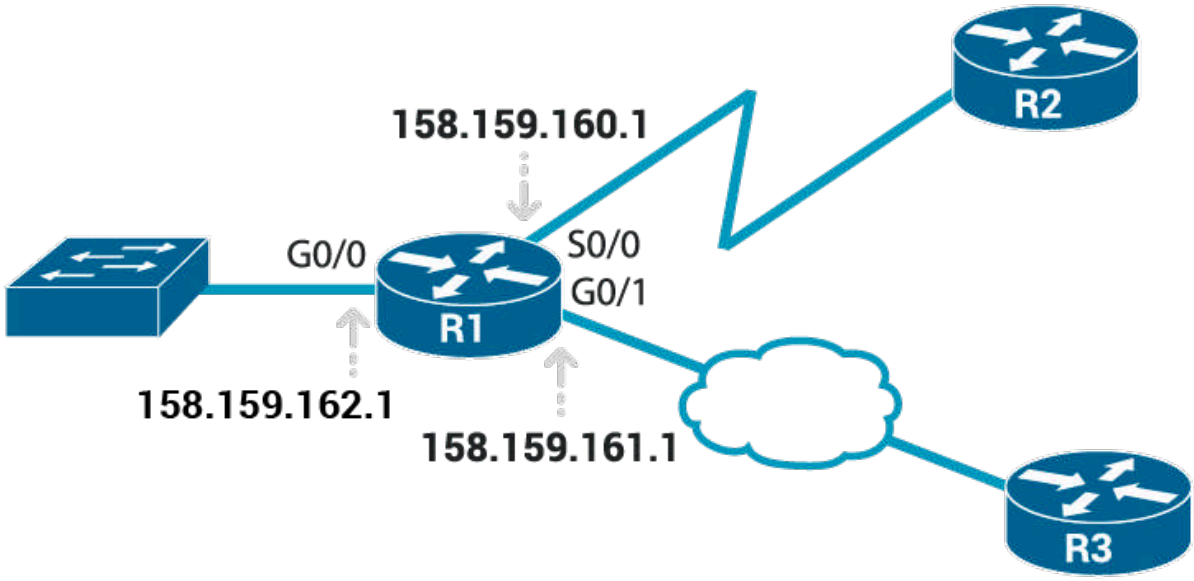
(D) ssh -l userexamsdigest 145.167.2.1 examsdigest

Explanation 99. **A is the correct answer.** The **ssh -l username host** command is used to connect on the R2 using SSH client.

The -l flag means that the next parameter is the login username.

In this case, the user begins logged in to Router R1 and then uses the **ssh -l userexamsdigest 145.167.2.1** command to SSH to Router R2. R2 expects a username/password of userexamsdigest/passexamsdigest, with userexamsdigest supplied in the command and passexamsdigest supplied when R2 prompts the user.

Question 100. The senior network engineer of your company, tells you to configure the interfaces of the R1 based on the diagram below. The subnet mask is 255.255.255.0.



(A) **R1# configure terminal**

R1(config)# interface G0/0

R1(config-if)# ip address 158.159.162.1 255.255.255.0

R1(config-if)# no shutdown

R1(config-if)# interface G0/1

R1(config-if)# ip address 158.159.161.1 255.255.255.0

R1(config-if)# no shutdown

R1(config-if)# interface S0/0

R1(config-if)# ip address 158.159.160.1 255.255.255.0

R1(config-if)# no shutdown

(B) R1# configure terminal

R1(config)# interface G0/1

R1(config-if)# ip address 158.159.162.1 255.255.255.0

R1(config-if)# no shutdown

R1(config-if)# interface G0/0

R1(config-if)# ip address 158.159.161.1 255.255.255.0

R1(config-if)# no shutdown

R1(config-if)# interface S0/0

R1(config-if)# ip address 158.159.160.1 255.255.255.0

R1(config-if)# no shutdown

(C)
```
R1# configure terminal
R1(config)# interface G0/0
R1(config-if)# ip address 158.159.162.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface G0/1
R1(config-if)# ip address 158.159.161.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface S0/1
R1(config-if)# ip address 158.159.160.1 255.255.255.0
R1(config-if)# no shutdown
```

(D)
```
R1# configure terminal
R1(config)# interface G0/0
R1(config-if)# ip address 158.159.162.1 255.255.0.0
R1(config-if)# no shutdown
R1(config-if)# interface G0/1
R1(config-if)# ip address 158.159.161.1 255.255.0.0
R1(config-if)# no shutdown
R1(config-if)# interface S0/0
R1(config-if)# ip address 158.159.160.1 255.255.0.0
R1(config-if)# no shutdown
```

Explanation 100. **A is the correct answer.**

```
R1# configure terminal
```

```
R1(config)# interface G0/0
R1(config-if)# ip address 158.159.162.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface G0/1
R1(config-if)# ip address 158.159.161.1 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# interface S0/0
R1(config-if)# ip address 158.159.160.1 255.255.255.0
R1(config-if)# no shutdown
```

Question 101. You have been tasked to set the router's IPv4 address and mask. What command will you type to complete the task?

(A) ip address [address mask]

(B) interface [address mask]

(C) set ip [address mask]

(D) add address [address mask]

Explanation 101. **ip address [address mask] is the correct answer.**

Question 102. You have been tasked to list a single line of information about each interface, including the IP address, line and protocol status, and the method with which the address was configured. What command will you type to complete the

task?

(A) show ip protocol brief

(B) show ip addresses brief

(C) show ip interface brief

(D) show ip status brief

Explanation 102. **show ip interface brief is the correct answer.**

Question 103. After configuring a working router interface with IP address/mask 10.1.1.100/26, which of the following routes would you expect to see in the output of the **show ip route** command? (Choose two answers.)

(A) A connected route for subnet 10.1.1.64 255.255.255.192

(B) A local route for host 10.1.1.64 255.255.255.255

(C) A local route for host 10.1.1.100 255.255.255.255

(D) A local route for host 10.1.1.100 255.255.255.192

(E) A connected route for subnet 10.1.1.0 255.255.255.0

Explanation 103. **A and C are the correct answers.** First, for the subnetting math, **address 10.1.1.100 with mask /26** implies a subnet ID of **10.1.1.64**. Also, mask /26 converts to a DDN mask of 255.255.255.192. For any working router interface, after adding the **ip address** command to configure an

address and mask, the router adds a connected route for the subnet.

In this case, the router adds a connected route for subnet **10.1.1.64 255.255.255.192**. The router also adds a route called a local route, which is a route for the interface IP address with a 255.255.255.255 mask. In this case, the router adds a local route for address **10.1.1.100 with mask 255.255.255.255.**

Question 104. What command will you type to enable a switch's interface to be a routed interface instead of a switched interface

(A) routed interface

(B) enable interface

(C) no switch interface

(D) no switchport

Explanation 104. no switchport is the correct answer. Enabling a switch interface to be a routed interface instead of a switched interface just use the **no switchport** subcommand on the physical interface.

The switchport tells the switch to treat the port like it is a port on a switch that is, a Layer 2 port on a switch.

To make the port stop acting like a switch port and instead act like a router port, use the no switchport command on the interface.

Question 105. You are responsible to configure a static route for the network 156.187.45.0/24 using the IP address 156.187.80.45 as the next-hop IP. Which command will you type to meet the requirement?

(A) ip route 156.187.45.0 255.255.0.0 156.187.80.45

(B) ip route 156.187.45.0 255.255.255.0 156.187.80.46

(C) ip route 156.187.0.0 255.255.255.0 156.187.80.45

(D) ip route 156.187.45.0 255.255.255.0 156.187.80.45

Explanation 105. **D is the correct answer.** The **correct syntax** lists a subnet number, then a subnet mask in dotted-decimal form, and then either an outgoing interface or a next-hop IP address.

The command to configure a static route for the network 156.187.45.0/24 using the IP address 156.187.80.45 as the next-hop IP is:

ip route 156.187.45.0 255.255.255.0 156.187.80.45

CHAPTER 5
OSPF ROUTING PROTOCOL

Questions 106-120

Question 106. The senior network engineer typed the following commands on the R1.

```
R1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# interface g0/0/0
R1(config-if)# ip ospf cost 6
R1(config-if)# interface g0/1/0
R1(config-if)# ip ospf cost 7
R1(config-if)# ^Z
```

What command will you type in order to confirm the OSPF interface costs?

(A) show ip ospf

(B) show ip ospf interface brief

(C) show ospf brief

(D) show ospf interface brief

Question 107. Per the command output, with how many

routers is router R4 full adjacent over its Gi0/1 interface?

R4# show ip ospf interface brief

```
Interface    PID Area      IP Address/Mask     Cost State Nbrs F/C
Gi0/1         1   0           23.2.2.1/24        1    DROTH 2/5
```

(A) 1

(B) 5

(C) 2

(D) 0

Question 108. You have been tasked to list the OSPF neighbors off interface serial 0/1. Which command will you type to complete the task?

(A) show ip ospf neighbor serial 0/1

(B) show ip ospf neighbor serial 1/0

(C) show ip ospf neighbor fastethernet 0/1

(D) show ip ospf serial 0/1

Question 109. The routing protocol that was designed and intended for use between different autonomous systems is called _____.

(A) interior gateway protocol

(B) different gateway protocol

(C) autonomous gateway protocol

(D) exterior gateway protocol

Question 110. Given the following OSPF network commands, type the wildcard masks to match the requirement.

Requirement: Match addresses that begin with 110.20
Command: network 110.20.0.0 {wildcard mask}

Which of the following wildcard mask will you use to meet the requirement?

(A) 0.0.255.255
(B) 0.0.0.255
(C) 0.255.255.255
(D) 0.0.0.0

Question 111. Which of the following commands produces the output below?

```
Codes: L – local, C – connected, S – static, R – RIP, M – mobile,
B – BGP
D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external
type 2
E1 – OSPF external type 1, E2 – OSPF external type 2

! Additional lines omitted for brevity

Gateway of last resort is not set
```

10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O 10.1.1.0/24 [110/2] via 10.1.14.1, 00:19:24, GigabitEthernet0/0/0
O 10.1.2.0/24 [110/2] via 10.1.14.1, 00:19:24, GigabitEthernet0/0/0
C 10.1.4.0/24 is directly connected, Vlan3
L 10.1.4.4/32 is directly connected, Vlan3
O 10.1.12.0/24 [110/2] via 10.1.14.1, 00:17:24, GigabitEthernet0/0/0
O 10.1.13.0/24 [110/2] via 10.1.14.1, 00:14:15, GigabitEthernet0/0/0
C 10.1.14.0/24 is directly connected, GigabitEthernet0/0/0
L 10.1.14.4/32 is directly connected, GigabitEthernet0/0/0
O 10.1.23.0/24 [110/3] via 10.1.14.1, 00:15:35, GigabitEthernet0/0/0

(A) show ip codes
(B) show ip route
(C) show ip interfaces
(D) show ip connected

Question 112. Routing protocol is a set of rules, and algorithms used by routers for the overall purpose of learning routes. This process includes the exchange and analysis of routing information.
(A) TRUE
(B) FALSE

Question 113. Routed protocol is a protocol that defines a packet structure and logical addressing, allowing routers to

forward or route the packets.

(A) TRUE

(B) FALSE

Question 114. Which of the following network commands following the command **router ospf 1**, tells the router to start using OSPF on interfaces whose IP addresses are **20.1.20.1, 20.1.30.1, and 20.1.40.1**?

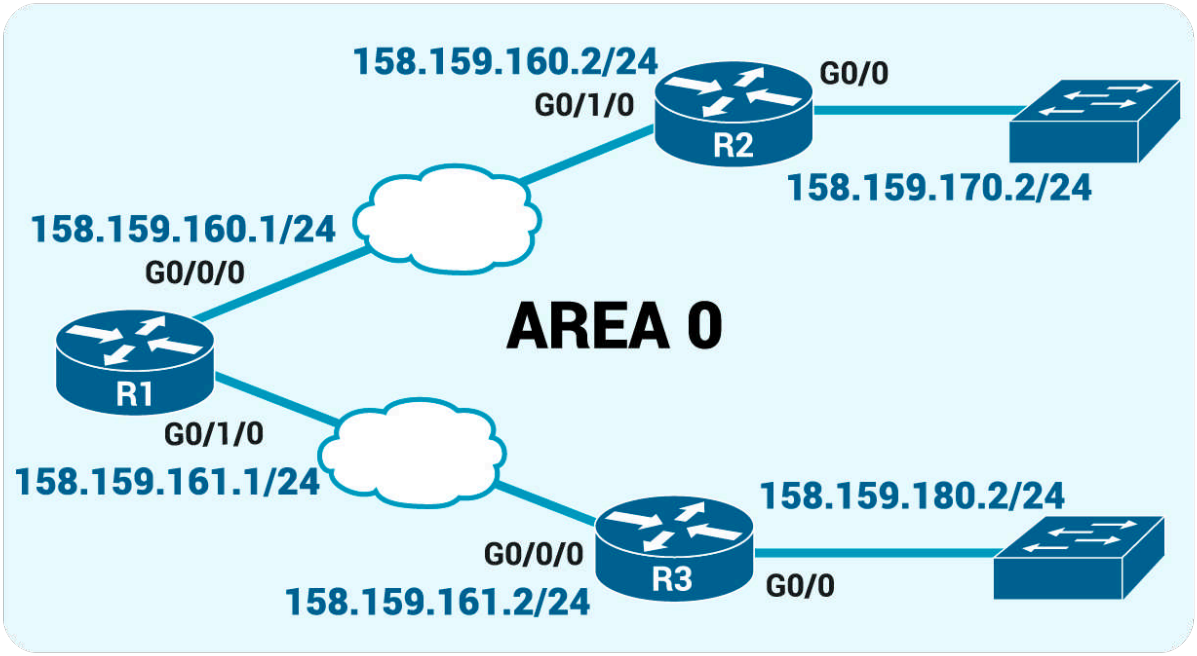
(A) network 20.0.0.1 0.0.255.255 area 0

(B) network 20.0.0.1 0.0.0.255 area 0

(C) network 20.0.0.0 255.0.0.0 area 0

(D) network 20.0.0.0 0.255.255.255 area 0

Question 115. The network designer provides the following network diagram for OSPF Single-Area to start the configuration process.



Based on the diagram, configure the R2 following the details below.

1. Enable OSPF process 2
2. Enable OSPF on all interfaces with a single command

(A) R2# router ospf 3
R2# network 0.0.0.0 255.255.255.255 area 0
R2# interface GigabitEthernet0/0
R2(config-if)# ip address 158.159.170.2 255.255.255.0
R2# interface GigabitEthernet0/1/0
R2(config-if)# ip address 158.159.160.2 255.255.255.0

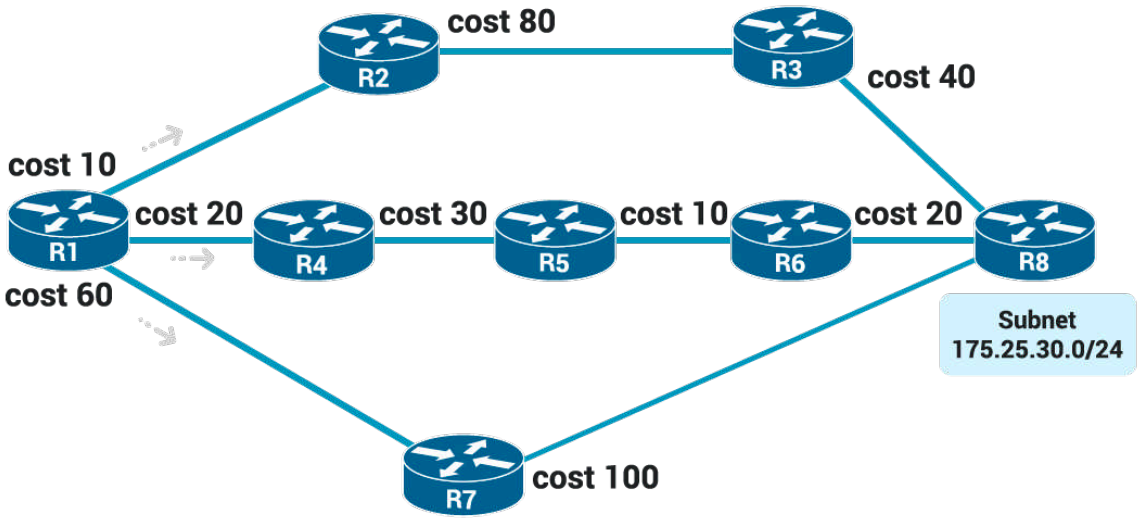
(B) R2# router ospf 2
R2# network 0.0.0.0 255.255.255.255 area 0
R2# interface GigabitEthernet0/0
R2(config-if)# ip address 158.159.170.2 255.255.255.0
R2# interface GigabitEthernet0/1/0
R2(config-if)# ip address 158.159.160.2 255.255.255.0

(C) R2# router ospf 2
R2# network 0.0.0.0 255.255.255.255 area 0
R2# interface GigabitEthernet0/0
R2(config-if)# ip address 158.159.170.2 255.255.0.0
R2# interface GigabitEthernet0/1/0
R2(config-if)# ip address 158.159.160.2 255.255.0.0

(D) R2# router ospf 2
R2# network 0.0.0.0 255.255.255.255 area 1

```
R2# interface GigabitEthernet0/0
R2(config-if)# ip address 158.159.170.2 255.255.255.0
R2# interface GigabitEthernet0/1/0
R2(config-if)# ip address 158.159.160.2 255.255.255.0
```

Question 116. Given the following OSPF network diagram, what router will be added to R1's routing table as a next-hop?



(A) R2
(B) R4
(C) R7
(D) R5

Question 117. You have been task to list the interfaces on which the OSPF protocol is enabled. Which of the following command will you type?

(A) show ip ospf brief
(B) show ip ospf interface brief

(C) show ip interface brief
(D) show ospf interface brief

Question 118. A network engineer connects routers R5 and R6 to the same Ethernet LAN and configures them to use OSPFv2. Which answers describe a combination of settings that would prevent the two routers from becoming OSPF neighbors?
(A) Both routers' interface IP addresses are in the same subnet
(B) Both routers' OSPF process uses process ID 3
(C) Both routers' OSPF process uses router ID 42.42.42.42
(D) Both routers' interfaces use an OSPF Dead interval of 80

Question 119. Which of the following terms described as an OSPF router with interfaces connected to the backbone area and to at least one other area?
(A) Backbone area
(B) Internal router
(C) Backbone router
(D) Area Border Router

Question 120. Which of the following route types has 110 as default Administrative Distance (AD)?
(A) IGRP
(B) OSPF
(C) RIP
(D) IS-IS

Answers 106-120

Question 106. The senior network engineer typed the following commands on the R1.

```
R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface g0/0/0
R1(config-if)#ip ospf cost 6
R1(config-if)#interface g0/1/0
R1(config-if)#ip ospf cost 7
R1(config-if)#^Z
```

What command will you type in order to confirm the OSPF interface costs?

(A) show ip ospf

(B) show ip ospf interface brief

(C) show ospf brief

(D) show ospf interface brief

Explanation 106. **show ip ospf interface brief is the correct answer.** The command **show ip ospf interface** lists the interfaces on which the OSPF protocol is enabled and lists the cost settings.

Question 107. Per the command output, with how many routers is router R4 full adjacent over its Gi0/1 interface?

```
Interface    PID Area       IP Address/Mask     Cost State Nbrs F/C
Gi0/1          1   0           23.2.2.1/24         1    DROTH 2/5
```

R4# show ip ospf interface brief

(A) 1

(B) 5

(C) 2

(D) 0

Explanation 107. **2 is the correct answer.** The show ip ospf interface brief command lists a pair of counters under the heading 'Nbrs F/C'.

The first of the two numbers represents **the number of fully adjacent neighbors** (2 full adjacent neighbors in this case), and the second number represents **the total number of neighbors**.

Question 108. You have been tasked to list the OSPF neighbors off interface serial 1/0. Which command will you type to complete the task?

(A) show ip ospf neighbor serial 0/1

(B) show ip ospf neighbor serial 1/0

(C) show ip ospf neighbor fastethernet 0/1

(D) show ip ospf serial 0/1

Explanation 108. **show ip ospf neighbor serial 1/0 is the correct answer.** There are **two commands** that can list the OSPF neighbors off interface serial 1/0:

1. show ip ospf neighbor serial 1/0

2. show ip ospf neighbor

Question 109. The routing protocol that was designed and intended for use between different autonomous systems is called _____.

(A) interior gateway protocol
(B) different gateway protocol
(C) autonomous gateway protocol
(D) exterior gateway protocol

Explanation 109. **exterior gateway protocol is the correct answer.** **Exterior Gateway Protocol (EGP)** is a protocol for exchanging routing information between two neighbor gateway hosts (each with its own router) in a network of autonomous systems.

EGP is commonly used between hosts on the Internet to exchange routing table information. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen.

Question 110. Given the following OSPF network commands, type the wildcard masks to match the requirement.

Requirement: Match addresses that begin with 110.20
Command: network 110.20.0.0 {wildcard mask}

Which of the following wildcard mask will you use to meet the requirement?

(A) 0.0.255.255
(B) 0.0.0.255
(C) 0.255.255.255
(D) 0.0.0.0

Explanation 110. 0.0.255.255 is the correct answer. The command should be **network 110.20.0.0 0.0.255.255.**

Question 111. Which of the following commands produces the output below?

```
Codes: L – local, C – connected, S – static, R – RIP, M – mobile,
B – BGP
D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area
N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external
type 2
E1 – OSPF external type 1, E2 – OSPF external type 2

! Additional lines omitted for brevity

Gateway of last resort is not set
10.0.0.0/8 is variably subnetted, 9 subnets, 2 masks
O 10.1.1.0/24 [110/2] via 10.1.14.1, 00:19:24,
GigabitEthernet0/0/0
O 10.1.2.0/24 [110/2] via 10.1.14.1, 00:19:24,
GigabitEthernet0/0/0
C 10.1.4.0/24 is directly connected, Vlan3
L 10.1.4.4/32 is directly connected, Vlan3
O 10.1.12.0/24 [110/2] via 10.1.14.1, 00:17:24,
GigabitEthernet0/0/0
```

```
O 10.1.13.0/24 [110/2] via 10.1.14.1, 00:14:15,
GigabitEthernet0/0/0
C 10.1.14.0/24 is directly connected, GigabitEthernet0/0/0
L 10.1.14.4/32 is directly connected, GigabitEthernet0/0/0
O 10.1.23.0/24 [110/3] via 10.1.14.1, 00:15:35,
GigabitEthernet0/0/0
```

(A) show ip codes
(B) show ip route
(C) show ip interfaces
(D) show ip connected

Explanation 111. show ip route is the correct answer.

Question 112. Routing protocol is a set of rules, and algorithms used by routers for the overall purpose of learning routes. This process includes the exchange and analysis of routing information.
(A) TRUE
(B) FALSE

Explanation 112. TRUE is the correct answer. Routing protocol is a set of rules, and algorithms used by routers for the overall purpose of learning routes.

This process includes the exchange and analysis of routing information. Each router chooses the best route to each subnet (path selection) and finally places those best routes in its IP routing table. **Examples include RIP, EIGRP, OSPF, and BGP.**

Question 113. Routed protocol is a protocol that defines a packet structure and logical addressing, allowing routers to forward or route the packets.

(A) TRUE

(B) FALSE

Explanation 113. TRUE is the correct answer. Routed protocol is a protocol that defines a packet structure and logical addressing, allowing routers to forward or route the packets. Routers forward packets defined by routed and routable protocols. **Examples include IP Version 4 (IPv4) and IP Version 6 (IPv6).**

Question 114. Which of the following network commands following the command **router ospf 1**, tells the router to start using OSPF on interfaces whose IP addresses are **20.1.20.1, 20.1.30.1, and 20.1.40.1**?

(A) network 20.0.0.1 0.0.255.255 area 0

(B) network 20.0.0.1 0.0.0.255 area 0

(C) network 20.0.0.0 255.0.0.0 area 0

(D) network 20.0.0.0 0.255.255.255 area 0

Explanation 114. network 20.0.0.0 0.255.255.255 area 0 is the correct answer.

The network command **network 20.0.0.0 0.255.255.255 area 0** matches all interfaces whose first octet is 20.

The network command **network 20.0.0.0 255.0.0.0 area 0** means all addresses that end with 0.0.0 (wildcard mask 255.0.0.0). **In this case, is a wrong answer.**

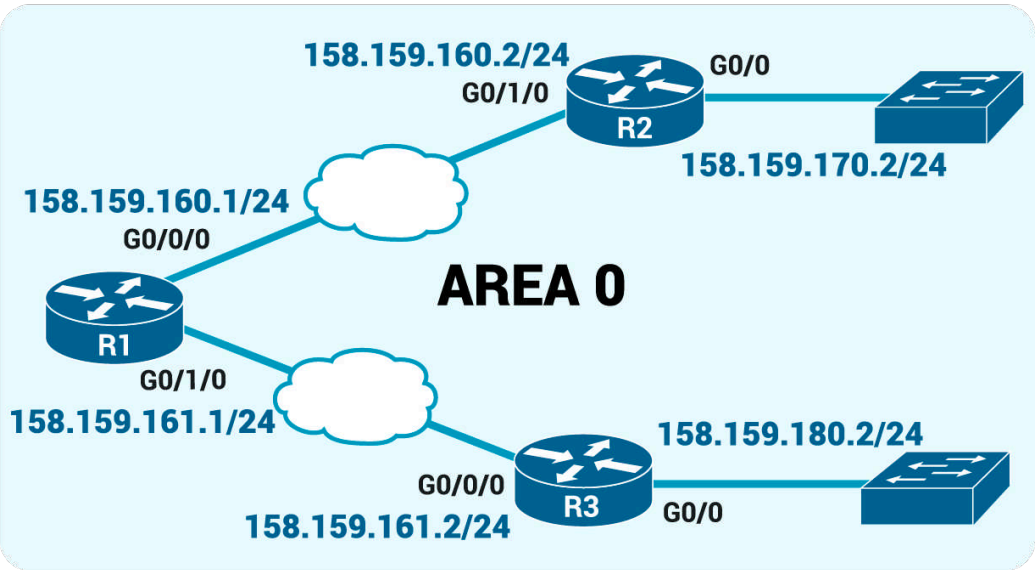
The network command **network 20.0.0.1 0.0.0.255 area 0** means all addresses that begin with 20.0.0 (wildcard mask 0.0.0.255). **In this case, is a wrong answer.**

The network command network 20.0.0.1 0.0.255.255 area 0 means all addresses that begin with 20.0 (wildcard mask 0.0.255.255). **In this case, is a wrong answer.**

Question 115. The network designer provides the following network diagram for OSPF Single-Area to start the configuration process.

Based on the diagram, configure the R2 following the details below.

1. Enable OSPF process 2
2. Enable OSPF on all interfaces with a single command



(A) R2# router ospf 3
R2# network 0.0.0.0 255.255.255.255 area 0
R2# interface GigabitEthernet0/0
R2(config-if)# ip address 158.159.170.2 255.255.255.0
R2# interface GigabitEthernet0/1/0
R2(config-if)# ip address 158.159.160.2 255.255.255.0

(B) R2# router ospf 2
R2# network 0.0.0.0 255.255.255.255 area 0
R2# interface GigabitEthernet0/0
R2(config-if)# ip address 158.159.170.2 255.255.255.0
R2# interface GigabitEthernet0/1/0
R2(config-if)# ip address 158.159.160.2 255.255.255.0

(C) R2# router ospf 2
R2# network 0.0.0.0 255.255.255.255 area 0
R2# interface GigabitEthernet0/0
R2(config-if)# ip address 158.159.170.2 255.255.0.0
R2# interface GigabitEthernet0/1/0
R2(config-if)# ip address 158.159.160.2 255.255.0.0

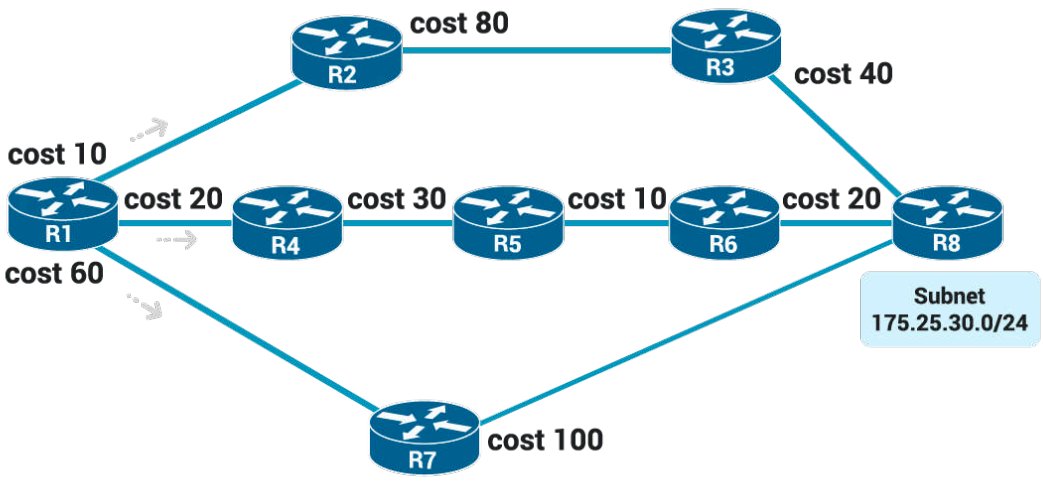
(D) R2# router ospf 2
R2# network 0.0.0.0 255.255.255.255 area 1
R2# interface GigabitEthernet0/0
R2(config-if)# ip address 158.159.170.2 255.255.255.0
R2# interface GigabitEthernet0/1/0

R2(config-if)# ip address 158.159.160.2 255.255.255.0

Explanation 115. **B is the correct answer.**

The answer A is incorrect as it has router ospf 3.
The answer C is incorrect as it has wrong subnet mask on the interfaces.
The answer C is incorrect as it has wrong area.

Question 116. Given the following OSPF network diagram, what router will be added to R1's routing table as a next-hop?



(A) R2
(B) R4
(C) R7
(D) R5

Explanation 116. **R4 is the correct answer.** The **SPF algorithm** calculates all the routes for a subnet—that is, all possible

routes from the router (R1) to the destination subnet (R8). If more than one route exists, the router compares the metrics, picking **the best (lowest) metric route** to add to the routing table.

Once SPF has identified a route, OSPF calculates the metric based on the sum of the OSPF interface costs for all outgoing interfaces in the route.

The three possible routes to 175.25.30.0/24 are:
Route 1: R1-R2-R3-R8
Cost: 10 + 80 + 40 = 130

Route 2: R1-R4-R5-R6-R8
Cost: 20 + 30 + 10 + 20 = 80

Route 3: R1-R7-R8
Cost: 60 + 100 = 160

As a result of the SPF algorithm's analysis of the LSDB, R1 adds a route to subnet 175.25.30.0/24 to its routing table, with the next-hop router of R4.

Question 117. You have been task to list the interfaces on which the OSPF protocol is enabled. Which of the following command will you type?
(A) show ip ospf brief
(B) show ip ospf interface brief
(C) show ip interface brief
(D) show ospf interface brief

Explanation 117. **show ip ospf interface brief is the correct answer.** The command **show ip ospf interface brief** lists the interfaces on which the OSPF protocol is enabled (based on the network commands), including passive interfaces.

Question 118. A network engineer connects routers R5 and R6 to the same Ethernet LAN and configures them to use OSPFv2. Which answers describe a combination of settings that would prevent the two routers from becoming OSPF neighbors?

(A) Both routers' interface IP addresses are in the same subnet

(B) Both routers' OSPF process uses process ID 3

(C) Both routers' OSPF process uses router ID 42.42.42.42

(D) Both routers' interfaces use an OSPF Dead interval of 80

Explanation 118. **Both routers' OSPF process uses router ID 42.42.42.42 is the correct answer.** The use of an identical OSPF router ID (RID) on the two routers prevents them from becoming neighbors.

Both routers must have the same Dead interval, so both using a Dead interval of 80 causes no issues.

The two routers can use any OSPF process ID either the same or a different value, making that answer incorrect.

Finally, the two routers' IP addresses must be in the same subnet, so again that scenario does not prevent R5 and R6 from becoming neighbors.

Question 119. Which of the following terms described as an OSPF router with interfaces connected to the backbone area and to at least one other area?

(A) Backbone area

(B) Internal router

(C) Backbone router

(D) Area Border Router

Explanation 119. Area Border Router is the correct answer. You should be familiar with the following terms for the CCNA 200-301

Area Border Router (ABR) – An OSPF router with interfaces connected to the backbone area and to at least one other area.
Backbone router – A router connected to the backbone area (includes ABRs).
Internal router – A router in one area (not the backbone area)
Area – A set of routers and links that shares the same detailed LSDB information, but not with routers in other areas, for better efficiency.
Backbone area – A special OSPF area to which all other areas must connect—area 0.
Intra-area route – A route to a subnet inside the same area as the router.
Interarea route – A route to a subnet in an area of which the router is not a part.

Question 120. Which of the following route types has 110 as default Administrative Distance (AD)?

(A) IGRP
(B) OSPF
(C) RIP
(D) IS-IS

Explanation 120. OSPF is the correct answer.
Administrative distance is the feature that routers use in order to select the best path when there are at least two different routes to the same destination from two different routing protocols.

Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) with the help of an administrative distance value.

The default Administrative Distances (AD) from the given route types are:

Route type	Administrative
Connected	0
Static	1
BGP (external routes [eBGP])	20
EIGRP (internal routes)	90
IGRP	100

OSPF	110
IS-IS	115
RIP	120
EIGRP (external routes)	170
BGP (internal routes [iBGP])	200
DHCP default route	254
Unusable	250

CHAPTER 6
IP VERSION 6

Questions 121-136

Question 121. Which of the following addresses is the unabbreviated version of IPv6 address 8002:AA3::100:30?

(A) 8002:0AA3:0000:0000:0000:0000:0100:0030

(B) 8002:0DAA3::0100:0030

(C) 8002:0AA3:0:0:0:0:0100:0030

(D) 82:AA3:0:0:0:0:1:3

Question 122. Which of the following IPv6 addresses appears to be a unique local unicast address? (Choose two)

(A) 1234:5:6:7::8

(B) FE80::1234:56FF:FF00:1234

(C) FDAD::2

(D) FF00::1

(E) FDBB::2

(F) FF80::1234

Question 123. You have been tasked to find the shortest valid abbreviation address for 5000:0400:0030:0006:

8000:0800:0010:0002.

(A) 5000:400:30:6:8000:800:10:0002

(B) 5000:400:30:6:8000:800:10:2

(C) 5000:0400:30:6:8000:800:10:2

(D) 5:4:3:6:8:8:1:2

Question 124. Given the following IPv6 address 2340:0000:0010:0100:1000:ABCD:0101:1010. Which of the following is the the abbreviated form?

(A) 2340:0:10:100:1:ABCD:11:1010

(B) 2340:0:10:100:1:ABCD:101:11

(C) 234:0:10:100:1:ABCD:101:1010

(D) 2340:0:10:100:1:ABCD:101:1010

Question 125. Given the following IPv6 address 1230::. Which of the following is the the unabbreviated form?

(A) 1230:0000:0000:0000:0000:0000:0000:0000

(B) 1230:0000:0000:0000:0000:0000:0000

(C) 1230:0000:0000:0000:0000:0000

(D) 1230:0000::0000::0000:0000:0000

Question 126. You have been tasked to give the router's G0/1 interface a unicast IPv6 address of 2005:1:2:3:4:5:6:A, with a /64 prefix length. What command will you type to mark the task as done?

(A) ipv6 address 2005:1:2:3:4:5:5:A/64

(B) ipv6 address 2005:1:2:3:4:5:6:A/46

(C) ipv4 address 2005:1:2:3:4:5:6:A/64

(D) ipv6 address 2005:1:2:3:4:5:6:A/64

Question 127. Which of the following is the prefix for address 1000:0000:0000:0001:0000:0000:0000:0000, assuming a mask of /64?

(A) 1000::1:10:0:0:0/64

(B) 1000:0:0:1::/64

(C) 2000:0:0:1::/64

(D) 1000::1::/64

Question 128. End-user hosts need to know the IPv6 address of a default router, to which the host sends IPv6 packets if the host is in a different subnet.

(A) TRUE

(B) FALSE

Question 129. Which of the following commands will you type to enable IPv6 routing on the router?

(A) ipv6 enable-routing

(B) ipv6 unicast-routing

(C) ipv6 on-routing

(D) ipv6 open-routing

Question 130. Which of the following commands will you type to configure the interface with ipv6 address 2002:1:2:3::4/64?

(A) ipv6 address 2002:1:1:2:3::4/64

(B) ipv6 address 2002:1:2:3::4

(C) ipv6 address 2002:1:2:3::4/64

(D) ipv6 address 2002:1:2:4::4/64

Question 131. One of the following multicast addresses is defined as the address for sending packets to only the IPv6 routers on the local link.

(A) FF02::1

(B) FF02::2

(C) FF02::5

(D) FF02::A

Question 132. PC1, PC2, and Router R1 all connect to the same VLAN and IPv6 subnet. PC1 wants to send its first IPv6 packet to PC2. What protocol or message will PC1 use to discover the MAC address to which PC1 should send the Ethernet frame that encapsulates this IPv6 packet?

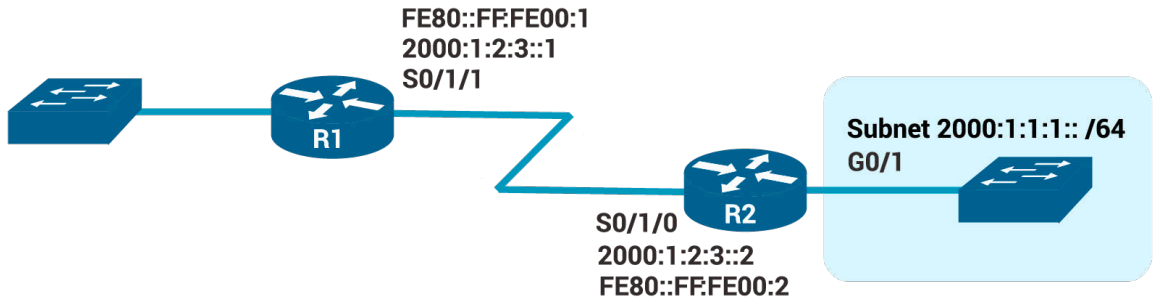
(A) NDP NS

(B) NAT

(C) DHCP

(D) ARP

Question 133. The router R2 has been configured with the ipv6 address 2000:1:1:1::1/64 command on its G0/1 interface as shown in the figure. The router creates a link-local address of FE80::FF:FE00:11 as well. The interface is working. Which of the following routes will the router add to its IPv6 routing table? (Choose two answers.)



(A) A route for FE80::FF:FE00:11/128

(B) A route for FE80::FF:FE00:11/64

(C) A route for 2000:1:1:1::1/128

(D) A route for 2000:1:1:1::/64

(E) A route for 2000:1:2:3::2/128

Question 134. Router R2 has an interface named Gigabit Ethernet 0/2, whose MAC address has been set to 5555.4444.3333. This interface has been configured with the

ipv6 address 7000:1:1:1::/64 eui-64 subcommand. What unicast address will this interface use?

(A) 7000:1:1:1:55FF:FE55:4444:3333

(B) 7000:1:1:1:5755:44FF:FE44:3333

(C) 7000:1:1:1:5555:4444:33FF:FE33

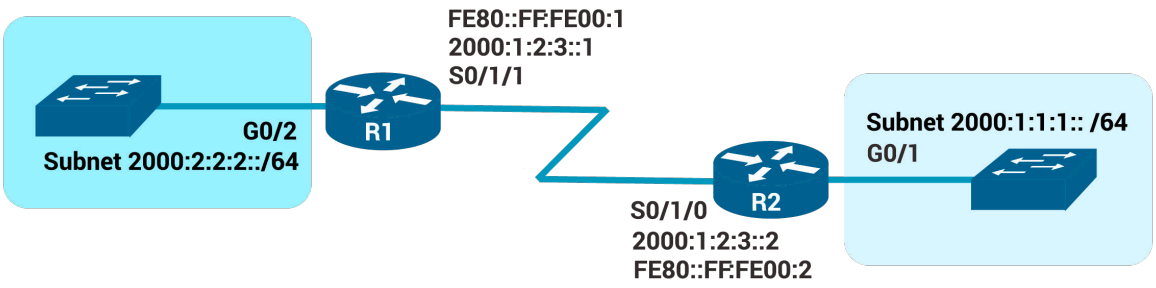
(D) 7000:1:1:1:200:FF:FE00:0

Question 135. The **show ipv6 interface brief** command gives you interface IPv6 address info, and prefix length info.

(A) TRUE

(B) FALSE

Question 136. You are responsible to configure a static route on R1's outgoing interface, in order to support traffic between the subnets. R2 is already configured. Which of the following commands will you type to configure a static route on R1's outgoing interface?



(A) ipv6 route 2000:1:1:1::/64 s0/1/1

(B) ipv6 route 2000:2:2:2::/64 s0/1/1

(C) ipv6 route 2000:1:2:3::/64 s0/1/1

(D) ipv6 route 2000:1:1:1::/64 g0/2

Answers 121-136

Question 121. Which of the following addresses is the unabbreviated version of IPv6 address 8002:AA3::100:30?

(A) 8002:0AA3:0000:0000:0000:0000:0100:0030

(B) 8002:0DAA3::0100:0030

(C) 8002:0AA3:0:0:0:0:0100:0030

(D) 82:AA3:0:0:0:0:1:3

Explanation 121.

8002:0AA3:0000:0000:0000:0000:0100:0030 is the correct answer. The unabbreviated version of an IPv6 address must have 32 digits, and only one answer has 32 hex digits.

In this case, the original number shows **four quartets (sets of four hex digits)** and a ::.

So, the :: was replaced with four quartets of 0000, making the number have eight quartets. Then, for each quartet with fewer than four digits, leading 0s were added so that each quartet has four hex digits.

Question 122. Which of the following IPv6 addresses appears to be a unique local unicast address? (Choose two)

(A) 1234:5:6:7::8

(B) FE80::1234:56FF:FF00:1234

(C) FDAD::2

(D) FF00::1

(E) FDBB::2

(F) FF80::1234

Explanation 122. **C and E are the correct answers.** **Unique local IPv6 addresses** have a similar function as IPv4 private addresses. They are not allocated by an address registry and are not meant to be routed outside their domain. Unique local IPv6 addresses begin with FD00::/8.

A unique local IPv6 address is constructed by appending a randomly-generated 40-bit hexadecimal string to the FD00::/8 prefix. The subnet field and interface ID are created in the same way as with global IPv6 addresses.

Unique local addresses begin with FD in the first two digits. **So, the correct answers are:**

1. FDAD::2

2. FDBB::2

Question 123. You have been tasked to find the shortest valid abbreviation address for 5000:0400:0030:0006:

8000:0800:0010:0002.

(A) 5000:400:30:6:8000:800:10:0002

(B) 5000:400:30:6:8000:800:10:2

(C) 5000:0400:30:6:8000:800:10:2

(D) 5:4:3:6:8:8:1:2

Explanation 123. 5000:0400:30:6:8000:800:10:2 is the correct answer. To abbreviate IPv6 addresses, only leading 0s in a quartet (one set of four hex digits) should be removed. Many of the quartets have trailing 0s (0s on the right side of the quartet), so make sure to **not** remove those 0s.

Question 124. Given the following IPv6 address 2340:0000:0010:0100:1000:ABCD:0101:1010. Which of the following is the the abbreviated form?

(A) 2340:0:10:100:1:ABCD:11:1010

(B) 2340:0:10:100:1:ABCD:101:11

(C) 234:0:10:100:1:ABCD:101:1010

(D) 2340:0:10:100:1:ABCD:101:1010

Explanation 124. 2340:0:10:100:1:ABCD:101:1010 is the correct answer. To **abbreviate** IPv6 addresses, only leading 0s in a quartet (one set of four hex digits) should be removed. Many of the quartets have trailing 0s (0s on the right side of the quartet), so make sure to not remove those 0s.

The **unabbreviated** version of an IPv6 address must have 32 digits. The :: was replaced with four quartets of 0000, making the number have eight sets of hex digits total (32 digits). Also, for each quartet with fewer than four digits, leading 0s were added so that each quartet has four hex digits.

Question 125. Given the following IPv6 address 1230::. Which of the following is the the unabbreviated form?

(A) 1230:0000:0000:0000:0000:0000:0000:0000

(B) 1230:0000:0000:0000:0000:0000:0000

(C) 1230:0000:0000:0000:0000:0000

(D) 1230:0000::0000::0000:0000:0000

Explanation 125.

1230:0000:0000:0000:0000:0000:0000:0000 is the correct answer. The **unabbreviated** version of an IPv6 address must have 32 digits. The :: was replaced with four quartets of 0000, making the number have eight sets of hex digits total (32 digits). Also, for each quartet with fewer than four digits, leading 0s were added so that each quartet has four hex digits.

To **abbreviate** IPv6 addresses, only leading 0s in a quartet (one set of four hex digits) should be removed. Many of the

quartets have trailing 0s (0s on the right side of the quartet), so make sure to not remove those 0s.

Question 126. You have been tasked to give the router's G0/1 interface a unicast IPv6 address of 2005:1:2:3:4:5:6:A, with a /64 prefix length. What command will you type to mark the task as done?

(A) ipv6 address 2005:1:2:3:4:5:5:A/64

(B) ipv6 address 2005:1:2:3:4:5:6:A/46

(C) ipv4 address 2005:1:2:3:4:5:6:A/64

(D) ipv6 address 2005:1:2:3:4:5:6:A/64

Explanation 126. **ipv6 address 2005:1:2:3:4:5:6:A/64 is the correct answer.** The command that gives the router's G0/1 interface a unicast IPv6 address of 2005:1:2:3:4:5:6:A, with a /64 prefix length is:

Question 127. Which of the following is the prefix for address 1000:0000:0000:0001:0000:0000:0000:0000, assuming a mask of /64?

(A) 1000::1:10:0:0:0/64

(B) 1000:0:0:1::/64

(C) 2000:0:0:1::/64

(D) 1000::1::/64

Explanation 127. **1000:0:0:1::/64 is the correct answer.** The /64 prefix length means that the last 64 bits, or last 16 digits, of the address, should be changed to all 0s.

That process gives the unabbreviated prefix as 1000:0000:0000:0001:0000:0000:0000:0000.

The last four quartets (last four sets of four hex digits) are all 0s, making that string of all 0s be the longest and best string of 0s to replace with ::.

After removing the leading 0s in other quartets, the correct answer is: 1000:0:0:1::/64.

Question 128. End-user hosts need to know the IPv6 address of a default router, to which the host sends IPv6 packets if the host is in a different subnet.

(A) TRUE

(B) FALSE

Explanation 128. **TRUE is the correct answer.** IPv6 routing looks just like IPv4 routing. IPv6 uses these ideas the same way as IPv4:

1. To be able to build and send IPv6 packets out an interface,

end-user devices need an IPv6 address on that interface.

2. End-user hosts need to know the IPv6 address of a default router, to which the host sends IPv6 packets if the host is in a different subnet.

3. IPv6 routers de-encapsulate and re-encapsulate each IPv6 packet when routing the packet.

4. IPv6 routers make routing decisions by comparing the IPv6 packet's destination address to the router's IPv6 routing table; the matched route lists directions of where to send the IPv6 packet next.

Question 129. Which of the following commands will you type to enable IPv6 routing on the router?

(A) ipv6 enable-routing

(B) ipv6 unicast-routing

(C) ipv6 on-routing

(D) ipv6 open-routing

Explanation 129. ipv6 unicast-routing is the correct answer.

Question 130. Which of the following commands will you type

to configure the interface with ipv6 address 2002:1:2:3::4/64?

(A) ipv6 address 2002:1:1:2:3::4/64

(B) ipv6 address 2002:1:2:3::4

(C) ipv6 address 2002:1:2:3::4/64

(D) ipv6 address 2002:1:2:4::4/64

Explanation 130. **ipv6 address 2002:1:2:3::4/64 is the correct answer.**

Question 131. One of the following multicast addresses is defined as the address for sending packets to only the IPv6 routers on the local link.

(A) FF02::1

(B) FF02::2

(C) FF02::5

(D) FF02::A

Explanation 131. **FF02::2 is the correct answer.** FF02::2 is used to send packets to all IPv6 routers on a link.

1. FF02::1 is used by all IPv6 hosts on the link

2. FF02::5 is used by all OSPFv3 routers

3. FF02::A is used by all EIGRPv6 routers

Question 132. PC1, PC2, and Router R1 all connect to the same VLAN and IPv6 subnet. PC1 wants to send its first IPv6

packet to PC2. What protocol or message will PC1 use to discover the MAC address to which PC1 should send the Ethernet frame that encapsulates this IPv6 packet?

(A) NDP NS

(B) NAT

(C) DHCP

(D) ARP

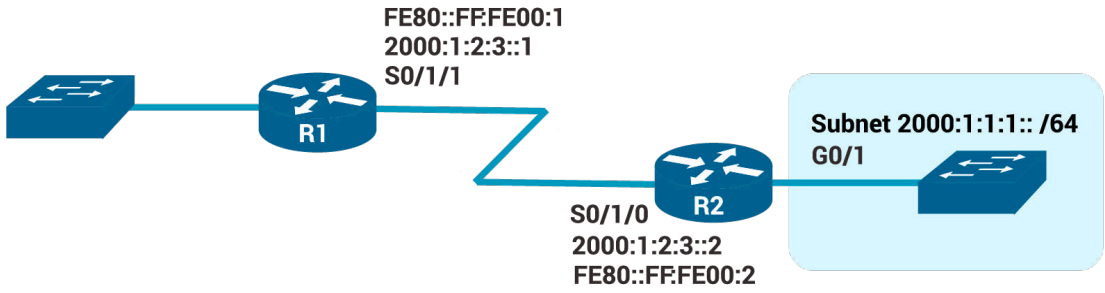
Explanation 132. **NDP NS is the correct answer.** PC1 needs to discover PC2's MAC address. Unlike IPv4, IPv6 does not use ARP, instead using NDP. Specifically, PC1 uses the NDP Neighbor Solicitation (NS) message to request that PC2 send back an NDP Neighbor Advertisement (NA)

NS — Neighbor Solicitation is a message that sent by a node to determine the link-layer address of a neighbor, or to verify that a neighbor is still reachable via a cached link-layer address. NSes are also used for Duplicate Address Detection (DAD).

NA — Neighbor Advertisement is a message that sent in response to an NS message. A node may also send unsolicited NAs to announce a link-layer address change.

Question 133. The router R2 has been configured with the

ipv6 address 2000:1:1:1::1/64 command on its G0/1 interface as shown in the figure. The router creates a link-local address of FE80::FF:FE00:11 as well. The interface is working. Which of the following routes will the router add to its IPv6 routing table? (Choose two answers.)



(A) A route for FE80::FF:FE00:11/128

(B) A route for FE80::FF:FE00:11/64

(C) A route for 2000:1:1:1::1/128

(D) A route for 2000:1:1:1::/64

(E) A route for 2000:1:2:3::2/128

Explanation 133. **C and D are the correct answers.** With an IPv6 address on a working interface, the router adds a connected route for the prefix (subnet) implied by the **ipv6 address** command.

It also adds a local host route (with a /128 prefix length) based on the unicast address. The router does not add a route based on the link-local address.

The router will add the following routes to its IPv6 routing table:

1. A route for 2000:1:1:1::/64

2. A route for 2000:1:1:1::1/128

Question 134. Router R2 has an interface named Gigabit Ethernet 0/2, whose MAC address has been set to 5555.4444.3333. This interface has been configured with the **ipv6 address 7000:1:1:1::/64 eui-64** subcommand. What unicast address will this interface use?

(A) 7000:1:1:1:55FF:FE55:4444:3333

(B) 7000:1:1:1:5755:44FF:FE44:3333

(C) 7000:1:1:1:5555:4444:33FF:FE33

(D) 7000:1:1:1:200:FF:FE00:0

Explanation 134. 7000:1:1:1:5755:44FF:FE44:3333 is the correct answer. With the **eui-64** parameter, the router will calculate the **interface ID portion** of the IPv6 address based **on its MAC address**.

Beginning with 5555.4444.3333, the router injects FF FE in the middle **(5555.44FF.FE44.3333)**. Then the router inverts the

seventh bit in the first byte.

Mentally, this converts hex 55 to binary 0101 0101, changing the seventh bit so the string is **0101 0111** and converting back to hex 52.

The final interface ID value is 5755:44FF:FE44:3333

Question 135. The **show ipv6 interface brief** command gives you interface IPv6 address info, and prefix length info.

(A) TRUE

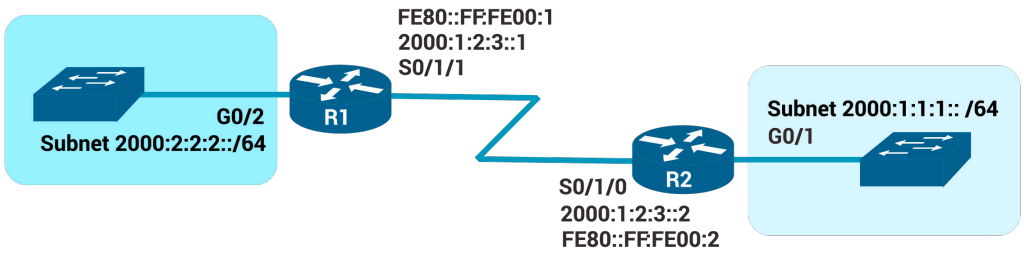
(B) FALSE

Explanation 135. **FALSE is the correct answer.** The **show ipv6 interface brief** command gives you interface IPv6 address info, but not prefix length info, similar to the IPv4 **show ip interface brief** command.

The **show ipv6 interface** command gives the details of IPv6 interface settings, much like the **show ip interface** command does for IPv4.

Question 136. You are responsible to configure a static route on R1's outgoing interface, in order to support traffic between the subnets. R2 is already configured. Which of the following

commands will you type to configure a static route on R1's outgoing interface?



(A) ipv6 route 2000:1:1:1::/64 s0/1/1

(B) ipv6 route 2000:2:2:2::/64 s0/1/1

(C) ipv6 route 2000:1:2:3::/64 s0/1/1

(D) ipv6 route 2000:1:1:1::/64 g0/2

Explanation 136. ipv6 route 2000:1:1:1::/64 s0/1/1 is the correct answer. IPv4 and IPv6 static routes, when the command references an interface, the interface is a local interface.

To support traffic between the subnets requires both routers to have a static route. R1 is now configured. Host A from the subnet 2000:1:1:1::/64 will forward all its IPv6 packets to its default router (R1), and R1 can now route those packets out S0/1/1 to R2 next.

The question declared that the R2 is already configured so, now both subnets can communicate. If the R2 wasn't config-

ured then you should have added the following command on R2.

R2(config)# ipv6 route 2000:2:2:2::/64 S0/1/0

Static routes instead of using the local interfaces, they can use the IP address of the next router as a next-hop.

Below we provide an example of how the command looks like on both routers if you were used the IP of the next router to create static route.

R1(config)# ipv6 route 2000:1:1:1::/64 2000:1:2:3::2
R2(config)# ipv6 route 2000:2:2:2::/64 2000:1:2:3::1

CHAPTER 7
SECURITY FUNDAMENTALS

Questions 137-153

Question 137. In a spoofing attack, which of the following parameters are commonly spoofed? (Choose two answers)

(A) Source IP address

(B) MAC address

(C) ARP address

(D) Routing table

(E) Destination IP address

(E) ARP table

Question 138. AAA servers usually support the protocol TACACS+ and _____ to communicate with enterprise resources.

(A) DHCP

(B) ARP

(C) RADIUS

(D) HTTP

Question 139. The senior network engineer assigns you a task related to port security. He needs your help to configure the fa0/1 from the SW-examsD to accept frames only from the MAC 0200.1111.2222.

Type the commands that need to be configured on the SW-examsD following the requirements below:

1. configure the FastEthernet0/1 to be an access port

2. enable port security on that interface

3. define the allowed MAC address

(A) SW-examsD#configure terminal
SW-examsD(config)#interface FastEthernet0/2
SW-examsD(config-if)#switchport mode access
SW-examsD(config-if)#switchport port-security
SW-examsD(config-if)#switchport port-security mac-address 0200.1111.2222

(B) SW-examsD#configure terminal
SW-examsD(config)#interface FastEthernet0/1
SW-examsD(config-if)#switchport mode access
SW-examsD(config-if)#switchport port-security

(C) SW-examsD#configure terminal
SW-examsD(config)#interface FastEthernet0/1
SW-examsD(config-if)#switchport mode access

SW-examsD(config-if)#switchport port-security

SW-examsD(config-if)#switchport port-security mac-address 0200.2222.2222

(D) SW-examsD#configure terminal

SW-examsD(config)#interface FastEthernet0/1

SW-examsD(config-if)#switchport mode access

SW-examsD(config-if)#switchport port-security

SW-examsD(config-if)#switchport port-security mac-address 0200.1111.2222

Question 140. _____ attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to additional users.

(A) Spoofing

(B) Phishing

(C) DoS

(D) SQL injection

Question 141. A _____ is malicious software that is hidden and packaged inside other software that looks normal and legitimate.

(A) Worm

(B) Virus

(C) Spyware

(D) Trojan

Question 142. What devices can be used to implement DHCP Snooping? (Choose two answers)

(A) Hub

(B) Layer 2 switches

(C) Routers

(D) Layer 3 switches

(E) Access Points

(F) End users

Question 143. Which of the following Cisco Firepower NGIPS's features provides more insights into and control over the users, applications, devices, threats, and vulnerabilities in your network with real-time visibility?

(A) Security automation

(B) Granular application visibility and control

(C) Contextual awareness

(D) Superior effectiveness

Question 144. What can be accomplished with a brute-force attack?

(A) Guess a user's password

(B) Make a server unavailable

(C) Spoof every possible IP address

(D) Alter a routing table

Question 145. Social engineering attack is accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

(A) TRUE

(B) FALSE

Question 146. Which of the following human security vulnerabilities attacks is a type of attack that targets high-profile employees, such as the CEO or CFO, in order to steal sensitive information from a company?

(A) Social engineering

(B) Phishing

(C) Whaling

(D) Pharming

Question 147. Which of the following human security vulnerabilities attacks is the attempt to obtain sensitive information such as passwords and credit card details by disguising oneself as a trustworthy entity?

(A) Social engineering

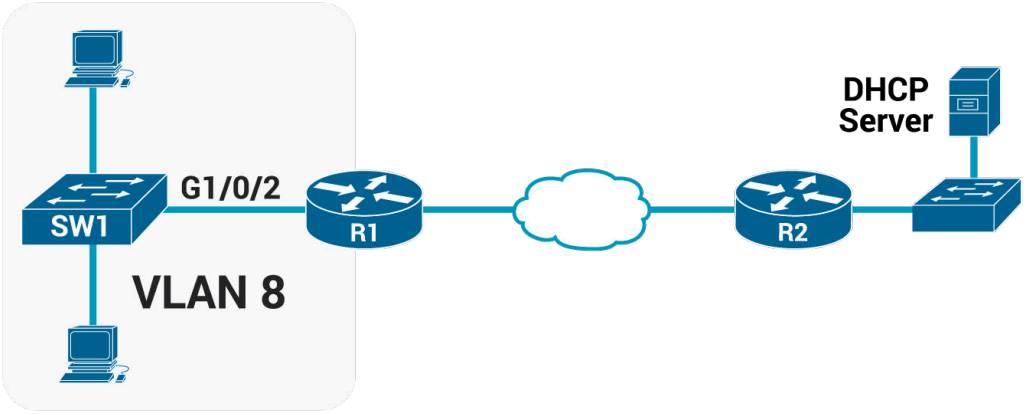
(B) Phishing

(C) Whaling

(D) Pharming

Question 148. You are responsible to enable DHCP snooping on the SW1. The R1 is a DHCP relay agent that needs to be trusted. SW1 places all the ports on VLAN 8.

Which commands will you type in order to configure DHCP snooping on the SW1 based on the diagram below?



(A)
```
SW1# configure terminal
SW1(config)# ip dhcp snooping
SW1(config)# ip dhcp snooping vlan 3
SW1(config)# interface GigabitEthernet1/0/2
SW1(config-if)# ip dhcp snooping trust
```

(B) SW1# configure terminal

SW1(config)# ip dhcp snooping
SW1(config)# ip dhcp snooping vlan 8
SW1(config)# interface GigabitEthernet1/1/2
SW1(config-if)# ip dhcp snooping trust

(C) SW1# configure terminal
SW1(config)# ip dhcp snooping
SW1(config)# ip dhcp snooping vlan 8
SW1(config)# interface GigabitEthernet1/0/2
SW1(config-if)# ip dhcp snooping trust

(D) SW1# configure terminal
SW1(config)# ip dhcp snooping
SW1(config)# ip dhcp snooping vlan 8
SW1(config)# interface GigabitEthernet1/0/2

Question 149. Which of the following security features rejects invalid and malicious ARP packets and prevents a class of man-in-the-middle attacks?

(A) DoS

(B) DAI

(C) Packet secure

(D) ARP protect

Question 150. In a reflection attack, the source IP address in

the attack packets is spoofed so that it contains the address of the victim.

(A) TRUE

(B) FALSE

Question 151. Type the command that needs to be configured on a switch to automatically recover from the err-disabled state, when caused by port security.

(A) recovery cause psecure-violation

(B) errdisable recovery psecure-violation

(C) errdisable recovery

(D) errdisable recovery cause psecure-violation

Question 152. A next-generation firewall sits at the edge of a company's connection to the Internet. A network engineer has been configured to prevent Telnet clients residing on the Internet from accessing Telnet servers inside the company. Which of the following might a next-generation firewall use that a traditional firewall would not?

(A) Match message destination well-known port 23

(B) Match message application data

(C) Match message IP protocol 23

(D) Match message source TCP ports lower than 5400

Question 153. Your PC connects to a LAN and uses DHCP to

lease an IP address for the first time. Of the usual four DHCP messages that flow between the PC (DHCP client) and the DHCP server, which ones do the server send? (Choose two answers)

(A) Acknowledgment

(B) Request

(C) Offer

(D) Discover

Answers 137-153

Question 137. In a spoofing attack, which of the following parameters are commonly spoofed? (Choose two answers)

(A) Source IP address

(B) MAC address

(C) ARP address

(D) Routing table

(E) Destination IP address

(E) ARP table

Explanation 137. **A and B are the correct answers.** Attackers usually spoof the **source IP address** in packets they send in order to disguise themselves and make the actual IP address owner into a victim of the attack. **MAC addresses** can also be spoofed in ARP replies to confuse other hosts and routers on the local network.

Question 138. AAA servers usually support the protocol TACACS+ and _____ to communicate with enterprise resources.

(A) DHCP

(B) ARP

(C) RADIUS

(D) HTTP

Explanation 138. **RADIUS is the correct answer.** AAA servers usually support the protocol TACACS+ and RADIUS to communicate with enterprise resources.

Authentication, authorization, and accounting (AAA) manage user activity to and through systems.

You can think of AAA in the following manner:
1. Authentication: Who is the user?
2. Authorization: What is the user allowed to do?
3. Accounting: What did the user do?
Cisco implements AAA services in its Identity Services Engine (ISE) platform.

AAA servers support the following two protocols to communicate with enterprise resources:

1) TACACS+: TACACS+ A Cisco proprietary protocol that separates each of the AAA functions. Communication is secure and encrypted over TCP port 49.

One of the key differentiators of TACACS+ is its ability to separate authentication, authorization, and accounting as separate and independent functions. This is why TACACS+ is so com-

monly used for device administration, even though RADIUS is still certainly capable of providing device administration AAA.

2) RADIUS: Radius is a network protocol that controls user network access via authentication and accounting. Commonly used by Internet Service Providers (ISPs), cellular network providers, and corporate and educational networks.

The RADIUS protocol serves three primary functions:
1. Authenticates users or devices before allowing them access to a network
2. Authorizes those users or devices for specific network services
3. Accounts for the usage of those services

Question 139. The senior network engineer assigns you a task related to port security. He needs your help to configure the fa0/1 from the SW-examsD to accept frames only from the MAC 0200.1111.2222.

Type the commands that need to be configured on the SW-examsD following the requirements below:

1. configure the FastEthernet0/1 to be an access port

2. enable port security on that interface

3. define the allowed MAC address

(A) SW-examsD# configure terminal
SW-examsD(config)# interface FastEthernet0/2
SW-examsD(config-if)# switchport mode access
SW-examsD(config-if)# switchport port-security
SW-examsD(config-if)# switchport port-security mac-address 0200.1111.2222

(B) SW-examsD# configure terminal
SW-examsD(config)# interface FastEthernet0/1
SW-examsD(config-if)# switchport mode access
SW-examsD(config-if)# switchport port-security

(C) SW-examsD# configure terminal
SW-examsD(config)# interface FastEthernet0/1
SW-examsD(config-if)# switchport mode access
SW-examsD(config-if)# switchport port-security
SW-examsD(config-if)# switchport port-security mac-address 0200.2222.2222

(D) **SW-examsD# configure terminal**
SW-examsD(config)# interface FastEthernet0/1
SW-examsD(config-if)# switchport mode access

SW-examsD(config-if)# switchport port-security

SW-examsD(config-if)# switchport port-security mac-address 0200.1111.2222

Explanation 139. **D is the correct answer.** The command **switchport mode access** forces that port to be an access port with no VLAN tagging allowed EXCEPT for the voice vlan.

The command **switchport port-security** enable port security on the interface.
The command **switchport port-security mac-address 0200.1111.2222** defines any allowed source MAC addresses for this interface.

Question 140. _____ attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to additional users.

(A) Spoofing
(B) Phishing
(C) DoS
(D) SQL injection

Explanation 140. **DoS is the correct answer.** A **denial-of-**

service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning.

DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to additional users. A DoS attack is characterized by using a single computer to launch the attack.

Question 141. A _____ is malicious software that is hidden and packaged inside other software that looks normal and legitimate.

(A) Worm

(B) Virus

(C) Spyware

(D) Trojan

Explanation 141. **Trojan is the correct answer.** A **trojan horse** is malicious software that is hidden and packaged inside other software that looks normal and legitimate. If a well-meaning user decides to install it, the trojan horse software is silently installed too. Then the malware can run attacks of its own on the local system or against other systems.

Trojan horse malware can spread from one computer to another only through user interaction such as opening email attachments, downloading software from the Internet, and inserting a USB drive into a computer.

Worms are another type of malware that is able to propagate to and infect other systems on its own. They use a computer network to spread, relying on security failures on the target computer to access it, and steal or delete data.

Viruses are malware that can propagate between systems more readily. To spread, virus software must inject itself into another application, then rely on users to transport the infected application software to other victims.

Viruses must execute to do their dirty work, so they target any type of file that the system can execute.

Spyware is, as the name implies, software that spies on you. Designed to monitor and capture your Web browsing and other activities, spyware, like adware, will often send your browsing activities to advertisers.

Spyware, however, includes capabilities not found in adware. It may, for example, also capture sensitive information like bank-

ing accounts, passwords, or credit card information.

Question 142. What devices can be used to implement DHCP Snooping? (Choose two answers)

(A) Hub

(B) Layer 2 switches

(C) Routers

(D) Layer 3 switches

(E) Access Points

(F) End users

Explanation 142. **B and D are the correct answers.** Layer 2 switches, as well as Layer 3 (multilayer) switches, perform DHCP Snooping.

DHCP Snooping must be implemented on a device that performs Layer 2 switching. The DHCP Snooping function needs to examine DHCP messages that flow between devices within the same broadcast domain (VLAN).

The fundamental use case for DHCP snooping is to prevent unauthorized (rogue) DHCP servers offering IP addresses to DHCP clients. Rogue DHCP servers are often used in man in the middle or denial of service attacks for malicious purposes.

Question 143. Which of the following Cisco Firepower NGIPS's features provides more insights into and control over the users, applications, devices, threats, and vulnerabilities in your network with real-time visibility?

(A) Security automation

(B) Granular application visibility and control

(C) Contextual awareness

(D) Superior effectiveness

Explanation 143. **Contextual awareness is the correct answer.** **Contextual awareness** provides more insights into and control over the users, applications, devices, threats, and vulnerabilities in your network with real-time visibility.

Security automation automatically correlate threat events, contextual awareness information, and vulnerability data to better focus your staff, implement better security and speed forensic investigations

Granular application visibility and control reduces threats to your network through precise control over more than 4000 commercial applications, with support for custom applications.

Superior effectiveness stops more threats, both known and unknown, with industry-leading threat protection. Speeds time

to detection of malware to reduce its damage and spread.

Question 144. What can be accomplished with a brute-force attack?

(A) Guess a user's password

(B) Make a server unavailable

(C) Spoof every possible IP address

(D) Alter a routing table

Explanation 144. Guess a user's password is the correct answer. Guess a user's password. A **brute force attack** is an attempt to crack a password or username using a trial and error approach. In a brute-force attack, an attacker's software tries every combination of letters, numbers, and special characters to eventually find a string that matches a user's password.

Question 145. Social engineering attack is accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

(A) TRUE

(B) FALSE

Explanation 145. TRUE is the correct answer.

Question 146. Which of the following human security vulnerabilities attacks is a type of attack that targets high-profile employees, such as the CEO or CFO, in order to steal sensitive information from a company?

(A) Social engineering

(B) Phishing

(C) Whaling

(D) Pharming

Explanation 146. **Whaling is the correct answer.** **Whaling** is a type of attack that targets high-profile employees, such as the CEO or CFO, in order to steal sensitive information from a company.

Question 147. Which of the following human security vulnerabilities attacks is the attempt to obtain sensitive information such as passwords and credit card details by disguising oneself as a trustworthy entity?

(A) Social engineering

(B) Phishing

(C) Whaling

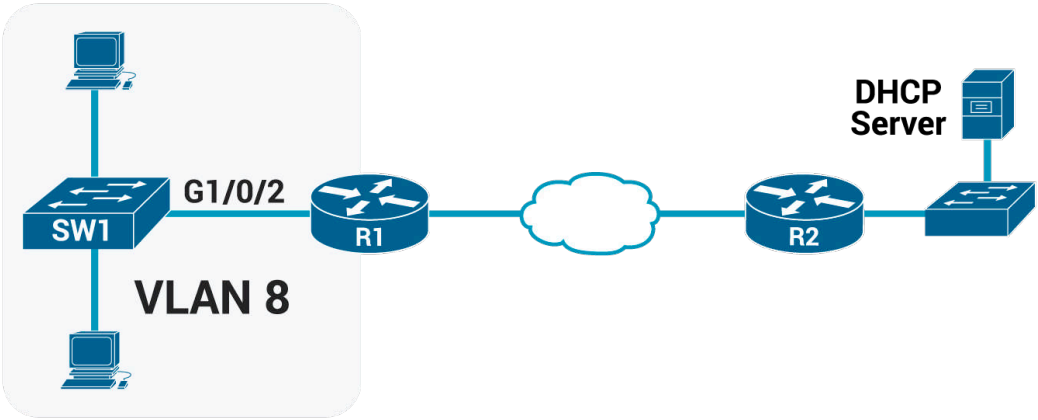
(D) Pharming

Explanation 147. **Phishing is the correct answer.** **Phishing** is the attempt to obtain sensitive information such as passwords

and credit card details by disguising oneself as a trustworthy entity.

Question 148. You are responsible to enable DHCP snooping on the SW1. The R1 is a DHCP relay agent that needs to be trusted. SW1 places all the ports on VLAN 8.

Which commands will you type in order to configure DHCP snooping on the SW1 based on the diagram below?



(A) SW1# configure terminal
SW1(config)# ip dhcp snooping
SW1(config)# ip dhcp snooping vlan 3
SW1(config)# interface GigabitEthernet1/0/2
SW1(config-if)# ip dhcp snooping trust

(B) SW1# configure terminal
SW1(config)# ip dhcp snooping
SW1(config)# ip dhcp snooping vlan 8
SW1(config)# interface GigabitEthernet1/1/2
SW1(config-if)# ip dhcp snooping trust

(C) SW1# configure terminal
SW1(config)# ip dhcp snooping
SW1(config)# ip dhcp snooping vlan 8
SW1(config)# interface GigabitEthernet1/0/2
SW1(config-if)# ip dhcp snooping trust

(D) SW1# configure terminal
SW1(config)# ip dhcp snooping
SW1(config)# ip dhcp snooping vlan 8
SW1(config)# interface GigabitEthernet1/0/2

Explanation 148. **C is the correct answer.**

Question 149. Which of the following security features rejects invalid and malicious ARP packets and prevents a class of man-in-the-middle attacks?

(A) DoS

(B) DAI

(C) Packet secure

(D) ARP protect

Explanation 149. **DAI is the correct answer.** The **Dynamic ARP Inspection (DAI)** feature on a switch examines incoming ARP messages on untrusted ports to filter those it believes to be part of an attack. DAI's core feature compares incoming ARP messages with two sources of data: the DHCP Snooping binding table and any configured ARP ACLs.

DAI relies on **DHCP snooping**. DHCP snooping listens to DHCP message exchanges and builds a bindings database of valid tuples (MAC address, IP address, VLAN interface).

Question 150. In a reflection attack, the source IP address in the attack packets is spoofed so that it contains the address of the victim.

(A) TRUE

(B) FALSE

Explanation 150. **TRUE is the correct answer.** **Reflection attacks** make use of a potentially legitimate third party component to send the attack traffic to a victim, ultimately hiding the attackers' own identity.

The victim will end up receiving a large volume of response packets it never had requested. With a large enough attack, the victim may end up with a congested network.

Question 151. Type the command that needs to be configured on a switch to automatically recover from the err-disabled state, when caused by port security.

(A) recovery cause psecure-violation

(B) errdisable recovery psecure-violation

(C) errdisable recovery

(D) errdisable recovery cause psecure-violation

Explanation 151. errdisable recovery cause psecure-violation is the correct answer. Once port security has placed a port in the **err-disabled state**, by default the port remains in an err-disabled state until someone takes action.

To recover from an err-disabled state, the interface must be shut down with the **shutdown** command and then enabled with the **no shutdown** command.
Alternately, the switch can be configured to automatically recover from the err-disabled state, when caused by port security, with these commands:

1. errdisable recovery cause psecure-violation: A global

command to enable automatic recovery for interfaces in an err-disabled state caused by port security.

2. errdisable recovery interval seconds: A global command to set the time to wait before recovering the interface.

Question 152. A next-generation firewall sits at the edge of a company's connection to the Internet. A network engineer has been configured to prevent Telnet clients residing on the Internet from accessing Telnet servers inside the company. Which of the following might a next-generation firewall use that a traditional firewall would not?

(A) Match message destination well-known port 23

(B) Match message application data

(C) Match message IP protocol 23

(D) Match message source TCP ports lower than 5400

Explanation 152. Match message application data is the correct answer. Traditional and next-generation firewalls can check TCP and UDP port numbers, but **next-generation firewalls are being able to also check application data** beyond the Transport layer header.

A next-generation firewall (NGFW) would look into the application data, identifying messages that contain data structures

used by Telnet, instead of matching with port numbers.

In other words, a next-generation firewall (NGFW) is defined as a deep-packet inspection firewall that moves beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall.

Question 153. Your PC connects to a LAN and uses DHCP to lease an IP address for the first time. Of the usual four DHCP messages that flow between the PC (DHCP client) and the DHCP server, which ones do the server send? (Choose two answers)

(A) Acknowledgment

(B) Request

(C) Offer

(D) Discover

Explanation 153. **A and C is the correct answer.** DHCP uses the following four messages between the client and the server:

1. Discover: Sent by the DHCP client to find a willing DHCP server.

2. Offer: Sent by a DHCP server to offer to lease to that client a specific IP address (and

inform the client of its other parameters).

3. Request: Sent by the DHCP client to ask the server to lease the IPv4 address listed in the Offer message.
4. Acknowledgment: Sent by the DHCP server to assign the address and to list the mask, default router, and DNS server IP addresses.

DHCP clients have a problem, they do not have an IP address yet, but they need to send these DHCP messages inside IP packets. To make that work, DHCP messages make use of two special IPv4 addresses that allow a host that has no IP address to still be able to send and receive messages on the local sub-net:

0.0.0.0: An address reserved for use as a source IPv4 address for hosts that do not yet have an IP address.
255.255.255.255: The local broadcast IP address. Packets sent to this destination address are broadcast on the local data link, but routers do not forward them.

CHAPTER 8
IP ACCESS CONTROL LIST

Questions 154-178

Question 154. Given the following URI https://courses.exams-digest.com/ccna, which part is the hostname?

(A) https

(B) courses

(C) courses.examsdigest.com

(D) examsdigest.com

(E) examsdigest.com/ccna

Question 155. Which of the following protocols uses the port 443?

(A) HTTPS

(B) HTTP

(C) SMTP

(D) SSH

Question 156. Which of the following protocols uses the port 80?

(A) HTTPS

(B) HTTP

(C) SMTP

(D) SSH

Question 157. Which of the following protocols uses the port 25?

(A) HTTPS

(B) HTTP

(C) SMTP

(D) SSH

Question 158. Which of the following protocols uses the port 22?

(A) HTTPS

(B) HTTP

(C) SMTP

(D) SSH

Question 159. Which of the following port numbers the SNMP protocol uses?

(A) 20

(B) 25

(C) 160

(D) 161

Question 160. Which of the following port numbers the POP3

protocol uses?

(A) 100

(B) 110

(C) 120

(D) 130

Question 161. Which of the following port numbers the DNS protocol uses?

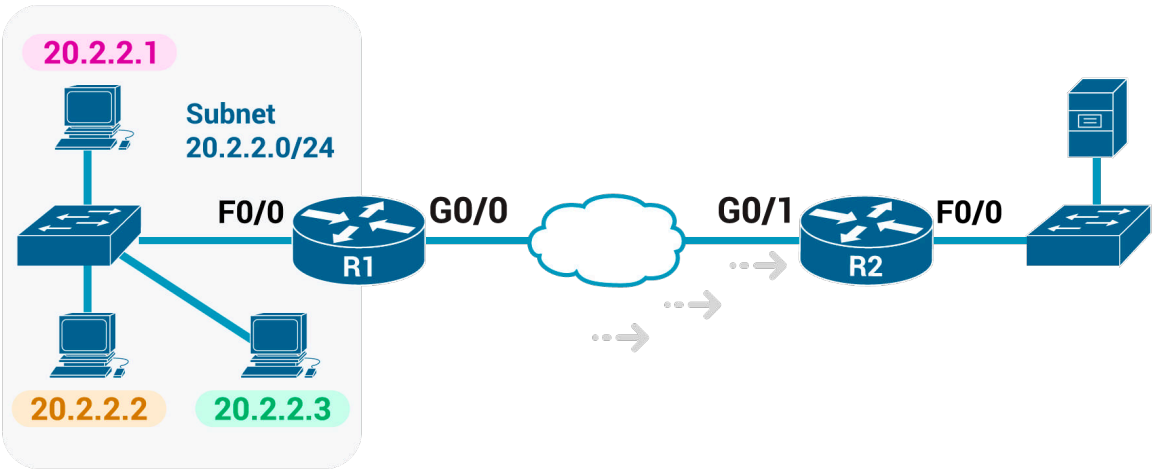
(A) 50

(B) 51

(C) 52

(D) 53

Question 162. The senior network engineer assigns you a task that requires ACL configuration. He provides the following diagram and the requirements below:



1. Enable the ACL inbound on R2's G0/1 interface.

2. Permit packets coming from the host with IP 20.2.2.1

3. Deny packets coming from the rest subnet 20.2.2.0/24

4. Permit packets coming from a network with subnet 155.165.0.0/16

Now you are responsible to configure the R2 using the ACL standard number 1. Which of the following commands will you type to complete the task?

(A) R2# configure terminal
R2(config)# access-list 1 permit 20.2.2.1
R2(config)# access-list 1 deny 20.2.2.0 0.0.0.255
R2(config)# access-list 1 permit 155.165.0.0 0.0.255.255
R2(config)# interface G0/2
R2(config-if)# ip access-group 1 in

(B) R2# configure terminal
R2(config)# access-list 1 permit 20.2.2.1
R2(config)# access-list 1 deny 20.2.2.0 0.0.0.255
R2(config)# access-list 1 permit 155.165.0.0 0.0.255.255
R2(config)# interface G0/1

R2(config-if)# ip access-group 1 in

(C) R2# configure terminal
R2(config)# access-list 1 permit 20.2.2.1
R2(config)# access-list 1 deny 20.2.2.0 0.0.0.255
R2(config)# access-list 1 permit 155.165.0.0 0.0.255.255
R2(config)# interface G0/1

(D) R2# configure terminal
R2(config)# access-list 1 deny 20.2.2.1
R2(config)# access-list 1 deny 20.2.2.0 0.0.0.255
R2(config)# access-list 1 permit 155.165.0.0 0.0.255.255
R2(config)# interface G0/1
R2(config-if)# ip access-group 1 in

Question 163. Which of the following options are things that a standard IP ACL could be configured to do? (Choose two answers.)

(A) Match the exact source IP address

(B) Match all IP addresses in a subnet with one access-list command without matching other IP addresses

(C) Match IP addresses 20.2.2.2 through 20.2.2.22 with one access-list command without matching other IP addresses

(D) Match only the packet's destination IP address

Question 164. One of the differences between named and numbered ACLs is that named ACLS using ACL subcommands, not global commands, to define the action and matching parameters.

(A) TRUE

(B) FALSE

Question 165. Given the following fields, which of those cannot be compared on an extended IP ACL?

(A) Application protocol

(B) Destination IP address

(C) Source IP address

(D) URL

(E) TOS Byte

Question 166. Your task is to type a one-line standard ACL that matches the following criteria. All access-list commands use the number 1 in the command.

Criteria #1: Permit packets from 186.33.2.3

ACL command #1: _____

(A) access-list 1 permit 186.33.2.3

(B) access-list 1 deny 186.33.2.3

(C) access-list 1 permit 186.33.2.0

(D) access-list 1 deny 186.33.0.0

Question 167. Your task is to type a one-line standard ACL that matches the following criteria. All access-list commands use the number 1 in the command.

Criteria #2: Permit packets from hosts with 56.57.2 as the first three octets

ACL command #2: _____

(A) access-list 1 permit 56.57.2.0 0.0.0.255

(B) access-list 1 permit 57.57.2.0 0.0.0.255

(C) access-list 1 permit 56.57.2.0 0.0.255.255

(D) access-list 1 deny 56.57.2.0 0.0.0.255

Question 168. Your task is to type a one-line standard ACL that matches the following criteria. All access-list commands use the number 1 in the command.

Criteria #3: Permit packets from hosts with 56.57 as the first two octets

ACL command #3: _____

(A) access-list 1 permit 56.57.0.0 0.255.255.255

(B) access-list 1 permit 56.57.0.0 0.0.255.255

(C) access-list 1 permit 56.58.0.0 0.0.255.255

(D) access-list 1 permit 56.57.0.0 0.0.0.0

Question 169. Your task is to type a one-line extended ACL that matches the following criteria. All access-list commands use the number 101 in the command.

Criteria #4: Permit packets from web client 65.5.5.5, sent to a web server in subnet 65.5.6.0/24

ACL command #4: _____

(A) access-list 101 permit tcp host 65.5.5.5 65.5.6.0 0.0.0.255 eq 23

(B) access-list 101 permit any any

(C) access-list 101 permit tcp host 65.5.5.5 65.5.6.0 0.0.0.255 eq www

(D) access-list 101 deny tcp host 65.5.5.5 65.5.6.0 0.0.0.255 eq www

Question 170. Your task is to type a one-line extended ACL that matches the following criteria. All access-list commands use the number 101 in the command.

Criteria #5: Permit any and every IPv4 packet

ACL command #5: _____

(A) access-list 101 permit ip any any

(B) access-list 101 deny ip any any

(C) access-list 101 permit ip 0.0.0.0 any

(D) access-list 101 permit ip any 0.0.0.0

Question 171. Which of the following commands display the configuration of an IPv4 ACL, including line numbers? (Choose two answers.)

(A) show running-config

(B) show startup-config

(C) show ip access-lists

(D) show access-lists

Question 172. Type the access-list command that permits all packets sent from hosts in subnet 14.15.16.0/24. Use the ACL number 50 for the ACL rule.

(A) access-list 50 permit 14.15.17.0 0.0.0.255

(B) access-list 50 deny 14.15.16.0 0.0.0.255

(C) access-list 50 permit 14.15.16.0 0.255.255.255

(D) access-list 50 permit 14.15.16.0 0.0.0.255

Question 173. Given the following access-list command **ac-**

cess-list 2 permit 192.168.4.0 0.0.0.255, choose the exact range of IP addresses, matched by the command.

(A) 192.167.4.0 – 192.168.4.255

(B) 192.168.4.0 – 192.168.5.255

(C) 192.168.4.0 – 192.168.4.255

(D) 192.0.0.0 – 192.168.4.255

Question 174. The range of valid ACL numbers for standard numbered IP ACLs is:

(A) 1-99 and 1700 - 1999

(B) 1-99 and 1300 - 1999

(C) 1-101 and 1300 - 1999

(D) 1-49 and 1400 - 1999

Question 175. The ACL 55 on R1 has four statements, in the following order, with address and wildcard mask values as follows:

1. 20.0.0.0 0.255.255.255

2. 20.20.0.0 0.0.255.255

3. 20.20.20.0 0.0.0.255

4. 2.2.2.0 0.0.0.255

If a router tried to match a packet sourced from IP address 20.20.20.20 using this ACL, which ACL statement does a router consider the packet to have matched?

(A) First statement

(B) Second statement

(C) Third statement

(D) Forth statement

(E) Implied deny at the end of the ACL

Question 176. Which of the following access-list denies packets with a UDP header, any source IP address with source port greater than 10455, a destination IP address 30.3.3.3 and a destination port equal to 25?

(A) access-list 101 deny udp any gt 10455 host 30.3.3.3 eq 28

(B) access-list 101 deny udp any gt 10455 host 30.3.3.3 eq 25

(C) access-list 101 deny tcp any gt 10455 host 30.3.3.3 eq 25

(D) access-list 101 deny udp any gt 25 host 30.3.3.3 eq 25

Question 177. Which of the following access-list denies packets with a UDP header, a source IP address 30.3.3.3 and a source port greater than 10455, any destination IP address 30.3.3.3 with destination port equal to 25?

(A) access-list 101 deny udp host 30.3.3.3 gt 10455 any eq 30

(B) access-list 101 deny udp host 30.3.3.3 gt 25 any eq 25

(C) access-list 101 deny udp host 30.0.0.0 gt 10455 any eq

25

(D) access-list 101 deny udp host 30.3.3.3 gt 10455 any eq 25

Question 178. Choose the wildcard mask that matches all IP packets in the subnet 46.45.44.0, and mask 255.255.255.0.

(A) 0.0.0.255

(B) 0.0.255.255

(C) 0.255.255.255

(D) 255.255.255.255

Answers 154-178

Question 154. Given the following URI https://courses.exams-digest.com/ccna, which part is the hostname?

(A) https

(B) courses

(C) courses.examsdigest.com

(D) examsdigest.com

(E) examsdigest.com/ccna

Explanation 154. **courses.examsdigest.com is the correct answer.** The hostname is the text between the // and the /. The **hostname** is all the text between the // and the /. The text before the // identifies the **application layer protocol**, and the text after the / represents the name of the web page.

Protocol: HTTPS

Hostname: courses.examsdigest.com

Webpage name: ccna

Question 155. Which of the following protocols uses the port 443?

(A) HTTPS

(B) HTTP

(C) SMTP

(D) SSH

Explanation 155. **HTTPS is the correct answer.** **Hypertext transfer protocol secure (HTTPS) – Port 443.** HTTPS is the secure version of HTTP which is the primary protocol used to send data between a web browser and a website.

HTTPS is encrypted in order to increase the security of data transfer. This is particularly important when users transmit sensitive data, such as by logging into a bank account, email service, or health insurance provider

Question 156. Which of the following protocols uses the port 80?

(A) HTTPS

(B) HTTP

(C) SMTP

(D) SSH

Explanation 156. **HTTP is the correct answer.** **Hypertext Transfer Protocol (HTTP) – Port 80.** HTTP is an application-layer protocol for transmitting hypermedia documents, such as HTML. It was designed for communication between web browsers and web servers

Question 157. Which of the following protocols uses the port 25?

(A) HTTPS

(B) HTTP

(C) SMTP

(D) SSH

Explanation 157. SMTP is the correct answer. Simple Mail Transfer Protocol (SMTP) – Port 25. SMTP is the protocol used for sending e-mail over the Internet.

Your e-mail client (such as Outlook, or Mac OS X Mail) uses SMTP to send a message to the mail server, and the mail server uses SMTP to relay that message to the correct receiving mail server. Basically, SMTP is a set of commands that authenticate and direct the transfer of electronic mail.

Question 158. Which of the following protocols uses the port 22?

(A) HTTPS

(B) HTTP

(C) SMTP

(D) SSH

Explanation 158. **SSH is the correct answer.** **Simple Mail Transfer Protocol (SMTP) – Port 25.** SMTP is the protocol

Question 159. Which of the following port numbers the SNMP protocol uses?

(A) 20

(B) 25

(C) 160

(D) 161

Explanation 159. **161 is the correct answer.** **Simple Network Management Protocol (SNMP) – Port 161.** SNMP is an application layer protocol used specifically for network device management.

For example, Cisco supplies a large variety of network management products, many of them in the Cisco Prime network management software product family.
They can be used to query, compile, store, and display information about a network's operation. To query the network devices, Cisco Prime software mainly uses SNMP protocols.

Question 160. Which of the following port numbers the POP3 protocol uses?

(A) 100

(B) 110

(C) 120

(D) 130

Explanation 160. 110 is the correct answer. Post Office Protocol version 3 (POP3) – Port 110. POP3 is a standard mail protocol used to receive emails from a remote server to a local email client.

POP3 allows you to download email messages on your local computer and read them even when you are offline.

Note, that when you use POP3 to connect to your email account, messages are downloaded locally and removed from the email server.

Question 161. Which of the following port numbers the DNS protocol uses?

(A) 50

(B) 51

(C) 52

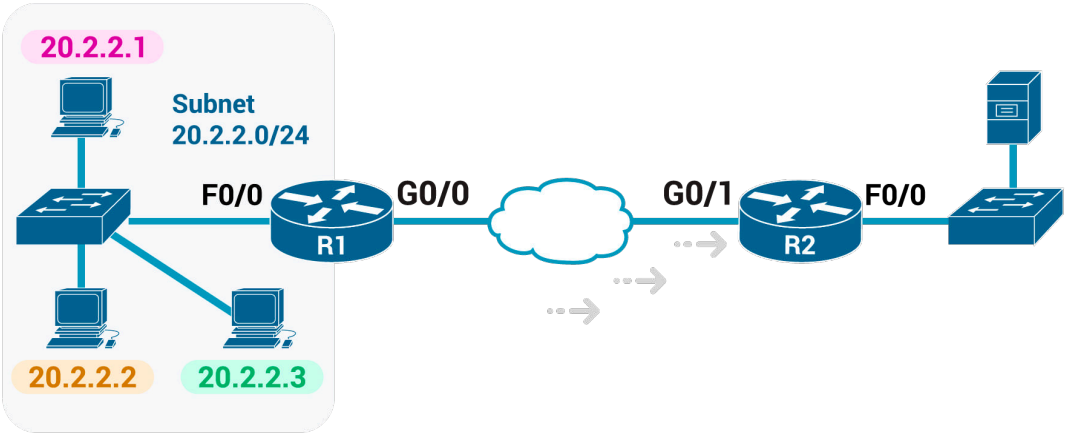
(D) 53

Explanation 161. 53 is the correct answer. The Domain Name System (DNS) – Port 53. DNS is the phonebook of the

Internet. Humans access information online through domain names, like examsdigest.com or cisco.com. Web browsers interact through Internet Protocol (IP) addresses.

DNS translates domain names to IP addresses so browsers can load Internet resources. The process of DNS resolution involves converting a hostname (such as www.examsdigest.com) into a computer-friendly IP address (such as 155.138.45.1).

Question 162. The senior network engineer assigns you a task that requires ACL configuration. He provides the following diagram and the requirements below:



1. Enable the ACL inbound on R2's G0/1 interface.
2. Permit packets coming from the host with IP 20.2.2.1
3. Deny packets coming from the rest subnet 20.2.2.0/24

4. Permit packets coming from a network with subnet 155.165.0.0/16

Now you are responsible to configure the R2 using the ACL standard number 1. Which of the following commands will you type to complete the task?

(A) R2# configure terminal
R2(config)# access-list 1 permit 20.2.2.1
R2(config)# access-list 1 deny 20.2.2.0 0.0.0.255
R2(config)# access-list 1 permit 155.165.0.0 0.0.255.255
R2(config)# interface G0/2
R2(config-if)# ip access-group 1 in

(B) R2# configure terminal
R2(config)# access-list 1 permit 20.2.2.1
R2(config)# access-list 1 deny 20.2.2.0 0.0.0.255
R2(config)# access-list 1 permit 155.165.0.0 0.0.255.255
R2(config)# interface G0/1
R2(config-if)# ip access-group 1 in

(C) R2# configure terminal
R2(config)# access-list 1 permit 20.2.2.1

R2(config)# access-list 1 deny 20.2.2.0 0.0.0.255

R2(config)# access-list 1 permit 155.165.0.0 0.0.255.255

R2(config)# interface G0/1

(D) R2# configure terminal

R2(config)# access-list 1 deny 20.2.2.1

R2(config)# access-list 1 deny 20.2.2.0 0.0.0.255

R2(config)# access-list 1 permit 155.165.0.0 0.0.255.255

R2(config)# interface G0/1

R2(config-if)# ip access-group 1 in

Explanation 162. **B is the correct answer.** The syntax of the ACL command is:

access-list access-list-number {deny | permit} source [source-wildcard]

The first command **access-list 1 permit 20.2.2.1** permits only the host with IP 20.2.2.1 to send packets through R2.

The second command **access-list 1 deny 20.2.2.0 0.0.0.255** denies all the subnet 20.2.2.0/24 to send packets through R2. This command uses a wildcard mask 0.0.0.255 which means

the first three octets have to be compared.

(Note, if the second command was before the first command then the host with IP 20.2.2.1 couldn't send packets, because ACLs "execute" the rules from top to bottom)

The third command **access-list 1 permit 155.165.0.0 0.0.255.255** permits all the packets coming from the 155.165.0.0/16. Again we use a wildcard mask 0.0.255.255 to tell the R2 to check if the packets coming from that particular network. So only packets from the range 155.165.0.0 – 155.165.255.255 are permitted.

If the wildcard mask was, 0.255.255.255, then the router would compare only the first octet which means, packets coming from 155.0.0.0 – 155.255.255.255 are permitted.

If the wildcard mask was, 0.0.0.255, then the router would compare the first three octets which means, packets coming from 155.165.0.0 – 155.165.0.255 are permitted.

The last commands **interface G0/1** and **ip access-group 1 in** enable the ACL inbound on R2's G0/1 interface.

Question 163. Which of the following options are things that a

standard IP ACL could be configured to do? (Choose two answers.)

(A) Match the exact source IP address

(B) Match all IP addresses in a subnet with one access-list command without matching other IP addresses

(C) Match IP addresses 20.2.2.2 through 20.2.2.22 with one access-list command without matching other IP addresses

(D) Match only the packet's destination IP address

Explanation 163. **A and B are the correct answers.** Standard ACLs check the source IP address. Matching all hosts in a subnet can be accomplished with the access-list 1 permit 20.2.2.0 0.0.0.255 command.

The address range 20.2.2.2 – 20.2.2.22 can be matched by an ACL, but it requires multiple access-list commands.

Question 164. One of the differences between named and numbered ACLs is that named ACLS using ACL subcommands, not global commands, to define the action and matching parameters.

(A) TRUE

(B) FALSE

Explanation 164. **TRUE is the correct answer.** Named IP

ACLs have many similarities with numbered IP ACLs. They can be used for filtering packets.

They can match the same fields as well: standard numbered ACLs can match the same fields as a standard named ACL, and extended numbered ACLs can match the same fields as an extended named ACL. Of course, there are differences between named and numbered ACLs.

Named ACLs originally had three big differences compared to numbered ACLs:

1. Using names instead of numbers to identify the ACL, making it easier to remember the reason for the ACL

2. Using ACL subcommands, not global commands, to define the action and matching parameters

3. Using ACL editing features that allow the CLI user to delete individual lines from the ACL and insert new lines

Working example:

```
RouterExamsDigest# configure terminal
RouterExamsDigest(config)# ip access-list extended examsdigestACL
RouterExamsDigest(config-ext-nacl)# permit tcp host 5.1.1.2 eq www any
RouterExamsDigest(config-ext-nacl)# deny udp host 5.1.1.1
```

```
10.1.2.0 0.0.0.255
RouterExamsDigest(config-ext-nacl)# deny ip 5.1.3.0
0.0.0.255 5.1.2.0 0.0.0.255
RouterExamsDigest(config-ext-nacl)# permit ip any any
RouterExamsDigest(config-ext-nacl)# interface g0/1
RouterExamsDigest(config-if)# ip access-group examsdigest-
ACL out
```

The ip access-list global configuration command defines whether an ACL is a standard or extended ACL and defines the name. In this case, the examsdigestACL is the name of the ACL.

The next commands permit and deny statements define the matching logic and action to be taken upon a match.

The last commands apply the named ACL on the interface.

Question 165. Given the following fields, which of those cannot be compared on an extended IP ACL?

(A) Application protocol

(B) Destination IP address

(C) Source IP address

(D) URL

(E) TOS Byte

Explanation 165. **URL is the correct answer.**

Extended ACLs can't look at the **URL** as this is an Application Layer information.

Extended ACLs can look at Layer 3 (IP) and Layer 4 (TCP, UDP) headers.

Question 166. Your task is to type a one-line standard ACL that matches the following criteria. All access-list commands use the number 1 in the command.

Criteria #1: Permit packets from 186.33.2.3
ACL command #1: _____

(A) access-list 1 permit 186.33.2.3
(B) access-list 1 deny 186.33.2.3
(C) access-list 1 permit 186.33.2.0
(D) access-list 1 deny 186.33.0.0

Explanation 166. **access-list 1 permit 186.33.2.3 is the correct answer.**

Criteria #1: Permit packets from 186.33.2.3
ACL command #1: access-list 1 permit 186.33.2.3

Question 167. Your task is to type a one-line standard ACL that matches the following criteria. All access-list commands use the number 1 in the command.

Criteria #2: Permit packets from hosts with 56.57.2 as the first three octets

ACL command #2: _____

(A) access-list 1 permit 56.57.2.0 0.0.0.255

(B) access-list 1 permit 57.57.2.0 0.0.0.255

(C) access-list 1 permit 56.57.2.0 0.0.255.255

(D) access-list 1 deny 56.57.2.0 0.0.0.255

Explanation 167. access-list 1 permit 56.57.2.0 0.0.0.255 is the correct answer.

Criteria #2: Permit packets from hosts with 56.57.2 as the first three octets

ACL command #2: access-list 1 permit 56.57.2.0 0.0.0.255

Question 168. Your task is to type a one-line standard ACL that matches the following criteria. All access-list commands use the number 1 in the command.

Criteria #3: Permit packets from hosts with 56.57 as the first two octets

ACL command #3: _____

(A) access-list 1 permit 56.57.0.0 0.255.255.255

(B) access-list 1 permit 56.57.0.0 0.0.255.255

(C) access-list 1 permit 56.58.0.0 0.0.255.255

(D) access-list 1 permit 56.57.0.0 0.0.0.0

Explanation 168. access-list 1 permit 56.57.0.0 0.0.255.255 is the correct answer.

Criteria #2: Permit packets from hosts with 56.57 as the first two octets

ACL command #2: access-list 1 permit 56.57.2.0 0.0.0.255

Question 169. Your task is to type a one-line extended ACL that matches the following criteria. All access-list commands use the number 101 in the command.

Criteria #4: Permit packets from web client 65.5.5.5, sent to a web server in subnet 65.5.6.0/24

ACL command #4: _____

(A) access-list 101 permit tcp host 65.5.5.5 65.5.6.0 0.0.0.255 eq 23

(B) access-list 101 permit any any

(C) access-list 101 permit tcp host 65.5.5.5 65.5.6.0 0.0.0.255 eq www

(D) access-list 101 deny tcp host 65.5.5.5 65.5.6.0 0.0.0.255 eq www

Explanation 169. access-list 101 permit tcp host 65.5.5.5 65.5.6.0 0.0.0.255 eq www is the correct answer.

Criteria #4: Permit packets from web client 65.5.5.5, sent to a web server in subnet 65.5.6.0/24

ACL command #4: access-list 101 permit tcp host 65.5.5.5 65.5.6.0 0.0.0.255 eq www

Because extended ACLs can match so many different fields in the various headers in an IP packet, the command syntax cannot be easily summarized in a single generic command. However, the commands below summarize the syntax options.

access-list access-list-number **{deny | permit}** • protocol • source IP address • source-wildcard • destination IP address • destination-wildcard [log | log-input]

access-list access-list-number **{deny | permit} {tcp | udp}** protocol • source IP address • source-wildcard • [operator [port]] • destination IP address • destination-wildcard • [op-

erator [port]] [established] [log]

The configuration process for extended ACLs mostly matches the same process used for standard ACLs. You must choose the location and direction in which to enable the ACL, particularly the direction, so that you can characterize whether certain addresses and ports will be either the source or destination.

Configure the ACL using **access-list** commands, and when complete, then enable the ACL using the same **ip access-group** command used with standard ACLs. All these steps mirror what you do with standard ACLs; however, when configuring, keep the following differences in mind:

1. Place extended ACLs as close as possible to the source of the packets that will be filtered. Filtering close to the source of the packets saves some bandwidth.

2. Remember that all fields in one access-list command must match a packet for the packet to be considered to match that access-list statement.

3. Use numbers of 100–199 and 2000–2699 on the access-list commands; no one number is inherently better than another.

Question 170. Your task is to type a one-line extended ACL that matches the following criteria. All access-list commands use the number 101 in the command.

Criteria #5: Permit any and every IPv4 packet
ACL command #5: _____

(A) access-list 101 permit ip any any
(B) access-list 101 deny ip any any
(C) access-list 101 permit ip 0.0.0.0 any
(D) access-list 101 permit ip any 0.0.0.0

Explanation 170. **access-list 101 deny ip any any is the correct answer.**
Criteria #5: Permit any and every IPv4 packet
ACL command #5: access-list 101 deny ip any any

Question 171. Which of the following commands display the configuration of an IPv4 ACL, including line numbers? (Choose two answers.)
(A) show running-config
(B) show startup-config
(C) show ip access-lists
(D) show access-lists

Explanation 171. **show ip access-lists and show access-lists are the correct answers.**

The **show ip access-lists and show access-lists** commands both display the configuration of IPv4 access lists, including ACL line numbers.

Neither the **show running-config nor show startup-config** commands list the ACL line numbers; in this case, the startup-config file does not contain the ACL configuration at all.

Question 172. Type the access-list command that permits all packets sent from hosts in subnet 14.15.16.0/24. Use the ACL number 50 for the ACL rule.

(A) access-list 50 permit 14.15.17.0 0.0.0.255

(B) access-list 50 deny 14.15.16.0 0.0.0.255

(C) access-list 50 permit 14.15.16.0 0.255.255.255

(D) access-list 50 permit 14.15.16.0 0.0.0.255

Explanation 172. **access-list 50 permit 14.15.16.0 0.0.0.255 is the correct answer.** The command **access-list 50 permit 14.15.16.0 0.0.0.255** matches all the addresses from the subnet 14.15.16.0/24

The syntax of the ACL command is:

access-list access-list-number {deny | permit} source [source-wildcard]

Each standard numbered ACL has one or more access-list commands with the same number, any number from the ranges 1–99 and 1300–1999.

Besides the ACL number, each access-list command also lists the action (permit or deny), and the matching logic (the IP addresses to permit or deny). In this case, the ACL permits all the IP addresses from the subnet 14.15.16.0/24

The wildcard mask (**not subnet mask**) allows standard ACLs to match a range of addresses. Instead of typing:

access-list 50 permit 14.15.16.0
access-list 50 permit 14.15.16.1
access-list 50 permit 14.15.16.2
access-list 50 permit 14.15.16.3
...
...
access-list 50 permit 14.15.16.255

you can just use a wildcard mask to match all the addresses within that range **with a single** command.

Question 173. Given the following access-list command **access-list 2 permit 192.168.4.0 0.0.0.255**, choose the exact range of IP addresses, matched by the command.

(A) 192.167.4.0 – 192.168.4.255

(B) 192.168.4.0 – 192.168.5.255

(C) 192.168.4.0 – 192.168.4.255

(D) 192.0.0.0 – 192.168.4.255

Explanation 173. 192.168.4.0 – 192.168.4.255 is the correct answer. The wildcard mask 0.0.0.255 matches all packets that have the same first three octets. In this case, the ACL rule applies to the range:

192.168.4.0 - 192.168.4.255

Wildcard masks use two simple rules:

Rule #1. When the decimal is 0 then the router has to compare the octet.
Rule #2. When the decimal is 255 then the router has to ignore the octet.

In this case, we have to find the range of the network 192.168.4.0 matched by the command access-list 2 permit 192.168.4.0 0.0.0.255

As you can see the wildcard mask is 0.0.0.255 which means that the packets that come from the network 192.168.4 (firs three octets) have to be compared once reach the router, and the 0 (last octet) has to be ignored.

The process is as follow:
A packet with IP address 192.168.4.20 reaches the router. The router then starts asking (compare), are the first three octets of the packet 192.168.4?

If so, then there is a match (it's a match). If not, then there isn't a match.

A new packet with IP address 192.168.2.20 reaches the router. The router then starts asking (compare), are the first three octets of the packet 192.168.4?

If so, then there is a match. If not, then there isn't a match (it's not a match).

As a result, the exact range of IP addresses, matched by the command is: **192.168.4.0 - 192.168.4.255**
Question 174. The range of valid ACL numbers for standard numbered IP ACLs is:
(A) 1-99 and 1700 - 1999
(B) 1-99 and 1300 - 1999

(C) 1-101 and 1300 - 1999

(D) 1-49 and 1400 - 1999

Explanation 174. **1-99 and 1300 - 1999 is the correct answer.** The range of valid ACL numbers for **Standard numbered IP ACLs** is 1 – 99 and 1300 – 1999.

The range of valid ACL numbers for **Extended numbered IP ACLs** is 100 – 199 and 200 – 2699.

Question 175. The ACL 55 on R1 has four statements, in the following order, with address and wildcard mask values as follows:

1. 20.0.0.0 0.255.255.255

2. 20.20.0.0 0.0.255.255

3. 20.20.20.0 0.0.0.255

4. 2.2.2.0 0.0.0.255

If a router tried to match a packet sourced from IP address 20.20.20.20 using this ACL, which ACL statement does a router consider the packet to have matched?

(A) First statement

(B) Second statement

(C) Third statement

(D) Forth statement

(E) Implied deny at the end of the ACL

Explanation 175. **First statement is the correct answer.** The router always searches the ACL statements in order (from top to bottom) and stops trying to match ACL statements after a statement is matched. In other words, it uses **first-match logic**.

A packet with a source IP address 20.20.20.20 would match any of the first three explicitly configured commands described in the question. **As a result, only the first statement will be used.**

Question 176. Which of the following access-list denies packets with a UDP header, any source IP address with source port greater than 10455, a destination IP address 30.3.3.3 and a destination port equal to 25?

(A) access-list 101 deny udp any gt 10455 host 30.3.3.3 eq 28

(B) access-list 101 deny udp any gt 10455 host 30.3.3.3 eq 25

(C) access-list 101 deny tcp any gt 10455 host 30.3.3.3 eq 25

(D) access-list 101 deny udp any gt 25 host 30.3.3.3 eq 25

Explanation 176. **access-list 101 deny udp any gt 10455 host 30.3.3.3 eq 25 is the correct answer.** The configuration process for extended ACLs mostly matches the same process used for standard ACLs.

You must choose the location and direction in which to enable the ACL, particularly the direction, so that you can characterize whether certain addresses and ports will be either the source or destination.

Configure the ACL using access-list commands, and when complete, then enable the ACL using the same **ip access-group** command used with standard ACLs. All these steps mirror what you do with standard ACLs; however, when configuring, keep the following differences in mind:

Place extended ACLs as close as possible to the source of the packets that will be filtered. Filtering close to the source of the packets saves some bandwidth.

Remember that **all fields in one access-list command must match a packet** for the packet to be considered to match that access-list statement.

Use numbers of **100–199 and 2000–2699 on the access-list commands;** no one number is inherently better than another.

For example, the command access-list 101 deny udp any lt 10455 host 30.3.3.3 eq 25 uses 101 as a number for the access-list (you can use any number between 100–199 and 2000–2699), then deny all packets with udp headers from any IP source with source port less than (lt) 10455, a destination IP address 30.3.3.3 and a destination port equals to 25.

Hypothetical scenario: If a packet with UDP header uses a port 10456 (which is greater than 10455), going to host 30.3.3.3 with destination port equals to 25, then this packet it's not gonna be denied, because the packet uses a port greater than 10455. If the port was less than 10455 then the packet would be denied.

Question 177. Which of the following access-list denies packets with a UDP header, a source IP address 30.3.3.3 and a source port greater than 10455, any destination IP address 30.3.3.3 with destination port equal to 25?

(A) access-list 101 deny udp host 30.3.3.3 gt 10455 any eq 30

(B) access-list 101 deny udp host 30.3.3.3 gt 25 any eq 25

(C) access-list 101 deny udp host 30.0.0.0 gt 10455 any eq 25

(D) access-list 101 deny udp host 30.3.3.3 gt 10455 any eq 25

Explanation 177. access-list 101 deny udp host 30.3.3.3 gt 10455 any eq 25 is the correct answer.

Question 178. Choose the wildcard mask that matches all IP packets in the subnet 46.45.44.0, and mask 255.255.255.0.

(A) 0.0.0.255

(B) 0.0.255.255

(C) 0.255.255.255

(D) 255.255.255.255

Explanation 178. 0.0.0.255 is the correct answer.

The wildcard mask 0.0.0.255 matches all packets that have the same first three octets.

The wildcard mask is used to match a range of addresses and tells IOS to ignore parts of the address when making comparisons.

Wildcard masks use two simple rules:

1) When the decimal is 0 then the router has to compare the

octet.
2) When the decimal is 255 then the router has to ignore the octet.

In this case, we had to match the network 46.45.44.0 255.255.255.0
So, the network part is **46.45.44** which means we have to tell the router to compare the first three octets.

The wildcard mask **0.0.0.255** which is the correct answer tells the router to compare the first three octets and ignore the last octet.
If an upcoming packet has a source IP address **46.45.44.145**, then **there is** a match and we either permit or deny that packet based on the access control list rules.
If an upcoming packet has a source IP address **20.56.20.145**, then **there is not** a match and we either permit or deny that packet based on the access control list rules.

CHAPTER 9
WIRELESS NETWORKS

Questions 179-193

Question 179. When APs are placed at different geographic locations, they can all be interconnected by a switched infrastructure. The 802.11 standard calls this an extended service set (ESS).

(A) TRUE

(B) FALSE

Question 180. A lightweight access point in which one of the following architectures participate?

(A) Light-MAC

(B) Tunnel-MAC

(C) Big-MAC

(D) Split-MAC

Question 181. Which of the following controller ports is used to connect to a peer controller for high availability (HA) operation?

(A) Service port

(B) Distribution system port

(C) Redundancy port

(D) Console port

Question 182. Which of the following wireless security tools is used to protect the integrity of data in a wireless frame?

(A) MIC

(B) WIPS

(C) WEP

(D) EAP

Question 183. Wi-Fi is based on _____ IEEE standards.

(A) 802.2

(B) 802.1

(C) 802.12

(D) 802.11

Question 184. Which of the following bridges can be used to provide wireless connectivity to a non-wireless device?

(A) Wireless repeater

(B) Workgroup bridge

(C) Transparent bridge

(D) Adaptive bridge

Question 185. Which controller interface type maps a WLAN to a VLAN?

(A) Management interface

(B) Redundancy management

(C) Virtual interface

(D) Service port interface

(E) Dynamic interface

Question 186. Which is the most preferred and secure way of connecting to a WLC GUI to configure a new WLAN?

(A) SSH

(B) HTTP

(C) HTTPS

(D) FTP

(E) None of the above

Question 187. The maximum configurable number of WLANs on a controller is _____.

(A) 5

(B) 152

(C) 251

(D) 512

Question 188. Which of the following IEEE 802.11 Wi-Fi standards use the 5 GHz band? (Choose all that apply)

(A) 802.11

(B) 802.11b

(C) 802.11g

(D) 802.11a

(E) 802.11n

(F) 802.11ac

(G) 802.11ax

Question 189. Wi-Fi commonly uses the 2.5GHz and _____ GHz bands.

(A) 5

(B) 3

(C) 1

(D) 4

Question 190. Choose the term that best describes a Cisco wireless access point that operates in a standalone, independent manner.

(A) Standalone Access point (AP)

(B) Autonomous Access Point (AP)

(C) Independent Access Point (AP)

(D) Cisco Access Point (AP)

Question 191. You are creating a new WLAN with the controller GUI, which of the following parameters are necessary? (Choose two)

(A) VLAN number

(B) SSID

(C) Interface

(D) BSSID

(E) IP subnet

Question 192. Which one of the following is a wireless encryption method that is not recommended for use due to vulnerability issues?

(A) Advanced Encryption Standard (AES)

(B) Wi-Fi Protected Access (WPA)

(C) Wired Equivalent Privacy (WEP)

(D) Extensible Authentication Protocol (EAP)

Question 193. Which of the following IEEE 802.11 Wi-Fi standards use the 2.4 GHz band? (Choose all that apply)

(A) 802.11

(B) 802.11b

(C) 802.11g

(D) 802.11a

(E) 802.11n

(F) 802.11ac

(G) 802.11ax

Answers 179-193

Question 179. When APs are placed at different geographic locations, they can all be interconnected by a switched infrastructure. The 802.11 standard calls this an extended service set (ESS).

(A) TRUE

(B) FALSE

Explanation 179. **TRUE is the correct answer.**

Normally, one **AP cannot cover the entire area** where clients might be located. For example, you might need wireless coverage throughout an entire floor of a business, hotel, hospital, or other large building. To cover more area than a single AP's cell can cover, you simply need to add more APs and spread them out geographically.

When APs are placed at different geographic locations, they can all be interconnected by a switched infrastructure. **The 802.11 standard calls this an extended service set (ESS).**

The idea is to make multiple APs cooperate so that the wireless service is consistent and seamless from the client's perspective.

Question 180. A lightweight access point in which one of the following architectures participate?

(A) Light-MAC

(B) Tunnel-MAC

(C) Big-MAC

(D) Split-MAC

Explanation 180. **Split-MAC is the correct answer.**

On a lightweight AP, the MAC function is divided between the AP hardware and the WLC. The LAP-WLC division of labor is known as **split-MAC architecture**.

The **Split MAC architecture divides** the implementation of the MAC functions between the **AP and the controller.**

The 802.11 AP at its simplest level is the 802.11 radio MAC layer providing bridging to a wired network for the WLAN client associated to the AP Basic Service Set Identifier (BSSID).

The 802.11 standard extends the single AP concept to allow multiple APs to provide an extended service set (ESS), where multiple APs use the same ESS identifier (ESSID; commonly referred to as an SSID) to allow a WLAN client to connect to the same network through different APs.

The **LWAPP split MAC concept breaks** the APs making up the ESS into two component types: the LWAPP AP, and the WLC. These are linked via the LWAPP protocol across a network to provide the same functionality of radio services, as well as bridging of client traffic in a package that is simpler to deploy and manage than individual APs connected to a common network.

Note: Although the split MAC provides a Layer 2 connection between the WLAN clients and the wired interface of the WLC, this does not mean that the LWAPP tunnel passes all traffic; the WLC forwards only IP Ethertype and its default behavior is not to forward broadcast or multicast traffic. This becomes important when considering multicast and broadcast in the WLAN deployment.

Question 181. Which of the following controller ports is used to connect to a peer controller for high availability (HA) operation?

(A) Service port

(B) Distribution system port

(C) Redundancy port

(D) Console port

Explanation 181. **Redundancy port is the correct answer.**

Service port: Used for out-of-band management, system re-

covery, and initial boot functions; always connects to a switch port in access mode.

Distribution system port: Used for all normal AP and management traffic; usually connects to a switch port in 802.1Q trunk mode.

Console port: Used for out-of-band management, system recovery, and initial boot functions.

Redundancy port: Used to connect to a peer controller for high availability (HA) operation.

Question 182. Which of the following wireless security tools is used to protect the integrity of data in a wireless frame?

(A) MIC

(B) WIPS

(C) WEP

(D) EAP

Explanation 182. **MIC is the correct answer.**

A **message integrity check (MIC)** is a security tool that can protect against data tampering.

You can think of a MIC as a way for the sender to add a secret

stamp inside the encrypted data frame. The stamp is based on the contents of the data bits to be transmitted.

Once the recipient decrypts the frame, it can compare the secret stamp to its own idea of what the stamp should be, based on the data bits that were received.

If the two stamps are identical, the recipient can safely assume that the data has not been tampered with.

Question 183. Wi-Fi is based on _____ IEEE standards.

(A) 802.2

(B) 802.1

(C) 802.12

(D) 802.11

Explanation 183. **802.11 is the correct answer.**

The **IEEE 802.11** standard defines Wi-Fi, while **802.3** standard defines Ethernet.

Question 184. Which of the following bridges can be used to provide wireless connectivity to a non-wireless device?

(A) Wireless repeater

(B) Workgroup bridge

(C) Transparent bridge

(D) Adaptive bridge

Explanation 184. **Workgroup bridge is the correct answer.** A **workgroup bridge** acts as a wireless client, but bridges traffic to and from a wired device connected to it.

In workgroup bridge mode, the device associates to another access point as a client and provides a network connection for the equipment connected to its Ethernet port.

For example, if you need to **provide wireless connectivity** for a group of network printers, you can connect the printers to a hub or to a switch, connect the hub or switch to the access point Ethernet port, and configure the access point as a workgroup bridge. **The workgroup bridge associates to an access point on your network**

Question 185. Which controller interface type maps a WLAN to a VLAN?

(A) Management interface

(B) Redundancy management

(C) Virtual interface

(D) Service port interface

(E) Dynamic interface

Explanation 185. **Dynamic interface is the correct answer.**

Cisco controllers support the following interface types:

1. Dynamic interface: Used to connect a VLAN to a WLAN.

2. Management interface: Used for normal management traffic, such as RADIUS user authentication, WLC-to-WLC communication, web-based, and SSH sessions, SNMP, Network Time Protocol (NTP), syslog, and so on. The management interface is also used to terminate CAPWAP tunnels between the controller and its APs.

3. Redundancy management: The management IP address of a redundant WLC that is part of a high availability pair of controllers. The active WLC uses the management interface address, while the standby WLC uses the redundancy management address.

3. Virtual interface: IP address facing wireless clients when the controller is relaying client DHCP requests, performing client web authentication, and supporting client mobility.

4. Service port interface: Bound to the service port and used for out-of-band management.

Question 186. Which is the most preferred and secure way of connecting to a WLC GUI to configure a new WLAN?

(A) SSH

(B) HTTP

(C) HTTPS

(D) FTP

(E) None of the above

Explanation 186. **HTTPS is the correct answer.**

You can use either HTTP or HTTPS to access the GUI but the HTTPS method is most preferred because it is far more secure than HTTP as it uses TLS (SSL) to encrypt normal HTTP requests and responses.

The only difference between the **Hypertext Transfer Protocol (HTTP)** and **Hypertext transfer protocol secure (HTTPS)** protocols is that HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses. As a result, HTTPS is far more secure than HTTP.

Question 187. The maximum configurable number of WLANs on a controller is _____.

(A) 5

(B) 152

(C) 251

(D) 512

Explanation 187. **512 is the correct answer.**

The maximum configurable number of WLANs on a controller is **512**.

Question 188. Which of the following IEEE 802.11 Wi-Fi standards use the 5 GHz band? (Choose all that apply)

(A) 802.11

(B) 802.11b

(C) 802.11g

(D) 802.11a

(E) 802.11n

(F) 802.11ac

(G) 802.11ax

Explanation 188. **D, E, F, G is the correct answer.**

The following table provides all the needed information to answer any question either on the interview as a junior network engineer or for the CCNA 200-301 exam. Make sure to memorize it.

IEEE Standard	2.4 GHz	5 GHz	Max Data Rate

802.11	Yes	No	2 Mbps
802.11b	Yes	No	11 Mbps
802.11g	Yes	No	54 Mbps
802.11a	No	Yes	54 Mbps
802.11n	Yes	Yes	600 Mbps
802.11ac	No	Yes	6.93 Gbps
802.11ax	Yes	Yes	4x higher than 802.11ac

Question 189. Wi-Fi commonly uses the 2.4GHz and _____ GHz bands.

(A) 5

(B) 3

(C) 1

(D) 4

Explanation 189. **5 is the correct answer.** Wi-Fi commonly uses the 2.5GHz and 5GHz bands.

The **2.4GHz and 5GHz** refer to two different "bands" that the Wi-Fi can use for its signal. The biggest difference between the two is speed. Under ideal conditions, 2.4 GHz Wi-Fi will sup-

port up to 450 Mbps or 600 Mbps, while. 5 GHz Wi-Fi will support up to 1300 Mbps.

The **2.4 GHz band** is a pretty crowded place because it's used by more than just Wi-Fi. Old cordless phones, garage door openers, baby monitors, and other devices tend to use the 2.4 GHz band, and this can cause dropped connections and slower-than-expected speeds.

The **5 GHz band** is much less congested, which means you will likely get more stable connections. You'll also see higher speeds. On the other hand, the shorter waves used by the 5 GHz band makes it less able to penetrate walls and solid objects.

Question 190. Choose the term that best describes a Cisco wireless access point that operates in a standalone, independent manner.

(A) Standalone Access point (AP)

(B) Autonomous Access Point (AP)

(C) Independent Access Point (AP)

(D) Cisco Access Point (AP)

Explanation 189. **Autonomous Access Point is the correct answer.** An autonomous AP can operate independently without the need for a centralized wireless LAN controller.

An autonomous AP is self-contained; it is equipped with both wired and wireless hardware so that the wireless client associations can be terminated onto a wired connection locally at the AP.

Autonomous APs offer **one or more fully functional, standalone basic service sets (BSSs).** They are also a natural extension of a switched network, connecting wireless service set identifiers (SSIDs) to wired virtual LANs (VLANs) at the access layer.

An autonomous AP offers a short and **simple path for data** to travel between the wireless and wired networks. Data has to travel only through the AP to reach the network on the other side. Two wireless users that are associated with the same autonomous AP can reach each other through the AP without having to pass up into the wired network.

Question 191. You are creating a new WLAN with the controller GUI, which of the following parameters are necessary? (Choose two)

(A) VLAN number

(B) SSID

(C) Interface

(D) BSSID

(E) IP subnet

Explanation 191. **SSID and Interface are the correct answers.** The SSID and controller interface are the only parameters from the list that are necessary in order to create a new WLAN.

Question 192. Which one of the following is a wireless encryption method that is not recommended for use due to vulnerability issues?

(A) Advanced Encryption Standard (AES)

(B) Wi-Fi Protected Access (WPA)

(C) Wired Equivalent Privacy (WEP)

(D) Extensible Authentication Protocol (EAP)

Explanation 192. **Wired Equivalent Privacy (WEP) and Interface are the correct answers.** WEP is known to have a number of weaknesses and has been compromised. Therefore, it has been officially deprecated and should not be used in a wireless network.

Question 193. Which of the following IEEE 802.11 Wi-Fi standards use the 2.4 GHz band? (Choose all that apply)

(A) 802.11

(B) 802.11b

(C) 802.11g

(D) 802.11a

(E) 802.11n

(F) 802.11ac

(G) 802.11ax

Explanation 193. **A, B, C, E and G are the correct answers.** The following table provides all the needed information to answer any question either on the interview as a junior network engineer or for the CCNA 200-301 exam. Make sure to memorize it.

IEEE Standard	2.4 GHz	5 GHz	Max Data Rate
802.11	Yes	No	2 Mbps
802.11b	Yes	No	11 Mbps
802.11g	Yes	No	54 Mbps
802.11a	No	Yes	54 Mbps
802.11n	Yes	Yes	600 Mbps
802.11ac	No	Yes	6.93 Gbps

802.11ax	Yes	Yes	4x higher than 802.11ac

CHAPTER 10
IP SERVICES

Questions 194-203

Question 194. Examine the following show command output on a router configured for dynamic NAT:

— Inside Source
access-list 1 pool examsdigest
pool examsdigest: netmask 255.255.255.240
start 190.1.1.1 end 190.1.1.10
type generic, total addresses 10, allocated 10 (100%), misses 595

You are responsible to find out why users are not being able to reach the Internet.

(A) The cause is not related to dynamic NAT

(B) The command output does not provide any clue to identify the problem

(C) Dynamic NAT can't use Standard ACLs

(D) The NAT pool does not have enough entries to fulfill the user's requests

Question 195. Log messages may tell you about some events, either critical or not. To help you make sense of the importance of each message, IOS assigns each message a severity level. Which of the following severity level means **Warning - Warning condition?**

(A) 2

(B) 3

(C) 4

(D) 5

Question 196. Log messages may tell you about some events, either critical or not. To help you make sense of the importance of each message, IOS assigns each message a severity level. Which of the following severity level means **Informational: Informational message only?**

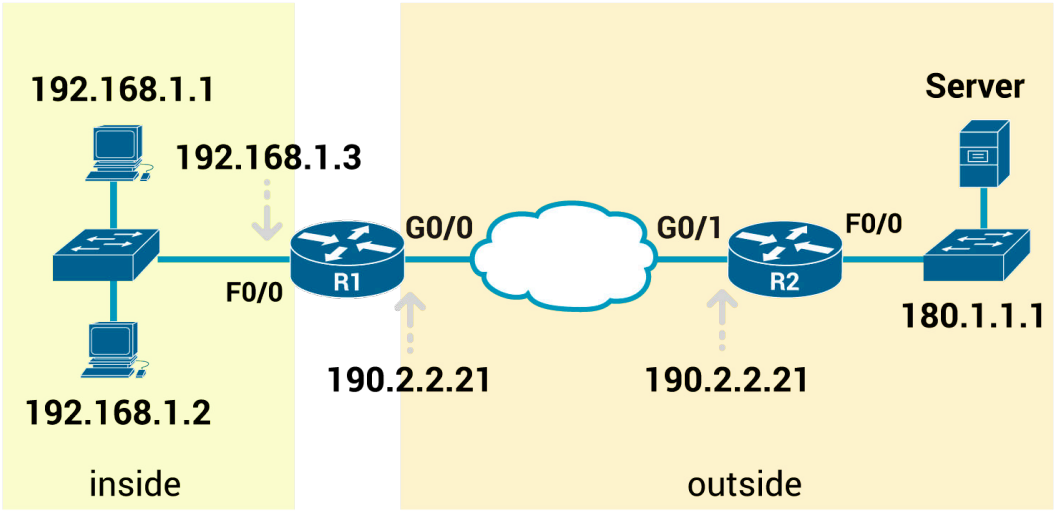
(A) 1

(B) 6

(C) 4

(D) 5

Question 197. Given the diagram below, complete the missing configuration command in order to make the static NAT functional.



Configuration snippet

R1# show running-config

! Lines omitted for brevity !

interface FastEthernet0/0

ip address 192.168.1.3 255.255.255.0

ip nat inside

interface GigabitEthernet0/0

ip address 190.2.2.21 255.255.255.0

ip _____ **(missing command)**

ip nat inside source static 192.168.1.2 200.1.1.2

ip nat inside source static 192.168.1.1 200.1.1.1

(A) nat source

(B) nat enable

(C) nat address

(D) nat outside

Question 198. One of the features of SNMPv3 is called message integrity.

(A) TRUE

(B) FALSE

Question 199. You have been tasked to find out whether the Cisco Discovery Protocol (CDP) is enabled globally. Which command will you type?

(A) show protocols

(B) show cdp

(C) show running-config

(D) show interface brief

Question 200. Which of the following protocols synchronize the time of different systems?

(A) NTP

(B) SMTP

(C) UDP

(D) CDP

Question 201. R1 and R2 are attached to the same Ethernet VLAN, with subnet 192.168.1.0/24, and addresses 192.168.1.1, 192.168.2 respectively. The routers use an FHRP. Host A and host B attach to the same LAN and have correct default router settings per the FHRP configuration. Which of the following

statements is true for this LAN?

(A) You can't connect two routers to the same LAN subnet.

(B) If one router fails, hosts can't send packets off-subnet

(C) If one router fails, both hosts will use the one remaining router as a default router

(D) if one router fails, only one of the two hosts will still be able to send packets off-subnet

Question 202. The snippet below is a Dynamic NAT configuration command?

```
ExamsDigestR1# show running-config
interface GigabitEthernet0/0
ip address 192.168.1.3 255.255.255.0
ip nat inside
interface Serial0/0/0
ip address 100.1.1.249 255.255.255.252 ip nat outside
ip nat inside source list 1 interface Serial0/0/0 overload
access-list 1 permit 192.168.1.2
access-list 1 permit 192.168.1.1
```

(A) TRUE

(B) FALSE

Question 203. Which of the following characteristics of network traffic can be managed by Quality of Service (QoS)?

(Choose all that apply)

(A) Bandwidth

(B) LLQ

(C) Loss

(D) Delay

(E) CoS

(F) Jitter

Answers 194-203

Question 194. Examine the following show command output on a router configured for dynamic NAT:

— Inside Source
access-list 1 pool examsdigest
pool examsdigest: netmask 255.255.255.240
start 190.1.1.1 end 190.1.1.10
type generic, total addresses 10, allocated 10 (100%), misses 595

You are responsible to find out why users are not being able to reach the Internet.

(A) The cause is not related to dynamic NAT

(B) The command output does not provide any clue to identify the problem

(C) Dynamic NAT can't use Standard ACLs

(D) The NAT pool does not have enough entries to fulfill the user's requests

Explanation 194. **The NAT pool does not have enough entries to fulfill the user's requests is the correct answer.** As

you can see, the last line mentions that the pool has ten addresses, with all ten allocated, with the misses counter 595, meaning that 595 new flows were rejected because of insufficient space in the NAT pool.

Question 195. Log messages may tell you about some events, either critical or not. To help you make sense of the importance of each message, IOS assigns each message a severity level. Which of the following severity level means **Warning - Warning condition?**

(A) 2

(B) 3

(C) 4

(D) 5

Explanation 195. **4 is the correct answer.** Log messages may tell you about some events, either critical or not.

To help you make sense of the importance of each message, IOS assigns each message a severity level: the lower the number, the more severe the event that caused the message.

The two top levels (**Emergency** and **Alerts**) are the most severe. Messages from this level mean a serious and immediate issue exists.

The next three levels (**Critical**, **Error**, and **Warning**), tell about events that impact the device, but they are not as immediate and severe. For instance, one common log message about an interface failing to a physically down state shows as a severity level 3 message.

IOS uses the next two levels (**Notification** and **Informational**) for messages that are more about notifying the user rather than identifying errors. The last level (**Debugging**) is used for messages requested by the **debug** command.

Numeral	Description
0	Emergency: System unusable
1	Alert: Immediate action needed
2	Critical: Critical condition—default level
3	Error: Error condition
4	Warning: Warning condition
5	Notification: Normal but significant condition
6	Informational: Informational message only

7	Debugging: Appears during debugging only

Question 196. Log messages may tell you about some events, either critical or not. To help you make sense of the importance of each message, IOS assigns each message a severity level. Which of the following severity level means **Informational: Informational message only?**

(A) 1

(B) 6

(C) 4

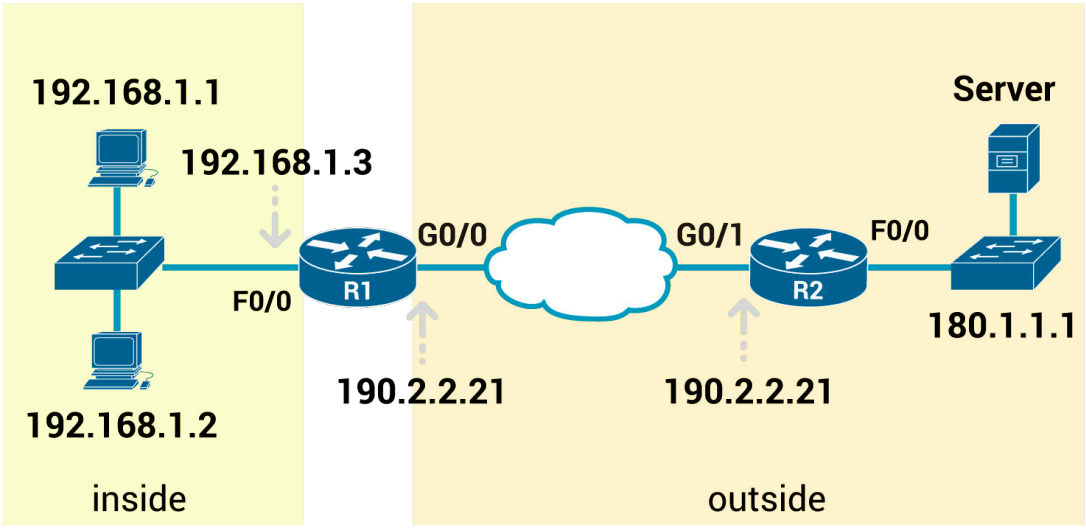
(D) 5

Explanation 196. **6 is the correct answer.**

Numeral	Description
0	Emergency: System unusable
1	Alert: Immediate action needed
2	Critical: Critical condition—default level
3	Error: Error condition
4	Warning: Warning condition

5	Notification: Normal but significant condition
6	Informational: Informational message only
7	Debugging: Appears during debugging only

Question 197. Given the diagram below, complete the missing configuration command in order to make the static NAT functional.



Configuration snippet

R1# show running-config

! Lines omitted for brevity !

interface FastEthernet0/0

ip address 192.168.1.3 255.255.255.0

ip nat inside

interface GigabitEthernet0/0

ip address 190.2.2.21 255.255.255.0

ip _____ **(missing command)**

ip nat inside source static 192.168.1.2 200.1.1.2

ip nat inside source static 192.168.1.1 200.1.1.1

(A) nat source

(B) nat enable

(C) nat address

(D) nat outside

Explanation 197. **nat outside is the correct answer.** The final configuration command should be like this:

```
interface FastEthernet0/0
ip address 192.168.1.3 255.255.255.0
ip nat inside
interface GigabitEthernet0/0
ip address 190.2.2.21 255.255.255.0
ip nat outside
ip nat inside source static 192.168.1.2 200.1.1.2
```

Static NAT configuration requires only a few configuration steps. Each static mapping between a local (private) address and a global (public) address must be configured.

In addition, because NAT may be used on a subset of interfaces, the router must be told on which interfaces it should use NAT. Those same interface subcommands tell NAT whether the interface is inside or outside. The specific steps are as follows:

Step 1. Use the ip nat inside command in interface configuration mode to configure interfaces to be in the inside part of the NAT design.

Step 2. Use the ip nat outside command in interface configuration mode to configure interfaces to be in the outside part of the NAT design.

Step 3. Use the ip nat inside source static inside-local inside-global command in global configuration mode to configure the static mappings.

Question 198. One of the features of SNMPv3 is called message integrity.

(A) TRUE

(B) FALSE

Explanation 198. **TRUE is the correct answer.** **Simple Network Management Protocol (SNMP)** is a way for different devices on a network to share information with one another. It allows devices to communicate even if the devices are different hardware and run different software.

Without a protocol like SNMP, there would be no way for network management tools to identify devices, monitor network performance, keep track of changes to the network, or determine the status of network devices in real-time.

Simple Network Management Protocol (SNMP) provides a message format for communication between what are termed, managers, and agents. An SNMP manager is a network management application running on a PC or server, with that host typically being called a **Network Management Station (NMS).**

As for the SNMP protocol messages, all versions of SNMP support a basic clear-text password mechanism, although none of those versions refer to the mechanism as using a password. SNMP Version 3 (SNMPv3) adds more modern security as well.

The following are SNMPv3 features:

1. Message integrity: This mechanism, applied to all SNMPv3 messages, confirms whether or not each message has been changed during transit.

2. Authentication: This optional feature adds authentication with both a username and password, with the password never sent as clear text. Instead, it uses a hashing method like many other modern authentication processes.

3. Encryption (privacy): This optional feature encrypts the contents of SNMPv3 messages so that attackers who intercept the messages cannot read their contents.

Question 199. You have been tasked to find out whether the Cisco Discovery Protocol (CDP) is enabled globally. Which command will you type?

(A) show protocols

(B) show cdp

(C) show running-config

(D) show interface brief

Explanation 199. **show cdp is the correct answer.** CDP discovers basic information about neighboring routers and switches without needing to know the passwords for the neighboring devices. To discover information, routers and switches send CDP messages out each of their interfaces.

The messages essentially announce information about the device that sent the CDP message. Devices that support CDP learn information about others by listening for the advertisements sent by other devices.

CDP discovers several useful details from the neighboring Cisco devices:

1. Device identifier: Typically the host name.
2. Address list: Network and data-link addresses.
3. Port identifier: The interface on the remote router or switch on the other end of the link that sent the CDP advertisement.
4. Capabilities list: Information on what type of device it is (for example, a router or a switch).
5. Platform: The model and OS level running on the device.

Question 200. Which of the following protocols synchronize the time of different systems?

(A) NTP
(B) SMTP
(C) UDP
(D) CDP

Explanation 200. NTP is the correct answer. NTP (network

time protocol) is a protocol for clock synchronization in computer systems.

NTP is a built-on UDP, where port 123 is used for NTP server communication and NTP clients use port 1023 (for example, a desktop). Unfortunately, like many legacy protocols, NTP suffers from security issues.

It is possible to spoof NTP packets, causing clocks to set to various times (an issue for certain services that run periodically). There are several cases of NTP misuse and abuse where servers are the victim of DoS attacks.

As a result, if clock synchronization is needed, it may be better to provide an internal NTP server (master clock) that synchronizes the remaining clocks in the internal network.

Cisco supplies two ntp configuration commands that dictate how NTP works on a router or switch, as follows:

ntp master {stratum-level}: NTP server mode—the device acts only as an NTP server, and not as an NTP client. The device gets its time information from the internal clock on the device.

ntp server {address | hostname}: NTP client/server mode—the

device acts as both client and server. First, it acts as an NTP client, to synchronize time with a server. Once synchronized, the device can then act as an NTP server, to supply time to other NTP clients.

Question 201. R1 and R2 are attached to the same Ethernet VLAN, with subnet 192.168.1.0/24, and addresses 192.168.1.1, 192.168.2 respectively. The routers use an FHRP. Host A and host B attach to the same LAN and have correct default router settings per the FHRP configuration. Which of the following statements is true for this LAN?

(A) You can't connect two routers to the same LAN subnet.

(B) If one router fails, hosts can't send packets off-subnet

(C) If one router fails, both hosts will use the one remaining router as a default router

(D) if one router fails, only one of the two hosts will still be able to send packets off-subnet

Explanation 201. **If one router fails, both hosts will use the one remaining router as a default router is the correct answer.** The use of an **FHRP** in this design purposefully allows either router to fail and still support off-subnet traffic from all hosts in the subnet. Both routers can attach to the same LAN subnet per IPv4 addressing rules.

FHRPs make this design work better. The two routers appear to be a single default router. The users never have to do anything: their default router setting remains the same, and their ARP table even remains the same.

To allow the hosts to remain unchanged, the routers have to do some more work, as defined by one of the FHRP protocols.

Generically, each FHRP makes the following happen:

1. All hosts act like they always have, with one default router setting that never has to change
2. The default routers share a virtual IP address in the subnet, defined by the FHRP
3. Hosts use the FHRP virtual IP address as their default router address
4. The routers exchange FHRP protocol messages so that both agree as to which router does what works at any point in time
5. When a router fails or has some other problem, the routers use the FHRP to choose which router takes over responsibilities from the failed router

The three FHRP protocols are:
1) Hot Standby Router Protocol (HSRP)
2) Virtual Router Redundancy Protocol (VRRP)

3) Gateway Load Balancing Protocol (GLBP)

Question 202. The snippet below is a Dynamic NAT configuration command?

```
ExamsDigestR1# show running-config
interface GigabitEthernet0/0
ip address 192.168.1.3 255.255.255.0
ip nat inside
interface Serial0/0/0
ip address 100.1.1.249 255.255.255.252 ip nat outside
ip nat inside source list 1 interface Serial0/0/0 overload
access-list 1 permit 192.168.1.2
access-list 1 permit 192.168.1.1
```

(A) TRUE

(B) FALSE

Explanation 202. **FALSE is the correct answer.** The configuration above is a PAT configuration **not Dynamic NAT**.

Port Address Translation (PAT) is another type of dynamic NAT that can map multiple private IP addresses to a single public IP address by using a technology known as Port Address Translation.

Here, when a client from inside network communicates to a host on the internet, the router changes the source port (TCP or UDP) number with another port number. These port mappings are kept in a table. When the router receives from the internet, it will refer to the table which keeps the port mappings and forward the data packet to the original sender.

The following checklist details the configuration when using an interface IP address as the sole inside global IP address:

Step 1.

As with dynamic and static NAT, configure the **ip nat inside** interface subcommand to identify inside interfaces.

Step 2.

As with dynamic and static NAT, configure the **ip nat outside** interface subcommand to identify outside interfaces.

Step 3.

As with dynamic NAT, configure an ACL that matches the packets entering inside interfaces.

Step 4.

Configure the **ip nat inside source list acl-number interface type/number overload** global configuration command, referring to the ACL created in step 3 and to the interface whose IP

address will be used for translations.

Question 203. Which of the following characteristics of network traffic can be managed by Quality of Service (QoS)? (Choose all that apply)

(A) Bandwidth

(B) LLQ

(C) Loss

(D) Delay

(E) CoS

(F) Jitter

Explanation 203. **A, C, D and F are the correct answers.** Cisco offers a wide range of QoS tools on both routers and switches. All these tools give you the means to manage four characteristics of network traffic:

1) Bandwidth
2) Delay
3) Jitter
4) Loss

Bandwidth refers to the speed of a link, in bits per second (bps).

Delay refers to the time between sending one packet and that same packet arriving at the destination host. Also, delay refers to the time between sending one packet and that same packet arriving at the destination host plus the time for the receiver of that packet to send back a packet.

Jitter is the variation in the latency on a packet flow between two systems, when some packets take longer to travel from one system to the other. Jitter results from network congestion, timing drift, and route changes.

Loss refers to the number of lost messages, usually as a percentage of packets sent.

CHAPTER 11
NETWORK DESIGN ARCHITECTURE

Questions 204-217

Question 204. The customer edge device is typically a router, that sits at a customer site on MPLS networks and connects to a provider edge router (PE router) to take communications from a customer site to a provider side.

(A) TRUE

(B) FALSE

Question 205. _____ is a network design that connects a link between each pair of nodes.

(A) Full Mesh

(B) Star

(C) Hybrid

(D) Partial Mesh

Question 206. With PoE, a LAN switch can act as the Power Sourcing Equipment (PSE).

(A) TRUE

(B) FALSE

Question 207. Which of the following protocols or technologies do you use each time you connect remotely through VPN?

(A) TLS

(B) IPsec

(C) SSH

(D) Telnet

(E) FTPS

Question 208. Which of the following roles of campus switches provides a connection point for end-user devices?

(A) Access

(B) Distribution

(C) Core

(D) Campus

Question 209. Which of the following roles of campus switches provides an aggregation point for access switches?

(A) Access

(B) Distribution

(C) Core

(D) Campus

Question 210. Which of the following roles of campus switches aggregates distribution switches in very large campus

LANs?

(A) Access

(B) Distribution

(C) Core

(D) Campus

Question 211. Your company plans to start using public cloud service and now you are considering different WAN options. Your main concern is security by keeping the data private while also providing good QoS services. Which of the following options are under consideration? (Choose two answers.)

(A) Using private WAN connections directly to the cloud provider

(B) Using an Internet connection without VPN

(C) Using an Internet connection with VPN

(D) Using an intercloud exchange

Question 212. One of the differences between Public Cloud and Private Cloud (On-Premise) is that on the Public Cloud solution you are responsible for all management, maintenance, and updating of data centers.

(A) TRUE

(B) FALSE

Question 213. A company uses a Metro Ethernet WAN with an Ethernet LAN (E-LAN) service, with the company headquarters plus 20 remote sites connected to the service. The enterprise uses OSPF at all sites, with one router connected to the service from each site. Which of the following are true about the Layer 3 details most likely used with this service and design? (Choose all that apply)

(A) The WAN uses one IP subnet

(B) The WAN uses 20 or more IP subnets

(C) A remote site router would have one OSPF neighbor

(D) A remote site router would have 20 OSPF neighbors

Question 214. The process of dividing a physical server into multiple unique and isolated virtual servers by means of a software application is called server _____.

(A) Integration

(B) Isolation

(C) Virtualization

(D) Segmentation

Question 215. Which cloud "As a Service" model is a form of cloud computing that delivers fundamental compute, network, and storage resources to consumers on-demand, over the internet, and on a pay-as-you-go basis?

(A) Software as a Service

(B) Platform as a Service

(C) Infrastructure as a Service

(D) Database as a Service

Question 216. Which cloud "As a Service" model is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet?

(A) Software as a Service

(B) Platform as a Service

(C) Infrastructure as a Service

(D) Database as a Service

Question 217. Which cloud "As a Service" model is a complete development and deployment environment in the cloud, with resources that enable you to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise applications?

(A) Software as a Service

(B) Platform as a Service

(C) Infrastructure as a Service

(D) Database as a Service

Answers 204-217

Question 204. The customer edge device is typically a router, that sits at a customer site on MPLS networks and connects to a provider edge router (PE router) to take communications from a customer site to a provider side.

(A) TRUE

(B) FALSE

Explanation 204. **TRUE is the correct answer.** The **customer** edge device is typically a router, that sits at a customer site on MPLS networks and connects to a provider edge router (PE router) to take communications from a customer site to a provider side.

Multi-protocol Label Switching (MPLS) is a protocol-agnostic routing technique designed to speed up and shape traffic flows across wide area- and service provider- networks. It's a way to insure reliable connections for real-time applications by establishing pre-determined, highly efficient routes.

MPLS users two important terms in context: **customer edge (CE)** and **provider edge (PE)**.

A CE router (customer edge router) is a router located on

the customer premises that provides an Ethernet interface between the customer's LAN and the provider's core network. CE routers, P (provider) routers and PE (provider edge) routers are components in an MPLS (multiprotocol label switching) architecture. Provider routers are located in the core of the provider or carrier's network.

Provider edge routers sit at the edge of the network. CE routers connect to PE routers and PE routers connect to other PE routers over P routers.

Question 205. _____ is a network design that connects a link between each pair of nodes.

(A) Full Mesh

(B) Star

(C) Hybrid

(D) Partial Mesh

Explanation 205. **Full Mesh is the correct answer.** Full Mesh is a network design that connects a link between each pair of nodes.

The networking world uses several common terms about LAN and WAN topology and design including these:

Star: A design in which one central device connects to several

others so that if you drew the links out in all directions, the design would look like a star with light shining in all directions.

Full mesh: For any set of network nodes, a design that connects a link between each pair of nodes.

Partial mesh: For any set of network nodes, a design that connects a link between some pairs of nodes, but not all. In other words, a mesh that is not a full mesh.

Hybrid: A design that combines topology design concepts into a larger (typically more complex) design.

Question 206. With PoE, a LAN switch can act as the Power Sourcing Equipment (PSE).

(A) TRUE

(B) FALSE

Explanation 206. **TRUE is the correct answer.** With **Power over Ethernet (PoE)**, some device, typically a LAN switch, acts as the Power Sourcing Equipment (PSE)—that is, the device that supplies DC power over the Ethernet UTP cable.

A device that has the capability to be powered over the Ethernet cable, rather than by some other power connector on the

device, **is called the Powered Device (PD).**

Question 207. Which of the following protocols or technologies do you use each time you connect remotely through VPN?

(A) TLS

(B) IPsec

(C) SSH

(D) Telnet

(E) FTPS

Explanation 207. **TLS is the correct answer.** The term remote access VPN, or client VPN, typically refers to a VPN for which one endpoint is a user device, such as a phone, tablet, or PC. In those cases, **Transport Layer Security (TLS)** is the more likely protocol to use. TLS is included in browsers and is commonly used to connect securely to websites.

Internet VPNs can provide important security features, such as the following:

Confidentiality (privacy): Preventing anyone in the middle of the Internet (man in the middle) from being able to read the data.

Authentication: Verifying that the sender of the VPN packet is

a legitimate device and not a device used by an attacker.

Data integrity: Verifying that the packet was not changed as the packet transited the Internet.

Anti-replay: Preventing a man in the middle from copying and later replaying the packets sent by a legitimate user, for the purpose of appearing to be a legitimate user.

To accomplish these goals, two devices near the edge of the Internet create a VPN, called a VPN tunnel.

Question 208. Which of the following roles of campus switches provides a connection point for end-user devices?

(A) Access

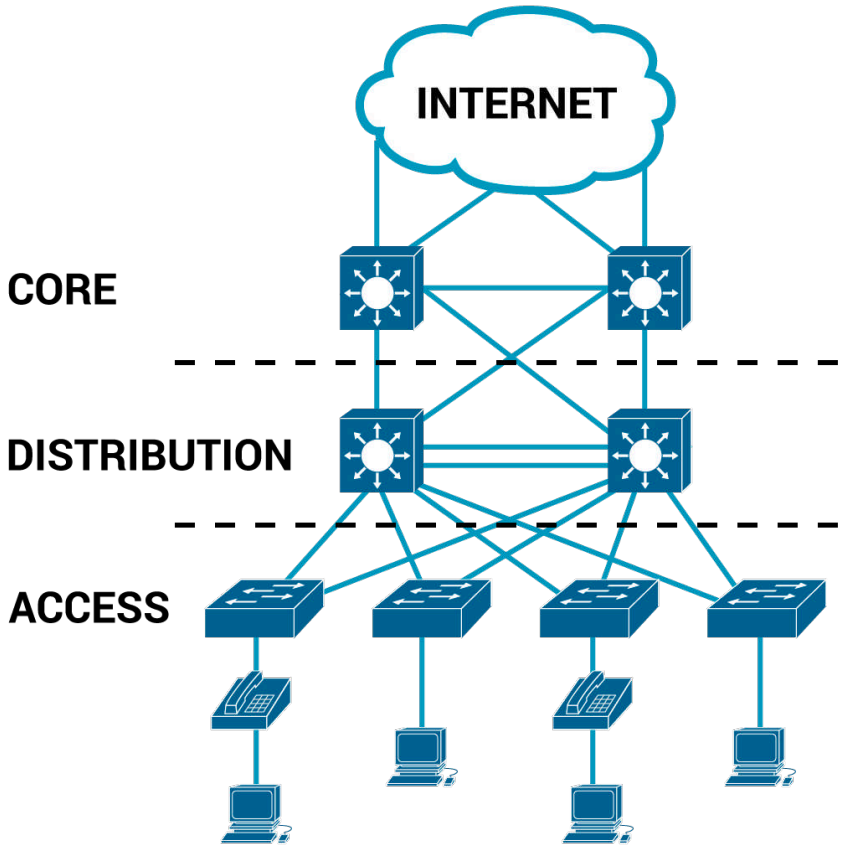
(B) Distribution

(C) Core

(D) Campus

Explanation 208. **Access is the correct answer.**

Access provides a connection point for end-user devices. Access does not forward frames between two other access switches under normal circumstances.



Question 209. Which of the following roles of campus switches provides an aggregation point for access switches?

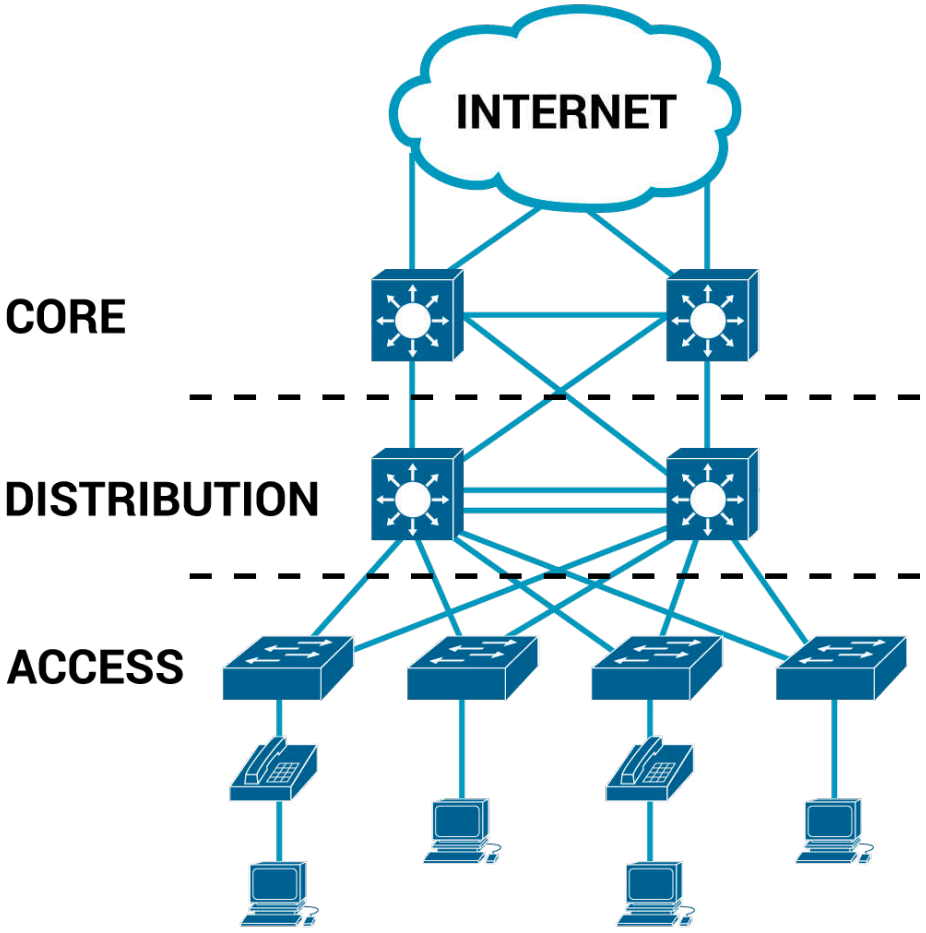
(A) Access

(B) Distribution

(C) Core

(D) Campus

Explanation 209. **Distribution is the correct answer.** **Distribution** provides an aggregation point for access switches, providing connectivity to the rest of the devices in the LAN, forwarding frames between switches, but not connecting directly to end-user devices.



Question 210. Which of the following roles of campus switches aggregates distribution switches in very large campus LANs?

(A) Access

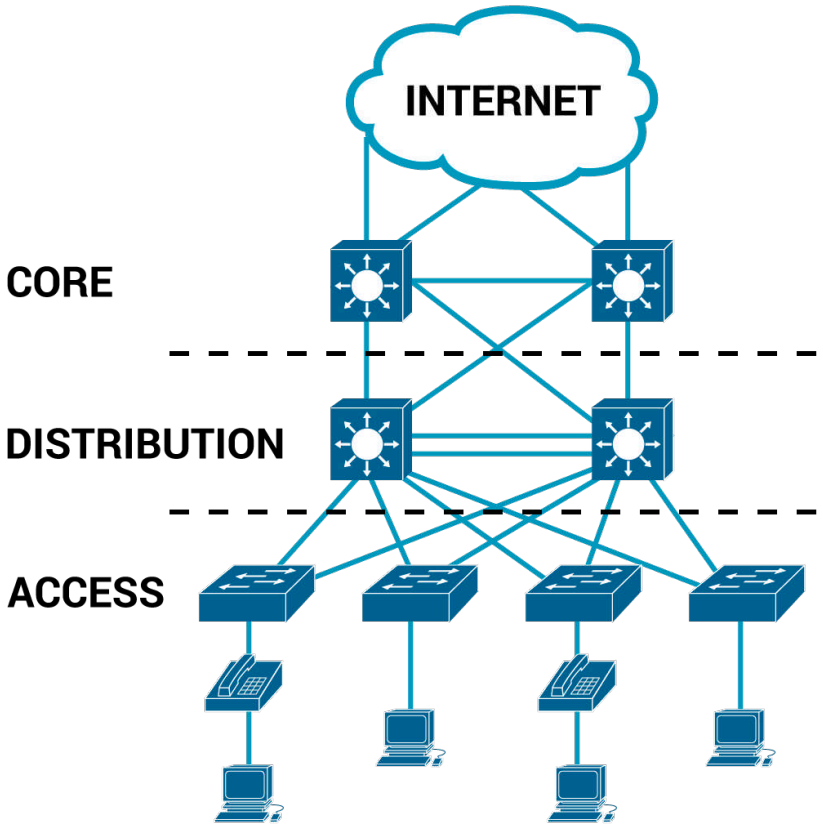
(B) Distribution

(C) Core

(D) Campus

Explanation 210. **Core is the correct answer.** **Core** aggregates distribution switches in very large campus LANs, provid-

ing very high forwarding rates for the larger volume of traffic due to the size of the network.



Question 211. Your company plans to start using public cloud service and now you are considering different WAN options. Your main concern is security by keeping the data private while also providing good QoS services. Which of the following options are under consideration? (Choose two answers.)

(A) Using private WAN connections directly to the cloud provider

(B) Using an Internet connection without VPN

(C) Using an Internet connection with VPN

(D) Using an intercloud exchange

Explanation 211. A and D are the correct answers. **Private WAN** options use technologies like Ethernet WAN and MPLS, both of which keep data private by their nature and which include QoS services.

Private WAN use technologies to transmit data between two or more locations, whilst prioritizing private internet traffic and avoiding public network to increase the level of security. Essentially it is a private network that allows a multi-sited business to share information, privately, with their own private internet.

An **intercloud exchange** is a purpose-built WAN service that connects to enterprises as well as most public cloud providers, using the same kinds of private WAN technology with those same benefits.

Intercloud exchange has come to be known as a company that creates a private network as a service. First, an intercloud exchange connects to multiple cloud providers on one side. On the other side, the intercloud connects to cloud consumers.

The pros is that you get the same benefits as when connecting with a private WAN connection to a public cloud, and the mi-

gration to a new cloud provider is easier.
The main con is that using an intercloud exchange introduces another company into the mix.

For the two incorrect answers, both use the Internet, so both cannot provide QoS services. The Internet VPN option does encrypt the data to keep it private.

Question 212. One of the differences between Public Cloud and Private Cloud (On-Premise) is that on the Public Cloud solution you are responsible for all management, maintenance, and updating of data centers.

(A) TRUE
(B) FALSE

Explanation 212. **FALSE is the correct answer.** A **Private Cloud (On-Premise)** solution, also known as an internal or enterprise cloud, resides on the company's hosted data center where all of your data is protected behind a firewall. However, the main drawback with a private cloud is that all management, maintenance and updating of data centers is the responsibility of the company.

On a **Public Cloud** solution, you aren't responsible for any of

the management. Your data is stored in the provider's data center and the provider is responsible for the management and maintenance of the data center.

This type of cloud environment is appealing to many companies because it reduces lead times in testing and deploying new products. However, the drawback is that many companies feel security could be lacking with a public cloud.

Question 213. A company uses a Metro Ethernet WAN with an Ethernet LAN (E-LAN) service, with the company headquarters plus 20 remote sites connected to the service. The enterprise uses OSPF at all sites, with one router connected to the service from each site. Which of the following are true about the Layer 3 details most likely used with this service and design? (Choose all that apply)

(A) The WAN uses one IP subnet

(B) The WAN uses 20 or more IP subnets

(C) A remote site router would have one OSPF neighbor

(D) A remote site router would have 20 OSPF neighbors

Explanation 213. **A and D are the correct answers.** An E-LAN service is one in which the **Metro Ethernet service** acts as if the WAN were a single Ethernet switch so that each device can communicate directly to every other device.

As a result, the routers sit in the same subnet.

With one headquarters router and 20 remote sites, **each router will have 20 OSPF neighbors.**

Question 214. The process of dividing a physical server into multiple unique and isolated virtual servers by means of a software application is called server _____.

(A) Integration
(B) Isolation
(C) Virtualization
(D) Segmentation

Explanation 214. **Virtualization is the correct answer.** The process of dividing a physical server into multiple unique and isolated virtual servers by means of a software application is called server virtualization. Each virtual server can run its own operating systems independently.

Key Benefits of Server Virtualization:

1. Higher server ability
2. Cheaper operating costs
3. Eliminate server complexity

4. Increased application performance

5. Deploy workload quicker

Without server virtualization, servers only use a small part of their processing power. This results in servers sitting idle because the workload is distributed to only a portion of the network's servers. Data centers become overcrowded with underutilized servers, causing a waste of resources and power.

By having each physical server divided into multiple virtual servers, server virtualization allows each virtual server to act as a unique physical device.

Each virtual server can run its own applications and operating system. This process increases the utilization of resources by making each virtual server act as a physical server and increases the capacity of each physical machine.

Question 215. Which cloud "As a Service" model is a form of cloud computing that delivers fundamental compute, network, and storage resources to consumers on-demand, over the internet, and on a pay-as-you-go basis?

(A) Software as a Service

(B) Platform as a Service

(C) Infrastructure as a Service

(D) Database as a Service

Explanation 215. **Infrastructure as a Service is the correct answer.** **Infrastructure as a Service (IaaS)** is a form of cloud computing that delivers fundamental compute, network, and storage resources to consumers on-demand, over the internet, and on a pay-as-you-go basis.

IaaS gives users cloud-based alternatives to on-premise infrastructure, so businesses can avoid investing in expensive on-site resources. With IaaS, you can buy what you need, as you need it, and purchase more as your business grows.

IaaS solutions are highly flexible and highly scalable, and you can replace it whenever you need without losing money on your initial investment.

IaaS examples: AWS EC2, Rackspace, Google Compute Engine (GCE), Digital Ocean

Question 216. Which cloud "As a Service" model is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet?

(A) Software as a Service

(B) Platform as a Service

(C) Infrastructure as a Service

(D) Database as a Service

Explanation 216. **Software as a Service is the correct answer.** **Software as a Service (SaaS)** is a software distribution model in which a third-party provider hosts applications and makes them available to customers over the Internet.

SaaS platforms make software available to users over the internet, usually for a monthly subscription fee. With SaaS, you don't need to install and run software applications on your computer (or any computer).

Everything is available over the internet when you log in to your account online. You can usually access the software from any device, anytime (as long as there is an internet connection).

SaaS examples: Google Apps, Salesforce, Dropbox, Slack.

Question 217. Which cloud "As a Service" model is a complete development and deployment environment in the cloud, with resources that enable you to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise applications?

(A) Software as a Service

(B) Platform as a Service

(C) Infrastructure as a Service

(D) Database as a Service

Explanation 217. Platform as a Service is the correct answer. Platform as a Service (PaaS) is a complete development and deployment environment in the cloud, with resources that enable you to deliver everything from simple cloud-based apps to sophisticated, cloud-enabled enterprise applications.

PaaS is primarily used by developers who are building software or applications. A PaaS solution provides the platform for developers to create unique, customizable software. This means developers don't need to start from scratch when creating applications, saving them a lot of time (and money) on writing extensive code.

PaaS is a popular choice for businesses who want to create unique applications without spending a fortune or taking on all the responsibility.

PaaS examples: Heroku, Apache Stratos, Magento Commerce Cloud.

CHAPTER 12
NETWORK AUTOMATION

Questions 218-230

Question 218. Which of the following configuration management tools uses agentless architecture for managing network devices?

(A) Ansible

(B) Puppet

(C) Chef

(D) Ansible and Puppet

(E) Puppet and Chef

Question 219. Given the following JSON object, how many object keys found in the sample below?

```
{ "response":
    { "id": "3",
        "name": "Cisco Catalyst",
        "ipAddress": {
            "private": "192.168.1.1",
            "public" : "156.157.1.1"
            }
```

```
    }
}
```

(A) 3

(B) 4

(C) 5

(D) 6

Question 220. CRUD is the acronym of the four primary actions performed by an application. What does CRUD stand for?

(A) Create, Read, Update, Delete

(B) Create, Read, Update, Done

(C) Create, Resolve, Update, Delete

(D) Create, Resolve, Update, Done

Question 221. A Layer 2 switch examines a frame's destination MAC address and forwards that frame out of the port G0/2. That action occurs as part of which plane of the switch?

(A) Data plane

(B) Management plane

(C) Control Plane

(D) None of the above

Question 222. Which answer correctly describes the format of the JSON text below? (Choose two answers)

(A) One JSON object that has one key:value pair

(B) One JSON object that has two key:value pairs

(C) One JSON object that has three key:value pair

(D) Two JSON objects that have two key:value pair

(E) A JSON object whose value is a second JSON object

Question 223. Identify the hostname part from the given URI: https://cluster.cisco.com/dna/intent/api/v1/business/sda/fabric?ipaddress=10.1.2.3.

(A) https://

(B) cluster.cisco

(C) cluster.cisco.com

(D) dna/intent/api/v1/business/sda/fabric

(E) ?ipaddress=10.1.2.3

Question 224. Which of the following features of Cisco DNA Center discovers the actual path the packets will take from the source to the destination based on the current forwarding tables?

(A) Encrypted traffic analysis

(B) Device 360 and Client 360

(C) Network time travel

(D) Path trace

Question 225. Which of the following features of Cisco DNA Center shows past client performance in a timeline for compar-

ison to current behavior?

(A) Encrypted traffic analysis

(B) Device 360 and Client 360

(C) Network time travel

(D) Path trace

Question 226. Which of the following features of Cisco DNA Center gives a comprehensive view of the health of the device?

(A) Encrypted traffic analysis

(B) Device 360 and Client 360

(C) Network time travel

(D) Path trace

Question 227. Which of the following features of Cisco DNA Center enables Cisco DNA to use algorithms to recognize security threats even in encrypted traffic?

(A) Encrypted traffic analysis

(B) Device 360 and Client 360

(C) Network time travel

(D) Path trace

Question 228. Your company decides to move away from manual configuration methods, making changes by editing centralized configuration files. The issues you are facing with non-centralized configuration files are:

1) You don't know who engineer made the changes in the configuration file.
2) You don't know the changes in the configuration file over time.
Which tool your company will use in order to solve these issues?

(A) Version Control System

(B) Version Control Configuration

(C) Version Control Change

(D) Version Control Edit

Question 229. One of the benefits of controller-based networks over traditional networks is that the configuration on the devices have fewer errors, and you spent less time troubleshooting the network.

(A) TRUE

(B) FALSE

Question 230. The _____ plane includes protocols that allow network engineers to manage the devices.

(A) Management

(B) Data

(C) Control

(D) Network

Answers 218-230

Question 218. Which of the following configuration management tools uses agentless architecture for managing network devices?

(A) Ansible

(B) Puppet

(C) Chef

(D) Ansible and Puppet

(E) Puppet and Chef

Explanation 218. **Ansible is the correct answer.** Agentless architecture means that the configuration management tools do not rely on any code (agent) running on the network device.

This is accomplished by communicating with the software that is already installed on the computer, including the operating system and natively installed components.

Ansible uses Agentless architecture and relies on features typical in network devices, namely SSH and/or NETCONF, to make changes and extract information.

Question 219. Given the following JSON object, how many object keys found in the sample below?

```
{
      "response": {
            "id": "3",
            "name": "Cisco Catalyst",
            "ipAddress": {
                  "private": "192.168.1.1",
                  "public" : "156.157.1.1"
                  }
            }
}
```

(A) 3

(B) 4

(C) 5

(D) 6

Explanation 219. **6 is the correct answer.** JSON defines variables as **key:value pairs**, with the key on the left of the colon (:) and always enclosed in double quotation marks, with the value on the right.

The keys are highlighted:

Key #1: "**response"**

Key #2: “**id**”

Key #3: “**name**”

Key #4: “**ipAddress**”

Key #5: “**private**”

Key #6: “**public**”

Question 220. CRUD is the acronym of the four primary actions performed by an application. What does CRUD stand for?

(A) Create, Read, Update, Delete

(B) Create, Read, Update, Done

(C) Create, Resolve, Update, Delete

(D) Create, Resolve, Update, Done

Explanation 220. **Create, Read, Update, Delete is the correct answer.** The software industry uses a memorable acronym CRUD, for the four primary actions performed by an application.

Those actions are:

Create: Allows the client to create some new instances of variables and data structures at the server and initialize their values as kept at the server.

Read: Allows the client to retrieve (read) the current value of

variables that exist at the server, storing a copy of the variables, structures, and values at the client.

Update: Allows the client to change (update) the value of variables that exist at the server.

Delete: Allows the client to delete from the server different instances of data variables.

Question 221. A Layer 2 switch examines a frame's destination MAC address and forwards that frame out of the port G0/2. That action occurs as part of which plane of the switch?

(A) Data plane

(B) Management plane

(C) Control Plane

(D) None of the above

Explanation 221. **Data plane is the correct answer.** A **Data plane** refers to the tasks that a networking device does to forward a message. In other words, anything to do with receiving data, processing it, and forwarding that same data—whether you call the data a frame, a packet, or, more generically, a message—is part of the data plane.

The **Control plane** refers to any action that controls the data

plane. Most of these actions have to do with creating the tables used by the data plane, tables like the IP routing table, an IP Address Resolution Protocol (ARP) table, a switch MAC address table, and so on. By adding to, removing, and changing entries to the tables used by the data plane, the control plane processes control what the data plane does.

The **Management plane** performs work that does not directly impact the data plane. Instead, the management plane includes protocols that allow network engineers to manage the devices.

Telnet and Secure Shell (SSH) are two of the most obvious management plane protocols.

To emphasize the difference with control plane protocols, think about two routers: one configured to allow Telnet and SSH into the router and one that does not. Both could still be running a routing protocol and routing packets, whether or not they support Telnet and SSH.

Question 222. Which answer correctly describes the format of the JSON text below? (Choose two answers)

(A) One JSON object that has one key:value pair

(B) One JSON object that has two key:value pairs

(C) One JSON object that has three key:value pair

(D) Two JSON objects that have two key:value pair

(E) A JSON object whose value is a second JSON object

Explanation 222. **B and E are the correct answers.**
JSON defines variables as **key:value pairs**, with the **key on the left** of the **colon (:)** and always enclosed in double quotation marks, with the **value on the right**.

The value of an object can be a simple **value, array or even another object.** The JSON object shown here includes two keys:

The first key is: "variable1"
The second key is: "var"
That means we have an object with a total of two keys, making the second answer correct.

The value in that **key:value pair** itself is a JSON object that contains another **key:value pair.**
The first key:value pair is: "variable1": { "var" :"1"}"
The second key:value pair is: "var" :"1"
That means we have an object with value a second object.

Question 223. Identify the hostname part from the given URI:
https://cluster.cisco.com/dna/intent/api/v1/business/sda/fabric?

ipaddress=10.1.2.3

(A) https://

(B) cluster.cisco

(C) cluster.cisco.com

(D) dna/intent/api/v1/business/sda/fabric

(E) ?ipaddress=10.1.2.3

Explanation 223. cluster.cisco.com is the correct answer. The URI for a REST API call uses a format of protocol://host-name/resource?parameters.

In this case:

protocol: HTTPS

hostname: cluster.cisco.com

resource: dna/intent/api/v1/business/sda/fabric

parameters: ipaddress=10.1.2.3

Question 224. Which of the following features of Cisco DNA Center discovers the actual path the packets will take from the source to the destination based on the current forwarding tables?

(A) Encrypted traffic analysis

(B) Device 360 and Client 360

(C) Network time travel

(D) Path trace

Explanation 224. Path trace is the correct answer.

Encrypted traffic analysis – Enables Cisco DNA to use algorithms to recognize security threats even in encrypted traffic.

Device 360 and Client 360 – Gives a comprehensive view of the health of the device.

Network time travel – Shows past client performance in a timeline for comparison to current behavior.

Path trace – Discovers the actual path packets would take from source to destination based on current forwarding tables.

Question 225. Which of the following features of Cisco DNA Center shows past client performance in a timeline for comparison to current behavior?

(A) Encrypted traffic analysis

(B) Device 360 and Client 360

(C) Network time travel

(D) Path trace

Explanation 225. Network time travel is the correct answer.

Encrypted traffic analysis – Enables Cisco DNA to use algo-

rithms to recognize security threats even in encrypted traffic.

Device 360 and Client 360 – Gives a comprehensive view of the health of the device.

Network time travel – Shows past client performance in a timeline for comparison to current behavior.

Path trace – Discovers the actual path packets would take from source to destination based on current forwarding tables.

Question 226. Which of the following features of Cisco DNA Center gives a comprehensive view of the health of the device?

(A) Encrypted traffic analysis

(B) Device 360 and Client 360

(C) Network time travel

(D) Path trace

Explanation 226. Device 360 and Client 360 is the correct answer.

Encrypted traffic analysis – Enables Cisco DNA to use algorithms to recognize security threats even in encrypted traffic.

Device 360 and Client 360 – Gives a comprehensive view of the health of the device.

Network time travel – Shows past client performance in a timeline for comparison to current behavior.

Path trace – Discovers the actual path packets would take from source to destination based on current forwarding tables.

Question 227. Which of the following features of Cisco DNA Center enables Cisco DNA to use algorithms to recognize security threats even in encrypted traffic?

(A) Encrypted traffic analysis

(B) Device 360 and Client 360

(C) Network time travel

(D) Path trace

Explanation 227. Encrypted traffic analysis is the correct answer.

Encrypted traffic analysis – Enables Cisco DNA to use algorithms to recognize security threats even in encrypted traffic.

Device 360 and Client 360 – Gives a comprehensive view of the health of the device.

Network time travel – Shows past client performance in a timeline for comparison to current behavior.

Path trace – Discovers the actual path packets would take from source to destination based on current forwarding tables.

Question 228. Your company decides to move away from manual configuration methods, making changes by editing centralized configuration files. The issues you are facing with non-centralized configuration files are:

1) You don't know who engineer the changes in the configuration file
2) You don't know the changes in the configuration file over time

Which tool your company will use in order to solve these issues?

(A) Version Control System
(B) Version Control Configuration
(C) Version Control Change
(D) Version Control Edit

Explanation 228. **Version Control System is the correct answer.** The version control system, applied to the centralized text files that contain the device configurations, automatically tracks changes.

That means the system can see which user edited the file, when, and exactly what change was made, with the ability to make comparisons between different versions of the files.

Question 229. One of the benefits of controller-based networks over traditional networks is that the configuration on the devices have fewer errors, and you spent less time troubleshooting the network.

(A) TRUE

(B) FALSE

Explanation 229. **TRUE is the correct answer.** A **network controller** is software that **orchestrates network functions.** It serves as an intermediary between the business and the network infrastructure. The organization enters their desired business objectives into the controller which in turn sets up the network to deliver on those objectives.

Network controllers do their jobs by:

1. Maintaining an inventory of devices in the network and their status.

2. Automating device operations such as configurations and image updates resulting in more consistent device configuration, **fewer errors, and less time spent troubleshooting the network.**

3. Analyzing network operations, identifying potential issues,

and suggesting remediations.

4. Providing a platform for integration with other applications such as reporting systems.

Question 230. The _____ plane includes protocols that allow network engineers to manage the devices.

(A) Management

(B) Data

(C) Control

(D) Network

Explanation 230. **Management is the correct answer.** The management plane includes protocols that allow network engineers to manage the devices.

Telnet and Secure Shell (SSH) are two of the most obvious management plane protocols. To emphasize the difference with control plane protocols, think about two routers: one configured to allow Telnet and SSH into the router and one that does not.

Both could still be running a routing protocol and routing packets, whether or not they support Telnet and SSH.

THE END

Enrich your online experience with Exams-digest.

Your purchase of this product includes free access to all 230+ practice questions online and much more at examsdigest.com. You will have access for one (1) month. You may also access our full library of Practice exams and share with other learners. Send us an email to info@examsdigest.com now and start your online practice experience!

Examsdigest includes:

✓ Access to 1000+ Questions

✓ Access to 150+ Quizzes

✓ 6+ Certification Paths

✓ 24/7 Support

✓ Interactive Interview Questions

✓ Access on the go

About examsdigest.

Examsdigest started in 2019 and haven't stopped smashing it since. Examsdigest is a global, education tech-oriented company that doesn't sleep. Their mission is to be a part of your life



transformation by providing you the necessary training to hit your career goals.