CDC 4A251A

Biomedical Equipment Journeyman

Volume 4. Medical Device Information Systems

Air Force Career Development Academy
Air University
Air Education and Training Command

4A251A 04 1812, Edit Code 04
AFSC 4A251

Author: MSgt Jason E. Johnson, CBET, Sec+
MSgt Matthew J. Colica, CBET, Sec+
382nd Training Squadron
59th Training Group (AETC)
382 TRS/TRR
3068 William Hardee Rd, MIF 1 Bldg 899
JBSA Ft Sam Houston, TX 78234
DSN: 420-1644
E-mail address: jason.johnson.32@us.af.mil
matthew.colica@us.af.mil

Instructional Systems Specialist: Gary L. McLean

Editor: Evangeline K. Walmsley

Air Force Career Development Academy (AFCDA)
Air University (AETC)
Maxwell AFB, Gunter Annex, Alabama 36114-3107

Material in this volume is reviewed annually for technical accuracy, adequacy, and currency. For Weighted Airman Promotion System (WAPS) Specialty Knowledge Test (SKT) purposes, the examinee should check the *Enlisted Promotions References and Requirements Catalog* to determine the correct references to study.

THIS FOURTH AND LAST VOLUME OF CDC 4A251A, *Biomedical Equipment Journeyman,* provides a foundation of knowledge for maintaining computer based medical systems.

Unit 1 serves as an introduction to healthcare information technology and topics including electromagnetic emission concerns to system accreditation. Unit 2 identifies computer core hardware and provides information on how they function. Unit 3 gives you a good working knowledge on how computer systems are networked and how protocols function and expand the network. Unit 4 covers some basic security information to protect network and computer components.

A glossary is included for your use.

Code numbers on figures are for preparing agency identification only.

The use of a name of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

To get a response to your questions concerning subject matter in this course, or to point out technical errors in the text, unit review exercises, or course examination, call or write the author using the contact information on the inside front cover of this volume.

NOTE: Do not use Air Force Instruction (AFI) 38-402, *Airmen Powered by Innovation,* to submit corrections for printing or typographical errors. For Air National Guard (ANG) members, do not use Air National Guard Instruction (ANGI) 38-401, *Suggestion Program.*

If you have questions that your supervisor, training manager, or education/training office cannot answer regarding course enrollment, course material, or administrative issues, please contact Air University Educational Support Services at http://www.aueducationsupport.com. Be sure your request includes your name, the last four digits of your social security number, address, and course/volume number.

This volume is valued at 15 hours and 5 points.

Acknowledgment

PREPARATION OF THIS VOLUME was aided through the cooperation and courtesy of Creative Commons (CC) for graphical support. The figures listed here have been reproduced and attributed in accordance with their release or applicable license.

Literature	CDC Figure Number
Motherboard (Licensed by Creative Common [CC] BY Share Alike [SA] 3.0)	F2–2
Motherboard Chipsets (CC BY SA 3.0)	F2–3
Router (CC BY SA 3.0)	F3–16
DDR4RAM (CC BY SA 4.0)	F2–5
Top and Bottom View of a CPU (CC BY SA 3.0)	F2–6
Diagram of CPU Control Unit, ALU, and registers (CC BY SA 4.0.)	F2–7
Clogged CPU Heatsink (CC BY SA 3.0)	F2–8
HDD External and Internal View (CC BY SA 3.0)	F2–14
NAS device (CC BY SA 3.0)	F2–18
IP Datagram Structure (CC BY SA 3.0)	F3–9
Switches (CC BY SA 3.0)	F3–15

In accordance with all of the copyright agreements, distribution of this volume is limited to DOD personnel. The material covered by this permission may not be placed on sale by the federal government and must follow proper attribution of each applicable license.

NOTE:

In this volume, the subject matter is divided into self-contained units. A unit menu begins each unit, identifying the lesson headings and numbers. After reading the unit menu page and unit introduction, study the section, answer the self-test questions, and compare your answers with those given at the end of the unit. Then complete the unit review exercises.

Page

Unit 1. Healthcare Information Technology

IN THE RAPID EVOLUTION of healthcare information technology (IT), hospitals have grown from having a few simple individual systems to operating robust, complex networked computer systems and applications. This expansion in IT has become a significant component of delivering patient care and established the need for medical facilities to have integrated networks, standards, and increased security. More medical devices are now designed to send, receive, or store data and you must have adequate IT knowledge and skills to maintain these medical devices and their interfaces properly.

1–1. Introduction to Healthcare Information Technology

There used to be a distinct separation between IT and biomedical equipment. This made it easier to delineate equipment responsibilities between biomedical equipment technicians (BMET) or systems administration personnel. For this reason, there was no need for BMETs to learn how to maintain IT equipment and networks. However, now a large amount of medical devices have IT incorporated into its design, which has blurred this line and increased the need to learn IT principles so you can appropriately support the equipment. This section provides an overview of the current state in healthcare IT, the Health Insurance Portability and Accountability Act (HIPAA) and some general IT applications.

601. Healthcare information technology principles overview

Healthcare IT involves the exchange of patient health information in electronic format. Medical devices such as X-ray systems, anesthesia equipment, picture archiving and communication systems (PACS), and patient monitoring devices are some examples of equipment that incorporate IT into its design and functionality. Some benefits of IT use in the health care industry are the following:

- Improves the quality of patient care.
- Assists in the prevention of medical errors.
- Reduces medical costs.
- Increases staff efficiencies.
- Decreases the amount of paperwork.
- Expands access to health care.

These benefits illustrate the importance of healthcare IT implementation. In addition to the benefits, a number of factors have contributed to the expansion of healthcare IT over the past few years:

- Increase in the number of network-enabled devices.
- Access to healthcare through mobile devices, patient portals, and cloud services.
- Cybersecurity threats.
- Integration of healthcare networks.
- Volume of patient data.
- The need to analyze big data.

Patients have embraced the use of mobile devices, portals, and the Internet for all aspects of healthcare. There is a demand for secure and easy access to healthcare information via healthcare applications and services delivered through the Internet. For example, electronic health records (EHR) were only core applications operating in a healthcare system's data center, but now are commonly a hosted service. It is important to ensure the privacy and security of health information when it is electronically or manually maintained and transmitted. HIPAA is United States legislation that addresses this concern.

Health Insurance Portability and Accountability Act

The purpose of HIPAA is to improve the portability and continuity of health insurance coverage and to simplify the administration of healthcare. For BMETs, the major component of HIPAA provisions is the protection and privacy of individually identifiable health information, which is in Title 45, Code of Federal Regulations (CFR) Parts 160 and 164. The HIPAA Privacy Rule governs this component, and Department of Defense (DOD) 6025.18-R, *DOD Health Information Privacy Regulation*, implements the requirements of the HIPAA Privacy Rule throughout the military health system.

You must review all new equipment requests to ensure it complies with the requirements of HIPAA. Your shop's acceptance inspection process must include procedures that verify compliance with the policies of your local military treatment facility (MTF) HIPAA privacy officer (HPO) and HIPAA security officer (HSO). It is important you ensure *all* of your shop's procedures or policies comply with your HPOs and HSOs policies. The MTF commander appoints the HPO and HSO and one person may fill both positions.

It is also important that contracts and leases include specific provisions required by the HIPAA privacy and security rules. This is so that contractors who have access to protected health information (PHI) as part of their provided service are fully aware of your MTF's HIPAA policies and the ramifications if they fail to comply.

BMETs are required to maintain a list of all equipment that stores PHI. If equipment has this capability, make sure to select Contains Patient Data in the Defense Medical Logistics Standard Support (DMLSS) Equipment Detail tab for the equipment control number (ECN). This enables DMLSS to produce an accurate list of all equipment that stores PHI by simply running the Equipment Containing Patient Data Report in the Equipment Maintenance module.

Every attempt to remove all PHI from medical devices without permanently damaging the device must be made before sending medical equipment to service providers outside of your MTF. If you *cannot* remove all PHI without damaging the device, ensure you have a signed business associate agreement with the service provider in accordance with your local MTF HIPAA policy before removing the equipment from your MTF or facility. A business associate agreement is a legal agreement between a covered entity (your MTF) and a business associate (service provider) that the business associate will appropriately safeguard any PHI it receives from the entity.

You must remove all PHI storage media from equipment prior to sending it to the Defense Logistics Agency Disposition Services (DLA-DS) or reporting it as excess. If you cannot remove the storage media, then you must clear and purge, or destroy it in accordance with Air Force Manual (AFMAN) 17-1301, *Computer Security (COMPUSEC)*, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, *Guidelines for Media Sanitization*. If the unit was fully functional prior to cleansing, attach a Department of Defense (DD) Form 1577-2, Unserviceable (Reparable) Tag - Materiel (referred to as a "green" tag), annotating that application software will need to be reinstalled and the unit fully tested before further operation. The following table provides more detail on the actions of clearing, purging, and destroying.

Type	Description
Clear	This is a method of sanitization that applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques. It is typically applied through the standard *read and write* commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported). Clearing must not allow information to be retrieved by data, disk, or file recovery utilities. It must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. There are overwriting software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table), but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not writeable. The media type and size may also influence whether overwriting is a suitable sanitization method. Most of today's media can be effectively cleared by one overwrite.
Purge	This is a method of sanitization that applies physical or logical techniques that render target data recovery infeasible using state of the art laboratory techniques. For some media, clearing media would not suffice for purging. However, for Advanced Technology Attachment (ATA) disk drives manufactured after 2001 (over 15 gigabytes) the terms clearing and purging have converged. Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is destroyed also. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A *degausser* is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (e.g., low energy or high energy) of magnetic media they can purge and operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, media with exceptionally large storage capacities, or for quickly purging diskettes. If purging media is not a feasible sanitization method for your organization, it is recommended that you destroy the media.
Destroy	This method, destruction of media, is the ultimate form of sanitization. After media is destroyed, it cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding, and melting. Disintegration, incineration, pulverization, and melting are designed to destroy the media completely. Typically, these actions are carried out at a facility with the specific capabilities to perform these activities effectively, securely, and safely. Paper shredders can destroy flexible media such as diskettes once the media is removed from its outer container physically. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality level that the information cannot be reconstructed. Optical mass storage media, including compact discs (CD), CD ReWritable (CD-RW), CD Recordable (CD-R), CD Read Only Memory (CD-ROM), and digital video discs (DVD) must be destroyed by pulverizing, crosscut shredding, or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of 5 millimeters and surface areas of 25-square millimeters.

Another general concern of healthcare IT and medical devices is electromagnetic emissions and their compatibility with one another.

Electromagnetic emission considerations

Electromagnetic emissions are electromagnetic energy emitted from a device; this generally falls into two categories: conducted and radiated. Both categories of emission can occur simultaneously, depending on the configuration of the device.

Type	Description
Conducted emissions	This type of emission is electromagnetic energy emanating from equipment through a conductor by means of resistance, inductance, or capacitance. Conductors *include* power cords, metallic enclosures of subsystems, or cables that interconnect subsystems or the patient to the equipment. Conducted emissions include power line harmonics, surges, and radio frequency (RF) energy, especially in the frequency range 150 kilohertz to 80 megahertz.
Radiated emissions	This type of emission is electromagnetic energy emanating from a device and propagating through space or a medium (which can affect the distance and direction of propagation). Radiated emissions include both intentional emissions such as radio transmissions carrying information and unintentional emissions associated with electrically powered equipment such as motors, power supplies, and computer components.

A primary concern of electromagnetic emission is RF energy and wireless technology. Although research shows risk to be extremely low, some medical units prohibit or limit the use of smartphones and cellular phones in an effort to help prevent any RF energy from causing any electromagnetic interference (EMI) with medical devices in close proximity. There are many medical devices with incorporated wireless technology and some considerations for the safe and effective use of these devices are the selection of wireless technology, security, and electromagnetic compatibility (EMC) with other devices.

Selection of wireless technology

When selecting or analyzing potential wireless technology you should consider safety-related requirements and issues relating to the integrity of the data wirelessly transmitted including latency (delay of signal) and throughput, detection, correction, and corruption control and/or prevention. Potential risks that can affect reliable wireless medical device functions include data corruption or loss and interference from simultaneous transmissions in a location, which may increase latency and transmittal signal error rates. BMETs should incorporate error control processes for wireless medical devices to assure the integrity of data wirelessly transmitted and to manage potential risks related to delays of data transfer. Parameters such as bit error rate, packet loss, and signal-to-noise ratio are useful tools in assessing and assuring data integrity and timeliness of data transmission.

You should also consider the device performance and specifications (e.g., Institute of Electrical and Electronics Engineers [IEEE] 802.11n) related to the wirelessly enabled medical device when choosing the appropriate RF wireless technology, and the RF frequency of operation. It is important to note that many medical devices are authorized to operate as unlicensed devices in the industrial, scientific, and medical frequency bands (e.g., 2400-2493.5 megahertz), and therefore, are not entitled to interference protection. There is a potential for interference in this frequency band, due to its heavy use by many other communications and industrial products. In many cases, RF wireless medical devices incorporate technology such as frequency hopping protocols and correction protocols to minimize effects of interference that may lead to data errors or corruption. In addition, to help protect against EMI to other medical devices in the vicinity, the United States Food and Drug Administration (FDA) recommends that wireless medical device manufacturers limit the RF output of their devices to the lowest power necessary to accomplish the intended functions reliably.

Security of wireless technology

Security of RF wireless technology is a means to prevent unauthorized access to patient data or hospital networks and to ensure that information and data received by a device are intended for that device. Authentication and wireless encryption play vital roles in an effective wireless security scheme. While most wireless technologies have encryption schemes available, wireless encryption needs to be enabled and assessed for adequacy for the medical device's intended use. Security management should also consider that certain wireless technologies incorporate sensing of similar technologies and attempt to make automatic connections to quickly assemble and use a network (e.g., a discovery mode such as that available in Bluetooth® communications). For some wireless medical devices, this kind of discovery mode could pose safety and effectiveness concerns.

The FDA recommends that wireless medical devices use wireless protection such as wireless encryption and data access controls at a level appropriate for the risks presented by the medical device, its environment of use, the type, and probability of the risks to which it is exposed, and the probable risks to patients from a security breach.

EMC with other devices

When analyzing the potential use of wireless medical devices, you should attempt to identify any potential issues associated with EMC and determine the risk acceptability criteria based on information about the device and its intended use. It should include any foreseeable misuses, sources of environmental electromagnetic disturbance (EMD), such as radio transmitters or computer RF wireless equipment, and the potential for RF emissions to affect other devices. If the RF wireless medical device is used in proximity to other RF wireless sources, you should address such risks by testing for coexistence of the devices.

When evaluating equipment request packages and performing acceptance inspections, it is important that you properly address HIPAA and EMC concerns to avoid costly problems or privacy violations later on down the road. Next, we will briefly cover a few general medical device information systems you are responsible to support in your MTF.

602. Basics of general healthcare information technology applications

In this lesson, we will discuss EHR management equipment interface and the clinical applications of automated & decentralized medication management systems. These are only a few applications and systems you support as a BMET. Career development course (CDC) 4A251B will cover pertinent diagnostic imaging, therapeutic, and support equipment.

The EHR management equipment interface

BMETs typically do not focus on EHRs. Your systems administration section will primarily be responsible for EHR's software and hardware. However, you will be involved with ensuring that equipment can connect and communicate with your MTF's EHR system. This process could include configuring a medical device's software or hardware so it can be compatible with the EHR system. Currently, medical devices are not manufactured to work seamlessly with a particular EHR system. Due to this reason, middleware is used to integrate medical devices and EHRs (fig. 1–1).

Middleware is software that provides services to software applications beyond those available from the operating system, by performing as a bridge between the operating system and application. The type of connection and hardware required will be dependent on the middleware that is used. The medical device may connect via registered jack (RJ) 45, recommended standard (RS)-232, or wirelessly (Bluetooth, 802.11x, etc.) Some middleware utilize aggregators, so the medical device may be required to connect to the aggregator before being sent to the EHR system. The aggregator simply collects and reformats data from the medical devices.

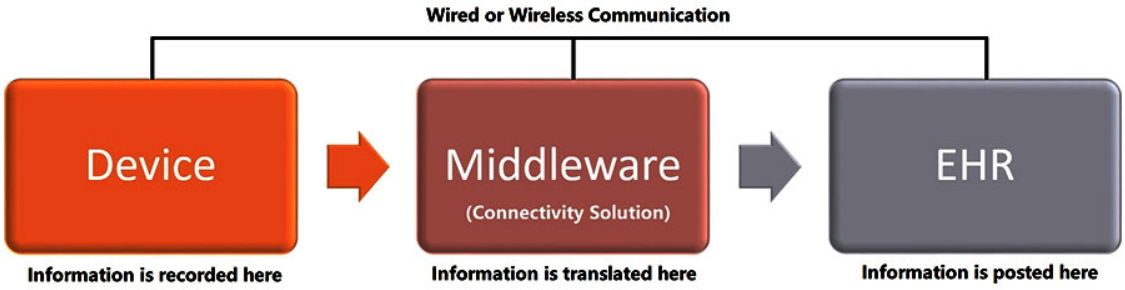


Figure 1–1. Middleware solution for EHR.

In your career, you will probably see multiple iterations of EHR systems incorporated in the Air Force Medical Service (AFMS) and each will function slightly different. You do not need to become an expert in EHR systems, but it is important that you understand the impact it has on medical devices. The input you provide as a BMET may drive your MTF to replace equipment that cannot connect to the proposed EHR system or to purchase additional equipment such as network interface controllers (NIC) and aggregators to make devices compatible.

Automated medication dispensing systems clinical applications

Automated dispensing systems are drug storage devices that electronically control and track medication distribution. Pharmacists and technicians scan medication bottles, assign it to a location, and then fill the container. On most models, the unit automatically counts the pills or capsules as the container is being filled. Most units can be replenished by one technician simultaneously while filling a prescription for another technician. This increases the efficiency of the pharmacy staff. Automated medication dispensing systems also generate refill requests when supplies fall below a preset level. Figure 1–2 shows a pharmacy technician using an automated medication dispensing system to fill a prescription.

Figure 1–2. Automated medication dispensing system.

Decentralized medication management systems clinical applications

The primary advantage that decentralized medication management systems offer is that it allows hospital staff to obtain medications for inpatients at the point of use. These units control access through some type of log on process (password, badge, and so forth). The system then tracks who

accesses the system and the patients for whom the medications were administered. Figure 1–3 depicts a staff member retrieving meds from a decentralized medication management system.

Figure 1–3. Decentralized medication management system.

Decentralized medication management systems generate reports on its medication levels. These units have the ability to be networked. This enables them to send the reports to the central pharmacy to alert staff of low medication levels in the decentralized medication management systems, so the units can be refilled. Use of these units reduces the need for hospital staff to access the central pharmacy and limits hospital staff access to controlled substances.

Self-Test Questions

After you complete these questions, you may check your answers at the end of the unit.

601. Healthcare information technology principles overview

1. List the factors contributing to the expansion of healthcare IT.

2. What is the major component of HIPAA as it pertains to BMET duties? Where is it located?

3. Whom should you contact in your MTF if you questions regarding HIPAA compliance?

4. How do you enable DMLSS's ability to produce an accurate list of equipment that stores PHI?

5. What is a business associate agreement and when would you use one?

6. What must you do prior to turning in a known functional medical device to DLA-DS after you cleanse PHI from it?

7. What is the protection difference between clearing, purging, and destroying?

8. Explain the two categories of electromagnetic emissions.

9. What three items should you consider for the safe and effective use of wireless devices?

602. Basics of general healthcare information technology applications

1. What role do BMETs typically have in regards to EHRs?

2. What is the purpose for middleware in an EHR system?

3. What actions do automated medication dispensing systems perform?

4. What equipment limits staff's access to controlled substances?

1–2. Roles and Responsibilities

The MTF staff must have the ability to collect, store, maintain, and retrieve timely and accurate information, which is essential for patient care and organizational needs. Successfully managed health information technology has established guidance, with unifying principles, and a minimum set of standardized practices. Each requirement and process has a common vision and understanding that supports what the MTF and all AFMS customers need in order to accomplish their mission. We will now cover the IT roles in the MTF and some responsibilities of BMETs with privileged access.

603. The information technology roles and relationships in the military treatment facility

To keep up with the rapidly transforming cyber environment, the DOD consistently updates and adjusts its regulations and directives. For example, you may have heard of the DOD Information Assurance Certification and Accreditation Process (DIACAP), it has been replaced by Risk Management Framework (RMF) to improve IT categorization and control selection, and risk management procedures.

Cybersecurity workforce functions must be identified and managed, and the personnel performing cybersecurity functions must be appropriately screened. DOD Instruction (DODI) 8500.01, *Cybersecurity*, establishes the roles and responsibilities required to maintain DOD systems, platforms, and networks. DOD 8570.01-M, *Information Assurance Workforce Improvement Program*, provides guidance and procedures for the training, certification, and management of personnel conducting information assurance (IA) functions for the DOD.

AFMS units are structured slightly different from other base organizations. Instead of the organization reporting directly to the base communication squadron, the MTF has a system administration flight that is directly responsible for the network, and associated hardware and software. The systems administration flight then reports to the Defense Health Agency (DHA) with coordination and support of base communication squadron as required. The systems administration flight typically consists of Medical Service Corps (MSC) officers, civilian government employees, and health services management technicians, commonly referred to as 4A0's due to their 4A0X1 Air Force specialty code (AFSC). Due to medical devices increase of network capabilities, BMETs are beginning to perform some of these 4A0 duties, only as it pertains to medical equipment. For this reason, it is important that you understand the roles and what is required for you to gain (and keep) privileged access to the network. These roles are in various organization levels as required. DHA has all of the positions at their level, and depending on the dynamics of the organization you will see have some equivalent squadron or group positions. The descriptions remain the same but the scale of duties change as you increase or decrease the organization level.

Authorizing official

The authorizing official (AO) is the official with the authority to assume responsibility for operating a computer system at an acceptable level of risk. The AO renders authorization decisions for DOD systems under their purview in accordance with DODI 8510.01, *Risk Management Framework (RMF) for DOD Information Technology (IT)*.

Security control assessor

The security control assessor (SCA) has the authority to formally evaluate the cybersecurity capabilities and services of a DOD system and issue an authorization recommendation. This recommendation accompanies the RMF security authorization package for review by the AO towards an authorization decision. The SCA continuously assesses and guides the quality and completeness of RMF activities and tasks. Some specific duties include:

- Develop, review, and approve a plan to assess the security controls.
- Assess the security controls in accordance with the assessment procedures defined in the security assessment plan
- Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment
- Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.

- Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.

Information system security manager

The information system security manager (ISSM) is the *primary* cybersecurity technical advisor to the AO. He or she is responsible for ensuring all products, services, and platform information technology has completed the appropriate evaluation and configuration processes prior to incorporation into or connection to a system.

Information system security officer

The information system security officer (ISSO) is responsible for the *technical* implementation of a cybersecurity program. He or she preserves the appropriate operational security posture for an information system or program and maintain approval and inventory documentation for authorized personally owned hardware and software.

Systems administration flight/cybersecurity office

This office manages all of your MTF's COMPUSEC requirements for all assigned units. They must evaluate all modifications, exceptions, and deviations to information systems. They also conduct COMPUSEC assessments and assist with vulnerability management.

The information assurance technical levels

The IA workforce is separated into IA technical (IAT) and IA management (IAM) categories. Any DOD position responsible for any IA tasks must correlate to a category and level; this enables a common framework for identifying position requirements. Due to our function, BMETs will fall into category IAT level 1 or 2. The following table shows the approved baseline certifications for each IAT level. You just need to possess one of the baseline certifications from each level to be eligible.

IAT Level 1	IAT Level 2	IAT Level 3
Computing Technology Industry Association (CompTIA) A+ CompTIA Network+ Systems Certified Practitioner (SSCP)	Global Information Assurance Certification (GIAC) Security Essentials Certification (GSEC) CompTIA Security+ Security Certified Network Professional (SCNP) SSCP	Certified Information Systems Auditor (CISA) GIAC Security Expert (GSE) Security Certified Network Architect (SCNA) Certified Information Systems Security Professional (CISSP) GIAC Certified Incident Handler (GCIH)

Air Force (AF) special experience identifiers (SEI) 260 and 264 correlate to the IAT level 1 and 2 positions, which you must obtain before performing any duties on the DOD network. The SEI 260, IAT level 1, requires assignment to perform IA technical support at the computing environment level (e.g., client support technician); certification as A+, Network+ or SSCP; and unit commander's recommendation. There are *no minimum* grade or skill level requirements to be awarded SEI 260. Figure 1–4 illustrates how the levels ascend.

SEI 264, IAT level 2, requires assignment to perform IA technical support at the network environment level (e.g., infrastructure technician); certification as GSEC, Security +, SCNP, or SSCP; and unit commander's recommendation. There are also *no minimum* grade or skill level requirements for award of SEI 264.

BMETs are able to get CompTIA's A+, Network +, and Security + certifications funded by their unit in accordance with Air Force Instruction (AFI) 41-104, *Professional Board and National Certification Examinations*. These certifications support SEIs 260 and 264. Our career field is in the

process of integrating medical device networking responsibilities to BMETs, so it is highly encouraged for you to pursue these certifications to be eligible to obtain these SEIs.

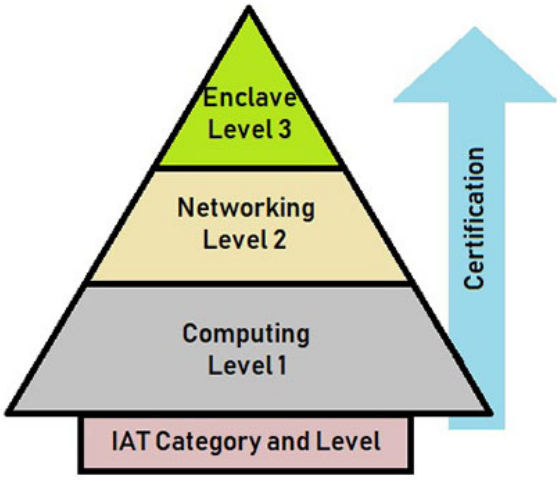


Figure 1–4. IAT levels.

604. Basics of biomedical equipment technician responsibilities in information technology

As BMETs responsibilities to support medical device information systems are increased, two areas you need to be aware of are the certification and accreditation process for devices (gaining authorization to connect equipment) and general preventive maintenance tasks for computer systems.

Medical device certification and accreditation

As stated in the previous lesson, DIACAP was replaced with RMF as the system used to authorize devices to be able to operate and connect to your MTF's network. RMF requirements for approval to connect (ATC) and authorization to operate (ATO) are now included in some contract terms for medical equipment. All the Military Health System (MHS), including the AFMS, follows DHA's process for certification and accreditation of medical device information systems. At the current moment, the role you will most likely play in getting a device certified is initiating and forwarding the paperwork to your systems administration flight or cybersecurity team. However, it is important to be aware of the entire process.

DHA's certification and accreditation process tailor DOD RMF requirements for the MHS environment. The types of decisions on authorizations that can be assigned are shown in the following table:

Type	Description
ATO	An ATO authorization must specify an authorization termination date (ATD), which indicates when the security authorization expires. The ATD must be *within* three years of the authorization date *unless* the system has a continuous monitoring program that is compliant with DOD policy.
ATO with Conditions	This authorization requires permission of the responsible DOD component's chief information officer. An ATO with conditions implies that important vulnerabilities must be addressed within a certain time for a system's authorization to remain valid.
Denial of an Authorization to Operate (DATO)	If the denial occurs after the system is already operational, the operation of the system must stop immediately. Network connections will be terminated immediately for any system issued a DATO.

Type	Description
Interim Authorization to Test (IATT)	IATTs should be granted only when an operational environment or live data is required to complete specific test objectives (e.g., replicating certain operating conditions in the test environment is impractical), and should expire at the completion of testing (normally for a period of less than 90 days). An IATT is generally valid for a number of weeks or months, and if testing is successful, it is followed by a request for a full ATO.

The RMF authorization process consists of six primary stages, each of which has a number of smaller tasks associated with it:

1. Categorize a system's security requirements.
2. Select applicable security controls.
3. Implement security controls.
4. Assess security controls.
5. Authorize a system.
6. Monitor security controls.

The complete workflow a system must go through to receive consideration for an ATO is shown in figure 1–5.

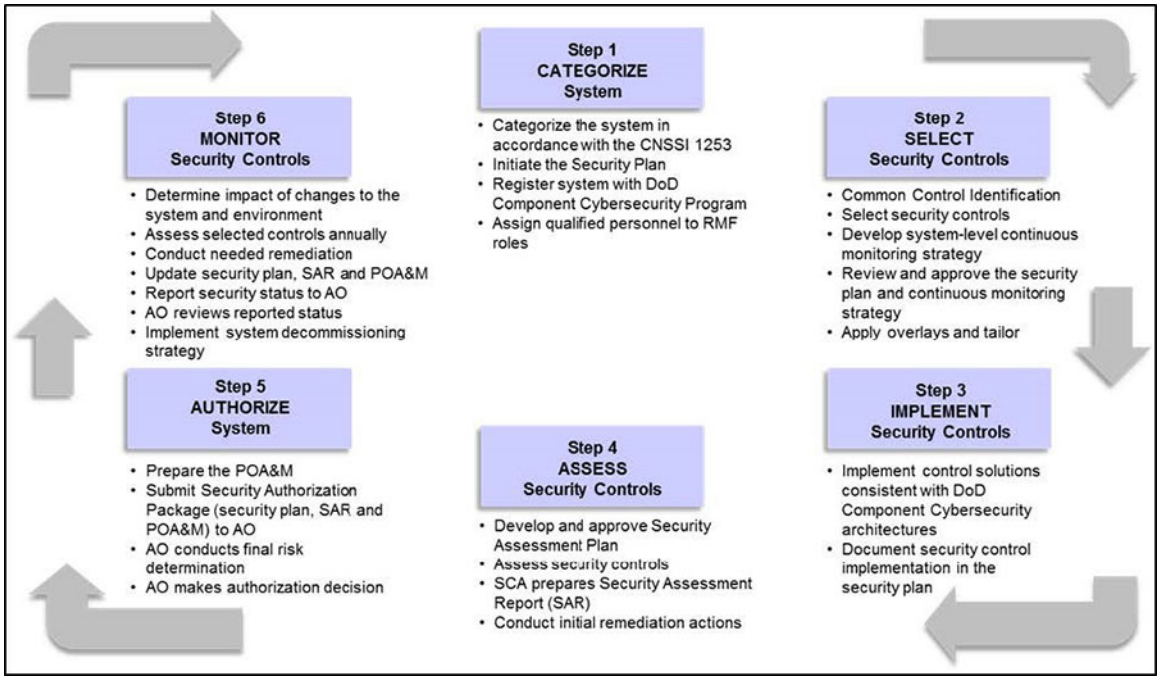


Figure 1–5. Six steps of RMF process.

In step 5, the AO considers the current security state of the system (as reflected by the risk assessment and recommendations provided in the security assessment report), and weighs this against the operational need for the system. The AO then issues an authorization decision document granting or rejecting the authorization requested and describing the level of risk the organization is accepting by permitting the system's operation.

Start a new authorization process prior to the expiration of the existing ATO. During the reauthorization, you need to reassess and reconsider everything because security controls may have changed and new threats may have emerged since the initial authorization.

ATCs are instances of the DOD implementation of reciprocity. For systems not already assessed by the DHA process, the AO allows ISSMs to use software products that are certified by another DOD AO or SCA after a formal evaluation of the risk of connecting systems to the receiving enclave. An enclave is a collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. The ATC expiration date will be no later than the ATD of the ATO.

General preventive maintenance tasks

As you are aware, many processes and procedures in your MTF and organization rely on the functionality of computers. Many factors can cause computers to malfunction. By ensuring the computer is in the correct operating environment and performing proper preventive maintenance, you can maximize the computer uptime and life expectancy. Throughout the volume as needed, we will cover the following tasks in further detail.

1. Ensure that you record all information on the system you are servicing, such as the operating system (OS) type and software versions.
2. Update all pertinent software and applications such as the OS, security programs, plugins, drivers, Java, and Adobe.
3. Scan for viruses and quarantine or destroy any dangerous files or applications found.
4. Run anti-malware in addition to the virus scan to catch other threats such as spyware and adware that the virus scan will fail to identify as dangerous.
5. Perform physical computer maintenance, to include:
    a. Cleaning the keyboard and mouse.
    b. Wiping down monitor. Use screen cleaner or a paper towel moist with water.
    c. Dusting the computer unit. After you ensure the computer has power removed, you can use compressed air to dislodge dust. If the unit is very dusty, you may have to remove the tower access panel and gently vacuum the dust out.
6. Delete temporary and browser files.
7. Uninstall any unused programs. These can bog down your computer’s speed and processing power.
8. Run disk cleanup to remove any cookies or file debris.
9. Check the hard drives for errors and capacity by running check disk utility.
10. Empty the recycle bin.
11. Defragment the hard drive. This is essential to maintaining the system’s performance. Hard drive fragmentation occurs when programs and data are continuously added and deleted. When writing a new program or data to a hard drive, the read/write mechanism seeks out the first empty space and starts the write process. If it encounters other information before it has completed the write process, it will skip over that data and continue to write in the next available space, which causes fragmenting. This slows the data access rate and impedes the computer system’s performance. Defragmenting realigns the separated files and moves them into a more defined structure increasing the data access rate and system performance.
12. Perform a system backup. This can save countless hours that would otherwise be spent rebuilding files if something should happen to the system. The most common files requiring backup are documents (e.g., Word, Excel, PowerPoint, government forms, etc.), e-mail outlook personal storage table (.pst) and Internet favorites. Choose files whose loss could be detrimental to operations. You do *not* need to back up actual programs (e.g., Outlook, Acrobat Reader, etc.), since they can be reloaded from existing sources.

Self-Test Questions

After you complete these questions, you may check your answers at the end of the unit.

603. The information technology roles and relationships in the military treatment facility

1. What guidance addresses training and certification of personnel conducting IA functions for DOD?

2. How does the structure of AFMS units differ from other base organizations?

3. What is the role of the AO?

4. What are the responsibilities of the ISSM?

5. What must BMETs obtain before performing any duties on the DOD network?

604. Basics of biomedical equipment technician responsibilities in information technology

1. What role do BMETs play in getting devices certified?

2. List the four types of authorization decisions.

3. What authorization process certifies medical devices? List the six steps.

4. Explain the AO’s role in step 5 of the certifying process.

5. Why is it necessary to reauthorize systems?

6. Why is it important to run anti-malware in addition to virus scans?

7. Explain how hard drives become fragmented.

8. Why do you *not* need to back up programs when performing a system backup?

Answers to Self-Test Questions

601

1. Increase in number of network-enabled devices; access to healthcare through mobile devices, patient portals, and cloud services; cybersecurity threats; integration of healthcare networks; volume of patient data; and the need to analyze big data.
2. Protection and privacy of individually identifiable health information. It is found in Title 45 CFR Parts 160 and 164.
3. Your local MTF HIPAA HPO and HIPAA HSO.
4. Select the Contains Patient Data in the DMLSS Equipment Detail tab for the ECN.
5. A business associate agreement is a legal agreement between a covered entity (your MTF) and a business associate (service provider) that the business associate will appropriately safeguard any PHI it receives from the entity. It is used whenever you are turning over a medical device that contains PHI to a service provider or agency outside of your MTF.
6. Attach a DD Form 1577-2, Unserviceable (Reparable) Tag - Materiel (referred to as a "green" tag), annotating that application software will need to be reinstalled and the unit fully tested before further operation.
7. Clearing uses techniques that protects against simple non-invasive data recovery techniques; purging uses techniques that render data recovery infeasible; and destroying uses techniques that render media completely unusable as originally intended.
8. Conducted emission is electromagnetic energy emanating from equipment through a conductor by means of resistance, inductance, or capacitance. Radiated emission is electromagnetic energy emanating from a device and propagating through space or a medium.
9. The selection of wireless technology, security, and EMC with other devices.

602

1. Ensuring that equipment can connect and communicate with your MTF's EHR system.
2. Medical devices are not manufactured to seamlessly work with a particular EHR system so middleware is used to integrate medical devices and EHR. Middleware provides services to software applications beyond those available from the operating system.
3. Electronically control and track medication distribution; automatically count pills or capsules as it is being filled; assist technician with filling prescriptions; and generate refill requests when supplies fall below preset levels.
4. Decentralized medication management systems.

603

1. DOD 8570.01-M, *Information Assurance Workforce Improvement Program.*
2. Instead of them reporting directly to the base communication squadron, MTFs have a system administration flight that is directly responsible for the network, and associated hardware and software
3. The AO renders authorization decisions for DOD systems under their purview.
4. Ensuring all products, services, and platform information technology have completed appropriate evaluation and configuration processes prior to incorporation into or connection to a system.
5. Air Force SEIs 260 and 264, which correlate to IAT level 1 and 2 positions.

604

1. Initiating and forwarding the paperwork to your systems administration flight or cybersecurity team.
2. ATO, ATO with Conditions, DATO, and IATT.
3. RMF. (1) Categorize a system's security requirements, (2) Select applicable security controls, (3) Implement security controls, (4) Assess security controls, (5) Authorize a system, and (6) Monitor security controls.
4. The AO considers the current security state of the system, and weighs that against the operational need for the system. The AO then issues an authorization decision document granting or rejecting the authorization requested.
5. Security controls may have changed and new threats may have emerged since the initial authorization.
6. To catch other threats such as spyware and adware that the virus scan will fail to identify as dangerous.
7. Hard drive fragmentation occurs when programs and data are continuously added and deleted. When writing a new program or data to a hard drive, the read/write mechanism seeks out the first empty space and starts the write process. If it encounters other information before it has completed the write process, it will skip over that data and continue to write in the next available space.
8. Because they can be reloaded from existing sources.

Complete the unit review exercises before going to the next unit.

Unit Review Exercises

Note to Student: Consider all choices carefully, select the *best* answer to each question, and *circle* the corresponding letter. When you have completed all unit review exercises, transfer your answers to the Field Scoring Answer Sheet.

Do not return your answer sheet to Air Force Career Development Academy (AFCDA).

1. (601) What must you do if you send a medical device to a service provider that contains protected health information (PHI) that you *cannot r*emove?
   a. Establish a service agreement.
   b. Establish a business associate agreement.
   c. Ship device with a Privacy Act cover sheet.
   d. You cannot ship equipment with PHI on it.

2. (601) What must you do *prior* to turning any medical device into Defense Logistics Agency Disposition Services (DLA-DS)?
   a. Remove all protected health information (PHI).
   b. Establish a service agreement.
   c. Establish a business associate agreement.
   d. Attach a Privacy Act cover sheet to device.

3. (602) Which type of software integrates medical devices and electronic health records?
   a. Application software.
   b. System software.
   c. Utility software.
   d. Middleware.

4. (603) Who has the authority to assume responsibility of operating a Department of Defense computer system at an acceptable level of risk?
   a. Authorizing official (AO).
   b. Security control assessor (SCA).
   c. Information system security officer (ISSO).
   d. Information system security manager (ISSM).

5. (603) Which of the following is *not* a requirement to obtain Air Force special experience identifier (SEI) 264?
   a. Work assignment to perform information assurance technical support.
   b. Unit commander’s recommendation.
   c. Appropriate certification.
   d. Minimum five-skill level.

6. (604) Which type of file or program do you *not* need to back up during the system backup process?
   a. Microsoft Word documents.
   b. Government forms or files.
   c. Internet favorites.
   d. Acrobat Reader.

Please read the unit menu for unit 2 and continue ➔

Student Notes

Unit 2. Computer and Operating Systems

WE ARE SURROUNDED with automation and connectivity in regards to modern medical devices. The next step in beginning to gain knowledge of maintaining or supporting networked systems is to learn about the typical architecture of an individual computer system. This baseline will help your understanding of later lessons about how these systems are networked and secured. This unit will cover basic computer components and operating system information.

2–1. Computer Systems

Computers are made of components categorized as hardware or software. They perform mathematical operations and logical comparisons during processing of data. It is important to understand that there are numerous devices considered computers, including smartphones, tablets, and netbooks. In this section, you will learn about common computer hardware.

605. Computer core hardware principles

Computer function consists of four stages: input, process, output, and storage. Computers are electronic devices that operate under the control of instructions stored within its own memory that can accept data (input), manipulate the data according to specified rules (process), produce results (output), and store results for future recall (storage). Computer hardware implies permanence and invariability. It is the physical electronic and mechanical equipment of the computer. This lesson will cover the following main hardware components: power supply, motherboard, and memory.

Power supply

The personal computer (PC) operates on direct current (DC) voltage, so conversion of the supplied alternating current (AC) must occur prior to operation. The power supply (fig. 2–1) converts 120 volts alternating current (VAC) commercial power down to low voltage DC (VDC) power for PC use.

Figure 2–1. PC power supply.

It is important to note that there is a 115/230 VAC voltage switch that must be properly set to avoid damage to the computer hardware. If you select 230 VAC and plug the PC into 120 VAC, it will most likely will not be able to boot up properly. However, if you select 115 VAC and plug the PC into 230 VAC it will destroy the power supply, and possibly the motherboard and other components.

There are numerous standards, but the advanced technology eXtended (ATX) is currently the most common power supply and motherboard standard. It provides five DC voltage levels: +3.3, +5, –5, +12, and –12. The microprocessor and memory use the +3.3 VDC, the motherboard uses the +5 VDC and –5 VDC, while the motors, cooling fans and storage drives use the +12 VDC and –12 VDC. The ATX continuously supplies power to the motherboard as long as it is plugged in, even when the PC is powered down.

The ATX power supply features “soft power” to turn the computer ON or OFF. This means the power button on the front of the PC is not a direct switch to the power supply and only sends the signal to the basic input output system (BIOS) or OS that the button was pressed. The BIOS or OS then takes the necessary steps to shut the system down. The benefits of soft power are that it ensures the OS is ready to be shut down prior to the system shutting down and allows your PC to use power-saving modes such as sleep mode, which saves power without completely turning it off.

Motherboard

The motherboard (fig. 2–2) is the main circuit board of the PC, and all other hardware components directly or indirectly connect to it. It consists of copper traces that serve as communication buses, central processing unit (CPU) socket, system clock, memory banks, peripheral ports, and expansion slots, which you can use to add additional adapter cards.

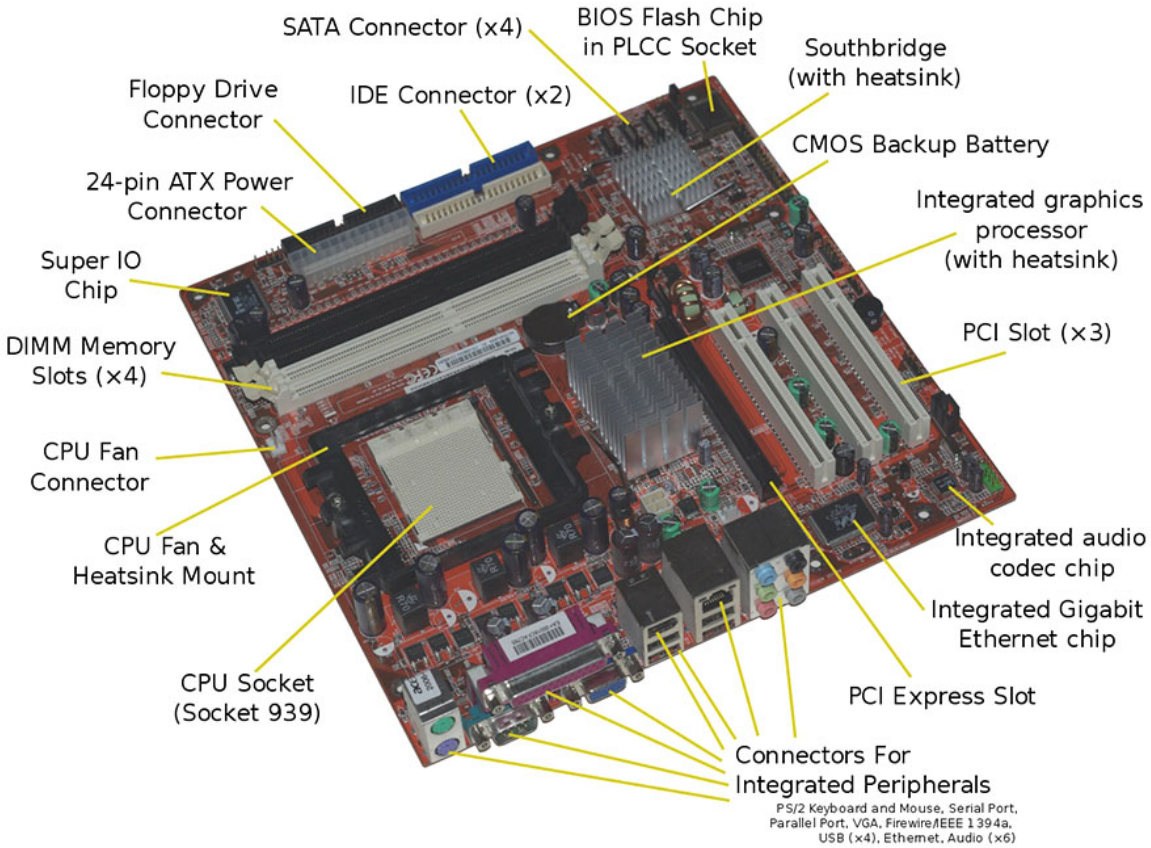


Figure 2–2. Motherboard.
(Graphic by Moxfyre at English Wikipedia, Licensed by CC BY SA 3.0.)

Hardware may be directly on the motherboard or connected to it through a secondary connection. For example, a sound card can be on the motherboard or through a connection with a peripheral component interconnect (PCI). The motherboard also distributes power from the power supply to all the other components. It is important to ensure that the components are compatible with the motherboard. The form factor and chipset identify the motherboard characteristics.

Form factor

Motherboards vary in sizes and have different connector layouts, which is categorized as the form factor. The PC case, power supply, and motherboard must have matching form factors. This ensures the correct power is applied to the board, the board fits inside the case with proper mounts, and the ports align with the openings. As stated in the power supply section, ATX is the most popular form factor standard, which includes the variations micro ATX and extended ATX. You must also consider the brand in addition to the form factor. The two most popular producers of motherboards are Intel and Advanced Micro Devices (AMD). It is important to note that the CPU chips are not interchangeable, so an Intel motherboard will only work with an Intel CPU and vice versa. Other companies that produce motherboards design them to fit AMD or Intel processors. Some other companies such as Sony, Samsung, and Dell make proprietary form factors to fit unique products or applications.

Chipset

A chipset is one or more integrated circuits that support and manage the interface of devices connected to the motherboard. It controls the flow of bits that travel between the CPU (also known as microprocessor), random access memory (RAM), and peripherals. Efficient data transfers, fast expansion bus support, and advanced power management features are just a few of the things for which the chipset is responsible. Chipsets typically only work with specific processors and they contribute to the overall performance of a PC.

Traditionally, the chipset was split into two sections—the Northbridge and Southbridge. Newer designs of motherboards and processors integrate the traditional functions of the Northbridge and Southbridge chips into the processors. Therefore, some newer chipsets do not even have a Northbridge or reduce it to simply facilitating video card communication. Figure 2–3 shows a typical classic chipset layout. As they continue to integrate the functions, however, the CPU performs more of the duties that traditionally were carried out by the chipset. It is also important to note that new technologies are being developed constantly that change the topology of the CPU and bus connections, so this is not the only layout currently used. (**NOTE:** Intel commonly refers to the Northbridge as the memory controller hub and the Southbridge as the input output (I/O) controller hub.) The Northbridge has a direct connection to the processor, known as the front side bus, and connects to high speed components such as RAM and graphics controllers. The Southbridge does not directly connect to the processor; instead, it connects to low speed peripherals, storage devices, and expansion devices. Chipsets typically perform one or more of three functions plus older technologies support (if not already integrated into the CPU) shown in the following table:

Function	Description
System controller	Brings the functions of the entire PC together, giving all the support the microprocessor needs to function.
Peripheral controller	Enables the microprocessor to operate I/O ports, expansion buses, and disk interfaces.
Memory controller	Links the microprocessor to the memory system and establishes the main memory and cache architectures, thus assuring the reliability of the data stored away in RAM.
Older technologies support	Sometimes another chip, known as the super I/O chip (fig. 2–3) handles some older technologies that still require support.

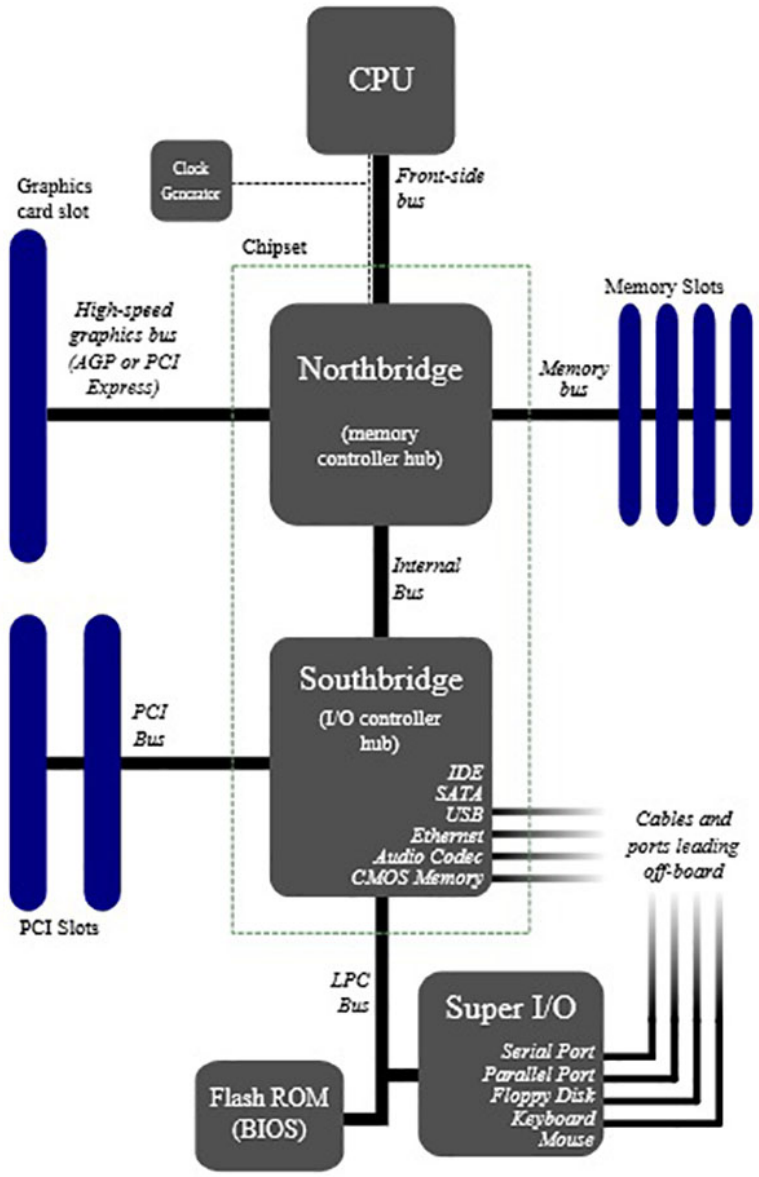


Figure 2–3. Motherboard chipsets.
(Graphic by Moxfyre at English Wikipedia, Licensed by CC BY SA 3.0.)

Super I/O chip

The super I/O chip integrates several devices formerly found on separate expansion cards into a single chip. At a minimum, super I/O chips typically contain components and functions describe in the following table:

Component	Function
Floppy drive controller	Acts as an interface between the system board and the diskette drives. Its primary function is to convert signals from the CPU into commands the mechanical parts of the disk drive will understand.
Hard drive controller	All the circuitry needed to connect a hard disk to a PC is contained here. Typically provided is an advanced hard drive interface such as the enhanced integrated drive electronics (EIDE) or small computer system interface (SCSI).

Component	Function
Dual serial port controller	Manages the system's interfaces (COM1, COM2 etc.). In most modern designs, the serial controller is made from two universal asynchronous receiver-transmitters (UART). A UART is essentially a serial-to-parallel and parallel-to-serial converter. Since most systems have two serial ports, one is required for each port.
Parallel port controller	Simply oversees the operation of the system's parallel interface.
Keyboard controller	Links the keyboard to the system board. The primary function of the keyboard controller is to translate the serial data that the keyboard sends out into the parallel form that can be used by the PC.
PS/2 mouse controller	Links the mouse or other pointing devices to the system board.

Expansion slots

An expansion slot is an opening or socket on the motherboard that allows you to insert an expansion card (fig. 2–4), which is a printed circuit board, for the purpose of adding new functions or upgrading existing capabilities *without* having to replace the entire motherboard.

Figure 2–4. Expansion cards. AGP video card (left) and PCIe Universal Serial Bus (USB) card (right).

The wires and support chips associated with the expansion slots are known as the expansion bus. The expansion bus connects to the rest of the system through the chipset. Some common expansion cards found in most of today's computers are the graphic card, sound card, and NIC. Graphics cards convert computer output to a video signal that is sent to the display monitor, sound cards enhances a PC's sound-generating capabilities, and network interface cards (also known as network interface controllers) are devices that allow the computer to communicate on a network. If you refer back to figure 2–3, you can see the typical layout or PCI, PCI Express (PCIe), accelerated graphics port (AGP), and memory slots. AGP has practically been phased out in favor of PCIe. Most modern motherboards will consists mostly of PCIe slots with a couple of legacy PCI slots. PCIe, introduced in 2004, is currently the most popular expansion bus used. Its software is compatible with the pre-existing PCI standards, making the conversion of PCI cards and systems to PCIe as simple as replacing the Physical layer (motherboard) without requiring a change to the supporting software. The increased bandwidth on PCIe has led to standardization, since it is fast enough to replace the majority of existing internal buses, including AGP and PCI.

PCIe slots come in a variety of physically different sizes depending on the maximum lane count they support, i.e. x1, x2, x4, x8, x16, and x32. A PCIe card will fit into a slot of its size or bigger, but *not* into a smaller slot. The number of lanes actually connected to a slot may also be less than the number supported by the physical slot size. An example is a x8 slot that actually only runs at x1; these slots will allow any x1, x2, x4 or x8 card to be used, though only running at the x1 speed. The advantage gained is that a larger range of PCIe cards can still be used without requiring the motherboard

hardware to support the full transfer rate, therefore keeping design and implementation costs down. The number of lanes is "negotiated" during power-up or operation; by making the lane count flexible a single standard can provide for the needs of high-bandwidth cards (e.g., graphics cards) while also being economical for less demanding cards.

Computer memory

The manner in which memory is organized and used in a computer determines it operation speed and efficiency. Memory comes is a form of electronic storage space located inside or outside of the computer where the computer can read or write data. Memory stores instructions for the OS, application programs, and data being processed by application programs. Once the data is in memory, the computer can process instructions as needed. Memory can be categorized as volatile and nonvolatile.

With volatile memory, the data contents are lost when power is removed. As a result, software programs use volatile memory for temporary storage of data. With nonvolatile memory, the data are retained after power is removed. System programs for computer start-up are stored in nonvolatile memory. Nonvolatile memory can be further categorized as erasable or non-erasable. Erasable nonvolatile memory can be reprogrammed and non-erasable nonvolatile memory once programmed cannot be changed.

Computers remember single pieces of information as one of two states: 1/0, high/low, yes/no, on/off. This small piece of information is a bit, which is short for binary digit. However, when combined with other bits, it can add up to substantial amounts of information. Now you might be thinking, "How can a group of binary bits have meaning significant enough to create the marvels we see the modern PC create?" This happens by making a specific group of binary digits represent something in terms that humans can relate. The terms used to describe quantities of bits are as follow:

- Individual "1"or "0" = a bit
- 4 bits = nibble.
- 8 bits = byte.
- 16 bits = word.
- 32 bits = double word.
- 64 bits = paragraph or quad word.

The byte is the basic storage unit memory commonly uses. When application program instructions and data transfers into memory from storage devices, they are stored as bytes, each in a precise location in memory, called an address. This address is simply a unique number identifying the location of the byte in memory. To access data or instructions in memory, the computer references the addresses that contain these bytes of data.

Manufacturers state memory and storage sizes in terms of the number of bytes the device has available for storage. A kilobyte (KB) of memory is equal to exactly 1,024 bytes. To make memory and storage definitions easier to identify, computer users often round a kilobyte down to 1,000 bytes. For example, if a memory chip can store 100 KB, it can hold approximately 100,000 bytes. The following terms are associated with memory size:

- Kilobyte = 1,000 (one thousand) bytes.
- Megabyte = 1,000,000 (one million) bytes.
- Gigabyte = 1,000,000,000 (one billion) bytes.
- Terabyte = 1,000,000,000,000 (one trillion) bytes.
- Petabyte = 1,000,000,000,000,000 (one quadrillion) bytes.

There are many different types of memory used in a computer. When troubleshooting, it is good to know which memory effects which processes. Without this knowledge, you may waste a great

amount of time and effort. Another thing to keep in mind is that computers have limitations with memory, so be aware of your PCs limitations before trying to upgrade it with additional memory or replacing pre-existing memory with the latest and greatest. Your plans to improve the computer may just slow the computer down or completely stop it from working.

Read-only memory

Read-only memory (ROM) can be read, but not changed, by the microprocessor, so it is considered permanent memory. ROM is nonvolatile; its contents are not lost when power is removed from the computer. ROM contains the computer's BIOS programming. The BIOS (discussed in detail later) enables the computer to communicate with various devices and provides instructions the computer needs to correctly start. These instructions are burned into the ROM chip, making it virtually impossible for the user or computer to erase. Manufacturers of ROM chips often record the data, instructions, or information on the chips as they are manufactured. The term firmware refers to any data or instructions stored on a ROM chip.

ROM variations

One variation of the ROM chip, called a programmable ROM (PROM), is a blank ROM chip on which you can permanently place items. Programmers use micro code instructions to program a PROM chip. Once a programmer writes the microcode onto the PROM chip, it functions like a regular ROM chip and cannot be erased or changed. A programmer can erase microcode on a type of PROM chip called an electrically erasable PROM (EEPROM). However, most modern computers use flash ROM. Flash ROM is a nonvolatile memory that you can electronically erase and re-program. This allows the user to update, or *flash*, the contents of the BIOS if necessary.

RAM

RAM is the *temporary* electrical storage space that holds program instructions and program data. All programs need to be loaded into RAM in order to run. Generally speaking, the more RAM you have, the larger the program you can operate and the faster it is likely to run. Therefore, the computer's purpose will determine the amount of RAM required.

RAM is volatile, which means that its contents are *lost permanently* when power is removed from the computer. This is why it is important to save documents to the hard drive or removable media before turning off the computer and frequently while in the middle of big tasks. It would be extremely frustrating to lose a day's work because you did not save your work and power to the computer was lost.

When users discuss memory in a computer, they typically are referring to RAM. RAM consists of memory chips where the processor and other devices can read from and write to. When the computer is powered on, certain OS files load from a storage device such as a hard drive into RAM. These files stay in RAM as long as the computer is running. As the user requests more programs and data, they also load from storage into RAM. The processor interprets the data while it is in RAM. The contents of RAM may change during this time. RAM can hold multiple programs simultaneously provided there is enough RAM to accommodate all of the programs. The amount of RAM a computer requires often depends on the types of applications the computer uses. RAM is similar to the workspace you have on the top of your workbench. Just as a workbench needs a certain amount of space to hold tools, equipment, and supplies, a computer needs a certain amount of memory to be able to store an application program and files. A software package usually indicates the minimum amount of RAM it requires to run. If you want the application to perform optimally, you need more than the software minimum specifications. The two basic types of RAM chips are static and dynamic.

Static RAM

Static RAM (SRAM) chips are faster and more reliable than any variation of dynamic RAM (DRAM) chips. Unlike DRAM, SRAM chips do not have to be refreshed. SRAM chips, however, are much more expensive than DRAM chips. They are used for cache memory typically.

DRAM

DRAM chips are the standard type of RAM used for PCs. If DRAM is not refreshed constantly, it loses its contents. Many variations of DRAM chips exist that are faster than the basic DRAM. Synchronous DRAM (SDRAM) chips are much faster than DRAM chips because they are synchronized to the system clock, which eliminates wasted time associated with wait states since the CPU and RAM are working off same frequency. Double data rate (DDR) SDRAM chips are faster than standard SDRAM chips because they transfer data twice for each clock cycle, instead of just once. Most computers today use some form of DDR SDRAM chips.

RAM chips often are smaller than processor chips and usually reside on a small circuit board, called a memory module. DDR SDRAM connects to the motherboard via sockets called dual inline memory module slots.

The standard DDR SDRAM, also called DDR1, has been superseded by DDR2, DDR3, and recently DDR4 (fig. 2–5). The table shows the different speeds by mega transfers per second each.

DDR Standard	Bus Clock (megahertz)	Transfer Rate (mega transfer per second)
DDR1	100 – 200	200 – 400
DDR2	200 – 533.33	400 – 1066.67
DDR3	400 – 1066.67	800 – 2133.33
DDR4	1066.67 – 2133.33	2133.33 – 4266.67

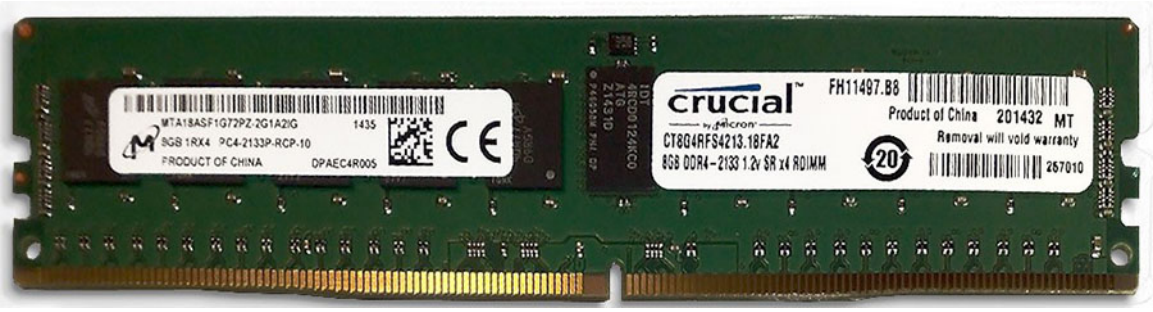


Figure 2–5. DDR4 RAM.
(Graphic by Kjerish at Wikimedia Commons, Licensed by CC BY SA 4.0.)

Parity

Parity was the first attempt at detecting errors in RAM. Parity RAM stored an extra bit of data that the Memory chip controller (MCC) used to verify the rest of the data. Parity worked by having the memory controller count the number of 1s in a piece of data about to be written and then stored either a 1 or a 0 in the parity bit depending on if there was an odd or even number of 1s. Then upon retrieval, the memory controller compared the number of ones (1) retrieved with the number stored in the parity bit.

If the numbers differ then it causes a parity error. A parity error can be the first signal of a host of problems, ranging from a one-time anomaly to faulty memory. Faulty memory can be the cause of repeated memory parity errors. Parity RAM did not always work due to the fundamental nature of its design, and when it did work it was unable to do more than simply detect an error. It has no mechanism to do anything to correct or identify the exact location of the error. Modern PCs that require RAM error monitoring typically use error correction code (ECC) RAM.

Error correction code

Unlike the parity method, ECC is a data integrity method that can both detect and correct errors. ECC can detect up to 4-bit memory errors; however, it can correct *only* 1-bit memory errors. However, since 1-bit errors are more common and 4-bit errors are very rare, this has not caused much of a concern. Like the parity method does with all errors, when ECC discovers a multiple bit error it simply reports it as a parity error. It may appear that ECC would be a good idea to have in any PC, but ECC RAM is expensive and can be supported only by certain motherboards. For this reason, ECC is used primarily in high-end PCs and servers.

Cache memory

As previously mentioned, cache memory is a type of SRAM that stores frequently accessed data to increase PC processing speeds. It may be integrated into the CPU or it may be a separate chip or area of memory. SRAM retains information written to it without having it refreshed; access is much faster than DRAM. DRAM's constant refreshing of its data is what results in DRAM being much slower than SRAM. SRAM is generally more expensive than DRAM. Most modern computers have two or three types of cache: level 1 (L1), level 2 (L2), and level 3 (L3). Most modern PCs split L1 cache into L1d (data) and L1i (instructions), which are integrated into the CPU. Usually, L1 cache has a very small capacity in comparison to L2 and L3.

L2 cache is slightly slower than L1 cache, but has more capacity. A large number of modern processors also have the L2 cache integrated in the processor. Some PCs include L3 cache, which is separate from the processor on the motherboard and slower than L1 and L2 cache, but L3 has more capacity than the other levels.

Cache speeds up processing time by storing frequently used instructions and data. When the processor needs an instruction or data, it searches memory in this order: L1 cache, then L2 cache, then L3 cache, and then RAM—with a greater delay in processing for each level of memory it must search. If the instruction or data is not found in memory, then it searches a slower speed storage device such as a hard drive.

Complementary metal oxide semiconductor memory

Another type of memory chip is the complementary metal-oxide semiconductor (CMOS) memory chip. The CMOS used to be an independent chip, but in most modern PCs it is integrated into the Southbridge chipset. CMOS memory stores device parameters, which the BIOS uses each time the system starts.

It also functions as a clock to keep the current date and time. The setup program is called CMOS setup program or system setup utility. CMOS stores information such as the total amount of memory available to the CPU and the type and number of hard drives, keyboard, and monitor. The CPU uses CMOS settings to communicate with each device in the computer system. CMOS settings must be available to the CPU each time the PC is turned on for it to work properly. CMOS chips retain information even when power to the computer is off via a lithium battery. This is what enables it to keep the calendar, date, and time current even when the computer powered down. The lithium battery must be replaced periodically to ensure CMOS settings are available. The battery can last up to ten years.

Unlike ROM, information stored in CMOS memory can be changed; it is important you keep the information updated. If you change any hardware, you must update the CMOS to reflect the change accurately. Failure to do so will prevent the PC from being able to use the device. Each BIOS is different, but to access the CMOS settings you will have to press a designated button (e.g., DELETE, ESCAPE, or F10) during boot up of the system to enter the menu. Ensure you read about your particular BIOS to know which button to press. There may be a very fast message on the screen showing which button to press for access during boot up.

The CPU accesses and relies on all of the components discussed in this lesson to carry out processes and control the PC.

606. Central processing unit operation principles and characteristics

This lesson covers the CPU. Due to the complexity of the CPU, we cannot cover it all, but the following information will give you a basic understanding of its operation. In regards to modern PCs, there is no real difference in the terms CPU, processor, or microprocessor, so you may hear it referred to as any of those terms. The CPU is considered the brain of a computer system (fig. 2–6). It performs the computer program's calculations, moves data, and executes the instructions provided by firmware and software. The CPU also manages interactions between itself and other computer components.

Figure 2–6. Top and bottom view of a CPU.
(Graphic by Eric Gama at Wikimedia Commons, Licensed by CC BY SA 3.0.)

We often determine the performance of a CPU by how fast it processes data. The CPU's clock speed is one of the major factors that influence the rate it processes data. The faster the clock speed, the more instructions the CPU can execute per second. The CPU clock speed is the *maximum* speed it can run, not the speed it must run. The CPU can run at any speed up to its maximum. In modern computers, the system clock synchronizes the timing of the CPU and all other components; it does not establish their operational speed though. The system clock operates as a metronome that constantly ticks in the form of signals. The heart of the system clock is the quartz crystal oscillator. It is contained in what resembles a small silver can mounted on the motherboard. The oscillator produces the frequency stability at which the computer operates. The crystal controls the oscillator's pulsing so that it is highly accurate and continually emits pulses at the same rate.

The CPU runs at a higher speed than the system clock by utilizing clock multipliers. It runs at a higher ratio than the system clock and usually is based on the frequency of the front side bus. Common speeds of modern CPUs range from 1 to 5 gigahertz. For example, if the system clock speed is 133 megahertz and the installed CPU has a clock multiplier of 10, the CPU clock speed would be 1.33 gigahertz (133,000,000 x 10 = 1,330,000,000). Recall that a hertz is one cycle per second and that giga- is the prefix that stands for billion. Thus, 1 gigahertz equates to one billion system clock cycles. Be sure not to confuse the system clock with the real-time clock the CMOS maintains.

The three main components that make up the CPU are the control unit, the arithmetic logic unit (ALU) also called combinational logic, and the registers. As you read about each component, you can refer to the diagram in figure 2–7, which illustrates how the control unit, ALU, and registers work together. In figure 2–7, the black lines represent data flow and the red lines represent control flow.

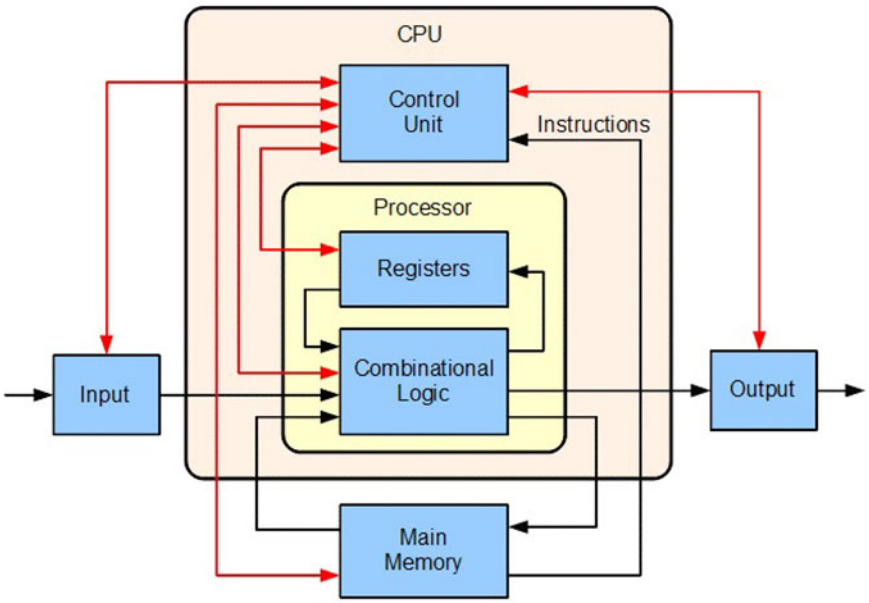


Figure 2–7. Diagram of CPU control unit, ALU, and registers.
(Graphic by Lambtron at Wikimedia Commons, Licensed by CC BY SA 4.0.)

Control unit

The control unit plays an important role in synchronizing the operations of the CPU as well as controlling the flow of instructions and data in and out of the ALU. The control unit directs and coordinates most of the operations in the computer. It has a role much like a traffic cop. It interprets each instruction issued by a program and then initiates the appropriate action to carry out the instruction. For every instruction, the control unit repeats a set of four basic operations:

1. *Fetch*—the process of getting a program instruction or data item from memory.
2. *Decode*—the process of translating the instruction into commands the computer can execute.
3. *Execute*—the process of carrying out the commands.
4. *Store*—the process of writing the result to memory if necessary.

Together, these four operations comprise the machine or instruction cycle. Instruction time is the time it takes the control unit to fetch and decode. Execution time is the time it takes the control unit to execute and store. You can compute the total time required for a machine cycle by adding together instruction and execution time.

Arithmetic logic unit

In essence, the ALU does all of the computing in the CPU. The ALU performs arithmetic, comparison, and logical operations. Arithmetic operations include addition, subtraction, multiplication, and division. Comparison operations involve comparing one data item to another to determine if the first item is greater than, equal to, or less than the other item. Depending on the result of the comparison, different actions may occur. Logical operations work with conditions and logical operators such as AND, OR and NOT.

Registers

Registers are high-speed storage locations the CPU uses to hold data and instructions temporarily. CPUs have many types of registers, each with a specific function. These functions include storing the location from where an instruction was fetched, storing an instruction while the control unit decodes it, storing data while the ALU processes it, and storing the results of a calculation. With larger and more advanced CPU registers the CPU can run larger and more complicated programs and it can accomplish all assigned tasks quicker.

Multithreading and multicore

Manufacturers continue to experiment with different CPU operating topologies to enhance CPU performance. Two common architecture technologies you should be familiar with are multithreading and multicore. A thread is the smallest sequence of instructions a CPU performs. *Multithreading* enables the CPU to run more than one thread at a time. For multithreading to properly function, the OS and the CPU must be designed for it. In multithreading, the OS perceives one CPU as two or more separate CPUs. A downside to multithreading is that the multiple threads still share resources, such as memory. This could cause delays in some processing.

A multicore CPU has two or more independent processors, called cores, embedded into a single chip. Each core generally functions as a separate CPU. A multicore CPU is capable of concurrently reading and executing multiple instructions on separate cores, which significantly increases processing speeds. Multicore CPUs' architecture are different depending on the manufacturer and model. Most modern CPUs contain both multithreading and multicore technologies.

The faster the CPU runs the more power it consumes, which generates more heat. Since not all tasks require the CPU to run at maximum speed, many modern CPUs have the ability to throttle down when the demand is low. When demand is high, clock boost (a boosting capability that is essentially system-controlled over clocking) enables it to perform temporarily at its maximum rated speed. It will only engage this boosting capability if the temperature is within allowable limits. Overheating of the CPU can cause abrupt system shutdowns, program freezing, and the dreadful blue screen crash. CPUs will generally have a heat sink attached to dissipate the heat, and a fan to move heat away from the CPU and heatsink. This is why it is important that computer vents are free of debris, fans properly function, and dust is removed and not allowed to accumulate. Figure 2–8 shows a heat sink with dust buildup that rendered the computer unserviceable due to overheating. Some higher-end systems may utilize a liquid-cooled system to remove the heat.

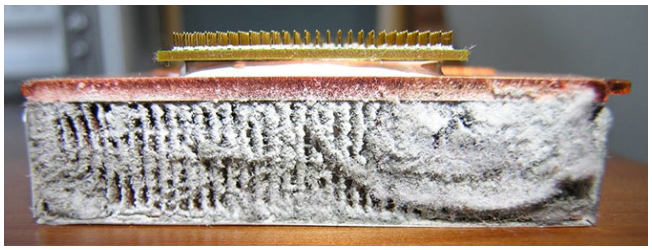


Figure 2–8. Clogged CPU heatsink.
(Graphic by Audrius Meskauskas at Wikimedia Commons, Licensed by CC BY SA 3.0.)

The CPU communicates with all components through connections known as buses. The purpose of a bus is to allow the connection of multiple items for a common purpose. Modern computer architecture has many different bus configurations, but we will focus on traditional computer architecture to grasp an understanding of how it works. The buses traditionally included are the address bus, data bus, and control bus. Figure 2–9 shows a diagram of a traditional bus system.

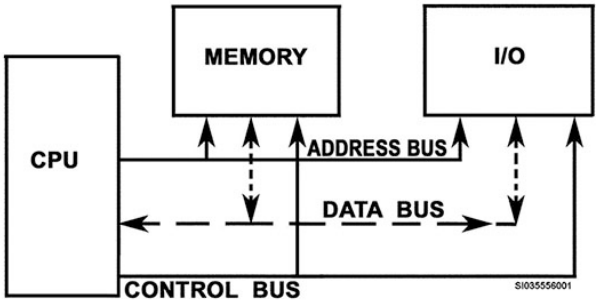


Figure 2–9. Three-bus system.

Address bus

The CPU is constantly communicating with different components of the system and must have a means of identifying which component it is talking to each time; this is the job of the address bus. Every device has its own address; system memory is divided into memory locations, each with its own address. When the CPU needs data from a specific memory location, the address for that memory location is sent from the CPU on the address bus, which connects to every device and memory location in the system and is unidirectional (one way only). The location addressed will recognize the address code as its own and respond to the CPU. Therefore, the address bus selects or enables the proper destination and return for communications.

Data bus

The data bus enables the CPU to send and receive data from various areas of the system. Data transfers on the data bus after the address bus selects the path. As with the address bus, the data bus connects the CPU to all system components and memory storage locations. The data bus is bi-directional, which means the data can travel in both directions from the CPU to components or from components to the CPU.

Control bus

You know that the address bus selects the path for communication and the data bus transfers the data to or from the microprocessor. The control bus has two purposes:

1. To signal the start and stop of communications.
2. To define the type of communication.

The control bus is unidirectional. Signals from the microprocessor are sent over the control bus to all locations in the system. The width of the control bus is based on the number of different functions the microprocessor can perform. Each line of the control bus has its own purpose. The following is a list of some examples used in microprocessors today:

- Memory read.
- Memory write.
- Input read.
- Output write.
- Interrupt.
- DMA.

For example, let’s say the CPU wants information from memory, then follow these steps:

1. The address bus outputs the memory location (address) that contains the needed information.
2. The “memory read” control bus line activates to signal the start of the action and the type of action needed.
3. The memory location recognizes the address as its own and responds to the control bus command by placing the stored information on the data bus. Now, the microprocessor uses the information on the data bus (fig. 2–9)

607. Principles of computer peripheral technologies

Devices typically not housed within the PC case are known as peripheral devices and are classified as input, output, or I/O devices. There are a large number of different computer peripheral devices. Input devices send information to the CPU for processing, output devices reproduce or display the result of that processing, and the I/O devices do *both*. Input devices include those used to input information into the system, such as a keyboard, mouse, or scanner. Output devices allow the computer to organize the information into a tangible form that we can understand. Some examples of output devices are monitors and printers. I/O devices perform both, such as a touchscreen monitor. It displays output information, but also allows you to send inputs by applying pressure on the screen. As

stated earlier, the CMOS retains the information of each hardware item, but the BIOS is what initializes the hardware and peripheral devices during boot up.

BIOS

The BIOS is a set of programs that contain instructions for the CPU to communicate with devices and checks the functionality of the computer's hardware. When power is applied to a PC, the CPU determines if proper power is available and then hands over start up control to the BIOS. The first thing run is the power-on self-test (POST). The POST is broken into two parts, with the first being the *before video test*, which test all the basic components of the PC. The POST tells all the chips on the motherboard to perform their own internal tests. The POST also tells the CPU and memory chips to run an internal diagnostic test. If any errors arise, the POST will stop and signal with a beep code. It sends out a beep code because the video portion of the computer has not been tested yet, so you will have no visual indicators of a problem. If part one passes all checks, the second part of the POST, the *after the video test* examines more complex parts of the PC. One test you can see on the monitor is the memory test. This is when the PC counts its bytes of memory looking for errors. If the POST finds an error, it will stop the test and give an error message on the monitor detailing the problem.

Next, the BIOS tries to communicate with hardware devices. If it cannot find a particular device, typically an error is displayed on-screen. Generally, these errors can be fixed by plugging in and/or turning on the offending piece of hardware and restarting the system.

After the POST has finished, the computer needs a way to find the programs to start the operating system. The POST passes control to the bootstrap loader, which is the last BIOS function, to find the PC's OS. The order of the search depends on the boot order set in the BIOS; see figure 2–10 for an example of a typical BIOS setup screen. Once it finds the OS, whether it is on the hard drive, or CD-ROM, the BIOS hands over control of the computer to the OS and the OS is loaded into your computer's RAM.

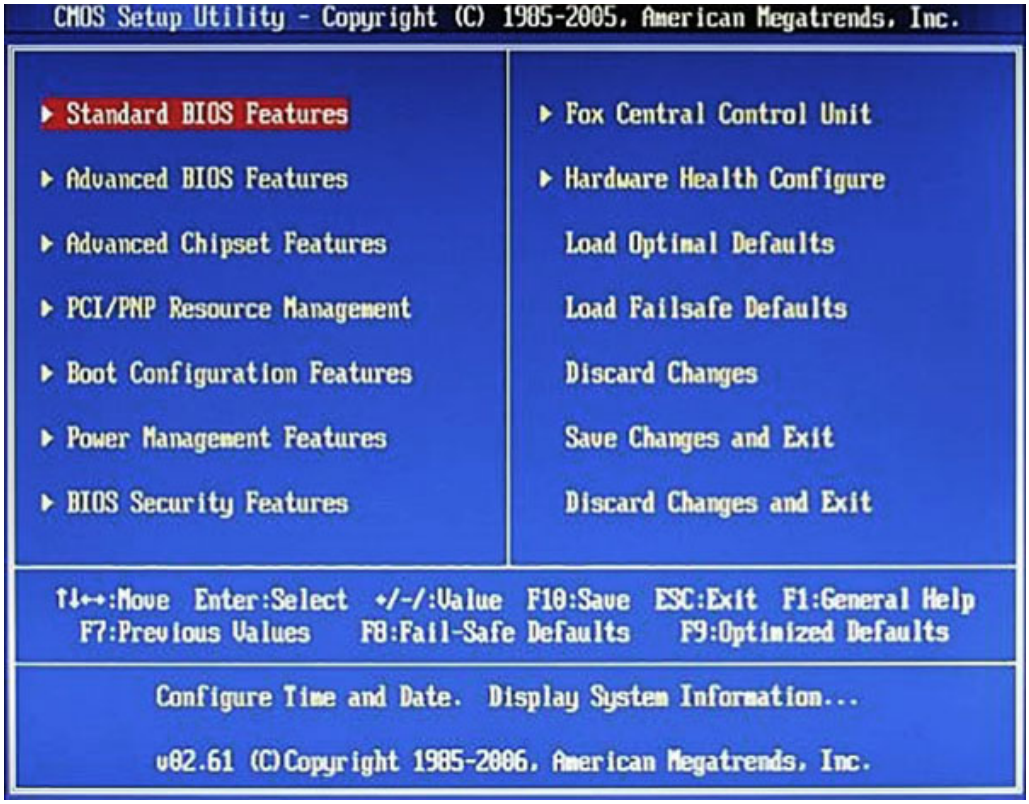


Figure 2–10. BIOS/CMOS setup screen.

BIOS is old technology that has not advanced much since the beginning of the PC. To enhance computing capability, Unified Extensible Firmware Interface (UEFI) is replacing BIOS. It replaces the traditional 16-bit x86 based BIOS with a 32 or 64-bit platform. Figure 2–11 shows an example of a UEFI BIOS setup screen. Some of the UEFI advantages include the following:

- Better security with pre-boot protection against boot-up attacks.
- Faster startup time and resume from hibernation times.
- Support for drives larger than 2.2 terabytes using globally unique identifiers (GUID) partition table.

Figure 2–11. UEFI BIOS/CMOS setup screen.

NOTE: Do not change any setting in the BIOS or UEFI unless you are sure of the impact it will have!

Device drivers

Device drivers are small, low-level programs that control devices and translate between the raw I/O format that hardware devices use and the higher-level format that the OS uses. Most programs access devices by using generic commands; however, each device has a set of specialized commands that only its driver knows. The driver accepts these generic commands from a program and then translates them into the specialized commands the device can understand. This translation by the device drivers enables the OS to operate seamlessly with many types of hardware. This allows new hardware developers to adapt their products to most OSs available in the market. OSs look at the device driver list during the boot process and copy those files into RAM, which gives the CPU the ability to communicate with the hardware supported by the device driver.

Ports

A port is a hardware interface that is the point of attachment to a computer system or unit. Ports can be located just about anywhere on a system (back, front, or side). Devices such as a keyboard, monitor, printer, and mouse are connected to the computer through ports—usually by cable. The different types of ports used to expand the capabilities of what is attached to a computer include serial, parallel, accelerated graphics, universal, and switching.

Serial port

A serial port is one type of interface that connects a device to the system unit by transmitting data one bit at a time. A serial port generally connects a device, such as a mouse, keyboard, or modem that

does not require fast data transmission rates. A communication port on a system unit is one type of serial port.

Parallel port

Unlike a serial port, a parallel port is an interface that connects devices and allows transferring of more than one bit at a time. Parallel ports were developed originally as an alternative to the slower speed of serial ports. Many older printers connect to the system unit using a parallel port. The parallel port can transfer eight bits of data simultaneously through eight separate lines in a single cable.

Universal serial bus port

Universal serial bus (USB) is a bus designed to eliminate the need of expansion cards and to standardize computer peripheral connections. It has replaced both serial and parallel ports in most modern computers. USB uses a host controller chip that controls all devices connected to it. A host controller allows the connection of up to 127 different devices. The more devices plugged in the host controller the slower the bus speed. The USB is easy to use and considered “plug and play.” Simply plug in whatever device you want to connect to the computer, there is no need to reboot the system to use the components plugged into a USB port.

If a PC does not have USB, you can add it with a PCIe card if the motherboard and BIOS support it. What if you have three USB ports and you have five USB devices to connect to the PC? Well if you do not need all five USB devices at the same time, you can plug and unplug them on the fly (even with power still on), called *hot swapping* and the PC will detect the devices automatically. If you need all five devices at the same time, you could use a USB hub to make the additional connections. USB hubs can be powered or unpowered depending on the requirements of the connecting devices. For example, if one of the devices you are using is a hard drive or scanner that requires a large amount of power, you would want to use a powered hub. However, if you were connecting a mouse, keyboard, or joystick, which are all relatively low power devices, you could use an unpowered hub.

USB cables have different ends to prevent damage to equipment. The A end connects to the PC or hub, and the B end connects to the USB device. USB comes in three different sizes: standard, mini, and micro. Standard is found on standard desktops, mini on mobile devices, and micro for tablets and accessories (e.g., watches, fitness bands, etc.). The following table shows the five different speeds currently available.

USB Standard	Name	Maximum Speed
1.1	Full speed	12 megabits per second
2.0	High speed	480 megabits per second
3.0	Super speed 5	5 gigabits per second
3.1	Super speed 10	10 gigabits per second
3.2	Super speed 20	20 gigabits per second

Display port

A display port provides the digital interface between a computer and monitor (fig. 2–12). The Video Electronics Standards Association (VESA) introduced it in 2008. Since its introduction, the display port has become the new video display standard for computer manufacturers, phasing out video graphics array (VGA) and high definition multimedia interface (HDMI) computer interfaces. A display port uses a small plug and socket with a thin cable that extends to 50 feet and it can handle multiple independent data streams, and drive up to six monitors daisy chained together.

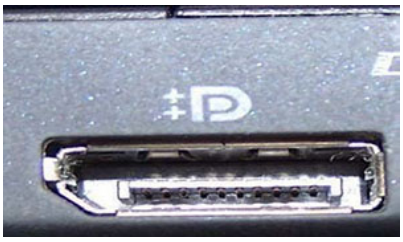


Figure 2–12. Display port.

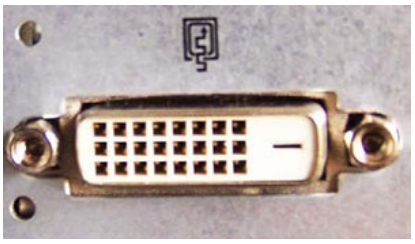


Figure 2–13. Digital visual interface.

Digital visual interface

The digital visual interface (DVI) is another widely-used port to display video digitally (fig. 2–13). It supports high-bandwidth content protection and replaces the analog VGA standard.

Storage drive technologies

One of the most important I/O devices are storage drives. Storage drives are nonvolatile memory storage for program and data not currently being used by the CPU. There are three types of storage drives currently available: hard disk drives (HDD), solid state drives (SSD), and hybrid drives. HDDs are currently the most popular primarily due to cost. Computers can accept multiple storage drives.

Hard disk drives

The HDDs are the traditional option for storage drives and consist of three primary parts: platters, read/write heads, and motor controlled actuator arm (fig. 2–14). Data are stored on the platters, which spin at very high speeds during operation. The read/write heads must perform movements with microscopic precision each time the HDD is accessed to read or write data. The tolerances are so tight that the gap between the heads and the platter is not big enough to fit a human hair.

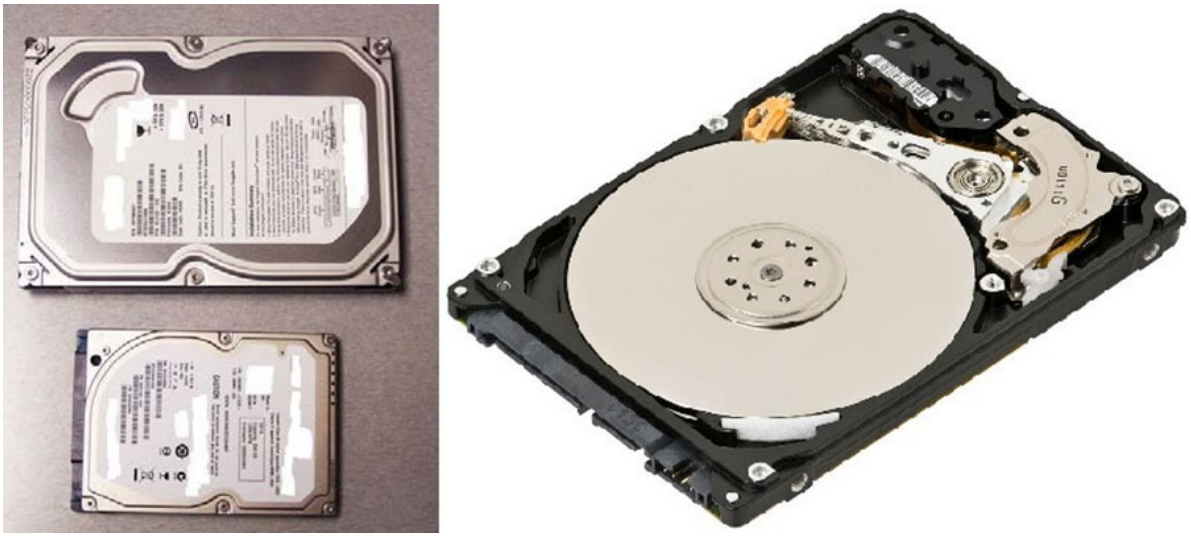


Figure 2–14. HDD external and internal view.
(Graphic by Evan Amos at Wikimedia Commons, Licensed by CC BY SA 3.0.)

HDDs used to have many different interfaces, which determined how it connected and transferred data. Most modern HDDs connect by an interface known as Serial Advanced Technology Attachment (SATA). With the correct BIOS settings, SATA supports hot swapping and auto detection. This means that without removing power, you can simply connect the power and controller cable, and the OS automatically detects the drive and it is ready for use.

HDDs are available with many spindle speeds; the following are three common spindle speeds and their applications:

1. 5,400 revolutions per minute (RPM)—used in low-end PCs.
2. 7,200 RPM—used in average mid-tier PCs.
3. 15,000 RPM—used in high-end PCs.

A sealed metal housing protects the internal components of a hard drive from contaminants. Any type of contaminant, such as dust or dirt, could block the narrow gap between the heads and the platter and cause the drive to crash by plowing a furrow in the platter's magnetic coating.

A printed circuit board, known as the *logic board*, located on the bottom of the drive, receives commands from the drive's controller, which the OS controls. The logic board translates those commands into voltage fluctuations that force the head actuator to move the read/write heads across the platter's surfaces. The board also ensures that the spindle is turning the platter at a constant speed, and tells the drive heads when to read and write to the disk. A spindle connected to an electric motor spins magnetically coated platters at several thousand RPM. The number of platters and the composition of the magnetic material coating establish the drive's capacity.

A head actuator pushes and pulls the group of read/write head arms across the surfaces of the platters with critical precision. It aligns the heads with tracks that lie in concentric circles on the surface of the platters. The read/write heads, which are attached to the arms, slide in unison across the surfaces of the hard drive's spinning platters. The heads write the data coming from the disk controller to the platters by aligning magnetic particles on the platters' surfaces. The heads read data by detecting the polarities of particles already aligned.

When you or your software tells the OS to read or write a file, the OS orders the hard disk controller to move the read/write heads to the drive's file system. The OS then reads the file system to determine in which clusters a preexisting file begins, or which portions of the disk are available to hold a new file. A single file may spread out among hundreds of separate clusters scattered across several platters; that is why it is important to run the disk defragment utility periodically on your PC in order to bring the scattered portions of a file together for faster accessing. The OS stores a file beginning in the first clusters it finds listed as free in the file system. The file system keeps a chained record of the clusters used by a file, each link in the chain leading to the next cluster containing more of the file.

Once the data from the file system passes through the drive's electronics and hard disk controller back to the operating system, the OS instructs the drive to skip its read/write heads across the surface of the platters, reading and writing clusters on the platters spinning below the heads. After the OS writes a new file to the disk, it sends the read/write heads back to the file system, where it records a list of all the file's clusters.

This unit is internal to your computer; therefore, it should not require much maintenance other than the obligatory dusting recommended in earlier sections of this volume. The hard drive is also a low replacement cost item on a PC, but could be a significant expense on a larger system. Ensure all computer diagnostics have been run before replacing the HDD.

Solid state drive

An SSD is also nonvolatile storage device that stores data. However, unlike HDDs, there are no moving parts in SSDs and they do not use magnetism. SSDs use semiconductor devices and integrated circuits to store data on flash memory chips. Due to them not having any moving parts, SSDs are inherently faster, more durable, and use less power than HDDs. SSDs do not become fragmented like HDDs, because SSDs do not have a physical read head, meaning the data can be stored and read anywhere. SSDs are ideal for both heavy read and random workloads. That lower latency is the direct result of the ability of flash SSD to read data directly and immediately from a specific flash SSD cell location. High-performance servers or any application that needs to deliver

information in real-time or near real-time can benefit from SSD technology. SSDs have a set life expectancy, as they have a finite number of write cycles before performance becomes erratic. This is not really a disadvantage per se, as HDDs degrade and eventually fail over time as well. In addition, SSDs employ wear leveling to increase drive lifespan. The flash controller typically manages wear leveling through an algorithm to distribute data write/erase cycles among all the blocks in the device. An important consideration to make with SSDs is that when left for long periods in storage without power they have a tendency to start losing data.

Hybrid drives

A hybrid hard drive contains both a traditional magnetic drive and a small amount of solid state storage. Hybrid hard drives appear as a single drive to your OS. You are not in charge of deciding which files go on the mechanical drive and which files go on the SSD. Instead, the drive's firmware manages what goes on the SSD portion.

The SSD portion of the drive acts as a "cache." Your firmware stores files you access frequently, such as your OS files and program files on the SSD portion of your drive. Although this is a cache, it is stored in nonvolatile solid state memory — that means it persists across reboots, so it speeds up your startup process.

The goal is to have the drive access system and program files with the speed of a solid state drive and provide the storage capacity of a magnetic drive for other files. The drive handles this on its own. A hybrid hard drive will be significantly faster than a mechanical drive, but a SSD will outperform a hybrid drive.

All the drives discussed above can interface with computer and networks systems in many different ways. For example, a drive could be connected internally, externally, by USB, by Ethernet, or wirelessly. There really are limitless options for interfacing or connecting storage devices.

Redundant arrays of independent disks

Redundant arrays of independent disks (RAID) is a technology that employs the simultaneous use of two or more storage drives to form a single logical storage drive for creating data redundancy. RAID is an umbrella term for computer data storage schemes that can divide and replicate data among multiple hard disk drives. RAID's various designs all involve three key design goals:

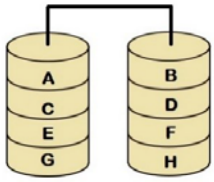
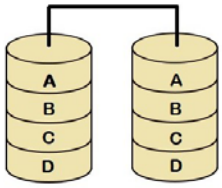
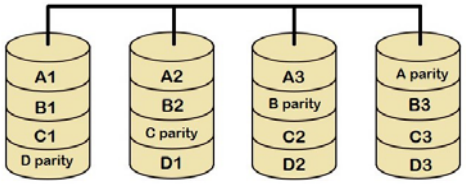
1. Increased data reliability.
2. Increased performance.
3. Larger capacity storage.

RAID principles

RAID's multiple physical hard disks are formed into a single logical unit by using hardware or software, and appear to the computer as a single hard drive. Typically, software solutions are implemented in the OS. As discussed earlier, some systems support hot swapping and others must be shut down when removing or adding a drive. Often RAID with hot-swap drives is used in PACS, where it is important the system keeps running continuously. PACS will be covered in the 4A251B CDC.

There are seven levels of RAID, numbered 0 through 6. The configuration affects reliability and performance in different ways. Out of the seven levels, only levels 0, 1, and 5 are primarily used.

RAID	Method Used	Description
0	Striping	Provides data striping (spreading data across multiple disks) but no redundancy. This improves performance but does not deliver fault tolerance. If one drive fails then all data in the array is lost. It requires a minimum of two drives (fig. 2–15).

RAID	Method Used	Description
		 **Figure 2–15. RAID 0.**
1	Mirroring/Duplexing	The same data are written to both (or all) disks, which provides a quicker read transaction rate than single drives. Data mirroring mode copies the same data to each drive one at a time using a single RAID controller and duplexing mode uses separate RAID controllers for each drive, which makes duplex mode faster than mirror mode. If one drive fails in RAID 1 (fig. 2–16) the data are still saved. Requires a minimum of two drives and if you want to add more they must be in even pair numbers (4, 6, 8, etc.). RAID 1 is ideal for data safety but consumes large amounts of storage capacity since you need double the amount of space for data (500 gigabyte for 250 gigabyte of data).  **Figure 2–16. RAID 1.**
5	Striping with Distributed Parity	Provides data striping evenly across all drives with error correction information. Protects data by adding parity data, which reconstructs data if one of the drives fails. This results in excellent performance and good fault tolerance. Level 5 (fig. 2–17) is the most popular RAID configuration and is the fastest way to provide data redundancy. It requires a minimum of three drives.  **Figure 2–17. RAID 5.**

Advantages

RAID has the following advantages:

1. By using error checking (parity), the total system is more reliable by being able to survive and repair the failure.
2. Striping is used for performance, where it allows sequences of data to be read from multiple drives at the same time.
3. Basic mirroring/duplexing can speed up reading data because a system can read different data from both drives.
4. If a drive goes bad, a new one can replace it, and the data on it reconstructed from the remaining data.

Disadvantages

On the other hand, RAID has the following disadvantages:

1. By using more disks, it is more likely that one will go wrong.
2. Mirroring may be slow for writing if the configuration requires that both disks must confirm the data is written correctly.
3. Error checking typically will slow the system as data needs to be read from several places and compared.
4. A redundant array allows less overall data to be stored.

It is important to note that redundant RAID is not an alternative to backing up data. Also, data may be damaged or destroyed without harm to the drive that it is stored. For example, part of the data may be overwritten by a system malfunction; a file may be damaged or deleted by user error or malice and not noticed for days or weeks.

Network attached storage

Network attached storage (NAS) is a networked connected storage device that permits large capacity data storage and retrieval for authorized users from a *centralized location*. The data are continuously accessible anytime and anywhere with a network connection. NAS functions similar to a private cloud configuration, but with NAS the owner has physical control over the device storing the data and with cloud services a third party maintains control. NAS devices do *not* have a keyboard or display; they are often controlled and configured over the network using a browser (fig. 2–18).

Figure 2–18. NAS device.
(Graphic by PJ at Wikimedia Commons, Licensed by CC BY SA 3.0.)

Many NAS devices have expandable capacity so that you can add additional storage. NAS devices increase availability of data because the data are not dependent on a server. If the server goes down, users can still access the data. They often are setup as RAIDs to offer data redundancy.

Self-Test Questions

After you complete these questions, you may check your answers at the end of the unit.

605. Computer core hardware principles

1. What are the four stages of computer function?

2. How does the PC get the necessary DC voltage to operate?

3. Explain what happens if the PC's AC voltage switch is improperly set.

4. What is shuts a PC down when it uses "soft power"?

5. How does power reach to all applicable computer components?

6. Why is important to ensure the PC case, power supply, and motherboard have matching form factors?

7. How are modern designs of motherboards and processers changing chipset design?

8. What three functions do chipsets typically perform? Explain each.

9. What components does a super I/O chip contain at a minimum?

10. What three types of expansion cards are found in most modern computers?

11. Explain the difference between volatile and non-volatile memory.

12. What is the basic storage unit that memory commonly uses? How many bits is it?

13. What is stored on ROM? Why is it important?

14. What is firmware?

15. Where must all programs be loaded before they can run?

16. Explain the process of how RAM is used.

17. What is the difference between SRAM and DRAM?

18. What do modern PCs use for RAM error monitoring?

19. Define cache memory

20. What order does the processor search memory when it needs data? What impact does this have on processing times?

21. What information does CMOS memory store?

22. How does CMOS retain data with the PC system power removed?

23. Why is it important to update CMOS if there are any hardware changes made?

606. Central processing unit operation principles and characteristics

1. What functions does the CPU perform?

2. How do the CPU clock and system clock differ?

3. What role does the crystal play in the system clock?

4. How is the CPU able to run at a higher speed than the system clock?

5. What are the four basic operations the control unit repeats for every function?

6. What operations does the ALU perform?

7. What role do registers have in CPU processing?

8. Briefly explain multithreading.

9. What adjustments can modern CPUs make when demand is low? When demand is high?

10. What happens if the CPU overheats?

11. What is the job of the address bus?

12. Which busses are unidirectional?

13. What are the two purposes of the control bus?

607. Principles of computer peripheral technologies

1. Briefly explain the three categories of peripheral devices.

2. What has to happen before the CPU hands over start up control to the BIOS?

3. When would the POST only send out an audible beep tone if an error is detected?

4. What BIOS functions find the OS?

5. What are some UEFI advantages over BIOS?

6. What is the function of a device driver?

7. What impact does the amount of devices plugged into a USB controller have on performance?

8. What is “hot swapping”?

9. How would you choose to use a powered or unpowered USB hub?

10. What must be established for a SATA HDD to utilize hot swapping?

11. What danger do contaminants pose to HDDs?

12. What determines a hard drive’s capacity?

13. What are two major differences of a SSD when compared to a HDD?

14. How do SSDs mitigate degradation of data?

15. What determines if data saves on the SSD or HDD portion of a hybrid drive?

16. List the three key design goals of RAID.

17. Briefly describe RAID 5.

18. What is a difference between NAS and private cloud configuration?

2–2. Operating Systems Administration

An OS is a software program that manages the sharing of computer resources. It is the interface between an application and the hardware. To execute a program, an OS must create a process. It does this by assigning memory and other resources as needed, establishing a priority for the process, loading program code into memory, and then executing the program. The program then interacts with the user or other devices and performs its intended function. The OS is the basic software that allows the user to interface with the computer. Within this section, we will cover some principles of the OS and some general information on OS installation and configuration.

608. Operating system principles

An OS is the most important software that runs on a computer. The OS manages almost every action that takes place inside the computer. A computer needs to have internal organization to run properly and its activities monitored, and the OS performs this job.

The OS affects the use of many components and resources. It decides how memory is used and is distributed, how drive space is used, how data is processed, how to accept data from the keyboard, how to send and display information on the monitor screen, and how to deal with assigned tasks. The OS is in charge and the hardware does the work.

Most of your interactions with the OS will involve disk or file management. Disk management refers to tasks that involve either your hard drive, optical discs drive (e.g., Blu-ray discs, digital video discs [DVD], CDs, etc.), or flash drives (small portable USB storage devices). These devices are affected by commands that tell your OS to perform some function. Examples of these functions include formatting a blank disk, and copying and erasing disks. Also, file management is accomplished by issuing OS commands. These commands can move, copy, erase, and rename files and directories.

Characteristics

The elements that separate one OS from another are its characteristics. This includes the way it looks and operates and the way it handles its functions, such as managing your system and the applications that run on it. An OS's most prominent characteristics are its operating environment and its user interface. These elements determine how an OS looks and how you use it. They both affect the way you communicate with it.

Multitasking

A capability characteristic of the modern OSs is multitasking. Multitasking allows you to work on two or more separate tasks from two or more different applications at the same time. For example, you could have an Internet browser open researching repair parts while also having DMLSS open as well as a word processor open to take notes.

The computer does not actually process multiple tasks simultaneously; instead, it switches between them at incredibly quick speeds, which give the appearance of running them simultaneously. CPUs have steadily improved performance and become faster over time. This allows you to run more applications on a computer at the same time and switch between them quicker. If not for multitasking, you would have to close an application each time you wanted to do something in another application.

Operating system tasks

Earlier you learned that the BIOS conducted the POST, went through the bootstrap loader, which finally loaded the OS. The OS, at the simplest level, does the following two things:

- Manages the hardware and software resources of the computer system. These resources include such things as the processor, memory, disk drives, sound card, and so forth.
- Provides a stable, consistent way for applications to deal with the hardware without having to know all the details of the hardware.

The first task, managing the hardware and software resources, is very important, as various programs and input methods compete for the attention of the CPU and demand memory, storage, and I/O bandwidth for their own purposes. In this capacity, the OS ensures each application gets the necessary resources while regulating the limited capacity of the system to the greatest good of all the users and applications.

The second task, providing a consistent application interface, is especially important if there is to be more than one of a particular type of computer using the OS, or if the hardware making up the computer is ever open to change. A consistent application programming interface allows a software developer to write an application on one computer and have a high level of confidence that it will run on another computer of the same type, even if the amount of memory or the quantity of storage is

different on the two machines. Even if a particular computer is unique, an OS can ensure that applications continue to run when hardware upgrades and updates occur.

After the computer has executed its POST and bootstrap loader, the OS functions fall into five categories:

- CPU management.
- Memory management.
- Device management.
- Application interface.
- User interface.

Some OS vendors build many more utility programs and auxiliary functions into their OS, but these six tasks define the core of nearly all OSs.

Central processing unit management

The heart of managing the CPU comes down to the following two related issues:

- Ensuring that each process and application receives enough of the CPU's time to function properly.
- Using as many CPU cycles for "real" work as is possible.

The basic unit of software that the OS deals with in scheduling the work done by the CPU is either a process or a thread, depending on the OS. It is tempting to think of a process as an application, but that gives an incomplete picture of how processes relate to the OS and hardware. The application you see (e.g., word processor, spreadsheet or game) is indeed a process, but that application may cause several other processes to begin for tasks like communications with other devices or other computers. Many processes run without giving you direct evidence that they ever exist. A process is software that performs some action and is controllable by a user, other applications, or the OS.

Memory management

When an OS manages the computer's memory, there are two broad tasks required. Each process must have enough memory to execute and it must not run into the memory space of another process nor ran into by another process. The system must properly use different types of memory so that each process can run effectively. Simply put, memory management ensures there is enough memory available to execute programs without interrupting each other.

The first task requires the OS to set up memory boundaries for types of software and for individual applications. As an example, let's look at a simple imaginary system with 1 megabyte (1,000 kilobytes) of RAM. During the boot process, the OS of our imaginary computer is designed to go to the top of available memory and then "back up" far enough to meet the needs of the OS. Let's say that the OS needs 300 kilobytes to run. Now, the OS goes to the bottom of the pool of RAM and starts building up with the various driver software required to control the hardware subsystems of the computer. In our imaginary computer, the drivers take up 200 kilobytes. Therefore, after getting the OS completely loaded, there are 500 kilobytes remaining for application processes.

The second task is to load applications into memory; they are loaded in block sizes determined by the OS. If the block size is 2 kilobytes, then every process that is loaded will be given a chunk of memory that is a multiple of 2 kilobytes in size. Applications will be loaded in these fixed block sizes, with the blocks starting and ending on boundaries established by words of 4 or 8 bytes. These blocks and boundaries help to ensure that applications will not be loaded on top of one another's space by a poorly calculated bit or two.

Device management

As previously stated, a driver's function is to translate between the electrical signals of the hardware subsystems and the high-level programming languages of the OS and application programs. Because

there are such wide differences in the hardware controlled through drivers, there are differences in the way driver programs function, but most are run when the device is required and function much the same as any other process. The OS will frequently assign high priority blocks to drivers so that the hardware resource can be released and readied for further use as quickly as possible. One reason that drivers are separate from the OS is so new functions can be added to the driver, and thus to the hardware subsystems, *without* requiring the OS itself to be modified, recompiled and redistributed.

Application program interface

Just as drivers provide a way for applications to make use of hardware subsystems without having to know every detail of the hardware's operation, the application program interface lets application programmers use functions of the computer and OS without having to keep track of all the details directly in the CPU's operation. For example, a programmer writing an application to record data from a scientific instrument might want to allow the scientist to specify the name of the file created.

User interface

The user interface is the style displayed on-screen that enables the user to interact with the system. A user interface consists of the on-screen design, the way options are presented, the way commands are issued and any other item that affects the method of communication. The three main types of user interfaces are command-driven, menu-driven, and graphical user interfaces (GUI). Let's look at each of these interfaces.

Command-line interface

When using a command-line interface, the user makes requests of the system by typing in commands at a prompt. The prompt is the user's cue to type a command. In this type of environment, the user must know what command to use and the correct syntax of the command. If the command is typed in wrong, the system will not understand the user's request and the function will not be carried out. It is a good idea to have a manual available that list each command and its purpose. Figure 2–19 shows a typical Windows command prompt ready for its next command.

A command-line interface may seem to put the user at a disadvantage, but in terms of system resource utilization, the command-line interface is the most beneficial. It uses less RAM and less power from the CPU than any other interface.

Menu-driven interface

A menu-driven interface goes one step further than the command-driven interface. It gives the user a list of commands to choose. These lists are displayed in menus, or boxed-in lists of choices. The user selects a menu item using the arrow keys on the keyboard, typing in a keyboard character to indicate a selection, or using a pointing device, such as the mouse.

Graphical user interface

A GUI provides pictures rather than just characters to represent options, programs, and parts of programs. Commands are displayed as icons, or pictorial representations. The user issues commands by selecting icons with a pointing device. GUIs also use menus to list some commands.

GUIs are designed to be user-friendly and are the most popular interface. It emulates the arrangement of your actual desktop where everything you need is laid out in front of you so you can just point and begin a program. The idea is that pointing and clicking a mouse button is faster and easier to learn than remembering and typing out a long command. However, GUIs take up more of your system's RAM and require the most CPU power. The data needed to produce icons requires a large amount of memory.

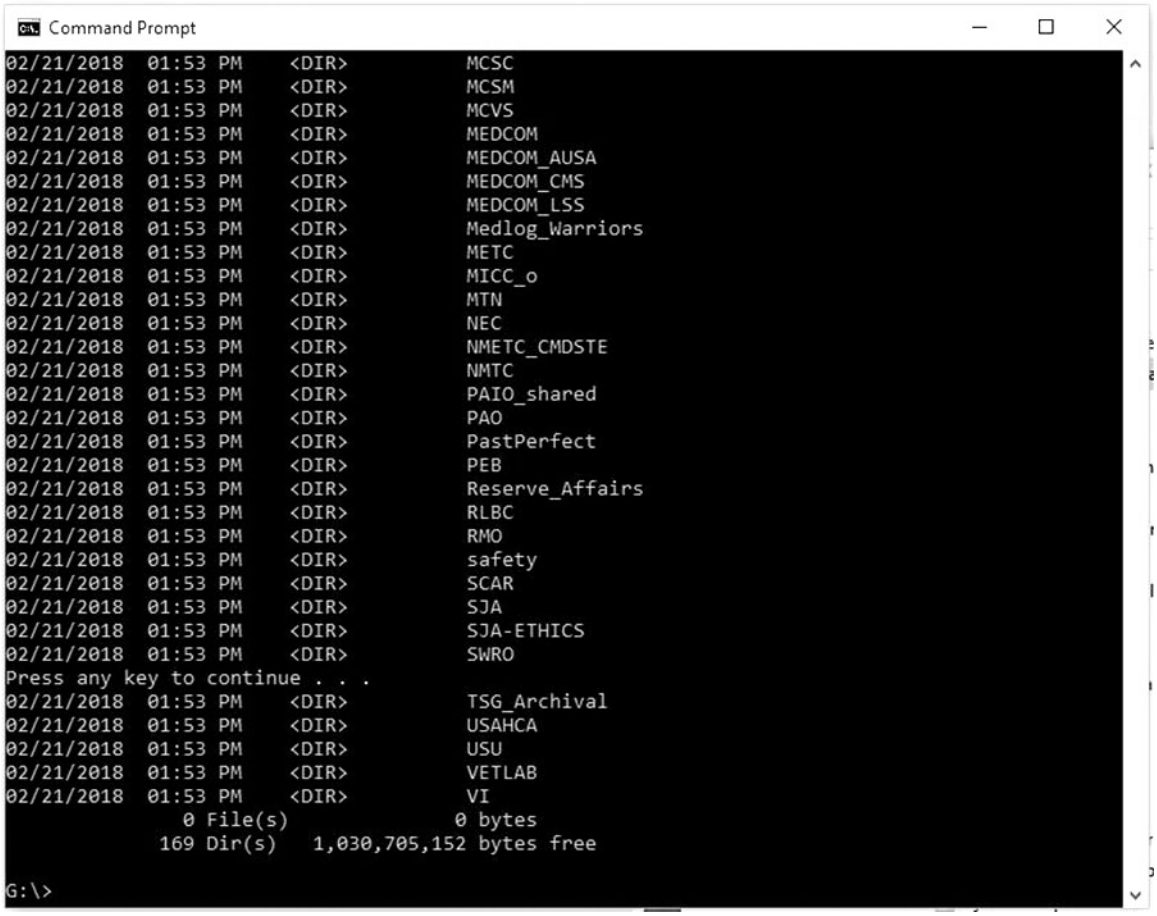


Figure 2–19. Windows 10 command prompt.

609. Installing and configuring an operating system

Remember that any software installed on DOD assets must be validated and approved *prior* to the installation. During the approval process, these items are tested to ensure products meet minimum system security requirements.

System requirements

To be used efficiently, all computer software needs certain hardware components or other software resources to be present on a computer system. These prerequisites are known as system requirements or installation requirements and are often used as a guideline as opposed to an absolute rule. The two sets of system requirements that most software defines are the minimum and the recommended requirements. With increasing demand for higher processing power and resources in newer versions of software, system requirements tend to increase over time. Industry analysts suggest that this trend plays a bigger part in driving upgrades to existing computer systems than technological advancements.

Minimum requirements

The minimum system requirements must be satisfied for the software to be usable at all. Computers with lower specifications than the minimum requirements may sometimes run the software, but it is suggested that the user will not have a representative experience of the software this way. Generally, this set is regarded more of a rule than a guideline. A system meeting this requirement will provide basic performance of a software application.

Recommended requirements

Recommended system requirements are suggestions made by vendors for optimal performance of software. Although not a necessity, this set of requirements is important for users who expect to gain a better experience of software usability. Recommended system requirements do not promise best possible performance of software and are treated as more of a guideline than a rule. A better system is usually available, or will be the in future, to provide better performance. In addition, exceeding these requirements by far does not guarantee to the user that everything will run with absolute smoothness and look its best.

Hardware requirements

The most common set of requirements defined by any OS or software applications is the physical computer resources, or hardware. A hardware requirements list often is accompanied by a hardware compatibility list (HCL), especially in case of OSs. An HCL lists tested, compatible, and sometimes incompatible hardware devices for a particular OS or application. Various aspects of hardware requirements include its architecture, processing power, memory, secondary storage, display adapter, and peripherals.

Architecture

All computers OSs are designed for a particular architecture. Most software applications are limited to a particular OS running on a particular architecture. Although architecture independent OS and applications exist, most need to be recompiled to run on a new architecture.

Processing power

The power of the CPU is a fundamental system requirement for any software. With software running on the x86 architecture, processing power is defined as the model and the clock speed of the CPU. Many other features of a CPU that influence its speed and power, like bus speed and cache, often are ignored. This definition of power is often erroneous, as CPUs at similar clock speed often have different throughput speeds.

Memory

All running software resides in the RAM of a computer. Memory requirements are defined after considering demands of the application, OS, supporting software and files, and other running processes. Optimal performance of other unrelated software running on a multitasking computer system also is considered when defining this requirement.

Secondary storage

Hard drive requirements vary depending on the size of software installation, temporary files created and maintained while installing or running the software, and possible use of swap space (if RAM is insufficient).

Display adapter

Software requiring a better than average computer graphics display, like graphics editors and high-end games, often define high-end display adapters in the system requirements.

Peripherals

Some software applications need to make extensive or special use of some peripherals, demanding the higher performance or functionality of such peripherals. Such peripherals include CD drives, keyboards, pointing devices, networks devices, etc.

Operating system installation

Installation requirements for an OS will vary depending on what you want to do, and why. Installing a new OS is different than upgrading an OS to the most current version. It is also different than reinstalling an OS. Many precautions are the same, but the processes are different. Before you install, reinstall, or upgrade an OS, first figure out exactly which of these you are planning to do. Once you have done that, you need the OS installation program. This can be in a CD, DVD, or a flash drive.

Let's look at the actual process:

1. Back up data. If you are reinstalling the current OS, you need to wipe the disk (drive). If you do not want to lose everything on the drive, back up the data before you wipe it. If simply upgrading, it is okay to skip this step, but it is highly advisable to save the most important files at minimum. Put them on a CD, DVD, or external hard drive so you can access them in case you end up wiping the hard drive.
2. Wipe the drive. There are "disk wiping" utilities you can use to facilitate this process.
3. Turn the computer back on and access the BIOS to enter the boot menu. Recall from earlier that you typically will have to press a designated button (e.g., DELETE, ESCAPE, or F10) during boot up of the system to enter the menu. You may need to read the manual for the computer or motherboard for instructions.
4. Once in the boot menu, rearrange the boot sequence order by placing the drive that will contain the setup disk as first drive on the list. Failure to do this step will result in the BIOS simply just loading the currently installed OS.
5. Insert the installation disc into the drive identified in previous step.
6. Then save setting, exit boot menu, and restart the computer.
7. The computer should automatically boot the installer. It is normal for the install program to take a few minutes to load. Once it has loaded, simply follow the on-screen instructions. The installer may ask for information while it is installing, but for the most part, you will just be waiting for it to finish what it needs to do. Near the end of the installation, the installer will ask for final information such as user name, name of the computer, sign in name, password, time zone, etc. If you are installing a consumer OS like Windows, you will have to enter a product identification (ID). These are typically on the CD case or provided directly from manufacturer. This does not apply if installing Linux.
8. Reboot the computer to finalize everything and to log you in once the installation is complete.
9. Install your drivers. Insert any driver disks that came with your computer or its parts, and allow the drivers to be installed (as necessary). Your OS can also find most drivers on the Internet automatically once you establish a connection. If it does not perform this action automatically, you will have to download the drivers from the manufacturer's Web site manually.
10. Install antivirus immediately after the OS installation is complete.
11. Install any necessary updates.
12. Set password, install programs, customize, create user accounts, and so forth. If you have any files backed up, you may restore them now.

Operating system minimum hardware specifications

Before installing an OS, special consideration must be taken to ensure the computer hardware you are loading the software on is compatible and powerful enough to run without constant problems. We must ensure the computer meets the minimum requirements for the OS to run. These minimum requirements are handed down by the software developer and should be at least met, if not exceeded.

Self-Test Questions

After you complete these questions, you may check your answers at the end of the unit.

608. Operating system principles

1. What is the job of the OS?

2. Explain OS multitasking.

3. What are two issues are at the core of CPU management?

4. What two broad tasks are required when an OS manages memory?

5. Why are drivers separated from OS software?

6. What are the three types of user interfaces?

7. What is a disadvantage of GUI?

609. Installing and configuring an operating system

1. Why is it important that software installed on DOD assets be validated *prior* to install?

2. Explain the difference between minimum and recommended requirements.

3. What information is on a HCL?

4. What is the *first* step in installing an OS? Why is it important to perform this action?

5. Why is it required to change the boot sequence when installing an OS?

6. How can you obtain device drivers if the device driver discs are not on hand?

Answers to Self-Test Questions

605

1. Input, process, output, and storage.
2. The power supply converts 120 volts AC commercial power down to low voltage DC power for PC use.
3. If you select 230V and plug the PC into 120V it will most likely just not be able to properly boot up. However, if you select 115 volts and plug the PC into 230 volts it will destroy the power supply, and possibly the motherboard and other components.
4. The BIOS or OS shuts the system down.
5. The motherboard distributes power from the power supply to all other components.
6. This ensures that the correct power is applied to the board, the board fits inside the case with proper mounts, and the ports align with the openings.
7. Newer motherboard and processor designs integrate traditional functions of a chipset into the processor themselves.
8. System controller, peripheral controller, and memory controller. System controller brings the functions of the entire PC together, giving all the support the microprocessor needs to function. Peripheral controller enables the microprocessor to operate I/O ports, expansion buses, and disk interfaces. Memory controller links the microprocessor to the memory system and establishes the main memory and cache architectures; thus assuring the reliability of the data stored away in RAM.
9. Controller for floppy drive, hard drive, dual serial port, parallel port, keyboard, and PS/2 mouse.
10. Sound card, graphic card, and network interface card.
11. With volatile memory, the data contents are lost when power is removed. As a result, software programs use volatile memory for temporary storage of data. With nonvolatile memory, the data is retained after power is removed.
12. The byte. 8 bits.
13. ROM contains the computer's BIOS programming which enables the computer to communicate with various devices and provides instructions the computer needs to correctly start
14. Firmware refers to any data or instructions stored on a ROM chip.
15. RAM.
16. When the computer is powered on, certain OS files load from a storage device such as a hard drive into RAM. These files stay in RAM as long as the computer is running. As the user requests more programs and data, they also load from storage into RAM. The processor interprets the data while it is in RAM. The contents of RAM may change during this time. RAM can hold multiple programs simultaneously provided there is enough RAM to accommodate all of the programs.
17. SRAM chips are faster and more reliable than any variation of DRAM chips. Unlike DRAM, SRAM chips do not have to be refreshed. SRAM chips, however, are much more expensive than DRAM chips. If DRAM is not constantly refreshed it loses its contents.
18. ECC RAM.
19. A type of SRAM that stores frequently accessed data to increase PC processing speeds.
20. It searches memory in this order L1 cache, then L2 cache, then L3 cache, and then RAM. There is a greater delay in processing for each level of memory it must search.
21. CMOS memory stores device parameters.
22. It uses a lithium battery.
23. Failure to update the CMOS to reflect the change of any hardware accurately will prevent the PC from being able to use the device.

606

1. It performs the computer program's calculations, moves data, executes the instructions provided by firmware and software, and manages interactions between itself and other computer components.
2. The CPU clock is how fast the CPU is operating; CPU clock speed is the maximum speed the CPU can run. The system clock synchronizes the timing of the CPU and all other components and not their operational speed.

3. The crystal controls the oscillator's pulsing so that it is highly accurate and continually emits pulses at the same rate.
4. By utilizing clock multipliers.
5. Fetch, decode, execute, and store.
6. Performs arithmetic, comparison, and logical operations.
7. Registers are high-speed storage locations the CPU uses to hold data and instructions temporarily.
8. Multithreading enables the CPU to run more than one thread at a time. For it to properly work, the OS and the CPU must be designed for it. The OS perceives one CPU as two or more separate CPUs when multithreading.
9. CPUs have the ability to throttle down when the demand is low. Clock boost enables it to perform temporarily at its max rated speed when demand is high.
10. Overheating of the CPU can cause abrupt system shutdowns, program freezing, and the dreadful blue screen crash.
11. Provide a means of identifying which component it is talking to each time. It selects or enables the proper destination and return for communications.
12. Address bus and control bus.
13. Two purposes are to signal the start and stop of communications and to define the type of communication.

607

1. Input devices input information into the system, output devices allow the computer to organize the information into a tangible form that we can understand, and I/O devices perform both.
2. The CPU verifies that proper power is available.
3. If any errors arise during the "before video test" the POST will stop and signal with a beep code because the video portion of the computer has not yet been tested.
4. Bootstrap loader.
5. Better security with pre-boot protection against boot-up attacks, faster startup time and resume from hibernation times, and it supports drives larger than 2.2 terabytes using GUID partition table.
6. Control devices and translate between the raw I/O format that hardware devices use and the higher-level format that the OS uses.
7. The more devices plugged in the host controller the slower the bus speed.
8. The ability to plug and unplug devices with power on or off and the computer automatically detects them.
9. If one of the devices you are using requires a large amount of power (a hard drive or scanner) then use a powered hub, but if they are all relatively low power devices (a mouse, keyboard, or joystick) then use an unpowered hub.
10. The correct BIOS setting.
11. Any type of contaminant, such as dust or dirt, could block the narrow gap between the heads and the platter and cause the drive to crash by plowing a furrow in the platter's magnetic coating.
12. The number of platters and the composition of the magnetic material coating.
13. SSDs do not have any moving parts and do not use magnetism.
14. To increase drive lifespan, SSDs employ wear leveling which the flash controller typically manages through an algorithm to distribute data write/erase cycles among all the blocks in the device.
15. The user is not in charge of deciding which files go on the mechanical drive and which files go on the SSD. The drive's firmware manages what goes on the SSD portion.
16. Increased data reliability, increased performance, and larger capacity storage.
17. Provides data striping evenly across all drives with error correction information. Protects data by adding parity data, which reconstructs data if one of the drives fails. It is the most popular configuration and requires a minimum of three drives.
18. With NAS the owner has physical control over the device storing the data and with cloud services a third party maintains control.

608

1. Manage the internal organization of a computer and monitor its activities.
2. Multitasking allows you to work on two or more separate tasks from two or more different applications at the same time.
3. Ensuring that each process and application receives enough of the CPU's time to function properly, and using as many CPU cycles for "real" work as is possible.
4. Each process must have enough memory to execute and it must not run into the memory space of another process nor ran into by another process.
5. So that new functions can be added to the driver and hardware without requiring the OS to be modified.
6. Command-driven, menu-driven, and GUI.
7. They take up more of the system's RAM and require the most CPU power.

609

1. Software is tested to ensure the product meets minimum security requirements during the approval process.
2. Minimum system requirements must be satisfied for the software to be usable at all, and recommended requirements are vendor's suggestions for optimal software performance.
3. An HCL lists tested, compatible, and sometimes incompatible hardware devices for a particular OS or application.
4. Back up data. If you are reinstalling the current OS, you need to wipe the disk (drive) and you will lose everything that is on the drive if you do not back up the data before wiping it.
5. The OS install will be carried out from an installation disc or other media. So you have to tell the BIOS the location of this disc or media and place it first so it will go there first and not run your old OS.
6. The OS can automatically find most drivers on the Internet.

Complete the unit review exercises before going to the next unit.

Unit Review Exercises

Note to Student: Consider all choices carefully, select the *best* answer to each question, and *circle* the corresponding letter.

Do not return your answer sheet to AFCDA.

7. (605) How many volts direct current (VDC) does a personal computer's (PC) power supply provide for the microprocessor and memory?
   a. +3.3.
   b. +5.0 and –5.0.
   c. +6.0.
   d. +12.0 and –12.0.

8. (605) Which feature ensures the operating system (OS) is ready to shut down *prior* to the system shutting down?
   a. Indirect power.
   b. Power saving.
   c. Sleep mode.
   d. Soft power.

9. (605) What categorizes a motherboard's size and connector layout?
   a. Manufacturer.
   b. Form factor.
   c. Model.
   d. Make.

10. (605) What do chipsets use to handle older technologies that still require support?
    a. Expansion card.
    b. System controller.
    c. Peripheral controller.
    d. Super input/output (I/O) chip.

11. (605) What allows the addition of new functions without having to replace the motherboard?
    a. Chipsets.
    b. Expansion slots.
    c. Read-only memory (ROM).
    d. Random access memory (RAM).

12. (605) Which *temporary* electrical storage space holds program instructions and program data?
    a. Random access memory (RAM).
    b. Read-only memory (ROM).
    c. Erasable programmable read-only memory (EPROM).
    d. Data processing read-only memory (DPROM).

13. (605) Which type of random access memory (RAM) is the fastest and most reliable?
    a. Static RAM (SRAM).
    b. Dynamic RAM (DRAM).
    c. Synchronous DRAM (SDRAM).
    d. Double data rate (DDR) SDRAM.

14. (605) In most modern computers, which level of cache is *usually* the smallest in capacity?
    a. Level 1 (L1).
    b. Level 2 (L2).
    c. Level 3 (L3).
    d. Level 4 (L4).

15. (605) Where does a processor search *first* when it needs an instruction?
    a. Random access memory (RAM).
    b. Level 1 (L1) cache.
    c. Level 2 (L2) cache.
    d. Level 3 (L3) cache.

16. (605) Which memory stores device parameters that the basic input/output system (BIOS) uses every time the system is started?
    a. Cache memory.
    b. Read-only memory (ROM).
    c. Random access memory (RAM).
    d. Complementary metal oxide semiconductor (CMOS).

17. (606) Which component is considered the brain of a computer system?
    a. Random access memory (RAM).
    b. Central processing unit (CPU).
    c. Operating system (OS).
    d. Motherboard.

18. (606) Which basic operation process of the central processing unit's control unit is responsible for carrying out commands?
    a. Fetch.
    b. Decode.
    c. Execute.
    d. Store.

19. (606) Which part of the central processing unit (CPU) does all the computing?
    a. Registers.
    b. Control unit.
    c. Memory controller.
    d. Arithmetic logic unit.

20. (606) In which type of central processing unit (CPU) architecture does the operating system (OS) *perceive* one CPU as two or more separate CPUs?
    a. Clock boost.
    b. Multicore.
    c. Multithread.
    d. Over-clocking.

21. (606) Which bus is bi-directional?
    a. Memory.
    b. Address.
    c. Control.
    d. Data.

22. (607) An example of an input/output (I/O) device is a
    a. mouse.
    b. printer.
    c. keyboard.
    d. touchscreen monitor.

23. (607) What is the *first* thing the basic input/output system (BIOS) accomplishes at start-up?
    a. Load programs to random access memory (RAM).
    b. Run the power-on self-test (POST).
    c. Read instructions from read-only memory (ROM).
    d. Read instructions from RAM.

24. (607) Which of the following initializes communication with all hardware devices?
    a. Read-only memory (ROM).
    b. Random access memory (RAM).
    c. Basic input/output system (BIOS).
    d. Power-on self-test (POST).

25. (607) Which are small low-level programs that translate between the raw input/output format that hardware devices use and the higher-level format that the operating system (OS) expects?
    a. Batch files.
    b. Device drivers.
    c. Software diagnostics.
    d. Hardware diagnostics.

26. (607) Up to how many different universal serial bus (USB) devices can be connected to a single host controller?
    a. 107.
    b. 117.
    c. 127.
    d. 137.

27. (607) Which does *not* require a system reboot when a new device is plugged into it?
    a. Accelerated graphics port (AGP).
    b. Industry standard architecture (ISA).
    c. Peripheral component interface (PCI).
    d. Universal serial bus (USB).

28. (607) Why are hard disk drives (HDDs) the most popular storage drive technology?
    a. Performance.
    b. Adaptability.
    c. Durability.
    d. Cost.

29. (607) What protects the internal components of a hard disk drive (HDD) from dust particles?
    a. Filter.
    b. Internal fan.
    c. Sealed metal housing.
    d. Preventive maintenance.

30. (607) What manages which files go on the solid state drive (SDD) or hard disk drive (HDD) portions of a hybrid drive?
    a. Operating system (OS).
    b. Hybrid drive's firmware.
    c. User selects when saving data.
    d. Automatically fills SSD first then the HDD.

31. (607) Which redundant arrays of independent disks (RAID) consumes large amounts of storage capacity because it requires double the amount of space for data?
    a. RAID 0.
    b. RAID 1.
    c. RAID 5.
    d. RAID 6.

32. (608) Which separates one operating system (OS) from another?
    a. Size.
    b. Price.
    c. Functionality.
    d. Characteristics.

33. (608) Why are device drivers made separate from operating systems (OS)?
    a. To allow addition of new hardware without requiring OS modification.
    b. The OS is not capable of performing device driver duties.
    c. To alleviate the workload of the OS.
    d. To increase system speed performance.

34. (608) Which operating system (OS) user interface uses the least amount of random access memory (RAM) and central processing unit (CPU) power?
    a. Graphical user interface (GUI).
    b. Command-line interface.
    c. Menu-driven interface.
    d. Point-to-point interface.

35. (608) Which operating system (OS) user interface is the most popular and user friendly?
    a. Graphical user interface (GUI).
    b. Menu-driven interface.
    c. Command-driven interface.
    d. Point-to-point interface.

36. (608) Which operating system (OS) user interface consumes the *most* system resources?
    a. Graphical user interface (GUI).
    b. Menu-driven interface.
    c. Command-driven interface.
    d. Point-to-point interface.

37. (609) Which computer software system requirement is regarded more as a rule than a guideline?
    a. Maximum requirements.
    b. Minimum requirements.
    c. Suggested requirements.
    d. Recommended requirements.

38. (609) Which computer software system requirement is regarded more as guideline than a rule?
    a. Maximum requirements.
    b. Minimum requirements.
    c. Suggested requirements.
    d. Recommended requirements.

39. (609) Where does all *running* software reside?
    a. Random access memory (RAM).
    b. Central processing unit (CPU).
    c. Read-only memory (ROM).
    d. Hard drive.

40. (609) What is the *first* step you perform when installing an operating system (OS)?
    a. Access the basic input output system (BIOS).
    b. Insert installation disc.
    c. Wipe the drive.
    d. Back up data.

Please read the unit menu for unit 3 and continue ➔

Unit 3. Networking

THE INCREASED INTEGRATION of it and medical equipment increases the need for you to understand how networks enable communication between medical devices in your MTF or across the world. In unit 2, you learned about individual computer system components and their functionality. This unit expands on that knowledge by looking at how those individual systems connect to each other to perform tasks. Even if you are at a facility that does not allow BMETs privileged access to the network quite yet, having knowledge about networks will still help you troubleshoot equipment or plan equipment installs.

3–1. Network Models and Protocols

Numerous medical devices and systems connect to each other by way of a network. These networks can be inside the MTF, outside the MTF, or a combination of both. Diagnostic imaging sections are good examples of a networked medical system. It allows a small MTF without a radiologist to transmit studies to a radiologist at a different facility to read. The radiologists can then transmit the report back to the originating MTF. Networks also make your maintenance operation visible to Air Force Medical Operations Agency (AFMOA). In this section, we will discuss types of networks, network models, and protocols.

610. Principles of network types

We will begin learning about networking by first discussing different types of networks including local area network (LAN), metropolitan area network (MAN), wide area network (WAN), and virtual private networks (VPN). The following table provides a few definitions to know before discussing network types.

Term	Definition
Internet	It is a series of private computer networks connected to each other, often also referred to as the World Wide Web or public Internet. Each individual private network is composed of a series of connected computers within an organization. Each organization takes responsibility for only the computers in its area of influence.

Term	Definition
Intranet	It exists as a portion of an organization's private network comprised of one or more inter-connected LANs within the organization. Intranets use the same software (e.g., Web browsers) and the same protocols as the public Internet, but, unlike the Internet, the content is restricted to authorized organization users only. Essentially, an Intranet is a private Internet.
Extranet	Extranet is an intranet that shares a portion of its content with customers, suppliers, or other businesses, but not with the public. As with intranets, they use the same Web browsers and other software to enable access to their content.

Local area network

A LAN is a network that encompasses two or more computer workstations connected by one or more types of media (fig. 3–1). Network media directly connects devices physically located in a LAN. Workstations are located within close proximity of each other. This distance can be a single office, between offices within a building, or sometimes between buildings. A LAN spans an area of up to 2 kilometers (about 1.25 miles). Technologically, LANs are simple to build and maintain. The LANs require only basic rules and protocols, as they are limited in scope to small areas and use similar systems, typically only basic networking devices. The LANs can also include wireless connectivity. Wireless local area networks (WLAN) are generally extensions of an existing wired infrastructure, although they may be a standalone network.

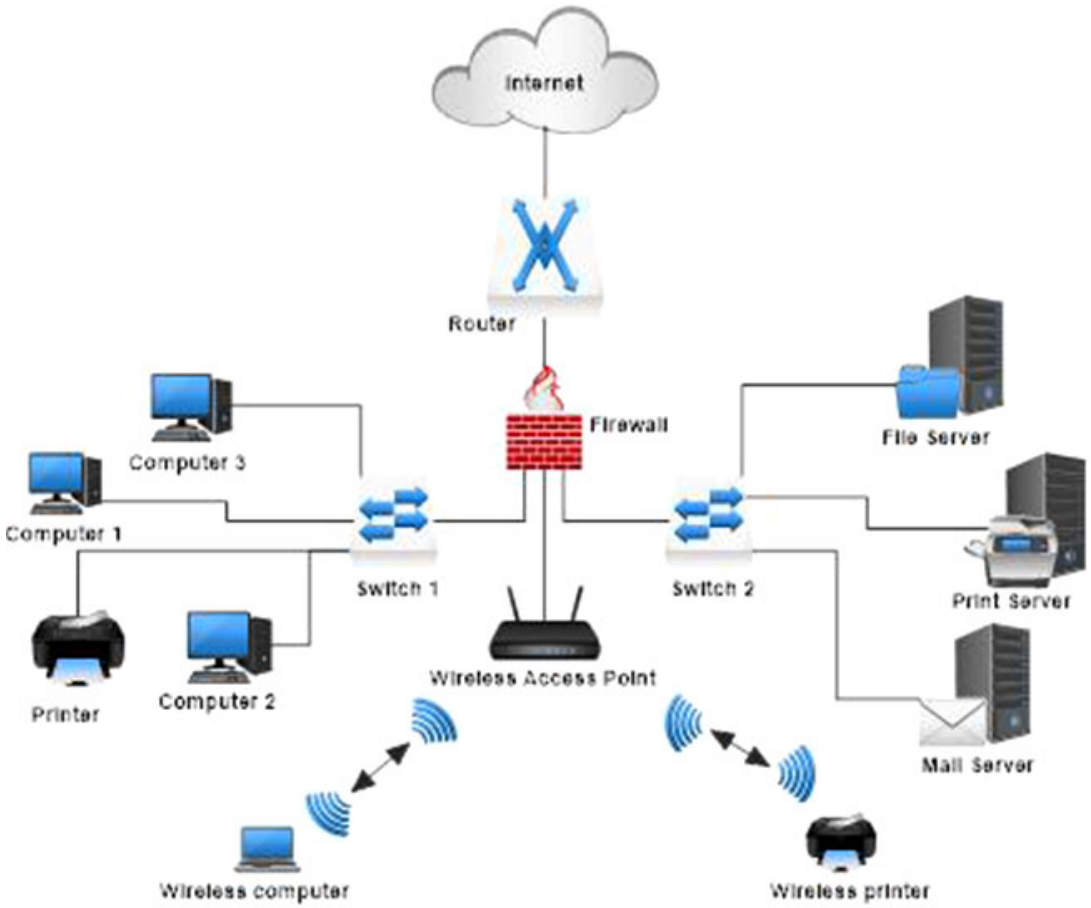


Figure 3–1. Example of a LAN.

The major benefits of using WLAN are as follows:

- *Mobility*. Users can move about anywhere coverage is available and not be restricted by the length or location of a wire.
- *Ease of installation and lower costs.* Installing network cabling in buildings can be a difficult and costly task. Thick masonry walls and plaster ceilings are difficult to drill holes through and snake cabling around. Wireless networks make it easier to modify offices with new cubicles or furniture. The design for a remodeled work center does not have to consider the location of a wall jack when relocating furniture or equipment. In addition, the time to install network cabling is significant. Technicians pull wires through the ceiling and drop cables down walls to network outlets. This can take hours or days to complete. Using a WLAN eliminates any disruption because there are no cables to install.

A major concern with using the WLAN is security. The threat of signal interception in traditional networks is relatively low since the signal is contained within a cable. With wireless networks however, there is no cable to contain the signal, which makes it easier for an attacker to intercept network traffic and analyze it for useful information. Because of this serious threat, wireless networks have their own unique vulnerabilities.

Metropolitan area network

A MAN is a network that connects two or more LANs in a geographic area or region greater than that covered by a LAN but smaller than the area covered by a WAN. A MAN connects computer networks within the same city or metropolitan area. A distance of up to 50 kilometers (about 31 miles) can separate the connected networks. MANs require more complicated sets of rules, protocols, and equipment than LANs. In addition to the basic LAN devices, MANs often employ any number of protocols and Internet-working devices that are required to route data between LANs and other MANs. Military bases' computer networks normally fall in this category.

Wide area network

A WAN is a network that links LANs or MANs using long-distance communication links such as telephone, microwave, or satellite communications (fig. 3–2). A WAN connects networks separated by large geographical distances that can be between two cities across a country or around the world.

In addition to the basic LAN devices, WANs (and MANs) employ "Internet-working" devices and protocols to route data between networks. Many of the active networks focus on information exchange such as e-mail, World Wide Web applications, or file transfers. Other popular services focus on real-time interactive communications such as video teleconferencing.

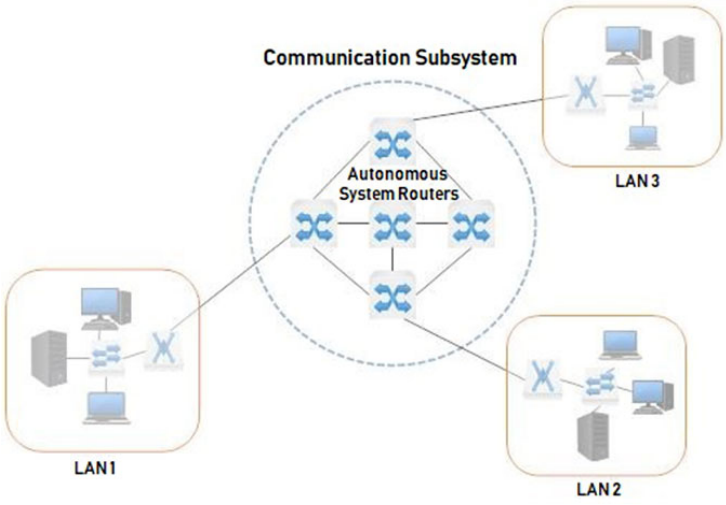


Figure 3–2. Example of a WAN.

The WANs can also be wireless. Wireless wide area networks (WWAN) systems typically provide wireless connectivity using cellular network technology. Some examples of WWAN technologies are Long-Term Evolution and Worldwide Interoperability for Microwave Access.

Virtual private networks

VPNs provide an encrypted means of transporting private network data through the Internet (a public network) (fig. 3–3). VPNs allow a device that is remote of the private network to function as if it is has a direct connection to the private network.

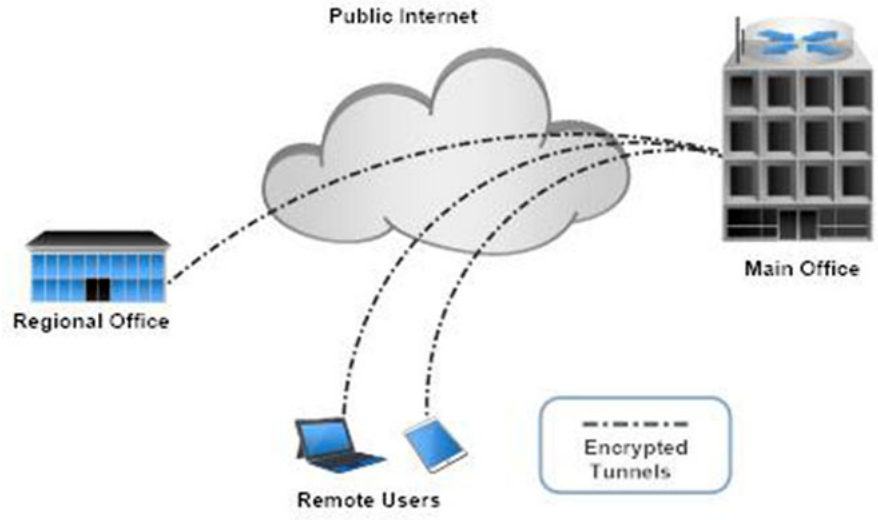


Figure 3–3. Example of a VPN.

VPNs may exist between an individual device and a private network, or a remote LAN and a private enterprise network. Secure VPNs make use of tunneling and security protocols to maintain the privacy of data transactions over the Internet.

The idea is to make a private network that provides a secure tunnel for the private exchange of data between two or more parties. To implement over a “real” private network, the dedicated lines and service required would be cost prohibitive. However, establishing a secure tunnel over a public network, such as the Internet, there is no additional cost because the service already exists. The two main drivers for using a VPN are remote access and extranet connections.

Remote access is a requirement for our networks. When users go to a temporary duty location, they may have a need to access their home network. A VPN allows for a secure, encrypted connection for the remote users, and can work over high-speed connections as well as dial-up connections, allowing for flexibility in operations.

A VPN can also work as an extranet connection. This allows outside users access to network data through a secure Web browser connection. The users will still need to authenticate before they can gain access.

The configuration of VPNs is usually a peer-to-peer or gateway-to-gateway connection. Most VPN traffic in the DOD occurs in the gateway-to-gateway configuration, securing the connection between the base and the rest of the enterprise network.

611. Open system interconnection reference model principles

The open system interconnection (OSI) model is a set of guidelines used for the development of open systems. The model describes how information from a software application in one computer moves through a network to a software application in another computer. The OSI model also establishes guidelines so software and hardware components from different manufacturers can interoperate

across diverse networking environments. This lesson introduces the characteristics of the OSI model, as well as how the model dictates communication between systems on a network.

It is important to note the OSI model is not a working protocol. It does not provide services or functions. Instead, it identifies how delivery of those services and functions should occur. Although the OSI model is a reference for all hardware and software manufacturers, it will also help you understand where components fit into the networking process.

The OSI reference model is a conceptual model composed of seven layers, each specifying particular network functions. Developed by the International Organization for Standardization (ISO) in 1984, the model allows different network vendors (both hardware and software) the ability to produce products that can communicate with each other across any type of media. The OSI model is now the primary architectural model for computer communications.

The OSI model divides the tasks involved with moving information between networked computers into seven smaller, more manageable task groups (layers). Each layer is reasonably self-contained, so implementation of the tasks assigned to each layer can occur independently. This allows vendors to update the capabilities of one layer without adversely affecting the other layers.

Our discussion will begin with the lower layers and progress into the upper layers. Figure 3–4 shows all seven layers.

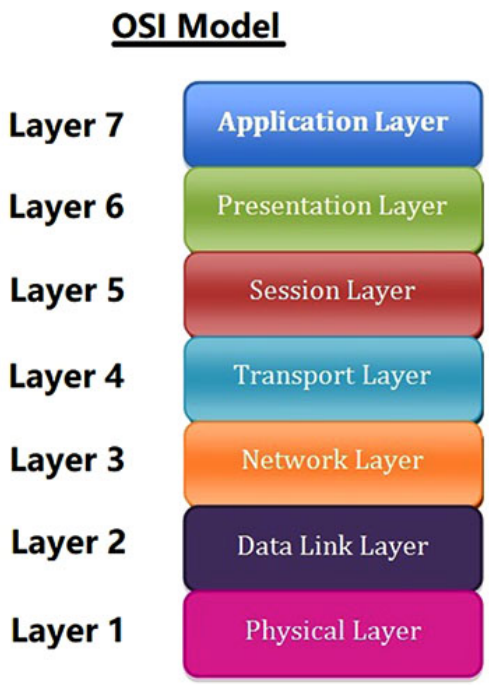


Figure 3–4. OSI model layers.

Layers one through four of the OSI model handle data transport issues and are responsible for defining how data moves across the physical media, through Internet-working devices, to the destination computer and to the application on the destination machine. Implementation of the Physical layer and Data Link layer occurs in hardware and software. Implementation of the remaining lower layers generally occurs only in software. The lowest layer, the Physical layer, is closest to the physical network medium (e.g., network cabling) and is responsible for placing information on the medium.

Layer 1–Physical

The Physical layer is a set of rules regarding the hardware used to transmit data. It defines the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between communicating network systems. At this layer, the OSI model is concerned with electrical considerations and bits (1s and 0s). Physical layer specifications define characteristics such as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, and physical connectors. The Physical layer establishes whether bits (data) are going to be sent half or full duplex. In half-duplex transmission, the transmission and reception of data must happen alternately. Full-duplex transmission means that communications between components simultaneously transmit and receive. A standard physical medium must exist in order to interconnect Physical layer entities. Hubs, repeaters, NICs, and cables operate at the Physical layer. NICs also operate at the Data Link layer.

Layer 2–Data Link

The Data Link layer provides reliable transit of data across a physical network link. Different Data Link layer specifications define different network and protocol characteristics, including physical addressing, network topology, error detection and correction, frames sequencing, and flow control. Physical addressing of devices (as opposed to network addressing) occurs at the Data Link layer. A network topology consists of the Data Link layer specifications that often define how devices are physically connected, such as in a bus or a ring topology. Error detection occurs through cyclic redundancy checks (CRC), while error correction alerts upper-layer protocols that a transmission error has occurred and requests retransmission of the frame. Frame sequencing corrects transmission of out of sequence frames by reordering the frames on the receiving end of a transmission. Finally, flow control moderates the transmission of data so that the receiving device is not overwhelmed with more traffic than it can handle at one time. NICs and network switches operate at the Data Link layer.

The IEEE has subdivided the Data Link layer into two sublayers: logical link control (LLC) and media access control (MAC).

Logical link control

This sublayer of the Data Link layer manages communications between devices over a single link of a network. The IEEE 802.2 specification defines the LLC sublayer. LLC supports both connectionless and connection-oriented services used by higher-layer protocols. IEEE 802.2 defines a number of fields in Data Link layer frames that allow multiple higher-layer protocols to share a single physical data link.

Media access control

This sublayer of the Data Link layer manages protocol access to the physical network medium. The IEEE MAC specification defines MAC addresses, which enable multiple devices to identify one another uniquely at the Data Link layer. Each system on a network must have a MAC address. NICs and network adapters have MAC addresses.

Layer 3–Network

The Network layer provides routing and routing-related functions that enable the combining of multiple data links on an internetwork. At this layer, packets are created and addressed. Addressing occurs through the logical addressing (as opposed to the physical addressing) of devices. The Network layer supports both connection-oriented and connectionless service from higher-layer protocols. Network-layer protocols typically are routing protocols, but other types of protocols exist at the Network layer as well.

Some common routing protocols include enhanced interior gateway routing protocol (EIGRP), open shortest path first (OSPF), and routing information protocol (RIP). Routers operate at the Network layer.

Layer 4–Transport

The Transport layer implements reliable internetwork data transport services that are transparent to upper layers. Information is broken down from large sections to smaller sections and then sequenced for reconstruction. For incoming information the reverse happens, smaller sequenced sections reform to larger ones. Transport-layer functions typically include flow control, multiplexing, virtual circuit management, error checking, and recovery. Flow control manages data transmission between devices, so that the transmitting device does not send more data than the receiving device can process. Multiplexing enables transmission of data from several applications onto a single physical link. The Transport layer establishes, maintains, and terminates virtual circuits for connection-oriented communication. Error checking involves creating various mechanisms for detecting transmission errors, while error recovery involves taking an action, such as requesting data retransmission to resolve any errors that occur.

Layers 5 through 7 handle application-related issues and generally occur only in software. The highest layer, application, is closest to the end user. Both user and Application layer processes interact with software applications that contain some form of a communications component. These layers deal with the user interface, formatting data, and access to applications.

Layer 5–Session

The Session layer establishes, manages, and terminates communication sessions between local and remote applications. Communication sessions consist of service requests and service responses that occur between applications located in different network devices. Coordination for these requests and responses occurs via protocols implemented at the Session layer. If a session somehow gets unintentionally broken, the Session layer will re-establish the connection. It controls data transfers and handles recovery from a system crash.

Checkpointing is one significant feature for very large data transfers. It involves periodically inserting recovery points into data transfers, so in the event a transfer fails, it can restart from the last recovery point. It saves re-transmitting large quantities of data when connections fail near to the end of a transfer.

Layer 6–Presentation

The Presentation layer provides a variety of coding and conversion functions for Application-layer data. These functions ensure that information sent from the Application layer of one system will be readable by the Application layer of another system. Examples of Presentation layer coding and conversion functions include common data representation formats, conversion of character representation formats, data compression schemes, and data encryption schemes. Common data representation formats, or the use of standard image, sound, and video formats, enable the interchange of application data between different types of computer systems. Conversion schemes exchange information between systems by using different text and data representations, such as extended binary coded decimal interchange code (EBCDIC), used in International Business Machines (IBM) mainframe computers, and American standard code for information interchange (ASCII), used in most modern computer systems. Data compression schemes enable decompression of compressed data once it has reached its destination. Data encryption schemes support the deciphering of encrypted data once data arrives at the destination device.

Presentation-layer implementations are not typically associated with a particular protocol stack. Some well-known standards for video include QuickTime and motion picture experts group (MPEG). QuickTime is an Apple computer specification for video and audio, and MPEG is a standard for video compression and coding. Among the well-known graphic image formats are graphics interchange format (GIF), joint photographic experts group (JPEG), and tagged image file format (TIFF). GIF and JPEG are standards for compressing and coding graphic images. TIFF is a standard coding format for graphics images.

Because it is necessary to ensure there is sufficient bandwidth to deliver services appropriately, compression of network services occurs to both provide acceptable quality, and reduce network load and overhead. Compression occurs by encoding information using fewer bits than the original representation, without degrading the overall quality beyond the point of usefulness or recognition.

A component, referred to as a codec, performs this compression. There are countless numbers of codecs used today, in items ranging from digital television transmissions to voice over Internet protocol (VoIP) implementations.

Common examples of *video* compression standards include the following:

- MPEG–4.
- H.264 (MPEG–4 advanced video coding).
- High efficiency video coding.

Common examples of *voice* compression standards include the following:

- G.711.
- G.722.
- G.726.
- G.729.

Layer 7–Application

The Application layer is the OSI layer closest to the end user, which means that both the OSI Application layer and the user interact directly with the software application. At the Application layer, you will find database management programs, email, file and print-server programs, and the command-and-response language of the OS.

Application-layer functions typically include identifying communication partners, determining resource availability, and synchronizing communication.

When identifying communication partners, the Application layer determines the identity and availability of communication partners for an application. When determining resource availability, the Application layer must decide whether sufficient network resources for the requested communication exist. In synchronizing communication, all communication between applications requires cooperation centrally managed by the Application layer.

Examples of protocols that operate at the Application layer include teletype network (Telnet), file transfer protocol (FTP), simple mail transfer protocol (SMTP), file transfer access and management (FTAM), virtual terminal protocol (VTP) and common management information protocol (CMIP).

Open system interconnection internetwork communication

Information transferred from a software application of one computer system to a software application of another computer, must pass through each of the OSI layers (fig. 3–5).

For example, if a software application in System A has information to transmit to a software application in System B, the application program in System A will pass its information to the Application layer (layer 7) of System A. The Application layer then passes the information to the Presentation layer (layer 6), which relays the data to the Session layer (layer 5), and so on down to the Physical layer (layer 1). At the Physical layer, the system places information onto a physical network medium (e.g., Ethernet cable) and transmits it across the medium to System B. The Physical layer of System B removes the information from the physical medium, and then its Physical layer passes the information up to the Data Link layer (layer 2), which passes it to the Network layer (layer 3), and so on until it reaches the Application layer (layer 7) of System B. Finally, the Application layer of System B passes the information to the recipient application program to complete the communication process.

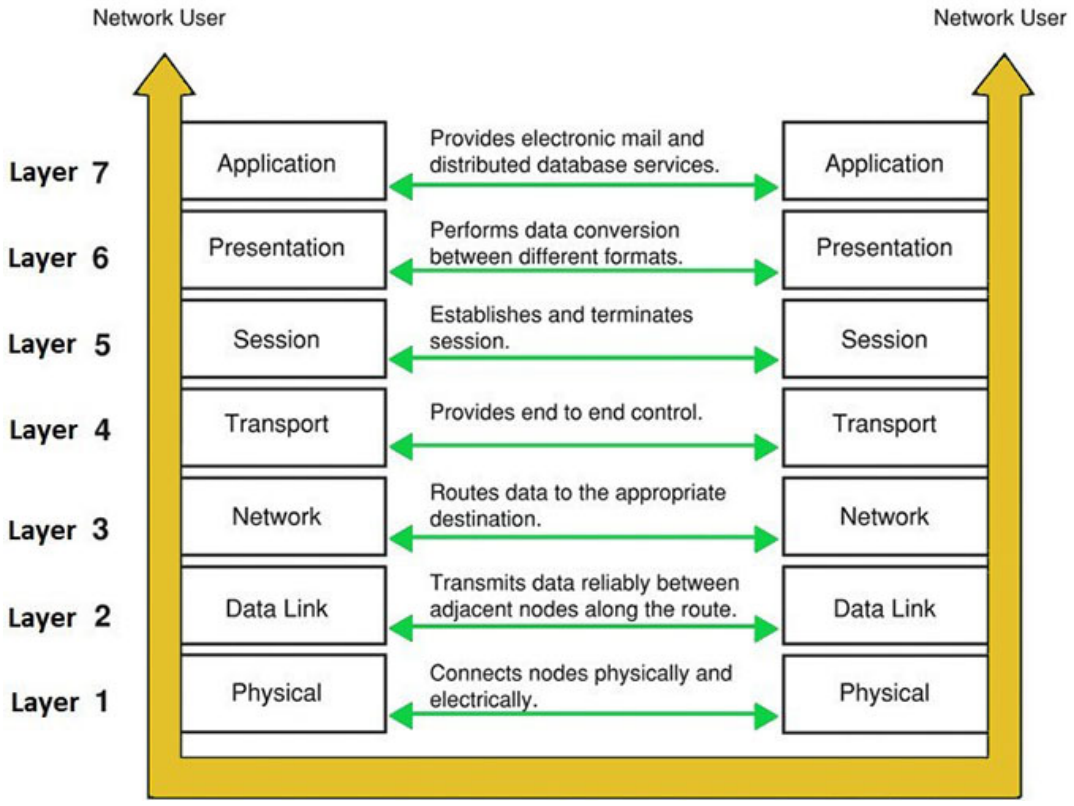


Figure 3–5. OSI internetwork communication.

Information exchange

The seven OSI layers use various forms of control information to communicate with their peer layers in other computer systems. This control information consists of specific requests and instructions exchanged between peer OSI layers.

Control information typically takes one of two forms: headers and trailers. As data passes from the upper layers to the lower layers, the addition of the headers and trailers occurs in a process called *encapsulation* (fig. 3–6).

Headers, trailers, and data are relative concepts depending on the layer that analyzes the information unit. For example, at the Network layer, an information unit consists of a layer 3 header and data. At the Data Link layer, however, all the information passed down by the Network layer (the layer 3 header and the data) is treated as data. In other words, the data portion of an information unit at a given OSI layer can potentially contain headers, trailers, and data from all the higher layers.

The information exchange process occurs between peer OSI layers. Each layer in the source system adds control information to the data, and each layer in the destination system analyzes and removes the control information from that data. The term used to describe this process on the sending side is encapsulation. On the receiving side of the data transmission process, it is decapsulation. If System A has data from a software application to send to System B, it passes the data to the Application layer. The Application layer in System A then communicates any control information required by the Application layer in System B by adding a header to the data stream. The resulting information unit (a header and the data) passes to the Presentation layer, which adds its own header containing control information intended for the Presentation layer in System B.

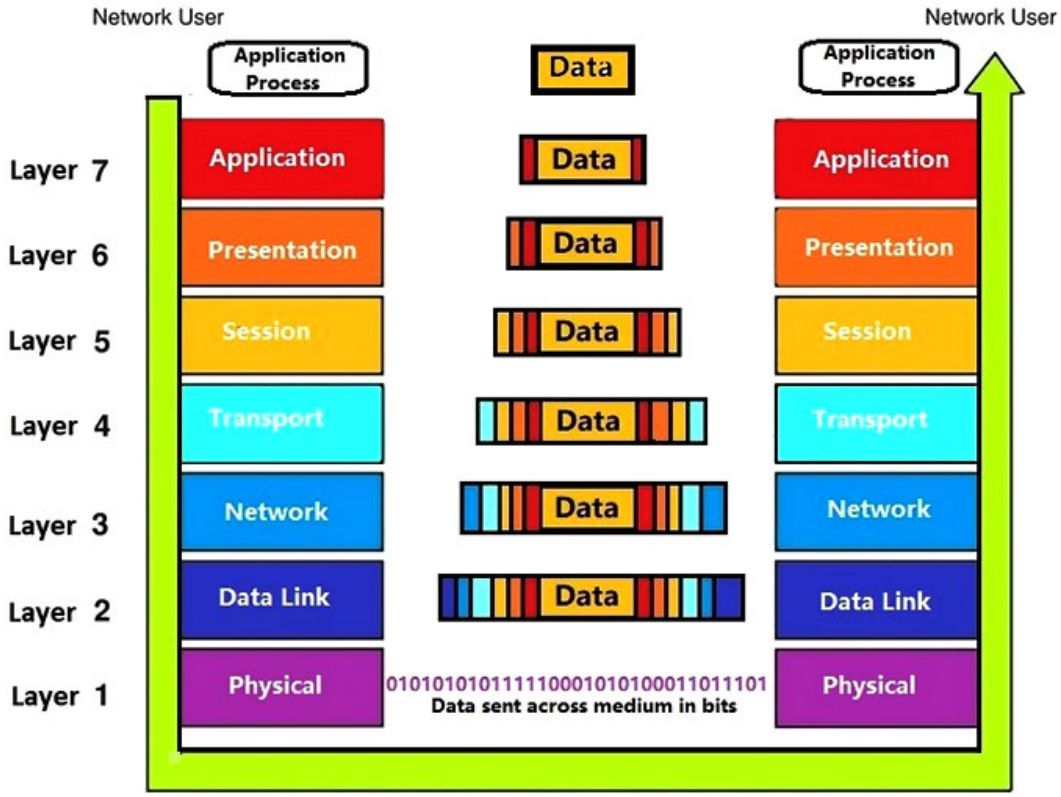


Figure 3–6. OSI data encapsulation and decapsulation.

The information unit grows in size as each layer adds its own header (and in some cases a trailer) that contains control information to be used by its peer layer in System B. At the Physical layer, the system places the entire information unit onto the network medium. The Physical layer in System B receives the information unit and passes it up to the Data Link layer. The Data Link layer in System B then reads the control information in the header added by the Data Link layer in System A. The system then removes the header, and the remainder of the information unit passes to the Network layer.

Each layer performs the same actions. The layer reads the header from its peer layer, strips off the header, and then passes the remaining information unit to the next highest layer. After the Application layer performs these actions, the data passes to the software application in System B, in exactly the same form of original transmission by the application in System A.

Information formats

Protocol data unit (PDU) describes data encapsulated with control information. A different PDU describes the data and control information as encapsulation occurs at different layers of the OSI model. The following are PDUs used in the OSI model: segment, packet, frame, and bit.

PDU	Description
Segment	Source and destination are *Transport* layer entities
Packet	Source and destination are *Network* layer entities. A packet is composed of the Network layer header (and possibly a trailer) and upper layer data. The header and trailer contain control information intended for the Network layer entity in the destination system. The Network layer header and trailer encapsulate data from upper layer entities.

PDU	Description
Frame	Source and destination are *Data Link* layer entities. A frame is composed of the Data Link layer header (and possibly a trailer) and upper layer data. The header and trailer contain control information intended for the Data Link layer entity in the destination system. The Data Link layer header and trailer encapsulate data from upper-layer entities.
Bit	The information is forwarded to the destination in a stream of bits, then de-encapsulated into the respective PDUs, and interpreted by each layer of the destination device.

612. Transmission control protocol/Internet protocol principles

Let us imagine that no traffic laws exist; there are no red lights, stop signs, or roadway signals; and people can drive on any side of the road and as fast as they wish, this probably would not work very well. We need laws or rules to ensure that traffic moves safely and efficiently from one point to another. The same is true for data communications and networks.

The OSI model provides a conceptual framework for communication between computers, but the model itself is not a method of communication. Actual communication occurs by using communication protocols. In the context of data networking, a protocol is a formal set of rules and conventions that governs how computers exchange information over a network medium. Think of it as a language. If two computers do not use the same network protocol, then they cannot communicate. A protocol implements the functions of one or more of the OSI layers.

Transmission control protocol/Internet protocol (TCP/IP) is the standardized network protocol suite the DOD uses and is the basic communication language or protocol stack of the Internet. TCP/IP is a suite of specialized protocols—including TCP, IP, user datagram protocol (UDP), address resolution protocol (ARP), along with many other protocols. Its origins lie with the DOD, which developed TCP/IP for its Advanced Research Projects Agency network (ARPANET)—the precursor to today's Internet—in the late 1960s. TCP/IP is the Internet's accepted standard and has become the protocol choice of LANs and WANs.

The development goals for TCP/IP protocol suite were to allow communication among a variety of independent systems. TCP/IP would not have become so popular if it were not routable. Protocols that can span more than one LAN (or LAN segment) are considered routable because they carry Network layer addressing information used by a router. Not all protocols are routable.

The TCP/IP suite offers a number of features and benefits, which offer interoperability, flexibility, and multi-vendor support. TCP/IP is the most universally available protocol today.

The multiple protocols within the TCP/IP suite provide for a variety of implementations. The choice between TCP, a connection-oriented method of communication that is reliable but slow, and UDP, a fast and efficient yet not as reliable method, is important when determining how a packet travels the network.

TCP/IP, like the OSI model, takes a layered model approach for network communication. While the OSI model has seven layers, TCP/IP only has four. The four layers are as follows:

1. Network Access layer (or Link layer).
2. Internet layer.
3. Transport layer.
4. Application layer.

The easiest way to break down the many protocols of the TCP/IP suite is according to where they operate within each of the models. Each of TCP/IP four layers correlates to one of the seven OSI layers, therefore, each TCP/IP protocol will map to one of the OSI layers. Figure 3–7 shows how each layer of the OSI model maps with TCP/IP.

When comparing TCP/IP protocols to OSI model, the Network Access layer includes the Physical and Data Link layers' functions. The Internet layer maps directly to the OSI Network layer and the Transport layer maps directly to OSI's Transport layer. TCP/IP's Application layer includes OSI's Session, Presentation, and Application layers' functions.

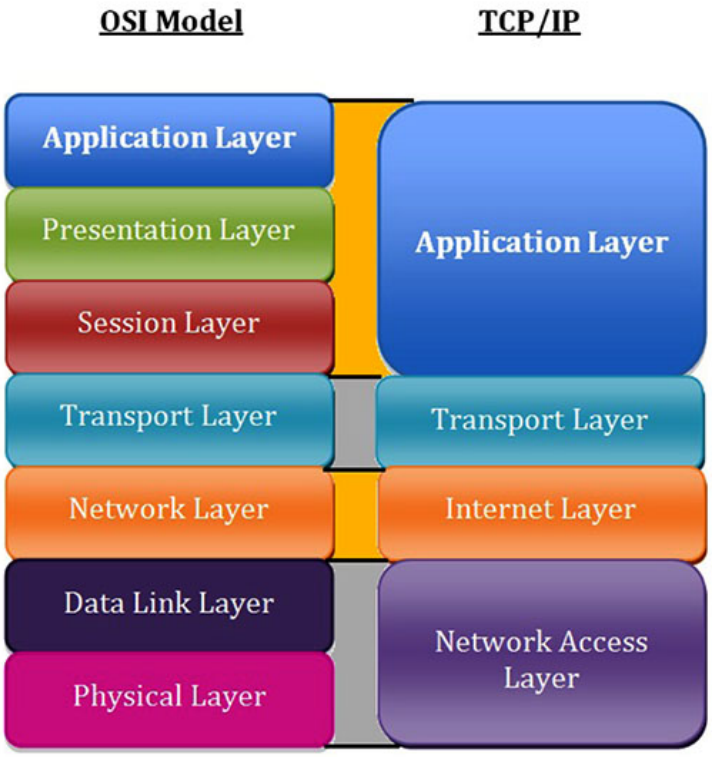


Figure 3–7. OSI relation to TCP/IP.

Before we discuss each layer, it is important to note that transport protocols fall into two categories of classifications based on the way data transports. These transport protocols are connection-oriented and connectionless-oriented.

Term	TCP/IP Protocol	Description
Connection-oriented protocol	TCP	Connection established between the sender and recipient happens prior to transfer of any data. An example is the telephone system. You place a call, a connection is established, and communication occurs. Connection-oriented protocol establishes, maintains, and breaks a connection with the receiving system.
Connectionless-oriented protocol	UDP	Simply sends out data packets to receiving system and does not require receipt acknowledgment.

Application layer

This layer serves as the user's point of access to the network and provides services such as email and file transfer. Within this layer reside protocols that are required to support Network Operating System software. Some examples of these protocols are FTP, Telnet, and SMTP. The following paragraphs provide basic information on some protocols that operate in this layer.

File transfer protocol

Networks use TCP/IP's FTP to send and receive files. In FTP exchanges, a host running a FTP server accepts commands from another host running an FTP client. FTP clients come with a set of simple commands that make up its user interface. In order to exchange data, the client depends on an FTP server that is always waiting for requests. Once a client connects to the FTP server, exchange of FTP data occurs via TCP, which means that FTP provides some assurance of delivery. FTP requires users to log on to the remote host with an ID and password in order to gain access to a directory and transfer files.

Trivial file transfer protocol

Trivial file transfer protocol (TFTP) is a protocol that enables file transfers between computers, but it is simpler (or more trivial) than FTP. A significant difference between FTP and TFTP is that TFTP relies on UDP at the Transport layer. Its use of UDP means that TFTP is *connectionless* and does not guarantee reliable data delivery. In addition, TFTP does not require users to log on to the remote host with an ID and password to gain access to a directory and transfer files. Instead, when you enter the TFTP command, your computer issues a simple request to access the host's files. The remote host responds with an acknowledgment, and then the two computers begin transferring data. Each time a packet of data transmits to the host, the local workstation waits for an acknowledgment from the host before issuing another packet. This is the way TFTP overcomes some of the limitations of relying on a connectionless Transport layer protocol. A final difference between FTP and TFTP is that the latter does not allow directory browsing. In FTP, you can connect to a host and navigate through all of the directories you have authorization to view.

TFTP is useful when you need to load data or programs on a diskless workstation. As you can imagine, however, not requiring a login also presents a security risk, so careful placement and monitoring of TFTP servers on the network must occur.

Simple mail transfer protocol

SMTP has the responsibility of transferring e-mail between computers. It uses the connection-oriented services of TCP for message transmission. It is important to note that although email servers and other mail transfer agents use SMTP to send and receive mail messages, user-level client mail applications typically only use it to for sending messages to a mail server for relaying; they use Internet message access protocol (IMAP) to retrieve messages.

Hypertext transfer protocol

Hypertext transfer protocol (HTTP) is used to access hypertext markup language (HTML) files on the Internet, and allows for clients and servers to exchange data very rapidly. HTTP allows the exchange of only two types of messages: requests from the client and responses from the server. It does not provide any security or memory of transactions that have taken place between the client and server. It can get files or send files, and that is about it.

Another version of HTTP is hypertext transfer protocol secure (HTTPS). The HTTPS implements security features lacking from the original HTTP protocol. This occurs through encryption and security checks.

NOTE: HTML is a scripting language that forms the building blocks of all Web sites. It allows users to use a browser to view documents and applications on the Internet.

Domain name system

Implementation of domain name system (DNS) occurred as a way to manage and centralize domain names on the Internet. It provides the service of matching a host name for a unique domain such as www.af.mil to the IP address of a server where the host is located.

A domain name has at least three levels. The first is the top-level domain, identified by the last characters of the domain name (.com for a commercial organization, .org for a non-profit, .mil for military, etc.). The second level in a domain name is the actual name of the organization (af). The

third level—the www—typically refers to a host, which is usually a server. It is also possible to have additional levels added to distinguish between locations or departments in an organization (i.e., www.airforcemedicine.af.mil).

Telnet

Telnet is a terminal emulation protocol used to log on to remote hosts using the TCP/IP protocol suite. Telnet establishes a TCP connection and keystrokes on the user's machine act like keystrokes on the remotely connected machine. Through Telnet, you can control a remote host over LANs and WANs such as the Internet. For example, technicians can use Telnet to log on to a router from a computer elsewhere on the network and modify the router's configuration.

Telnet is notoriously insecure, meaning that someone with malicious intent could easily falsify the credentials required to log on to a device. Therefore, connecting to a router with Telnet across a public would not be wise. Other more secure methods of remotely connecting to a host have replaced Telnet for this reason.

Dynamic host configuration protocol

Dynamic host configuration protocol (DHCP) is an automated means of assigning a unique IP address to every device on a network. The Internet Engineering Task Force is the responsible body for the development of DHCP. The major advantage of DHCP is that it does not require the network administrator to maintain a table of IP and MAC addresses on the server. However, DHCP does require the network administrator in charge of IP address management to install and configure the DHCP service on a DHCP server.

Reasons for implementing DHCP include the following:

- Make IP addressing transparent for mobile users.
- Reduce the time spent on IP address management.
- Reduce the potential for errors in assigning IP addresses.
- Enable movement of network devices without having to change the TCP/IP configuration.

Simple network management protocol

Simple network management protocol (SNMP) offers the ability to configure, monitor, and manage network resources and devices. As with the other application protocols, implementation of SNMP occurs in software, and all the devices on the network must be able to understand the protocol.

Network time protocol

Network time protocol (NTP) is a protocol used to synchronize the clocks of computers on a network. NTP depends on UDP for Transport layer services. Time is critical in routing to determine the most efficient path for data over a network. Time synchronization across a network is also important for time-stamped security methods and maintaining accuracy and consistency between multiple storage systems. NTP is a protocol that benefits from UDP's quick, connectionless nature at the Transport layer. NTP is time-sensitive and cannot wait for the error checking that TCP would require.

Transport layer

This is the layer where TCP and UDP reside. TCP is responsible for establishing and monitoring the network connection between end-systems to provide reliable delivery of data. TCP ensures data is delivered error free, in sequence with no loss or duplication of data. TCP separates data into packets, tagged with the remote end systems IP address, and handed down to the Internet layer. TCP is also responsible for the reassembly of the data at the destination. TCP is a connection-oriented protocol because it establishes and monitors the entire end-to-end connection. UDP is the format used as the connectionless transport protocol in the TCP/IP stack. Let us look at TCP and UDP.

Transmission control protocol

TCP provides reliable full-duplex data transmission. In a connection-oriented environment, a connection establishes between both ends before transfer of information can begin. TCP is responsible for breaking messages into segments, reassembling them at the destination station, resending anything not received, and reassembling the message from the segments. TCP supplies a virtual circuit between end-user applications.

The following protocols use TCP:

- FTP.
- HTTP.
- SMTP.
- DNS.

TCP works by providing transport support from the source host to the destination host. It constitutes a logical connection between the endpoints of the network. Transport services segment and reassemble data sent by several upper-layer applications onto the same transport services. The Transport layer data is a logical connection between the endpoints of a network. The Transport layer defines end-to-end connectivity between host applications.

The Transport layer provides the following basic services:

- Segment upper-layer application data.
- Establish end-to-end operations.
- Send segments from one end host to another end host.
- Ensure flow control by providing sliding windows.
- Ensure reliability provided by sequence numbers and acknowledgements.

Since TCP is connection-oriented, it requires connection establishment before data transfer begins. To do this TCP uses a three-way handshake (an asynchronous connection mechanism), which is necessary because the mechanisms of a three-way handshake are not tied to a global clock. The handshake contains three steps:

1. The requestor sends a packet specifying the port number it plans to use and its initial sequence number (ISN) to the server.
2. The server acknowledges with its ISN, which consists of the requestor's ISN, plus (+) 1.
3. The requestor acknowledges the acknowledgement with the server's ISN, plus (+) 1.

In the most basic form of reliable, connection-oriented data, transfer and receipt of data packets must occur in the same order of transmission. Let us take look at some mechanisms of TCP that ensure reliable delivery of data.

Stream data transfer

TCP transfers a continuous stream of bytes through the Internet. TCP does this by grouping bytes in TCP segments and then delivering to IP for transmission to the destination. TCP decides how to segment the data and it may forward the data at its own convenience. To ensure that all data are sent, a push function delivers all remaining data in storage to the destination. A push also occurs at the close of the connection.

Reliability

Reliable delivery guarantees that a stream of data sent from one machine is delivered through a data link to another machine without duplication or data loss. Positive acknowledgement with retransmission is one technique that guarantees reliable delivery of data. Positive acknowledgement requires a recipient to communicate with the source by sending back an acknowledgement message when it receives data. The sender keeps a record of each data packet (TCP segment) that it sends and

expects an acknowledgement. The sender also starts a timer when it sends a segment and retransmits a segment if the timer expires before an acknowledgement arrives.

TCP further ensures reliable data delivery through sequencing and checksums. Without such measures, transmission of data would occur indiscriminately without checking to see if the destination node was offline, or if data became corrupt during transmission. Figure 3–8 illustrates a TCP segment and the table following it describes each field of a TCP segment.

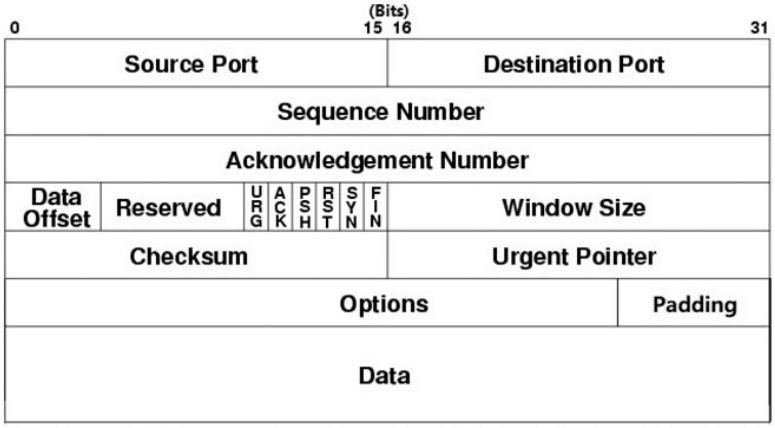


Figure 3–8. TCP segment.

Field name	Description
Source Port	Indicates the port number at the source node. A *port* is the address on a host where an application makes itself available to incoming or outgoing data. One example of a port is port 80. Port 80 accepts Web page requests from HTTP protocol. The Source Port field is 16 bits long.
Destination Port	Indicates the port number at the destination node. The destination port field is 16 bits long.
Sequence Number	Identifies the data segment's position in the stream of data segments already sent. The sequence number field is 32 bits long.
Acknowledgement	Confirms receipt of the data via a return message to the sender. The acknowledgment number field is 32 bits long.
Data Offset	Indicates the length of the TCP header. This field is 4 bits long.
Reserved	A 6-bit field reserved for later use.
Flags	A collection of six 1-bit fields that signal special conditions through flags. The following flags are available for the sender's use: • **URG**—If set to "1," the Urgent Pointer field contains information for the receiver. • **ACK**—If set to "1," the Acknowledgment field contains information for the receiver. (If set to "0," the receiver will ignore the Acknowledgment field.) • **PSH**—If set to "1," it indicates that data should be sent to an application without buffering. • **RST**—If set to "1," the sender is requesting to reset the connection. • **SYN**—If set to "1," the sender is requesting a synchronization of the sequence numbers between the two nodes. Used when TCP requests a connection to set the initial sequence number. • **FIN**—If set to "1," the segment is the last in a sequence and should therefore be closed.

Field name	Description
Sliding-Window Size (or window)	Indicates how many bytes the sender can issue to a receiver while acknowledgment for this segment is outstanding. This field performs flow control, preventing overrunning the receiver with bytes. For example, suppose a server indicates a sliding window size of 4,000 bytes. Also, suppose the client has already issued 1,000 bytes, of which the server has received and acknowledged 250 bytes. That means that the server is still buffering 750 bytes. Therefore, the client can only issue 3,250 additional bytes before it receives acknowledgment from the server for the 750 bytes. This field is 16 bits long.
Checksum	Allows the receiving node to determine if the corruption of the TCP segment occurred during transmission. The Checksum field is 16 bits long.
Urgent Pointer	Can indicate a location in the data field where urgent data resides. This field is 16 bits long.
Options	Used to specify special options, such as the maximum segment size a network can handle. The size of this field can vary between 0 and 32 bits.
Padding	Contains filler information to ensure that the size of the TCP header is a multiple of 32 bits. The size of this field varies; it is often 0.
Data	Contains data originally sent by the source node. The size of the Data field depends on the amount of data requiring transmission, the constraints on the TCP segment size imposed by the network type and the limitation that the segment must fit within an IP datagram.

Flow control

TCP uses flow control methods to prevent network congestion by ensuring that transmitting devices do not overwhelm receiving devices with data. There are three commonly used methods for handling network congestions as shown in the table below:

Network congestion handling method	Description
Buffering	Network devices temporarily store burst of excess data in memory until the receiving device utilizes it. Excess data bursts can exhaust memory, forcing the device to discard any additional datagrams that arrive.
Source-quench messages	The receiving unit sends messages to sending units to prevent buffer overflow. The receiving device sends source-quench messages to request that the source reduce its current rate of data transmission.
Windowing	Windowing requires the source device to receive an acknowledgement from the destination device after it transmits a certain amount of data.

To govern the flow of data between devices, the receiving TCP device reports a window to the sending TCP device. This window specifies the number of octets, starting with the acknowledgment number, that the receiving TCP device currently is capable of receiving. For example, with a window size of three, the source device can send three octets to the destination. It must then wait for an acknowledgment. If the destination receives the three octets, it sends an acknowledgement to the source device, which now can transmit three more octets. If the destination does not receive the three octets because of overflowing buffers, it does not send an acknowledgement. Because the source does not receive an acknowledgement, it knows that the octets need retransmission and to lower the transmission rate.

Ports

Protocol port numbers reference the location of a particular application or process on each device (in the Application layer). Just as an IP address identifies the address of a host on the network, the port

address identifies the application to the Transport layer, thus providing a complete connection. Think of it as several people living in one house. The IP address correlates to street address and the port number correlates to the person's name. This way, when a letter arrives, the right person opens it.

As previously discussed, certain higher-level programs (such as Telnet and FTP) are protocols and use the same port number in all TCP/IP implementations. The Internet Assigned Numbers Authority (IANA) controls and assigns these port numbers or well-known ports. Most systems can be used only by system processes or by programs executed by privileged users. IANA does not control registered ports. The following table provides a breakdown of port ranges commonly used today. Dynamic and/or private ports are not used by any one specific application.

Common Port Ranges	
Range	**Type**
0 - 1023	Well-known ports
1024 - 49151	Registered ports
49152 - 65535	Dynamic and/or private ports

The following table shows frequently used well-known ports that are important for you to know.

Common Well-Known Ports		
Port	**Transport Protocol**	**Service**
7	TCP	Echo
20	TCP	FTP (data transfer)
21	TCP	FTP (control - command)
22	CP	Secure Shell
23	TCP	Telnet
25	TCP	SMTP
53	TCP/UDP	DNS
69	UDP	TFTP
80	TCP	HTTP
110	TCP	POP3
123	UDP	NTP
143	TCP	IMAP4
161	TCP/UDP	SNMP
443	TCP	HTTPS

Sockets

A socket is a combination of a port number and IP address used by a process to request network services and passes as an argument between layers. An example in TCP would be 186.52.124.58: 21 (IP address, port number).

Sliding windows

A sliding window regulates how much information passes over a TCP connection before the receiving host must send an acknowledgement. Each computer has both a send and a receive window that it utilizes to buffer data and make the communication process more efficient. A sliding window allows the sending computer to transmit data in a stream without having to wait for each packet acknowledgement. This allows the receiving machine to receive packets out of order and reorganize them while it waits for more packets. The sending window keeps track of data sent, and if no acknowledgement received within a given amount of time, the packets are re-sent.

User datagram protocol

UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery. Speed is the primary importance. UDP is best for sending small amounts of data for which guaranteed delivery is not required and minor packet loss is acceptable, such as with Internet phone, real-time video conferencing, streaming audio and video, and online games. While UDP uses ports, they are different from TCP ports; therefore, they can use the same numbers without interference.

This simplicity is evident when comparing the UDP segment format with TCP. Error processing and retransmission requires handling by upper-layer protocols. For example, if a FTP download interruption occurs for some reason, the human operator can just retry until it successfully delivers.

The following list defines the fields in the UDP segment:

- Source Port—Number of the calling port.
- Destination Port—Number of the calling port.
- Length—Number of bytes, including header and data.
- Checksum—Calculated checksum of the header and data fields.
- Data—Upper layer protocol data.

UDP does not use windowing or acknowledgements. Therefore, the Application layer protocols provide reliability. UDP is for applications that do not need to put sequences of segments together.

The following protocols use UDP:

- TFTP.
- SNMP.
- DHCP.
- DNS.

Internet layer

The Internet layer is responsible for the logical addressing of devices on the network, as well as routing data between a source and destination. The Internet layer is where the IP resides. IP is responsible for getting data from one end system to another end system by any means possible. IP handles moving the data one node at a time. The Internet layer accepts a packet from the Transport layer along with an identification of the packet's destination. It adds to the packet an IP header, which uses a routing algorithm to determine how to direct the packet to the next node in the route. IP is a connectionless-protocol because it transmits every packet of information individually, regardless of the end-to-end connection. The following protocols function at the Internet layer:

- IP.
- ARP.
- Internet control message protocol (ICMP).

Internet protocol

IP provides information about how and where to deliver data, including the data's source and destination address. IP is the protocol that enables TCP/IP to internetwork—that is, to traverse more than one LAN segment and more than one type of network through a router. IP is a routed protocol.

The Network layer of the OSI model is where the formation of data into packets occurs. In the context of TCP/IP, a packet, also known as an IP datagram, acts as an envelope for data and contains information necessary for routers to transfer data between different LAN segments. IP is an unreliable, connectionless protocol, which means that it does not guarantee delivery of data. Higher-level protocols of the TCP/IP suite, however, use IP to ensure delivery of data packets to the right address. Note that the IP datagram does contain one reliability component, the Header checksum, which verifies only the integrity of the routing information in the IP header. If the checksum accompanying the message does not have the proper value upon receipt of the packet, the packet is

presumed to be corrupt. The packet is disregarded and is resent. Figure 3–9 illustrates an IP datagram structure and the following table describes the structure of an IP datagram (packet).

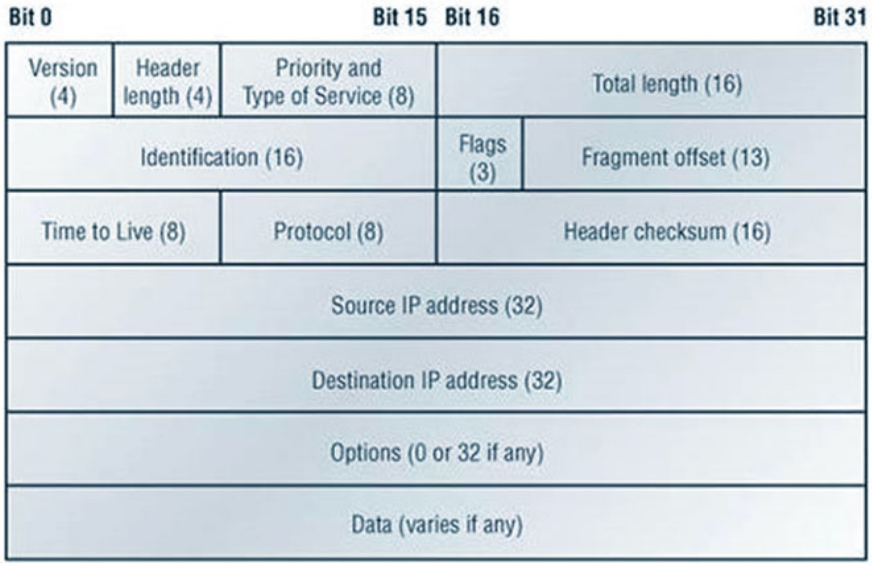


Figure 3–9. IP datagram structure.
(Graphic by BenJerry137 at Wikimedia Commons, Licensed by CC BY SA 3.0.)

Field	Description
Version (4 bits)	Version field is set to the value 4 or 6 in decimal or 0100 or 0110 in binary. The value indicates the version of IP (IPv4 or IPv6).
Header Length (4 bits)	Describes how big the header is in 32-bit words. The minimum value is 5. That is the minimum size of an IP header that contains all the correct fields. This allows the receiver to know exactly where the payload data begins.
Priority and Type of Service	Informs routers what level of precedence should apply when processing an incoming packet.
Total Length (16 bits)	Informs the receiver where the end of the data in this packet is. This is the length of the entire datagram in octets, including header. An IP datagram can be up to 65,535 bytes long, that is the maximum value of a 16-bit field.
Identification (16 bits)	Identifies the message to which a datagram belongs and enables the receiving node to reassemble fragmented messages. This field and the Flags and Fragment offset fields assist in reassembling fragmented packets.
Flags (3 bits)	Indicates if a message is fragmented and, if fragmented, whether the datagram is the last fragment.
Fragment Offset (13 bits)	Numbers the fragment in such a way to enable reassembly, if necessary.
Time to Live (8 bits)	Determines how long a datagram will exist. At each hop along a network path, the datagram is opened and it is time to live field is decremented by one (or more than one in some cases). When the time to live field reaches zero, the datagram is “expired” and discarded. This prevents congestion on the network.
Protocol (8 bits)	Indicates what type of protocol encapsulates within the IP datagram. Some of the common values in this field include ICMP (1), TCP (6) and UDP (17).

Field	Description
Header Checksum (16 bits)	Allows router to detect datagrams with corrupted headers and discard them. When a datagram arrives at a router, the router calculates the checksum of the header and compares it to the checksum field. If they do no match, the router discards the datagram. Since the time to live field changes at each hop, the checksum must re-calculate at each hop.
Source Address (32 bits)	IP address of the sender of the packet.
Destination Address (32 bits)	IP address of the intended receiver of the packet.
Options and Padding (variable length)	Various options can be included in the header by a particular vendor's implementation of IP. If options are included, the header requires padding with zeroes to fill in any unused octets so that the header is a multiple of 32 bits, and matches the count of bytes in the header length field.

Address resolution protocol

While an IP address is necessary to route data between networks in the TCP/IP environment, the physical address, called the MAC address in an Ethernet network, is also necessary to provide intercommunication between devices. It is not always possible for a source device to know the physical address of the destination device.

ARP provides the service of matching a known IP address for a destination device to a MAC address. ARP sends a MAC broadcast request to the entire destination network, asking for the MAC address of a particular known destination IP. The device identified by the IP address in the packet responds to the request, and replies by sending its MAC address. Thus, the source device is capable of correctly addressing communication packets without having to broadcast all messages and slow down the network.

A MAC broadcast is a broadcast packet sent on the network with the MAC address of FF-FF-FF-FF-FF-FF. It requires all devices to pass the packet to the Network layer for address identification.

Internet control message protocol

ICMP is a valuable protocol for assessing the network. ICMP provides error and control messaging that can help with troubleshooting. ICMP messages are included in the IP datagram. The most common error and control messages sent include:

- Destination unreachable.
- Time exceeded.
- Redirect.
- Echo.
- Echo reply.
- Information request.
- Information reply.
- Address mask request.

Packet internetwork groper (ping) is a network administration utility that operates by sending ICMP packets. Ping can verify that TCP/IP is installed, bound to the NIC, configured correctly, and communicating with the network. The use of ping often occurs simply to determine whether a host is responding (or "up").

Ping uses ICMP services to send *echo request* and *echo reply* messages that determine the validity of an IP address. These two types of messages work in much the same way that sonar operates, which is how the program earned its name. First, the computer transmits a signal called an echo request to another computer/device. The other computer/device then rebroadcasts the signal, in the form of an echo reply, to the sender. The process of sending this signal back and forth is pinging.

You can ping either an IP address or a host name. For example, to determine whether the www.af.mil site is responding, you could type: ping www.af.mil and press ENTER. Alternately, you could type: ping xxx.xxx.xxx.xxx (the IP address of the site or device you want to reach) and press ENTER. If the site/device is operating correctly, you receive a response that includes multiple replies from that host.

This is an important tool for troubleshooting medical devices having network connectivity issues. If the site/device is not operating correctly, you will receive a response indicating that the request timed out or that the host was unreachable. You could also get a "request timed out" message on a workstation not properly connected to the network or if the network is malfunctioning. Figure 3–10 shows a successful ping from one user computer to another using the IP address.

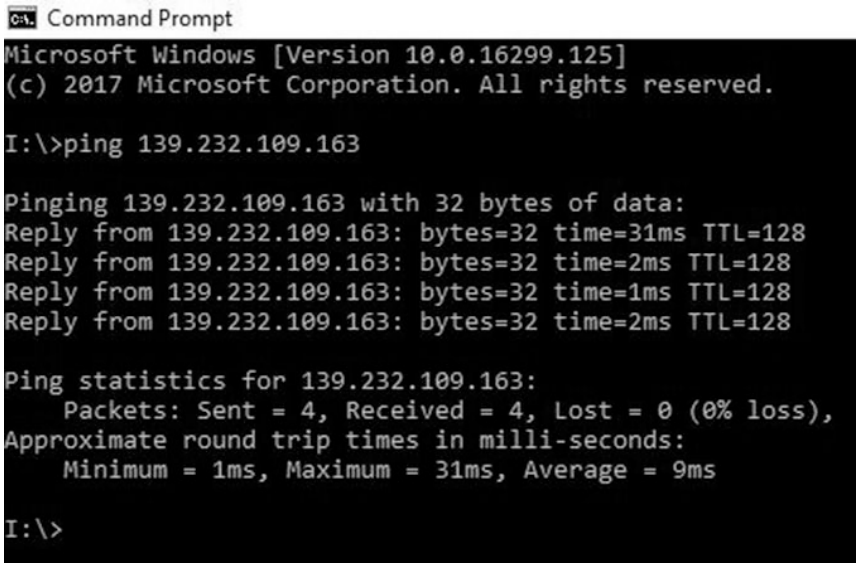


Figure 3–10. Ping to IP address.

By pinging the loopback address (127.0.0.1), you can determine whether your workstation's TCP/IP services are running. By pinging a host on another subnet, you can determine whether the problem lies with a connectivity device between the two subnets.

As with other TCP/IP commands, implementation of the ping utility occurs with a number of different options, or switches. The syntax of the command may vary depending on the operating system. However, the ping command will always begin with the word "ping" followed by a space then a hyphen (-) and a switch, followed by a variable pertaining to that switch. If you type in "ping -?" it will display the help text for the ping command, including its syntax and a full list of switches. Figure 3–11 shows the "ping -?" command and the options available.

Network Access layer

The TCP/IP Network Access layer covers the Data Link and Physical layers of the OSI model and defines the access method for the network media and architecture. It also defines how devices interface with the Physical layer of the network. It does not have strict definitions as far as a specific type of network to be used. The purpose of this layer is to allow higher layers to gain connectivity to the transmission media, and in turn, other networks. The two categories for protocols operating at this layer are LAN protocols and WAN protocols.

Examples of LAN protocols at this layer include Ethernet, Token Ring, and fiber distributed data interface (FDDI). Ethernet is by far the most common. WANs use diverse networking equipment and

technology that differs from LANs. WAN protocols address exchanging information across wide geographic areas, which is out of the scope of any system administration or BMET task.

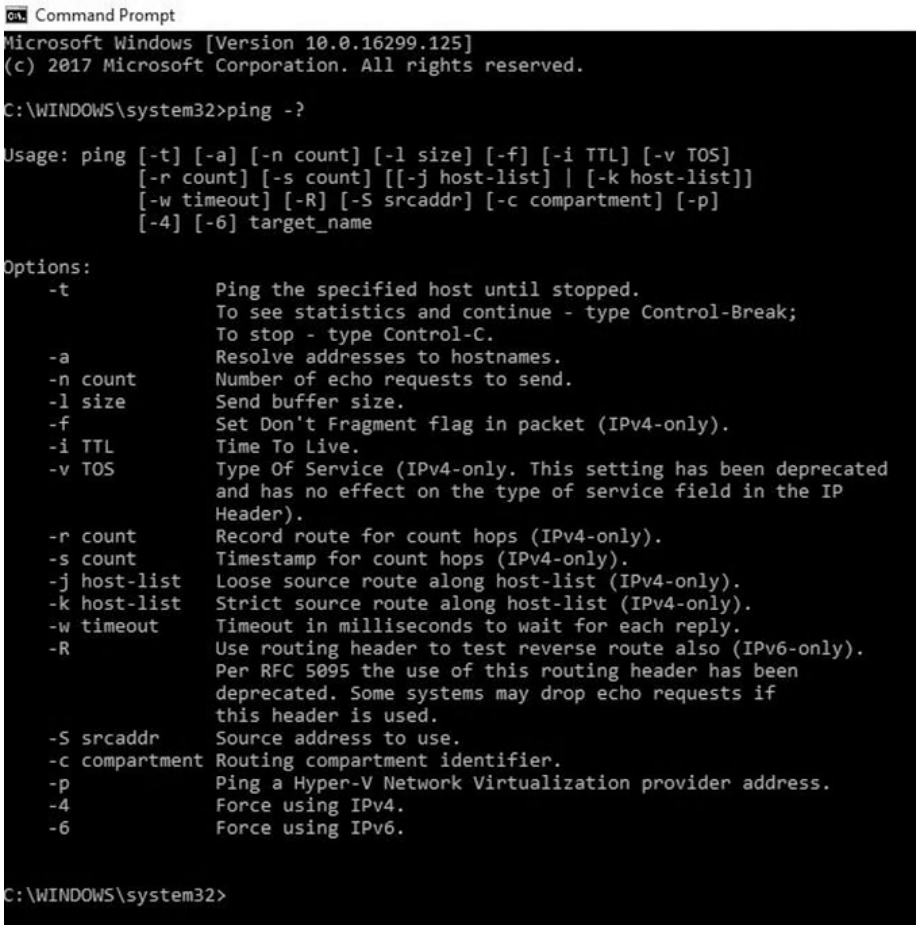


Figure 3–11. Ping help options screen.

Ethernet

Ethernet protocol is known as the IEEE 802.3 standard. The IEEE 802.3 standard describes Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) as their scheme for accessing the network.

When the IEEE 802 committees began their deliberations, they faced a de facto standard, Xerox's Ethernet LAN. By 1980, Intel and Digital Equipment Corporation had joined Xerox in indicating that all their products would be Ethernet-compatible. Rather than requiring that all LANs follow the Ethernet standard, a subcommittee provided 802.3 as an acceptable Ethernet-like standard. The IEEE 802 subcommittees developed standards based on the first three layers of the OSI model. They developed the Data Link layer into two sub-layers: a LLC sublayer and a MAC sublayer. The MAC sublayer is concerned with detecting data collisions.

In addition to specifying the type of data frames that can be packed in a packet and the type of cable that can be used to send this information, the standard also specified the maximum length of a single cable and the ways repeaters can be used to regenerate the signal throughout the network.

The IEEE 802.3 subcommittee specified the way that a LAN using the bus topology constructs its frames of information and sends them over the network to avoid collisions (CSMA/CD). To understand CSMA/CD, visualize a network user who wishes to send a message. The Physical layer of the user's workstation generates a carrier-sense signal and then listens to detect a carrier-sense signal

from another user who is about to send a message. If no other signal is detected, the user sends their message.

The IEEE 802.3 standard continues to evolve very quickly. Changes are mostly backward compatible, so older iterations of technology and cables continue to work with the new, improved standards. Modern developments have increased Ethernet speeds up to and beyond 1,000 megabits per second (or 1 gigabits per second) while retaining compatibility with the CSMA/CD standard. IEEE ratified the use of Gigabit Ethernet (1000 Base – 1000 megabits per second) in 1999 and gradually supplanted Fast Ethernet (100 Base – 100 megabits per second) in wired networks. Over the years, many changes occurred to the 802.3 standard; below we will take a closer look at the specific Gigabit Ethernet standards:

- IEEE 802.3ab (1000BASE-T)–1,000 megabits per second operation over category 5 balanced copper cabling.
- IEEE 802.3z (1000BASE-X)–1,000 megabits per second operation over fiber optic cables.
    - 1000BASE-SX–Gigabit Ethernet over multimode fiber-optic cabling. You can remember this by the S, meaning “short distance.” Multimode fiber cabling is the type of cabling that used over distances less than two kilometers.
    - 1000BASE-LX–Gigabit Ethernet over single mode fiber-optic cabling. You can remember this by the L, meaning “long distance.” Single mode fiber is the type of fiber used to cover distances greater than two km.
    - 1000BASE-CX–Gigabit Ethernet over coaxial cable supporting distances up to 25 meters.

Self-Test Questions

After you complete these questions, you may check your answers at the end of the unit.

610. Principles of networks types

1. Define the Internet.

2. What is a LAN?

3. What are the major benefits of using a WLAN?

4. What type of network connects networks separated by large geographical distances?

5. How do WANs provide wireless connectivity (WWANs)? Provide an example.

6. What are two main drivers for using VPNs?

611. Open system interconnection reference model principles

1. What information does the OSI model provide?

2. What are some characteristics defined in the Physical layer?

3. Explain the difference between half-duplex and full-duplex transmission.

4. Name at least three devices that operate at the Physical layer.

5. Briefly explain the two IEEE Data Link sublayers.

6. In which layer are packets created and addressed?

7. What are the six typical functions of the Transport layer?

8. What functions does the Sessions layer perform?

9. How does the Presentation layer ensure information sent from one Application layer of one system can be read by another?

10. Why do network services get compressed?

11. List at least five protocols that operate at the Applications layer.

12. What is included in control information during OSI information exchange? How is it formed?

13. Briefly explain encapsulation and decapsulation.

14. What is a segment PDU?

612. Transmission control protocol/Internet protocol principles

1. What is the relationship between OSI and TCP/IP?

2. Describe how the TCP/IP layers correlate with the OSI layers.

3. Explain how connection-oriented protocol differs from connectionless-oriented protocol.

4. What does FTP require before use of service?

5. What type of transport protocol does TFTP use? What concerns are associated with its transport protocol?

6. What is the responsibility of SMTP? How does it interact with user-level client mail applications?

7. What is used to access HTML files?

8. What service does DNS provide?

9. List the four reasons for implementing DHCP.

10. Explain why UDP works well for NTP? Would TCP work?

11. What are some responsibilities of TCP?

12. How does TCP establish connection before data transfer?

13. How does TCP transfer a continuous stream of bytes through the Internet?

14. What does the sequence number reveal?

15. What is the purpose of checksum?

16. What are the three flow control methods TCP uses?

17. What do port numbers identify?

18. Match the port in column B with the service in column A.

Column A	*Column B*
____(1) IMAP4	a. 80
____(2) DNS	b. 110
____(3) HTTP	c. 143
____(4) POP3	d. 53

19. What types of applications are UDP best suited for using?

20. What is the responsibility of IP?

21. What information does IP provide?

22. What does the flag field of an IP datagram indicate?

23. Explain the concept of time-to-live.

24. How does ARP match known IP addresses for a destination device to a MAC address?

25. Explain how pinging works.

26. What is the difference in pinging the loopback address and a host on another subnet?

27. What does Ethernet use to help avoid collisions in the network?

3–2. Network Addressing

All networking components must have a unique way of identifying themselves on a network; otherwise, the data traveling on the network would not find its correct destination. In the beginning, legacy networks were small and only required administrators to connect devices physically on the same network. In this setting, a single physical network address design was easily manageable and served most organizations well. However, as the popularity of using networks to share information increased and the need to interconnect the networks grew, it became essential for address design techniques to evolve. This need drove the development and introduction of IP addressing.

613. Addressing fundamentals

This lesson presents principles associated with network addressing fundamentals. These principles include MAC addressing and IP version 4 (IPv4) addressing.

Media access control address fundamentals

The MAC is the physical (hardware) address of a device provided by the NIC in a computer. The MAC is a *unique* 48-bit, 6-byte (octet), hexadecimal address and has two equal parts. The first three bytes (octets), or 24-bits (in transmission order), include an organizationally unique identifier. The organizationally unique identifier identifies the manufacturer, vendor, or organization that issued the NIC. The second 3 bytes, or 24-bits (in transmission order), includes the specific address of the NIC itself. A MAC address might look something like this example: 00-04-76-33-72-F1. For you to find your MAC address and other network related information, go to the command prompt on your computer and enter the command “ipconfig /all”. Figure 3–12 shows the MAC address provided, highlighted in yellow.

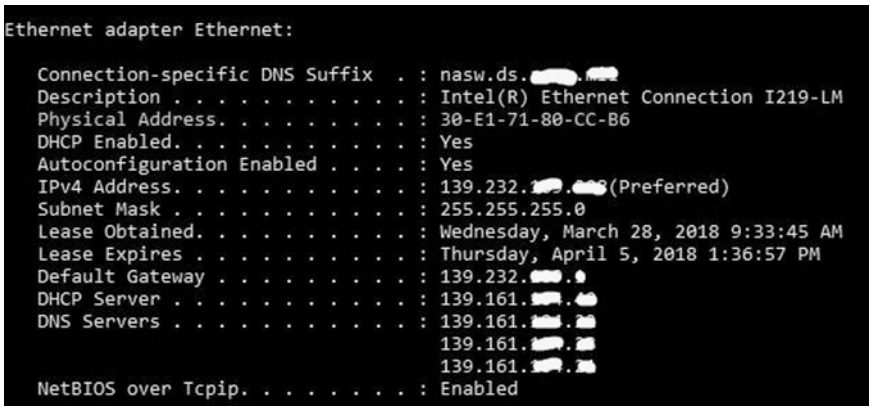


Figure 3–12. MAC address.

The MAC address scheme was sufficient when all network devices physically connected to the same network. However, as network growth occurred and the requirement to route information to/from different networks increased, the sole use of MAC addressing became insufficient. The introduction of a logical addressing design, commonly known as IP addressing, helped solve this problem.

Internet protocol version 4

The IPv4 addressing method is widely used throughout the entire Internet community. Its popularity is due to the wide acceptance and use of the TCP/IP protocol suite. This addressing occurs at the Network layer of the OSI model. An IP address identifies both the individual node and the network to which the node attaches and each device gets a unique IP address. IP addresses group together computers into logical networks so that one LAN can be distinguished from another, allowing communication between LANs connected into a WAN without broadcasting MAC addresses.

An IPv4 address consists of four bytes or octets, when referring to IPv4 addresses. Each octet consists of eight binary bits, totaling 32 bits per address. The IP address is shown in dotted decimal notation with each octet separated by a period (e.g., 187.115.202.12).

Each IP address has specific components and follows the same format. To differentiate LANs from one another, each computer on the same LAN share a similar IP address. Each TCP/IP network has a 32-bit logical address assigned that divides into two main parts: the network number (similar portion) and the host number (unique portion).

Network number

The network number identifies a specific network and requires assignment by IANA if the network is to be part of the Internet. Network numbers are obtainable from authorized representatives of IANA, Internet service providers (ISP) that have obtained blocks of numbers from one of the authorized representatives of IANA.

Host number

The host number identifies a specific host (or any node) on a network and assigned by the local network administrator.

Dotted decimal notation

Dotted decimal notation (DDN) is a representation of a binary IP address in a more user-friendly manner. The notation uses the combination value of each bit that is turned on (represented by a 1) in each byte or octet and adds them together. This occurs for each octet individually; octet values never add together.

The 32-bit binary address of 1101 0001 0001 1111 0100 1011 0010 0011 is represented as 209.31.75.35. This DDN representation is easier to write and remember than binary representation. The *minimum* value for any given octet is zero (represented by 0000 0000) and the *maximum* value for any given octet is 255 (represented by 1111 1111). The following table displays binary and DDN of an IP address.

Binary	1101 0001	0001 1111	0100 1011	0010 0011
Decimal	209	31	75	35
DDN	209.31.75.35			

Classes

There are five classes of IP addresses: Class A, B, C, D, and E. Class D and E are reserved for broadcast and experimental networks.

The IANA manages the network allocations for classes A through C. IANA generally allocates super-blocks to Regional Internet Registries, who in turn allocate smaller blocks to ISPs and enterprises.

By looking at the first octet of an IP address in either its decimal or its binary form, you can easily identify the "class" of the address. In the decimal version, the number of the first octet tells you immediately the class of the address. In the binary version, the first bit or bits in the first octet—the high-order bits—tells you the address class.

Class A address

Class A addresses are used for large networks. The first bit (**0**) identifies the address class and, together with the next seven bits, identifies the network number. The last 24 bits identify the node number. There are 126 class A networks (addresses 1–126), with 16,777,214 hosts on each network.

Class B address

Class B addresses are used for intermediate sized networks. The first two bits (**10**) identify the address class and together with the next fourteen bits, identify the network number. The last sixteen bits identify the node number. There are about 16,384 class B networks (addresses 128–191), with 65,534 hosts on each network.

Class C address

Class C addresses are used for networks with about 250 nodes. The first three bits (**110**) identify the address class and, together with the next twenty-one bits, identify the network number. The last eight bits identify the node number. There are about 2,097,152 class C networks (addresses 192–223), with 254 hosts on each network.

Class D address

Class D addresses are reserved for *multicast* addressing. The first four bits (**1110**) identify the address class and, together with the rest of the address, identify the network number.

Class E address

Class E addresses are reserved for research and development. The first four bits (**1111**) identify the address class and, together with the rest of the address, identify the network number.

The first few bits in the string of binary digits that comprise the address identify the class of an IP address. For this lesson, we will only be looking at classes A, B, and C.

Each class uses a different quantity of octets to identify the network portion of the address.

32 Bit IP Address		
Class	**Quantity of Network Octets**	**Quantity of Node Octets**
A	1	3
B	2	2
C	3	1

The following table shows the five network classes and the corresponding decimal values of an IP address' first octet.

Address Class	*	**Class A**	*	**Class B**	**Class C**	**Class D**	**Class E**	*
First Octet	0	1 - 126	127	128 - 191	192 - 223	224 - 239	240 – 254	255
*Commonly, the octets 0, 127, and 255 are not included as part of the class structure as they are for special use.								

Reserved Internet protocol addresses

In addition to the addresses assigned for use by each node in the network, there are some addresses serving special purposes, denoting networks or sets of computer nodes. Hosts never receive these addresses. The following table displays a few basic reserved IP addresses used in IPv4.

Network Field	Host Field	Type of Address	Purpose	Example
All 0s	All 0s	This computer	Used during bootstrap	0.0.0.0
127	Any	Loop back	Testing	127.0.0.1
255	255	Limited broadcast	Broadcast on local network	255.255.255.255
Network address	All 0s	Network	Identifies network	203.82.104.0
Network address	All 1s	Directed broadcast	Broadcast on a specified network	207.55.157.255

Internet protocol version 4 subnet masking

Subnet masking is a mechanism that allows a network device to divide an IP address into a network and host number. When a network device wants to send an IP packet, it must make a decision. If the destination IP address is on its own network, the IP packet simply transmits onto the same network. If the destination IP address belongs on a different network, the IP packet routes to another network. The subnet mask allows the network device to make this decision.

In a subnet mask, bits represented by ones (1) identify the network address and bits represented by zeroes (0) identify host addresses. There are two methods of subnet masking: classful and classless. An example of a classful subnet mask is 255.255.0.0 and a classless would be 255.252.0.0.

Classful subnet masking

Classful subnet masking uses the default mask to separate the network number given by IANA from the host number. The table displays the default mask of classes A, B, C, and D. Classful subnet masks must have all ones (1) or all zeroes (0) in each octet.

Default Subnet Mask	
Class A	255.0.0.0 *or* 11111111.00000000.00000000.00000000
Class B	255.255.0.0 *or* 11111111.11111111.00000000.00000000
Class C	255.255.255.0 *or* 11111111.11111111.11111111.00000000
Class D	255.255.255.255 *or* 11111111.11111111.11111111.11111111

Default Mask	
Example	
157.28.13.114	The 157 signifies an address of Class B thus indicating a class full boundary of 2 octets (16 bits) for network address.
Converting to binary	10011101 00011100 00001101 01110010
Partitions	Network= 10011101 00011100 Host= 00001101 01110010
Subnet mask	255.255.0.0
Network ID	157.28.0.0
Host ID	0.0.13.114

Classless subnet masking

If a further subdividing of the network is necessary beyond the classful boundary, then the system borrows bits from the host or node field to create a subnet field. This means that the octets beyond the class boundary can become values to mask out the subnet field. Classless subnet masking, also known as classless inter-domain routing (CIDR, pronounced *cider*), offers more flexibility over the classful address ranges of A-D. CIDR uses variable length subnet. The following table displays classless subnet values.

Classless Subnet	
Subnet masks	11111111 = 255; 11111110 = 254; 11111100 = 252; 11111000 = 248; 11110000 = 240; 11100000 = 224; 11000000 = 192; 10000000= 128
Example	
Address	172.16.32. 4
Subnet mask	255.255.255.252
CIDR notation	172.16.32.14/30 (30 bits are used for the subnet mask). The 172 signifies an address of Class B thus indicating a class full boundary of 2 octets (16 bits) for network address. The mask identifies how many bits to use for the subnet.
Address conversion	10101100 00010000 00100000 00001110
Mask conversion	11111111 11111111 11111111 11111100
Partitions	Network= 10101100 00010000 Subnet= 00100000 000011 Host= 10
Network ID	172.16.0.0
Subnet ID	0.0.32.12
Host ID	0.0.0.2

As you can see, an IP address consists of a network number and a host number. A third field, the subnet number expresses to system administrators that “sub” networks are in use. Benefits of subnets are that they ease administration; improve network performance, and security. Because of the subnet mask, the network device still only sees a network number and host number. Keep in mind the network concept of there is a network and host number, as we go into the next lesson to discuss IP version 6 (IPv6).

614. Principles of Internet protocol version 6

IPv6 is the successor to IPv4. IPv6 provides a nearly unlimited number of IP addresses. It took the next step from IPv4 by creating addresses that are 16 bytes long, four times as large as IPv4 addresses (128 bits vs. 32 bits). Since IPv4 addresses consists of 32 bits, it has approximately 4.3 billion host addresses. IPv6’s extremely large addresses space can support up to 3.4 x 1038 (340,282,366,920,938,463,463,374,607,431,768,211,456) or 340 undecillion addresses, approximately 4.7*10^28 (47 octillion) addresses for every 7.6 billion people alive.

Unlike IPv4, we express IPv6 in 16-byte fields, which is considerably more user friendly. Instead of using the DDN, IPv6 uses eight groups of 16-bit sections displayed in a colon hexadecimal format.

Recall that hexadecimal is base 16 and decimal is base 10. So like in decimal how we count from 0 to 9 and then adding a column to make 10, counting in hexadecimal goes from 0 to F before adding a column. The characters A through F represent the decimal values of 10 through 15. The following table shows corresponding decimal, hexadecimal, and binary values.

Decimal	Hexadecimal	Binary
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Colon hexadecimal format comparison

The following examples are a comparison between the two address formats:

- IPv4: 192.168.123.100.
- IPv6: FEDC:BA98:7654:3210:FEDC:BA98:7654:3210.

If we converted the above IPv6 address into a decimal, it might look like this:

65244:47768:30292:12816:65244:30292:12816

Compressing

In the IPv6 format, there are two ways to shorten the expression of its addresses: leading zero compression and zero compression.

1. Leading zero compression drops leading zeroes in an address, in any field, as long as there is at least one number left:
    - Original IPv6 format – 1234:1234:0000:0000:1234:0000:0000:1234.
    - Using leading zero compression – 1234:1234:0:0:1234:0:0:1234.
2. Zero compression allows suppression of consecutive fields of zeroes. This method is allowed once per address:
    - Before suppression – 1080:0:0:0:8:0:0:417A.
    - After suppression – 1080::8:0:0:417A (48-bits suppressed) or 1080:0:0:0:8::417A (32-bits suppressed).
    - Suppression not allowed – 1080::8::417A.

In the last example above, this expression of suppressing zeroes is not allowed because it is impossible to determine the number of suppressed bits.

Address range

The text representation of IPv6 address prefixes is similar to the way IPv4 addresses prefixes are in CIDR notation. An IPv6 address prefix utilizes the following notification for representation: ipv6-address/prefix-length. The following is an example of IPv6 address range:

- FEDC:BA98:7654:3200::/56 – The number 56 signifies that from the leftmost part of the address and counting to the right 56 places belongs to the prefix.
- FEDC:BA98:7654:3200:: – This address is the start of the address range for host numbers using the prefix given above.
- FEDC:BA98:7654:32FF:FFFF:FFFF:FFFF:FFFF is the end of the address range for host numbers.

Assignment

IPv6 provides more efficient and useful addressing. In IPv4, CIDR allowed us to “borrow” bits from the host portion of the address in order to create a greater number of networks with fewer hosts per network. In most cases, IPv6 host address portion is a fixed 64-bit field and will never have bits borrowed from it to be able to create more networks. IPv6 addresses are 128-bit identifiers for interfaces and sets of interfaces. IPv6 covers three main types of addresses: unicast, multicast, and anycast.

- *Unicast* addresses identify a single interface. A packet sent to a unicast address delivers to the interface identified by that address.
- *Multicast* addresses (FF00::/8) identify a group of interfaces belonging to different nodes. Multicast packets send to all interfaces identified by that address
- *Anycast* addresses also identify a set of interfaces, but the packets deliver to and accept by the closest interface.

IPv6 does not utilize a broadcast address. The multicast address in IPv6 has taken over the function of the broadcast address from IPv4.

Unicast address scopes

Typically, interfaces using IPv6 have multiple addresses that identify the scope of the network traffic. Unicast addresses have two main segments—the network ID and the interface ID. Use this IP address as your reference, FEDC:BA98:7654:32FF:0000:FFFF:9800:FFFF. The network ID is represented by the first 64 bits (FEDC:BA98:7654:32FF) and interface IDs are represented by the second 64 bits (0000:FFFF:9800:FFFF). As you can see, it is similar to the IPv4 addresses two parts of network ID and host ID, but it is more flexible. Prefixes, within the network ID, designate a specific type of address or a subnet. The interface ID is a 48-bit MAC address with a 16-bit filler or a 64-bit Global Identifier, also known as an Extended User Interface–64. The 64-bits used for the host allows for 18.4 quintillion (1.84 x 1018) interface IDs per network! IPv6 defines three unicast address scopes: link, site, and global.

Link-local unicast

The first type of unicast address, the link-local address, operates within a network segment and will not originate from or be destined to an interface that requires a router to direct traffic. In this case, link-local addresses operate similarly to layer–2 MAC addresses allowing for quicker and more direct communication to interfaces on the same segment. Prefix length notation is FE80::/64.

Site-local unicast

A private address for IPv6 protocol always starts with FEC0. Assigning a site-local address to a system is equivalent to using a private address in IPv4, such as 10.0.0.0. The site-local address cannot communicate off the local site or network and is not reachable by other sites or systems on the Internet.

Global unicast

Finally, the last unicast address we will discuss is the global unicast address. Global unicast addresses are essentially publicly accessible addresses. The network ID portion of the address is broken up into different areas allowing for hierarchical design and allocation. This address type is equivalent to a public IP address with IPv4.

Reserved addresses

Designers of IPv6 took a more efficient approach when reserving addresses. The Internet Engineering Task Force reserves any address that begins with "0000 0000" for various uses. This represents 1/256 of the total address space of IPv6. Two special addresses are used in IPv6:

- 0:0:0:0:0:0:0:1 or ::1 is the loopback address.
- 0:0:0:0:0:0:0:0 or :: is the unspecified address (similar to the bootstrap address of a device that does not know its own address in IPv4).

Transition mechanisms

IPv6 is underway but transitioning fully from IPv4 will take a long time and perhaps indefinitely. There may be IPv6 network infrastructures out there that do not need IPv4 interoperability. However, in an environment where IPv4 and IPv6 resources need to interoperate, the table list mechanisms that are the initial core set of transitions.

Transition Mechanism	Purpose
Dual IP layer (also known as *dual stack*)	Technique for providing complete support for both Internet protocols: IPv4 and IPv6 (in hosts and routers).
Configured tunneling of IPv6 over IPv4	Point-to-point tunnels made by encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing infrastructures.
IPv4 compatible IPv6 addresses	IPv6 address format that employs embedded IPv4 addresses.
Automatic tunneling of IPv6 over IPv4	Mechanism for using IPv4-compatible addresses to automatically tunnel IPv6 packets over IPv4 networks.

The dual-stack protocol implementation in an OS is a fundamental IPv4-to-IPv6 transition technology. Dual stack protocol implements IPv4 and IPv6 protocol stacks either independently or in a hybrid form. The hybrid form is common in modern OSs supporting IPv6.

Modern hybrid dual stack implementations of IPv4 and IPv6 allow today's programmers to write networking code that works transparently on IPv4 or IPv6 networks. The software may use hybrid sockets designed to accept both IPv4 and IPv6 packets. When used in IPv4 communications, hybrid stacks use an IPv6 application-programming interface and represent IPv4 addresses in a special address format utilizing the IPv4-mapped IPv6 address.

Self-Test Questions

After you complete these questions, you may check your answers at the end of the unit.

613. Addressing fundamentals

1. What provides the MAC address in a computer?

2. What solved the problem that MAC addressing scheme was having with network growth?

3. What is identified in the IP address?

4. Why is DDN used in IP addressing?

5. What are the five classes of IP addresses? What are each used for?

6. Explain subnet masking.

7. What is the default subnet mask for a Class B network?

8. What would the subnet mask be for IP address 192.168.23.112?

9. What would be required to use if further subdividing of the network is necessary beyond the classful boundary?

614. Principles of Internet protocol version 6

1. What are the sizes of IPv6 addresses fields?

2. How are IPv6 addresses displayed?

3. Explain the two ways to compress IPv6 addresses.

4. What three main types of addresses does IPv6 cover?

5. Which unicast address scope accessible by the public?

6. Which IPv4 to IPv6 transition method is provides complete support for both protocols?

3–3. Local Area Network Technologies

This section introduces concepts related to local area networking technologies. The local area concepts discussed include network devices, communication media, topologies, and wireless technologies.

615. Principles of network devices

You create a network when you link computers together to share data and communicate. Networks come in many different sizes, as little as two computers up to hundreds of thousands, all interconnected through network devices. You should understand common network devices to facilitate troubleshooting and maintaining medical equipment. We will cover modems, converters, multiplexers, repeaters, bridges, hubs, switches, routers, gateways.

Hubs

A hub serves as a central connecting point and extends the physical media by repeating the signal it receives in one port out to all its other ports indiscriminately. Generally, a hub is a box with a number of connectors to which nodes are attached. Hubs usually connect nodes that have a common architecture (e.g., Ethernet).

An active hub serves as a wiring and signal relay center, and additionally cleans and boosts signals. A passive hub merely serves as a wiring and relay center. A collision domain is a group of devices connected to the same physical media such that if two devices access the media at the same time, the result is a collision of the two signals. A broadcast domain is a group of devices in the network that receive one another's broadcast messages. All devices connected to a hub share the same media, and consequently, the same collision domain, broadcast domain, and bandwidth. Hubs have been mostly phased out in favor of switches.

Repeaters

A repeater is a simple add-on device for extending a network by regenerating the signal carried within the cable (fig. 3–13). As electrical signals transmit on cable, they tend to degenerate in proportion to the length of the cable, known as attenuation. The main purpose of a repeater is to help reduce attenuation problems. Repeaters do their best to filter noise, but do not change the signal. A repeater can provide an extension to a network that reaches a distant workstation, but if many additional workstations are involved, use bridges or routers to extend the network. Unlike repeaters, bridges and routers help control traffic problems.

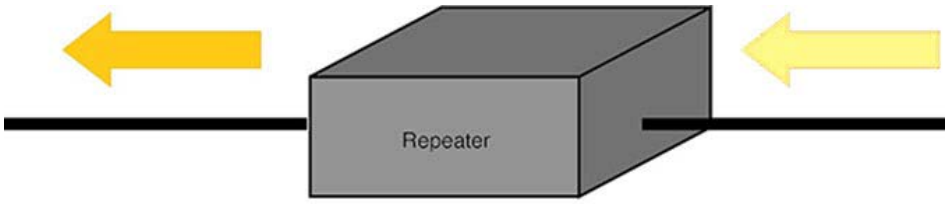


Figure 3–13. Example of a repeater.

Modem

The term modem is actually an acronym that stands for MOdulator/DEModulator. A modem is a device that modulates signals to encode digital information and demodulates signals to decode the transmitted information. The modem produces a signal that enables ease of transmission and provides decoding to reproduce the original data. A common type of modem is one that turns the digital data of a computer into a modulated electrical signal for transmission over telephone lines and demodulated by another modem at the receiver side to recover the digital data.

The original telephone modem connected users to the Internet by sending and receiving signals in the voice band of telephone networks. Two types of commonly used modems are dial-up and dedicated/leased.

A primary use of modems is to enable transmission of data over greater distances with the lowest possible signal loss. Another use for modems is to interface specific equipment through different types of media. For instance, although not typically used in military applications, cable modems enable high-speed digital transmission through existing architecture provided by cable companies. They enable simultaneous use of computer and television signals on the same transmission line without interfering with one another.

Media converters

A media converter is a cost-effective and flexible device intended to implement and optimize fiber links in every kind of network. Among media converters, the most often used type is a device that works as a transceiver, which converts the electrical signal used in copper unshielded twisted pair (UTP) network cabling to light waves used for fiber optic cabling. It is essential to have the fiber optic connectivity if the distance between two network devices is greater than a copper cable's transmission distance. The copper-to-fiber conversion allows connection of two network devices having copper ports across long distances by means of fiber optic cabling.

A media converter offers fiber-to-fiber conversion as well, from multi-mode fiber into single-mode fiber. It also converts a dual fiber link to single fiber with the help of bi-directional data flow. In addition, media converters have the capability to convert between wavelengths for applications that use wavelength division multiplexing.

Generally, media converters are protocol specific and they support an extensive array of data rates and network types. They are Physical layer (layer 2) switching systems. Media converters that include layer 2 switching functionality offer rate-switching as well as other innovative features.

Media converters permit fiber usage when required and integrate new devices into existing cabling infrastructure. Media converters provide seamless incorporation of fiber and copper, and various fiber forms in LAN networks. They support a multitude of protocols, media types and data rates to build a more trustworthy and cost-effective network.

Multiplexers

The term multiplexing means either combining (multiplex) many different signals into one serial digital data stream (transmit), or to split apart (demultiplex) a serial digital data stream into many different signals (receive) as shown in figure 3–14.

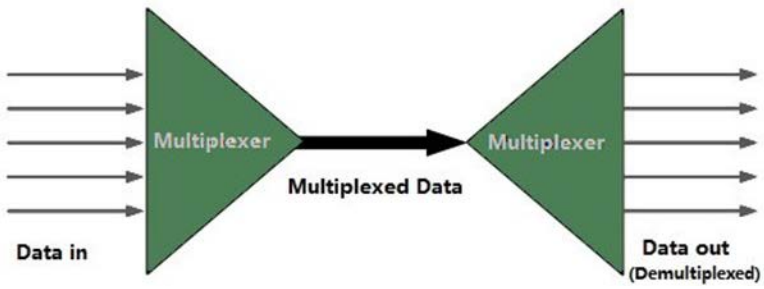


Figure 3–14. Multiplexer.
(Original graphic by The Anome at Wikimedia Commons, Colors and labels added, Licensed by CC BY SA 3.0.)

Any data communications environment that has more than one line going between common locations can benefit by installing a pair of multiplexers. A multiplexer performs the function of combining several data or voice communication channels into one composite signal, which can be transmitted between two locations cheaper than the cost of individual lines.

The most effective combination of lines in a multiplexed environment is between four and eight. Studies show that as little as 10 to 15 percent utilization of such lines is a common occurrence. Individual users connect to channels and the composite (logical) communication line between the two locations is the link. Link protocol is the communications discipline used between the two multiplexers.

Although the primary reason for installing a multiplexer is to save on communications costs, two other benefits are also present. One is the inherent error correction in a multiplexed environment and the other is inherent data security. Since a multiplex functions by taking individual data and transmitting it as data frames, there is an error detection and retransmission scheme built in. Error correction is so vital in many data transmission types, such as graphic data and program transmission, that many multiplexes are used primarily for their error correction capabilities. The other benefit is data security (not encryption), which is achieved by individual data streams formatted into a single communication line on one end of the link and then broken up into individual components on the other end. Someone wishing to “tap” into a multiplexed signal must have the link protocol and know the individual channel assignment schemes and data formats.

Bridges

A network bridge is an OSI layer 2 network device or software set that logically separates a single network into multiple segments or collision domains in Ethernet networks. The primary use for a bridge is to decrease network congestion but it also propagates a signal like a repeater. In an Ethernet network, if two computers transmit at the same time, a collision occurs. The larger the network, without bridges, the more likely you are to have a collision and attenuation. If using a bridge, computers/devices (nodes) only detect collisions on the same side of the bridge that the collision occurred. However, the nodes will not detect the collision on the opposite side of the bridge on the other segment. A bridge decreases the amount of network congestion by passing only the frames destined for computers/devices on the segment on the other side of the bridge.

Switches

Switches are OSI layer 2 and 3 devices that provide central connection to network devices used in the same manner as hubs but function more like bridges (fig. 3–15). They can provide higher bandwidth and frame-level filtering as well as dedicated port speed to specific devices on a segment. Many types of switches exist: LAN switches, asynchronous transfer mode (ATM) switches, and different types of WAN switches.

Figure 3–15. Switches.
(Original graphic by Dsimic at Wikimedia Commons, Labels added, Licensed by CC BY SA 3.0.)

LAN switches provide collision-free, high-speed communication between network devices. Switches operate like a one-way bridge with multiple ports. They do this by remembering the MAC address or addresses that are at each port and forward frames directly to the port. This provides the full bandwidth for each port, unlike hubs, which must share the bandwidth with each port. Because ports on a switch operate like a bridge, each physical port is logically a separate segment, also referred to as

a collision domain. This greatly reduces or eliminates collisions on a network. If you connected two file servers to individual ports, up to two simultaneous connections between workstations and file servers can occur. Switches not only eliminate collisions and speed up the network; they offer flexibility to the network.

Physical connections of different speeds such as 10 megabits per second and 100 megabits per second communicate using a switch, which accomplishes this through buffering. Store-and-forward switching is required whenever a frame moves from a low-speed connection to a high-speed connection. Look at the methods a switch uses to forward frames.

Layer 3 switches function like routers due to the similar layer 3 forwarding decision handling. The fundamental difference between layer 2 and layer 3 switch operation is the layer at which each forwarding decision occurs. Layer 2 switches make their forwarding decisions based on tables that store the mapping between MAC addresses and switch ports. Layer 3 switches build a table of network addresses and switch ports, making the forwarding decisions based on the network address information found in layer 3, rather than just the MAC address found in layer 2

Routers

Routers (fig. 3–16) operate at layer 3 (Network layer) of the OSI model. A typical router has an internal processor, an OS, memory, I/O jacks for different types of network connectors (depending on the network type) and usually a management console interface. Routers can be devices dedicated to routing or they can be off-the-shelf computers configured to perform routing services. Routing involves two basic activities: determining optimal routing paths and transporting information groups (typically called packets) through an Internetwork (also known as switching). Although switching is relatively straightforward, path determination can be very complex. Let us examine how a router or multilayer switch determines the best path.

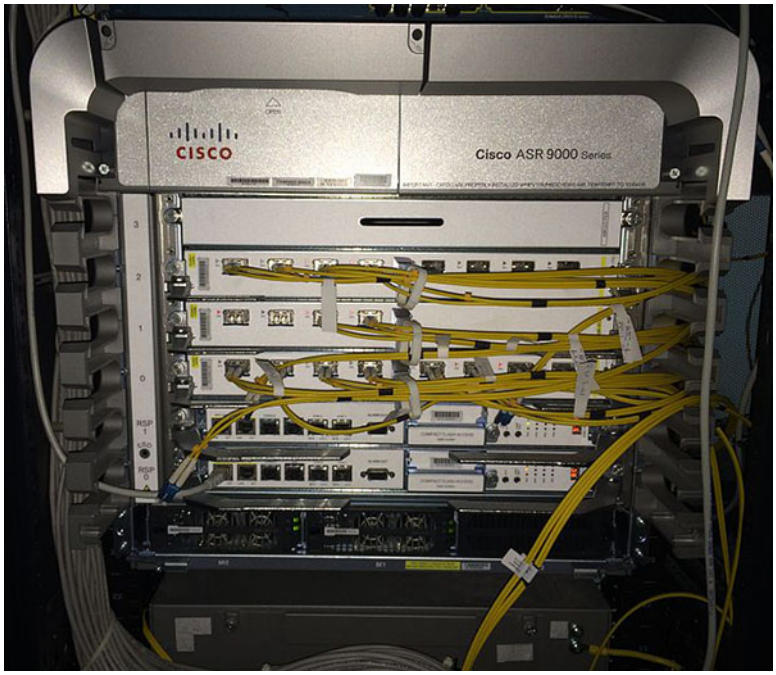


Figure 3–16. Router.
(Graphic by Redfox Hq at Romanian Wikipedia, Labels, Licensed by CC BY SA 3.0.)

Path determination

Metrics are standards of measurement (e.g., path length) used by routing algorithms to determine the optimal path to a destination. To aid the process of path determination, routing algorithms initialize

and maintain routing tables, which contain route information. Route information varies depending on its routing algorithm.

Routing algorithms fill routing tables with a variety of information. Destination and next hop associations tell a router that the optimal data path to a particular destination requires packet transmission to a particular router representing the “next hop” on the way to the final destination. When a router receives an incoming packet, it checks the destination address and attempts to associate this address with a next hop.

Routing tables can also contain other information, such as data about the desirability of a path. Routers compare metrics to determine optimal routes and these metrics differ depending on the design of the routing algorithm used. Routers communicate with one another and maintain their routing tables through the transmission of a variety of messages. The routing update message is one such message that generally consists of all or a portion of a routing table. By analyzing routing updates from all other routers, a router can build a detailed picture of network topology. A link-state advertisement, another example of a message sent between routers, informs other routers of the state of the sender’s links. Link information can also build a complete picture of topology to enable routers to determine optimal routes to network destinations.

Switching

Switching algorithms are relatively simple and are the same for most routing protocols. In most cases, a host determines that it must send a packet to another host. Having acquired a router’s address by some means, the source host sends a packet addressed specifically to a router’s MAC address; this time with the Network-layer protocol address of the destination host.

As the router examines the packet’s destination protocol address, the router determines that it either knows or does not know how to forward the packet to the next hop. If the router does not know how to forward the packet, it typically drops the packet. If the router knows how to forward the packet, it changes the destination physical address to that of the next hop and transmits the packet.

The next hop, in fact, may be the ultimate destination host. If not, the next hop is usually another router, which executes the same switching decision process. As the packet moves through the Internetwork, its physical address changes, but its protocol address remains constant.

Terms

The preceding discussion describes switching between a source and a destination end system. The ISO has developed a hierarchical terminology that is useful in describing this process. Using this terminology, network devices without the capability to forward packets between sub networks are end systems, whereas, network devices that can forward packets are intermediate systems. Intermediate systems can communicate within an autonomous system by using interior and exterior gateway protocols.

Autonomous system

Each network is an autonomous system managed by a single administration. An autonomous system is synonymous with a routing domain. Routing protocols that manage traffic within an autonomous system are interior gateway protocols (IGP).

Interior gateway protocols

The RIP, OSPF, and EIGRP are examples of IGPs. The IGPs would be responsible for routing within an Air Force base. The IGPs are designed for intra-autonomous system or intra-domain routing. The IGPs rely on a single composite metric to choose the best route to a destination. They may use one or several cost factors to develop the composite metric used to base their routing decisions. The IGPs occur on all networks from very small to extremely large.

Exterior gateway protocols

When several autonomous systems connect together, a different type of routing protocol known as exterior gateway protocols (EGP) is used. The Internet is composed of autonomous systems that use the border gateway protocol (BGP) to implement inter-autonomous system or inter-domain IP routing policies. BGP is the predominant EGP in use today.

Static vs. dynamic

Routers may use one of two methods for directing data on the network: static or dynamic routing.

Routing	Description
Static	Router is programmed to use specific paths between nodes. Static routing is not optimal because it does not account for occasional network congestion, failed connections, or device moves. If a router or a segment connected to a router moves, someone must reprogram the static routes. Static routing requires human intervention, so it is less efficient and accurate than dynamic routing.
Dynamic	Automatically calculates the best path between two nodes and compiles this information into a routing table. If congestion or failures affect the network, a router using dynamic routing can detect the problems and reroute data through a different path if possible. As a part of dynamic routing, routing protocols update routing tables by default when adding a router to a network.

Most networks primarily use dynamic routing, but may include some static routing to indicate, for example, a router of last resort. Termed the gateway of last resort, it is a static route used by the router when no other known route exists to transmit the packet. Routers are not simple to install on sizable networks because of their complexity and network interaction.

616. Principles of servers

A server is a network-connected computer system that provides services to network users. The term may refer to both the hardware and software or just the software that performs the service. Servers respond to the requests of users by providing a service, like printing a document or retrieving a file. The server is like the worker behind the counter in the fast food restaurant—retrieving files or services ordered by the customer.

It is a common practice to group servers physically (e.g., database, file, mail, print, etc.) within a single room for ease of maintenance, wiring, and administration. These groupings of servers are called server clusters.

Servers can provide network services in either a full-time or a part-time capacity. A server is dedicated if it is set aside to perform a specific task or function all the time. A dedicated server is not used for any function other than providing services to the network. A server is considered nondedicated if it will function in any other capacity. A typical nondedicated server is a node acting as a workstation for one worker and providing a service for another worker. A client-server network is a network with services provided strictly by dedicated servers. A peer-to-peer network is a network where nondedicated servers provide services. Client-server network is what you will ordinarily see in an organization. Let us examine some common types of servers and the service that each provide.

File server

A file server stores programs and data files which users share. It acts like a remote hard drive. An effective file server must be fast, reliable, and provide sufficient storage for all the data and programs users need.

Print server

A print server provides access to networked printers and manages the information sent by users. Print servers run programs to create and operate print queues for jobs sent to network printers from devices

on the network. Two terms you should know that are associated with network printing are print queues and print spooling.

Print queue

A print queue is a temporary storage location for files waiting to be printed. When users send files to the networked print device, the print server captures and temporarily stores those files in a section of memory or hard drive (print queue). A print queue is required due to the differences between the physical speed of the print device and the processing speed of the workstation generating the print job, since a print device operates slower than the computer processes data. Once a file has printed, the print server deletes the temporarily stored copy of the file.

Print spooling

To spool a document is to read it in and store it, usually on a hard drive or larger storage medium so it can be printed or otherwise processed at a more convenient time. For example, after a print device finishes printing the current document. Print spooling refers to the entire process of queuing (lining up) print jobs all waiting for their turn to be printed then feeding those files to the print device as it becomes available.

On networks, multiple users might send documents to the same print device. These documents are sent to a spooler, where they wait their turn to be printed. Spooling frees the computer's attention so the user can continue working while waiting for a document to print. When a file is sent to the networked print device and the print server has temporarily stored the file in the queue, the print server then manages the physical printing of the files. This entire process is called print spooling.

There are two methods to spool files. These methods can be used independently or in conjunction with each other. The first method is to store and print the files as the print queue receives them—first in/first out. The second method allows the print server administrator to assign a priority or precedence to files as required. After the spooler receives a file, the priority can be changed to a higher priority number than the other jobs in the queue. This will move a job in front of other jobs with lower priority numbers. Priorities numbers start at 1 (the lowest priority) to 99 (the highest priority) and can only be changed by someone with explicit permissions to do so. If no priority is assigned, the spooler reverts to the first in/first out method.

Database server

A database server consists of software to provide access to database records for programs running on networked devices. A database server is a computer attached to a network that runs a client-server database management system (DBMS). Workstations, acting as clients, can send requests to the server over the network, and then the server responds. Client workstations handle the presentation of data and interact with users while the server performs the workhorse operations such as sorting, indexing, and delivering data to users.

A database server is a central depository for information that many users access. Most of the database architectures and query languages, such as structured query language (SQL), used to access the DBMS on a database server have roots in traditional mainframe computers. However, LAN-based database servers use client-server models in which the processing load is divided between the back-end database server and the front-end client. This model takes advantage of the processing power of both client and server computers.

Communications server

Communications server provides access to modems or other communication facilities that provide network capabilities to the user. It is a dedicated system and provides communication services for users on a network who need to transfer files or access information on systems or networks at remote locations over telecommunication links. The communication server provides communication channels for one or more users simultaneously, depending on the software and the hardware capabilities. Some can also provide connections to remote systems or networks.

Application server

An application server allows users to run applications located on it, which take some burden off the user's computer. An application server runs programs in a networked environment. The applications may be network versions of commercial, off-the-shelf software that allow multiple users to access and run the program. This avoids loading the program on each user's computer and allows central updates to take place on the server. Custom built or off-the-shelf client-server applications may run on application servers as well. A client-server application distributes processing between the client handling presentation and user input.

Domain name system server

When you access Web sites on the Internet, you can type the IP address of the site or the DNS name. Since most of us have no desire to keep track of IP addresses, DNS is a valuable service. It helps people refer to Internet sites by name. DNS servers are located on the Internet strategically to convert domain names to IP addresses. Your own ISP may do this conversion or connect to a specific DNS server that does. When you type a domain name in a Web browser, you send a query to the primary DNS server defined in your Web browser's configuration dialog box. The DNS server converts the name you specified to an IP address and returns this address to your system. From then on, it uses the IP address in all subsequent communications.

Proxy server

The proxy server breaks the connection between the sender and receiver, and acts as an intermediary between a workstation user and the Internet so an organization can ensure security, administrative control, and caching service. All input is forwarded out a different port, closing a straight path between two networks and preventing a hacker from obtaining internal addresses and details of a private network.

Proxy servers are available for common Internet services; for example, you use an HTTP proxy for Web access, and a SMTP proxy for e-mail.

Proxy servers generally employ network address translation, which presents one organization-wide IP address to the Internet. It funnels all user requests to the Internet and fans responses back to the appropriate users. Proxies may also cache Web pages, so that the next request can be obtained locally. Proxy servers are only one tool that can be used to build a firewall.

A proxy server is associated with or part of a gateway server that separates the organizational network (intranet) from the public network (Internet) and a firewall server that protects the organizational network from outside intrusion. A proxy server receives a request for an Internet service (e.g., Web page) from a user. If it passes filtering requirements, the proxy server looks in its local cache of previously downloaded Web pages. If it finds the page, it returns it to the user without needing to forward the request to the Internet.

If the page is not in the cache, the proxy server, acting as a client on behalf of the user, uses one of its own IP addresses to request the page from the appropriate server out on the Internet. When the page is returned, the proxy server relates it to the original request, saves a copy in cache, and forwards it on to the user.

To the user, the proxy server is invisible; all Internet requests and returned responses appear to be communicating directly with the addressed Internet server. An advantage of a proxy server is that its cache (memory) can serve all users. Internet sites frequently requested are likely to be in the proxy's cache, which will improve user response time. In fact, there are special servers called cache servers. It still functions as a proxy server, but with very specific duties. It stands between the user and the Internet and provides requests for Web pages to the user. Requests to a proxy cache server can only come from inside the local network. Anyone attempting to access the proxy cache from outside the local network is denied access effectively hiding or making the local network invisible to the Internet.

Mail server

A mail server provides “post office” facilities. It stores incoming mail for distribution to users and forwards outgoing mail through the appropriate channels. The term may refer to just the software that performs this service, which can reside on a machine with other services. They automatically connect with other LANs or electronic “post offices” to pick up and deliver e-mail.

Dynamic host configuration protocol server

The DHCP server helps reduce configuration time for TCP/IP networks by automatically assigning IP addresses to clients when they log on. DHCP centralizes IP address management on central computers that run the DHCP server program. A server has a pool of IP addresses, known as a scope, available for lease by a client for a specific time. The DHCP server can also assign other values such as default gateway, domain name, and DNS server.

617. Principles of communication media

In the previous lesson, we discussed several of the most common network devices. Now we will cover how these devices interconnect. As you might imagine, a number of different network media types are available. Some faster than others, some work over relatively long distances, and some do not require a physical connection to the network at all. In this lesson, we will cover major network media types and their characteristics, uses, and features.

In general, most networks utilize metallic cable for connection at some point; the most common types are twisted pair cable and coaxial cable.

Coaxial cable

Coaxial cable is the grandfather of mainstream network media types and it is associated with the original designs of the Ethernet standard. Today, you typically use coaxial cable when you need a broadband solution.

Coaxial cable consists of a single wire core surrounded by an insulation layer; an outer metal screen made of a woven copper mesh; a metal-covered plastic or foil; and an exterior protective sheath.

The metal screen shields the conductor from corruption by external signals, such as radio waves, and other sources of EMI, such as power cables, cellular phones, motors, fluorescent light fixtures, and electrical storms. This shield also significantly reduces the amount of radiation given off via EMI, essentially eliminating a source of interference that causes problems for other systems. Coaxial cable gets its name from its physical characteristics, specifically because the conductor wire and the shielding braid share a common axis or centerline.

New LAN installations rarely use coax except for highly specialized settings, such as elevator shafts where EMI causes significant problems. Applications where a high-speed broadband solution is required also use coaxial.

There are many different types of coax cable; each suited for a different purpose, such as audio, video, television, satellite, cable, radio, and data transmission. Cable types match the characteristics of the signal they are transmitting. The radio guide (RG) is an identifier of coaxial cable types. For example, RG–6 defines a specific type of coaxial cable used to transmit cable TV signals with a nominal impedance of 75 ohms. The following table shows some common coaxial cable types.

Cable type	Nominal impedance	Distance limitation (in meters)
RG–6	75 ohms	300
RG–58	50 ohms	185
RG–8	50 ohms	500
RG–11	50 ohms	500

The nominal impedance is the measure of the wire's resistance. Nominal impedance shows how much the cable impedes or resists the flow of electric current, which one of the factors that determines the RG. This difference is why you always use the correct cable types for the job. Mismatched RG types could cause equipment damage and/or system failure.

Unshielded twisted pair cable

Most, if not all, modern networks use a metallic cable known as UTP cable. UTP cable is typically a copper wire medium. A paired cable consists of two wires individually insulated from one another and twisted together to make one pair. Wire pairs then twist together with other pairs to form a cable. The twisting cancels out induced signals that can interfere with the communication signals. A protective sheath such as lead or plastic then covers the cable to protect the pairs against physical and or environmental damage. UTP has an effective range of 100 meters.

UTP cable comes in a variety of categories numbered 1 through 6a. These categories, developed throughout the years, facilitate faster and faster network designs with each new development. In the following table, the "Base" refers to baseband signaling, which means that only Ethernet signals are carried on the medium and the "T" represents twisted pair. The following is a description of each category and their capabilities:

Category	Bandwidth	Standard
1 (obsolete)	1 megabits per second	Voice only analog phone lines (not used for data communications)
3 (obsolete)	10 megabits per second	Ethernet (10BaseT)
4 (obsolete)	100 megabits per second	Ethernet (100BaseT)
5e	1,000 megabits per second	Ethernet (1000BaseT)
6	1 gigabits per second	1 Gigabit Ethernet (1 GbE)
6a	10 gigabits per second	10 Gigabit Ethernet (10 GbE)

Most current cabling installations use category 6 or category 6a cabling, since they support all current and planned data speeds and standards. Manufacturers typically print the cable category on its sheathing.

The RJ45 is the *standard* connector used for category 5e/6/6a network cables.

Ethernet color code

Within a multi-pair UTP cable, different colors of coated insulation help identify each wire or pair of wires. Cables often contain many wires and come in many different sizes. A wrapping, called a binder, within the cable jacket groups the wires together (twisted pairs, two wires each). The T568A and T568B wiring standard, identified in figure 3–17, is used with RJ45 network (Ethernet) connections. The design of the T568A and T568B color schemes enable high data rates on twisted pair cable. While these configurations represent two different standards, most newly installed equipment follows the T568B standard. Regardless of what standard you are using, the key is to be consistent throughout the network.

Wiring RJ45 jacks and plugs

The RJ45 jacks and plugs are the standards for terminating twisted pair cable used for data networks. However, use of the networking standards used to configure the jack and plug connections of these connectors is common (see tables following the figure). While RJ45 describes the Universal Service Ordering Code (USOC) jack and plug used to make the connections in a data network, there are other standards used to describe the actual wiring of the jack and plug.

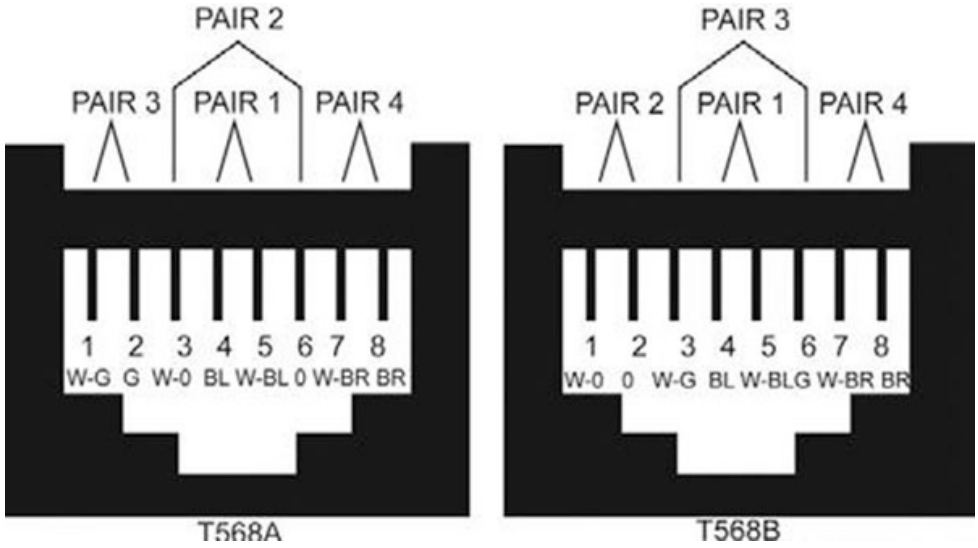


Figure 3–17. T568A and T568B Ethernet RJ45 color code.

Color Code: Color	
BL: blue	W-BL: white – blue
BR: brown	W-BR: white – brown
G: green	W-G: white – green
O: orange	W-O: white – orange

The two wiring standards used to define how to attach twisted pair cable to an RJ45 jack or plug are the Electronics Industry Association/Telecommunications Industry Association (EIA/TIA) 568A and 568B standards. The primary difference between these two cable standards is the sequence and placement of the green and orange wire pairs on the plug or receptacle. Actually, for a computer network installation, there is actually no difference in performance between the two standards because the color of a wire's jacket has no bearing on the transmitted signal. However, if the cable carries both data and voice (telephone) traffic, the 568A standard is backward compatible with the older USOC telephone standards. The EIA/TIA 568B does not support voice signals.

When you install an RJ45 jack or plug on the end of a UTP cable, it is important that you match the correct pin to the correct wire color. There are differences between the pinout patterns required to support different types of connections made between different types of hardware. The pattern you use depends on the requirements of the equipment.

Straight-through pinout

Straight-through cables connect devices that operate at different layers of the OSI model, such as a switch (layer 2) to a router (layer 3). A straight-through pinout on an RJ45 connector matches the same color wires on both the plug and the receptacle. In other words, the orange, blue, green, and brown wires on the plug match up and connect to the orange, blue, green, and brown wires on the receptacle.

The following tables list the pinouts for the EIA/TIA 568A and EIA/TIA 568B straight-through connections.

EIA/TIA 568A Straight-through Pinouts		
	Connector	
A Pin	**Wire Color**	**B pin**
1	White-green	1
2	Green	2
3	White-orange	3
4	Blue	4
5	White-blue	5
6	Orange	6
7	White-brown	7
8	Brown	8

EIA/TIA 568B Straight-through Pinouts		
	Connector	
A Pin	**Wire Color**	**B Pin**
1	White-orange	1
2	Orange	2
3	White-green	3
4	Blue	4
5	White-blue	5
6	Green	6
7	White-brown	7
8	Brown	8

Crossover pinout

The 568A and 568B crossover patterns reverse two of the wire pairs to connect the transmit pins at one end of the cable to the receive pins at the other end. We use crossover cables to connect devices that operate at similar layers of the OSI model, like a router (layer 3) to another router (layer 3). The following tables list the pinouts for the jacks and plugs at each end of a cross-connect or crossover connection for EIA/TIA 568A and 568B, respectively, and figure 3–18 illustrates the wiring patterns.

EIA/TIA 568A Crossover Pinouts		
	Connector	
A Pin	**Wire Color**	**B Pin**
1	White-green	3
2	Green	6
3	White-orange	1
4	Blue	7

EIA/TIA 568A Crossover Pinouts		
	Connector	
A Pin	**Wire Color**	**B Pin**
5	White-blue	8
6	Orange	2
7	White-brown	4
8	Brown	5

EIA/TIA 568B Crossover Pinouts		
	Connector	
A Pin	**Wire Color**	**B Pin**
1	White-orange	3
2	Orange	6
3	White-green	1
4	Blue	7
5	White-blue	8
6	Green	2
7	White-brown	4
8	Brown	5

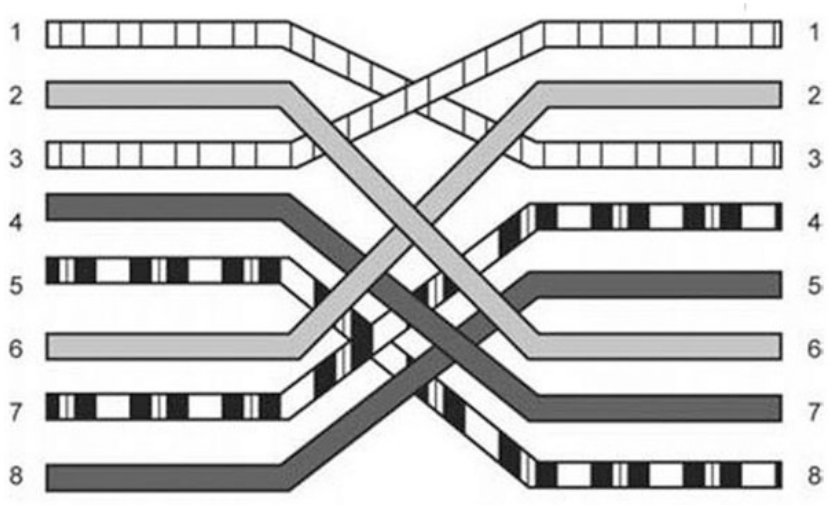


Figure 3–18. Pinout crossover sequence for EIA/TIA 568A and 568B connections.

Attaching an RJ45 connector

To attach an RJ45 plug to a UTP cable, follow these steps:

1. Strip away about 1 inch of the outer jacket of the UTP cable. Use a CatX (the X represents category cables 3 and above) cable stripper, if one is available. Do not strip the cable sheathing more than 1.25 inches from the connection end of the cable (1 inch is best).

2. Untwist the exposed wire pairs but avoid untwisting the wires at the end of the jacket. UTP wire should not be untwisted more than 0.5 inch and 0.375 inch is preferred.
3. Arrange the wires in a flat row in the order that matches the pinout pattern for the cable purpose. For example, for a straight-through connector, arrange the wires left to right as white-green, green, white-orange, blue, white-blue, orange, white-brown, and brown.
4. Use wire-cutters to trim the length of the wires to 0.5 inch. There is no need to strip the individual wires.
5. Insert the wires into the RJ45 plug ensuring that the wires remain in the required pattern.
6. Use an RJ45 crimping tool to push the gold insulation displacement contacts into contact with the wires. The crimper pushes down a hinged tab that presses against the insulation of the wire to hold it into the plug and create a strain relief. Some crimper tools when used with certain connectors also cut the wires extending beyond the other side of the connector.

Shielded twisted pair cable

Shielded twisted pair (STP) cable has the combined features of the twisted pair cable and coaxial cable. STP cable has a thin aluminum foil or a copper braid like the one used in coaxial cable wraps around the pairs. The conductors are spaced uniformly during manufacture. This leaves each wire perfectly balanced capacitive to the surrounding conductor. Maintaining the balance minimizes certain detrimental effects such as high capacitance to ground when grounding the shield. This line does not radiate energy because of the shield, so nearby magnetic fields do not affect it.

Plenum grade cable

A plenum is the shallow space in many buildings between the false ceiling and the floor above; it helps circulate warm and cold air through the building. Computer rooms and magnetic resonance imaging (MRI) or computerized tomography (CT) equipment rooms that have a raised floor often use them. Fire codes give very specific instructions about the type of wiring that can be routed through this area, because any smoke or gas in the plenum will eventually blend with the air breathed by everyone in the building.

Plenum-grade cabling contains special materials in its insulation and cable jacket. These materials are fire resistant certified and produce a minimum amount of smoke; this reduces poisonous chemical fumes. Plenum cable is for use in plenum area and in vertical runs (e.g., in a wall) without conduit.

Fiber optic cable

In the mid-1960s, the first fiber cables were developed but they attenuated the signal too much to be usable. By 1970, silica glass fibers were in development. They are as thin as a human hair and bendable. These fibers were the first practical optic waveguides that opened the door to further advances. Simultaneously, semiconductor technology made possible the fabrication of efficient light sources that allowed modulation with an external signal.

Advantages and disadvantages of optical communication systems

Just as it is possible to send Morse code signals to a receiver some distance away using a flashlight, it is also possible to send signals by light emitting diode (LED) or light amplification by stimulated emission of radiation (LASER). An optical communications system requires a light source (transmitter), a transmission medium (cable), and a sensor (receiver). Transmission over fiber optic systems' advantages over conventional cable systems include larger bandwidths, freedom from interference, low cost, and lightweight. Fiber optics enables transmission of much more information than the lower-microwave frequency properties.

Advantages of fiber systems

Fiber optic provided the necessary materials for the light sources and detectors, and optical waveguide technology, which provided the medium—the optical fiber cable.

The reason fiber optic is so highly praised is its many advantages over other transmission media, both traditional (copper wire) and non-traditional (microwave) as shown in table below.

Property/Type of cable	Fiber optic	Twisted pair	Coaxial
EMI immunity	Yes	No	No
RF interference immunity	Yes	No	No
Electromagnetic pulse immunity	Yes	No	No
High degree of transmission security	Yes	No	No
Electrical isolation	Yes	No	No
No crosstalk	Yes	No	No
No echoes or ringing	Yes	No	No
Temperatures to 1000 degrees Celsius	Yes	No	No
Elimination of spark/fire hazards	Yes	No	No
Low cost	No	Yes	No

Broad bandwidth

Fiber optic cable systems have more potential bandwidth than any system. The potential information carrying capacity or the amount of information that transmittable over a communications channel increases with frequency. Since the frequencies of light are much higher (in the terahertz range) than radio frequencies, an optical fiber has the potential for a lot of information. Theoretically, the higher bandwidth of fiber permits thousands of channels carried over the same fiber at the same time.

Low attenuation

Not only does fiber optic cable have a higher information carrying capacity than metallic cable, it also introduces less attenuation and distortion into the system. More important, attenuation in fiber cable does not increase with signal frequency as it does in metallic cables.

Electromagnetic immunity

EMI is unwanted energy given off by electronic circuits and picked up by other circuits. Since fiber optic cable does not radiate or absorb energy through its outer jacket, it is immune to both EMI and RF interference. Parallel installation of several fiber optic cables, even in the same enclosure, without the signals interfering with each other is possible. This is because the fibers in optic cables are made of a dielectric material (glass or plastic).

Size

Fiber optic cables are considerably smaller than metallic cable. Overall, the small size of fiber cables lead to simplified installation and maintenance.

Weight

Glass weighs less than metal. Weight savings are important since the bandwidth and low line loss of fiber allow a single fiber to replace several metallic cables.

Security

Fiber is almost impossible to tap without affecting the transmission enough for authorized users to notice. In addition, fiber does not radiate energy. This feature makes electromagnetic field sensing eavesdropping equipment useless.

Safety

The dielectric composition of fiber isolates it electrically. The fiber presents no spark hazard and proves its use in flammable environments where metallic cables present hazards. Fiber cables do not

attract or respond inductively to lightning. In addition, they do not short out or produce electric shocks.

Disadvantages

The advantages of fiber optic cable systems far outnumber the disadvantages. However, there are some drawbacks.

Cost

Although the cost is decreasing, it is a drawback in some areas, such as installation and end equipment. Unfortunately, the high cost of interfacing equipment somewhat offsets the simplicity and economy of fiber optics.

Physical handling/installation

Technicians skilled in working with copper cables now have to learn new methods of cable splicing. They must receive special training to learn these new techniques. Because fiber optics is a relatively new field, they are making rapid progress in solving or reducing the seriousness of the problems involved and dropping the cost. Fiber optic cables have already shown their cost effectiveness in long distance communications links. The low line loss of fiber optic cables means fewer repeaters are required.

618. Principles of topology types

A network's topology consists of the physical and logical arrangement of its stations in relation to one another. There is a variety of topologies available to LANs. In this lesson, we will describe topologies and the relationships between them, both physically and logically.

We commonly use the word topology to discuss the properties of various types of networks. Topology is the branch of mathematics that examines the characteristics of geometric shapes. Networks have shapes and the shape a network takes affects the way it functions.

When we refer to a network's topology, we can be referring to either its physical or logical topology. When used alone, the word "topology" often refers to the physical topology. A physical topology acts as a map; it shows how the devices on the network physically connect. The physical topologies available are bus, ring, star, hybrid, and mesh. A logical topology defines the way in which devices communicate and data transmission occurs throughout the network. This may be in the form of a bus or ring. The rule of thumb that distinguishes physical from logical topology is that it is physical if you can see it and touch it, and it is logical if you cannot.

A network's topology affects its capabilities. The choice of one topology over another will have an impact on the following:

- Type of equipment the network requires.
- Capabilities of the equipment.
- Growth of the network.
- Management of the network.

We will first discuss physical topology.

Physical topology

In order to share resources, computers need a connection. Most networks use cable to connect one computer to another. However, it is not as simple as just plugging cables into computers. Different types of cable, network cards, and network OS require different types of arrangements. A network topology takes planning to work well. For example, a particular topology can determine not only the type of cable used, but also how it is routed through floors, ceilings, and walls. Topology can also determine how computers communicate on the network. Different topologies require different communication methods and these methods have great influence on the network. The most common modern physical topology is the hybrid (typically with a mix of star topology).

All networks typically stem from the three basic topologies—bus, star, and ring. It is rare to see these used individually in today's networks. Although considered legacy, it is important to understand how they function as they are integrated in hybrid topologies.

Before choosing a topology for operations, the following are some factors to consider:

- Cost.
- Scalability (ability to be change in size or scale).
- Bandwidth capacity.
- Ease of installation.
- Ease of troubleshooting.

Now, let's take a closer look at the topologies.

Bus topology

In a bus topology, also known as a linear bus, a single cable connects all devices in a straight line (fig. 3–19). These devices share the responsibility for getting data from one point to another. Each station on a bus network passively listens for data directed to it. When one station wants to transmit data to another station, it broadcasts an alert to the entire network, informing all stations that it is transmitting; the destination station then picks up the transmission. Stations other than the sending and receiving stations ignore the message.

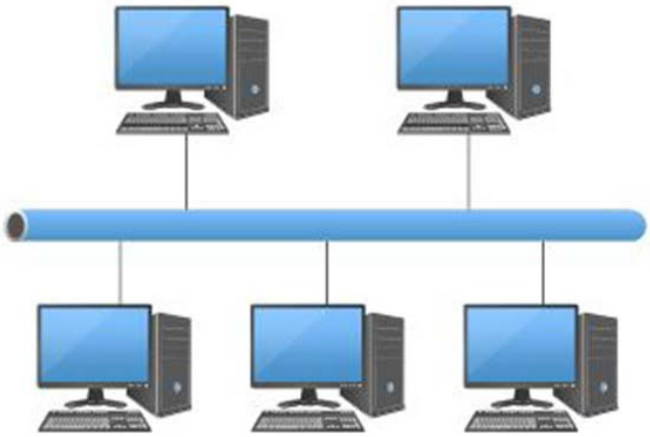


Figure 3–19. Bus topology.

Bus networks use coaxial cable as their physical medium. At the ends of each bus network are 50-ohm resistors known as terminators. Terminators stop signals after they have reached the end of the wire. Without these devices, signals on a bus network would travel endlessly between the two ends of the network, a phenomenon known as signal bounce, and new signals could not get through. On a network, terminators prevent this problem by halting the transmission of old signals. In some cases, a hub provides termination for one end of a segment. Furthermore, grounding a bus network protects the network from static electricity and EMI, which could affect the signal.

Networks that have a physical bus topology typically use thin coaxial cable that connects to the NIC using a Bayonet Neill-Concelman (BNC) connector, which can also connect two or more computers.

Advantages

The advantages of a bus topology include the following:

- Inexpensive to install.
- Easy to add more workstations.

- Require less cable than all other topologies.
- Works well for small networks (2-10 devices).

Disadvantages

The disadvantages of a bus topology include the following:

- No longer a recommended option for new installations.
- Network is down if backbone breaks.
- Only a limited number of devices can be included.
- Difficult to isolate location of a problem.
- Sharing same cable means slower access time.

Ring topology

The ring topology consists of workstations connected in the form of a ring or circle in which data flows from station to station in a circle (logical ring) or a combination of both (fig. 3–18). It has no beginning or end that needs termination. This allows every device an equal advantage to accessing media. The signals travel around the loop in one direction and passes through each station, which can act as a repeater to boost the signal and send it on to the next computer.

Each workstation acts as a repeater for the transmission. The fact that all workstations participate in delivery makes the ring topology an active topology. A ring topology differs from a bus topology in this way. A ring topology also differs in that it has no “ends” and data stops at its destination. In most ring networks, twisted pair or fiber-optic cabling is the physical medium. The two types of ring topologies are single ring and dual ring.

The first ring networks used a single-ring topology (fig. 3–20). In a single-ring network, all the devices share a single cable and the data travels in one direction like a merry-go-round. Each device waits its turn and then transmits. When the data reaches its destination, another device can transmit. The drawback of a single ring topology is that a single malfunctioning station can disable the network.

In addition, just as in a bus topology, the more stations that must participate in data transmission, the slower the response time. Consequently, pure ring topologies are not very flexible or scalable.

The most common implementation of the ring is in a Token Ring network. Token Ring networks use a physical ring or star topology. As technology evolved, a dual-ring topology was developed. This topology allows two rings to send data, each in a different direction. Not only does this let more packets travel over the network; it allows packets to continue along the media, creating redundancy.

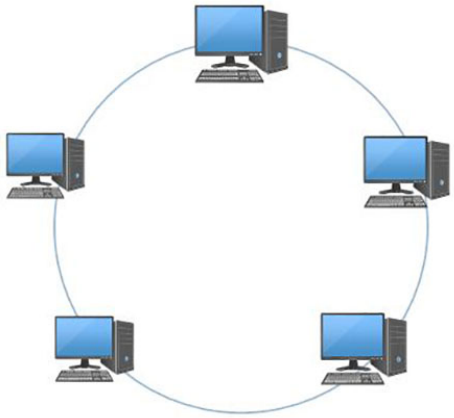


Figure 3–20. Ring topology.

FDDI is a technology similar to Token Ring, but it uses light instead of electricity to transmit data. FDDI networks use two rings for redundancy. FDDI is unique compared to other types of ring networks because it will keep functioning in the event there is a break in one or both rings.

Advantages

The advantages of a ring topology are as follows:

- Data packets can travel at greater speeds.
- There are no collisions.
- It is easier to locate problems with devices and cable.
- No terminators needed.

Disadvantages

The disadvantages of a ring topology are as follows:

- It requires more cable than a bus network.
- A break in the cable will bring down many types of ring networks.
- Adding devices to a ring network temporarily disrupt network traffic.
- It is not as common as the bus topology, so there is not as much equipment available.

Star topology

In star topology, cable segments from each computer connect to a centralized component (fig. 3–21). The central component can be one of a variety of devices. It can be an active or passive device like a hub or an intelligent device such as a router, switch, or a bridge. Some intelligent devices can incorporate diagnostic features that make it easier to troubleshoot network problems. Each device in a star network connects to a centralized component with its own cable. Although this does require more media, it has many advantages over both the bus and ring topologies. Data signals transmit from the sending computer through the central component to all computers on the network. This topology originated in the early days of computing when computers connected to a centralized mainframe computer.

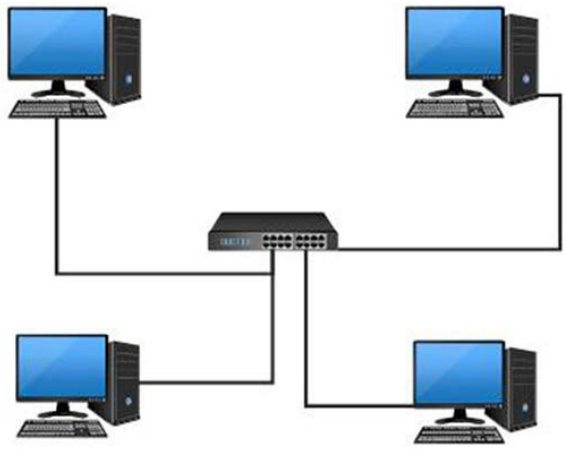


Figure 3–21. Star topology.

Usually, star topologies are built with twisted pair or fiber-optic cabling. Any single cable on a star network connects only two devices (e.g., a workstation and a switch), so a cabling problem will affect two stations at most. Devices such as workstations or printers transmit data to the centralized device, which then retransmits the signal to the network segment containing the destination station.

Star networks and extended star networks have become a popular topology type for networks. One of the advantages of a star topology is that it is easy to make changes and additions to the network

without disrupting users. You can add a new workstation or expand the network without ever affecting the network's performance. Star networks can support a maximum of only 1024 addressable stations on a logical network.

Advantages

The advantages of a star topology are as follows:

- It is easy to add more devices as your network expands.
- The failure or malfunction of one cable will not bring down the entire network.
- The centralized device provides centralized management.
- It is easy to troubleshoot device and cable problems.
- It supports faster network transmission speeds than ring and bus.

Disadvantages

The disadvantages of a star topology are as follows:

- Requires more cabling than ring or bus.
- Failure of centralized device can bring down entire network.
- Installation and equipment costs are higher than ring or bus.

Hybrid topology

Hybrid topologies combine two or more different physical topologies in a single network. They are the most commonly seen today. Hybrid topology inherits positive and negative qualities of all the incorporating topologies. Figure 3–22 represents a hybrid topology. The combining topologies may contain attributes of star, ring, bus, and mesh topologies. Most WANs connect by means of dual-ring topology and networks connected to them are mostly star topology networks. The Internet is the best example of the largest hybrid topology.

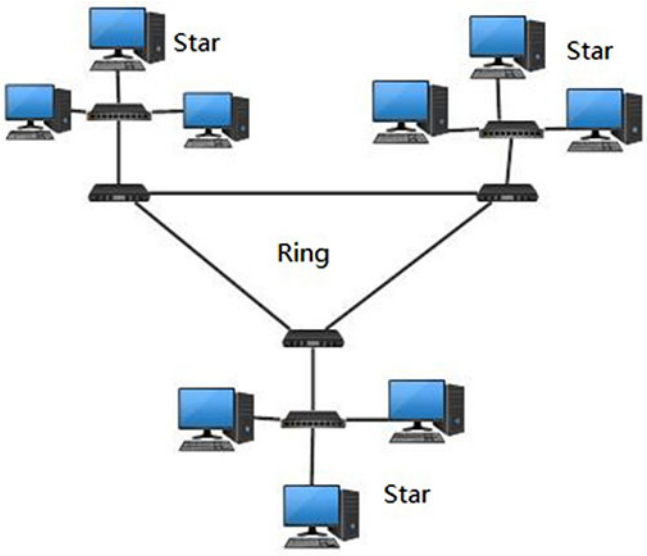


Figure 3–22. Hybrid topology.

Mesh topology

Network devices share multiple interconnections between stations such as routers and switches in mesh network topology. In the event of cable or stations failure, mesh topology offers redundant paths for transmission of data. While troubleshooting and increased reliability are definite advantages, mesh networks are expensive to install because they require a large amount of cabling. Full mesh topology (fig. 3–23) occurs when every station has a circuit connecting it to every other station in the

network. Full mesh is very expensive to implement and yields the greatest amount of redundancy, so in the event that one of those stations fails, network traffic reroutes to any of the other nodes. Backbone networks typically incorporate a full mesh topology.

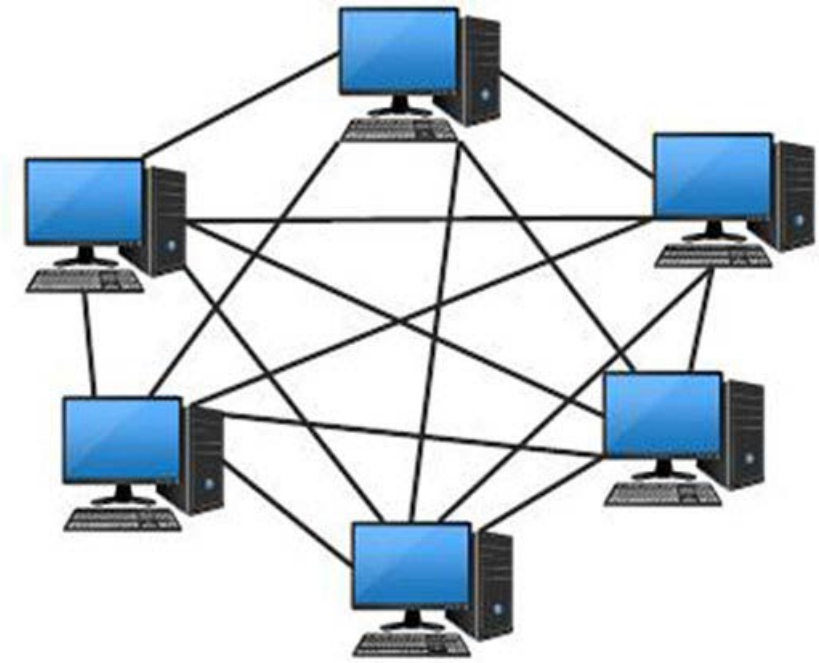


Figure 3–23. Full mesh topology.

When some nodes connect with all the other nodes using direct links, while some only connect to one or two stations it is referred to as a partial mesh topology. It is less expensive to implement and yields less redundancy than full mesh topology.

Logical topologies

A logical topology is a concept in networking that defines the architecture of the communication mechanism for all stations in a network. Using network equipment such as routers and switches, the logical topology of a network can be dynamically maintained and reconfigured. Logical topologies contrast with physical topologies, which refer to the physical interconnections of all devices in the network.

The logical topology defines how the data should transfer. Contrast this to the physical topology, which consists of the layout of cables, network devices, and wiring. Two of the most common logical topologies are listed in the table.

Topology	Description
Bus	Ethernet uses the logical bus topology to transfer data. Under a bus topology, a node broadcasts the data to the entire network. *All* other nodes on the network hear the data and check if the data is for them.
Ring	In this topology, *only* one node transfers data in a network at a given time. The token provides a collision free network.

Logical topologies are bound to network protocols that direct how the data moves across a network. The Ethernet protocol is a common logical bus topology protocol. A network's logical topology is not the same as its physical topology. For example, twisted pair Ethernet is a logical bus topology in a physical star topology layout. While IBM's token ring is a logical ring topology, it is physically set up in a star topology.

619. Principles of wireless technologies

In today's networking environment, the means of connecting LAN devices has evolved to a more versatile, cost effective, but less secure technology. More and more networks today are utilizing air as a medium of choice over copper. This technology reduces the costs involved with physically implementing a network, while also increasing the speed of installation. This transmission process presents a collision problem that modern switched networks solved. Remember CSMA/CD. The use of switches solved the collision problem in modern LANs. Switching technology also multiplied the speed by allowing full-duplex operations. However, now that we move our transmission medium to the air we are down to a single shared bus. Therefore, collisions are going to happen with WLAN implementation. If more than one device transmits concurrently, at the same frequency, no signal will be intelligible. The Carrier Sense Multiple Access Collision Avoidance (CSMA/CA) algorithm *avoids* this multiple signal interference.

CSMA/CA works much like CSMA/CD; both listen to see if busy, use wait timers to reduce chances of collision, and then listen for acknowledgement frames. The main difference is that in CSMA/CA the transmitter station listens for network silence and then sends a warning signal telling all other stations not to transmit, before it sends its packet. Because of the single bus architecture of the radio transmission medium, WLANs are constricted to half-duplex operations.

Wireless standards

To ensure interoperability between different vendor's equipment, the IEEE developed several models of wireless standards to meet the demands of network security, speed, and flexibility. The IEEE 802.X series is a set of standards that provides guidance on how equipment should operate in a given network environment. This section covers the current IEEE standards that pertain to wireless networking.

The IEEE 802.11 standards specify the wireless "over-the-air" interface between a wireless client and a base station or access point and other wireless clients. The 802.11 standards are comparable to the IEEE 802 Ethernet standard for wired LANs. The IEEE 802.11 specifications address both the Physical and MAC layers and exist to resolve compatibility issues between different manufacturers of wireless LAN equipment. Within the IEEE 802.11 standard, several series apply to different wireless operational environments, including IEEE 802.11a, b, g, n, and ac series.

Institute of Electrical and Electronics Engineers 802.11a

The IEEE 802.11a specification offers data transmission speeds up to 54 megabits per second. Networks using IEEE 802.11a operate at radio frequencies between 5.725 and 5.850 gigahertz. The specification uses a modulation scheme known as orthogonal frequency-division multiplexing (OFDM) that is especially well suited for use in office settings. There is less interference with 802.11a than with IEEE 802.11b, because 802.11a provides more channels that are available and because 802.11b shares a frequency spectrum (2.400 to 2.4835 gigahertz) with various household appliances and medical devices. This makes the 802.11b standard more susceptible to interference caused by these devices.

Institute of Electrical and Electronics Engineers 802.11b

The IEEE 802.11b specification offers data transmission up to 11 megabits per second. Networks employing 802.11b operate at radio frequencies between 2.400 and 2.4835 gigahertz. IEEE 802.11b uses the Ethernet protocol and CSMA/CA for path sharing. The modulation used by Ethernet has historically been phase-shift keying. The modulation method selected for 802.11b is complementary code keying. It provides higher data speeds and is less susceptible to multi-path-propagation interference.

Institute of Electrical and Electronics Engineers 802.11g

The IEEE 802.11g specification offers transmission over relatively short distances at up to 54 megabits per second, just like the 802.11a standard. Networks employing 802.11g *operate* at radio

frequencies between 2.400 and 2.4835 gigahertz, the same band as 802.11b, but the IEEE 802.11g specification employs OFDM. OFDM is the same modulation scheme used in IEEE 802.11a to obtain higher data speeds. Computers or terminals set up for 802.11g can also fall back to speeds of 11 megabits per second. This feature makes 802.11b and 802.11g devices compatible within a single network. Modification of an 802.11b access point to be 802.11g compliant usually involves only a firmware upgrade.

Institute of Electrical and Electronics Engineers 802.11n

The IEEE 802.11n specification *improves* upon legacy wireless standards by utilizing the multiple-input multiple-output (MIMO) method. MIMO increases the capacity of wireless communications by implementing multiple paths for sending and receiving data over the same channel. 802.11n supports a max of four paths with a channel width of 40 megahertz. The use of multiple paths allows this technology to achieve data rates from 54 Mbps to 450 megabits per second. The 802.11n technology operates on both the 2.4 gigahertz and 5 gigahertz frequency bands.

Institute of Electrical and Electronics Engineers 802.11ac

The IEEE 802.11ac specification significantly improved speed, offering data transmission up to 1.3 gigabits per second. 802.11ac only transmits over the 5 gigahertz spectrum. Similar to the 802.11n technology, 802.11ac uses the MIMO method. However, 802.11ac doubles the amount of MIMO streams from four to eight paths and increases the channel widths to 80 MHz. It is backwards compatible with 802.11a and 5 gigahertz 802.11n (all previous versions that operate in the 5 gigahertz frequency band).

Wireless requirements

In order to implement a wireless network (fig. 3–24), two key devices must first be gathered or obtained. These devices are the wireless NIC (WNIC) and an access point.

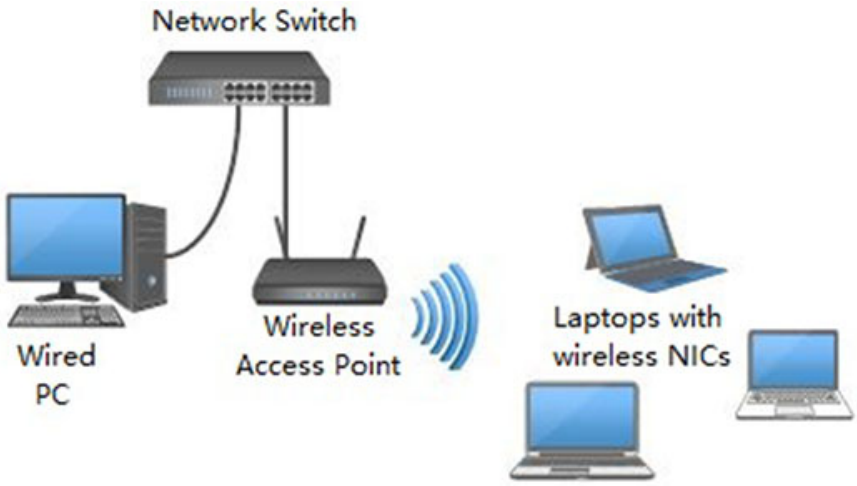


Figure 3–24. Example of a WLAN.

Wireless network interface controller

A WNIC shares the same functionality as a NIC, but is capable of transmitting the information through air. The WNIC has the following components: a transmitter (transceiver) and an antenna used to transmit and receive the wireless information.

Wireless access point

As the name implies, an access point is where all the wireless devices will convey or “connect” to share information. The main reason the access point is not called a wireless switch it because it does not perform any type of switching function. It only broadcasts signals out, amplifies incoming

signals, and forwards signals throughout the network. If the access point connects to a switch or a router, the access point will forward the information to the appropriate device within the wired network. These forwarding decisions occur using the MAC address of the devices, making the access point a layer 2 (Data Link layer) device, like an Ethernet switch.

In addition, access points are capable of grouping wireless users into virtual local area networks (VLAN). The use of VLANs is implemented within the access point by grouping devices in different frequencies within the frequency range of the wireless technology used (e.g., IEEE 802.11a, b, g, n, and ac).

Wireless design

There are four key phases or steps to follow when designing a wireless network. The four phases are planning, deployment, securing, and management & support. By following or integrating these four steps, you will simplify and reduce the design process. We will discuss the planning and deployment phases. Security will be discussed in next unit and management & support is similar to wired LANs.

Planning

During the planning phase, you should account for multiple factors. Some of these factors include the following:

- Training for both the users and the administration.
- Current and future technologies available for the installation.
- Current and future amount of users on the network.
- Amount of resources the network must support.
- Access requirements for the wireless network.
- Integrity and security requirements of network data.

When developing a wireless solution it is important to pay close attention to data security and integrity. In addition, make sure the frequencies used will not interfere with military frequencies used in the area the wireless network will be deployed.

Ensure that the existing infrastructure will support the wireless network. Take in to account the following factors:

- Building structure and material.
- Network devices currently in place.
- Wireless devices currently in place (e.g., cell phones, radios, etc.).

Deployment

The implementation of a wireless network is simpler than a wired network because minimal cable requirements exist. The only cables that you may have to install are the cables that will connect the access point to a router or a switch. Otherwise, the installation of the NICs and the access point is the only thing that will require installation and configuration.

When installing access points, remember to consider range limitations and readjust access point locations to allow for convergence. This will allow mobile wireless users to have constant connectivity as they move from access point to access point.

Because the access point is a radio device, it is susceptible to common causes of interference that can reduce throughput and range. Install the access point in an area where large steel structures such as shelving units, bookcases and filling cabinets do not block the radio signal to and from the access point. Furthermore, install the access point away from devices that operate at the same frequency as the access point, which can cause signal interference.

Before configuring the access point, make sure that you have the appropriate information on hand. This includes the IP address for the access point and the service set identifier (SSID). The SSID is a 32-character network identifier attached to the header of packets sent over a WLAN and allows wireless clients to identify the network they are intending to join. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID.

An access point connected to at least one wireless station creates a basic service set (BSS). The BSS simply refers to the AP along with its associated wireless stations. A device cannot join the BSS unless it can provide the unique SSID.

The following are basic steps required to configure an access point:

1. Console into the access point.
2. Disable SSID broadcast if possible. Normally the access point broadcasts its SSID so that wireless devices that come within range can detect the network and join. This can help add an obstacle in securing the network from intruders.
3. Assign a SSID for the wireless network (do not use default SSID).
4. Assign an IP address.
5. Enable wireless security.
6. Enable SNMP.

After completing the configuration, ping the access point from a wireless workstation and from your wired network to test connectivity.

620. Using a network analyzer

Network test equipment provides a means of checking and controlling the operational characteristics of equipment on LANs, MANs, or WANs. We will look at general concepts of a protocol/network analyzer. There are many makes and models available, so your shop's equipment operating characteristics may differ somewhat from those presented in this lesson.

Operational characteristics of a protocol analyzer

A protocol analyzer provides a capability for digital network diagnostics and for developing communications software. Use of these analyzers has increased over the years and will certainly continue to do so in the future.

General description

The protocol analyzer may be a specialized laptop computer, small handheld unit, or software application operated on a common personal computer. In most cases, the analyzer is portable and transportable to the physical location of the individual network connection. Protocol analyzers count total frames, collisions, error frames, broadcasts, and other statistical data. It displays this data in a numerical, graph, or speedometer gauge format. The protocol analyzer's disk storage provides the capability to capture and save the data for later viewing. We will now discuss some common features of protocol analyzers.

Theory of operation

Network devices connect to a LAN via an internal NIC. As data moves across the network, the NIC only processes broadcast frames and frames addressed to its MAC address. The NIC configuration in a protocol analyzer allows it to process all frames. In serial circuits, the selection of frames for processing is not a concern. All frames that enter a serial interface are processed and then sent to the other components of the protocol analyzer for further processing.

These components are presented in the following table:

Protocol Analyzer	
Component	**Description**
Counter	This component counts bytes, frames, and errors as the NIC processes them.
Filter	Discards frames based on filter definition or activates a trigger based on trigger definition.
Buffer	This component stores all frames based on the user configuration inputs.
Protocol analyzer CPU	This specialized processor processes the frames based on the selected test and the user configuration inputs.
Personal computer CPU	This processor provides the operating system capabilities, user interface and display information based on the user inputs.

The protocol analyzer stores the received frames in a buffer in RAM. Once stored, it processes them according to the protocol rules identified in the frame's data-type field. For example, it processes AppleTalk® frames using the protocol rules of AppleTalk and high-level data link control (HDLC) frames using the protocol rules of HDLC.

The operator may configure the protocol analyzer to display the captured frames in a specified manner using a filter. After the operator defines the filter, it suppresses any unwanted information and displays only the desired data. In the event the filtered information is ever required, it remains stored in the buffer for retrieval. For easier reading, the analyzer converts hexadecimal data fields to ASCII text. Since network addresses identify the network nodes, the operator may convert them to their commonly used node names. For example, it is easier to identify the e-mail server by its name than by its IP address.

Interfaces

Multiple interfaces are located at the rear or side panel of most protocol analyzers. For some protocol analyzers, the operator can change the interfaces. These different interfaces allow connections to different types of packet and serial networks. Depending on the type and model, the interface for the protocol analyzer can be Ethernet, FDDI, Token Ring, ATM, frame relay, HDLC, and so forth. These interfaces may have different types of physical connectors including straight tip and FDDI for fiber, RJ45 and 25-pin D-sub size B (DB–25) for twisted pair, and BNC for coaxial cable.

Capture filters

The protocol analyzer can analyze all data that enters the network interface. In most cases, so much data moves across the network that finding a specific problem is equivalent to finding a needle in a haystack. Capture filters display and store only the data you are interested in analyzing. You may also use a capture filter to exclude specific types of frames. The following are common types of capture filters:

- Protocol.
- MAC address.
- IP address.
- VLAN.
- Frame attributes.

You can define specific types of filters to capture only a specific type of protocol data, such as World Wide Web (WWW) traffic. You can create a MAC address filter if you only desire to see the traffic from, to, or between specific hosts. Using the network address of one or more hosts, the IP address filter accomplishes the same task as the MAC address filter. The VLAN filter only captures frames

transmitted across a specific VLAN. The protocol analyzer can capture specific frame attributes as well, including runts, collisions, and frames with a bad frame check sequence (FCS).

Modes of operation

In transmit mode, the protocol analyzer generates a constant stream of data, a single burst of data or a repetitive burst of data. Configuration of the data frames may include random data, all zeros, all ones, and other patterns. Configuration may also be of constant or variable length. Generation of VLAN tags occurs for packets within a VLAN.

In the receive mode, the protocol analyzer monitors and captures data frames across the network. Configuring triggers will capture frames that contain specific data patterns. Configuring counters will display the number of specific occurrences, such as the following:

- Packets transmitted.
- CRC errors.
- Under and oversize packets.
- ARP requests.
- Collisions.
- Bit errors.

Most protocol analyzers run on high-performance personal computer or laptop platforms. Specialized protocol analysis application software and data capture and analysis hardware perform the tests. The hardware connects to the network by common LAN connectors, such as an RJ45 connection. When connected to the network, the analyzer may passively monitor all traffic or act as a node to generate data traffic.

Menus

After starting the protocol analysis application, the user interface provides drop-down menus and toolbars. Drop-down menus are above the toolbar. The RUN drop-down menu allows you to start, stop, or pause the collection or generation of data. The VIEW drop-down menu allows you to specify the desired display. The available displays include protocols and frames. You can display the data in a pie chart or grid chart. The Go To drop-down menu allows you to display a specific record. You can display a record-by-record number, time stamp, or locations in the capture buffer. The Setup drop-down menu allows you to configure the protocol analyzer for the desired operation. The configuration includes the physical interface type, protocols, line speed, buffer size, filter type, and so forth.

After selecting the appropriate toolbar button, the test window appears and lists several test windows:

- Line vital statistics.
- Protocol statistics.
- MAC node statistics.
- Node discovery.
- Connection statistics.
- Active testing.

Line vital statistics

Line vital statistics provide information concerning the network utilization, total number of frames transmitted and frame errors on the entire subnet. Selecting the appropriate button on the toolbar activates the line vital statistics window. You must start the line vital statistics frame capture to display the statistics. Current and peak values for each statistic displays in a table. An accompanying graph shows the value of each statistic over a given time period.

Some of the statistics displayed are as follows:

- Utilization.
- Frames.
- Local collisions.
- Remote collisions.
- Late collisions.
- Bad FCS.
- Runts.

Protocol statistics

Protocol statistics provide information concerning the network utilization and frame errors that relate to a specific protocol. Selecting the appropriate button on the toolbar activates the protocol statistics window. You must start the frame capture to display the statistics. Current and average peak statistics for each protocol displays after selected. Several sub statistics for each protocol type are available for display. Listed below are some of these substatistics:

- Utilization.
- Fragment count.
- Time-to-live packets.
- SNMP packets.
- Bad FCS.
- Collisions.
- Broadcasts.

All statistics display in a table viewed on the screen. The table shows each protocol and substatistic. Selecting the appropriate button on the toolbar activates the graph feature.

Media access control node statistics

MAC node statistics report errors that occur at the Physical layer of the OSI model, such as a bad FCS, short frames, and jabbers**.** These types of problems usually indicate a bad cable, connector, or NIC. Selecting the appropriate button on the toolbar activates the MAC node statistics window. You must start the frame capture to display the statistics. Statistics for the top 20 nodes automatically display. Selecting a specific node displays detailed information about the frames for that node. You may also create a filter so that only information concerning specific frames or nodes displays.

Node discovery

Node discovery automatically runs in the background when the protocol analyzer application activates. Selecting the appropriate button on the toolbar activates the MAC discovery window. The node discovery window shows the MAC address of each node. A drop-down menu allows you to view nodes by protocol, IP address, error events, or DNS name. You may manually add nodes and edit node names.

Connection statistics

Connection statistics provide information concerning the bandwidth utilization and the number of connections related to specific nodes. Selecting the appropriate button on the toolbar activates the connection statistics window. You must start the frame capture to display the statistics. The data displays in a statistics table, a connection graph, and a pie chart.

The data for each node in the statistics table includes MAC address, IP address, bits sent and received, protocols used, network utilization, and number of connections. Selecting the appropriate button on the toolbar activates the connection graph or pie chart within the connection statistics window. The pie chart shows the number of frames, utilization, frames per second, and bytes per second transmitted by all nodes or a specific node. The tables and graphs help you determine the following:

- Which users consume the most bandwidth.
- Number of connections to a particular network or site.
- Volume of traffic leaving a network, VLAN, or subnet.
- Which router or switch interface is the busiest.

Active testing

Most network analyzers passively monitor the network to diagnose problems and report statistics. Active tests generate data traffic on the network to analyze network performance. Before generating any traffic, configure the protocol analyzer with a valid IP address. You must activate the Go To drop-down menu and select Configure Analyzer. At the configuration window, enter an IP address and default router. Now you may select the appropriate button on the toolbar to activate the active tests window. In the active tests window, you may configure a filter or select an active test. Some of the active tests are ping, trace route, and traffic generator.

Ping

Use the ping utility to determine if a network node is connected or responding. This functions the same as the ping command in the command prompt discussed earlier. The ping utility sends a series of ICMP echo request messages to the target node. The results identify the target node's response, and the time (delay in milliseconds) it took the target to receive the request and respond.

Trace route

Use the trace route test to see the path that packets are traveling and the time (delay in milliseconds) it takes the packets to complete the trip. Each node that processes the packet responds with the IP address of its network interface. The results list the IP address of the network interface of each node the packet routes through until the packet reaches the target node. The response time (delay in milliseconds) it took for each node to respond is also displayed. As with ping, trace route can also be ran from the command prompt. At the command prompt, simply type "tracert" followed by a space, and then the address (www.google.com). In figure 3–25, the user traced the route from their device to www.google.com.

Traffic generator

The traffic generator allows you to send frames to a specific node. You may send frames that have a default pattern or create your own pattern. Some of the types of frames you may send are ICMP, ARP, and FTP. A separate window displays the response frames from the receiving node. For stress testing, you may configure the traffic generator to send enough frames to use a specific percentage of the network bandwidth. You can also configure the number of frames for the generator to send.

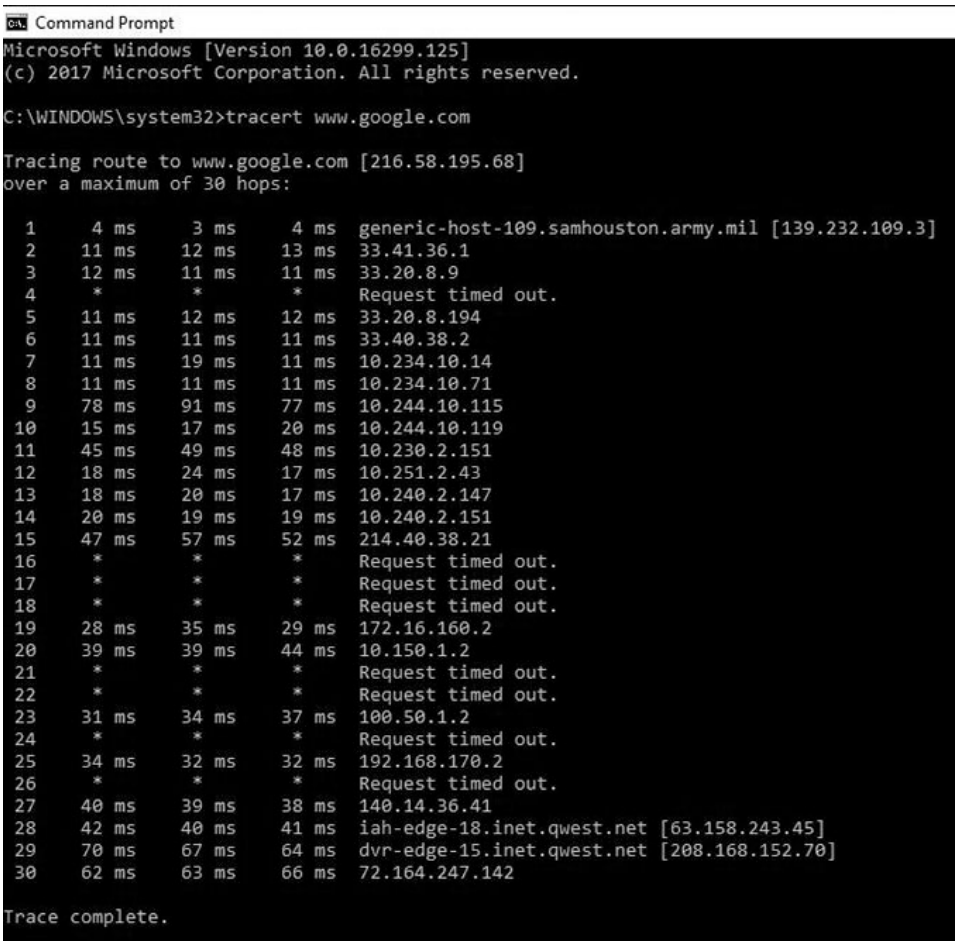


Figure 3–25. Sample trace route command.

Self-Test Questions

After you complete these questions, you may check your answers at the end of the unit.

615. Principles of network devices

1. What is the difference between an active and passive hub?

2. What purpose do repeaters serve in a network?

3. What are two uses of modems?

4. What does a transceiver media converter do?

5. What is multiplexing?

6. What are three benefits to using multiplexers?

7. What is the primary use of a bridge in a network?

8. How do switches provide collision free, high-speed communication?

9. What is the fundamental difference of a layer 2 and 3 switch?

10. Typically, what components are part of a router?

11. What does a router do when it receives a packet?

12. What type of routing protocol would an Air Force base use? Name two examples.

13. What method of routing is used primarily?

616. Principles of servers

1. What is the purpose of a server?

2. What is the most common server configuration used? How is it arranged?

3. What is the function of a print queue?

4. Describe the two methods of print spooling.

5. Explain the roles of the client and server in a database server.

6. What does using an application server enable?

7. Explain how a proxy server ensures security.

8. What is the DHCP server's role?

617. Principles of communication media

1. When is coaxial cable used in modern networks?

2. What type of medium do the majority of modern networks use?

3. What is the key to using Ethernet T568A and T658B?

4. What type of jacks and plugs are used to terminate and connect twisted pair cable?

5. What is the *primary* difference between Ethernet T568A and T658B?

6. When are crossover cables used to connect devices?

7. How are RJ45 plugs secured on cables?

8. What are unique specifications of plenum grade cable?

9. What three components does an optical communications system require?

10. How does the bandwidth of fiber optic compare with other transmission media?

11. Discuss security of fiber optic.

618. Principles of topology types

1. What is the difference between physical and logical topology?

2. How does the choice of a topology affect the network?

3. What three topologies do all network typically originate?

4. List the factors to consider before choosing a topology.

5. How is a bus topology connected?

6. What are the disadvantages of a bus topology?

7. What are advantages of using a ring topology?

8. What devices can be the central component in a star topology?

9. List advantages of a star topology.

10. What is the *best* example of the largest hybrid topology?

11. What is the difference between full mesh and partial mesh topology?

12. What type of logical topology does Ethernet use?

619. Principles of wireless technologies

1. How does CSMA/CA differ from CSMA/CD?

2. Why are WLANs constricted to half-duplex operation?

3. Describe the MIMO method.

4. What improvements do 802.11ac MIMO methods have compared to 802.11n MIMO methods?

5. 802.11ac is backwards compatible with what two older standards? Why those two?

6. What two devices are required to implement a wireless network?

7. Why is an access point *not* considered a switch?

8. What factors should be accounted for in the planning phase?

9. What should be considered when installing access points?

10. Why should the SSID be disabled if possible?

620. Using a network analyzer

1. What actions do a protocol analyzers perform?

2. Explain the five components of protocol analyzer.

3. How are capture filters used?

4. What action does the analyzer perform in transit mode?

5. Which test window provides information on which users consume the most bandwidth?

6. What test reveals the path that packets are traveling?

Answers to Self-Test Questions

610

1. A series of private computer networks connected to each other.
2. A network that encompasses two or more computer workstations connected by one or more types of media.
3. Mobility, ease of installation, and cost.
4. WAN.
5. Typically provide wireless connectivity using cellular network technology. Examples of WWAN technologies are Long-Term Evolution and Worldwide Interoperability for Microwave Access.
6. Remote access and extranet connections.

611

1. How information from a software application in one computer moves through a network to a software application in another computer. It also establishes guidelines so software and hardware components from different manufacturers can interoperate across diverse networking environments.
2. Voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, and physical connectors.
3. In half-duplex transmission, the transmission and reception of data must happen alternately. Full-duplex transmission means that communications between components simultaneously transmit and receive.
4. Any three: hubs, repeaters, NICs, and cables.

5. The IEEE subdivided the Data Link layer into the LLC and MAC sublayers. The LLC manages communications between devices over a single link of a network and the MAC manages protocol access to the physical network medium and its specification defines MAC addresses, which enable multiple devices to identify one another uniquely at the Data Link layer.

6. Layer 3-Network.

7. Flow control, multiplexing, virtual circuit management, error checking and recovery.

8. The Session layer establishes, manages, and terminates communication sessions between local and remote applications.

9. By providing a variety of coding and conversion functions for Application-layer data.

10. It is necessary to ensure there is sufficient bandwidth to deliver services appropriately, compression of network services occurs to provide acceptable quality, and reduce network load and overhead.

11. Telnet, FTP, SMTP, FTAM, VTP, and CMIP.

12. Control information consists of specific requests and instructions exchanged between peer OSI layers and it typically takes the form of headers and trailers.

13. As data passes from the upper layers to the lower layers, the addition of the headers and trailers occurs in a process called encapsulation. Each layer in the source system adds control information to the data, and each layer in the destination system analyzes and removes the control information from that data. The term used to describe this process on the sending side is encapsulation. On the receiving side of the data transmission process, it is decapsulation.

14. PDU with Transport layer source and destination.

612

1. The OSI model provides a conceptual framework for communication between computers, but the model itself is not a method of communication. Actual communication occurs by using communication protocols and TCP/IP is the standardized network protocol suite the DOD and Internet use.
2. When comparing TCP/IP protocols to OSI model, TCP/IP's Network Access layer includes the OSI Physical and Data Link layers' functions. The TCP/IP Internet layer maps directly to the OSI Network layer. The TCP/IP Transport layer maps directly to OSI's Transport layer. TCP/IP's Application layer includes OSI's Session, Presentation, and Application layers' functions.
3. With connection-oriented protocol, a connection is established between the sender and recipient prior to the transfer of any data. Connectionless-oriented protocol simply sends out data packets to receiving system and does not require receipt acknowledgment.
4. FTP requires users to log on to the remote host with an ID and password in order to gain access to a directory and transfer files.
5. Relies on UDP. Since it is connectionless, it does not guarantee reliable data delivery and does not require users to log on to the remote host with an ID and password to gain access to a directory and transfer files.
6. Transferring e-mail between computers. User-level client mail applications typically only use SMTP for sending messages to a mail server for relaying and they actually use IMAP to retrieve messages.
7. HTTP.
8. Matching a host name for a unique domain such as www.af.mil to the IP address of a server where the host is located.
9. Make IP addressing transparent for mobile users, reduce the time spent on IP address management, reduce the potential for errors in assigning IP addresses, and enable movement of network devices without having to change the TCP/IP configuration.
10. NTP synchronizes the clocks of computers on a network. Time is critical in routing to determine the most efficient path for data over a network, so time synchronization across a network is important for time-stamped security methods and maintaining accuracy and consistency between multiple storage systems. For these reasons NTP benefits from UDP's quick, connectionless nature. NTP is time-sensitive and cannot wait for the error checking that TCP would require.
11. TCP is responsible for breaking messages into segments, reassembling them at the destination station, resending anything not received and reassembling the message from the segments.
12. TCP uses a three-way handshake. The requestor sends a packet specifying the port number it plans to use and its initial sequence number (ISN) to the server. Next, the server acknowledges with its ISN, which

consists of the requestor's ISN, plus (+) 1. Finally, the requestor acknowledges the acknowledgement with the server's ISN, plus (+) 1.

13. By grouping bytes in TCP segments and then delivering to IP for transmission to the destination.
14. The data segment's position in the stream of data segments already sent.
15. Allows the receiving node to determine whether the corruption of the TCP segment occurred during transmission.
16. Buffering, source-quench messages, and windowing.
17. The location of a particular application or process on each device (in the Application layer).
18. 1c, 2d, 3a, and 4b.
19. UDP is best for sending small amounts of data for which guaranteed delivery is not required and minor packet loss is acceptable, such as with Internet phone, real-time video conferencing, streaming audio and video, and online games.
20. Getting data from one end system to another end system by any means possible.
21. IP provides information about how and where to deliver data, including the data's source and destination address.
22. Indicates whether a message is fragmented, and if fragmented, whether the datagram is the last fragment.
23. Determines how long a datagram will exist. At each hop along a network path, the datagram is opened and it is time to live field is decremented by one (or more than one in some cases). When the time to live field reaches zero, the datagram is 'expired' and discarded. This prevents congestion on the network
24. ARP sends a MAC broadcast request to the entire destination network, asking for the MAC address of a particular known destination IP. The device identified by the IP address in the packet responds to the request, and replies by sending its MAC address.
25. Ping uses ICMP services to send echo request and echo reply messages that determine the validity of an IP address. These two types of messages work in much the same way that sonar operates, which is how the program earned its name. First, the computer transmits a signal called an echo request to another computer/device. The other computer/device then rebroadcasts the signal, in the form of an echo reply, to the sender.
26. By pinging the loopback address (127.0.0.1), you can determine whether your workstation's TCP/IP services are running. By pinging a host on another subnet, you can determine whether the problem lies with a connectivity device between the two subnets.
27. CSMA/CD.

613

1. NIC.
2. Logical addressing, commonly known as IP addressing.
3. It identifies the individual node and the network to which the node attaches.
4. To represent a binary IP address in a more user-friendly manner.
5. Class A, B, C, D, and E. Class A is used for large networks, Class B is used for intermediate networks, Class C is used for networks with around 250 nodes, and Class D and E are reserved.
6. Subnet masking is a mechanism that allows a network device to divide an IP address into a network and host number.
7. 255.255.0.0.
8. 255.255.255.0.
9. Classless subnet masking.

614

1. 16-byte fields.
2. IPv6 uses eight groups displayed in a colon hexadecimal format.
3. Leading Zero compression drops leading zeroes in an address, in any field, as long as there is at least one number left; and zero compression allows suppression of consecutive fields of zeroes but only allowed once per address.
4. Unicast, multicast, and anycast.
5. Global unicast.

6. Dual IP layer (Dual stack).

615

1. They both serve as a wiring and signal relay center, but an active hub additionally cleans and boosts signals.
2. Repeaters extend a network by regenerating the signal carried in the cable.
3. A primary use of modems is to enable transmission of data over greater distances with the lowest possible signal loss. Another use for modems is to interface specific equipment through different types of media.
4. Converts the electrical signal used in copper UTP network cabling to light waves used for fiber optic cabling.
5. Multiplexing means either combining (multiplex) many different signals into one serial digital data stream (transmit), or to split apart (demultiplex) a serial digital data stream into many different signals (receive).
6. Save on communications costs, inherent error correction, and inherent data security.
7. Decrease network congestion.
8. Switches operate like a one-way bridge with multiple ports by remembering the MAC address or addresses that are at each port and forward frames directly to the port, which provides the full bandwidth for each port, unlike hubs, which must share the bandwidth with each port. Each physical port is logically a separate segment, referred to as a collision domain, which greatly reduces or eliminates collisions on a network.
9. The difference between layer 2 and layer 3 switch operation is the layer at which each forwarding decision occurs.
10. An internal processor, an OS, memory, input and output jacks for different types of network connectors and a management console interface.
11. It checks the destination address and attempts to associate this address with a next hop.
12. IGP. Any two of the following: RIP, OSPF, and EIGRP.
13. Dynamic.

616

1. To provide services to network users.
2. Client-server. A client-server network is a network with services provided strictly by dedicated servers.
3. When users send files to the networked print device, the print server captures and temporarily stores those files in a section of memory or hard drive (print queue). This is needed due to the differences between the physical speed of the print device and the processing speed of the workstation generating the print job.
4. The first method is to store and print the files as the print queue receives them—first in/first out. The second method allows the print server administrator to assign a priority or precedence to files as required.
5. Workstations, acting as clients, can send requests to the server over the network, and then the server responds. Client workstations handle the presentation of data and interact with users while the server performs the workhorse operations such as sorting, indexing, and delivering data to users.
6. Avoids loading the program on each user's computer and allows central updates to take place on the server.
7. The proxy server breaks the connection between the sender and receiver, and acts as an intermediary between a workstation user and the Internet. All input is forwarded out a different port, closing a straight path between two networks and preventing a hacker from obtaining internal addresses and details of a private network.
8. DHCP centralizes IP address management on central computers that run the DHCP server program. A server has a pool of IP addresses, known as a scope, available for lease by a client for a specific period of time. The DHCP server can also assign other values such as default gateway, domain name, and DNS server.

617

1. When a broadband solution is needed.
2. UTP cable. Category 6 or 6a.
3. Whichever standard is used must be used consistently throughout the network.
4. RJ45.
5. The primary difference between these two cable standards is the sequence and placement of the green and orange wire pairs on the plug or receptacle.

6. To connect devices that operate at similar layers of the OSI model, like a router (layer 3) to another router (layer 3).
7. The crimper pushes down a hinged tab that presses against the insulation of the wire to hold it into the plug and create a strain relief.
8. It contains special materials in its insulation and cable jacket that are fire resistant certified and produce a minimum amount of smoke; this reduces poisonous chemical fumes.
9. It requires a light source (transmitter), a transmission medium (cable), and a sensor (receiver).
10. Fiber optic cable systems have more potential bandwidth than any system.
11. Fiber is almost impossible to tap without affecting the transmission enough for authorized users to notice. In addition, fiber does not radiate energy. This feature makes electromagnetic field sensing eavesdropping equipment useless.

618

1. A physical topology acts as a map; it shows how the devices on the network physically connect, and A logical topology defines the way in which devices communicate and data transmission occurs throughout the network.
2. Type of equipment the network requires, capabilities of the equipment, growth of the network, and management of the network.
3. Bus, star, and ring.
4. Cost, scalability, bandwidth, ease of installation, and ease of troubleshooting.
5. A single cable connects all devices in a straight line.
6.. They are no longer a recommended option for new installations, network is down if the backbone breaks, only a limited number of devices can be included, difficult to isolate location of a problem, and sharing the same cable means slower access time.
7. Data packets can travel at greater speeds, there are no collisions, it is easier to locate problems with devices and cable, and no terminators are needed.
8. It can be an active or passive device like a hub or an intelligent device such as a router, switch, or a bridge.
9. It is easy to add more devices as your network expands, the failure or malfunction of one cable will not bring down the entire network, the centralized device provides centralized management, it is easy to troubleshoot device and cable problems, and it supports faster network transmission speeds than ring and bus.
10. The Internet.
11. Full mesh topology occurs when every station has a circuit connecting it to every other station in the network. Partial mesh topology is when some nodes connect with all the other nodes using direct links, but some only connect to one or two stations.
12. Bus topology

619

1. The main difference is that in CSMA/CA the transmitter station listens for network silence and then sends a warning signal telling all other stations not to transmit, before it sends its packet.
2. Because of the single bus architecture of the radio transmission medium.
3. MIMO increases the capacity of wireless communications by implementing multiple paths for sending and receiving data over the same channel.
4. 802.11n supports a max of four paths with a channel width of 40 megahertz and 802.11ac doubled the amount of MIMO streams from four to eight paths and increased the channel widths to 80 megahertz.
5. It is backwards compatible with 802.11a and 5 gigahertz 802.11n. Because they also operate in the 5 gigahertz frequency band.
6. WNIC and access point.
7. Because it does not perform any type of switching function. It only broadcasts signals out, amplifies incoming signals, and forwards signals throughout the network.
8. Training for both the users and the administration; current and future technologies available for the installation; current and future amount of users on the network; amount of resources the network must support; access requirements for the wireless network; and integrity and security requirements of network data.

9. Range limitations. Readjust access point locations to allow for convergence. This will allow mobile wireless users to have constant connectivity as they move from access point to access point. They are susceptible to common causes of interference that can reduce throughput and range. Install the access point in an area where large steel structures such as shelving units, bookcases and filling cabinets do not block the radio signal to and from the access point. Furthermore, install the access point away from devices that operate at the same frequency as the access point, which can cause signal interference.
10. It can help add an obstacle in securing the network from intruders.

620

1. A protocol analyzer generates, monitors, and captures data traffic moving across a network connection. Once the protocol analyzer receives and deciphers the network data according to the protocol rules, it displays the results.
2. Counter—this component counts bytes, frames, and errors as the NIC processes them; filter—discards frames based on filter definition or activates a trigger based on trigger definition; buffer—this component stores all frames based on the user configuration inputs; protocol analyzer CPU—this specialized processor processes the frames based on the selected test and the user configuration inputs; and personal computer CPU—this processor provides the operating system capabilities, user interface and display information based on the user inputs.
3. They can be used to display and store only the data you are interested in analyzing. Also, they can be used to exclude specific types of frames.
4. It generates a constant stream of data, a single burst of data or a repetitive burst of data. Data stream can include random data, all zeros, all ones and other patterns.
5. Connection statistics.
6. Trace route.

Complete the unit review exercises before going to the next unit.

Unit Review Exercises

Note to Student: Consider all choices carefully, select the *best* answer to each question, and *circle* the corresponding letter.

Do not return your answer sheet to AFCDA.

41. (610) A network encompassing two or more computer workstations connected by one or more types of media is defined as a
    a. wide area network (WAN).
    b. local area network (LAN).
    c. metropolitan area network (MAN).
    d. virtual private network (VPN).

42. (610) Which type of network uses long-distance communication links to connect networks separated by large geographical distances?
    a. Wide area network (WAN).
    b. Local area network (LAN).
    c. Metropolitan area network (MAN).
    d. Virtual private network (VPN).

43. (610) Which type of network proves an encrypted means of transporting private data through the Internet?
    a. Wide area network (WAN).
    b. Local area network (LAN).
    c. Metropolitan area network (MAN).
    d. Virtual private network (VPN).

44. (611) Which open system interconnection (OSI) model layer handles data in bits?
    a. Physical.
    b. Network.
    c. Data link.
    d. Transport.

45. (611) Logical addressing of devices occurs at open system interconnection (OSI) model layer
    a. one.
    b. two.
    c. three.
    d. four.

46. (611) Which Session layer feature involves the periodic insertion of recovery points into large data transfers to enable recovery point restart in case of failure?
    a. Checkpointing.
    b. Checksum.
    c. Flow control.
    d. Error control.

47. (611) Which open system interconnection (OSI) model layer ensures that information sent from the Application layer of one system will be readable by the Application layer of another system?
    a. Session.
    b. Network.
    c. Presentation.
    d. Transport.

48. (611) An example of a video compression standard is
    a. motion picture experts group–4 (MPEG–4).
    b. joint photographic experts group (JPEG).
    c. graphics interchange format (GIF).
    d. G.711.

49. (611) What is the process of adding headers and trailers to data as it passes from the upper open system interconnection (OSI) model layers to the lower layers?
    a. Decapsulation.
    b. Encapsulation.
    c. Encryption.
    d. Decryption.

50. (612) Which transport protocol is connectionless-oriented?
    a. File transfer protocol (FTP).
    b. User datagram protocol (UDP).
    c. Transmission control protocol (TCP).
    d. Simple mail transfer protocol (SMTP).

51. (612) The scripting language that forms the building blocks of all websites is
    a. hypertext markup language (HTML).
    b. hypertext transfer protocol (HTTP).
    c. Internet protocol (IP).
    d. Javascript.

52. (612) What provides an automated means of assigning a unique Internet protocol (IP) address to every device on a network?
    a. Domain name system (DNS).
    b. Hypertext transfer protocol (HTTP).
    c. Simple network management protocol (SNMP).
    d. Dynamic host configuration protocol (DHCP).

53. (612) On which transmission control protocol/Internet protocol (TCP/IP) layer do TCP and user datagram protocol (UDP) reside?
    a. Network Access.
    b. Application.
    c. Transport.
    d. Internet.

54. (612) Which transmission control protocol/Internet protocol (TCP/IP) layer defines end-to-end connectivity between host applications?
    a. Network Access.
    b. Application.
    c. Transport.
    d. Internet.

55. (612) Which port does Telnet use?
    a. 7.
    b. 20.
    c. 23.
    d. 53.

56. (612) Which port does hypertext transfer protocol (HTTP) use?
    a. 21.
    b. 80.
    c. 110.
    d. 443.

57. (612) Which port does hypertext transfer protocol secure (HTTPS) use?
    a. 21.
    b. 80.
    c. 110.
    d. 443.

58. (612) Which protocol is valuable for assessing the network by enabling services such as ping?
    a. Internet protocol (IP).
    b. Address resolution protocol (ARP).
    c. Hypertext transfer protocol (HTTP).
    d. Internet control message protocol (ICMP).

59. (612) Which local area network (LAN) protocol uses carrier sense multiple access/collision detection (CSMA/CD) to avoid collisions while transmitting data?
    a. Fiber distributed data interface (FDDI).
    b. Internet protocol (IP).
    c. Token Ring.
    d. Ethernet.

60. (613) What is the unique identification number a network interface controller (NIC) provides to a personal computer?
    a. Media access control (MAC) address.
    b. Institute of Electrical and Electronics Engineers (IEEE) address.
    c. Organizationally unique identifier (OUI) address.
    d. Serial attached small computer system interface (SAS) address.

61. (613) Which logical addressing method is *widely* used throughout the public Internet?
    a. Internet Protocol version 2 (IPv2).
    b. Internet Protocol version 4 (IPv4).
    c. Internet Protocol version 6 (IPv6).
    d. Internet Protocol version 8 (IPv8).

62. (613) What is the *maximum* value of an octet in Internet protocol version 4 (IPv4)?
    a. 239.
    b. 254.
    c. 255.
    d. 256.

63. (613) Which class allows for a *maximum* of 254 hosts per network?
    a. Class A address.
    b. Class B address.
    c. Class C address.
    d. Class D address.

64. (613) The default subnet mask for a Class C address is
    a. 255.255.255.255.
    b. 255.255.255.0
    c. 255.255.0.0.
    d. 255.0.0.0.

65. (614) Which protocol provides a nearly unlimited number of Internet protocol (IP) addresses?
    a. Transmission control protocol (TCP).
    b. Internet protocol version 4 (IPv4).
    c. Internet protocol version 6 (IPv6).
    d. Hypertext transfer protocol (HTTP).

66. (614) Which Internet protocol version 6 (IPv6) transition method involves providing complete support for both IPv6 and Internet protocol version 4 (IPv4)?
    a. Dual Internet protocol (IP) layer.
    b. IPv4 compatible IPv6 addresses.
    c. Automatically tunneling of IPv6 over IPv4.
    d. Configured tunneling of IPv6 over IPv4.

67. (614) What Internet protocol version 6 (IPv6) transition method involves encapsulating IPv6 packets within IPv4 headers to carry them over IPv4 routing systems?
    a. Dual Internet protocol (IP) layer.
    b. IPv4 compatible IPv6 addresses.
    c. Automatically tunneling of IPv6 over IPv4.
    d. Configured tunneling of IPv6 over IPv4.

68. (615) Which network device converts the electrical signal used in copper unshielded twisted pair (UTP) network cabling to light waves used for fiber optic cabling?
    a. Media converter.
    b. Switch.
    c. Modem.
    d. Router.

69. (615) Which is an advantage to using multiplexers in a network?
    a. Helps boost signal strength.
    b. Filters out noise from signal.
    c. Contains inherent error correction.
    d. Acts as a local firewall.

70. (615) Switching conducted at the layer 2 category is based solely upon what information?
    a. Source address.
    b. Destination address.
    c. Internet protocol (IP) address.
    d. Media access control (MAC) address.

71. (615) How do routing algorithms determine the optimal path to a destination?
    a. Use of metrics.
    b. Use pre-programmed routing tables.
    c. Send to the next hop that is first available.
    d. Path is predetermined by sender.

72. (616) Which kind of server is set aside to perform a specific task or function all the time?
    a. File server.
    b. Network server.
    c. Dedicated server.
    d. Intranet server.

73. (616) Which type of server is sent a query to convert a domain name to an Internet Protocol (IP) address when the domain name system is typed into a Web browser?
    a. Applications.
    b. Communications.
    c. Domain name system.
    d. Proxy.

74. (616) Which type of server prevents a hacker from obtaining internal addresses and details of a private network?
    a. Proxy.
    b. Print.
    c. File.
    d. Mail.

75. (617) Which is the effective range for unshielded twisted pair cable?
    a. 100 feet.
    b. 100 meters.
    c. 300 feet.
    d. 300 meters.

76. (617) Which type of network communication medium has combined features of twisted pair and coaxial cable?
    a. Unshielded twisted pair (UTP).
    b. Shielded twisted pair (STP).
    c. Plenum cable.
    d. Fiber optic.

77. (618) Which network topology consists of a single cable that connects devices in a straight line?
    a. Star.
    b. Bus.
    c. Ring.
    d. Mesh.

78. (618) Which network topology combines two or more different physical topologies in a single network?
    a. Star.
    b. Mesh.
    c. Dual Ring.
    d. Hybrid.

79. (618) What does a logical topology define?
    a. How cables should connect.
    b. How data should transfer.
    c. Placement of network devices.
    d. Type of wiring.

80. (619) What do wireless local area networks (WLAN) use to address network collisions?
    a. Checksums.
    b. Checkpointing.
    c. Carrier sense multiple access collision detection (CSMA/CD).
    d. Carrier sense multiple access collision avoidance (CSMA/CA).

81. (619) Which two wireless standards are backwards compatible with 802.11ac?
    a. 802.11a and 802.11n.
    b. 802.11b and 802.11g.
    c. 802.11g and 802.11n.
    d. 802.11a and 802.11g.

82. (619) In which wireless network design phase should you ensure frequencies will *not* interfere with military frequencies used in the area?
    a. Planning.
    b. Securing.
    c. Deployment.
    d. Management & support.

83. (619) Why should you disable the service set identifier (SSID) broadcast in a wireless network if possible?
    a. Increases data capacity.
    b. Speeds up data transfer.
    c. Adds obstacle for intruder.
    d. To avoid potential electromagnetic interference (EMI).

84. (620) Which component of a protocol analyzer discards frames based on its definition or activates a trigger based on the trigger definition?
    a. Filter.
    b. Buffer.
    c. Counter.
    d. Central processing unit.

85. (620) Which protocol analyzer capture filter would you use if you desire to see traffic between specific hosts?
    a. Protocol.
    b. Frame attributes.
    c. Internet Protocol (IP) address.
    d. Media access control (MAC) address.

86. (620) Which protocol analyzer test window reports errors that occur at the Physical layer such as bad frame check sequence (FCS), short frames, and jabbers?
    a. Media access control (MAC) node statistics.
    b. Connection statistics.
    c. Protocol statistics.
    d. Node discovery.

87. (620) Which active test on a protocol analyzer do you use to see the path that the packets are traveling and the time it takes the packets to compete the trip?
    a. Packet internetwork groper (ping).
    b. Traffic generator.
    c. Route generator.
    d. Trace route.

Please read the unit menu for unit 4 and continue ➔

Unit 4. Information Systems Security

UNFORTUNATELY, NETWORK ATTACKS and breaches are a continuous, non-stop threat. As time passes, these attacks become more sophisticated by using new technologies and methods. Cyber-attacks to healthcare networks and systems are climbing because hospitals store massive amounts of sensitive information, which is a prime target for attackers, and they are known for being "soft" targets. Medical devices are being developed continuously to store and transmit more information. It is important that you understand some basic security fundamentals so that you do not contribute to or create any vulnerabilities of the network while carrying out your duties. As BMETs continue to transition to taking on more IT tasks as it pertains to medical devices, it is important that you keep in mind that security of the network is vital to MTF and military operations. Your local systems office and DHA are responsible for securing networks at MTFs, but there are certain locations and deployments where BMETs may be tasked to do more.

4–1. Network Hardening

The purpose of a network is to connect multiple users together and allow them to access serving systems. This very purpose is what makes networks vulnerable to attacks. As security incidents continue to increase steadily, information system security has become a critical area of concern. This section will cover threats, vulnerabilities, and network hardening.

621. Principles of threats and vulnerabilities

The objective of computer security is to ensure the employment of countermeasures to protect and maintain the confidentiality, integrity, availability, and nonrepudiation of resources and data processed throughout the network. It is important that you understand these terms in regards to information systems security. The following table provides a description for each term.

Term	Description
Confidentiality	Set of rules that limit access of information to *only* those authorized to view the data in question.
Integrity	Involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that unauthorized people cannot alter the data.
Availability	Reliable access to information for authorized user.
Nonrepudiation	Not being able to deny who performed a particular network action, such as sending a message.

Under RMF, there are three core security objectives used to determine a system's risk exposure: confidentiality, integrity, and availability (CIA). Assigning a system the appropriate CIA value (categorizing a system), is at the center of properly applying RMF. A system's categorization determines what security controls will be put in place.

Information system owners assign system risk values (e.g., low, moderate, or high) in each of the three categories and then use those combined risk values to derive a set of tailored cybersecurity controls against which to test the system.

A rating of "low" indicates a security breach would cause limited damage to organizations, individuals, or operations; a "moderate" rating indicates the potential for serious damage in those areas; and a "high" rating predicts severe or catastrophic adverse effects in case of a security breach.

Vulnerabilities

A vulnerability is a problem, or weakness, in a computer system that allows an intruder or hacker to exploit the system's information security. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker's access to the flaw, and attacker's capability to exploit the flaw. The following table describes *general* vulnerabilities.

Vulnerability	Deficiency/Weakness
Physical	Weaknesses in the control and accountability of physical access to controlled areas. The controls can be implemented either through automated or manual means.
Environmental	Weaknesses or deficiencies in maintaining the environmental stability, control, and safety of the data processing area.
Personnel	Deficiencies in the controls that make sure all personnel who have access to sensitive information have the required authority and appropriate clearance.
Hardware	Deficiencies with installation, operating, and maintaining the systems and network hardware.
Software	Deficiencies in the control of network and computer operating systems, software versions, data, and related security software.
Media	Deficiencies in the control and maintenance of magnetic and hard copy media.
Network Communications	Deficiencies in the security and controls of the various communications mediums used to transmit data between the servers and network users.
Procedural	Deficiencies in the development and maintenance of procedures, rosters, and forms, which provide guidance, definition of responsibilities, and identification of personnel.

The following table outlines some common network and software vulnerabilities found in organizations.

Vulnerability	Description
Cleartext Credentials	Older protocols offer a false sense of security. Protocols such as FTP, Telnet, and Post Office Protocol (POP) 3, require you to use a valid user name and password, but both the user name and password are sent in cleartext (unencrypted, readable data), so the credentials can be captured.
Unencrypted Channels	Using unsecure transmission when the user should be using more secure, encrypted channels. For example, performing a bank transaction online using HTTP instead of HTTPS.
RF Emanation	Radio waves penetrate structures, which can possibly lead to an attacker gaining access to information with the proper equipment.
Unpatched and Legacy Systems	Since threats are always changing, manufacturers release patches so that you can update equipment to resist current threats. If the system stays unpatched, it is obvious that it is now open to attack. Legacy systems are older systems that the manufacturer no longer supports. These systems are extremely problematic since, not only do they not have new patches installed, they have been in market for a long time and attackers are typically more proficient attacking older technology. If you cannot avoid using unpatched or legacy systems, then it is important to isolate it from the network to decrease the vulnerability of an attack.

Vulnerability	Description
Running Unnecessary Services	When OSs run they use services to listen to open TCP or UDP ports, which leaves the system open to attacks. Computers often have a large number of services simultaneously running. Attackers sometimes use services to plant malware. Closing unnecessary services closes any ports that do not need to be open.

It is unlikely that a network can ever achieve total information system security, even with controls and safeguards in place. New threats and vulnerabilities continue to emerge at a rapid pace, so network administrators and technicians with privileged access to the MTF network must always work to identify and analyze threats, so they can maintain an appropriate level of protection through established safeguards based on security requirements. DHA and local program managers develop and coordinate the schedules and details of network assessments. The details of a network risk assessment depend on the system design, environment, and classification of data on that network.

Threats

Computer security threats cause harm to information (data) or to the information system that processes that data. Threats exist from natural, environmental, and human. The following table discusses each briefly.

Threat	Description
Natural	Nature causes natural threats such as earthquakes, floods, hurricanes, snow/ice, tornado/windstorms, lightning, or severe storms. Every location is subject to different types of threats and must have precautionary measures to minimize system damages.
Environment	Environmental threats result from man-made items in the environment. These can include flaws in building construction, improper implementation of utilities, inadequate wiring, and poor housekeeping practices. Program managers along with the facility management should work together to identify environmental inadequacies.
Human	Human threats can be either intentional or unintentional. Intentional threats are deliberate attacks by an individual to degrade or damage information systems, network resources, or information. Reasons for intentional attacks could include degrading system integrity, revenge, or personal gain. Unintentional threats cause inadvertent damage to information systems due to lack of training, carelessness, or accidental intrusions. A computer system is no more secure than the persons responsible for its operation are. Malicious individuals have regularly penetrated well-designed, secure computer systems by taking advantage of the carelessness of trusted individuals or by deliberately deceiving them.

There are many types of human threats concerning computer systems. Let’s take a brief look at some common human threats.

Malicious software

One of the most common computer security threats is malicious software. Malicious software can destroy data on computers that contract them and can spread from computer system to computer system. Viruses can reformat a hard disk; erase programs and files; add unrecognizable characters to files; or destroy disk directories and file allocation tables preventing the computer from using the tables or directories to locate files. Some software can mutate, evolve, or escape detection by some antivirus programs. One of the newest threats comes from spyware.

Spyware is computer software that *collects personal information* about users *without their informed consent*. It secretly records personal information with a variety of techniques that includes collecting cookies, logging keystrokes, recording Internet web browsing history, and scanning documents on the computer’s hard disk.

Some spyware designs retrieve passwords and financial details or record Internet search history for targeted advertising. Spyware attempts to collect different types of information. Some variants

attempt to track the Web sites a user visits and then send this information to an advertising agency. More malicious spyware variants attempt to intercept passwords or credit card numbers as a user enters them into a Web-based form or online applications.

The spread of spyware has led to the development of an entire anti-spyware industry. These products remove or disable existing spyware on the computers; anti-spyware is installed on computers to prevent the installation of spyware. To protect against viruses and spyware, use good antivirus and anti-spyware software products as well as the following practical tips:

- Take precautions with any removable media (CD-ROMs or flash drives). Viruses can spread through infected disks; do *not* share disks unless it is necessary. Virus check any discs before accessing files on it.
- Only use original software and do not share software with anyone else or put copies of someone else's software on another computer.
- Always back-up files. If a computer is infected with a virus that wipes out the hard drive, the data can still recover up to the last backup.
- Schedule time to scan your system's hard drive. Scan removable media for viruses before each use. Hard drive media scans can be automated if antivirus software is configured properly.

Data spillage

Data spillage occurs by placing a higher classified level of data on a lower classification level system/device. This can happen when a user takes a file, such as a word document, and copies it to removable media (e.g., DVD or CD) from the Secret Internet Protocol Router Network (SIPRNet) and then takes that media and loads the data onto a Non-classified Internet Protocol Router Network (NIPRNet) computer.

Backdoor

A backdoor in a computer system, a cryptosystem, or an algorithm, is a method of bypassing standard authentication, securing remote access to a computer, obtaining access to plain text, and so on, while attempting to remain undetected. A special form of asymmetric encryption attack, known as a kleptographic attack, *cannot* be reverse engineered (deconstructed to reveal its design or architecture) even after it is detected and analyzed.

The backdoor may take the form of an installed program or could be a modification to an existing program or hardware device. A specific form of backdoor is a rootkit, which replaces system binaries and/or hooks into the function calls of an operating system to hide the presence of other programs, users, services, and open ports. It may also fake information about disk and memory damage.

Denial-of-service attack

Unlike other exploits, denial-of-service (DoS) attacks are not used to gain unauthorized access or control of a system. Instead, it simply renders the system unusable. Attackers can deny service to individual victims, for example, by deliberately entering a wrong password enough consecutive times to cause the victim's account to lock or they may overload the capacity of a machine or network and block all users at once. The most common DoS attack is when the attacker uses his computer to flood a targeted server with so many requests that it gets overwhelmed and stops working. The goal of the attacker is send as many packets as possible. Distributed denial-of-service (DDoS) attacks is when an attacker has single control of a large number of compromised hosts, commonly referred to as "zombie" computers, used as part of a botnet (a network of private computers infected with malicious software) to launch coordinated attack against a target. These attacks flood a target system with network requests in an attempt to render it unusable through resource exhaustion. Another technique to exhaust victim resources is through an attack amplifier, where the attacker takes advantage of poorly designed protocols on third-party machines, such as NTP or DNS, in order to instruct these

hosts to launch the flood. Some vulnerabilities in applications or operating systems can be exploited to make the computer or application malfunction or crash to create a DoS.

Direct-access attacks

An unauthorized user gaining physical access to a computer can perform many functions or install different types of devices to compromise security, including operating system modifications, software worms, key loggers, and covert listening devices. The attacker can also easily download large quantities of data onto backup media. Another common technique is to boot an operating system contained on a CD-ROM or other bootable media and read the data from the hard drive(s) this way. The only way to prevent this is to encrypt the storage media and store the key separate from the system. Direct-access attacks are the *only* type of threat to physically isolated computers in most cases.

Eavesdropping

Eavesdropping is the act of secretively listening to a private conversation, typically between hosts on a network. For instance, the Federal Bureau of Investigations (FBI) and the National Security Agency (NSA) have used programs such as Carnivore and NarusInsight to eavesdrop on Internet service providers systems. Even computers that operate as a closed system (i.e., with no contact to the outside world) can be eavesdropped upon by monitoring the faint electromagnetic transmissions generated by the hardware.

Man-in-the-middle

In a man-in-the-middle attack, an individual interjects into communication between two systems or parties, covertly intercepting traffic. The attacker can then read or in some cases change the data and then send the data forward. To the two unsuspecting systems or parties, it will appear as if they are communicating directly with each other, but in reality, they are sending everything to the attacker. Then he or she can read or manipulate the data before forwarding it to its original target.

Spoofing

Spoofing of user identity is a situation in which a person or program successfully masquerades as another by falsifying data.

Information disclosure

Information disclosure (i.e., privacy breach or data leak) describes a situation where information thought to be secure is released in an untrusted environment.

Privilege escalation

Privilege escalation occurs when an attacker gains elevated privileges or access to resources that were once restricted to them.

Port scanning

Port scanning is the act of systematically scanning a computer's ports. Since a port is a place where information goes in and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer. This is very similar to a thief roaming the neighborhood and checking every door and window at each house to see which ones are open or locked. Port scanning software simply sends out a request to connect to the target computer on each port sequentially and makes a note of which ports responded or appeared open to more in-depth probing. The following table lists some common types.

Port Scans	
Type	**Description**
Vanilla	The vanilla scan is the *most* basic and attempts to scan *all* 65,535 ports.
Strobe	Scanner conducts a more focused scan looking *only* for known services to exploit.

Port Scans	
Type	**Description**
Fragmented Packets	The scanner sends packet fragments to see which get through simple packet filters in a firewall.
Sweep	Scanner connects to the *same* port on more than one machine.
FTP Bounce	In an FTP bounce scan, the scanner goes through an FTP server in order to *disguise* the source of the scan.
Stealth	In a stealth scan, the scanner *blocks* the scanned computer from recording the port scan activities.
TCP	TCP scans work on the principle that computers connected to the Internet predominantly communicate with each other using the TCP/IP suite. TCP port numbers are specific addresses by which distant applications locate each other once the computers establish network connection. TCP is a connection-oriented protocol offering reliable connectivity, and a scanner attempts to connect to a server and listen on the *specified* TCP port numbers.
UDP	UDP scans work on the principle that UDP is a connectionless-oriented protocol. This type of port scan is just looking for open UDP ports.
Synchronous (SYN) scan	A SYN scan is also known as a half-open scan, since, in this type of scan, the TCP connection is not yet completed. A SYN packet is sent just to see if the distant host is listening. This sending will go undetected by the impacted host or server because the TCP handshake is incomplete. In this type of attack, the server is flooded with TCP-SYN packets.

Common methods used to prevent unauthorized port scanning include using access control lists (ACL), setting up black hole firewalls, keeping software current, and managing unused ports. These are explained in the following table.

Preventing Port Scans	
Method	**Description**
ACL	ACLs are used to block inbound and/or outbound traffic (where suspicious traffic is internal). ACLs will be covered in more detail later in this section.
Black hole firewalls	Most firewalls can be configured to discard packets addressed to forbidden hosts or ports silently, resulting in small or large “black holes” in the network. Firewalls will also be discussed in later in this section.
Current software	Keep all security software up to date (firewalls, proxies, and antivirus). This could be ensuring the latest versions of security patches and software are loaded. Always ensure the version is properly authorized to be loaded by the appropriate higher authorities, DHA or Air Force depending on organization structure. Never download a software patch or version from the Internet and load onto any of your systems. **NOTE**: All software must be properly tested and approved *prior* to installing.
Unused ports	Keep unused ports closed. Again, the idea here is to give the attacker the least opportunity to break into the network. Just as you do for your home, make sure all of the doors are locked!

Port scanning itself is not a malicious act; yet, it is a common intrusion method. There is no way to prevent an external port scan from occurring on a computer while on the Internet because, in reality, access to a networked computer system requires a connection to an open port. This access requirement and subsequent connection opens a door to this computer system, which may grant an intruder access to the network too.

622. Principles of network and application security

Just as a gate guard at a military installation protects the base from infiltration, a system must be in place on the network to ensure that personnel wanting access to the network have authorization to have that access. We will cover general access considerations, authentication, passwords, encryption, and public key infrastructure (PKI). Let us first look at identification and authentication.

Identification is the process where an individual or network device asserts a specific identity and authentication is the process of verifying the identity of a user or network device.

In terms of day-to-day computer usage, identification takes place when one inserts their common access card (CAC) into a computer and then enters a personal identification number (PIN). Authentication takes place once the network validates the identification presented and only allows access to authorized users.

General access considerations

There are three central considerations for granting access to the network. Personnel should have the following:

1. A valid need to access the information on the network.
2. The security clearance equal to or greater than the information available.
3. The proper training (such as Cyber Awareness training) to access the network and handle the information.

Security requirements

The use of security requirements is vital to maintaining confidentiality, integrity, availability, and non-repudiation of information systems. These security requirements include authentication, encryption, and data integrity.

Authentication

To ensure authentication, a network antispoofing capability to preclude unauthorized use of data (impersonating, masquerading, piggybacking, and mimicking are forms of spoofing) should be used. User password (i.e., log-on, screen saver) protection, official guidance, and any automated controls require adherence at all times. If any vendor-selected default passwords exist on the medical devices, you are required to *change* them during system installation or immediately thereafter. Ensure you never left null or blank passwords for system access.

The use of remote access for changing passwords must be severely restricted, unless a strongly encrypted VPN protects the entire session. System administrators must maintain a complete list of all people, devices, and locations authorized to change passwords remotely. Disable remote changing of device maintenance port passwords and do not transmit unencrypted passwords over any network. This is especially critical for system and device maintenance port passwords. Normally, users can change passwords for Web applications, but the logon and password management screens require encryption with Transport layer security (TLS), which is a cryptographic protocol. *Never* e-mail forgotten passwords to any user or technician.

Encryption

Encryption is the process of encoding data in such a way that *only* authorized personnel can access it and all others cannot. Encryption does not prevent interception, it simply denies access to the content should an attacker intercept it. With encryption, the information or message (data) in plaintext (readable and unencrypted) is encrypted using an encryption algorithm (a cipher) which turns the plaintext to ciphertext, which can then be read *only* if decrypted. In principle, it is possible to decrypt a message without possessing the key, but it would require considerable resources and skills. The authorized recipient easily decrypts the message with the key that the originator provided if using symmetric encryption or their private key if using asymmetric (public key) encryption. Encryption protects data in transit (i.e., data transferred on networks, mobile telephones, or Bluetooth devices)

and in storage. Users should always encrypt sensitive data when transmitted across networks to protect against eavesdropping of network traffic by unauthorized users. The NSA approved using encryption for all classified traffic transmitted across unsecured channels. It also approves the encryption for tunneling SECRET and TOP SECRET data over networks that have a lower classification or releasability restrictions. Tunneling solutions are usable to transmit sensitive unclassified data over unclassified networks according to the NSA protection profile.

Data integrity

To ensure data integrity, standardized transmission check sums should be throughout the network. In case of an incident or catastrophic failure, the use of routine data backup helps ensure data integrity.

Public key infrastructure

DODI 8520. 2, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling*, directs the use of PKI by the DOD. PKI is a framework established to issue, maintain, and revoke public key certificates, including systems, processes, and people. PK certificates provide digital signature and encryption capabilities, which address the security *core* objectives by the following security services.

Security Service	Description
Identification and Authentication	PKI provides for identification and authentication through digital signature. If the signature is valid, the relying party (i.e., the person or system relying on the presented certificate for authentication or other security services) has assurance that the entity participating in the transaction is the subscriber (i.e., the identity asserted by the certificate).
Data Integrity	PKI provides for data integrity through digital signature of information. If the recipient of digitally signed information is able, verify the signature on the information using the public key of the certificate used to generate the signature, and then the recipient knows that the content has *not* changed since its signing.
Confidentiality	PKI provides confidentiality through encryption. If the public key in a certificate is used to encrypt information, only the associated private key, held (and kept secret) by the entity named in the certificate, can decrypt that information.
Technical Non-Repudiation	PKI assists with technical non-repudiation through digital signatures. Technical non-repudiation can be considered a form of attribution, namely that the digitally signed information can be attributed to the entity identified in the certificate used to generate the signature

The CAC provides access to the capabilities of PKI. The CAC and your PIN are your keys to certificates that were loaded onto your card upon issue. Certificates are special files that contain information about you, the one who issued the certificate, and when it expires. It also contains your keys. The purpose of the certificates is for identification, signing e-mail, and encryption.

One of your certificates allows you to sign e-mail. This supports non-repudiation, as you must type in your pin prior to sending the e-mail. Encryption supports data confidentiality and the certificate allows for encryption of your e-mail. Encryption, although not a secure solution alone, is a powerful tool used to secure the privacy and integrity of data. There are two primary forms of encryption: asymmetric and symmetric. Public key encryption is a cryptographic asymmetric system that uses two keys—public to encrypt the data and private to decrypt the data. Private key or symmetric encryption uses only one secret key to perform the encryption and decryption process. If a device, personal computer, or laptop is lost or stolen, it is important that the government data contained on the device be as secure as possible to avoid compromise. The best means to protect the data is by encrypting the files on the device itself.

Normally certificates are set to *expire* after three years. If you still need to continue using the certificate after expiration, it must be reissued. If you have encrypted e-mails, and your certificates expire, your e-mails will become inaccessible. To regain access to them, you will have to retrieve your old certificates, which is a separate process from getting your certificate reissued.

After receiving your CAC and certificates, you must upload your public keys to the global access list (GAL). The GAL serves as the public key repository, allowing access to and use of the keys by other users. This part of the process is where verification takes place.

Access prevention

The purpose of access control systems and practices is to protect information from the threats of unauthorized disclosure, modification, or destruction. Access controls fortify CIA by identifying and authenticating both data and users. Access control is a broad topic that incorporates many basic security practices.

Access controls related to information security fall into the following *two* categories:

1. Technical controls, such as passwords and encryption that are part of normal network security.
2. Administrative controls, such as segregation of duties and security screening of users.

These types of access controls may overlap with other personnel and information security procedures. The following paragraphs are some sound practices involving technical and administrative controls useful in managing information systems.

Access authentication

Use strong authentication to restrict access to critical systems, processes, and sensitive data; control remote access to networks; and limit access to control functions of critical network devices. Strong authentication methods include, but not limited to, one-time passwords, digital certificates, and biometrics. One-time passwords change for each user access session and are generated by programmable devices. Control access to the programmable device through a reusable password for additional protection. Digital certificates authenticate the identity of the user. Biometrics refers to an identification process based on physical or behavioral characteristics unique to a user, such as fingerprints, keystroke patterns, patterns associated with the voice, retina or iris, and facial characteristics.

Securing desktop systems

Protect against loss or corruption of critical process logic and sensitive data residing on desktop systems. Because of the susceptibility of desktop systems to theft, access by unauthorized people, and destruction or failure, transfer the storage of sensitive data or critical processes on desktop systems to servers located in secure areas. If business reasons require sensitive data or critical processes to reside on desktop systems, protect them by access controls, encryption, and periodic backup procedures.

Control access to desktop systems connected to critical networks or network segments, and to desktop systems supporting sensitive data or critical operation processes, by a power-on logon ID and password combination or locked office. Most desktop systems have a feature that requires a BIOS password to gain access when powered up. Implement this feature to prevent unauthorized people from gaining control of desktop systems connected to critical networks or network segments and those supporting sensitive data or critical processes.

Equip desktop systems with an automatic time-out feature that makes them inaccessible to an unauthorized individual after a period of keyboard inactivity. Simple examples of time-out features are password-protected screen savers and automatic logoffs. The sensitivity of the application determines the length of the period of inactivity that triggers the time-out feature.

Securing notebook and laptop computers

Password-protect access to notebook and laptop computers and consider encryption of all sensitive files on these computers' hard drives. Because portable computers are easy to steal, minimize opportunities for thieves to obtain sensitive information that may be stored on them.

The first line of defense is to require a logon ID and password combination to gain access to the computer's OS. Encrypt sensitive files so that even if the portable computer is stolen and successfully penetrated, thieves cannot access the data.

Securing utility programs

Control utility programs that provide unrestricted access to sensitive data. Some utility programs provide unrestricted access to system commands and data to "super users" (e.g., system administrators). When implementing software that gives super users these capabilities, provide compensating controls, such as segregation of duties to limit their capability for autonomous actions. As an additional precaution, review logs of all super user actions frequently. Provide the same level of physical and logical access control to backup files of sensitive data, particularly those stored at offsite locations, as you provide to the original versions of the system.

623. Basics of firewalls

The firewall is a network security tool that often receives more attention than any other does. As the name implies, firewalls serve as a powerful barrier for the network and are often amongst the first security tool encountered when interfacing with another network.

Network security does not simply begin and end with installing and activating a firewall. While firewalls are a must-have device to protect hosts and network systems, they do not work alone and must be part of a greater ensemble of security tools that we actively employ and manage to best protect our network and achieve the defense-in-depth mindset.

Firewall overview

In the past, the construction of buildings and homes were so close to each other that when a fire occurred in one building, it would easily spread to the others before it could be contained. To decrease the risk of numerous destroyed buildings, construction crews built firewalls. These firewalls were brick walls built in between each structure to contain the fire in one building. The same theory applies when we think of firewalls in networks.

A firewall is an access control method that acts as a barrier between two of more segments of a network or infrastructure. Just like with any access control method, there are things a firewall can and cannot do. Firewalls perform the following:

- Block unauthorized traffic from entering the network.
- Direct inbound traffic to public or internal networks.
- Hide vulnerable systems from the Internet.
- Log traffic to and from internal servers.
- Provide an audit and alarm system for intrusion detection.
- Hide system names and network topologies.

Firewalls *cannot* prevent:

- accidental or deliberate disclosure of information,
- threats to the integrity of information that may arise prior to it reaching the firewall, or
- unauthorized access to systems already inside the firewall.

Internet protocol firewall

Physically, an IP firewall consists of one or more routers and host machines with filtering software containing a series of rules that accept or reject packets of information, connection types, or

application specific communications attempting to cross the firewall. You may put an IP firewall between the Internet and your organization's Internet servers or Intranet network segments.

There are four categories of IP firewalls:

1. Personal small office/home office (SOHO).
2. Corporate enterprise.
3. Network-level firewall.
4. Application-level firewall.

Personal/SOHO firewalls

Installing a personal firewall at home is an excellent way to learn how one works. A personal firewall is usually software-based, very susceptible to hacking, and typically protects only the local computer. The personal/SOHO firewall takes little to no system administration experience.

Corporate/enterprise firewalls

There are many differences between personal/SOHO and corporate enterprise firewalls. One of the differences is corporate/enterprise firewalls use two or more NICs to separate the bad people from the good ones. The enterprise firewall is an appliance (a combination of software and hardware) and uses two separate protocol stacks for enhanced security. Many enterprise firewalls also include Secure Split (DNS)/Mail architecture, which means that one or more name servers reside behind the firewall and contain an "inside" hostname and IP address information. On the external side of the firewall, an organization has one or more name servers hosting zone files that contain minimal information.

Network-level firewall

Network-level firewalls run at layer 3 (Network) and sometimes layer 4 (Transport) of the OSI model and are only able to make "decisions" that fall under these two layers. Network-level firewalls scan for source and destination information and allow or disallow packets based on this information. Network layer firewalls typically fall under one of the following two categories: packet filter gateways and circuit layer gateways.

Packet filter gateway

Packet filter gateways operate in the OSI layer 3. It examines IP packets and makes a decision to accept or deny traffic based upon criteria such as source and destination IP address and source and destination TCP/UDP port numbers. Use packet filter gateways as a deterrent for DoS and IP spoofing attacks.

Circuit layer gateway

Circuit layer gateways take it a step further and operate in the OSI layer 4. As such, they can make basic authorization decisions based on source and destination IP address as well as protocol type and port. This provides a higher level of flexibility since they can make decisions on whether inbound requests to ports are valid. Routers and switches have the ability to function as network firewalls.

Implementation of network-level firewalls typically occurs when speed is essential. Packet processing occurs quicker since no packets pass to the Application layer and no examination of packet contents take place. This configuration can be advantageous for firewalls that scan for connections to Web and e-mail servers, especially servers that have high amounts of traffic. This configuration also offers a layer of protection to the network and does not impede connectivity. Network-level firewalls are generally a cheap alternative. Most logical network devices offer at least some level of packet filtering. This allows use of pre-existing equipment to perform firewall duties. Some OSs have packet-filtering capabilities. This may prove to be an inexpensive solution but can often produce problems. The most evident is that the firewall would be susceptible to any attacks or vulnerabilities that the OS possesses.

Network-level firewalls run on an ACL and do not provide the same high level of protection that application firewalls do, since they cannot monitor the contents of packets. To put it simply, the ACL

verifies if the source and destination data are valid. Only checking ACLs can present a problem if you are actively trying to scan for vulnerabilities in the data itself. Typically, network-level firewalls do not provide a high level of auditing or logging. This too may present problems if the traffic requires more detailed scanning.

Application-level firewalls

Application-level firewalls operate in the Application layer (layer 7) of the OSI model and view information as a data stream and not as a series of packets. In this way, they are able to scan information to ensure it is acceptable based on its own set of rules. Application-level firewalls use proxy servers (which mean no traffic passes directly between networks) and perform elaborate logging and auditing of traffic.

An Application-level firewall scans packets for rogue data at a higher layer and the cost comes in performance. Since the firewall operates at the Application layer, the datagram passes through all the subordinate layers (1-6) of the OSI model. The difference may not appear substantial, but when the system is scanning thousands of packets, the performance difference becomes more evident.

Due to the amount of work firewalls must do, application firewalls are less susceptible to attacks that hide data in legitimate traffic; however, it is *more* susceptible to DDoS attacks. Application firewalls can easily cease to operate if overrun with data from this type of attack.

It appears that a benefit in one firewall is a drawback in the other. In reality, the differences between network-level firewalls and Application-level firewalls are quickly diminishing. Modern firewalls perform some tasks in both the Network and Application layer. Many network operating systems have the ability to scan traffic for vulnerabilities beyond layer 3, even though it may be a layer 3 device. No matter how powerful the firewall is, it is only as strong as the policy enforcement. Ensure that the firewall is up to date on security vulnerabilities and that all ACLs are accurate.

624. Basics of intrusion detection

The capability exists to detect and deny unauthorized intrusions into the network in real-time (less than five seconds). Remote notification of unauthorized internal and external activity occurs in real-time as the activity is happening.

There are several ways to detect an intrusion. A primary detection tool is automated security incident measurement (ASIM) sensors, which are deployed across the DOD network. Additional techniques employed to detect incidents include, but are not limited to review of critical audit logs by network professionals (e.g., firewall logs); virus detection and prevention software; and reporting of anomalous network/information system events by end-users and network professionals. Reporting accurate incident information as close to near real-time as possible is crucial to effective response.

An intrusion detection system (IDS) is a system that scans, audits, and monitors the network for signs of attacks in progress. IDSs monitor network traffic and changes to computer settings to detect patterns that can indicate known intrusion attempts. IDSs can monitor all traffic on a network or it can monitor only a single computer. An IDS may also use an independent computer or device that receives data from hubs, routers, and computers on a network. This type of computer or device, called an agent or probe, forwards data to a central computer running IDS management software.

IDS software can also analyze data and alert security administrators to potential infrastructure problems. It can be comprised of a variety of hardware sensors, IDS software, and IDS management software, depending on the security needs and components chosen for the network. If you have a system that is highly critical, then it would be ideal to have more sensors placed throughout the network.

IDSs may be active or passive. Active IDSs block network traffic when it detects an intrusion. Normally, they are incorporated into firewalls. Passive IDSs monitor network traffic and *only* alerts administrators about suspicious traffic.

Here are some key points to remember when using an IDS:

- Consider using both network-based IDS and host-based IDS.
- Frequently update IDS signatures.
- Understand the nature of intrusions that IDS can detect.
- Distinguish between real intrusions and false positives.
- Deploy IDS on each network segment.
- Use a centralized management console to manage the IDS.

Types of intrusion detection methods

The three types of intrusion detection methods we will cover are host-based, network-based, and application-based. These types of intrusion detection methods not only help discover intrusions, but also help deal with them in an appropriate and timely fashion. It is important to know that the different types of detection methods have different capabilities and considerations that must considered with each.

Host-based intrusion detection system

Host-based intrusion detection system (HIDS) is a system that primarily uses software installed on a specific host (e.g., server, workstation, etc.). The disadvantage of a HIDS is it consumes resources on the host it resides on and slows that device down. However, the advantage of the HIDS is it can analyze any encrypted data, as long as decryption occurs before reaching the target host.

Network-based intrusion detection system

Network-based intrusion detection system (NIDS) is a system that primarily uses passive hardware sensors to monitor traffic on a specific segment of a network. A major drawback of a NIDS is that it cannot analyze encrypted packets because it has no method for decrypting the data. One advantage of the NIDS is that it uses very few network resources.

Application-based intrusion detection system

Current networks do *not* commonly use application-based IDSs due to the expense of implementation. However, when they are used, deployment is in conjunction with either a HIDS or NIDS to add another layer of defense in protecting critical applications.

Host-based intrusion detection system versus network-based intrusion detection system

HIDS and NIDS have a number of similarities yet have distinct differences in many areas. The following table compares the similarities and differences.

Category	Similarities and Differences
Components	HIDS primarily use software sensors, but NIDS primarily use hardware sensors.
Monitoring method	HIDS monitors traffic on the installed host, while NIDS monitors traffic on specific network segments only.
Monitoring target	HIDS monitors log files for inadvisable settings or passwords and any other type of policy violations. On the other hand, NIDS monitors packets for protocol anomalies and known virus signatures.
Encrypted data	HIDS can analyze the encrypted data if decryption occurs before reaching the target host, but NIDS cannot analyze encrypted data.
Passive or active	HIDS can be either passive or active, but NIDS can be passive only.
Resource utilization	HIDS uses the monitoring host's resources, but NIDS uses network resources.
Capabilities	HIDS has a narrow and very specific scope, while NIDS has a very broad and general scope.

Category	Similarities and Differences
Alerts	Both HIDS and NIDS alert administrators of trouble conditions via management console or e-mail messages.
Best use	In the end, the best use of HIDS is to secure a specific resource, such as a Web server that has critical data. Unfortunately, doing so is somewhat cost prohibitive. Conversely, NIDS utilization is best in securing a large area with non-critical data. Doing so provides an overall broad-based security and is most cost effective.
Management issues	In regards to HIDS, there may be management issues with service agreements or other policy restrictions that prevent the installation on a host. On the other hand, with NIDS, there are generally not these types of management issues when installing on a network.
Legal issues	Findings using HIDS may be admissible as evidence in court. Unfortunately, findings with NIDS would be hard to use as evidence in court.

Our discussion on IDS has centered on the wired IDS due to majority of DOD networked systems primarily employ wired. Additionally, the principles of intrusion detection are essentially the same wired and wireless platforms.

Current wired IDS systems will not detect any wireless threat that we receive until the threat transforms from being wireless to a wired. Adequately detecting a wireless threat requires the installation of devices specifically configured to operate and scan in the wireless arena.

Intrusion detection system log

Intrusion detection logs clearly indicate if or when a network intrusion has occurred, and if the intrusion was properly handled and appropriately blocked. Log entries typically begin with a date-time stamp followed by an abbreviated description of the error followed by the IP address. Some examples are provided purely for illustration purposes:

12/1/2014 3:30:01 PM TCP-Port-Scan detected Network Intrusion 192.68.
12/1/2014 3:34:07 PM UDP-Port-Scan detected Network Intrusion 192.69.
12/1/2014 3:35:01 PM TCP-SYN-Port-Scan detected Host Intrusion 192.69.5.19
12/1/2014 3:35:01 PM TCP-Ping 192.69.5.17
12/1/2014 3:35:04 PM TCP-Ping 192.69.5.18
12/1/2014 3:47:01 PM TCP-SYN-Port-Scan detected Host Intrusion 192.69.5.18
12/1/2014 3:59:14 PM TCP-SYN-Port-Scan detected Host Intrusion 192.69.5.35
12/1/2014 4:00:14 PM Host intrusion detected and handled Host intrusion (hip.Files) 192.69.5.17 Blocked
12/1/2014 6:52:47 PM Host intrusion detected and handled Host intrusion (hip.Registry) 192.69.5.17 Blocked
12/1/2014 11:04:08 PM Host intrusion detected and handled Host intrusion (hip.Files) 192.69.5.18 Blocked
12/2/2014 11:03:22 PM Host intrusion detected and handled Host intrusion (hip.Files) 192.69.5.19 Blocked
12/3/2014 7:08:46 PM Network intrusion detected Network intrusion detected 192.69.5.25
12/3/2014 7:09:15 PM Network intrusion detected Network intrusion detected 192.69.5.25
12/3/2014 7:09:25 PM Network intrusion detected and handled Network intrusion detected 192.69.5.5 Blocked
12/3/2014 7:09:55 PM Network intrusion detected and handled Network intrusion detected 192.69.5.25 Blocked
12/3/2014 7:10:05 PM Network intrusion detected and handled Network intrusion detected 192.69.5.40 Blocked
12/3/2014 7:11:23 PM Network intrusion detected and handled Network intrusion detected 192.69.5.10 Blocked

In the example, take note of where the IDS discovered an intrusion, noted a ping, and, ultimately, blocked the intrusion attempt. Again, keep in mind that this is *an example only*. While any log that you may view may have similar data, there will most certainly be changes in terms of format along with possible addition or deletion of field columns as necessary

625. Principles of wireless security

One of the newest computer security threats comes from hand held portable electronic devices and wireless technologies. Because a wireless device transmits radio signals over a broad area, security becomes a major concern. Wireless services are susceptible to interference (friendly and unfriendly) and are easily jammed, resulting in no service. Wireless networks introduce their own unique set of requirements for security. It is possible for an intruder to be in the parking lot with a laptop computer and wireless NIC intercepting signals from a wireless network. Because much of a unit's network traffic may contain sensitive information, this is not an acceptable. The table below briefly covers four common WLAN threats.

Threat	Description
War Drivers	A person who drives around scanning for WLAN access points that have no or weak authentication/encryption measures enabling them free Internet access and possibly gaining access to local data.
Employees	An authorized client may assist outside parties to gain network access either unknowingly or maliciously.
Hackers	Motivated individuals who attempt to deny services or steal information. They may exploit a weakly secured WLAN to gain access to a network.
Rogue Access Points	Attackers capture WLAN traffic. Dissect the traffic and then set up their WLAN access point that emulates the true network. Then network users begin information transactions with the rogue access point revealing usernames, passwords, and other vital network information.

Preventing unauthorized access to wireless clients and access points is critical to the overall security of the network. One of the best ways of hiding a message is by talking in a special code, which is encryption. Encryption is the process of transforming a plain text message into cipher text. Decryption is the process of transforming cipher text into plain text. In order for these processes to work, both the sending and receiving systems must share a common key (passphrase) and use the same algorithm. With wireless encryption, there are three major encryption algorithms wired equivalent privacy (WEP), wireless fidelity (Wi-Fi) protected access (WPA), and WPA 2 (WPA2).

Wired equivalent privacy

WEP was the original wireless encryption algorithm. Debuting in 1999, WEP was the original wireless encryption algorithm that was used extensively in early WLANs. However, at the time of its release, United States law prevented the export of encryption keys over 40-bits. This coupled with the fact that the encryption key was based on the network passphrase that never changed, meant that the encryption key was both weak and static. WEP provides some margin of security compared with no security at all, but both are highly undesirable. You should never use WEP encryption in today's networks. Because of the weak key, WEP quickly became unsecure and superseded in 2003 by WPA.

WPA was the successor of WEP. It was developed by the Wi-Fi Alliance primarily to address the shortcomings of WEP and not as a permanent solution. WPA was an intermediate step used to provide better security until a more reliable solution could be developed and released. Although it used the same algorithm as WEP, WPA introduced the temporal key integrity protocol (TKIP). TKIP added a random variable to the encryption algorithm to ensure that each packet had its own unique encryption key. Although it does provide better protection than WEP, both WPA and WEP utilize the Rivest Cipher 4 (RC4) encryption, which was found to have many vulnerabilities within itself. Along with WEP, WPA is now outdated.

Wireless fidelity protected access 2

WPA2 provides specifications that strongly increase the level of data protection and access control for existing and future wireless LAN systems. WPA2 became available in 2006 as the permanent replacement for WEP encryption. WPA2 works primarily just like WPA with one major exception. Instead of using TKIP like WPA, WPA2 utilized a new encryption algorithm called counter mode

cipher block chaining message authentication code protocol (CCMP). CCMP was essentially the same as TKIP in the fact that it ensures the encryption key receives a random variable with each packet. However, the biggest difference between TKIP and CCMP is that CCMP utilizes the advanced encryption standard (AES). AES is a far superior encryption algorithm than RC4 and provides a higher level of security. WPA2 has become the industry standard in wireless encryption.

WPA2 provides the following improvements for wireless security:

- Secure replacement for WEP.
- Strong encryption.
- Interoperable with existing infrastructure.
- Software upgradeable for existing Wi-Fi certified products.
- Applicable for both home use and large enterprise networks.

NOTE: The Wi-Fi Alliance announced that WPA3 would begin replacing WPA2 in 2018.

MAC filtering

One of the most popular ways of securing a network is MAC filtering. Every networked device has its own globally unique MAC address. An administrator can configure a wireless access point to accept traffic only from known MAC addresses. Although this does seem like a great way to secure an access point, in reality it provides *only* a false sense of security, because attackers can spoof MAC addresses. If the only thing that is preventing unauthorized access to your network is MAC filtering, then by spoofing an authorized MAC address, the attacker can gain access to your network. However, MAC filter does have a place in network security since it does serve as an obstacle to attackers.

Service set identifier broadcasting

An SSID is the name of your wireless network. By default, most wireless router configurations advertise the network via broadcast for ease of use. Most average users believe that if they turn off the broadcast, the public cannot see their network. This is simply not true. In order for a wireless client to communicate with a wireless access point, every packet transmitted must have the SSID attached. An attacker can use a tool called a protocol analyzer or packet sniffer to discover your SSID quickly. Much like the MAC filtering, relying on disabling the SSID broadcast will provide a false sense of security. However, in home networking, disabling SSID broadcast can ensure that your non-technical neighbor is not stealing your network bandwidth!

626. Principles of physical security

While previous lessons highlighted a number of principles related to protecting information and securing a network, they focused on logical implementations. It is also important to understand the physical implementations required to secure equipment operating on a network.

Communication room security

Rooms that contain sensitive or critical network equipment should be free of electrostatic or magnetic interference, and they should have temperature and humidity control. If continuous operation of the equipment is *critical*, install an uninterruptible power supply (UPS) and make sure to have spare components on hand. The room should always be locked and only accessible by authorized personnel.

Once an individual has physical access to a piece of networking equipment, there is no way to stop them from modifying the system There are things that can be done to make this more difficult, but a knowledgeable attacker with access can never be completely defeated, only slowed down. One of the best additions to the security features of a computer network is to limit access. Limiting access to network infrastructure components, like routers, is especially important. These devices often protect segments of the network, and if compromised can be used for launching attacks against valuable network resources.

To illustrate a reason why physical security is critical to overall router security, consider the password recovery procedure for Cisco routers. Using this procedure, an individual with physical access can gain full privileged access to a Cisco router without using a password. The details of the procedure vary between router models, but always involve an administrator (or an attacker) connecting a terminal or computer to the console port, and then changing the password in test system mode.

Anyone with experience or training using Cisco routers can parley physical access into full privileged administrative access; the procedure takes only a couple of minutes.

A second reason for controlling physical access to the router involves flash memory cards. Many Cisco router and switch models offer PC-card slots or CompactFlash slots that can hold additional flash memory. Devices equipped with these kinds of slots will give preference to memory installed in a slot over memory installed in the chassis. An attacker with physical access to a router on your network can install a flash memory card, or replace an old one. They could then boot the router with their flash, thus causing the router to run their OS version and configuration. If done carefully, this kind of attack can be very difficult to detect. The best defense against it is good physical security.

Network equipment, especially routers and switches, should be located in a limited access area. If possible, this area should only be accessible by personnel with administrative responsibilities for the equipment. This area should be under supervision 24 hours a day, 7 days a week. This can occur using guards, system personnel, or electronic monitoring. Proximity readers used with access badges are very popular for controlling access. For extremely critical equipment, organizations can use biometrics to control access. Biometric identifiers are distinctive, measurable characteristics used to identify individuals. The system can be setup to scan one or more characteristics. Some common characteristics scanned include face recognition, iris (eye) recognition, and fingerprints.

Centralize the connection points of an organization’s network in secure locations. Physically secure and closely monitor network connection points, as they are vulnerable to sniffing. Install network connection points in physically secure closets or rooms with other critical network devices.

Asset tracking systems

Accountability of equipment is an important part of device security. Radio frequency identification (RFID) is the *most* popular type of asset tracking. RF embedded chips in mobile devices transmit a unique signature, or identity, that a receiver can read. Modern RFID systems often provide real-time monitoring with alarm configurations, so the location and movement of the device is always known. These systems can be used on sensitive mobile network equipment, desktop workstations, and laptops. This technology can also be used to track mobile medical devices (infusion pumps, ventilators, defibrillators, etc.).

Self-Test Questions

After you complete these questions, you may check your answers at the end of the unit.

621. Principles of threats and vulnerabilities

1. What is the objective of computer security?

2. Describe the three system risk values.

3. Vulnerability is the intersection of what three elements?

4. What action should be taken if an unpatched or legacy system's use cannot be avoided?

5. Who develops and coordinates network assessment schedules and details?

6. What is the difference between natural and environment threats?

7. What are some effects of a virus?

8. What actions should you take to protect against viruses and spyware?

9. What is the most common type of DoS attack?

10. Explain a man-in-the-middle attack.

11. What is spoofing?

12. Match the type of scan in column B to its description in column A.

Column A	*Column B*
___(1) More focused scan looking only for known services to exploit.	a. Vanilla.
___(2) Most basic; attempts to scan all ports.	b. Sweep.
___(3) Scanner goes through a FTP server to disguise source of scan.	c. Strobe.
___(4) Scanner connects to same port on more than one machine.	d. FTP bounce.

13. What methods prevent unauthorized port scanning?

622. Principles of network and application security

1. Briefly explain the encryption process.

2. How does the authorized recipient decrypt the message?

3. How does PKI provide data integrity?

4. What provides access to PKI capabilities?

5. Where must you upload your public keys on your CAC?

6. What are some examples of technical controls in access prevention?

623. Basics of firewalls

1. What can firewalls not prevent?

2. Which type of network level firewall is used as a deterrent for DoS attacks?

3. What is a potential problem with network level firewalls?

4. How are Application-level firewalls able to scan information to determine if it is acceptable?

624. Basics of intrusion detection

1. What is an IDS?

2. What is the difference between active and passive IDSs?

3. What is a disadvantage of a HIDS?

4. What is an advantage of a NIDS?

5. How do HIDS and NIDS differ when it comes to encryption?

6. What are the best uses for HIDS and NIDS?

625. Principles of wireless security

1. What are the three major encryption algorithms?

2. Which wireless encryption algorithm introduced TKIP? What did TKIP provide?

3. What improvements did WPA2 provide over WEP and WPA?

4. Why is MAC address filtering a false sense of security?

5. What is the SSID?

626. Principles of physical security

1. What are some features a room should have that contain sensitive or critical network equipment?

2. What are some characteristics that biometric scanners check to establish identity?

3. What is the most popular type of asset tracking?

Answers to Self-Test Questions

621

1. Ensure the employment of countermeasures to protect and maintain the confidentiality, integrity, availability, and nonrepudiation of resources and data processed throughout the network.
2. A rating of “low” indicates a security breach would cause limited damage to organizations, individuals or operations; a “moderate” rating indicates the potential for serious damage in those areas; and a “high” rating predicts severe or catastrophic adverse effects in case of a security breach.
3. A system’s susceptibility or flaw, attacker’s access to the flaw, and attacker’s capability to exploit the flaw
4. Isolate it from the network to decrease the vulnerability of an attack.
5. DHA and local program managers.
6. Nature causes natural threats and environmental threats result from man-made items.
7. Viruses can reformat a hard disk; erase programs and files; add unrecognizable characters to files; or destroy disk directories and file allocation tables preventing the computer from using the tables or directories to locate files.

8. Use good antivirus and anti-spyware software products. Take precautions with any removable media (CD-ROMs or flash drives) because viruses can spread through infected disks. Do not share disks unless it is necessary. Virus check any disks before accessing files on it. Only use original software and do not share software with anyone else or put copies of someone else's software on another computer. Always back-up files. If a computer is infected with a virus that wipes out the hard drive, the data can still recover up to the last backup. Finally, schedule time to scan your system's hard drive.
9. When the attacker uses his computer to flood a targeted server with so many requests that the server gets an individual interjects into communication between two systems or parties, covertly intercepting traffic overwhelmed and stops working.
10. When an individual interjects into communication between two systems or parties and covertly intercepts traffic.
11. A situation in which a person or program successfully masquerades as another by falsifying data.
12. (1) c, (2) a, (3) d, (4) b.
13. Using ACL, setting up black hole firewalls, keeping software current, and managing unused ports.

622

1. Encryption is the process of encoding data in such a way that only authorized personnel can access it and all others cannot. The information or message (data) in plaintext (readable and unencrypted) is encrypted using an encryption algorithm (a cipher) which turns the plaintext to ciphertext, which can then be read only if decrypted.
2. The authorized recipient easily decrypts the message with the key that the originator provided if using symmetric encryption or their private key if using asymmetric (public key) encryption.
3. PKI provides data integrity through digital signature of information. If the recipient of digitally signed information is able verify the signature on the information using the public key of the certificate used to generate the signature, then the recipient knows that the content has not changed since it was signed.
4. CAC.
5. GAL.
6. Passwords and encryption.

623

1. Firewalls cannot prevent accidental or deliberate disclosure of information, threats to the integrity of information that may arise prior to it reaching the firewall, or unauthorized access to systems already inside the firewall.
2. Packet filter gateway.
3. Network-level firewalls run on an ACL and do not provide the same high level of protection that application firewalls do, since they cannot monitor the contents of packets. The ACL verifies if the source and destination data are valid. Only checking ACLs can present a problem if actively trying to scan for vulnerabilities in the data itself.
4. They are able to scan information because they view information as a data stream and not as a series of packets.

624

1. A system that scans, audits, and monitors the network for signs of attacks in progress.
2. Active IDSs block network traffic when it detects an intrusion; normally they are incorporated into firewalls. Passive IDSs monitor network traffic and only alerts administrators about suspicious traffic.
3. It consumes resources on the host it resides on and slows that device down.
4. It uses very few network resources.
5. HIDS can analyze the encrypted data if decryption occurs before reaching the target host, but NIDS cannot analyze encrypted data.
6. The best use of HIDS is to secure a specific resource, such as a Web server that has critical data. NIDS utilization is best in securing a large area with non-critical data.

625

1. WEP, WPA, and WPA2.

2. WPA. TKIP added a random variable to the encryption algorithm to ensure that each packet had its own unique encryption key
3. Secure replacement for WEP, strong encryption, interoperable with existing infrastructure, software upgradeable for existing Wi-Fi certified products, and applicable for both home use and large enterprise networks.
4. Because attackers can spoof MAC addresses.
5. The name of the wireless network.

626

1. Rooms should be free of electrostatic or magnetic interference, and should also have temperature and humidity control. If continuous operation of the equipment is critical, install a UPS and make sure to have spare components on hand. The room should always be locked and only accessible by authorized personnel.
2. Face recognition, iris (eye) recognition, and fingerprints.
3. RFID.

Unit Review Exercises

Note to Student: Consider all choices carefully, select the *best* answer to each question, and *circle* the corresponding letter. When you have completed all unit review exercises, transfer your answers to the Field Scoring Answer Sheet.

Do not return your answer sheet to AFCDA.

88. (621) Which information system security objective involves individuals *not* being able to deny who performed a particular network action?
    a. Nonrepudiation.
    b. Confidentiality.
    c. Availability.
    d. Integrity.

89. (621) Which type of software vulnerability involves a user sending their valid user name or password as readable and unencrypted text?
    a. Cleartext credentials.
    b. Unencrypted channels.
    c. Unpatched and legacy systems.
    d. Radio frequency (RF) emanation.

90. (621) How can attackers identify open doors on a computer?
    a. Port scanning.
    b. Spoofing.
    c. Eavesdropping.
    d. Backdoor.

91. (622) What actions must you take if a vendor-selected default password exists on a medical device?
    a. Safeguard the password.
    b. Change it as soon as possible.
    c. No action is required if the complexity meets your unit's policy.
    d. Disable the password feature.

92. (622) What helps ensure data integrity in the event of a system incident or catastrophic failure?
    a. Public key infrastructure (PKI).
    b. Virtual private network (VPN).
    c. Asymmetric encryption.
    d. Routine data backup.

93. (622) Which security service does public key infrastructure (PKI) encryption support?
    a. Authentication.
    b. Data integrity.
    c. Confidentiality.
    d. Technical non-repudiation.

94. (623) Which of the following is *not* a function of a firewall?
    a. Block unauthorized traffic from entering the network.
    b. Prevent accidental disclosure of information.
    c. Hide vulnerable systems from the Internet.
    d. Log traffic to and from internal servers.

95. (623) Which type of firewall is *most* susceptible to distributed denial of service (DDoS) attacks?
    a. Network level firewall.
    b. Circuit layer gateway firewall.
    c. Packet filter gateway firewall.
    d. Application-level firewalls.

96. (624) Which type of intrusion detection system (IDS) is uncommon due to implementation costs?
    a. Network-based intrusion detection system (NIDS).
    b. Application-based intrusion detection system.
    c. Host-based intrusion detection system (HIDS).
    d. Open system interface (OSI) layer 4 IDS.

97. (624) Which type of intrusion detection system (IDS) can *only* be passive?
    a. Network-based intrusion detection system (NIDS).
    b. Application-based intrusion detection system.
    c. Host-based intrusion detection system (HIDS).
    d. Open system interface (OSI) layer 4 IDS.

98. (625) Which wireless encryption algorithm should *never* be used in modern wireless local area networks (WLAN)?
    a. Wired equivalent privacy (WEP).
    b. Wireless fidelity protected access (WPA).
    c. WPA2.
    d. WPA3.

99. (625) What was a secure replacement for wired equivalent privacy (WEP)?
    a. Wireless fidelity protected access (WPA).
    b. WPA2.
    c. WPA3.
    d. Temporal key integrity protocol (TKIP).

100. (626) The *most* preferred method of asset tracking is
    a. radio frequency identification (RFID).
    b. database spreadsheet.
    c. Bluetooth.
    d. barcode.

Glossary

Abbreviations and Acronyms

.pst	personal storage table
AC	alternating current
ACL	access control list
AES	advanced encryption standard
AF	Air Force
AFI	Air Force instruction
AFMAN	Air Force manual
AFMOA	Air Force Medical Operations Agency
AFMS	Air Force Medical Service
AFSC	Air Force specialty code
AGP	accelerated graphics port
ALU	arithmetic logic unit
AMD	Advanced Micro Devices
AO	authorizing official
ARAPANET	Advanced Research Projects Agency network address
ARP	resolution protocol
ASCII	American standard code for information interchange
ASIM	automated security incident measurement
ATA	Advanced Technology Attachment
ATC	approval to connect
ATD	authorization termination date
ATM	asynchronous transfer mode
ATO	authorization to operate
ATX	advanced technology eXtended
BGP	border gateway protocol
BIOS	basic input output system
BMET	biomedical equipment technician
BNC	Bayonet Neill-Concelman

BSS	basic service set
CAC	common access card
CCMP	counter mode cipher block chaining message authentication code protocol
CD	compact disc
CDC	career development course
CD-R	compact disc Recordable
CD-ROM	compact disc Read Only Memory
CD-RW	compact disc ReWritable
CFR	Code of Federal Regulations
CIA	confidentiality, integrity, and availability
CIDR	classless inter-domain routing
CISA	certified information systems auditor
CISSP	certified information systems security professional
CMIP	common management information protocol
CMOS	complementary metal-oxide semiconductor
COMPUSEC	computer security
CompTIA	Computing Technology Industry Association
CPU	central processing unit
CRC	cyclic redundancy check
CSMA/CA	Carrier Sense Multiple Access Collision Avoidance
CSMA/CD	Carrier-Sense Multiple Access with Collision Detection
CT	computerized tomography
DATO	denial of an authorization to operate
DBMS	database management system
DC	direct current
DD	Department of Defense (form)
DDN	dotted decimal notation
DDoS	distributed denial-of-service
DDR	double data rate

DHA	Defense Health Agency
DHCP	dynamic host configuration protocol
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DLA-DS	Defense Logistics Agency Disposition Services
DMLSS	Defense Medical Logistics Standard Support
DNS	domain name system
DOD	Department of Defense
DODI	Department of Defense instruction
DoS	denial-of-service
DRAM	dynamic random access memory
DVD	digital video disc
DVI	digital visual interface
EBCDIC	extended binary coded decimal interchange code
ECC	error correction code
ECN	equipment control number
EEPROM	electrically erasable programmable read-only memory
EGP	exterior gateway protocol
EHR	electronic health record
EIA/TIA	Electronics Industry Association/Telecommunications Industry Association
EIDE	enhanced integrated drive electronics
EIGRP	enhanced interior gateway routing protocol
EMC	electromagnetic compatibility
EMD	electromagnetic disturbance
EMI	electromagnetic interference
FBI	Federal Bureau of Investigations
FCS	frame check sequence
FDA	Food and Drug Administration
FDDI	fiber distributed data interface
FTAM	file transfer access and management

FTP	file transfer protocol
GAL	global access list
GCIH	global information assurance certification certified incident handler
GIAC	global information assurance certification
GIF	graphics interchange format
GSE	global information assurance certification security expert
GSEC	global information assurance certification security essentials certification
GUI	graphical user interface
GUID	globally unique identifier
HCL	hardware compatibility list
HDD	hard disk drive
HDLC	high-level data link control
HDMI	high definition multimedia interface
HIDS	host-based intrusion detection system
HIPAA	Health Insurance Portability and Accountability Act
HPO	Health Insurance Portability and Accountability Act privacy officer
HSO	Health Insurance Portability and Accountability Act security officer
HTML	hypertext markup language
HTTP	hypertext transfer protocol
HTTPS	hypertext transfer protocol secure
I/O	input output
IA	information assurance
IAM	information assurance management
IANA	Internet Assigned Numbers Authority
IAT	information assurance technical
IATT	interim authorization to test
IBM	International Business Machines
ICMP	Internet control message protocol
ID	identification

IDS	intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
IGP	interior gateway protocol
IMAP	Internet message access protocol
IP	Internet protocol
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6
ISN	initial sequence number
ISO	International Organization for Standardization
ISP	Internet service provider
ISSM	information system security manager
ISSO	information system security officer
IT	information technology
JPEG	joint photographic experts group
KB	kilobyte
L1	level 1
L1d	level 1 data
L1i	level 1 instructions
L2	level 2
L3	level 3
LAN	local area network
LASER	light amplification by stimulated emission of radiation
LED	light emitting diode
LLC	logical link control
MAC	media access control
MAN	metropolitan area network
MCC	memory chip controller
MHS	Military Health System
MIMO	multiple-input multiple-output

MPEG	motion picture experts group
MRI	magnetic resonance imaging
MSC	Medical Service Corps
MTF	military treatment facility
NAS	network attached storage
NIC	network interface controller
NIDS	network-based intrusion detection system
NIPRNet	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NTP	network time protocol
OFDM	orthogonal frequency-division multiplexing
OS	operating system
OSI	open system interconnection
OSPF	open shortest path first
PACS	picture archiving and communication system
PC	personal computer
PCI	peripheral component interconnect
PCIe	peripheral component interconnect express
PDU	protocol data unit
PHI	protected health information
PIN	personal identification number
ping	packet internetwork groper
PK	public key
PKI	public key infrastructure
POP	post office protocol
POST	power-on self-test
PROM	programmable read-only memory
RAID	redundant arrays of independent disks

RAM	random access memory
RC4	Rivest Cipher 4
RF	radio frequency
RFID	radio frequency identification
RG	radio guide
RIP	routing information protocol
RJ	registered jack
RMF	Risk Management Framework
ROM	read-only memory
RPM	revolutions per minute
RS	recommended standard
SATA	Serial Advanced Technology Attachment
SCA	security control assessor
SCNA	security certified network architect
SCNP	security certified network professional
SCSI	small computer system interface
SDRAM	synchronous dynamic random access memory
SEI	special experience identifier
SIPRNet	Secret Internet Protocol Router Network
SMTP	simple mail transfer protocol
SNMP	simple network management protocol
SOHO	small office/home office
SP	special publication
SQL	structured query language
SRAM	static random access memory
SSCP	systems certified practitioner
SSD	solid state drive
SSID	service set identifier
STP	shielded twisted pair

SYN	synchronous
TCP	transmission control protocol
TCP/IP	transmission control protocol/Internet protocol
Telnet	teletype network
TFTP	trivial file transfer protocol
TIFF	tagged image file format
TKIP	temporal key integrity protocol
TLS	Transport layer security
UART	universal asynchronous receiver-transmitter
UDP	user datagram protocol
UEFI	Unified Extensible Firmware Interface
UPS	interruptible power supply
USB	universal serial bus
USOC	Universal Service Ordering Code
UTP	unshielded twisted pair
VESA	Video Electronics Standards Association
VAC	volts alternating current
VDC	volts direct current
VGA	video graphics array
VLAN	virtual local area network
VoIP	voice over Internet protocol
VPN	virtual private network
VTP	virtual terminal protocol
WAN	wide area network
WEP	wired equivalent privacy
Wi-Fi	wireless fidelity
WLAN	wireless local area network
WNIC	wireless network interface controller
WPA	wireless fidelity protected access

WPA2	wireless fidelity protected access 2
WWAN	wireless wide area network
WWW	World Wide Web

Student Notes

Student Notes

AFSC 4A251A
4A251A 04 1812
Edit Code 04