

TABLE OF CONTENTS

LIST OF TABLES.....	6
LIST OF FIGURES.....	6
LIST OF ACRONYMS.....	7
Topic 1: Networking Fundamentals.....	18
Section 1.1: The OSI Reference Model	18
1.1.1: Interaction Between OSI Layers.....	19
Section 1.2: TCP/IP and the OSI Reference Model	20
1.2.1: The TCP/IP Protocol Architecture.....	20
1.2.2: TCP/IP Data Encapsulation	21
Section 1.3: Networks	21
1.3.1: Network Definitions	22
1.3.2: Types of Networks.....	22
1.3.3: Network Topologies	23
1.3.4: Network Technologies.....	24
1.3.4.1: Ethernet.....	24
1.3.4.2: Fast Ethernet	25
1.3.4.3: Gigabit Ethernet.....	25
1.3.5: Network Addressing	26
1.3.6: Bridging	26
1.3.7: LAN Switching	27
1.3.8: Wireless Networks.....	28
1.3.8.1: Wireless Network Standards.....	28
1.3.8.2: Wireless Network Modes.....	30
1.3.8.3: Security Features.....	30
Section 1.4: The Cisco IOS Software.....	30
1.4.1: The Cisco IOS Software Command-Line Interface.....	31
1.4.1.1: The CLI Help Features	31
1.4.1.2: Syslog Messages and the debug Command.....	31
1.4.2: Configuring Cisco IOS Software.....	32
1.4.2.1: Managing Configuration Files	32
1.4.2.2: Upgrading Cisco IOS Software	33
1.4.2.3: The Cisco IOS Software Boot Sequence	34
Section 1.5: Spanning-Tree Protocol (STP).....	35
1.5.1: Root Bridge Election	36
1.5.2: Root Ports Election	37
1.5.3: Designated Ports Election.....	38
1.5.4: STP States	38
1.5.5: STP Timers	39
1.5.6: Optional STP Features.....	40

1.5.6.1: EtherChannel	40
1.5.6.2: PortFast	40
1.5.6.3: Rapid Spanning Tree (IEEE 802.1w)	40
Topic 2: Virtual LANs and Trunking	42
Section 2.1: VLAN Membership	42
Section 2.2: Extent of VLANs	42
Section 2.3: VLAN Trunking	43
2.3.1: Inter-Switch Link (ISL)	43
2.3.2: IEEE 802.1Q	44
Section 2.4: VLAN Trunking Protocol (VTP)	44
2.4.1: VTP Modes	44
2.4.1.1: Server Mode	44
2.4.1.2: Client Mode	45
2.4.1.3: Transparent Mode	45
2.4.2: VTP Pruning	45
2.4.3: VTP Configuration	46
2.4.3.1: Configuring a VTP Management Domain	46
2.4.3.2: Configuring the VTP Mode	46
2.4.3.3: Configuring the VTP Version	46
Topic 3: IP Addressing and Subnetting	48
Section 3.1: IP Addressing	48
3.1.1: Binary Format	48
3.1.2: Dotted Decimal Format	49
3.1.3: IP Address Classes	49
3.1.4: Classless Interdomain Routing (CIDR) Notation	50
3.1.5: Variable-Length Subnet Masks	51
Section 3.2: Subnetting	51
Section 3.3: Summarization	52
3.3.1: Automatic Summarization	52
3.3.2: Manual Summarization	52
Section 3.4: Determining the Network ID using the Logical AND Operation	53
Section 3.5: IP Version 6	53
3.5.1 IPv6 Address Representation	54
3.5.2 Allocated IPv6 Addresses	55
Topic 4: Routing	56
Section 4.1: Routing Tables	56
4.1.1: Static Routing	56
4.1.2: Dynamic Routing	57

4.1.3: Routing Updates	57
4.1.4: Verifying Routing Tables	57
Section 4.2: Routing Protocols	57
4.2.1: Distance-Vector Routing	58
4.2.1.1: Route Poisoning	58
4.2.1.2: Split Horizon.....	58
4.2.1.3: Split Horizon with Poison Reverse	58
4.2.1.4: Hold-Down Timer.....	59
4.2.1.5: Triggered Updates.....	59
4.2.2: Link-State Routing.....	59
4.2.3: Classful Routing	59
4.2.4: Classless Routing	60
Section 4.3: Basic Switching Functions.....	60
Section 4.4: Convergence.....	61
4.4.1: Distance-Vector Routing Convergence	61
4.4.1.1: RIP and IGRP Convergence	61
4.4.1.2: EIGRP Convergence.....	62
4.4.2: Link-State Convergence	62
Section 4.5: Testing and Troubleshooting Routes.....	62
4.5.1: The ping Command.....	62
4.5.2: The traceroute Command.....	63
Topic 5: Link-State Protocols	65
Section 5.1: Building Routing Table on New OSPF-Configured Routers	65
Section 5.2: Steady-State Operation.....	67
Section 5.3: OSPF Areas.....	67
5.3.1: OSPF Area Types	67
5.3.2: Router Responsibilities	68
Section 5.4: Balanced Hybrid Routing Protocol and EIGRP	68
5.4.1: EIGRP Loop Avoidance	69
Section 5.5: Router Configuration.....	69
5.5.1: Configuring OSPF	69
5.5.2: Verifying the OSPF Configuration	70
5.5.3: Configuring EIGRP	70
5.5.4: Verifying the EIGRP Configuration.....	70
Topic 6: Advanced TCP/IP	72
Section 6.1: Private IP Addressing.....	72
Section 6.2: Network Address Translation (NAT).....	72
6.2.1: Variations of NAT	73

6.2.1.1: Static NAT	73
6.2.1.2: Dynamic NAT.....	73
6.2.1.3: Overloading NAT with Port Address Translation (PAT).....	73
6.2.1.4: Translating Overlapping Addresses.....	74
6.2.2: Configuring NAT.....	74
6.2.2.1: Configuring Static NAT.....	74
6.2.2.2: Configuring Dynamic NAT	74
6.2.2.3: Configuring NAT Overload and PAT	75
Section 6.3: Internet Control Message Protocol (ICMP)	75
Section 6.4: FTP and TFTP	75
Section 6.5: MTU and Fragmentation	76
Topic 7: Wide Area Networks (WANs)	77
Section 7.1: Point-to-Point Leased Lines	77
7.1.1: Overview.....	77
7.1.2: Data-Link Protocols.....	77
7.1.3: Configuring HDLC and PPP.....	79
Section 7.2: Frame Relay.....	79
7.2.1: Virtual Circuits	80
7.2.2: LMI and Encapsulation Types.....	80
7.2.3: DLCI Addressing.....	81
7.2.4: Frame Relay Configuration	82
7.2.4.1: Determining the Interface	82
7.2.4.2: Configuring Frame Relay Encapsulation.....	82
7.2.4.3: Configuring Protocol-Specific Parameters	82
7.2.4.4: Configuring Frame Relay Characteristics.....	83
7.2.4.5: Verifying Frame Relay Configuration.....	83
Topic 8: IP Access List Security	85
Section 8.1: Standard IP Access Lists	85
8.1.1: Wildcard Masks	86
8.1.2: Standard IP Access List Configuration.....	86
Section 8.2: Extended IP Access Lists.....	86
Section 8.3: Named IP Access Lists.....	87
Section 8.4: Controlling Telnet Access with IP Access Lists.....	87
Appendix A: Decimal to Binary Conversion Table	88
Appendix B: Common TCP and UDP Ports Assignments.....	93

LIST OF TABLES

Table 1.1: The TCP/IP Architectural Model and Protocols.....	21
Table 1.2: Network Definitions	22
Table 1.3: Coaxial Cable for Ethernet	24
Table 1.4: Twisted-Pair and Fiber Optic Cable for Ethernet.....	25
Table 1.5: Fast Ethernet Cabling and Distance Limitations	25
Table 1.6: Gigabit Ethernet Cabling and Distance Limitations.....	26
Table 1.7: The boot system Commands.....	34
Table 4.1: Parameters for the ping Command	63
Table 4.2: Parameters for the traceroute Command	63
Table 5.1: EIGRP, IGRP and OSPF Compared.....	69
Table 6.1: ICMP Messages	75

LIST OF FIGURES

Figure 1.1: The OSI Reference Model.....	18
Figure 1.2: OSI and TCP/IP Models.....	20
Figure 1.3: The Star Topology.....	23
Figure 1.4: The Bus Topology	23
Figure 1.5: The Ring Topology	24
Figure 3.1: Binary Code 1111 1111.....	48
Figure 3.2: Binary Code 1110 1101.....	49
Figure 3.3: Binary Code 1100 0000.1010 1000.0111 1011.....	49
Figure 3.4: The Logical AND Operation.....	53
Figure 4.1: Count To Infinity.....	58

LIST OF ACRONYMS

AAA	Authentication, Authorization, and Accounting
ABR	Area Border Router
ACF	Advanced Communications Function
ACK	Acknowledgment bit (in a TCP segment)
ACL	Access Control List
ACS	Access Control Server
AD	Advertised Distance
ADSL	Asymmetric Digital Subscriber Line
ANSI	American National Standards Institute
API	Application Programming Interface
APPC	Advanced Program-to-Program Communications
ARAP	AppleTalk Remote Access Protocol
ARE	All Routes Explorer
ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
ARPANET	Advanced Research Projects Agency Network
AS	Autonomous System
ASA	Adaptive Security Algorithm
ASBR	Autonomous System Boundary Router
ASCII	American Standard Code for Information Interchange
ASIC	Application Specific Integrated Circuits
ATM	Asynchronous Transfer Mode
AUI	Attachment Unit Interface
Bc	Committed burst (Frame Relay)
B channel	Bearer channel (ISDN)
BDR	Backup Designated Router
Be	Excess burst (Frame Relay)
BECN	Backward Explicit Congestion Notification (Frame Relay)
BGP	Border Gateway Protocol
BGP-4	Border Gateway Protocol version 4
BIA	Burned-in Address (another name for a MAC address)
BOD	Bandwidth on Demand.

BPDU	Bridge Protocol Data Unit
BRF	Bridge Relay Function
BRI	Basic Rate Interface (ISDN)
BSD	Berkeley Standard Distribution (UNIX)
CBT	Core Based Trees
CBWFQ	Class-Based Weighted Fair Queuing
CCITT	Consultative Committee for International Telegraph and Telephone
CCO	Cisco Connection Online
CDDI	Copper Distribution Data Interface
CEF	Cisco Express Forwarding
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Interdomain Routing
CIR	Committed Information Rate. (Frame Relay)
CGMP	Cisco Group Management Protocol
CLI	Command-Line Interface
CLSC	Cisco LAN Switching Configuration
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CR	Carriage Return.
CRC	Cyclic Redundancy Check (error)
CRF	Concentrator Relay Function
CST	Common Spanning Tree
CSU	Channel Service Unit
DB	Data Bus (connector)
DCE	Data Circuit-Terminating Equipment
dCEF	Distributed Cisco Express Forwarding
DDR	Dial-on-Demand Routing
DE	Discard Eligible Indicator
DECnet	Digital Equipment Corporation Protocols
DES	Data Encryption Standard
DHCP	Dynamic Host Control Protocol
DLCI	Data-Link Connection Identifier
DNIC	Data Network Identification Code. (X.121addressing)
DNS	Domain Name System

DoD	Department of Defense (US)
DR	Designated Router
DRiP	Duplicate Ring Protocol
DS	Digital Signal
DS0	Digital Signal level 0
DS1	Digital Signal level 1
DS3	Digital Signal level 3
DSL	Digital Subscriber Line
DSU	Data Service Unit
DTE	Data Terminal Equipment
DTP	Dynamic Trunking Protocol
DUAL	Diffusing Update Algorithm
DVMRP	Distance Vector Multicast Routing Protocol
EBC	Ethernet Bundling Controller
EGP	Exterior Gateway Protocol
EIA/TIA	Electronic Industries Association/Telecommunications Industry Association
EIGRP	Enhanced Interior Gateway Routing Protocol
ESI	End-System Identifier
FCC	Federal Communications Commission
FCS	Frame Check Sequence
FC	Feasible Condition (Routing)
FD	Feasible Distance (Routing)
FDDI	Fiber Distributed Data Interface
FEC	Fast EtherChannel
FECN	Forward Explicit Congestion Notification
FIB	Forwarding Information Base
FIFO	First-In, First-Out (Queuing)
FR	Frame Relay
FS	Feasible Successor (Routing)
FSSRP	Fast Simple Server Redundancy Protocol
FTP	File Transfer Protocol
GBIC	Gigabit Interface Converters
GEC	Gigabit EtherChannel
GSR	Gigabit Switch Router

HDLC	High-Level Data Link Control
HDSL	High data-rate digital subscriber line
HSRP	Hot Standby Router Protocol
HSSI	High-Speed Serial Interface
HTTP	Hypertext Transfer Protocol
I/O	Input/Output
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IDN	International Data Number
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
ILMI	Integrated Local Management Interface
IOS	Internetwork Operating System
IP	Internet Protocol
IPSec	IP Security
IPv6	IP version 6
IPX	Internetwork Packet Exchange (Novell)
IRDP	ICMP Router Discovery Protocol
IS	Information Systems
IS-IS	Intermediate System-to-Intermediate System
ISDN	Integrated Services Digital Network
ISL	Inter-Switch Link
ISO	International Organization for Standardization
ISOC	Internet Society
ISP	Internet Service Provider
ITU-T	International Telecommunication Union–Telecommunication Standardization Sector
kbps	kilobits per second (bandwidth)
LAN	Local Area Network
LANE	LAN Emulation
LAPB	Link Access Procedure, Balanced
LAPD	Link Access Procedure on the D channel
LEC	LAN Emulation Client

LECS	LAN Emulation Configuration Server
LED	Light Emitting Diode
LES	LAN Emulation Server
LLC	Logic Link Control (OSI Layer 2 sublayer)
LLQ	Low-Latency Queuing
LMI	Local Management Interface
LSA	Link-State Advertisement
MAC	Media Access Control (OSI Layer 2 sublayer)
MAN	Metropolitan-Area Network
MD5	Message Digest Algorithm 5
MLS	Multilayer Switching
MLS-RP	Multilayer Switching Route Processor
MLS-SE	Multilayer Switching Switch Engine
MLSP	Multilayer Switching Protocol
MOSPF	Multicast Open Shortest Path First
MSAU	Multistation Access Unit
MSFC	Multilayer Switch Feature Card
MTU	Maximum Transmission Unit
NAK	Negative Acknowledgment
NAS	Network Access Server
NAT	Network Address Translation
NBMA	Nonbroadcast Multiaccess
NetBEUI	NetBIOS Extended User Interface
NetBIOS	Network Basic Input/Output System
NFFC	NetFlow Feature Card
NMS	Network Management System
NNI	Network-to-Network Interface
NSAP	Network Service Access Point
NVRAM	Nonvolatile Random Access Memory
OC	Optical Carrier
ODBC	Open Database Connectivity
OLE	Object Linking and Embedding
OSI	Open Systems Interconnection (Model)
OSPF	Open Shortest Path First

OTDR	Optical Time Domain Reflectometer
OUI	Organizationally Unique Identifier
PAgP	Port Aggregation Protocol
PAP	Password Authentication Protocol
PAT	Port Address Translation
PDN	Public Data Network
PDU	Protocol Data Unit (i.e., a data packet)
PIM	Protocol Independent Multicast
PIM	SM Protocol Independent Multicast Sparse Mode
PIMDM	Protocol Independent Multicast Mode
PIX	Private Internet Exchange (Cisco Firewall)
PNNI	Private Network-to-Network Interface
POP	Point of Presence
POTS	Plain Old Telephone Service
PPP	Point-to-Point Protocol
PQ	Priority Queuing
PRI	Primary Rate Interface (ISDN)
PSTN	Public Switched Telephone Network
PTT	Poste, Telephone, Telegramme
PVC	Permanent Virtual Circuit (ATM)
PVST	Per-VLAN Spanning Tree
PVST+	Per-VLAN Spanning Tree Plus
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RAS	Remote Access Service
RIF	Routing Information Field
RIP	Routing Information Protocol
RJ	Registered Jack (connector)
RMON	Embedded Remote Monitoring
RP	Rendezvous Point
RPF	Reverse Path Forwarding
RSFC	Route Switch Feature Card
RSM	Route Switch Module
RSP	Route Switch Processor

RSTP	Rapid Spanning Tree Protocol
RTP	Reliable Transport Protocol
RTO	Retransmission Timeout
SA	Source Address
SAID	Security Association Identifier
SAP	Service Access Point; also Service Advertising Protocol (Novell)
SAPI	Service Access Point Identifier
SAR	Segmentation and Reassembly
SDLC	Synchronous Data Link Control (SNA)
SIA	Stuck in Active (EIGRP)
SIN	Ships-in-the-Night (Routing)
SLIP	Serial Line Internet Protocol
SMDS	Switched Multimegabit Data Service
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture (IBM)
SNAP	SubNetwork Access Protocol
SNMP	Simple Network Management Protocol
SOF	Start of Frame
SOHO	Small Office, Home Office
SONET	Synchronous Optical Network
SONET/SDH	Synchronous Optical Network/Synchronous Digital Hierarchy
SPAN	Switched Port Analyzer
SPF	Shortest Path First
SPID	Service Profile Identifier
SPP	Sequenced Packet Protocol (Vines)
SPX	Sequenced Packet Exchange (Novell)
SQL	Structured Query Language
SRAM	Static Random Access Memory
SRB	Source-Route Bridge
SRT	Source-Route Transparent (Bridging)
SRTT	Smooth Round-Trip Timer (EIGRP)
SS7	Signaling System 7
SSAP	Source service access point (LLC)
SSE	Silicon Switching Engine.

SSP	Silicon Switch Processor
SSRP	Simple Server Redundancy Protocol
STA	Spanning-Tree Algorithm
STP	Spanning-Tree Protocol; also Shielded Twisted-Pair (cable)
SVC	Switched Virtual Circuit (ATM)
SYN	Synchronize (TCP segment)
TA	Terminal Adapter (ISDN)
TAC	Technical Assistance Center (Cisco)
TACACS	Terminal Access Controller Access Control System
TCI	Tag Control Information
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TCN	Topology Change Notification
TDM	Time-Division Multiplexing
TDR	Time Domain Reflectometers
TFTP	Trivial File Transfer Protocol
TIA	Telecommunications Industry Association
TLV	Type-Length-Value
ToS	Type of Service
TPID	Tag Protocol Identifier
TrBRF	Token Ring Bridge Relay Function
TrCRF	Token Ring Concentrator Relay Function
TTL	Time-To-Live
UDP	User Datagram Protocol
UNC	Universal Naming Convention or Uniform Naming Convention
UNI	User-Network Interface
URL	Uniform Resource Locator
UTC	Coordinated Universal Time (same as Greenwich Mean Time)
UTL	Utilization
UTP	Unshielded Twisted-Pair (cable)
VBR	Variable Bit Rate
VC	Virtual Circuit (ATM)
VID	VLAN Identifier
VIP	Versatile Interface Processor

VLAN	Virtual Local Area Network
VLSM	Variable-Length Subnet Mask
VMPS	VLAN Membership Policy Server
VPN	Virtual Private Network
VTP	VLAN Trunking Protocol
vtty	Virtual terminal line
WAIS	Wide Area Information Server
WAN	Wide Area Network
WFQ	Weighted Fair Queuing
WLAN	Wireless Local Area Network
WWW	World Wide Web
XNS	Xerox Network Systems
XOR	Exclusive-OR
XOT	X.25 over TCP
ZIP	Zone Information Protocol (AppleTalk)

INTRODUCTION

Exam Code: 640-802

Certifications:

Cisco Certified Network Associate (CCNA)

Prerequisites:

None

About This Study Guide

This Study Guide is based on the current pool of exam questions for the Cisco CCNA 640-802 composite exam. As such it provides all the information required to pass the 640-802 exam and is organized around the specific skills that are tested in that exam. Thus, the information contained in this Study Guide is specific to the 640-802 exam and does not represent a complete reference work on the subject of Interconnecting Cisco Networking Devices. Topics covered in this Study Guide includes: Designing or Modifying a simple Local Area Network (LAN) using Cisco Products; Designing an IP Addressing Scheme; Selecting Appropriate Routing Protocols; Designing a simple Internetwork using Cisco products; Developing an Access List to Meet User Specifications; Choosing Wide Area Network (WAN) Services; Managing System Image and Device Configuration Files Performing an Initial Configuration on a Switch; Configuring Routing Protocols; Configuring IP Addresses, Subnet Masks, and Gateway Addresses on Routers and Hosts; Configuring a Router for Additional Administrative Functionality; Configuring a Switch with Virtual LANs (VLANs) and Inter-switch Communication; Implementing a LAN; Customizing a Switch Configuration; Implementing Access Lists; Implementing Simple WAN Protocols; Utilizing the OSI Reference Model as a Guide for Systematic Network Troubleshooting; Performing LAN and VLAN Troubleshooting; Troubleshooting Routing Protocols; Troubleshooting IP Addressing and Host Configuration; Troubleshooting a Device as Part of a Working Network; Troubleshooting an Access List; Performing Simple WAN Troubleshooting; Understanding Network Communications based on Layered Models; Understanding the Components of Network Devices; Understanding the Spanning Tree Process; Evaluating the Characteristics of LAN Environments; Evaluating the TCP/IP Communication Process and its Associated Protocols; Evaluating the Characteristics of Routing Protocols; Evaluating Rules for Packet Control; and Evaluating Key Characteristics of WANs.

Intended Audience

This Study Guide is targeted specifically at people who wish to take the Cisco CCNA 640-802 Composite exam. This information in this Study Guide is specific to the exam. It is not a complete reference work. Although our Study Guides are aimed at new comers to the world of IT, the concepts dealt with in this Study Guide are complex. Knowledge of CompTIA's A+ and Network+ courses would be advantageous.

Note: Because the 640-802 exam is a composite of the 640-822 and 640-816 exams, there is a fair amount of overlap between this Study Guide and the 640-822 and 640-816 Study Guides. However, this Study Guide does not

combine the 640-822 and 640-816 Study Guides but addresses the 640-802 exam specifically. As such, we would not advise using this Study Guide for the 640-822 exam and/or the 640-816 exam.

How To Use This Study Guide

To benefit from this Study Guide we recommend that you:

- Study each chapter carefully until you fully understand the information. This will require regular and disciplined work. Where possible, attempt to implement the information in a lab setup.
- Be sure that you have studied and understand the entire Study Guide before you take the exam.

Note: Remember to pay special attention to these note boxes as they contain important additional information that is specific to the exam.

Good luck!

Topic 1: Networking Fundamentals

Section 1.1: The OSI Reference Model

The OSI is the Open System Interconnection reference model for communications. As illustrated in Figure 1.1, the OSI reference model consists of seven layers, each of which can have several sublayers. The upper layers of the OSI reference model define functions focused on the application, while the lower three layers define functions focused on end-to-end delivery of the data.

- The **Application Layer (Layer 7)** refers to communications services to applications and is the interface between the network and the application. Examples include: Telnet, HTTP, FTP, Internet browsers, NFS, SMTP gateways, SNMP, X.400 mail, and FTAM.
- The **Presentation Layer (Layer 6)** defining data formats, such as ASCII text, EBCDIC text, binary, BCD, and JPEG. Encryption also is defined as a presentation layer service. Examples include: JPEG, ASCII, EBCDIC, TIFF, GIF, PICT, encryption, MPEG, and MIDI.
- The **Session Layer (Layer 5)** defines how to start, control, and end communication sessions. This includes the control and management of multiple bidirectional messages so that the application can be notified if only some of a series of messages are completed. This allows the presentation layer to have a seamless view of an incoming stream of data. The presentation layer can be presented with data if all flows occur in some cases. Examples include: RPC, SQL, NFS, NetBios names, AppleTalk ASP, and DECnet SCP
- The **Transport Layer (Layer 4)** defines several functions, including the choice of protocols. The most important Layer 4 functions are error recovery and flow control. The transport layer may provide for retransmission, i.e., error recovery, and may use flow control to prevent unnecessary congestion by attempting to send data at a rate that the network can accommodate, or it might not, depending on the choice of protocols. Multiplexing of incoming data for different flows to applications on the same host is also performed. Reordering of the incoming data stream when packets arrive out of order is included. Examples include: TCP, UDP, and SPX.
- The **Network Layer (Layer 3)** defines end-to-end delivery of packets and defines logical addressing to accomplish this. It also defines how routing works and how routes are learned; and how to fragment a packet into smaller packets to accommodate media with smaller maximum transmission unit sizes. Examples include: IP, IPX, AppleTalk DDP, and ICMP. Both IP and IPX define logical addressing, routing, the learning of routing information, and end-to-end delivery rules. The IP and IPX protocols most closely match the OSI network layer (Layer 3) and are called Layer 3 protocols because their functions most closely match OSI's Layer 3.
- The **Data Link Layer (Layer 2)** is concerned with getting data across one particular link or medium. The data link protocols define delivery across an individual link. These protocols are necessarily concerned with the type of media in use. Examples include: IEEE 802.3/802.2, HDLC, Frame Relay, PPP, ATM, and IEEE 802.5/802.2.
- The **Physical Layer (Layer 1)** deals with the physical characteristics of the transmission medium. Connectors, pins, use of pins, electrical currents, encoding, and light modulation are all part of different

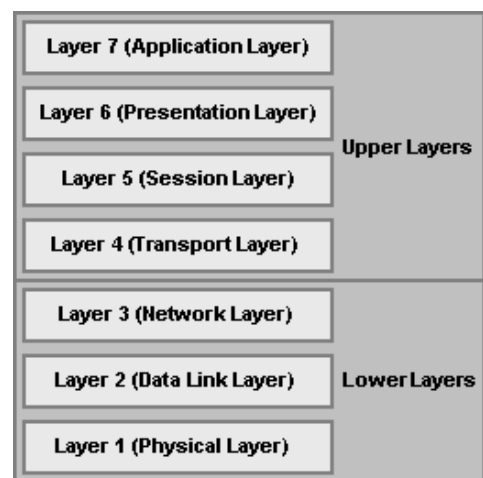


Figure 1.1: The OSI Reference Model

physical layer specifications. Examples includes: EIA/TIA-232, V.35, EIA/TIA-449, V.24, RJ-45, Ethernet, 802.3, 802.5, NRZI, NRZ, and B8ZS.

The upper layers of the OSI reference model, i.e., the Application Layer (Layer 7), the Presentation Layer (Layer 6), and the Session Layer (Layer 5), define functions focused on the application. The lower four layers, i.e., the Transport Layer (Layer 4), the Network Layer (Layer 3), the Data Link Layer (Layer 2), and the Physical Layer (Layer 1), define functions focused on end-to-end delivery of the data. As a Cisco Certified Network Associate, you will deal mainly with the lower layers, particularly the data link layer (Layer 2) upon which switching is based, and the network layer (Layer 3) upon which routing is based.

1.1.1: Interaction Between OSI Layers

When a host receives a data transmission from another host on the network, that data is processed at each of the OSI layers to the next higher layer, in order to render the data transmission useful to the end-user. To facilitate this processing, headers and trailers are created by the sending host's software or hardware, that are placed before or after the data given to the next higher layer. Thus, each layer has a header and trailer, typically in each data packet that comprises the data flow. The sequence of processing at each OSI layer, i.e., the processing between adjacent OSI layers, is as follows:

- The **Physical Layer** (Layer 1) ensures **bit synchronization** and places the received binary pattern into a buffer. It notifies the Data Link Layer (Layer 2) that a frame has been received after decoding the incoming signal into a bit stream. Thus, Layer 1 provides delivery of a stream of bits across the medium.
- The **Data Link Layer** (Layer 2) examines the **frame check sequence (FCS)** in the trailer to determine whether errors occurred in transmission, providing **error detection**. If an error has occurred, the frame is discarded. The current host examines data link address is examined to determine if the data is addressed to it or whether to process the data further. If the data is addressed to the host, the data between the Layer 2 header and trailer is handed over to the Network Layer (Layer 3) software. Thus, the data link layer delivers data across the link.
- The **Network Layer** (Layer 3) examines the destination address. If the address is the current host's address, processing continues and the data after the Layer 3 header is handed over to the Transport Layer (Layer 4) software. Thus, Layer 3 provides end-to-end delivery.
- If error recovery was an option chosen for the **Transport Layer** (Layer 4), the counters identifying this piece of data are encoded in the Layer 4 header along with acknowledgment information, which is called **error recovery**. After error recovery and reordering of the incoming data, the data is given to the Session Layer (Layer 5).
- The **Session Layer** (Layer 5) ensures that a series of messages is completed. The Layer 5 header includes fields signifying sequence of the packet in the data stream, indicating the position of the data packet in the flow. After the session layer ensures that all flows are completed, it passes the data after the Layer 5 header to the Presentation Layer (Layer 6) software.
- The **Presentation Layer** (Layer 6) defines and manipulates the data format of the data transmission. It converts the data to the proper format specified in the Layer 6 header. Typically, this header is included only for initialization flows, not with every data packet being transmitted. After the data formats have been converted, the data after the Layer 6 header is passed to the Application Layer (Layer 7) software.
- The **Application Layer** (Layer 7) processes the final header and examines the end-user data. This header signifies agreement to operating parameters by the applications on the two hosts. The headers are used to signal the values for all parameters; therefore, the header typically is sent and received at application initialization time only.

In addition to processing between adjacent OSI layers, the various layers must also interact with the same layer on another computer to successfully implement its functions. To interact with the same layer on another computer, each layer defines additional data bits in the header and, in some cases, trailer that is created by the sending host's software or hardware. The layer on the receiving host interprets the headers and trailers created by the corresponding layer on the sending host to determine how that layer's processing is being defined, and how to interact within that framework.

Section 1.2: TCP/IP and the OSI Reference Model

As illustrated in Figure 1.2, the Transmission Control Protocol/Internet Protocol (TCP/IP) model consists of four layers, each of which can have several sublayers. These layers correlate roughly to layers in the OSI reference model and define similar functions. Some of the TCP/IP layers correspond directly with layers in the OSI reference model while others span several OSI layers. The four TCP/IP layers are:

- The **TCP/IP Application Layer** refers to communications services to applications and is the interface between the network and the application. It is also responsible for presentation and controlling communication sessions. It spans the Application Layer, Presentation Layer and Session Layer of the OSI reference model. Examples include: HTTP, POP3, and SNMP.
- The **TCP/IP Transport Layer** defines several functions, including the choice of protocols, error recovery and flow control. The transport layer may provide for retransmission, i.e., error recovery, and may use flow control to prevent unnecessary congestion by attempting to send data at a rate that the network can accommodate, or it might not, depending on the choice of protocols. Multiplexing of incoming data for different flows to applications on the same host is also performed. Reordering of the incoming data stream when packets arrive out of order is included. It correlates with the Transport Layer of the OSI reference model. Examples include: TCP and UDP, which are called Transport Layer, or Layer 4, protocols.
- The **TCP/IP Internetwork Layer** defines end-to-end delivery of packets and defines logical addressing to accomplish this. It also defines how routing works and how routes are learned; and how to fragment a packet into smaller packets to accommodate media with smaller maximum transmission unit sizes. It correlates with the Network Layer of the OSI reference model. Examples include: IP and ICMP.
- The **TCP/IP Network Interface Layer** is concerned with the physical characteristics of the transmission medium as well as getting data across one particular link or medium. This layer defines delivery across an individual link as well as the physical layer specifications. It spans the Data Link Layer and Physical Layer of the OSI reference model. Examples include: Ethernet and Frame Relay.

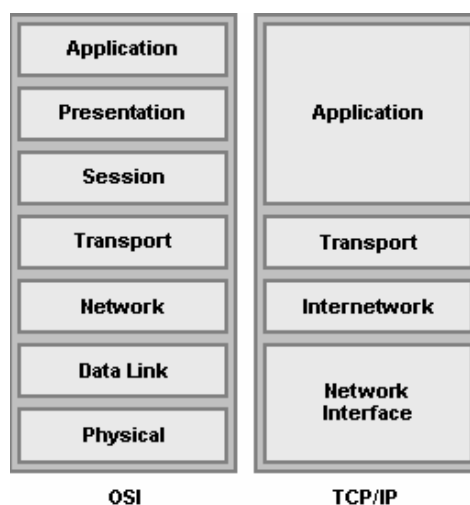


Figure 1.2: OSI and TCP/IP Models

1.2.1: The TCP/IP Protocol Architecture

TCP/IP defines a large collection of protocols that allow computers to communicate. Table 1.1 outlines the protocols and the TCP/IP architectural layer to which they belong. TCP/IP defines the details of each of these protocols in **Requests For Comments (RFC)** documents. By implementing the required protocols defined in TCP/IP RFCs, a computer that implements the standard networking protocols defined by TCP/IP can communicate with other computers that also use the TCP/IP standards.

Table 1.1: The TCP/IP Architectural Model and Protocols

TCP/IP Architecture Layer	Protocols
Application	HTTP, POP3, SMTP
Transport	TCP, UDP
Internetwork	IP
Network interface	Ethernet, Frame Relay

1.2.2: TCP/IP Data Encapsulation

The term encapsulation describes the process of putting headers and trailers around some data. A computer that needs to send data encapsulates the data in headers of the correct format so that the receiving computer will know how to interpret the received data. Data encapsulation with TCP/IP consists of five-steps:

Step 1: Create the application data and headers.

Step 2: Package the data for transport, which is performed by the transport layer (TCP or UDP). The Transport Layer creates the transport header and places the data behind it.

Step 3: Add the destination and source network layer addresses to the data, which is performed by the Internetwork Layer. The Internetwork Layer creates the network header, which includes the network layer addresses, and places the data behind it.

Step 4: Add the destination and source data link layer addresses to the data, which is performed by the Network Interface Layer. The Network Interface Layer creates the data link header, places the data behind it, and places the data link trailer at the end.

Step 5: Transmit the bits, which is performed by the Network Interface Layer. The Network Interface Layer encodes a signal onto the medium to transmit the frame.

Section 1.3: Networks

A network is defined as a group of two or more computers linked together for the purpose of communicating and sharing information and other resources, such as printers and applications. Most networks are constructed around a cable connection that links the computers, however, modern wireless networks that use radio wave or infrared connections are also becoming quite prevalent. These connections permit the computers to communicate via the wires in the cable, radio wave or infrared signal. For a network to function it must provide connections, communications, and services.

- **Connections** are defined by the hardware or physical components that are required to connect a computer to the network. This includes the **network medium**, which refers to the hardware that physically connects one computer to another, i.e., the network cable or a wireless connection; and the **network interface**, which refers to the hardware that attaches a computer to the network medium and is usually a network interface card (NIC).
- **Communications** refers to the network protocols that are used to establish the rules governing network communication between the networked computers. Network protocols allow computers running different operating systems and software to communicate with each.
- **Services** define the resources, such as files or printers, that a computer shares with the rest of the networked computers.

1.3.1: Network Definitions

Computer networks can be classified and defined according to geographical area that the network covers. There are four network definitions: a Local Area Network (LAN), a Campus Area Network (CAN), a Metropolitan Area Network (MAN), and a Wide Area Network (WAN). There are three additional network definitions, namely the Internet, an intranet and an Internetwork. These network definitions are discussed in Table 1.2.

Table 1.2: Network Definitions

Definition	Description
Local Area Network (LAN)	A LAN is defined as a network that is contained within a closed environment and does not exceed a distance of 1.25 mile (2 km). Computers and peripherals on a LAN are typically joined by a network cable or by a wireless network connection. A LAN that consists of wireless connections is referred to as a Wireless LAN (WLAN) .
Campus Area Network (CAN)	A CAN is limited to a single geographical area but may exceed the size of a LAN
Metropolitan Area Network (MAN)	A MAN is defined as a network that covers the geographical area of a city that is less than 100 miles.
Wide Area Network (WAN)	A WAN is defined as a network that exceeds 1.25 miles. A WAN often consists of a number of LANs that have been joined together. A CAN and a MAN is also a WAN. WANs typically connected numerous LANs through the internet via telephone lines, T1 lines, Integrated Services Digital Network (ISDN) lines, radio waves, cable or satellite links.
Internet	The Internet is a world wide web of networks that are based on the TCP/IP protocol and is not own by a single company or organization.
Intranet	An intranet uses that same technology as the Internet but is owned and managed by a company or organization. A LAN or a WAN s usually an intranet.
Internetwork	An internetwork consists of a number of networks that are joined by routers. The Internet is the largest example of an internetwork.

Of these network definitions, the most common are the Internet, the LAN and the WAN.

1.3.2: Types of Networks

These network definitions can be divided into two types of networks, based on how information is stored on the network, how network security is handled, and how the computers on the network interact. These two types are: **Peer-To-Peer (P2P) Networks** and **Server/Client Networks**. The latter is often also called Server networks.

- On a **Peer-To-Peer (P2P) Network**, there is no hierarchy of computers; instead each computer acts as either a server which shares its data or services with other computers, or as a client which uses data or services on another computer. Furthermore, each user establishes the security on their own computers and determines which of their resources are made available to other users. These networks are typically limited to between 15 and 20 computers. Microsoft Windows for Workgroups, Windows 95, Windows 98, Windows ME, Windows NT Workstation, Windows 2000, Novell's NetWare, UNIX, and Linux are some operating systems that support peer-to-peer networking.
- A **Server/Client Network** consists of one or more dedicated computers configured as servers. This server manages access to all shared files and peripherals. The server runs the network operating system (NOS) manages security and administers access to resources. The client computers or workstations connect to the network and use the available resources. Among the most common network operating systems are Microsoft's Windows NT Server 4, Windows 2000 Server, and Novell's NetWare. Before the release of Windows NT, most dedicated servers worked only as hosts. Windows NT allows these servers to operate as an individual workstation as well.

1.3.3: Network Topologies

The layout of a LAN design is called its topology. There are three basic types of topologies: the star topology, the bus topology, and the ring topology. Hybrid combinations of these topologies also exist.

- In a network based on the **star topology**, all computers and devices are connected to a centrally located hub or switch. The hub or switch collects and distributes the flow of data within the network. When a hub is used, data from the sending host are sent to the hub and are then transmitted to all hosts on the network except the sending host. Switches can be thought of as intelligent hubs. When switches are used rather than hubs, data from the sending host are sent to the switch which transmits the data to the intended recipient rather than to all hosts on the network.
- In a network based on the **bus topology**, all computers and devices are connected in series to a single linear cable called a trunk. The trunk is also known as a backbone or a segment. Both ends of the trunk must be terminated to stop the signal from bouncing back up the cable. Because a bus network does not have a central point, it is more difficult to troubleshoot than a star network. Furthermore, a break or problem at any point along the bus can cause the entire network to go down.

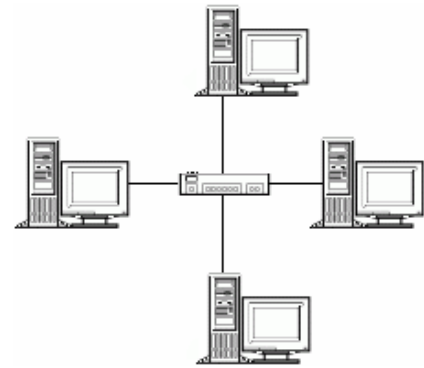


Figure 1.3: The Star Topology



Figure 1.4: The Bus Topology

