

# Official CompTIA Study Guide for Network+ (Exam N10-007)

CompTIA®

# Acknowledgements



Official CompTIA Study Guide for Network+ (N10-007)

## PROJECT TEAM

Thomas Reilly, Vice President Learning  
Katie Hoenicke, Director of Product Management  
James Chesterfield, Manager, Learning Content and Design  
Becky Mann, Senior Manager, Product Development  
James Pengelly, Courseware Manager  
Rob Winchester, Senior Manager, Technical Operations

## 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 NOTICES

CompTIA®, Comp TIA® Security+® 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

Copyright © 2018 CompTIA, Inc. All rights reserved. Screenshots used for illustrative purposes are the property of the software proprietor. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission CompTIA, 3500 Lacey Road, Suite 100, Downers Grove, IL 60515-5439.

This book conveys no rights in the software or other products about which it was written; all use or licensing of such software or other products is the responsibility of the user according to terms and conditions of the owner. If you believe that this book, related materials, or any other CompTIA materials are being reproduced or transmitted without permission, please call 1-866-835-8020 or [www.help.comptia.org](http://www.help.comptia.org).

# Table of Contents

---

## Course Introduction i

---

Table of Contents.....	iii
About This Course .....	ix
About CompTIA Certifications .....	xiii

## Module 1 / Local Area Networks 1

---

### Module 1 / Unit 1 3

#### *Topologies and the OSI Model*

---

Key Features of Networks.....	4
Network Topologies .....	6
The OSI Model.....	11
Physical Layer .....	14
Data Link Layer.....	14
Network Layer.....	17
Transport Layer .....	18
Upper Layers .....	19
OSI Model Summary.....	21

### Module 1 / Unit 2 23

#### *Ethernet*

---

Transmission Media.....	24
Media Access Control .....	27
Broadcast Domains.....	28
Ethernet Frames .....	30
Ethernet Deployment Standards .....	32
MAC Addressing.....	35
Address Resolution Protocol (ARP) .....	37
Packet Sniffers.....	40

### Module 1 / Unit 3 43

#### *Hubs, Bridges, and Switches*

---

Hubs and Bridges .....	44
Switches .....	47
Switch Interface Configuration .....	50
Spanning Tree Protocol (STP) .....	52
Power over Ethernet (PoE) .....	55

### Module 1 / Unit 4 59

#### *Infrastructure and Design*

---

Network Infrastructure Implementations.....	60
Planning an Enterprise Campus Network.....	61
Network Hierarchy and Distributed Switching.....	64
Software Defined Networking.....	66
Planning a SOHO Network .....	67
TCP/IP Protocol Suite .....	69

<b>Module 1 / Unit 5</b>	
<i>Policies and Best Practices</i>	<b>74</b>
Procedures and Standards .....	75
Safety Procedures .....	75
Incident Response Policies .....	78
Security and Data Policies .....	79
Password Policy .....	84
Employee Policies .....	85
<b>Module 1 / Summary</b>	
<i>Local Area Networks</i>	<b>91</b>
<b>Module 2 / IP Addressing</b>	<b>93</b>
<b>Module 2 / Unit 1</b>	
<i>Internet Protocol</i>	<b>95</b>
IPv4 .....	96
IPv4 Address Structure .....	98
Subnet Masks .....	100
IP Routing Basics .....	101
ipconfig / ifconfig .....	103
ICMP and ping .....	105
<b>Module 2 / Unit 2</b>	
<i>IPv4 Addressing</i>	<b>110</b>
Broadcast, Multicast, and Unicast .....	111
Classful Addressing .....	112
Public versus Private Addressing .....	113
Subnetting and Classless Addressing .....	115
Planning an IPv4 Addressing Scheme .....	117
Public Internet Addressing .....	119
Variable Length Subnet Masks (VLSM) .....	121
<b>Module 2 / Unit 3</b>	
<i>IPv6 Addressing</i>	<b>126</b>
IPv6 Address Format .....	127
IPv6 Addressing Schemes .....	130
IPv6 Address Autoconfiguration .....	134
Migrating to IPv6 .....	135
<b>Module 2 / Unit 4</b>	
<i>DHCP and APIPA</i>	<b>138</b>
IPv4 Address Autoconfiguration .....	139
Configuring DHCP .....	142
DHCPv6 .....	145
<b>Module 2 / Summary</b>	
<i>IP Addressing</i>	<b>149</b>

**Module 3 / Unit 1*****Routing*** 153

Routing Basics .....	154
Routing Algorithms and Metrics .....	158
Dynamic Routing Protocols .....	160
Administrative Distance and Route Redistribution .....	164
IPv4 and IPv6 Internet Routing .....	165
High Availability Routing .....	166
Installing and Configuring Routers .....	167
Routing Troubleshooting Tools .....	169

**Module 3 / Unit 2*****TCP and UDP*** 177

Transmission Control Protocol (TCP) .....	178
User Datagram Protocol (UDP) .....	181
TCP and UDP Ports .....	181
Port Scanners .....	183
Protocol Analyzers .....	188

**Module 3 / Unit 3*****Name Resolution and IPAM*** 191

Host Names and FQDNs .....	192
Domain Name System .....	194
Configuring DNS Servers .....	196
Resource Records .....	198
Name Resolution Tools .....	203
IP Address Management (IPAM) .....	206

**Module 3 / Unit 4*****Monitoring and Scanning*** 208

Performance Monitoring .....	209
Network Monitoring Utilities .....	210
Logs and Event Management .....	213
Simple Network Management Protocol .....	217
Analyzing Performance Metrics .....	220
Patch Management .....	222
Vulnerability Scanning .....	224

**Module 3 / Unit 5*****Network Troubleshooting*** 228

Troubleshooting Procedures .....	229
Identifying the Problem .....	230
Establishing a Probable Cause .....	232
Establishing a Plan of Action .....	235
Troubleshooting Hardware Failure Issues .....	237
Troubleshooting Addressing Issues .....	240
Troubleshooting DHCP Issues .....	244
Troubleshooting Name Resolution .....	245
Troubleshooting Services .....	247

**Module 3 / Summary*****Internetworking*** 249

**Module 4 / Unit 1***Applications and Services* **253**

TCP/IP Services .....	254
HTTP and Web Servers.....	255
SSL / TLS and HTTPS.....	256
Email (SMTP / POP / IMAP) .....	260
Voice Services (VoIP and VTC) .....	262
Real-time Services Protocols.....	264
Quality of Service .....	267
Traffic Shaping .....	269
Bottlenecks and Load Balancing.....	270
Multilayer Switches.....	272

**Module 4 / Unit 2***Virtualization, SAN, and Cloud Services* **275**

Virtualization Technologies .....	276
Network Storage Types .....	280
Fibre Channel and InfiniBand .....	282
iSCSI .....	284
Cloud Computing.....	285
Configuring Cloud Connectivity.....	288

**Module 4 / Unit 3***Network Security Design* **293**

Security Basics .....	294
Common Networking Attacks.....	296
Network Segmentation and DMZ .....	300
Virtual LANs (VLAN) .....	303
VLAN Trunks .....	305
Network Address Translation (NAT) .....	309
Device and Service Hardening .....	313
Honeypots and Penetration Tests.....	316

**Module 4 / Unit 4***Network Security Appliances* **319**

Basic Firewalls.....	320
Stateful Firewalls .....	321
Deploying a Firewall .....	323
Configuring a Firewall .....	326
Deploying a Proxy .....	328
Intrusion Detection Systems (IDS).....	331
Denial of Service .....	336

**Module 4 / Unit 5***Authentication and Endpoint Security* **340**

Authentication and Access Controls .....	341
Social Engineering.....	343
Authentication Technologies.....	346
PKI and Digital Certificates .....	351
Local Authentication .....	353
RADIUS and TACACS+.....	355
Directory Services .....	356

Endpoint Security.....	359
Network Access Control.....	360

<b>Module 4 / Summary</b>	
<i>Applications and Security</i>	365

## **Module 5 / Operations and Infrastructure** **367**

<b>Module 5 / Unit 1</b>	
<i>Network Site Management</i>	371

Network Cabling Solutions .....	372
Distribution Frames.....	374
Change and Configuration Management.....	376
Network Documentation and Diagrams.....	378
Labeling .....	381
Physical Security Devices .....	382
Business Continuity and Disaster Recovery.....	386
Network Link Management .....	389
Power Management.....	391
Backup Management .....	394

<b>Module 5 / Unit 2</b>	
<i>Installing Cabled Networks</i>	397

Twisted Pair Cable (UTP / STP / ScTP) .....	398
Twisted Pair Connectors .....	401
Wiring Tools and Techniques.....	403
Cable Testing Tools .....	404
Troubleshooting Wired Connectivity.....	407
Other Copper Cable Types .....	409
Fiber Optic Cable and Connectors .....	412
Transceivers and Media Converters.....	416

<b>Module 5 / Unit 3</b>	
<i>Installing Wireless Networks</i>	419

Wireless Standards (IEEE 802.11).....	420
Wireless Network Topologies.....	423
Wireless Site Design.....	424
Troubleshooting Wireless Connectivity .....	428
Wireless Security .....	433
Wi-Fi Authentication.....	435
Extensible Authentication Protocol.....	437
Troubleshooting Wireless Security.....	440
Wireless Controllers.....	442

<b>Module 5 / Unit 4</b>	
<i>Installing WAN Links</i>	445

Wide Area Networks (WAN).....	446
Telecommunications Networks .....	448
Modern Telecommunications Networks .....	451
Local Loop Services.....	453
Installing WAN Links .....	458
Wireless WAN Services .....	462
Internet of Things.....	464

<b>Module 5 / Unit 5</b>	
<i>Configuring Remote Access</i>	<b>468</b>
Remote Access Services (RAS) .....	469
MPLS and PPP .....	472
SIP Trunks.....	474
Virtual Private Networks (VPN) .....	475
SSL / TLS / DTLS VPNs .....	477
IPsec .....	478
Internet Key Exchange / ISAKMP .....	482
Remote Access Servers .....	483
Remote Administration Tools.....	485
Managing Network Appliances .....	489
Remote File Access.....	491
<b>Module 5 / Summary</b>	
<i>Operations and Infrastructure</i>	<b>495</b>
 <b>Taking the Exam</b>	 <b>497</b>
 <b>Answers for Review Questions</b>	 <b>508</b>
 <b>Glossary</b>	 <b>527</b>
 <b>Index</b>	 <b>547</b>



# About This Course

---

This course is intended for those wishing to qualify with CompTIA Network+ certification.

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 a foundation-level certification designed for IT professionals with around 1 year's experience whose job role is focused on network administration.

*This exam will certify the successful candidate has the knowledge and skills required to troubleshoot, configure, and manage common network devices; establish basic network connectivity; understand and maintain network documentation; identify network limitations and weaknesses; and implement network security, standards, and protocols. The candidate will have a basic understanding of enterprise technologies, including cloud and virtualization technologies.*

## CompTIA Network+ Exam Objectives Blueprint

## Course Outcomes

This course will teach you the fundamental principles of installing, configuring, and troubleshooting network technologies and help you to progress a career in network administration. It will prepare you to take the CompTIA Network+ N10-007 exam by providing 100% coverage of the objectives and content examples listed on the syllabus. Study of the course can also help to prepare you for vendor-specific technical support qualifications and act as groundwork for more advanced training.

On course completion, you will be able to:

- Describe the features of different network protocols and products for LANs, WANs, and wireless networks.
- Understand the functions and features of TCP/IP addressing and protocols.
- Identify threats to network security and appropriate countermeasures and controls.
- Install and configure network cabling and appliances.
- Manage, monitor, and troubleshoot networks.

## Target Audience and Course Prerequisites

CompTIA Network+ is the first certification IT professionals specializing in network administration and support should earn. Network+ is aimed at IT professionals with job roles such as network administrator, network technician, network installer, help desk technician and IT cable installer.

To get started with this course, you should have successfully completed "CompTIA A+ Study Guide" courses and obtained A+ certification, and / or have around 9-12 months' experience of IT administration. It is not *necessary* that you pass the A+ exams before completing Network+ certification, but it is *recommended*.

Regardless of whether you have passed A+, it is recommended that you have the following skills and knowledge before starting this course:

- Configure and support PC, laptop, mobile (smartphone / tablet), and print devices.
- Know basic network terminology and functions (such as Ethernet, TCP/IP, switches, routers).
- Configure and manage users, groups, and shared resources in a simple SOHO network.
- Understand the use of basic access control measures, such as authentication, security policy, encryption, and firewalls.

## About the Course Material

The CompTIA Network+ exam contains questions based on objectives and example content listed in the exam blueprint, published by CompTIA. The objectives for the N10-007 exam are divided into five **domains**, as listed below. Each domain has a **weighting**, indicating its relative importance in terms of questions in the exam:

CompTIA Network+ Certification Domain Areas	Weighting
1.0 Networking Concepts	23%
2.0 Infrastructure	18%
3.0 Network Operations	17%
4.0 Network Security	20%
5.0 Network Troubleshooting and Tools	22%

This course is divided into five **modules**, each covering a different subject area:




- Module 1 / Local Area Networks
- Module 2 / IP Addressing
- Module 3 / Internetworking
- Module 4 / Applications and Security
- Module 5 / Operations and Infrastructure

As you can see, the course modules do not map directly to the CompTIA exam domains. Instead, we try to present topics and technologies in the order that will make it easiest for you to understand them. Each module and each unit starts with a list of the CompTIA domain objectives and content examples that will be covered so that you can track what you are learning against the original CompTIA syllabus.

Each unit in a module is focused on explaining the exam objectives and content examples. Each unit has a set of **review questions** designed to test your knowledge of the topics covered in the unit. Answers to the review questions are provided on the course support website.

At the back of the book there is an **index** to help you look up key terms and concepts from the course and a **glossary** of terms and concepts used.

The following symbols are used to indicate different features in the course book:

Icon	Meaning
	A tip or warning about a feature or topic.
	A reference to another unit or to a website where more information on a topic can be found.
	Review questions to help test what you have learned.

## Making a Study Plan

If you are completing this course as self-study, you need to plan your study habits. The best way to approach the course initially is to *read through* the whole thing quite quickly. On this first reading, do not worry if you cannot recall facts, get two similar technologies mixed up, or do not completely understand some of the topics. The idea is to get an overview of everything you are going to need to know. The first reading shouldn't take you too long - a few hours is plenty of time. You don't have to do it at one sitting, but try to complete the read through within about a week.

When you have completed your first read through, you should make a **study plan**. For your study plan keep in mind the following things:

- How much you know about network technologies *already*.
- How much *time* you have to study each day or each week.
- *When* you want to (or have to) become CompTIA Network+ Certified.

In your study plan, you'll identify how much time you want to spend on each unit and when you're going to sit down and do that study. We recommend that you study no more than one or two units per day. Studying a unit means reading it closely, making notes about things that come to mind as you read, using the glossary to look up terms you do not understand, then using the review questions to test and reinforce what you have learned.

Only you can decide how long you need to study for in total. Network+ Certification is supposed to represent the knowledge and skills of someone with 9-12 months of practical network support experience. If you cannot get that experience, you will need to do a corresponding amount of study to make up.

You also need to think about *where* you are going to study. You need to find somewhere comfortable and where you are not subject to interruptions or distractions. You will also need a computer or tablet with an Internet connection for the review and practical activities.

## Preparing for the Exams

When you've completed reading the units in detail, you can start to prepare for the exam. The "Taking the Exam" chapter contains tips on booking the test, the format of the exam, and what to expect.

# About CompTIA Certifications

CompTIA is the certification globally trusted to validate foundational, vendor-neutral IT security knowledge and skills. As a benchmark for best practices in IT security, this certification covers the essential principles for network security and risk management – making it an important stepping stone of an IT security career.



*It is CompTIA's policy to update the exam regularly with new test items to deter fraud and for compliance with ISO standards. The exam objectives may therefore describe the current "Edition" of the exam with a date different to that above. Please note that this training material remains valid for the stated exam code, regardless of the exam edition. For more information, please check the FAQs on CompTIA's website ([support.comptia.org](http://support.comptia.org)).*

## CompTIA Exam Vouchers

When you are ready to take your CompTIA Network+ exam, visit [comptiastore.com](http://comptiastore.com) and purchase an exam voucher for CompTIA Network+ N10-007 exam. Select a certification exam provider and schedule a time to take your exam. You can find exam providers at <http://www.pearsonvue.com/comptia/>.

Visit CompTIA online - [comptia.org](http://comptia.org) - to learn more about getting CompTIA certified. Contact CompTIA - call 866-835-8020 ext. 5 or email [questions@comptia.org](mailto:questions@comptia.org).

## CompTIA Career Pathway

Study of this course can help to prepare you for vendor-specific technical support qualifications and act as groundwork for more advanced training.

CompTIA offers a number of credentials that form a foundation for your career in technology and allow you to pursue specific areas of expertise. Depending on the path you choose to take, CompTIA certifications help you build upon your skills and knowledge, supporting learning throughout your entire career.

Other qualifications in a career pathway from CompTIA and other vendors include:

- **CompTIA Network and Cloud Technologies track** - Network+ is an excellent starting point for pursuing certifications in cloud and hosting technologies, such as CompTIA Linux+ and CompTIA Cloud+.
- **CompTIA Hardware and Services track** - in conjunction with CompTIA Server+, Network+ provides a basis for competencies in services management and provisioning.

- **CompTIA Information Security track** - Network+ is a prerequisite for starting CompTIA Security+ training, which itself leads to advanced-level certifications such as CompTIA Cybersecurity Analyst (CySA+) and CompTIA PenTest+.
- **Cisco Certified Network Associate (CCNA)** - a foundation-level certification of competency in Cisco networking appliance installation and configuration.
- **Microsoft Certified Solutions Expert (MCSE)** - Windows-specific qualifications covering support and design of client and server infrastructure, as well as other Microsoft technologies.
- **Help Desk Support Analyst** - The Help Desk Analyst certification series, administered by the Help Desk Institute ([www.thinkhdi.com](http://www.thinkhdi.com)), certifies learners' customer service and Help Desk management skills. Various levels of certification are available, including Customer Support Specialist, Help Desk Analyst, and Help Desk Manager.

# Module 1 / Local Area Networks

The following CompTIA Network+ domain objectives and examples are covered in this module:

CompTIA Network+ Certification Domain Areas	Weighting
1.0 Networking Concepts	23%
2.0 Infrastructure	18%
3.0 Network Operations	17%
4.0 Network Security	20%
5.0 Network Troubleshooting and Tools	22%

Refer To	Domain Objectives/Examples
<a href="#">Unit 1.1/ Topologies and the OSI Model</a>	<b>1.2 Explain devices, applications, protocols and services at their appropriate OSI layers</b> <i>Layer 1 (Physical) • Layer 2 (Data link) • Layer 3 (Network) • Layer 4 (Transport) • Layer 5 (Session) • Layer 6 (Presentation) • Layer 7 (Application)</i>
	<b>1.3 Explain the concepts and characteristics of routing and switching</b> <i>Properties of network traffic (Protocol Data Units)</i>
	<b>1.5 Compare and contrast the characteristics of network topologies, types and technologies</b> <i>Wired topologies (Logical vs. physical, Star, Ring, Mesh, Bus)</i>
<a href="#">Unit 1.2/ Ethernet</a>	<b>1.3 Explain the concepts and characteristics of routing and switching</b> <i>Properties of network traffic (Broadcast domains, CSMA/CD, CSMA/CA, Collision domains, MTU, Broadcast, Unicast) • Segmentation and interface properties (ARP table)</i>
	<b>2.1 Given a scenario, deploy the appropriate cabling solution</b> <i>Ethernet deployment standards (100BASE-T, 1000BASE-T, 1000BASE-LX, 1000BASE-SX, 10GBASE-T)</i>
	<b>5.2 Given a scenario, use the appropriate tool</b> <i>Software tools (Packet sniffer, Command line {tcpdump, arp})</i>
<a href="#">Unit 1.3/ Hubs, Bridges, and Switches</a>	<b>1.3 Explain the concepts and characteristics of routing and switching</b> <i>Segmentation and interface properties (Port mirroring, Switching loops / spanning tree, PoE and PoE+ [802.3af, 802.3at], MAC address table)</i>
	<b>2.2 Given a scenario, determine the appropriate placement of networking devices on a network and install / configure them</b> <i>Switch • Hub • Bridge</i>
	<b>4.6 Explain common mitigation techniques and their purposes</b> <i>Switch port protection (Spanning tree, Flood guard, BPDU guard, Root guard)</i>

Refer To	Domain Objectives/Examples
<u>Unit 1.4/</u> <u>Infrastructure</u> <u>and Design</u>	<b>1.3 Explain the concepts and characteristics of routing and switching</b> <i>Distributed switching • Software Defined Networking</i>
	<b>1.5 Compare and contrast the characteristics of network topologies, types and technologies</b> <i>Types (LAN, WLAN, MAN, WAN, CAN, SAN, PAN)</i>
<u>Unit 1.5/</u> <u>Policies and</u> <u>Best</u> <u>Practices</u>	<b>3.5 Identify policies and best practices</b> <i>Privileged user agreement • Password policy • Onboarding / offboarding procedures • Licensing restrictions • International export controls • Data Loss Prevention • Remote access policies • Incident response policies • BYOD • AUP • NDA • System life cycle (Asset disposal) • Safety procedures and policies</i>



# Module 1 / Unit 1

## *Topologies and the OSI Model*

---

### Objectives

On completion of this unit, you will be able to:

- Describe the key features and components of networks.
- Understand what is meant by a topology and identify the key physical and logical network topologies, such as star, mesh, and bus.
- Describe the functions of the layers of the OSI Model.

### Syllabus Objectives and Content Examples

This unit covers the following exam domain objectives and content examples:

- 1.2 Explain devices, applications, protocols and services at their appropriate OSI layers  
Layer 1 (Physical) • Layer 2 (Data link) • Layer 3 (Network) • Layer 4 (Transport) • Layer 5 (Session) • Layer 6 (Presentation) • Layer 7 (Application)
- 1.3 Explain the concepts and characteristics of routing and switching  
Properties of network traffic (Protocol Data Units)
- 1.5 Compare and contrast the characteristics of network topologies, types and technologies  
Wired topologies (Logical vs. physical, Star, Ring, Mesh, Bus)

# Key Features of Networks

---

A **network** is two or more computer systems linked together by some form of transmission medium that enables them to share information. It does not matter whether the network contains two or thousands of machines; the concept is essentially the same.

A network will provide services to its users. Historically, these services have included access to shared files, folders, and printers plus email and database applications. Modern networks provide more diverse services, including web applications, Voice over IP, and multimedia conferencing.

## Network Boundaries

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 types and sizes of networks though. It can include both residential networks with a couple of computers and enterprise networks with hundreds of servers and thousands of workstations.

Networks in different geographic locations but with shared links are called **Wide Area Networks (WAN)**.



*LAN and WAN are only two of the terms used to describe networks of different scales and sizes. See [Unit 1.4](#) for more on this topic.*

## Network Components

The following terms are used to describe components of the network:

### Node, Stations, and Hosts

A **node** is any device that can communicate on the network via one or more network **interfaces**. The term node can be used to describe endpoint devices, such as computers, laptops, servers, IP phones, smartphones, or printers, and connecting or forwarding devices, such as switches and routers. A node on a wireless network is often called a **station**.

The term **host** is often used in TCP/IP networking to mean an end system device, such as a computer, with a unique address on the network.

### Transmission Media

A **link** between network nodes is created using some form of **transmission** (or **physical**) **media**. Typically, this takes the form of a cable but wireless media using technologies such as radio can provide the same function.

## Local Network Devices, Segments, and Backbones

Relatively few networks are based on directly connecting computers together. Rather than making hosts establish direct links with one another, each host is connected to a central node, such as a switch or wireless access point. The central node provides a forwarding function, receiving the communication from one node and sending it to another.

A central device such as a switch implies that the connected nodes are part of the same physical network and use the same type of transmission media. The term **switching** is used for this forwarding function taking place within the same physical network. The addresses of interfaces within the same network are described as **local addresses**.

The term **segment** can be used to refer to a specific physical region of a network, though the scope of a segment depends on the exact technology in use. One typical usage now is to describe the link between a computer and a switch. Another usage is to refer to a region of the network where all the nodes use the same type of transmission media and have the same bandwidth.

A network is typically divided into segments either to cope with the physical restrictions of the network media used or to improve performance or to improve security (or all three). A **backbone** describes a fast link between other segments of a network. The backbone carries all the communications occurring between nodes in separate segments.

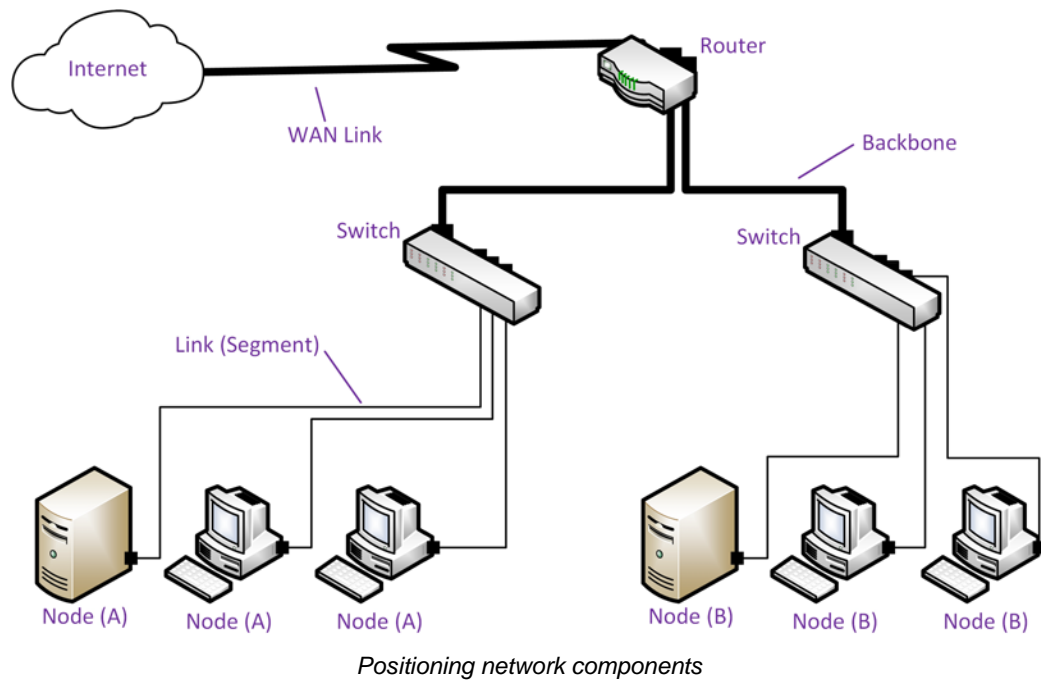
## Routing Devices and Subnets

Local and remote networks can be joined using nodes such as **routers** that can make distinctions between logically separate networks. Such networks may use different types of transmission media and network protocols. A network of hosts all installed in the same building may still be subdivided into separate logical networks, often referred to as **subnetworks** (or **subnets**). In a network of networks, each interface must have a **network address** in addition to a local address.

## Typical Network Layout

The graphic below illustrates how the network components described above might be positioned. The whole network is connected to the wider Internet via a **router**. The router is also used to divide the network into two **subnets** (A and B).

Within each subnet, a **switch** is used to allow **nodes** to communicate with one another and (through the router) the other subnet and the Internet. The link between each node and the switch is a **segment**.



High bandwidth **backbone segments** are used between the router and the Internet and the router and the two switches.

## Network Protocols

A **protocol** is a set of rules enabling systems to communicate by exchanging data in a structured format. Two of the most important functions of a protocol are to provide **addressing** (describing where data should go) and **encapsulation** (describing how data should be packaged for transmission). The basic process of encapsulation is for the protocol to add 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. For example, the concept of local and network addressing for switching and routing within and between networks is usually performed by different protocols.

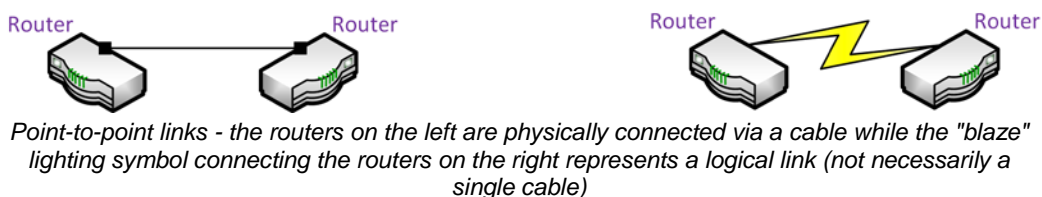
## Network Topologies

A network **topology** can describe the physical *or* logical structure of the network. This topology is described in terms of nodes and links.

- The **physical** network topology describes the placement of nodes and how they are connected by the network media. For example, in one network nodes might be directly connected via a single cable; in another network, each node might connect to a switch via separate cables. These two networks have different physical topologies.
- The **logical** topology describes the flow of data through the network. For example, given the different physical network topologies described above, if in each case the nodes can send messages to one another, the logical topology is the same. The different physical implementations (directly connected via a cable versus connected to the same switch) achieve the same logical layout.

## Point-to-Point Links

In the simplest type of topology, a single link is established between two nodes. This is called a **point-to-point** (or **one-to-one**) connection. Because only two devices share the connection, they are guaranteed a level of bandwidth.

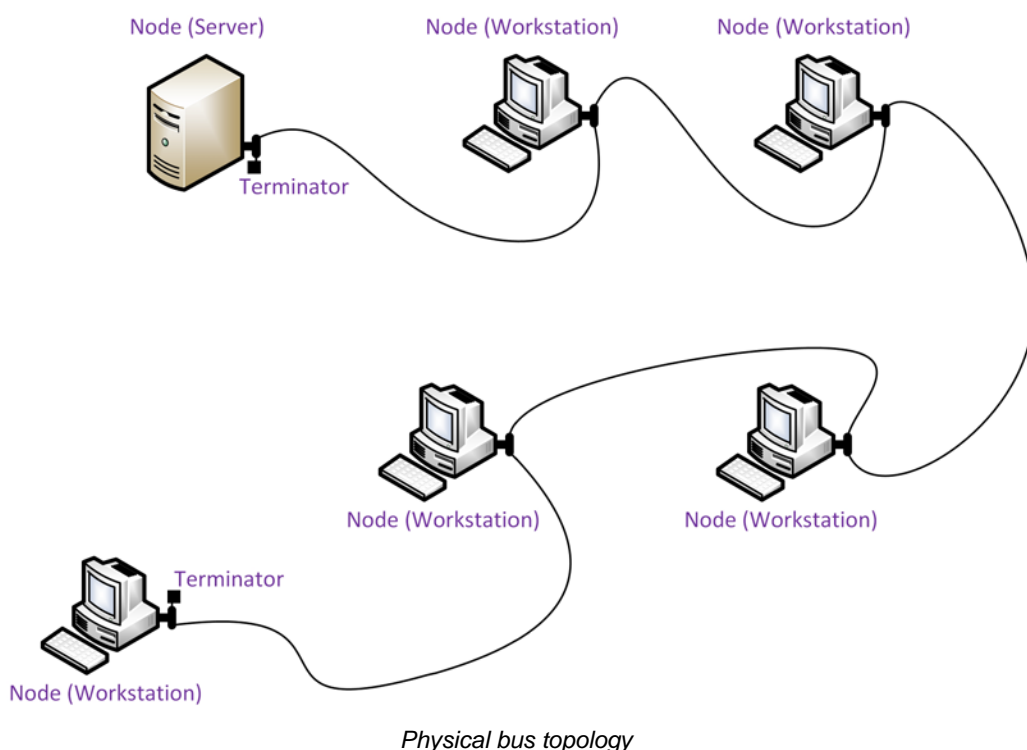


A point-to-point link can be a physical or logical topology. For example, on a WAN, two routers might be physically linked via multiple intermediate networks and physical devices but still share a logical point-to-point link, where each can only address the other router. With either a physical or logical topology, it is the 1:1 relationship that defines a point-to-point link.

On a local network, physical point-to-point links are more likely to be implemented using **switching** devices.

## Bus Topology

A **physical bus** topology with more than two nodes is a shared access topology. All nodes attach directly to a single main cable via cable taps. The signal travels down the bus in both directions from the source and is received by all nodes connected to the cable. The bus is terminated at both ends of the cable to absorb the signal when it has passed all connected devices.





*A bus network does allow cables to be connected using a device called a **repeater**. Two lengths of cable joined by a repeater is considered one length of cable for the purpose of the bus topology. A repeater is a passive device and would not be considered a network node in the way that a hub, switch, or router would.*

This type of *physical* bus topology is no longer in widespread use. Bus networks are comparatively difficult to reconfigure (adding or removing nodes can disrupt the whole network), impose limitations on the maximum number of nodes on a segment of cable, and are difficult to troubleshoot (a cable fault could be anywhere on the segment of cable). Perhaps most importantly, a fault anywhere in the cable means that *all* nodes will be unable to communicate.

The *logical* bus topology however remains the basis of most local networks.

## Star Topology

In a **star** network, each endpoint node is connected to a central forwarding node, such as a hub, switch, or router. The central node mediates communications between the endpoints.

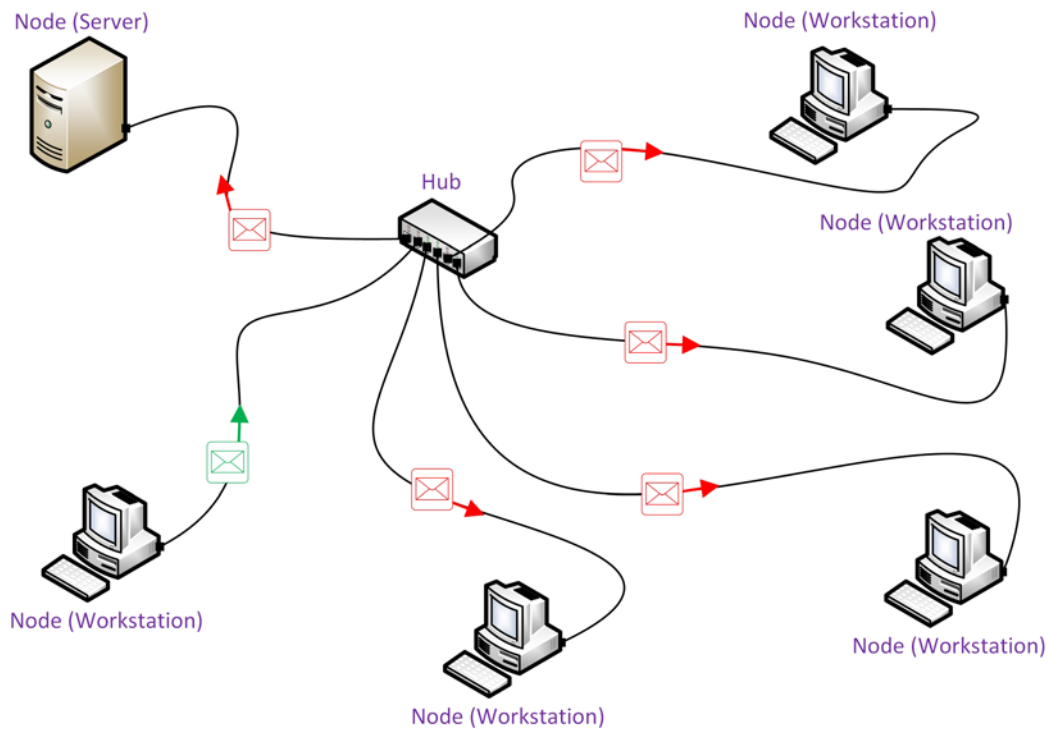
The star topology is the most widely used physical topology. It is easy to reconfigure and easy to troubleshoot, because all data goes through a central point, which can be used to monitor and manage the network. Faults are automatically isolated to the media, node (network card), or the hub, switch, or router at the center of the star.

You may also encounter the **hub and spoke** topology. This is the same layout as a star topology. The hub and spoke terminology is used when speaking about WANs with remote sites.

## Physical Star - Logical Bus Topology

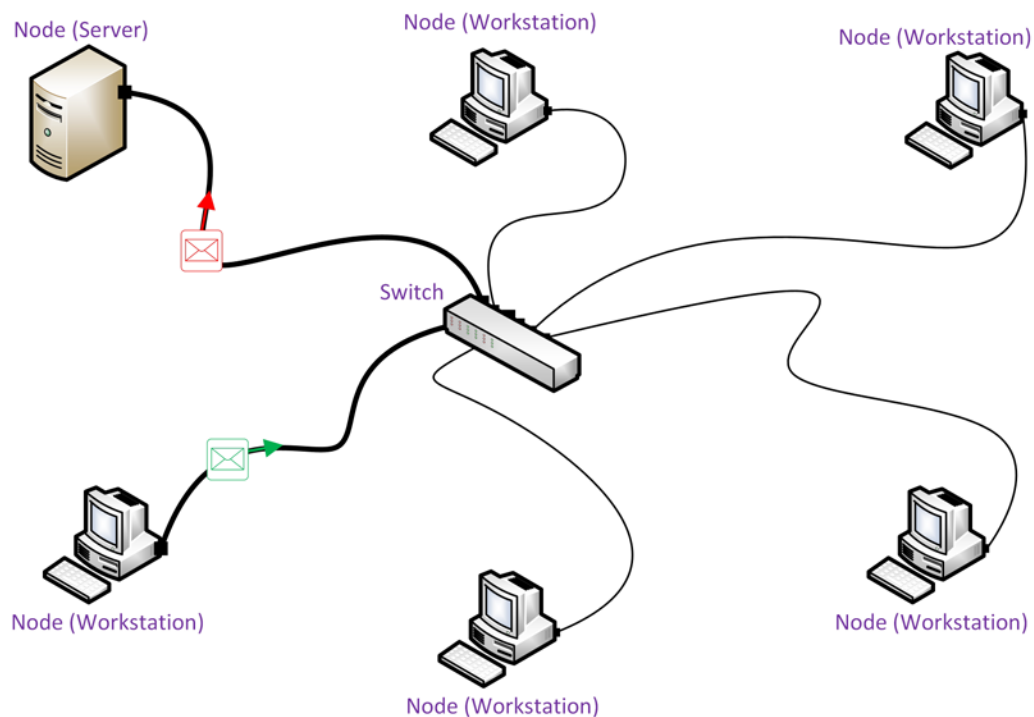
A physical star network can be used to implement a **logical bus** topology. Each node in a **star-wired logical bus** topology behaves as though it will be sharing the network medium with other nodes.

When a device such as a **hub** is used at the center of the star, transmissions are still repeated to each node. Logically the topology works like a single cable bus and the bandwidth is still shared between all nodes, which are all contending for the same network media. This means that some of the limitations of a physical bus topology are retained.



*Star topology with a hub at the center of the star*

When a device such as a **switch** is used at the center of the star, point-to-point links are established between each node as required. The logical topology is still a bus but the way the switch operates allows each node to use the full bandwidth of the link.



*Star topology with a switch at the center of the star*

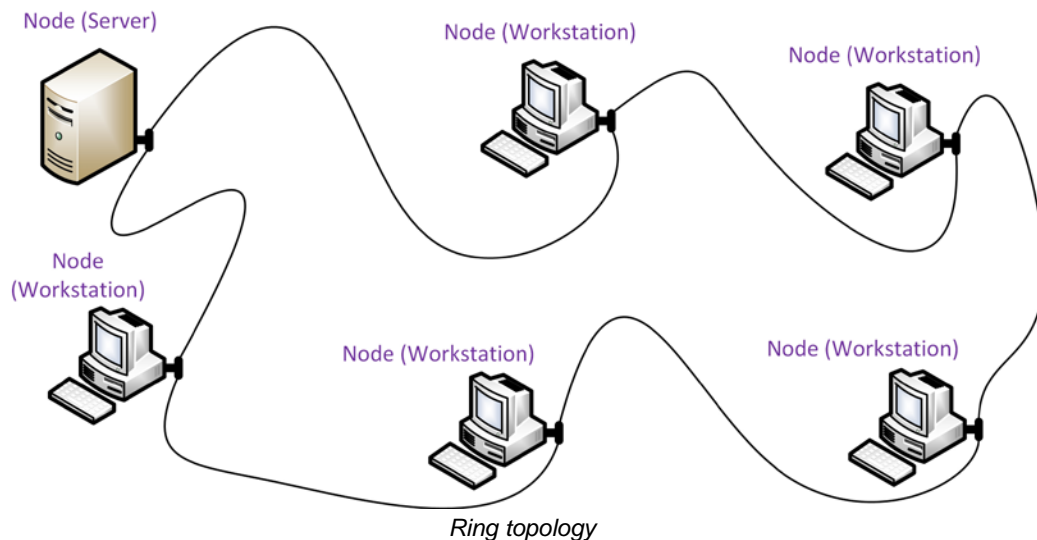


The functions of hubs and switches and the differences between them are discussed in more detail in [Unit 1.3](#).



## Ring Topology

In a **physical ring** topology, each node is wired to its neighbor in a closed loop. A node receives a transmission from its upstream neighbor and passes it to its downstream neighbor until the transmission reaches its intended destination. Each node can regenerate the transmission, improving the potential range of the network.



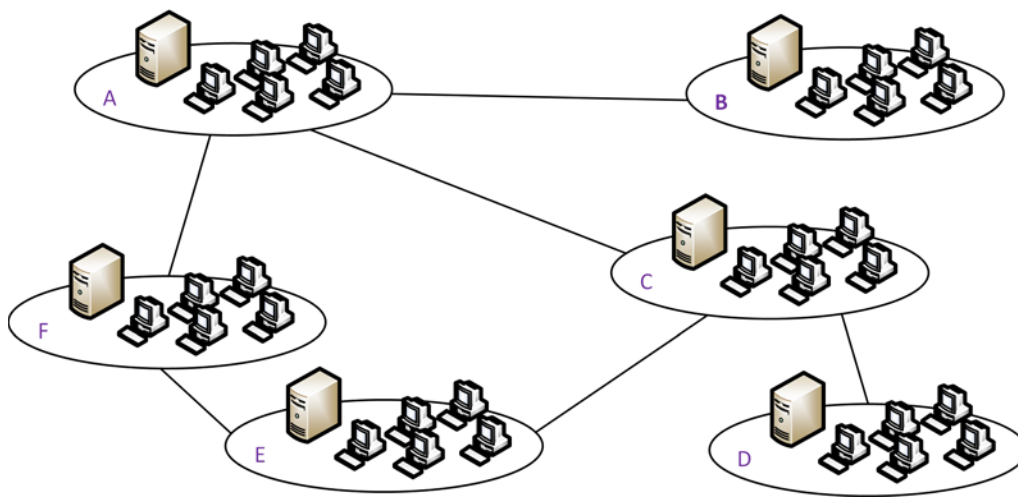
The physical ring topology is no longer used on LANs but it does remain a feature of many WANs. Two ring systems (dual counter-rotating rings) can be used to provide fault tolerance. These dual rings allow the system to continue to operate if there is a break in one ring.

## Mesh Topology

**Mesh** network topologies are commonly used in WANs, especially public networks like the Internet. In theory, a mesh network requires that each device has a point-to-point link with every other device on the network (**fully connected**). This approach is normally impractical however. The number of links required by a full mesh is expressed as  $n(n-1)/2$ , where " $n$ " is the number of nodes. For example, a network of just 4 nodes would require 6 links, while a network of 40 nodes would need 780 links!

Consequently, often a "hybrid" approach is used with only the most important devices interconnected in the mesh, perhaps with extra links for fault tolerance and redundancy. In this case, the topology is referred to as a **partial mesh**.





*Partial mesh - each site is linked but not always directly to every other site*

Mesh networks provide excellent redundancy, because other routes, via intermediary devices, are available between locations if a link failure occurs.

## The OSI Model

The **International Organization for Standardization (ISO)** developed the **Open Systems Interconnection (OSI)** reference model in 1977. It was designed to aid understanding of how a network system works in terms of both the hardware and software components by separating the function of such components to discrete layers. The model was published in 1983 as [ISO 7498](#).



*The OSI model*



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

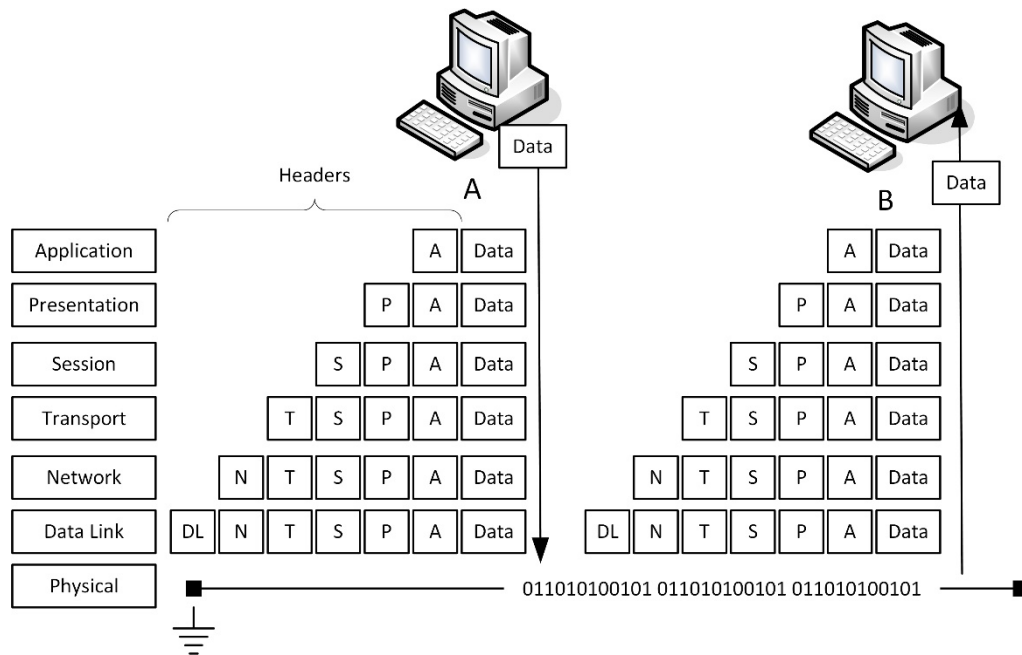
As the complexity of computer hardware and software increases, the problem of successfully communicating between these systems becomes more difficult. Dividing these difficult problems into "sub-tasks" allows them to be readily understood and solved more easily. Using this layered approach means that a vendor can work on the design and debugging for a particular layer without affecting any of the others.

Each layer performs a different group of tasks required for network communication. Although not all network systems implement layers using this *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.

## Encapsulation and De-encapsulation

For two nodes to communicate they must be running the same protocol. Each layer communicates with its equivalent (or **peer**) layer on the other node via the lower layers of the model. Each layer provides services for the layer above and uses the services of the layer below.

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 **Protocol Data Unit (PDU)**. This process is known as **encapsulation**.

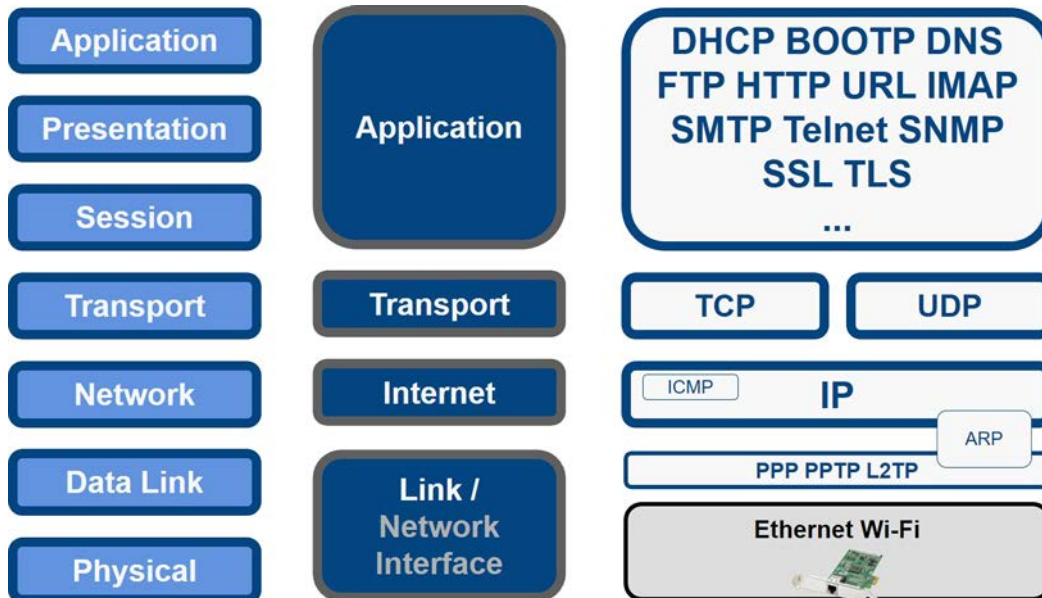


On a typical local network for example, on the sending node, data is generated by an application such as HTTP, which will include its own application header. At the transport layer, a TCP header is added to this application data. At the network layer, the TCP segment is wrapped in an IP header. The IP packet is put into 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.

The receiving node performs the reverse process (**de-encapsulation** or **decapsulation**). For example, 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 application data for processing by a software program.

## The OSI Model and Network Protocols

The OSI model is only intended to be a *conceptual* framework for discussing and designing protocols. As a result, the computer industry often struggles to categorize various protocols and networking technologies into the model.



OSI reference model and TCP/IP

The example above demonstrates how the OSI model (a theoretical model) compares with the TCP/IP protocol stack (a real system). Some of the OSI layers are performed by a single protocol, some layers are performed by several protocols, and some protocols cover several layers.

This reflects the emphasis on performance and efficiency in "real world" networking. Each layer of encapsulation consumes processing power and bandwidth as each header consists of a number of bytes that must be transmitted and decoded in addition to the application data. Consequently, actual protocol stacks tend to be simpler than the OSI model.

## Physical Layer

The **physical** layer (PHY) of the OSI model (layer 1) is responsible for the transmission and receipt of bits from one node to another node. It specifies the following:

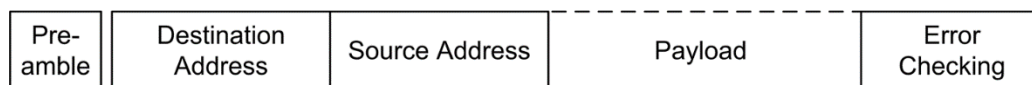
- Physical network topology - mechanical specifications for the network medium, such as cable specifications, the medium connector and pin-out details (the number and functions of the various pins in a network connector), or radio transceiver specifications.
- The process of transmitting and receiving signals from the network medium including modulation schemes and timing / synchronization.

Devices operating at the physical layer include:

- **Transceiver** - the part of a network interface that sends and receives signals over the network media.
- **Media Converter** - converts one media signaling type to another.
- **Repeater** - amplifies the signal to extend the maximum allowable distance for a media type.
- **Hub** - a multiport repeater, deployed as the central point of connection for nodes wired in a star topology.
- **Modem** - a device that converts between digital and analog signal transmissions.

## Data Link Layer

The **data link** layer (layer 2) is responsible for transferring data between nodes on the same network segment. For incoming data, it organizes the 1s and 0s into 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 contain a source and destination hardware address and error checking values. Other information (not shown in the figure) includes the frame length and network layer protocol identifier.



*Construction of a frame*

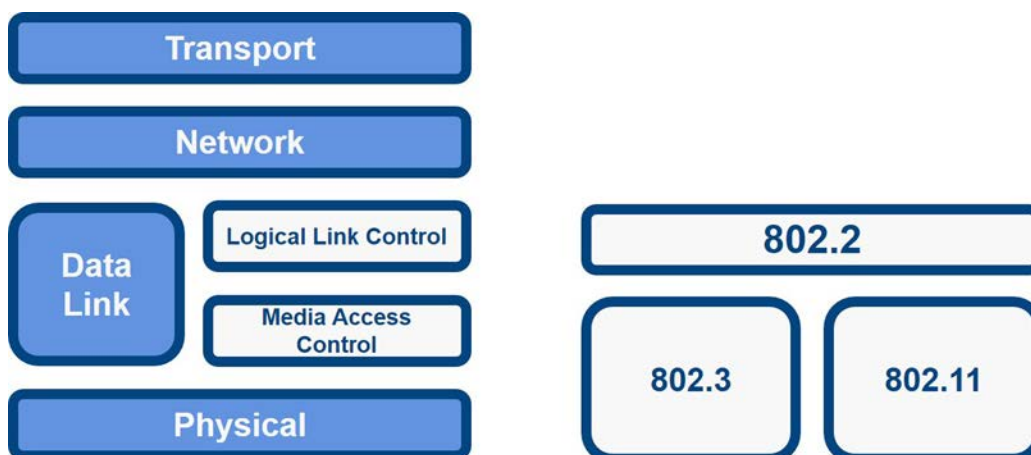
Some network products use multiple different frame types. For example, Ethernet specifies four frame types. The basic structure remains the same but each frame type contains a slightly different header structure. Devices must communicate using the same frame type.

The last part of the frame usually contains some sort of error checking. Protocols at most layers perform a consistency check to verify that data has been transferred correctly. The data link layer is only capable of very basic error checking, such as identifying truncated or corrupt frames. There is no function to acknowledge or retransmit damaged frames. That function is handled at higher layers of the OSI model.

Another important function at the data link layer is determining how multiple nodes can share access to the network media, establishing the logical network topology. For example, a bus-based topology uses contention as a media access method. A ring-based topology uses a token-passing access method.

## IEEE 802 Standards

Over the years, a number of protocols, standards, and products have been developed to cover technologies working at the physical and data link layers of the OSI model. The most important of these are the **IEEE 802 standards**, published by the **LAN / MAN Standards Committee** ([www.ieee802.org](http://www.ieee802.org)) of the **Institute of Electrical and Electronics Engineers (IEEE)**. The IEEE is a professional body that oversees the development and registration of electronic standards.



*Comparison of IEEE 802 and the OSI model*

There are a number of separate working groups within the LAN / MAN Standards Committee developing different standards. These are collectively known as 802.x. The IEEE splits the functions of the data link layer into two sub-layers. These two sub-layers are known as **Media Access Control (MAC)** and **Logical Link Control (LLC)**.

## IEEE 802.2 (Logical Link Control)

The **IEEE 802.2** standard for the **Logical Link Control (LLC)** sub-layer is used with other 802 protocols, such as 802.3 and 802.11. The LLC protocol provides a standard network layer service interface regardless of which MAC sub-layer protocol is used.

## IEEE 802.3 (Ethernet) and the MAC Sub-layer

The **Media Access Control (MAC)** sub-layer defines the way in which multiple network interfaces share a single transmission medium. It covers the following:

- Logical topology - bus or ring.
- Media access method - contention or token passing.
- Addressing - the hardware address of the network interface.
- Error detection.
- Frame format.

The **IEEE 802.3** standard specifies protocols that implement the functions of the MAC sub-layer plus signaling and media specifications at the physical layer. IEEE 802.3 is based on the **Ethernet** networking product, developed by the DIX consortium (Digital Equipment Corporation [DEC], Intel, and Xerox). While the product name is not used in 802.3 standards documentation, it is otherwise universally referred to as Ethernet.

Ethernet is now the only widely supported standard for cabled LANs. Legacy products such as ARCNET and Token Ring may persist in networks that are difficult to upgrade or reconfigure. The IEEE 802.11 series of standards (Wi-Fi) are used to implement Wireless Local Area Networks (WLAN).

## Layer 2 Devices

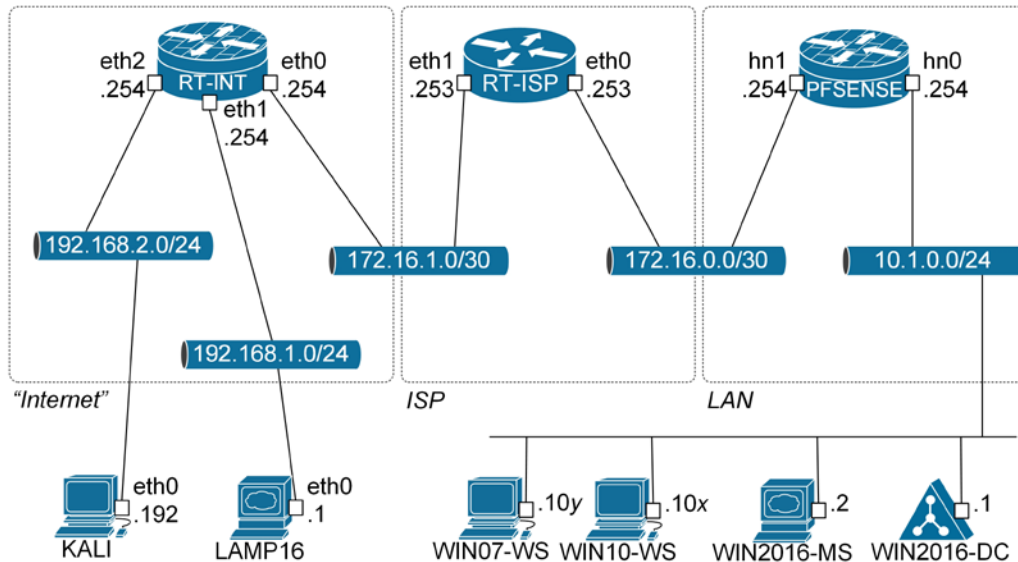
Connectivity devices found at the data link layer include:

- **Network adapter** (or **Network Interface Card [NIC]**) - joins a host computer to network media (cabling or wireless) and enables it to communicate over the network by assembling and disassembling frames.
- **Bridge** - joins two network segments while minimizing the performance reduction of having more nodes on the same network.
- **Basic switch** - a multiport bridge that creates links between nodes more efficiently.
- **Wireless Access Point (AP)** - allows nodes with wireless network cards to communicate and joins wireless networks to wired ones.



# Network Layer

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



The key function of the network layer is to identify logical network IDs and route communications between different networks

The network layer transfers information between networks by examining the destination network layer address or logical network address, and routing the packet through the internetwork using intermediate systems (**routers**). Selection of the path or route to the destination network address is determined **dynamically** or **statically**. The packet moves, hop by hop, through the internetwork to the target network. Once it has reached the destination network, the hardware address can be used to move the packet to the target node. This process requires each logically separate network to have a unique network address.



The general convention is to describe Protocol Data Units (PDU) packaged at the network layer as packets or datagrams and distinguish messages packaged at the data link layer by calling them frames and those at the transport layer by calling them segments. "Packet" is also used to describe PDUs at any layer however.

The main appliance working at layer 3 is the router. Other devices include Layer 3 switches (combining the function of switches and routers) and basic firewalls.



Network addressing and routing using the Internet Protocol are covered in detail in [Unit 2.1](#), [Unit 2.2](#), [Unit 2.3](#), and [Unit 3.1](#).

# Transport Layer

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 starts to become significant.

Any given host on a network will be communicating with many other hosts using many different types of networking data. One of critical functions of the transport layer is to identify each type of network application by assigning it a **port number**. For example, data from the HTTP web browsing application can be identified as port 80 while data from 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 **segments** and each segment is tagged with the application's port number. The segment is then passed to the network layer for delivery. The host could be transmitting multiple HTTP and email segments at the same time. These are **multiplexed** using the port numbers onto the same network link.



*In fact, each host assigns two port numbers. On the client, the destination port number is mapped to the service that the client is requesting (HTTP on port 80 for instance). The client also assigns a random source port number (47,747 for instance). The server uses this client-assigned port number (47,747) as the destination port number for its replies and its application port number (80 for HTTP) as its source port. This allows the hosts to track multiple "conversations" for the same application protocol.*

At the network and data link layers, the port number is not significant - it becomes part of the data payload and is "invisible" to routers and switches working at the network and data link layers. At the receiving host, each segment is extracted from its frame and then identified by its port number and passed up to the relevant handler at the upper session and application layers. Put another way, the traffic stream is de-multiplexed.

The transport layer is also responsible for ensuring *reliable* data delivery so that packets arrive error-free and without loss. The transport layer can overcome any lack of reliability in the lower level protocols. This reliability is achieved using **acknowledgement** messages that inform the sender the data was successfully received. The kinds of problems that may occur during the delivery of the data are non-delivery and delivery in a damaged state. In the first case, the lack of acknowledgement results in the retransmission of the data and, in the second case, a **Negative Acknowledgement (NACK)** forces retransmission.



The transport layer also accomplishes reliable delivery through other mechanisms:

- Orderly connection establishment and teardown - under normal circumstances a single connection is created between computers. However, multiple connections can be established to improve throughput.
- Segmentation - breaking PDUs from the session layer into a segment format where sequence numbers are used by the receiver to rebuild the message correctly.
- Flow control - enables one side to tell the other when the sending rate must be slowed.



*These features are typical of connection-oriented protocols. Connectionless protocols operate without such mechanisms and are therefore faster, but less reliable.*

Devices working at the transport layer (or above) include multilayer switches (incorporating load balancing) and security appliances such as more advanced firewalls and Intrusion Detection Systems (IDS).



See [Unit 3.2](#) for more information about the functions of protocols working at the transport layer.

## 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 network layer.

### Session Layer

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 the **dialog control** functions that administer the process of establishing the dialog, managing data transfer, and then ending (or "tearing down") the session.

Sessions can work in three modes:

- One-way / simplex - only one system is allowed to send messages; the other receives only.
- Two-Way Alternate (TWA) / half-duplex - the hosts establish some system for taking turns to send messages, such as exchanging a token.
- Two-Way Simultaneous (TWS) / duplex - either host can send messages at any time.

The session layer can also provide a synchronization service for long transactions in which checkpoints are inserted into the data stream (**dialog separation**). If a problem occurs, only the data transferred after the last checkpoint is resent.

## Presentation Layer

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. The communicating computers may use different character coding systems (such as American Standard Code for Information Interchange [ASCII] and Unicode); the peer presentation layers agree to translate the data into one of the formats or they will both translate the data into a third format. The presentation layer can also be conceived as supporting data compression and encryption (scrambling a message so that it can only be read in conjunction with a valid "key"). However, in practical terms these functions are often implemented by encryption devices and protocols running at lower layers of the stack.

## Application Layer

The **application** layer (layer 7) is at the top. An application layer protocol doesn't encapsulate any other protocols or provide services to any protocol. An application layer protocol provides an interface for software applications on network hosts that have established a communications channel using the lower level protocols to exchange data. For example, one of the most utilized services provided by the application layer is file transfer. Different file systems may use entirely different file naming conventions and data syntax and the application layer must overcome these differences. More widely, upper layer protocols provide most of the services that make a network useful, rather than just functional, including network printing, electronic mail and communications, directory lookup, and database services.



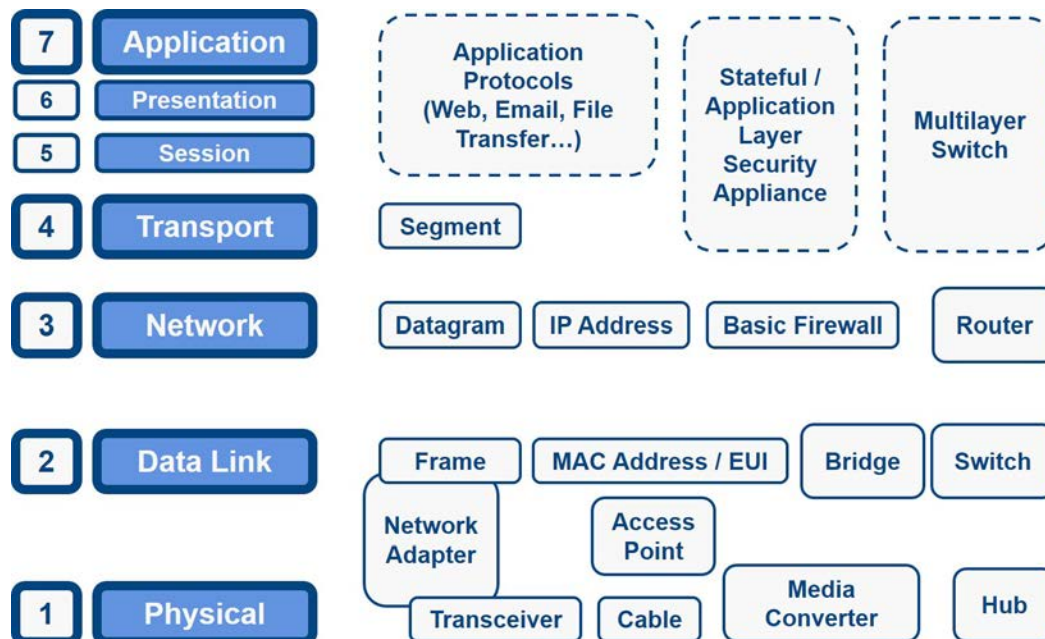
*As mentioned above, the OSI model has a stricter definition of the session, presentation, and application layers than is typical of actual protocols used on networks. You do not need to identify specific differences between these upper layers for the exam.*

## Application Protocols and Software Applications

It is important to distinguish between network application protocols and the software application code (programs and shared programming libraries) that runs on computers. Software programs and operating systems make use of **Application Programming Interfaces (API)** to call functions of the relevant part of the network stack. Examples of APIs include:

- Network card drivers could use the Network Driver Interface Specification (NDIS) API to implement functions at the data link layer.
- The Sockets / WinSock APIs implement transport and session layer functions.
- High-level APIs implement functions for services such as file transfer, email, web browsing, or name resolution.

## OSI Model Summary



*Devices and concepts represented at the relevant OSI model layer*

**Review Questions / Module 1 / Unit 1 / Topologies and the OSI Model**

Answer these questions to test what you have learned in this unit.

- 1) What term is used to describe a topology in which two nodes share a single link?
- 2) What is characteristic of the bandwidth of a bus topology?
- 3) What type of device is used to implement a star topology?
- 4) You need operations to continue if one link fails. How many links does it take to connect three sites?
- 5) In which sub-layer of the OSI model do network adapter cards operate?
- 6) Which component is responsible for translating the computer's digital signals into electrical or optical signals that travel on network cable?
- 7) 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.
- 8) Which OSI layer handles the concept of logical addressing?
- 9) At which OSI layer is the concept of a port number introduced?
- 10) Which two OSI layers define how multiple computers can simultaneously use the network media without interfering with each other?