Internetwork Training

The Free
CCNA Study Guide

Please consider the environment before printing this document

Introduction

We decided to put together this free CCNA study guide after we received a large number of requests from our visitors for free CCNA training.

Whilst it is quite feasible that you could pass using just the information and links contained within this free guide, it is more of an introduction to the CCNA course, for you to evaluate whether the CCNA is right for you.

At the time of writing, the CCNA exam costs US $250, it is not an easy exam to pass, if you try and sit the exam without structured training you might as well send us a cheque for $250.

If you want ensure you learn the whole CCNA syllabus, including Cisco IOS configuration and troubleshooting (not covered in this guide), as well as making your study time easier and more enjoyable, while increasing your chances of passing the exam, enroll on our CCNA Bootcamp and get first class video training online for an unbeatable price!

Early Networking

Before networks existed people used to share files by sneakernet, basically passing floppy disks to one another. It wasn't long before the Local Area Network was born, which enabled network hosts to communicate with each other via hubs by installing network interface cards.
Each network host has a physical address, known as the MAC address and logical address, known as the IP address. When hosts are connected to a hub, they are in the same collision and broadcast domain. Network switches do a similar job to hubs, however they break up collision domains making a LAN more efficient.

LANs link hosts together in small areas such as offices and schools. To communicate between LANs they must be connected to Wide Area Networks (WANs) using routers.

The internet is the biggest WAN and uses the Domain Name System to translate domain names into IP addresses that networking devices understand and communicate with.
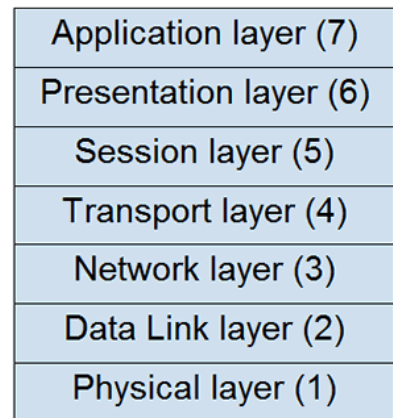
The OSI model

The Open Systems Interconnection (OSI) model is a standard model used in networking to abstract the processes involved in network communication. It consists of seven layers:
The Application layer, Presentation layer, Session layer, Transport layer (which uses flow control and acknowledgements), the Network layer, the Data link layer and the Physical layer.
Each layer has its own protocol data unit which encapsulates the data received from the upper layers.

The OSI model is fundamental to networking theory and troubleshooting, so make sure you understand and memorize what is happens at each layer.

Application layer (7)
Presentation layer (6)
Session layer (5)
Transport layer (4)
Network layer (3)
Data Link layer (2)
Physical layer (1)

The TCP/IP model

The TCP/IP protocol suite is the closest implementation of the OSI model there is, it consists of only four layers. The Application layer, Transport layer, Internet layer and Link layer.
There are a lots of similarities between the OSI model and the TCP/IP model.

The transport layer contains a reliable protocol called TCP and an unreliable protocol called UDP. To enable the transport layer to allow multi-protocol communication between hosts it uses port numbers.

The network layer features the routed protocol called IP protocol and Internet Control Message Protocol (ICMP).

TCP/IP Model
Application
Transport
Internet
Network Access
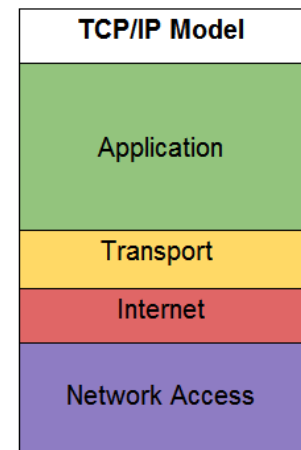
TCP/IP Protocols

The TCP/IP suite contains lots of protocols that operate at various layers, including Telnet, FTP, TFTP, NFS, POP, SMTP, SNMP, DNS, DHCP, TCP, UDP, IP, ICMP, ARP and RARP. You will need a good understanding of each of these protocols.

Binary and Hexadecimal Numbering Systems

The binary numbering system is the numbering system natively used by computers.
Binary consists of ones and zeros. A single one or zero is called a bit. A byte is eight bits, and a nibble is just four bits.
The hexadecimal numbering system is used for network addressing in IP version 6.

You need to be familiar with converting between decimal, hexadecimal and binary for the exam.

Local Area Networks (LANs)

A Local Area Network (LAN) is a computer network within a office, school or home.
LANs can have different network topologies and different cabling types such as UTP category 5, single mode fiber, and multi-mode fiber. Some cables are susceptible to crosstalk and/or electromagnetic interference.
Ethernet is the most common type of LAN today, it is defined by the IEEE 802.3 standard and uses the Ethernet frame, it is a broadcast transmission technology which means frame collisions can occur, which are dealt with by Carrier Sense Multiple Access with Collision Detection (CSMA/CD).

Ethernet cabling standards are defined by the TIA/EIA standards.
Ethernet was originally a half-duplex technology, but can now be either full or half-duplex.
Network devices are connected together using either crossover or straight-through cables depending on the devices you are connecting together.

Cisco Hierarchical Model

Cisco developed a three-layer model to help network engineers design efficient and scalable networks. It has three layers. The core, distribution and access layer.
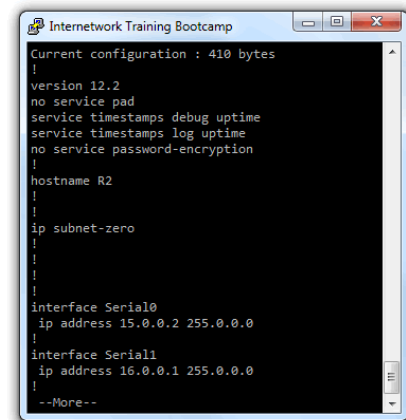
CORE

DISTRIBUTION

ACCESS
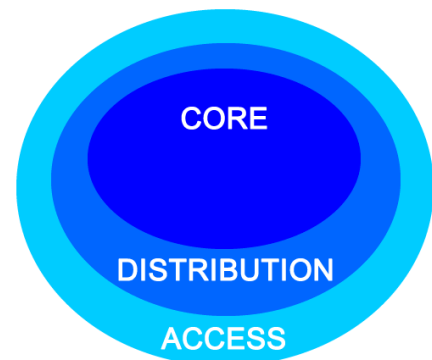
Cisco IOS

Cisco IOS is the operating system software used on most Cisco routers and switches.
It features an IOS command line interface used to configure the devices.

You will need to learn IOS configuration and troubleshooting to pass your CCNA exam.

```
Internetwork Training Bootcamp
Current configuration : 410 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname R2
!
ip subnet-zero
!
!
!
interface Serial0
 ip address 15.0.0.2 255.0.0.0
!
interface Serial1
 ip address 16.0.1 255.0.0.0
!
--More--
```

IP Addressing

Each network device requires a logical layer 3 IP address to be able to communicate over the network. IP version 4 addresses use dotted decimal notation and consist of 4 octets.
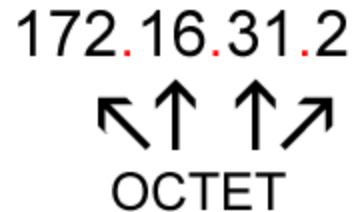
There are three different classes of IP address. A, B, C, and each class has its own private IP address range for use within a LAN, which are not routable over WANs.

There are also a number of reserved IP addresses that are reserved for special purposes.
For example: the IP address 127.0.0.1 is called the loopback address and is used to troubleshoot the TCP/IP stack on a host.

Subnetting

Subnetting is the process of dividing an IPv4 network into a number of smaller subnetworks.
A subnet mask is used by network hosts to determine the subnet. CIDR notation is often used to abbreviate the subnet mask.

You will need to know how to subnet a network using a pen and paper in the exam.

Our premium account includes our excellent **Subnetting Made Easy eBook** which will help you learn how to subnet, sign-up here!

IP Version 6

IP version 6 is the next version of Internet Protocol. It was created to solve the problem of diminishing available IPv4 addresses due to the exponential increase in the number of the devices connected to the internet.

IPv6 addresses are expressed in hexadecimal, and devices can send unicast, multicast and anycast datagrams, but not broadcasts.

IPv6 uses newer versions of DHCP and ICMP (DHCPv6 and ICMPv6).

Layer 2 Switching

Layer 2 switches improve network performance by reducing the size of collision domains, resulting in less collisions on the network. Switches and bridges use MAC addresses to reduce traffic on the network by only sending frames to the network segments which contain the destination hosts. In contrast, hubs repeat the frames out all ports.

Switches can use three different types of switching techniques, Cut-through, store-and-forward and fragment free.

The Spanning Tree Protocol (STP)

The Spanning Tree Protocol is used to prevent switching loops from causing problems on a switched network. Switching loops are caused when redundant links are added to a network to provide resilience. STP is defined by the IEEE 802.1D standard.

Virtual LANs (VLANs)

Virtual LANs are logical LANs created on existing hardware. They allow traffic and users on a LAN to be logically grouped together. VLANs can be shared between multiple switches by using VLAN trunking, enabling users to be grouped by function regardless of their physical location. VLAN trunking can be implemented on trunk ports using either IEEE 802.1Q and Cisco ISL trunking protocols.
Management of VLANs can then be centralized using a VLAN Management Policy Server.

EtherChannel is a method of creating redundant high-bandwidth logical trunk links between switches.

Voice over IP (VoIP)

Voice over IP (VoIP) is a set of technologies enabling voice communications over IP networks.
Quality of Service and Class of Service are used to prioritize voice traffic to enhance the call quality.

Routing

Routing is the process of determining the best path to forward layer 3 packets to their destination.

Routers use dynamic routing to choose the best route through the internetwork, these routes update automatically when the network changes by using routing protocols. Administrators can also configure static and default routes.
Each routing protocol has an administrative distance and metrics such as hop count to help the router to determine the best route.
Routing protocols can be categorized as either distance vector, link state or hybrid.

Be sure you know the difference between routed and routing protocols!

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a distance vector routing protocol that uses the Bellman-Ford algorithm to determine the best route to forward packets.
RIP is an interior gateway protocol that uses hop count as its only metric. It also uses Split

Horizon and poison reverse to prevent routing loops. There are two versions of RIP, RIPv1 is a classful routing protocol, whereas RIPv2 is classless.

Enhanced Interior Gateway Routing Protocol (EIGRP)

Enhanced Interior Gateway Routing Protocol (EIGRP) is a Cisco proprietary routing protocol which uses a number of metrics, and an algorithm called the Diffusing Update Algoithm (DUAL) to make its routing decisions. Cisco refers to EIGRP as a hybrid routing protocol because it has characteristics of both Distance Vector and Link State routing protocols.

Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is a non-proprietary Link-State interior gateway routing protocol operating in a single autonomous system, it uses the Dijkstra algorithm.

Wireless LAN (WLAN)

WLAN is a set of technologies defined by the IEEE 802.11 standard that enable wireless network access. WLAN can operate in either ad-hoc mode or infrastructure mode using a wireless access point. Each access point has an Service Set Identifier (SSID) to enable users to easily discover and connect.
There are several 802.11 standards which use either 5GHz or 2.4GHz bands and different frequency modulation techniques including DSSS, OFDM and Mimo.
WLAN is susceptible to interference and being cracked, there are several security protocols such as the insecure WEP and WPA which was developed by the Wi-Fi Alliance.

WLAN uses Collision Sense Multiple Access/Collision Avoidance (CSMA/CA) rather CSMA/CD used by Ethernet.

Network Security Basics

Lack of network security can be costly to a business. Networks are under almost constant attack from password cracking, trojan horses, keylogging, denial of service, IP spoofing and man-in-the-middle to name a few.

Network administrators have a range of tools to mitigate the risk of attack including firewalls, DMZ, access control lists and context -based access control devices.

IP Access Lists

Access Control Lists (ACL) are a method of filtering traffic based on destination, source IP address or protocol and port numbers.

There are three types of Cisco ACL, standard access lists, extended access lists and named access lists.

Wildcard masks can be used to apply a filter to a range of IP addresses.

Wide Area Networks (WANs)

A Wide Area Network (WAN) connects LANs together over long distances. At each end of the WAN connection you either have Data Communications Equipment (DCE) or Data circuit-Terminating Equipment (DTE). The DCE is usually located at the service provider whereas the DTE is customer premise equipment.

There are numerous WAN technologies which are classed as either circuit switching, packet switching or cell relay.

You need to understand the following WAN technologies, HDLC, PPP, Frame Relay, and ATM.

Network Address Translation (NAT)

Network Address Translation (NAT) is a process of changing the IP address of packets as they travel in and out of a network.

There are several different types of NAT. Static, Dynamic and Port Address Translation.

NAT has become a useful tool to mitigate the effects of IPv4 IP address exhaustion.

Virtual Private Networks (VPN)

Virtual Private Network (VPN) is a technology that creates a secure private connection between two end-points over a public network such as the internet.

VPN has become popular because it is a cheap alternative to a permanent WAN connection.

It works by creating an IP tunnel through the public network and secures the data using the IPsec protocol.

High-Level Data Link Control (HDLC)

HDLC is a ISO standard WAN encapsulation, although Cisco has created its own version of HDLC which adds multiple layer 3 support.
HDLC is the default encapsulation on serial interfaces of Cisco routers.

Point-to-Point Protocol (PPP)

Point-to-Point Protocol (PPP) is an industry standard WAN protocol that can be used over synchronous and asynchronous circuits.
PPP features Link Control Protocol (LCP) to initiate and terminate the connection and Network Control Protocol (NCP) to provide layer 3 encapsulation.
PPP has two options for encryption, Password Authentication Protocol (PAP) and the more secure Challenge Handshake Authentication Protocol (CHAP).

Frame Relay

Frame Relay is a high-performance packet-switching WAN protocol that features congestion control.
Data-Link Control Identifiers (DLCIs) are assigned by the service provider to identify the virtual circuits. Local Management Interface (LMI) messages used to share virtual circuit status.

Customers are guaranteed a maximum bandwidth by the service provider called the Committed Information rate (CIR).

Other Free Stuff

If you found this guide useful, [sign-up for a free account at Internetwork Training](#) and get all this:

- Free daily CCNA question and answer by email
- Free trial CCNA practice tests
- Free trial CCNA flash cards
- Free trial CCNA flash games

# Complete CCNA Bootcamp (Best for CCNA newbies)

- **Over 10½ hours of high quality CCNA video lessons** that cover the whole CCNA syllabus ready to watch online
- Videos include **30 lab walkthroughs** to help you grasp the key configuration techniques
- Printable workbooks accompany each lesson to help reinforce the knowledge you'll learn with pop quizzes, fill in the blanks and a handy list of commands covered in each video
- **Complete printable IOS configurations** for you to recreate in your own lab
- **13 interactive games** to make learning networking fun
- Master subnetting with our **Subnetting Made Easy eBook**
- Practice IOS configurations on our online simulator
- Get ready for the exam with over **650 practice questions** on every CCNA topic
- And over **300 flash cards** to help you recall important facts and commands
- Plus download our popular **CCNA cheat sheet** to help you cram for the exam

[Click here to enroll on our complete CCNA Bootcamp today!](#)

Premium Account (Best for Student Revision)

Our premium account covers the entire CCNA syllabus unlike the free material, and includes:

- Full exam objective coverage of ALL the required material
- Over 650 practice questions on every topic; retake questions you get wrong
- Over 300 flash cards with the ability to create a personalized deck
- Practice your IOS configuration on our simulator
- Learn by playing ALL our CCNA Flash games
- Practice while you travel with our mobile prep center
- The full CCNA cheat sheet to help you revise
- Subnetting made easy eBook
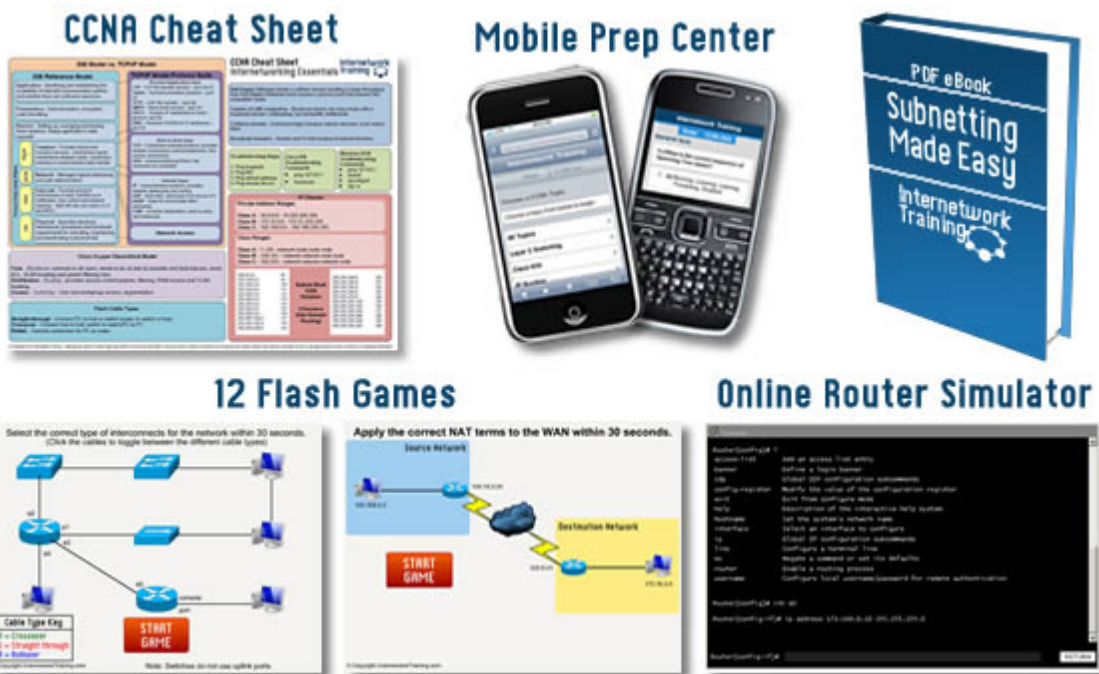
Create an account or log-in with an existing account to get access to all these resources!

This material is not sponsored, endorsed or affiliated with Cisco Systems, Inc. Cisco, Cisco Systems, CCIP, the CCIP Logo, the CCNA Logo, the CCNP Logo, the CCDA Logo and the CCDP Logo are trademarks of Cisco Systems, Inc. and its affiliates. CCENT®, CCNA®, CCNP®, CCDA® and CCDP® are registered trademarks of Cisco Systems, Inc. and its affiliates.

Although the authors of this guide have made every effort to ensure the information contained within these pages is correct, the authors do not assume and hereby disclaim any liability to any party for loss or damage caused by errors, omissions or misleading information.

The external links contained within this guide were selected and reviewed when the guide was published. However, the authors are not responsible for the content of external websites. This is because:

- the authors do not produce them or maintain/update them
- the authors cannot change them
- they can be changed without the authors knowledge or agreement.

The inclusion of links to external websites should not be understood to be an endorsement of that website or the site's owners (or their products/services).

Please consider the environment before printing this document