CompTIA

The Official CompTIA

Network+ Study Guide

Exam N10-008

Official CompTIA Content Series for CompTIA Performance Certifications

The Official CompTIA Network+ Study Guide (Exam N10-008)

Course Edition: 1.0

Acknowledgments

James Pengelly, Author
Thomas Reilly, Senior Vice President, Learning
Katie Hoenicke, Senior Director, Product Management
Evan Burns, Senior Manager, Learning Technology Operations and Implementation
James Chesterfield, Manager, Learning Content and Design
Becky Mann, Director, Product Development
Katherine Keyes, Content Specialist

Notices

Disclaimer

While CompTIA, Inc. takes care to ensure the accuracy and quality of these materials, we cannot guarantee their accuracy, and all materials are provided without any warranty whatsoever, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. The use of screenshots, photographs of another entity's products, or another entity's product name or service in this book is for editorial purposes only. No such use should be construed to imply sponsorship or endorsement of the book by nor any affiliation of such entity with CompTIA. This courseware may contain links to sites on the Internet that are owned and operated by third parties (the "External Sites"). CompTIA is not responsible for the availability of, or the content located on or through, any External Site. Please contact CompTIA if you have any concerns regarding such links or External Sites.

Trademark Notice

CompTIA®, Network+®, and the CompTIA logo are registered trademarks of CompTIA, Inc., in the U.S. and other countries. All other product and service names used may be common law or registered trademarks of their respective proprietors.

Copyright Notice

Table of Contents

About This Course

CompTIA is a not-for-profit trade association with the purpose of advancing the interests of IT professionals and IT channel organizations, and its industry-leading IT certifications are an important part of that mission. CompTIA's Network+ Certification is an entry-level certification designed for professionals with 9-12 months' work experience in roles such as a junior network administrator or network support technician.

> The CompTIA Network+ certification exam will verify the successful candidate has the knowledge and skills required to:
>
> - Establish network connectivity by deploying wired and wireless devices.
> - Understand and maintain network documentation.
> - Understand the purpose of network services.
> - Understand basic datacenter, cloud, and virtual networking concepts.
> - Monitor network activity, identifying performance and availability issues.
> - Implement network hardening techniques.
> - Manage, configure, and troubleshoot network infrastructure.
>
> *CompTIA Network+ Exam Objectives*

Course Description

Course Objectives

This course can benefit you in two ways. If you intend to pass the CompTIA Network+ (Exam N10-008) certification examination, this course can be a significant part of your preparation. But certification is not the only key to professional success in the field of network support. Today's job market demands individuals have demonstrable skills, and the information and activities in this course can help you build your network administration skill set so that you can confidently perform your duties in any entry-level network support technician role.

On course completion, you will be able to:

- Deploy and troubleshoot Ethernet networks.
- Support IPv4 and IPv6 networks.
- Configure and troubleshooting routers.
- Support network services and applications.
- Ensure network security and availability.
- Deploy and troubleshooting wireless networks.
- Support WAN links and remote access methods.
- Support organizational procedures and site security controls.
- Summarize cloud and datacenter architecture.

Target Student

The Official CompTIA Network+ Guide (Exam N10-008) is the primary course you will need to take if your job responsibilities include network administration, installation, and security within your organization. You can take this course to prepare for the CompTIA Network+ (Exam N10-008) certification examination.

Prerequisites

To ensure your success in this course, you should have basic IT skills comprising nine to twelve months' experience. CompTIA A+ certification, or the equivalent knowledge, is strongly recommended.

The prerequisites for this course might differ significantly from the prerequisites for the CompTIA certification exams. For the most up-to-date information about the exam prerequisites, complete the form on this page: www.comptia.org/training/resources/exam-objectives.

How to Use The Study Notes

The following sections will help you understand how the course structure and components are designed to support mastery of the competencies and tasks associated with the target job roles and will help you to prepare to take the certification exam.

As You Learn

At the top level, this course is divided into **lessons,** each representing an area of competency within the target job roles. Each lesson is composed of a number of topics. A **topic** contains subjects that are related to a discrete job task, mapped to objectives and content examples in the CompTIA exam objectives document. Rather than follow the exam domains and objectives sequence, lessons and topics are arranged in order of increasing proficiency. Each topic is intended to be studied within a short period (typically 30 minutes at most). Each topic is concluded by one or more activities, designed to help you to apply your understanding of the study notes to practical scenarios and tasks.

Additional to the study content in the lessons, there is a glossary of the terms and concepts used throughout the course. There is also an index to assist in locating particular terminology, concepts, technologies, and tasks within the lesson and topic content.

In many electronic versions of the book, you can click links on key words in the topic content to move to the associated glossary definition, and on page references in the index to move to that term in the content. To return to the previous location in the document after clicking a link, use the appropriate functionality in your eBook viewing software.

Watch throughout the material for the following visual cues.

Student Icon	Student Icon Descriptive Text
	A **Note** provides additional information, guidance, or hints about a topic or task.
	A **Caution** note makes you aware of places where you need to be particularly careful with your actions, settings, or decisions so that you can be sure to get the desired results of an activity or task.

As You Review

Any method of instruction is only as effective as the time and effort you, the student, are willing to invest in it. In addition, some of the information that you learn in class may not be important to you immediately, but it may become important later. For this reason, we encourage you to spend some time reviewing the content of the course after your time in the classroom.

Following the lesson content, you will find a table mapping the lessons and topics to the exam domains, objectives, and content examples. You can use this as a checklist as you prepare to take the exam, and review any content that you are uncertain about.

As A Reference

The organization and layout of this book make it an easy-to-use resource for future reference. Guidelines can be used during class and as after-class references when you're back on the job and need to refresh your understanding. Taking advantage of the glossary, index, and table of contents, you can use this book as a first source of definitions, background information, and summaries.

Lesson 1

Comparing OSI Model Network Functions

LESSON INTRODUCTION

Computer networks are complex systems that incorporate multiple functions, standards, and proprietary technologies. The Open Systems Interconnection (OSI) model is used to try to simplify some of this complexity. It divides network technologies between seven functional layers. This makes it easier to separate and focus on individual concepts and technologies while retaining an understanding of relationships to the functions of technologies placed in other layers.

This lesson uses the OSI model to give you an overview of the technologies that you will be studying in the rest of the course. You will compare the functions of these layers in the OSI model and apply those concepts to the installation and configuration of a small office/home office network.

Lesson Objectives

In this lesson, you will:

- Compare and contrast OSI model layers.
- Configure SOHO networks.

Topic 1A

Compare and Contrast OSI Model Layers

EXAM OBJECTIVES COVERED

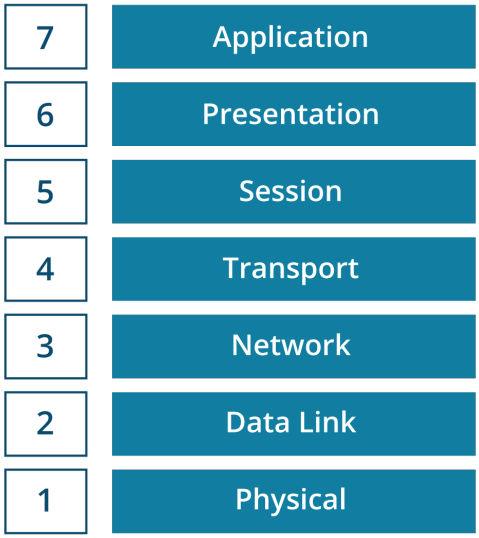
1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.

Networks are built on common standards and models that describe how devices and protocols interconnect. In this topic, you will identify how the implementation and support of these systems refer to an important common reference model: the Open Systems Interconnection (OSI) model. The OSI model breaks the data communication process into discrete layers. Being able to identify the OSI layers and compare the functions of devices and protocols working at each layer will help you to implement and troubleshoot networks.

Open Systems Interconnection Model

A network is two or more computer systems that are linked by a transmission medium and share one or more protocols that enable them to exchange data. You can think of any network in terms of nodes and links. The nodes are devices that send, receive, and forward data and the links are the communications pathways between them.

The International Organization for Standardization (ISO) developed the **Open Systems Interconnection (OSI) reference model** (iso.org/standard/20269.html) to promote understanding of how components in a network system work. It does this by separating the function of hardware and software components to seven discrete layers. Each layer performs a different group of tasks required for network communication.



The OSI model.

Although not all network systems implement layers using this precise structure, they all implement each task in some way. The OSI model is not a standard or a specification; it serves as a functional guideline for designing network protocols, software, and appliances and for troubleshooting networks.

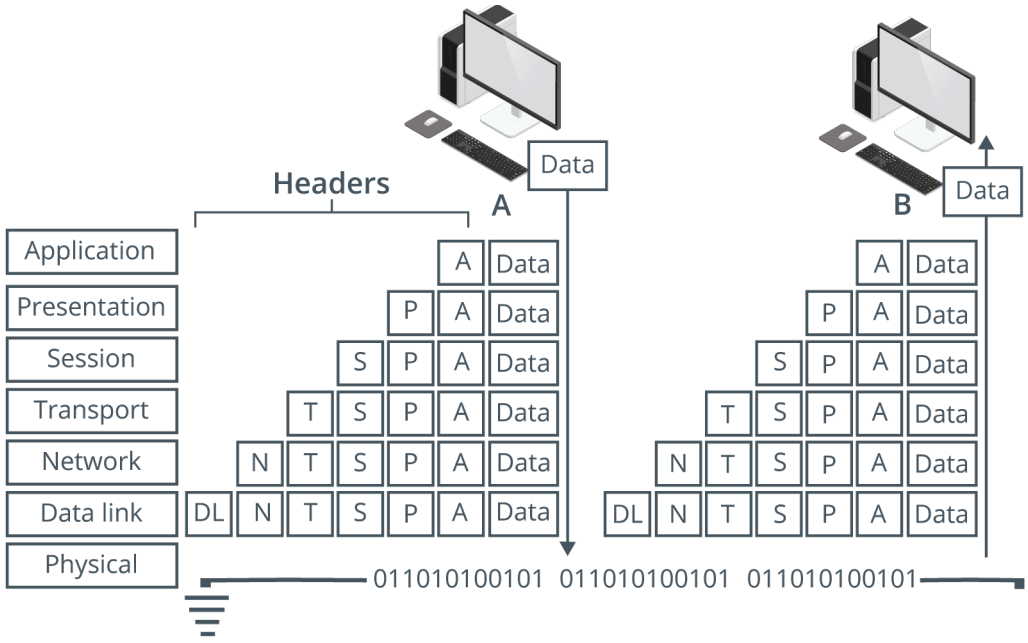
To remember the seven layers, use the following mnemonic: All People Seem To Need Data Processing.

Data Encapsulation and Decapsulation

A network protocol is a set of rules for exchanging data in a structured format. A network protocol has two principal functions:

- **Addressing**—Describing where data messages should go. At each layer, there are different mechanisms for identifying nodes and rules for how they can send and receive messages.
- **Encapsulation**—Describing how data messages should be packaged for transmission. Encapsulation is like an envelope for a letter, with the distinction that each layer requires its own envelope. At each layer, the protocol adds fields in a header to whatever data (payload) it receives from an application or other protocol.

A network will involve the use of many different protocols operating at different layers of the OSI model. At each layer, for two nodes to communicate they must be running the same protocol. The protocol running at each layer communicates with its equivalent (or peer) layer on the other node. This communication *between* nodes at the same layer is described as a same layer interaction. To transmit or receive a communication, *on* each node, each layer provides services for the layer above and uses the services of the layer below. This is referred to as adjacent layer interaction.



Encapsulation and decapsulation. (Images © 123RF.com.)

When a message is sent from one node to another, it travels down the stack of layers on the sending node, reaches the receiving node using the transmission media, and then passes up the stack on that node. At each level (except the physical layer), the sending node adds a header to the data payload, forming a "chunk" of data called a protocol data unit (PDU). This is the process of encapsulation.

For example, on the sending node, data is generated by an application, such as the HyperText Transfer Protocol (HTTP), which will include its own application header. At the transport layer, a Transport Control Protocol (TCP) header is added to this application data. At the network layer, the TCP segment is wrapped in an Internet Protocol (IP) header. The IP packet is encapsulated in an Ethernet frame at the data link layer, then the stream of bits making up the frame is transmitted over the network at the physical layer as a modulated electrical signal.

The receiving node performs the reverse process, referred to as decapsulation. It receives the stream of bits arriving at the physical layer and decodes an Ethernet frame. It extracts the IP packet from this frame and resolves the information in the IP header, then does the same for the TCP and application headers, eventually extracting the HTTP application data for processing by a software program, such as a web browser or web server.

You might notice that this example seems to omit some OSI layers. This is because "real-world" protocols do not conform exactly to the OSI model.

Layer 1—Physical

The **physical layer (PHY)** of the OSI model (layer 1) is responsible for the transmission and receipt of the signals that represent bits of data from one node to another node. Different types of transmission media can be classified as cabled or wireless:

- **Cabled**—A physical signal conductor is provided between two nodes. Examples include cable types such as copper or fiber optic cable. Cabled media can also be described as bounded media.
- **Wireless**—Uses free space between nodes, such as microwave radio. Wireless media can also be described as unbounded media.

The Physical layer specifies the following:

- **Physical topology**—The layout of nodes and links as established by the transmission media. An area of a larger network is called a segment. A network is typically divided into segments to cope with the physical restrictions of the network media used, to improve performance, or to improve security. At the Physical layer, a segment is where all the nodes share access to the same media.
- **Physical interface**—Mechanical specifications for the network medium, such as cable specifications, the medium connector and pin-out details (the number and functions of the various pins in a network connector), or radio transceiver specifications.
- The process of transmitting and receiving signals over the network medium, including modulation schemes and timing/synchronization.

Devices that operate at the Physical layer include:

- **Transceiver**—The part of a network interface that sends and receives signals over the network media.
- **Repeater**—A device that amplifies an electronic signal to extend the maximum allowable distance for a media type.

- **Hub**—A multiport repeater, deployed as the central point of connection for nodes.
- **Media converter**—A device that converts one media signaling type to another.
- **Modem**—A device that performs some type of signal modulation and demodulation, such as sending digital data over an analog line.

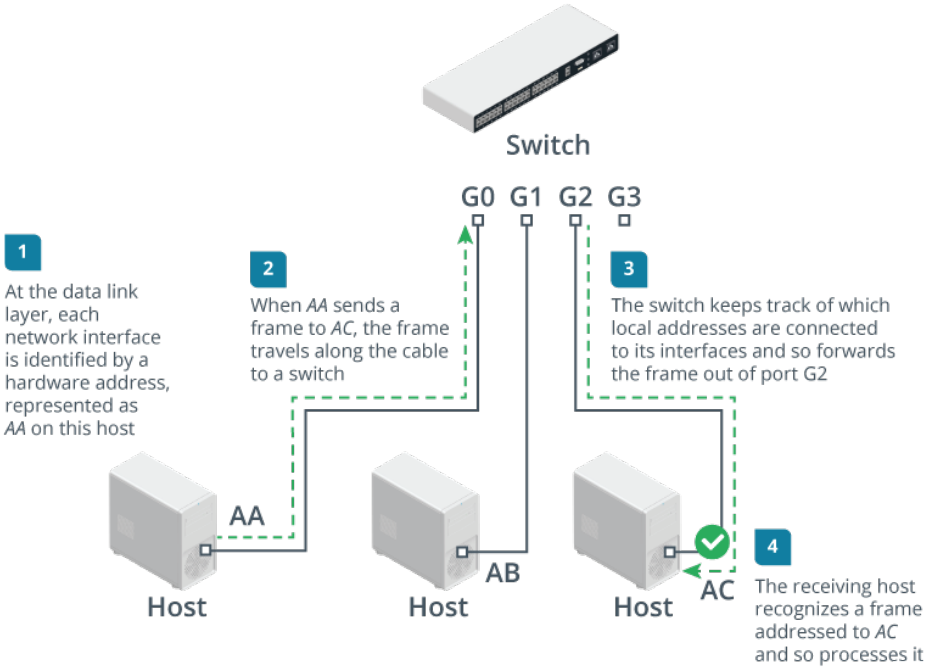
Layer 2—Data Link

The **data link layer (layer 2)** is responsible for transferring data between nodes on the same logical segment. At the Data Link layer, a segment is one where all nodes can send traffic to one another using hardware addresses, regardless of whether they share access to the same media. A layer 2 segment might include multiple physical segments. This is referred to as a logical topology.

Relatively few networks are based on directly connecting hosts together. Rather than making hosts establish direct links with one another, each host is connected to a central node, such as a switch or a wireless access point. The central node provides a forwarding function, receiving the communication from one node and sending it to another. The addresses of interfaces within the same layer 2 segment are described as local addresses or hardware addresses.

Nodes that send and receive information are referred to as end systems or as host nodes. This type of node includes computers, laptops, servers, Voice over IP (VoIP) phones, smartphones, and printers. A node that provides only a forwarding function is referred to as an intermediate system or infrastructure node.

The data link layer organizes the stream of bits arriving from the physical layer into structured units called frames. Each frame contains a network layer packet as its payload. The data link layer adds control information to the payload in the form of header fields. These fields include source and destination hardware addresses, plus a basic error check to test if the frame was received intact.



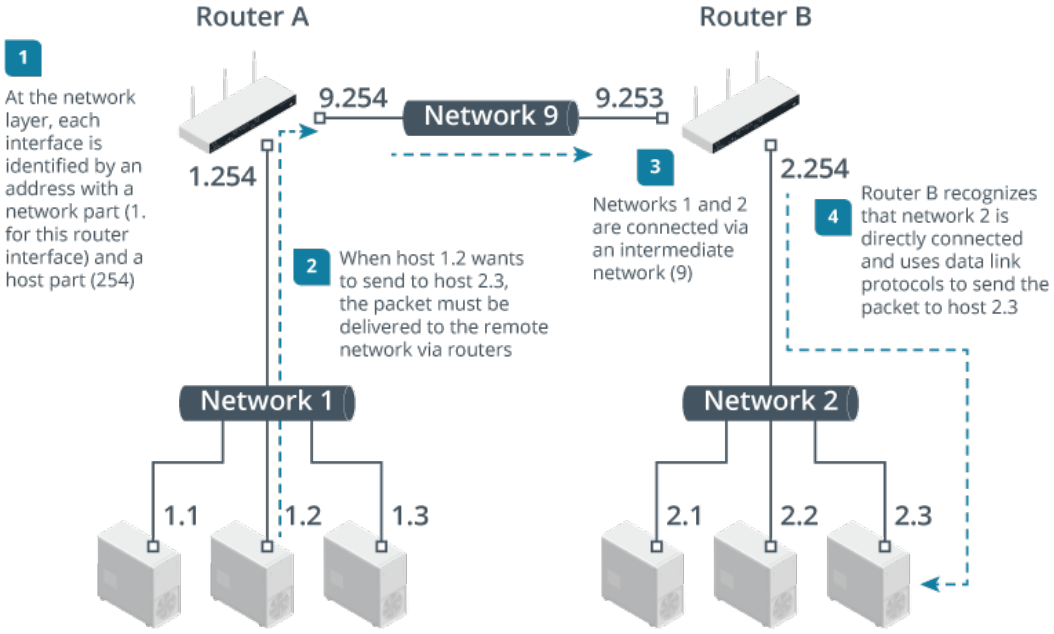
Communications at layer 2 of the OSI model. (Images © 123RF.com)

Devices that operate at the data link layer include:

- **Network adapter or network interface card (NICs)**—An NIC joins an end system host to network media (cabling or wireless) and enables it to communicate over the network by assembling and disassembling frames.
- **Bridge**—A bridge is a type of intermediate system that joins physical network segments while minimizing the performance reduction of having more nodes on the same network. A bridge has multiple ports, each of which functions as a network interface.
- **Switch**—An advanced type of bridge with many ports. A switch creates links between large numbers of nodes more efficiently.
- **Wireless access point (AP)**—An AP allows nodes with wireless network cards to communicate and creates a bridge between wireless networks and wired ones.

Layer 3—Network

The **network layer (layer 3)** is responsible for moving data around a network of networks, known as an internetwork or the Internet. While the data link layer is capable of forwarding data by using hardware addresses within a single segment, the network layer moves information around an internetwork by using logical network and host IDs. The networks are often heterogeneous; that is, they use a variety of physical layer media and data link protocols. The main appliance working at layer 3 is the **router**.



Communications at layer 3 of the OSI model. (Images © 123RF.com)

The network layer forwards information between networks by examining the destination network-layer address or logical network address. The packet is forwarded, router by router (or hop by hop), through the internetwork to the target network. Once it has reached the destination network, the hardware address can be used to deliver the packet to the target node.

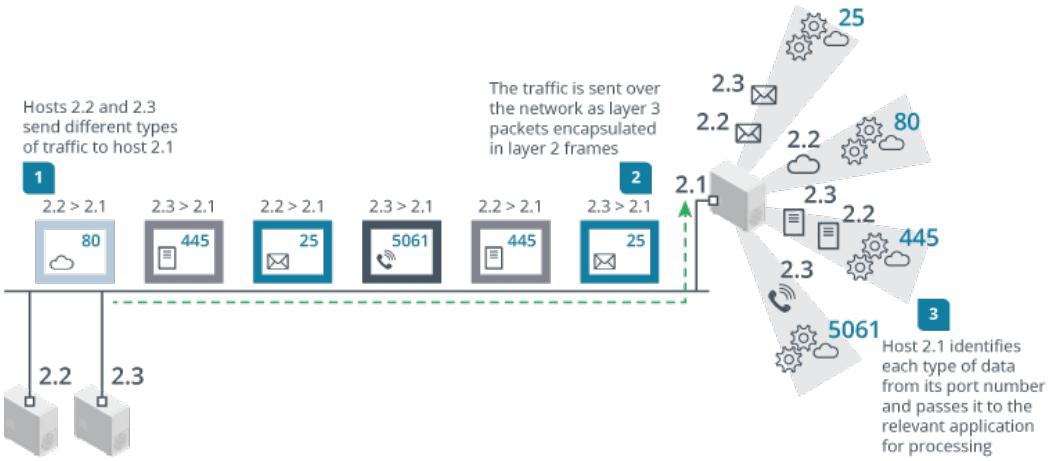
The general convention is to describe PDUs packaged at the network layer as packets or datagrams, and messages packaged at the data link layer as frames. Packet is often used to describe PDUs at any layer, however.

It is usually important for traffic passing between networks to be filtered. A basic firewall operates at layer 3 to enforce an access control list (ACL). A network ACL is a list of the addresses and types of traffic that are permitted or blocked.

Layer 4—Transport

The first three layers of the OSI model are primarily concerned with moving frames and datagrams between nodes and networks. At the **transport layer**—also known as the end-to-end or host-to-host layer—the content of the packets becomes significant. Any given host on a network will be communicating with many other hosts using many different types of networking data. One of the functions of the transport layer is to identify each type of network application by assigning it a port number. For example, data requested from an HTTP web application can be identified as port 80, while data sent to an email server can be identified as port 25.

At the transport layer, on the sending host, data from the upper layers is packaged as a series of layer 4 PDUs, referred to as segments. Each segment is tagged with the application's port number. The segment is then passed to the network layer for delivery. Many different hosts could be transmitting multiple HTTP and email packets at the same time. These are multiplexed using the port numbers along with the source and destination network addresses onto the same link.



Communications at layer 4 (transport) of the OSI model. (Images © 123RF.com)

At the network and data link layers, the port number is ignored—it becomes part of the data payload and is invisible to the routers and switches that implement the addressing and forwarding functions of these layers. At the receiving host, each segment is decapsulated, identified by its port number, and passed to the relevant handler at the application layer. Put another way, the traffic stream is de-multiplexed.

The transport layer can also implement reliable data delivery mechanisms, should the application require it. Reliable delivery means that any lost or damaged packets are resent.

Devices working at the transport layer include multilayer switches—usually working as load balancers—and many types of security appliances, such as more advanced firewalls and intrusion detection systems (IDSs).

Upper Layers

The upper layers of the OSI model are less clearly associated with distinct real-world protocols. These layers collect various functions that provide useful interfaces between software applications and the transport layer.

Layer 5—Session

Most application protocols require the exchange of multiple messages between the client and server. This exchange of such a sequence of messages is called a session or dialog. The **session layer (layer 5)** represents functions that administer the process of establishing a dialog, managing data transfer, and then ending (or tearing down) the session.

Layer 6—Presentation

The **presentation layer (layer 6)** transforms data between the format required for the network and the format required for the application. For example, the presentation layer is used for character set conversion, such as between American Standard Code for Information Interchange (ASCII) and Unicode. The presentation layer can also be conceived as supporting data compression and encryption. However, in practical terms, these functions are often implemented by encryption devices and protocols running at lower layers of the stack or simply within a homogenous application layer.

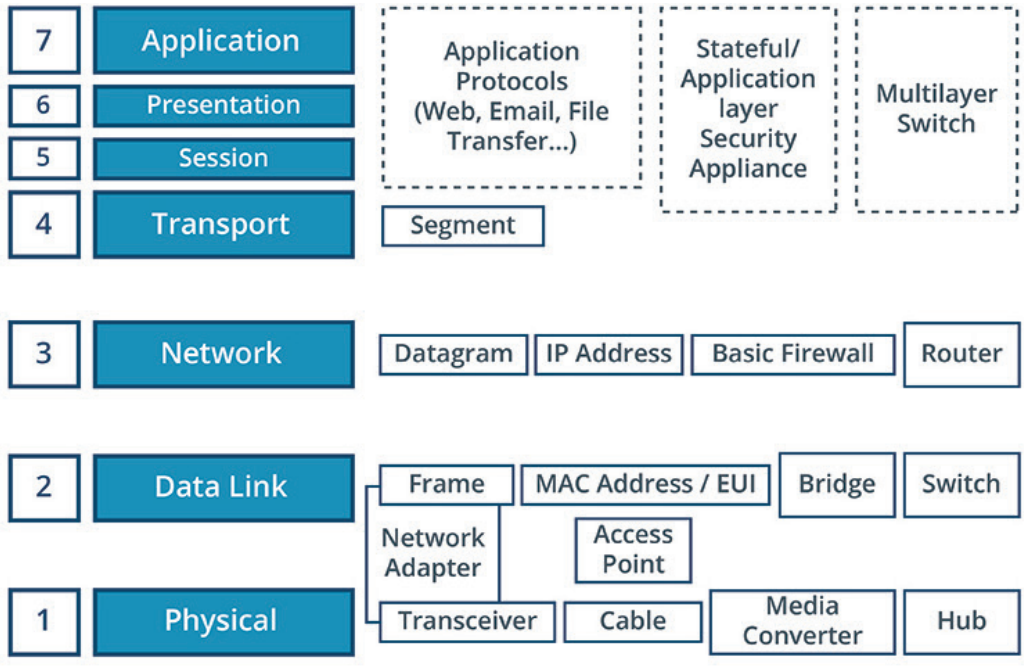
Layer 7—Application

The **application layer (layer 7)** is at the top of the OSI stack. An application-layer protocol doesn't encapsulate any other protocols or provide services to any protocol. Application-layer protocols provide an interface for software programs on network hosts that have established a communications channel through the lower-level protocols to exchange data.

More widely, upper-layer protocols provide most of the services that make a network useful, rather than just functional, including web browsing, email and communications, directory lookup, remote printing, and database services.

OSI Model Summary

The following image summarizes the OSI model, listing the PDUs at each layer, along with the types of devices that work at each layer.



Devices and concepts represented at the relevant OSI model layer.

Review Activity:

OSI Model Layers

Answer the following questions:

1. **At which OSI layer is the concept of a port number introduced?**

2. **At which layer of the OSI model is no header encapsulation applied?**

3. **What component performs signal amplification to extend the maximum allowable distance for a media type?**

4. **Which OSI layer packages bits of data from the Physical layer into frames?**

5. **True or False? The Session layer is responsible for passing data to the Network layer at the lower bound and the Presentation layer at the upper bound.**

Topic 1B

Configure SOHO Networks

EXAM OBJECTIVES COVERED

1.1 Compare and contrast the Open Systems Interconnection (OSI) model layers and encapsulation concepts.

The OSI model involves quite a lot of abstraction. As a practical example, it is worth examining how a basic network is implemented. In this topic, you will learn the connection and configuration options for components within a typical small office/home office (SOHO) router.

SOHO Routers

Networks of different sizes are classified in different ways. A network in a single location is often described as a **local area network (LAN)**. This definition encompasses many different sizes of networks with widely varying functions and capabilities. It can include both residential networks with a couple of computers, and enterprise networks with hundreds of servers and thousands of workstations.

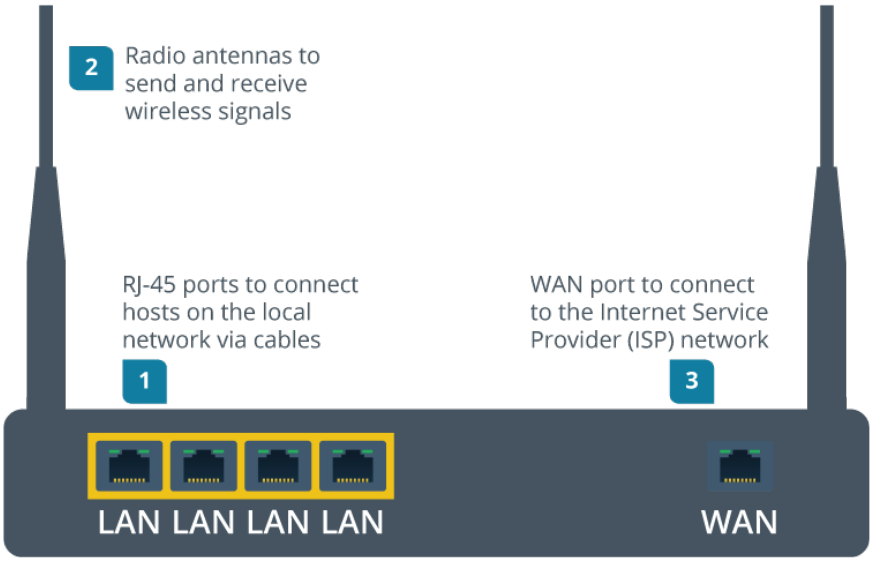
Small office/home office (SOHO) is a category of LAN with a small number of computing hosts that typically rely on a single integrated appliance for local and Internet connectivity.

Networks such as the Internet that are located in different geographic regions but with shared links are called **wide area networks (WANs)**. The intermediate system powering SOHO networks is usually described as a SOHO router because one of its primary functions is to forward traffic between the LAN and the WAN. However, routing is actually just one of its functions. We can use the OSI model to analyze each of these in turn.

Physical Layer Functions

Starting at layer 1, the SOHO router provides the following physical connections:

- A number of RJ-45 ports (typically four) to connect to a local cabled network. These are typically labeled as the LAN ports.
- Radio antennas to transmit and receive wireless signals.
- A type of modem (typically cable or digital subscriber line) to connect to the Internet Service Provider's (ISP's) network. This is typically labeled as the WAN port. On the example in the diagram, the interface is another RJ-45 port, designed to connect to a fiber to the premises Internet service using the same Ethernet technology as the local network. On other SOHO routers, there may be a different type of WAN modem, such as an RJ-11 port to connect to a digital subscriber line (DSL) service.

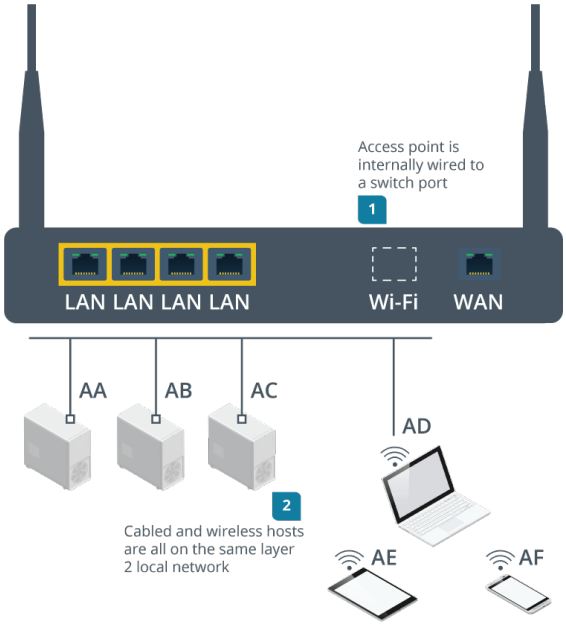


Physical layer connectivity options on a SOHO router.

Data Link Layer Functions

At layer 2, the SOHO router implements the following functions to make use of its physical layer adapters:

- **Ethernet switch**—the RJ-45 jacks are connected internally by an Ethernet switch.
- **Wireless access point**—the radio antennas implement some version of the Wi-Fi standard. The access point functions as a wireless hub, allowing stations (PCs, tablets, smartphones, and printers) to form a wireless network. The access point it also wired to the Ethernet switch via an internal port. This forms a bridge between the cabled and wireless segments, creating a single logical local network.

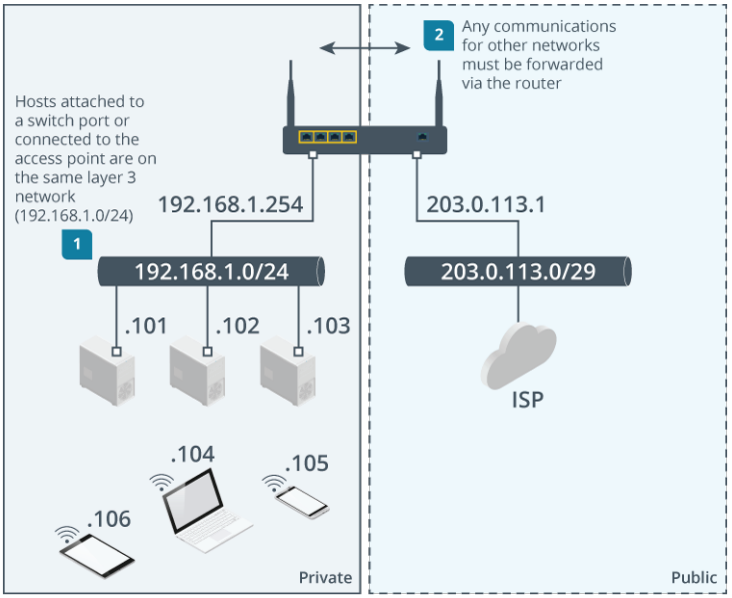


Data link layer local network segment. (Images © 123RF.com)

At this layer, each host interface is identified by a media access control (MAC) address.

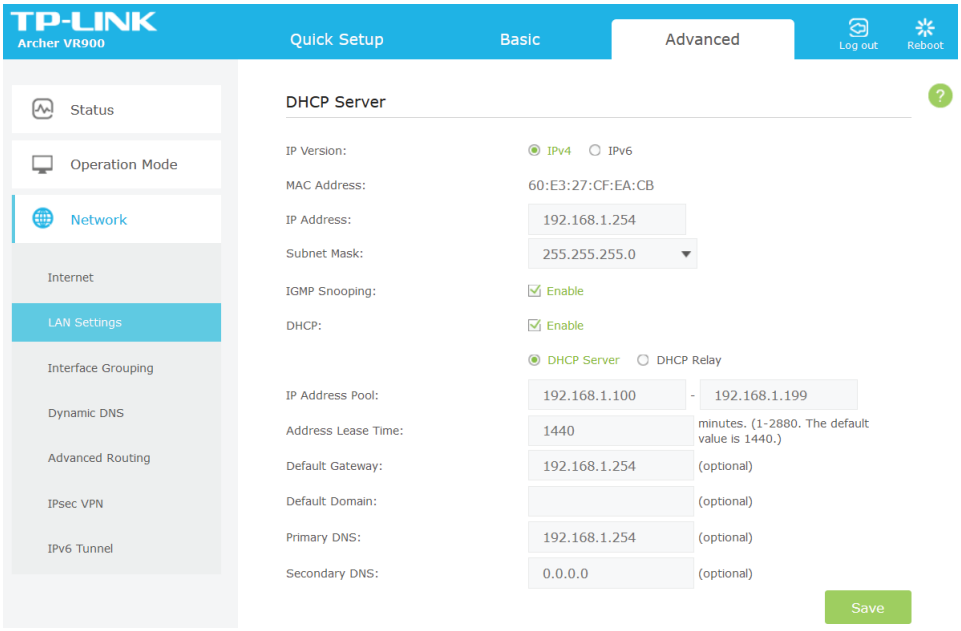
Network Layer Functions

At layer 3, the network layer, the routing part of the SOHO router makes forwarding decisions between the local private network and public Internet. These zones are distinguished by internet protocol (IP) addresses. The local network uses a private IP address range, such as `192.168.1.0/24`. The SOHO router itself is identified by an address in this range, such as `192.168.1.1` or `192.168.1.254`.



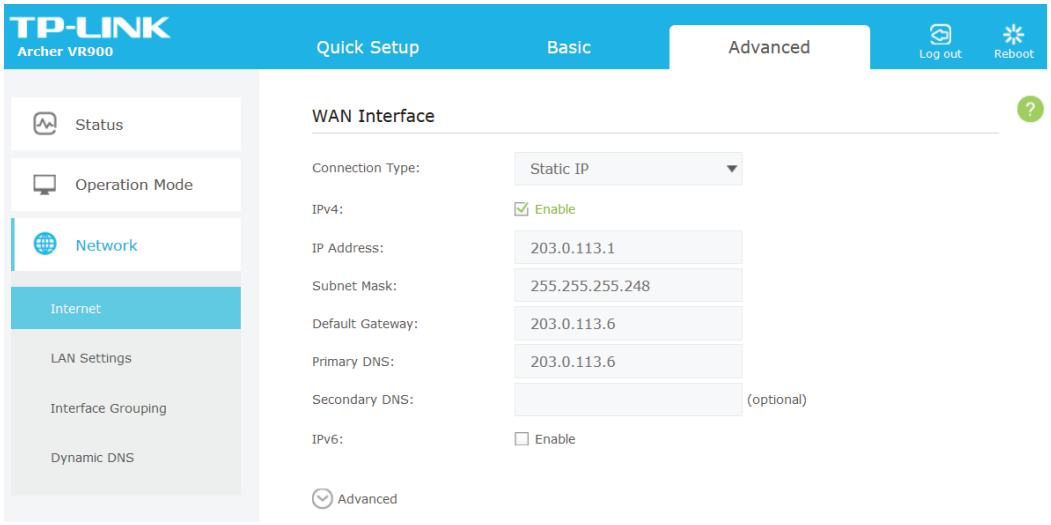
Network layer private and public segments. (Images © 123RF.com)

The router runs a dynamic host configuration protocol (DHCP) server to allocate a unique address to each host that connects to it over either an Ethernet port or via the wireless access point. The addresses assigned to clients use the same first three octets as the router's address: `192.168.1`. The last octet can be any value from 1 to 254, excluding whichever value is used by the router.



Configuring the LAN addresses using DHCP on a wireless router. (Screenshot courtesy of TP-Link Technologies Co., Ltd.)

The SOHO router's WAN interface is allocated a public IP address, say `203.0.113.1`, by the internet service provider. When a host on the local network tries to access any valid IP address outside the `192.168.1.0/24` range, the router forwards that packet over its WAN interface and directs any replies back to the host on the LAN.



Configuring the WAN (internet) interface on a wireless router. These parameters are supplied by the ISP. Many ISP services use DHCP to allocate a dynamic WAN address, but some offer static addressing. (Screenshot courtesy of TP-Link Technologies Co., Ltd.)

Transport and Application Layer and Security Functions

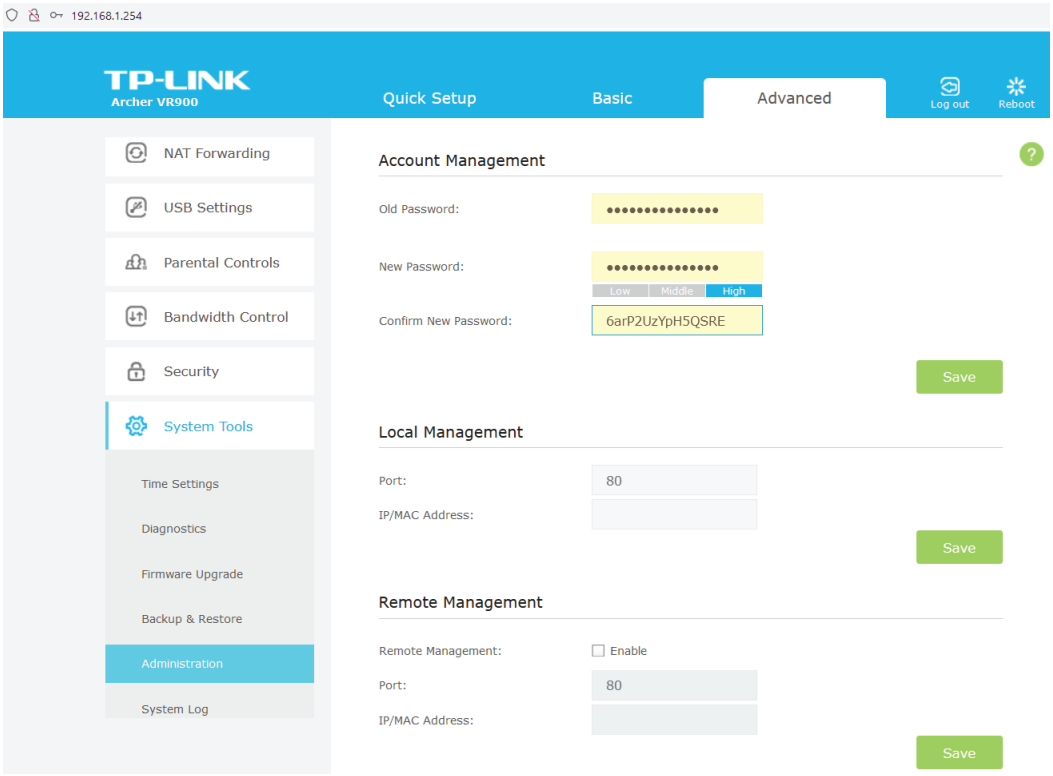
There is no separate OSI model layer for security. Instead, security issues can arise and solutions are needed at every layer. Network security is essentially a matter of allowing or preventing devices, users, and services (applications) from using the network. The WAN interface is the network perimeter. The SOHO router can apply filtering rules to traffic sent between the public and private zones, implementing a firewall. The firewall can be configured to block traffic based on source or destination IP addresses and also on the type of application.

At layer 4, each application is identified by a port number, such as 80 for hypertext transfer protocol (HTTP) web traffic or 25 for Simple Mail Transfer Protocol (SMTP) email traffic.

The firewall in the router can be configured with rules specifying behavior for each port. For example, computers on the network might use the server message block (SMB) protocol to share files. It would not be appropriate for hosts on the Internet to be able to access these shared files, so the SMB port would be blocked by default on the WAN interface but allowed on the LAN and WLAN interfaces.

Any host can connect to the RJ-45 ports on the router and join the network. The wireless network is usually protected by an encryption system that requires each station to be configured with a passphrase-based key to join the network.

Access to the router's management interface and its configuration settings is protected by an administrative account passphrase. As the router is connected to the Internet, it is critical to configure a strong passphrase.



Configuring a management interface on a wireless router. (Screenshot courtesy of TP-Link Technologies Co., Ltd.)

The Internet

The WAN interface of the router connects the SOHO network to the Internet.

The Public Switched Telephone Network

Most SOHO subscriber Internet access is facilitated via the **public switched telephone network (PSTN)**. The SOHO router is described as customer premises equipment (CPE). More widely, this is any termination and routing equipment placed at the customer site. Some of this equipment may be owned or leased from the telecommunications company (or telco); some may be owned by the customer.

The CPE is connected via its modem and WAN port to the local loop. This is cabling from the customer premises to the local exchange. The point at which the telco's cabling enters the customer premises is referred to as the demarcation point (often shortened to demarc).

Internet Service Providers

The major infrastructure of the Internet consists of high bandwidth trunks connecting Internet eXchange Points (IXPs). Within an IXP datacenter, ISPs establish links between their networks, using transit and peering arrangements to carry traffic to and from parts of the internet they do not physically own. There is a tiered hierarchy of ISPs that reflects to what extent they depend on transit arrangements with other ISPs.

Internet Standards

Although no single organization owns the Internet or its technologies, several organizations are responsible for the development of the internet and agreeing common standards and protocols.

- **Internet Assigned Numbers Authority (IANA) (iana.org)**—manages allocation of IP addresses and maintenance of the top-level domain space. IANA is currently run by Internet Corporation for Assigned Names and Numbers (ICANN). IANA allocates addresses to regional registries who then allocate them to local registries or ISPs. The regional registries are Asia/Pacific (APNIC), North America and Southern Africa (ARIN), Latin America (LACNIC), and Europe, Northern Africa, Central Asia, and the Middle East (RIPE NCC).
- **Internet Engineering Task Force (IETF) (ietf.org)**—focuses on solutions to Internet problems and the adoption of new standards, published as Requests for Comments (RFCs). Some RFCs describe network services or protocols and their implementation, while others summarize policies. An older RFC is never updated. If changes are required, a new RFC is published with a new number. Not all RFCs describe standards. Some are designated informational, while others are experimental. The official repository for RFCs is at rfc-editor.org.

References to RFCs in this course are for your information should you want to read more. You do not need to learn them for the certification exam.

The OSI model has a stricter definition of the Session, Presentation, and Application layers than is typical of actual protocols used on networks. The Internet model (tools.ietf.org/html/rfc1122) uses a simpler four layer hierarchy, with a link layer representing OSI layers 1 and 2, layer 3 referred to as the Internet layer, a Transport layer mapping approximately to layers 4 and 5, and an Application layer corresponding to layers 6 and 7.

Hexadecimal Notation

To interpret network addresses, you must understand the concept of base numbering systems. To start with the familiar; decimal numbering is also referred to as base 10. Base 10 means that each digit can have one of ten possible values (0 through 9). A digit positioned to the left of another has 10 times the value of the digit to the right. For example, the number 255 can be written out as follows:

```
(2x10x10)+(5x10)+5
```

Binary is base 2, so a digit in any given position can only have one of two values (0 or 1), and each place position is the next power of 2. The binary value 11111111 can be converted to the decimal value 255 by the following sum:

```
(1x2x2x2x2x2x2x2)+(1x2x2x2x2x2x2)+(1x2x2x2x2x2)+
(1x2x2x2x2)+(1x2x2x2)+(1x2x2)+(1x2)+1
```

As you can see, it takes 8 binary digits to represent a decimal value up to 255. This number of bits is called a byte or an octet. The four decimal numbers in the SOHO router's WAN IP address 203.0.113.1 are octets.

While computers process everything in binary, the values make for very long strings if they have to be written out or entered into configuration dialogs. Hexadecimal notation (or hex) is a convenient way of referring to the long sequences of bytes used in some other types of network addresses. Hex is base 16 with the possible values of each digit represented by the numerals 0 through 9 and the characters A, B, C, D, E, and F.

Use the following table to help to convert between decimal, binary, and hexadecimal values.

Decimal	Hexadecimal	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111

Decimal	Hexadecimal	Binary
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

As you can see from the table, every hex digit lines up neatly with four binary digits (a nibble). Each byte or octet can be expressed as two hex digits. For example, the decimal value 255 is FF in hex. This would sometimes be written as 0xFF for clarity.

Review Activity:

SOHO Networks

Answer the following questions:

1. **True or false? The WAN port on a SOHO router is connected to the LAN ports by an internal switch.**

2. **What type of address is used by the switch to forward transmissions to the appropriate host?**

3. **True or false? The DHCP server in the SOHO router assigns an IP address to the WAN interface automatically.**

4. **What function or service prevents an Internet host from accessing servers on the LAN without authorization?**

5. **How is the decimal value 12 expressed in hex?**

6. **How is the decimal value 171 expressed in hex?**

Lesson 1

Summary

You should be able to compare and contrast OSI model layers and encapsulation concepts and apply them to analyzing the function of networks and networking components.

Guidelines for Comparing OSI Model Network Functions

Follow these guidelines to make effective use of the OSI model:

- Use characteristics of physical layer media and devices to plan wiring topologies and identify potential performance issues.
- Use the data link layer to plan logical segments to isolate groups of hosts for performance or security reasons.
- At the network layer, map data link segments to logical network IDs and work out rules for how hosts in one network should be permitted or denied access to other networks.
- Evaluate service requirements at the transport layer to determine which ports a host should expose.
- Use the session, presentation, and application layers to determine performance and security requirements for the services that the network is providing.