
## National Security Agency (NSA) / Central Security Service (CSS)

# COMPUTER NETWORKING TEST

# PREPARATION GUIDE

## OVERVIEW

This preparation guide is intended to help you prepare for the Computer Networking Test (CNT). The CNT is a multiple-choice test assessing your knowledge of computer networking. The knowledge assessed through the CNT is required of individuals entering into certain Agency jobs. The CNT content is grouped into five areas: *Fundamentals & Theory of Computing*, *Networking, Operating Systems, Programming – Scripting and Interpreted, and Security*.

## CONTENT AREAS

### Fundamentals and Theory of Computing

This content area refers to the fundamentals and theory behind computer design, networking, and entry level computing concepts. This includes knowledge of types of basic computer components, CPU architectures, and OS concepts.

*Examples of specific content that would compose this content area include:*

a. Math numbering systems & conversions (e.g., binary, decimal, hex)
b. Computer concepts (e.g., CPU architectures, endianness, virtualization)
c. Basic knowledge of memory organization and layout
    i. Basic knowledge of offsets and lengths
d. Storage concepts (e.g., hard disk drive, solid state drive)
e. Differences between kernel and user space

### Networking

This content area is comprised of two knowledge areas, Network Design Fundamentals and Networking Applications and Services.

Network Design Fundamentals includes knowledge of the operation, management, and maintenance of computer networks, protocols and standards and how they integrate with one another. Knowledge of the rules, conventions, and data structure that govern how computers and network components/devices exchange information over a network. It also includes uses and types of computer network hardware (including routers, switches, and firewalls) as well as foundational knowledge needed to understand networking

*Examples of specific content that would compose this content area include:*

a. IP / subnetting
b. Ethernet
c. Routing
d. Lower level protocols & standards and how they integrate with one another
e. Layout & Design (network topology)
    i. LAN
    ii. WAN
f. How a packet transits a network and how the packet is modified as it transits a network with regard to OSI model layer 2-4 (e.g., packet routing, encapsulation, steps required to resolve associated addresses).
g. Concept of open and closed ports including associated flags.
h. TCP/IP 3 way handshake.
i. Networking device concepts [e.g., switches, routers, firewalls, intrusion detection systems (IDS), VLAN]

Networking Applications and Services refers to network facing functions on a computer system. This content includes knowledge of network services and their administration. This content should not be dependent on OS specific syntax.

*Examples of specific content that would compose this content area include:*

a. Description, protocols, and ports for standard network services (e.g., FTP, DNS, DHCP, ARP, SSH, HTTP, Telnet, Kerberos)
b. Network services and ports on a standard Window/Unix install (e.g., RPC, NetBIOS, NFS, Kerberos)
c. Interpreting the output from network related commands (e.g., netstat, ip/ifconfig, route, iptables)
d. Network service administration and configuration
e. Encryption fundamentals (e.g., public/private key, asymmetric encryption, symmetric encryption)

**Operating Systems**
This content area refers to knowledge of Computer systems administration, software interactions, and I/O interactions. Knowledge in this category is required in either Windows or Unix implementations.

*Examples of specific content that would compose this content area include:*

a. Understanding of standard administrative commands and the interpretation of output. (e.g., ps, tasklist, netstat, ifconfig, ipconfig )
b. Local system configurations (ifconfig, host file, logging)
c. Data security & integrity concepts (e.g., hashing, encryption)
d. Antivirus concepts: signature vs. heuristics
e. Data integrity protection concepts (e.g., tripwire, windows file protection)
f. Knowledge of different shells (e.g., cmd, bash, wmic )
g. Shell usage (e.g., i/o, process control , variables, operators, substitution, shell expansion)
h. Know how to research commands and command syntax
i. Hard drive partitioning and layout (file system basics)
j. Navigating the Unix file system via the command line and performing routine tasks. (e.g., file modification, output redirect)
k. Navigating the Windows file system via the command line and performing routine tasks. (e.g., file modification, output redirect)
l. Basic knowledge of Windows registry organization and structure
m. Basic knowledge of creating and changing registry values via command line or GUI
n. Basic knowledge of software/code signing
o. Basic knowledge of what a device driver is
p. Basic understanding of Unix, Linux and windows services and configuration locations.
q. Knowledge of executable file types & extensions on Windows and Unix.

**Programming – Scripting and Interpreted**
This content area refers to knowledge of reading and interpreting scripts/code and a basic understanding of programming concepts. Includes PERL, Python, Shell (bash/power), JAVA, C, C++, etc.

*Examples of specific content that would compose this content area include:*

a. Basic knowledge of shell scripting (e.g., cmd, wmic, bash)
b. Basic knowledge of interpreted languages (e.g., PERL, Python)
c. Interpreting source code and scripts (e.g., Flow, variables, loops)

**Security**

This content area involves knowledge of malware, botnets, rootkits, security products, host analysis, and general network vulnerability.

*Examples of specific content that would compose this content area include:*

a. Classes of malware and their key features of abilities
b. Noise signatures from various malware and how they can affect ability to operate remotely
c. Identification of malicious programs on remote hosts
d. Observable fingerprints of malware
e. Types of rootkits, their methods of infection, privilege levels, and methods for detection
f. Built-in security mechanisms for both UNIX and Windows operating systems
g. Capabilities and use of security products
h. Network monitoring applications and products
i. Network vulnerabilities

## PRACTICE TEST

To help you prepare for the CNT, the NSA/CSS has included a short practice test containing four questions similar to those on the actual test. Read each question, determine which of the four options represents the correct answer, and record your answer in the space provided. Continue until you have recorded your answers for all four questions on the practice CNT. Once you are done, look at the next section and compare your answers to the answers and explanations that we have provided for you. *Although it may be tempting to check an answer before completing the entire practice test, you will receive the most benefit from the practice situations if you answer all questions first.*

## TEST TAKING TIPS

Before starting the practice CNT, review these test taking tips:

1. Read each question carefully before determining the correct response.
2. Answer all questions even if you are unsure which option represents the correct answer. You are not penalized for incorrect responses.
3. Finally, take time to study the explanation for each of the questions/answers very carefully. This will help you fine-tune your reasoning on the actual test.

**INSTRUCTIONS**

This practice test includes 4 questions similar to those included on the computer networking test administered as part of the selection process. Read each question carefully and enter the letter associated with the option that represents the best response in the space provided.

___ **1.** Given that the only values A, B, and C can hold are 0 or 1, simplify the following binary logic problem: ((A OR B) AND (!A OR C)) AND !C

A. !A OR B AND !C
B. A AND B AND C
C. !A AND B AND !C
D. A OR B AND C

___ **2.** Which routing protocol has an administrative distance of 120?

A. OSPF
B. EIGRP
C. BGP
D. RIP

___ **3.** Which version of Windows first adopted Kerberos as an authentication policy?

A. Windows Server 2000
B. Windows Server 2003 R2
C. Windows NT
D. Windows Server 2008

___ **4.** Based on the script and output, what search algorithm is being used?

```
list = [1,2,3,4,5,6,7,8,9]
find = 6
test = False

while not test:
  list_length = len(list) / 2
  print list[list_length]
  if (list[list_length]) == find:
    test = True
  elif (list[list_length]) < find:
    list = list[list_length:]
  elif (list[list_length]) > find:
    list = list[:list_length]
```

Output:
5
7
6

A. interpolation
B. binary
C. linear
D. sequential

# NSA COMPUTER NETWORKING TEST: PRACTICE TEST ANSWERS AND EXPLANATIONS

**1.** The correct answer is **C**

This is a step by step process requiring knowledge of binary logic problems, a fundamental when it comes to computer and networking theory. The problem breaks down to:

(A OR B) AND (!A OR C) = !A*A + A*C + !A*B + B*C = A*C + !A*B +B*C
Then,
(A*C + !A*B +B*C) AND !C = A*C*!C + !A*B*!C + B*C*!C = !A*B*!C

In the above rational, * equates to AND and + equates to OR. ! indicates a NOT value, and a !A*A = 0. This is why that removes terms from the problem when next to ORs. The other options are flawed versions of the correct answer – they are mathematical errors.

**2.** The correct answer is **D**

The correct answer is “D” because RIP has an administrative distance of 120. OSPF is incorrect because it has an administrative distance of 110. EIGRP is incorrect because it has an administrative distance of 90. BGP is incorrect because it has an administrative distance of 200.

**3.** The correct answer is **A**

Originally developed by MIT in the 1980s, Kerberos was adapted by most Unix-based operating systems as the preferred authentication method by the late 1980s. Microsoft adopted the Kerberos authentication policy as the default authentication method with the release of its Windows Server 2000 operating system.

**4.** The correct answer is **B**

The script works by cutting the list in half, comparing that value to what is being searched for and then splitting the list in half. The next half is determined based on whether the returned value is less than or greater than the value being searched for. In this stem the first value returned is 5, which is less than 6 so the lower half of the list is cut. The next iteration returns 7, which is greater than 6 so that upper half is cut. The final iteration returns 6, which is a match and the loop is escaped through a bool named ‘test’. The other response options are often compared search algorithms that differ in functionality.