

The Official CompTIA A+ Core 1 Student Guide

CompTIA.[®]



Copyright © 2025 CompTIA, Inc. All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. CompTIA, Inc. does not have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.



Note: Copyright © 2025 CompTIA, Inc. All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. CompTIA, Inc. does not have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

The Official CompTIA A+ Core 1 Student Guide

About This Course

The CompTIA A+ certification, broken into a Core 1 exam and a Core 2 exam, is a foundational-level certification designed for professionals with 12 months hands-on experience in a help desk support technician, desktop support technician, or field service technician job role.

This course can benefit you in two ways. If you intend to pass the CompTIA A+ Core 1 (Exam 220-1201) exam to receive an A+ certification, this course can be a significant part of your preparation. However, certification is not the only key to professional success in the field of IT support. Today's job market demands individuals have demonstrable skills, and the information and activities in this course can help you build your skill set so that you can confidently perform your duties in any entry-level IT support role.

Upon course completion, you will be able to:

- Define the role of an IT Specialist
- Install Motherboards and Connectors
- Install System Devices
- Troubleshoot PC Hardware
- Compare Local Networking Hardware
- Configure Network Addressing and Internet
- Support Network Services
- Summarize Virtualization and Cloud Concepts
- Support Mobile Devices
- Support Print Devices

Course Design

This course is designed to optimize knowledge acquisition and skills development related to the learning objectives and related job task requirements through a learning progression model. The learning progression model follows a series of steps to contextualize, elaborate, provide relevance through practice and personalized feedback, contextualized application, and demonstrable evidence of skills gained.

Different activities throughout the course will help you practice and develop your skills as well as gauge your understanding of the various topics covered. The course is broken into modules and lessons. At the end of each module, a quiz will confirm your knowledge retention. Most modules also end with a challenge live lab to test your skills.

Prerequisites

To ensure your success in this course, have a minimum of 12 months of hands-on experience in a help desk technician, desktop support technician, or field service technician job role.

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



Note: Copyright © 2025 CompTIA, Inc. All Rights Reserved. Reference to any specific product, service, process, or method by trade name, trademark, manufacturer or otherwise on this website is for educational purposes only and does not constitute an implied or expressed recommendation or endorsement by said third party. CompTIA, Inc. does not have any affiliation with any of these companies, and the products and services advertised herein are not endorsed by them.

Module 1

What Does an IT Specialist Do?

Module Overview

You have finally secured a position in information technology (IT), and it begins today! Awesome, but what can you expect of your new position, and what work assignments should you expect each day? Answering the question of what your day-to-day "routine" will be is not an easy one, as different companies utilize technology for different purposes.

Module Summary

Prepare for A+ Certification by:

- Describing what an IT specialist is and their responsibilities
- Describing the skills an IT specialist needs
- Describing the role of certifications for an IT specialist

Lesson 1A

The Hero of Problem Solving

Lesson Overview

It's your first day walking into the office, and you've already had three problems to solve. The receptionist, Aurora, is asking for help connecting their laptop to their email account. Two other colleagues are asking why the database server will not connect to their desktop systems. "The Internet must be down," Jim from accounting says. These are just a few examples of issues that you may be asked to solve for your company. Understanding what your role is as an IT specialist and how you can provide timely solutions that ultimately enable the company to continue to move forward with their projects can be time-consuming but also rewarding.

Learning Outcomes

As you study this lesson, answer the following questions:

- What is an IT specialist?
- What are the responsibilities of an IT specialist?
- What are the skills required to be an IT specialist?

Role of an IT Specialist

An IT specialist is the frontline problem-solver of IT issues and problems that an organization may experience. The position of an IT specialist comes with many different requirements. A majority of these requirements are centralized around your job responsibilities.

When it comes to troubleshooting and resolving issues for users, there is a wide array of problems that can occur. From fixing an issue with a user's login credentials to configuring the network to support more users, every day an IT specialist can expect to be asked to respond to different issues. This dynamic and variable work environment is what attracts many individuals to this role.

For example, when a company purchases a new server or printer for the organization, they will rely on an IT specialist to unpack, set up, and configure the system for operations. They may even require you to provide training to other employees on how to use the new server or printer. The new printer may also come with new software that must be installed by you in order to ensure the printer works correctly and users can access all the features of the printer.

A commonly used printer in many organizations



Image © 123rf.com.

While getting new equipment is always exciting, an IT specialist will also be called upon to provide support to existing systems and applications. From performing a memory upgrade on the server to improve its performance or replacing a hard drive that decided to fail, you can expect to spend a good portion of your time responding to problems and issues facing your users. Some of these issues may be a quick fix, while others may take several technicians many hours to resolve. This direct support of the organization's IT systems will also include ensuring those systems and data remain secure from users who are not authorized access.

When it comes to the role of an IT specialist, the ever-changing problems you will be asked to resolve and the many different users you are asked to support lead many who choose this career to find their job very rewarding.

Skills and Abilities

Since the tasks that you will be called upon to fix are changing, the skills and abilities that an IT specialist must have are generally very broad but can also be specific to the company or organization you work for.

A great IT specialist should be able to problem solve, communicate effectively, be organized in their communications and within their workspace, and utilize their technical acumen to provide solutions.

Problem Solving

Problem solving skills require that an IT specialist can identify the problem and establish a theory of the probable cause of that problem. Understanding the company's network

configuration, policies, and practices will also play a role in determining what may be causing the issue.

Consider this: A user reports that their computer is not working, and they need it right now to complete a project. When talking with the user, you learn that the computer is on and functioning. However, the project application is not able to locate the file the user is trying to open. You click the mouse and attempt to use the keyboard, but it seems the application is just not able to find the file.

To determine what may be causing the issue, you begin to think about how this application is installed on the local computer and how the files the user is trying to access are located on a server across town at the company's headquarters. You brainstorm that the problem might be that the network connection between your building and the headquarters building is not working.

You run a connection test and find that the headquarters building is currently experiencing a power outage. You then explain to the user that the file they need is on the file server across town, but there is no power at that location. Therefore, the server cannot be accessed. You suggest that the user inform their supervisor of the problem and tell them that you will contact them once power has been restored at headquarters to ensure they can access the file.

Power Outage



Image © 123rf.com.

One of the keys to being a great problem solver is to establish a step-by-step process that you use for every issue you are asked to resolve. Being consistent with your process and attention to detail ensures that, as an IT specialist, you do not miss something easy by skipping steps. Some companies will require you to use standard operating procedures (SOPs) that have been established by the management for problem solving. These SOPs are customized to the

organization's information technology environment and ensure a repeatable process is followed by all technicians.

While there is value in using the same process every time you troubleshoot, a great IT specialist will also consider potential causes and solutions that have not been considered before. By thinking outside the box, you may find a solution that works more effectively for you and the organization.

Communication and Organization

When coming across new ideas and solutions, an IT specialist will need to be able to communicate that new idea to the company in the most appropriate manner. Some suggestions can be quickly disseminated through a phone call, while more elaborate ideas may require written communication to be effective. Communication skills for an IT specialist will require both good oral and written communication. This communication should be direct and professional at all times. This ensures that the content is shared swiftly and can be understood by all involved.

Consider the previous example with the power outage causing issues for employee access to the file server. You might decide to recommend the organization consider installing another server at your location. This will cost the company money to purchase the new server, but it could be cost-effective if it ensures that work can still be completed at your site.

To communicate this suggestion, you might want to research the cost of the new server along with the requirements to configure the server to operate on the network. This type of suggestion would most likely be communicated most effectively through an email rather than a phone call. By writing the suggestion up with all the necessary details, you are able to communicate the suggestion while also presenting your research to your supervisor.

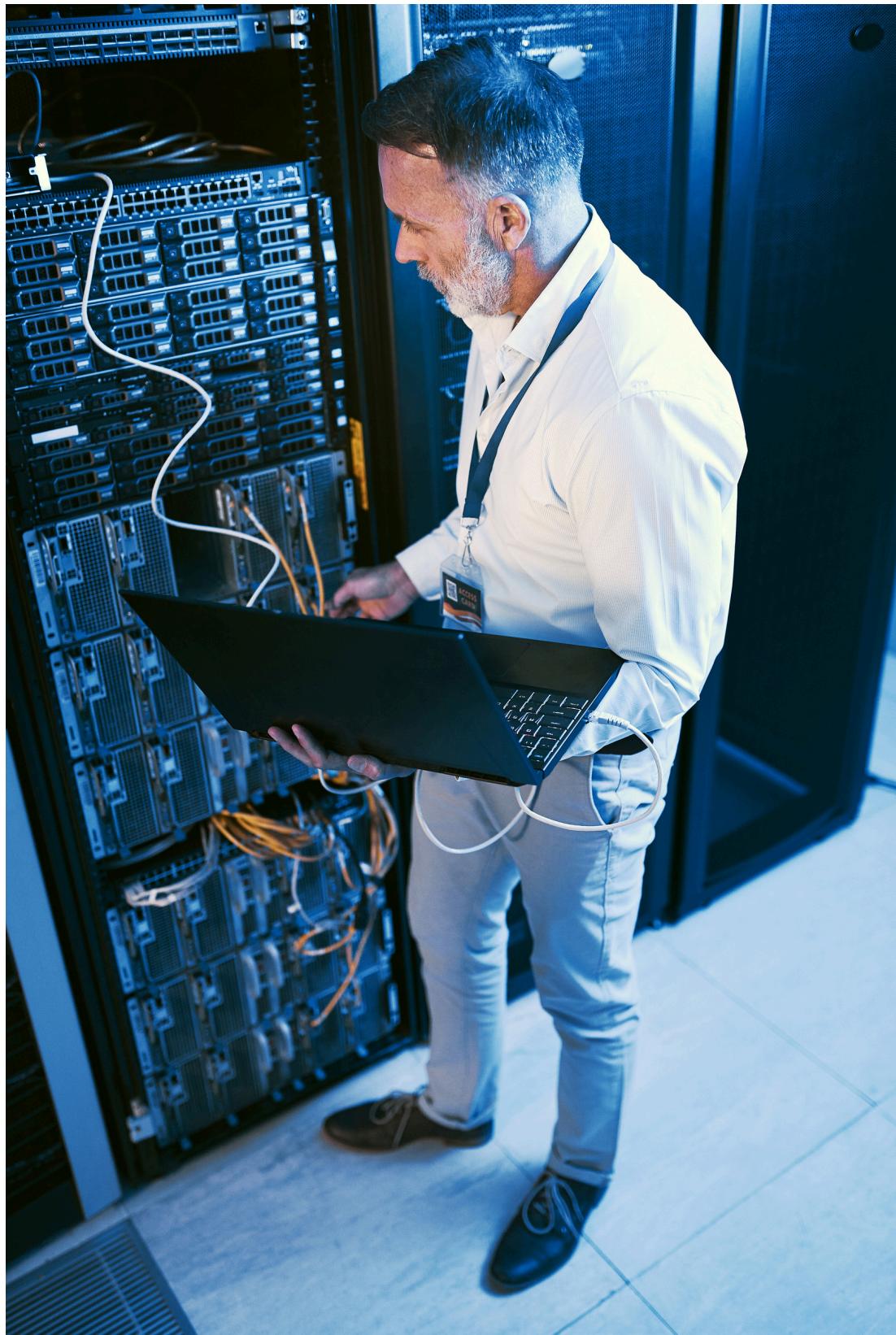
Organization also applies to your work environment. Ensuring you are able to find the tools and parts needed will allow you to resolve a problem quickly. As an IT specialist, you will likely need a set of tools and equipment to assist in the problem solving for an issue. The tools needed will vary, from screwdrivers and a multimeter to a toning probe and a cable tester. These tools will allow you to take equipment apart and test various components to ensure they are working correctly and are not defective. Ensuring your tools are organized can allow you to quickly locate what you need without needing to go search for that screwdriver or flashlight when you need it.

An IT specialist also needs organizational skills to ensure accurate documentation and records are kept about the issues that have been resolved and the maintenance on a system that has been completed. Some organizations utilize an electronic trouble ticket system to accurately track reported problems and the solutions that a specialist has used to resolve them. This single location for all the information and details surrounding the issue ensures other technicians can check on the status of a repair or use the solution to a previous issue to resolve a newly reported problem.

Technical Knowledge

Today, the role of an IT specialist has expanded from management and troubleshooting the devices users interact with to now include an understanding of new technologies and skill sets, including security and management of external resources such as cloud-based servers and networks. Technical skills and knowledge can be obtained through training programs and classes, as well as research. Some courses and classes are for specific types of technology or software applications. For example, a user may need to watch an online video covering the Windows operating system and how it interacts with the hardware of the computer. You may also be asked to attend formal training courses to learn how to troubleshoot a copy machine your company just purchased. Being an IT specialist will require you to become a lifelong learner, always pursuing new opportunities to expand your technical knowledge and skills.

Server Room



An IT specialist may also learn technical concepts, ranging from the basics of how a central processing unit (CPU) takes input from the user and processes it to provide output to how a wireless network uses encryption to ensure the security of the data on that network. While you may not be expected to be the expert on all things IT-related, you will be expected to conduct research and work to keep expanding your knowledge level. Becoming a lifelong learner is a byproduct of being in the IT field, with existing systems being upgraded and expanded and new technology being developed every day.

IT specialists require a lot of different skills to be great in their role. From understanding the technical content and infrastructure to effective oral and written communication, a great technician must obtain these skills and abilities to ensure they are both effective and efficient at solving the IT issues that organizations face today.

Lesson 1B

The Troubleshooting Methodology

Lesson Overview

To some extent, being an effective troubleshooter simply involves having a detailed knowledge of how something is supposed to work and the sort of things that typically go wrong. However, the more complex a system is, the less likely it is that this sort of information will be at hand. Consequently, it is important to develop general troubleshooting skills to approach new and unexpected situations confidently.

Learning Outcomes

As you study this lesson, answer the following questions:

- What is the troubleshooting methodology?
- Why would a technician want to utilize a process to troubleshoot?

Best Practice Methodology

Troubleshooting starts with a process of problem solving. It is important to realize that problems have causes, symptoms, and consequences. For example:

- A computer system has a fault in the hard disk drive (cause).
- Because the disk drive is faulty, the operating system is displaying a "blue screen" (symptom).
- Because of the fault, the user cannot do any work (consequence).

From a business point of view, resolving the consequences or impact of the problem is more important than solving the original cause. For example, the most effective solution might be to provide the user with another workstation, then get the drive replaced.

Problems also need to be dealt with according to priority and severity. The disk issue affects a single user and cannot take priority over issues with wider impact, such as a data center suddenly losing power.

It is also important to realize that the cause of a specific problem might be the symptom of a larger problem. This is particularly true if the same problem recurs. For example, you might ask why the disk drive is faulty; is it a one-off error, or are there problems in the environment, supply chain, and so on?

These issues mean that the troubleshooting procedures should be developed in the context of best practice methodologies and approaches. One such best practice framework is CompTIA's troubleshooting model, or methodology.



Note: The troubleshooting methodology is not tied to an exam objective, but covers background information that an IT specialist will be expected to know.

The steps in this model are as follows:

1. Identify the problem:
 - a) Gather information from the user, identify user changes, and, if applicable, perform backups before making changes.
 1. Begin documentation of the problem. Update as necessary throughout the full process.
 - b) Inquire regarding environmental or infrastructure changes.
2. Establish a theory of probable cause (question the obvious):
 - a) If necessary, conduct external or internal research based on symptoms.
3. Test the theory to determine the cause:
 - a) Once the theory is confirmed, determine the next steps to resolve the problem.
 - b) If the theory is not confirmed, reestablish a new theory or escalate.
4. Establish a plan of action to resolve the problem and implement the solution:
 - a) Refer to the vendor's instructions for guidance.
5. Verify full-system functionality and, if applicable, implement preventive measures.
6. Document the findings, lessons learned, actions, and outcomes.

Identify the Problem

The troubleshooting process starts by **identifying the problem**. Identifying the problem means establishing the consequence or impact of the issue and listing symptoms. The consequence can be used to prioritize each support case within the overall process of problem management.

Gather Information from the User

The first report of a problem will typically come from a user or another technician, and this person will be one of the best sources of information if you can ask the right questions. Before you begin examining settings in Windows or taking the PC apart, spend some time **gathering information from the user** about the problem. Ensure you ask the user to describe *all* the circumstances and symptoms. Some good questions to ask include:

- What are the exact error messages appearing on the screen or coming from the speaker?
- Is anyone else experiencing the same problem?
- How long has the problem been occurring?
- What changes have been made recently to the system? Were these changes initiated by you or via another support request?
- If something worked previously, then **experiences** mechanical failures, are there any changes made by the user or from **environmental or infrastructure change**?
- Have you tried anything to solve the problem?

Perform Backups

Consider the importance of data stored on the local computer when you open a support case. Check when a **backup** was last made. If a backup has not been made, perform one before changing the system configuration, if possible.

Establish and Test a Theory

If you obtain accurate answers to your initial questions, you will have determined the severity of the problem (how many are affected), a rough idea of what to investigate (hardware or OS, for instance), and whether to consider the cause as deriving from a recent change, an oversight in the initial configuration, or some unexpected environmental or mechanical event.

You diagnose a problem by identifying the symptoms. By knowing what causes such symptoms, you can consider possible causes to determine the probable cause and then devise tests to show whether it is the cause or not. If you switch your television on and the screen remains dark, you could ask yourself, "Is the problem in the television? Has the fuse blown? Is there a problem at the broadcasting station rather than with my television?" With all problems, we run through a list of possibilities before deciding. The trick is to do this methodically (so that possible causes are not overlooked) and efficiently (so that the problem can be solved quickly).

Conduct Research

You cannot always rely on the user to describe the problem accurately or comprehensively. You may need to use research techniques to identify or clarify symptoms and possible causes. One of the most useful troubleshooting skills is being able to perform research to find information quickly. Learn to use web and database search tools so that you can locate information that is relevant and useful. Identify different knowledge sources available to you. When you research a problem, be aware of both internal documentation and information and external support resources, such as vendor support or forums.

- Make a physical inspection; look and listen. You may be able to see or hear a fault (scorched motherboard, "sick"-sounding disk drive, no fan noise, and so on).
- If the symptoms of the problem are no longer apparent, a basic technique is to reproduce the problem; that is, repeat the exact circumstances that produced the failure or error. Some problems are intermittent, though, which means that they cannot be repeated reliably. Issues that are transitory or difficult to reproduce are often the hardest to troubleshoot.
- Check the system documentation, installation and event logs, and diagnostic tools for useful information.
- Consult other technicians who might have worked on the system recently or might be working now on some related issue. Consider that environmental or infrastructure changes might have been instigated by a different group within the company. Perhaps you are responsible for application support, and the network infrastructure group has made some changes without issuing proper notice.
- Consult vendor documentation and use web search and forum resources to see if the issue is well-known and has an existing fix.

Question the Obvious

As you identify symptoms and diagnose causes, take care not to overlook the obvious; sometimes seemingly intractable problems are caused by the simplest things. Diagnosis requires both attention to detail and a willingness to be systematic.

One way to consider a computer problem systematically is to step through what should happen, either by performing the steps yourself or by observing the user. Hopefully, this will identify the exact point at which there is a failure or error.

If this approach does not work, break the troubleshooting process into compartments or categories, such as power, hardware components, drivers/firmware, software, network, and user actions. If you can isolate your investigation to a particular subsystem by eliminating non-causes, you can troubleshoot the problem more quickly. For example, when troubleshooting a PC, you might work as follows:

1. Decide whether the problem is hardware or software related.
2. Decide which hardware subsystem is affected, including the hard drive, power supply, and random access memory.
3. Decide whether the problem is in the physical disk unit or the connectors and cabling. With software issues, you may want to uninstall and then reinstall the software or perform a repair of the file system.
4. Test your theory.

Tip: A basic technique when troubleshooting a cable, connector, or device is to have a "known good" duplicate on hand. This is another copy of the same cable or device that you know works that you can use to test by substitution.

Related information

[\(R\) Question the Obvious 01 question](#) on page 0

[\(Ap\) Question the Obvious 02 question](#) on page 0

[\(Ap\) Question the Obvious 03 question](#) on page 0

[\(An\) Question the Obvious 04 question](#) on page 0

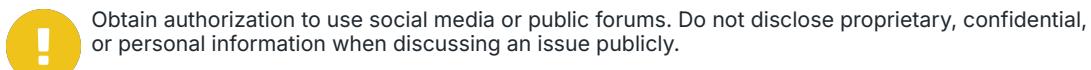
Establish a New Theory or Escalate

If your theory is not proven by the tests you make or the research you undertake, you must **establish a new theory**. If one does not suggest what you have discovered so far, there may be more lengthy procedures you can use to diagnose a cause. Remember to assess business needs before embarking on very lengthy and possibly disruptive tests. Is there a simpler workaround that you are overlooking?

If a problem is particularly intractable, you can take the system down to its base configuration (the minimum needed to run). When this works, you can then add peripherals and devices or software subsystems one by one, testing after each, until eventually the problem is located. This is time-consuming but may be necessary if nothing else provides a solution.

If you cannot solve a problem yourself, it is better to use issue [escalation](#) than to waste a lot of time trying to come up with an answer. Formal escalation routes depend on the type of support service you are operating and the terms of any warranties or service contracts that apply. Some generic escalation routes include:

- Senior technical and administrative staff, subject matter experts (SMEs), and developers/programmers within your company.
- Suppliers and manufacturers via warranty and support contracts and helplines or web contact portals.
- Other support contractors/consultants, websites, and social media.



Obtain authorization to use social media or public forums. Do not disclose proprietary, confidential, or personal information when discussing an issue publicly.

Choosing whether to escalate a problem is complex because you must balance the need to resolve a problem in a timely fashion against the possibility of incurring additional costs or adding to the burdens that senior staff are already coping with. You should be guided by policies and practices in the company you work for. When you escalate a problem, make sure that what you have found out or attempted so far is documented. After that, describe the problem clearly to whoever takes over or provides you with assistance.

Implement a Plan of Action

When you have a reliable theory of probable cause, you then need to determine the **next steps to solve the problem**.

Troubleshooting is not just a diagnostic process. Devising and implementing a plan to solve the problem requires effective decision-making. Sometimes, there is no simple solution. There may be several solutions, and which is best might not be obvious. An apparent solution might solve the symptoms of the problem but not the cause. A solution might be impractical or too costly. Finally, a solution might be the cause of further problems, which could be even worse than the original problem.

There are typically three generic approaches to resolving an IT problem:

- **Repair:** You need to determine whether the cost of repair makes this the best option.
- **Replace:** This is often more expensive and may be time-consuming if a part is not available. There may also be an opportunity to upgrade the part or software.
- **Workaround:** Not all problems are critical. If neither repair nor replacement is cost-effective, it may be best to either find a workaround or just document the issue and move on.

 If a part or system is under warranty, you can return the broken part for a replacement. To do this, you normally need to obtain a returned materials authorization (RMA) ticket from the vendor.

Establish a Plan of Action

When you determine the best solution, you must devise a **plan of action** to put the solution in place. You have to assess the resources, time, and cost required. Another consideration is potential **impacts** on the rest of the system that your plan of action may have. A typical example is applying a software patch, which might fix a given problem but cause other programs not to work.

An effective change and configuration management system will help you to understand how different systems are interconnected. You must seek the proper authorization for your plan and conduct all remedial activities within the constraints of **corporate policies and procedures**.

Implement the Solution

If you do not have authorization to implement a solution, you will need to escalate the problem to more senior personnel. If applying the solution is disruptive to the wider network or business, you also need to consider the most appropriate time to schedule the reconfiguration work and plan how to notify other network users.

When you make a change to the system as part of **implementing a solution**, test after each change. If the change does not fix the problem, reverse it and then try something else. If you make a series of changes without recording what you have done, you could find yourself in a tricky position.

 **Note:** Remember that troubleshooting involves more than fixing a particular problem; it is about maintaining the resources that users need to do their work.

Refer to Vendor Instructions

If you are completing troubleshooting steps **under instruction** from another technician—the vendor's support service, for instance—make sure you properly understand the steps you are being asked to take, especially if it requires disassembly of a component or reconfiguration of software that you are not familiar with.

Verify and Document

When you apply a solution, test that it fixes the reported problem and that the **system as a whole continues to function normally**. Tests could involve any of the following:

- Trying to use a component or performing the activity that prompted the problem report
- Inspecting a component to see whether it is properly connected or damaged or whether any status or indicator lights show a problem
- Disabling or uninstalling the component (if it might be the cause of a wider problem)
- Consulting logs and software tools to confirm a component is configured properly
- Updating software or a device driver

Before you can consider a problem closed, you should both be satisfied in your own mind that you have resolved it and get the customer's acceptance that it has been fixed. Restate what the problem was and how it was resolved, and then confirm with the customer that the incident log can be closed.

Implement Preventive Measures

To fully solve a problem, you should implement **preventive measures**. This means eliminating any factors that could cause the problem to reoccur. For example, if the power cable on a PC blows a fuse, you should not only replace the fuse, but you should also check to see if there are any power problems in the building that may have caused the fuse to blow in the first place. If a computer is infected with a virus, ensure that the antivirus software is updating itself regularly and users are trained to avoid malware risks.

Document Findings, Lessons Learned, Actions, and Outcomes

Most troubleshooting takes place within the context of a ticket system. This shows who is responsible for any particular problem and what its status is. This gives you the opportunity to add a complete description of the problem and its solution (**findings, lessons learned, actions, and outcomes**).

This is very useful for future troubleshooting, as problems fitting into the same category can be reviewed to see if the same solution applies. Troubleshooting steps can be gathered into a "Knowledge Base" or Frequently Asked Questions (FAQ) of support articles. They also help to analyze IT infrastructure by gathering statistics on what types of problems occur and how frequently.

The other value of a log is that it demonstrates what the support department is doing to help the business. This is particularly important for third-party support companies, who need to prove the value achieved in service contracts. When you complete a problem log, remember that people other than you may come to rely on it. Also, logs may be presented to customers as proof of troubleshooting activity. Write clearly and concisely, checking for spelling and grammar errors.

Module 2

Installing Motherboards and Connectors

Module Overview

One of the main roles of a CompTIA A+ technician is to install and configure personal computer (PC) hardware. This hands-on part of the job is what draws many people to a career in information technology (IT) support. As an IT professional, you will set up desktop computers and help end users select a system configuration and peripheral devices that are appropriate to their work. You will often have to connect peripheral devices using the correct cables and connectors and install plug-in adapter cards.

To complete these tasks, you must understand how the peripheral devices and internal PC components are connected via the motherboard. As you may encounter many different environments in your work, you must also be able to distinguish and support both modern and legacy connection interfaces.

Module Summary

Prepare for A+ Core 1 by:

- Explaining cable types and connectors.
- Installing and configuring motherboards.
- Explaining legacy cable types.

Lesson 2A

Cables and Connectors

Lesson Overview

As an IT professional, you are tasked with setting up a new office for a small business. The office includes multiple workstations, a conference room, and various types of network equipment. You must ensure all components are properly connected, configured, and functional. In this lesson, you will learn the different components of a PC and how they all communicate with each other and function properly.



Objectives Covered

- 3.1 Compare and contrast display components and attributes.
- 3.2 Summarize basic cable types and their connectors, features, and their purposes.

Learning Outcomes

As you study this lesson, answer the following questions:

- How would you upgrade the internal components of the older PCs?
- What video adapters (e.g., HDMI to DisplayPort) are appropriate for connecting monitors to PCs?
- When is it necessary to use powered USB hubs to support multiple devices?
- How can USB hubs be used to expand the number of available USB ports on each workstation?
- How do you mount a 4K display in the conference room and connect it to the power source?
- What steps should be taken to ensure all connections are secure and to test each input source for proper video and audio transmission?
- What are the steps to use Lightning to USB adapters to connect iPhones and iPads to PCs for data transfer and charging?
- How do you open the tower cases of file servers and install new SATA hard drives?

Personal Computers

PC components are divided into user-handled peripheral devices and internal components housed in the system case, which could be damaged or dangerous if exposed. Peripherals include input devices (keyboard, mouse, microphone, camera), output devices (reference display/monitor, speakers), and external storage. The case or chassis, typically a vertical tower, contains the internal components, such as the motherboard, CPU, memory modules, adapter cards, fixed disks, and power supply unit.



PCs can also be purchased as all-in-one units. All-in-one means that the internal components are contained within a case that is also a monitor.

To perform PC maintenance, you must understand how to open a desktop computer's case.

- A tower case has a side cover that slides off, secured by screws or clips, and may have anti-tamper mechanisms. Always refer to system documentation and follow recommended steps.
- The front panel provides access to removable media drives, a power switch, and LEDs. It can be removed but may require removing the side panel first to access its screws or clips.

The front of a typical PC case

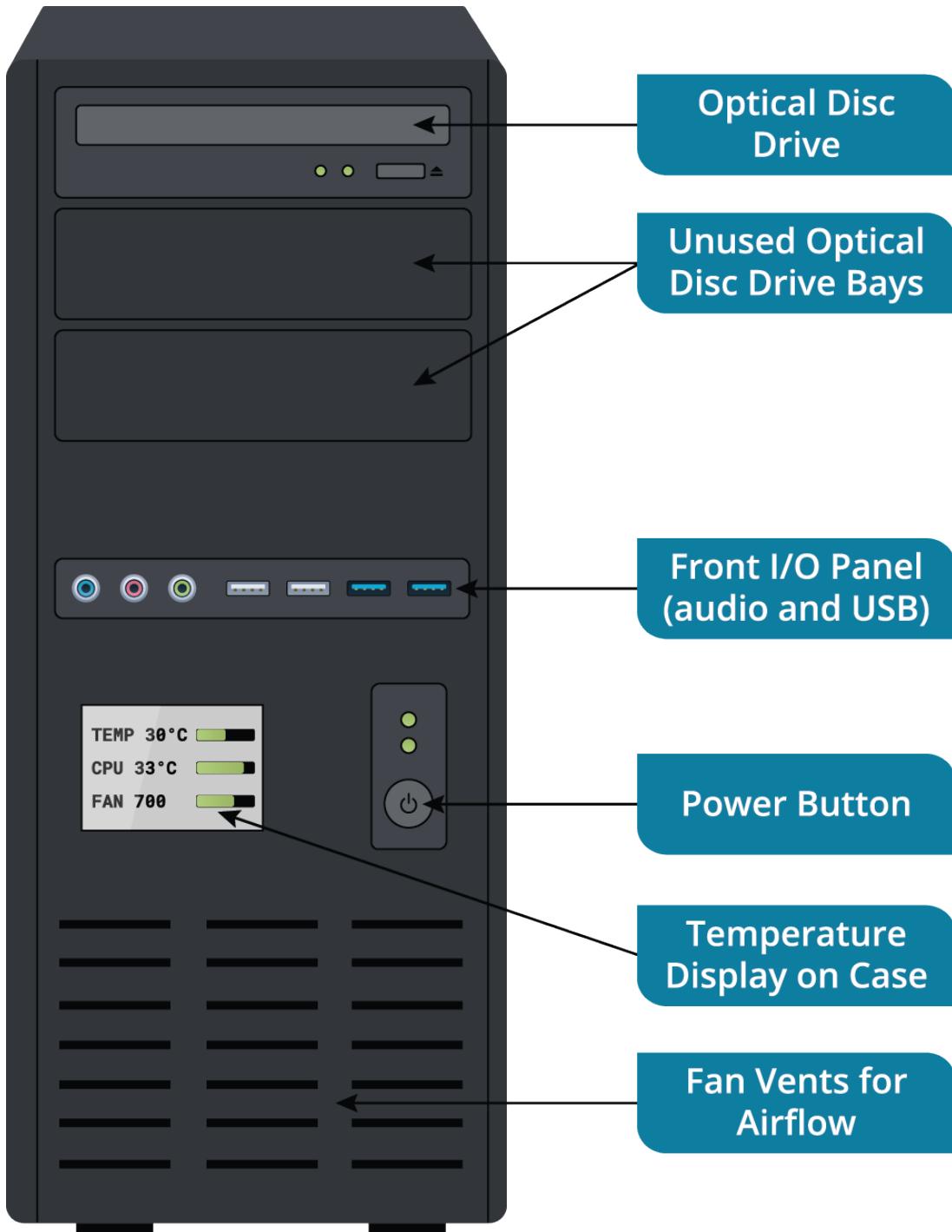


Image © 123RF.com.

The rear panel provides access to the power supply unit (PSU) sockets, which include an integral fan exhaust. Ensure the fan is unobstructed to maintain proper cooling. There may also be an additional case fan.

The rear panel of a typical PC case

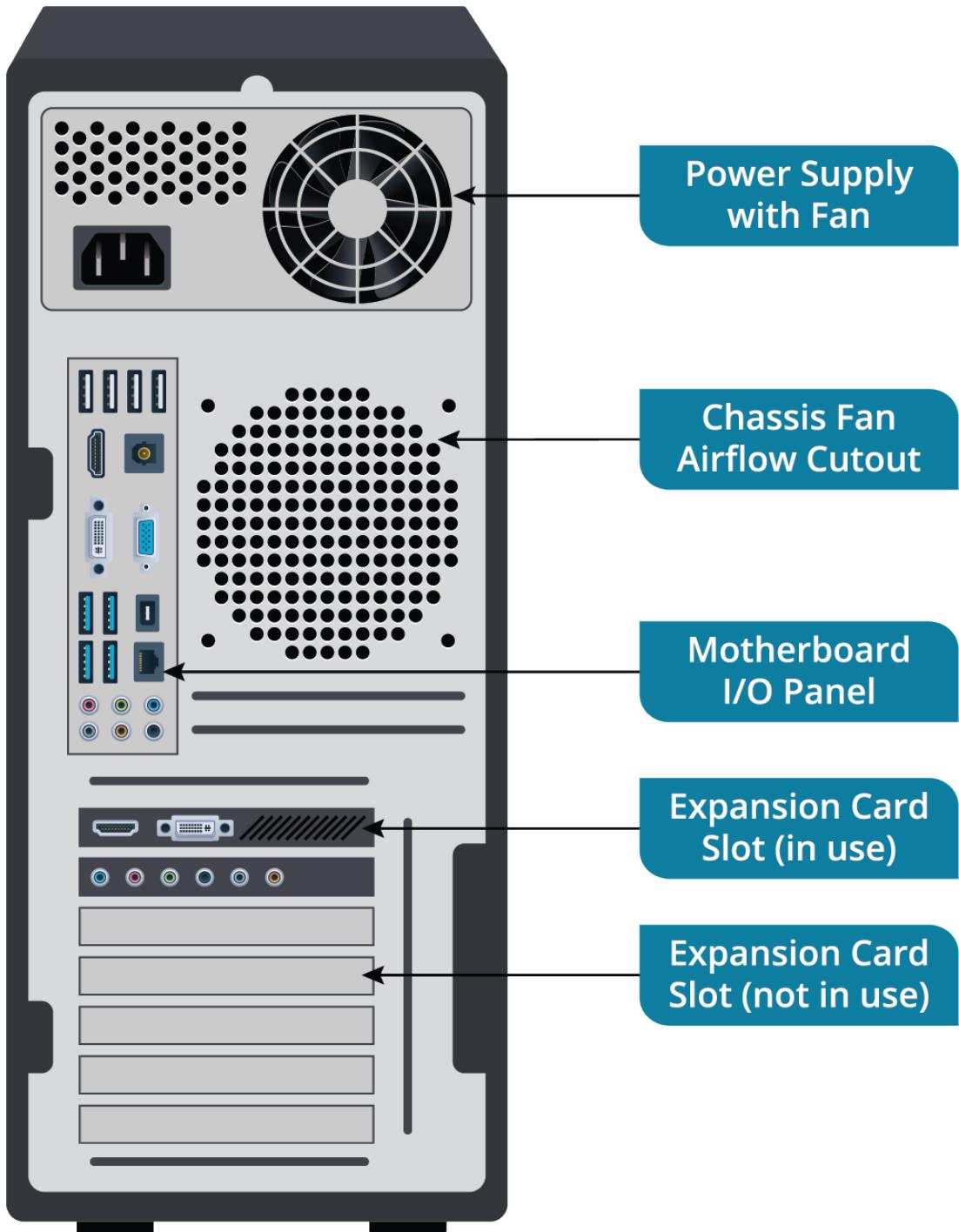


Image © 123RF.com

Power supply with fan is located at the top. Chassis fan airflow cutout is a circular vent below the power supply. Motherboard input output panel is a section containing various ports. Expansion card slot in use and expansion card slot not in use are located below the motherboard input output panel and chassis fan airflow cutout.

Below the PSU, a cutout aligns with the motherboard's input/output (I/O) ports for peripheral connections, covered by an I/O shield to keep out dust. At the bottom of the rear panel, cutout slots align with adapter card slots, covered by either an adapter card or a blanking plate. These shields and plates prevent gaps in the case, which can cause:

- Dust entry, leading to component overheating.
- Increased exposure to electrostatic discharge (ESD), which can damage chips. The I/O shield's pins connect external metal parts to the metal case and PSU, providing a safe path for ESD to ground.
- Increased exposure to electromagnetic interference (EMI). EMI is energy from magnetic and electrical sources, such as motors or other electronic devices, which can cause temporary or permanent faults. The case absorbs EMI, but gaps reduce this protection.

Peripheral Devices

An input/output (I/O) port connects devices to the PC via peripheral cables. Some ports are specific, like a graphics port for a monitor, while others support various devices. External ports are located at the rear or front of the PC through case cutouts and can be on the motherboard or an expansion card.

I/O ports on a motherboard

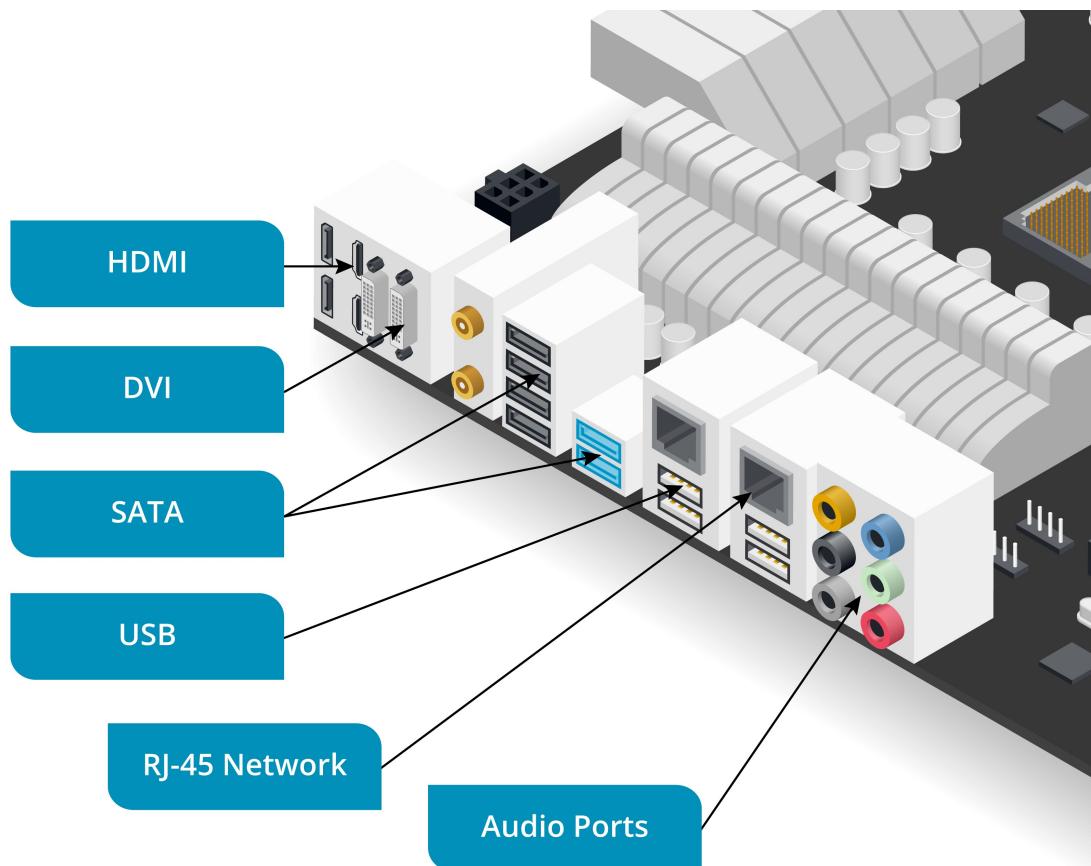


Image © 123RF.com.

The ports are as follows: H D M I, D V I, S A T A, U S B, R J-45 Network, and audio ports.

Interfaces, Ports, and Connectors

A hardware port is the external connection point for a bus interface, allowing data transfer to and from devices. The connector is the part of a peripheral cable that fits into a matching port. Each bus interface may use multiple connector types. Most connectors and ports now use edge contacts and are either asymmetric or keyed to prevent incorrect insertion or are reversible.

Peripheral cable for the Universal Serial Bus (USB) interface

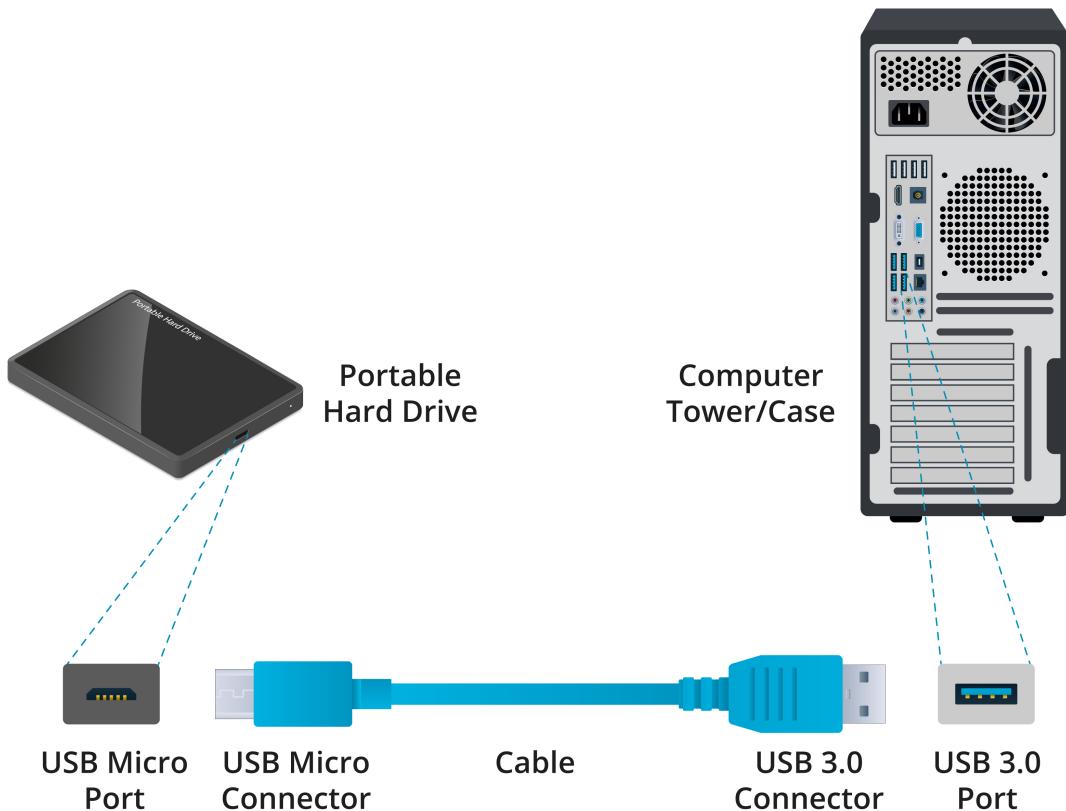


Image © 123RF.com.

A portable hard drive has a U S B micro port labeled. A U S B cable is shown with two ends: a U S B micro connector on the left and a U S B 3.0 Connector on the right. A back view of the computer tower has a U S B 3.0 Port.

Binary Data Storage and Transfer units

When comparing bus interfaces, use appropriate units. Computers process binary data, where each digit or bit (b) is a 0 or 1. Storage is measured in bytes (B), which are eight bits. A lowercase "b" refers to a bit, while an uppercase "B" means a byte.

Transfer rates are expressed in units per second of the following multiples of bits and bytes:

- 1000—Kilobits (Kb/s or Kbps) and kilobytes (KB/s and KBps).
- 1000×1000 —Megabits (Mb/s) or megabytes (MB/s).

- $1000 \times 1000 \times 1000$ —Gigabits (Gb/s) and gigabytes (GB/s).

Universal Serial Bus Cables

The Universal Serial Bus (USB) is the standard for connecting most peripheral devices to a computer. USB devices are categorized into classes like human interface (keyboards and mice), mass storage (disk drives), printers, and audio devices. A USB is managed by a host controller, which supports multiple ports on the same bus. Each controller can theoretically support up to 127 devices, but to overcome bandwidth limitations, most PC motherboards have multiple USB controllers, each with three or four ports.

USB port symbol



USB Connector Types

USB 2 connector form factors include:

- Type A: Flat rectangular connector for host and some peripheral devices, inserted with the USB symbol facing up.
- Type B: Square connector with a beveled top for large devices like printers.
- Type B Mini: Smaller connector for smaller peripheral devices like early digital cameras, but now rarely used.
- Type B Micro: Flatter connector for smaller devices like smartphones and tablets.

USB 2 ports and connectors



Image © 123RF.com

The ports and the connectors are as follows. Type A: A flat rectangular connector with a matching rectangular port. Type B: A square connector with a slightly beveled top and a matching port. Type B Mini: A smaller trapezoidal connector with a matching port. Type B Micro: An elongated trapezoidal connector with a matching port.

A USB cable can have Type A to Type A connectors or convert between types (e.g., Type A to Type B or Type A to Micro Type B).

USB 3 introduces new versions of Type A, Type B, and Type B Micro connectors with additional signaling pins and wires, often distinguished by a blue connector tab or housing. USB 3.0 Type A connections are physically compatible with USB 1.1 and 2.0, but Type B and Type B Micro connections are not. For example, you can plug a USB 2 Type A cable into a USB 3 Type A port, but not a USB 3 Type B cable into a USB 2 Type B port.

USB 3 connectors and ports (from left to right): Type A, Type B, Micro Type B, Type C

USB 3.0 and 3.1

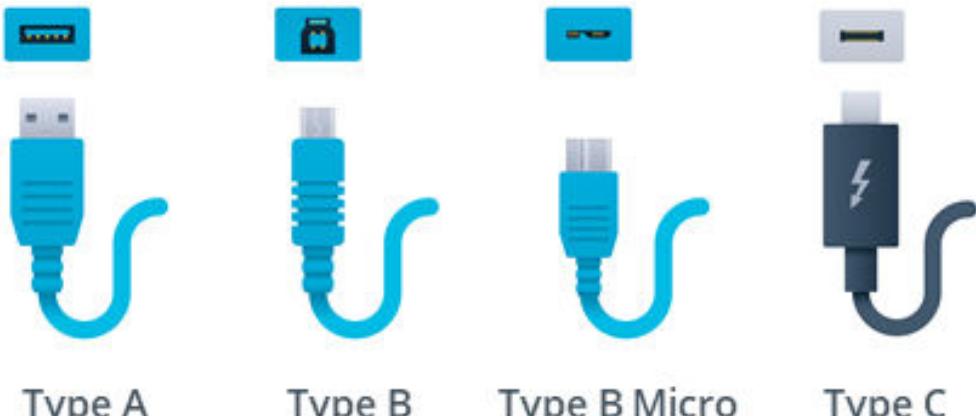


Image © 123RF.com

The ports and the connectors are as follows. Type A: A flat rectangular connector with a matching rectangular port. Type B: A square connector with a slightly beveled top and a matching port. Type B Micro: A smaller connector with a dual-layer design with a matching port. Type C: A connector with rounded edges and a thunderbolt symbol on it with a matching port.

USB 3.1 introduces the USB-C connector, a compact, reversible, and durable design aimed at providing a consistent hardware interface. USB-C connectors can be used at both ends of a cable or paired with converter cables to connect to USB Type A or Type B ports.

Cable Length

The maximum cable length is 3 meters for LowSpeed devices and 5 meters for FullSpeed and HighSpeed devices. While vendors may offer longer cables, performance may degrade beyond these lengths. For SuperSpeed-capable cables, a recommended length is up to 3 meters, though there is no official maximum.

Power

In addition to supplying a data signal, the USB bus can supply power to connected devices. Most USB Type A and Type C ports can charge device batteries.



Note: Basic USB ports can provide up to 4.5 watts, depending on the version. Power Delivery (PD) ports can supply up to 100 watts with suitable connectors and cables.

USB Standards

The evolution of the USB standard has brought significant improvements in speed, power delivery, and functionality:

1. USB 1.0 (1996): Introduced with speeds of 1.5 Mbps (Low Speed) and 12 Mbps (Full Speed), using Type-A and Type-B connectors.

2. USB 1.1 (1998): Enhanced USB 1.0 with the same speeds but improved compatibility and reliability.
3. USB 2.0 (2000): Increased speed to 480 Mbps (High Speed) and introduced Mini-A/B and Micro-A/B connectors.
4. USB 3.0 (2008): Introduced SuperSpeed at 5 Gbps and new connectors like Micro-B, later rebranded as USB 3.1 Gen 1.
5. USB 3.1 (2013): Brought SuperSpeed+ at 10 Gbps and the versatile Type-C connector, rebranded as USB 3.1 Gen 2.
6. USB 3.2 (2017): Offered Gen 1 (5 Gbps), Gen 2 (10 Gbps), and Gen 2x2 (20 Gbps) speeds, using Type-A, Type-B, and Type-C connectors.
7. USB4 (2019): Achieved speeds up to 40 Gbps, unified with Thunderbolt 3, exclusively using the Type-C connector, and supported advanced features like multiple data and display protocols.



Note: SuperSpeed branding has been deprecated in favor of simpler bitrate labels: USB 5Gbps, USB 10Gbps, USB 20Gbps, and USB 40Gbps.

Display Types

Display technologies have evolved significantly, offering various types to meet different needs. Liquid Crystal Displays (LCDs) are the most common, with three main subtypes:

- **In-Plane Switching (IPS):** A type of liquid crystal display technology where the liquid crystals are aligned parallel to the screen, allowing for consistent light transmission and color reproduction.
- **Twisted Nematic (TN):** A type of liquid crystal display technology where the liquid crystals twist 90 degrees between the electrodes to control light passage and create images on the screen.
- **Vertical Alignment (VA):** A type of liquid crystal display technology where the liquid crystals are aligned vertically to the glass substrates and tilt when voltage is applied to control light passage and create images.

In addition to LCDs, display technologies include OLED and Mini-LED options. An **Organic Light-Emitting Diode (OLED)** display is a type of display technology where each pixel emits its own light through organic compounds when an electric current is applied. A **Mini-LED** display is a type of display technology that uses thousands of tiny LEDs for backlighting, allowing for more precise control of brightness and contrast in the image.

When comparing display technologies, it is essential to consider the pros and cons of IPS-LCD, TN-LCD, VA-LCD, OLED, and Mini-LED displays to determine which option best meets specific needs for color accuracy, viewing angles, contrast, and overall performance.

- In-Plane Switching (IPS) LCD:
 - Pros: Superior color accuracy and wide viewing angles, making them ideal for graphic design and professional use.
 - Cons: Typically, slower response times compared to TN panels, which may affect fast-paced gaming.
- Twisted Nematic (TN) LCD:
 - Pros: Faster response times and higher refresh rates, which are preferred for gaming.
 - Cons: Poorer color reproduction and limited viewing angles.
- Vertical Alignment (VA) LCD:
 - Pros: Better color accuracy and viewing angles than TN.

- Cons: Slower response times than TN but better than IPS in some cases. VA panels can exhibit color shifting when viewed from extreme angles.
- Organic Light-Emitting Diode (OLED):
 - Pros: Excellent color accuracy, contrast ratios, energy efficiency, and true blacks due to self-emissive pixels.
 - Cons: Potential for burn-in, where static images can leave permanent marks if displayed for long periods.
- Mini-LED Technology:
 - Pros: Mini-LED technology offers improved brightness, better contrast and black levels, enhanced color accuracy, and reduced halo effect, allowing for thin and lightweight display designs suitable for a variety of applications.
 - Cons: Mini-LED displays are more expensive, can consume more power than OLEDs, and while they reduce blooming, they do not achieve the true blacks of OLED technology and add complexity to the manufacturing process.



Mini-LED is an enhancement for LCDs, not a type of OLED.

Display Components

Understanding display components and attributes is essential for evaluating the performance and suitability of various screens. Key elements include touch screens and digitizers for interactivity, inverters for older LCD backlighting, and critical attributes like pixel density, refresh rates, and screen resolution that determine image quality and clarity.

1. Touch Screens and Digitizers:

- Integral for interactive displays, allowing direct interaction through touch or stylus. This is common in smartphones, tablets, and some laptops.

2. Inverter:

- Crucial in older LCDs for converting DC power to AC for the backlight. Modern displays with LED backlighting typically do not require an inverter.

3. Pixel Density, Refresh Rates, and Screen Resolution:

- Pixel Density: Higher density results in sharper images.
- Refresh Rates: Higher rates (measured in Hz) provide smoother motion, which is important for gaming and video playback.
- Screen Resolution: Defines clarity and detail of the display. Common resolutions include:
 - Full HD (1920×1080)
 - Quad HD (2560×1440)
 - 4K (3840×2160)
 - Newer Resolutions: 5K (5120×2880) and 8K (7680×4320) are emerging, offering even higher clarity and detail.
- Color Gamut: Refers to the range of colors a display can produce based on the RGB color model. A wider color gamut allows for more vibrant and accurate color reproduction, enhancing the visual experience for activities such as photo editing, video production, and gaming. Common color gamuts include sRGB, Adobe RGB, and DCI-P3, with DCI-P3 offering a broader range of colors compared to sRGB. Additionally, color depth plays a crucial role, with 24-bit color (often referred to as true color) supporting approximately 16.7 million

colors, while 32-bit color includes an alpha channel for transparency, providing even more detailed color representation and smoother gradients.

Video Cable Bandwidth

Video cable bandwidth is determined by two main factors:

- Resolution: Measured in pixels (e.g., 1920×1080 for Full HD, 3840×2160 for 4K).
- Refresh Rate: Measured in hertz (Hz) or frames per second (fps).

For example, uncompressed HD video at 60 fps requires 4.5 Gbps, while 4K at 60 fps requires 8.91 Gbps.

 **Note:** Frame rate (fps) describes the video source, while hertz (Hz) indicates the display's refresh rate. To avoid artifacts like ghosting and tearing, the refresh rate should match or be divisible by the frame rate. For example, a 60 fps video will play smoothly on a 120 Hz display.

 **Note:** An LCD/TFT is often called a flat-panel or LED display, named after its backlight technology (older models use fluorescent tubes). Premium monitors use organic LED (OLED) technology, where each pixel is its own light source, offering superior contrast and color fidelity.

HDMI and DisplayPort Video Cables

Both HDMI (High-Definition Multimedia Interface) and DisplayPort cables have their distinct advantages, and it's important to select the appropriate cable based on the specific needs of the device and the desired performance outcomes.

High-Definition Multimedia Interface (HDMI)

HDMI cables are essential for multimedia setups due to its simplicity and versatility:

- **Functionality:** Transmits both high-definition video and audio signals through a single cable.
- **Standard Use:** Commonly used for connecting consumer electronics such as:
 - Televisions
 - Monitors
 - Gaming consoles
- **Versions:** Available in various versions, with the latest offering:
 - Higher resolutions
 - Increased refresh rates
 - Advanced features like HDR (High Dynamic Range) for enhanced color and contrast
- **Advantages:**
 - Single-cable solution simplifies connections
 - Broad compatibility with a wide range of devices

DisplayPort

DisplayPort offers superior performance for high-resolution and multi-display configurations, making it a top choice for demanding visual applications.

- **Purpose:** Digital display interface for connecting a video source to a display device, such as a computer monitor.
- **Preferred Use:**

- Professional environments
 - Gaming setups
- **Key Features:**
 - Supports higher resolutions and refresh rates than HDMI
 - Multi-Stream Transport (MST) allows multiple displays to connect through a single port, ideal for multi-monitor setups
 - **Additional Capabilities:**
 - Transmits audio
 - Supports adaptive sync technologies like:
 - AMD FreeSync
 - NVIDIA G-Sync
 - Reduces screen tearing in gaming applications

Thunderbolt Interface

Although the Thunderbolt and Lightning interfaces are most closely associated with Apple computers and mobile devices, Thunderbolt is increasingly implemented on Windows and Linux PCs too.

Thunderbolt can be used as a display interface like DisplayPort or HDMI and as a general peripheral interface like USB.

- Thunderbolt 1 and 2: Use the same physical interface as MiniDP and are compatible with DisplayPort, allowing a monitor with a DisplayPort port to connect via a Thunderbolt port and adapter cable. Thunderbolt ports are marked with a lightning bolt icon. Thunderbolt 2 supports up to 20 Gbps and allows daisy-chaining multiple monitors.
- Thunderbolt 3: Switches to the USB-C physical interface, using the same port, connector, and cabling. Converter cables are available for connecting Thunderbolt 1 or 2 devices to Thunderbolt 3 ports. USB devices function normally in Thunderbolt 3 ports, but Thunderbolt devices won't work in non-Thunderbolt USB-C ports. Thunderbolt 3 supports up to 40 Gbps over short, high-quality cables (up to 0.5 meters).
- Thunderbolt 4: Maintains the USB-C interface and supports up to 40 Gbps, with improved minimum performance requirements and expanded capabilities, such as support for docks with up to four Thunderbolt 4 ports.
- Thunderbolt 5: Also uses the USB-C interface, offering even higher speeds and enhanced features, though specific details may vary as the technology evolves. Thunderbolt ports are versatile, supporting high-speed data transfer, video output, and daisy-chaining multiple devices.

The USB-C form factor adopted for Thunderbolt 4

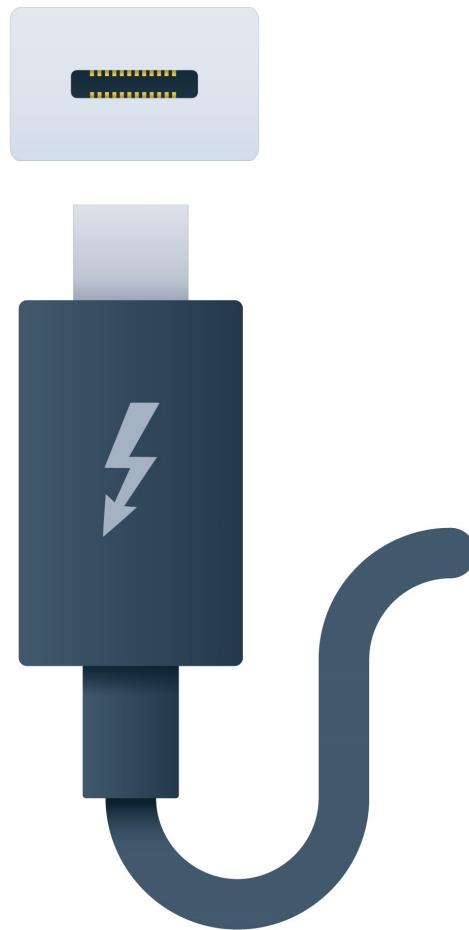


Image ©123RF.com



Note: Not all USB-C ports support Thunderbolt interfaces. Look for the flash icon on the port or check the system documentation to confirm.

Lightning Interface

The Lightning interface, developed by Apple, is a proprietary connector used primarily in iPhone and iPad devices. Introduced in 2012, it replaced the older 30-pin dock connector with a more compact and reversible design, enhancing user convenience.

Exclusively found in Apple's mobile devices, the Lightning port requires a Lightning-to-USB A or Lightning-to-USB C adapter cable for connections to PCs and other devices, facilitating both charging and data transfer.

However, the Lightning interface is being phased out in favor of the USB-C standard. This transition is driven by:

- **Industry Standardization:** USB-C is widely adopted for its versatility, faster data transfer, and higher power delivery.

- **Regulatory Pressure:** Bodies like the European Union advocate for a common charging standard to reduce electronic waste and improve convenience.
- **Technological Advancements:** USB-C offers superior features, making it a more future-proof option.

Apple Lightning connector and port



Image ©123RF.com

Serial Advanced Technology Attachment Interface

As well as external cabling for peripheral devices, some types of internal components use cabling to attach to a motherboard port.

Serial Advanced Technology Attachment (SATA) is the standard for connecting internal storage drives in desktop PCs, using up to 1-meter cables with compact 7-pin connectors, each supporting a single device.

SATA connectors and ports (from left to right): SATA data, SATA power (with 3.3V orange wire)

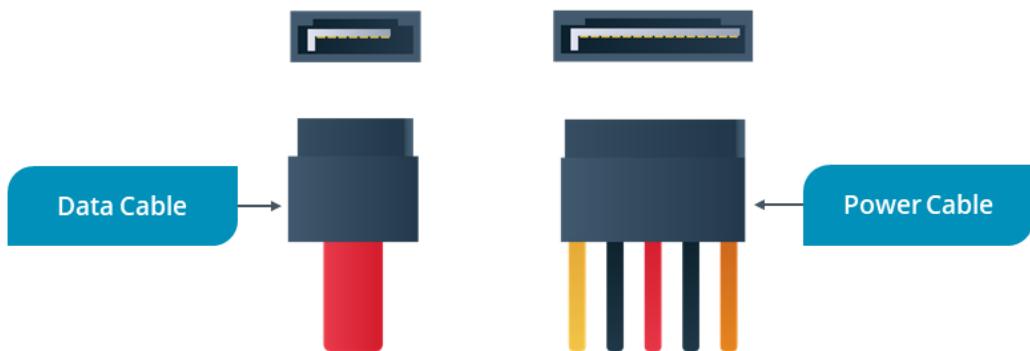


Image ©123RF.com

The 7-pin data connector does not supply power; a separate 15-pin connector is used for power. The initial SATA standard supported speeds up to 150 MBps, which were later increased to 300 MBps with SATA revision 2 and 600 MBps with SATA revision 3.

SATA Revisions 3.1 to 3.5 introduced enhancements like the SATA Universal Storage Module, SATA Express specification, and better integration with I/O protocols but did not increase speeds.

Motherboard SATA and legacy PATA/IDE ports

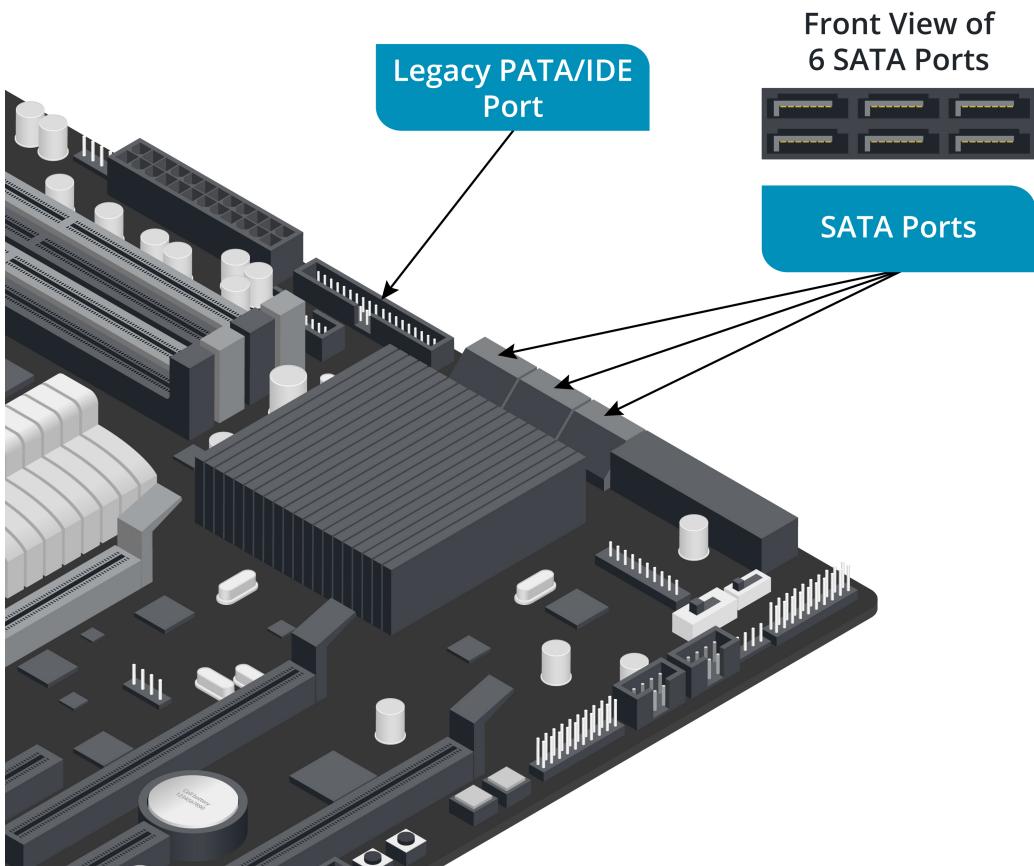


Image ©123RF.com

Molex Power Connectors

Internal storage device data cables are designed solely for data transfer and do not carry power. To supply power, newer devices utilize a SATA power connector, whereas legacy components connect to the power supply unit (PSU) using a 4-pin Molex connector. These connectors are typically made of white or clear plastic.

The Molex connector features wire insulation color codes to indicate different voltage levels: red for 5 volt direct current (VDC), yellow for 12 volt direct current (VDC), and black for ground. Direct current (DC) refers to the unidirectional flow of electric charge, which is essential for powering electronic components.

Molex connector

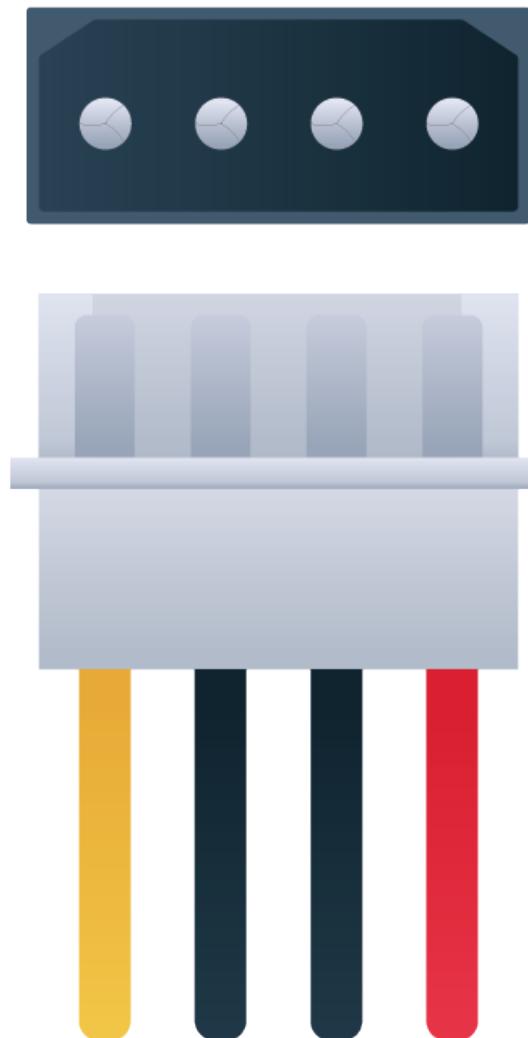


Image ©123RF.com



Some devices might have both SATA and Molex power connectors.

External SATA

The External Serial Advanced Technology Attachment (eSATA) standard allows peripheral drives to connect using a cable up to 2 meters (78 in.) in length. An eSATA cable is required for connection to an external eSATA port; internal SATA cables are not compatible. Some vendors offer a nonstandard powered port called eSATAp, which works with both USB and SATA using an eSATAp cable. Despite this, the USB interface remains the dominant choice for external drives.

Lesson 2B

Motherboards

Lesson Overview

As an IT professional, you are tasked with building and maintaining a set of desktop PCs for a new office. The project involves selecting and installing components, ensuring proper connectivity, and configuring the systems for optimal performance and reliability. In this lesson, you will learn the different motherboard types and capabilities as well as connector types. Knowledge of this will enable you to perform component upgrades and repairs efficiently.



Objectives Covered

- 3.3 Compare and contrast RAM characteristics.
- 3.4 Compare and contrast storage devices.
- 3.5 Given a scenario, install and configure motherboards, CPUs, and add-on cards.

Learning Outcomes

As you study this lesson, answer the following questions:

- What are the steps to install the CPU into the socket, apply thermal paste, and attach the heat sink and fan to manage heat?
- What is the process for installing RAM modules into the color-coded DIMM slots, ensuring they are properly seated and secured?
- How do you use SATA ports on the motherboard to connect SSDs or HDDs for persistent storage?
- What is the process for installing NICs into available PCIe slots to provide network connectivity?
- How do you choose ATX motherboards for full-size cases with up to seven expansion slots?
- How do you identify the correct headers for the power button, HDD activity lights, audio ports, and USB ports?

Motherboard Functions

All computer software and data are processed using binary code (ones and zeroes). Software operates by executing instructions in the central processing unit (CPU), known as the compute or processing function of a PC.

Instructions and data also require storage. The CPU can store only a limited number of instructions internally. Additional storage for running programs and open data files is provided by system memory, or random-access memory (RAM). RAM is *nonpersistent*, meaning it holds data only when the PC is powered on. Mass storage devices are used to preserve data when the computer is turned off.

CPU, cache, and RAM are fast but volatile. Mass storage and removable storage devices provide slower but permanent data retrieval

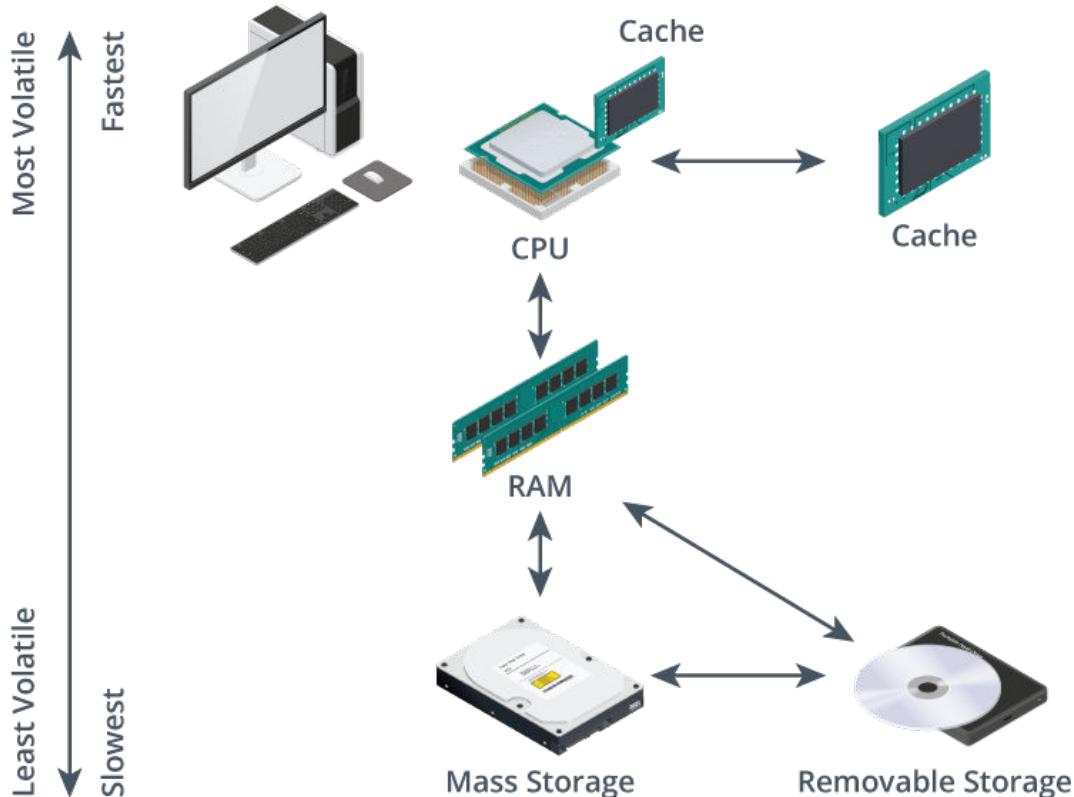


Image ©123RF.com

Data flow between CPU and Cache and that between CPU and RAM is most volatile and fastest. The data flow between RAM and mass storage, between RAM and removable storage, and that between mass storage and removable storage is least volatile and slowest.

Processing and storage components are connected by bus interfaces on the motherboard. Instructions and data are stored using transistors and capacitors and transmitted via electrical signals over the bus. The motherboard's system clock synchronizes all PC operations and provides the basic timing signal for the CPU, measured in megahertz (MHz) or gigahertz (GHz). Clock multipliers adjust the timing signal to produce different speeds for various buses, allowing them to operate at different frequencies.

The type of motherboard affects system speed and determines the range of devices and adapter cards that can be installed or upgraded. Major motherboard manufacturers include AOpen (Acer), ASRock, ASUSTek, Biostar, EVGA Corporation, Gigabyte, Intel, and MSI. Each motherboard supports specific CPU ranges, with PC CPUs primarily made by Intel and Advanced Micro Devices (AMD).

Electrical Safety and ESD

When you open the case to perform upgrades or troubleshooting, you must follow proper operational procedures to ensure your safety and minimize the risk of damaging components.

Electrical Safety

When working with a PC, ensure your safety by disconnecting it from the power supply before opening the case. After unplugging the power cord, hold the power button for a few seconds to drain any remaining charge from internal components. Do not attempt to disassemble non-field-repairable components, such as the power supply.

Electrostatic Discharge

To minimize the risk of damaging sensitive electronic components inside the PC, use appropriate tools and procedures. Components like the CPU, system RAM, adapter cards, and the motherboard are vulnerable to electrostatic discharge (ESD), which occurs when a static charge from your clothes or body is suddenly released into a circuit by touch. Handle components by their edges or plastic parts, and ideally, use an anti-ESD wrist strap and other protective equipment and procedures.

ESD wrist strap on ESD mat



Image by Audrius Merfeldas ©123RF.com



Note: Operational procedures covering personal safety and the use of anti-ESD equipment are covered in more detail in the Core 2 course.

Motherboard CPU and System Memory Connectors

All motherboards have a variety of **connector types** and socket types for the system devices: CPU, memory, fixed disk drives, and adapter cards.

Motherboard connectors

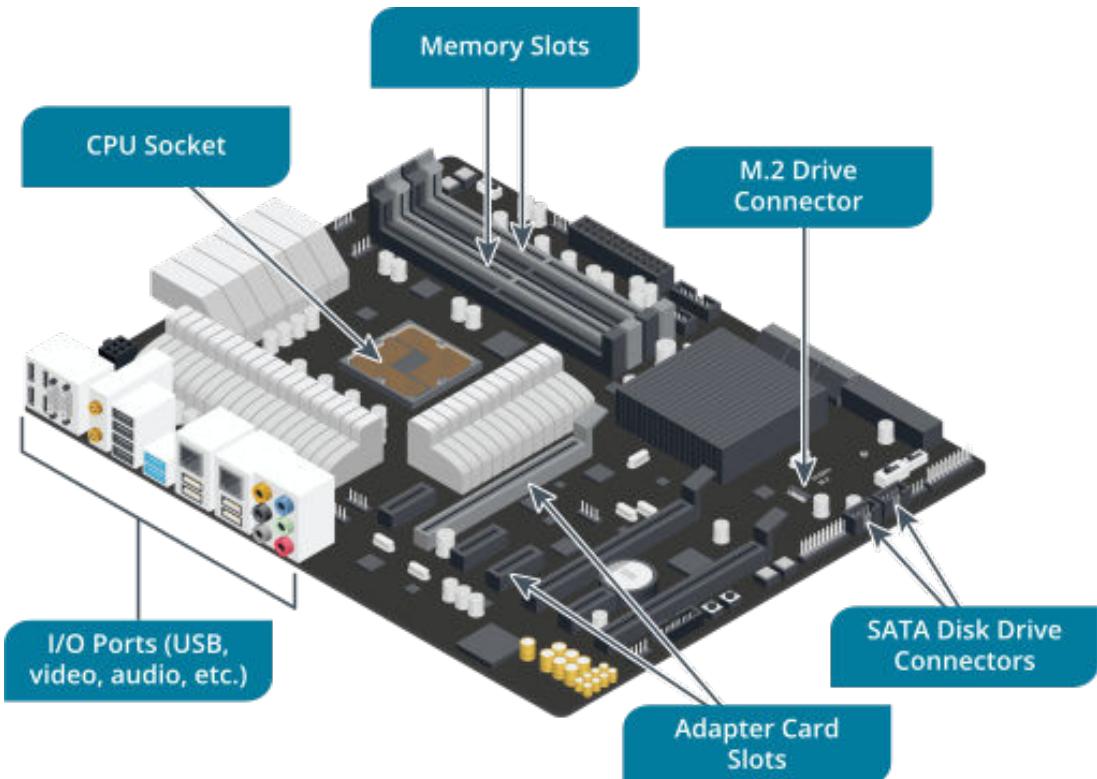


Image © 123RF.com

CPU Sockets

New motherboards are typically released to support the latest CPU models from major manufacturers like Intel and AMD, each of which uses different socket designs. Due to rapid advancements in CPU technology, a motherboard will only support a limited range of processor models.

The CPU socket has a distinctive square shape. Once the CPU is installed, it is covered with thermal paste, a heat sink, and a fan to manage heat.

The motherboard's chipset supports the CPU by managing data transfer between the CPU and various devices. This chipset is soldered onto the motherboard and cannot be upgraded. The chipset determines the compatible processors, the type and maximum amount of RAM, and support for integrated interfaces such as video, sound, and networking. Interfaces not supported by the chipset can be added or upgraded via adapter cards.

System Memory Slots

System memory uses random-access memory (RAM) technology, which is volatile and loses its contents when power is removed. Program code and data are loaded into RAM for access and execution by the processor.

System RAM is typically packaged as dual inline memory modules (DIMMs) that fit into motherboard slots near the CPU socket. These slots have catches at either end and are often numbered and color-coded. Labels next to the slots usually indicate the type of DIMMs supported.

RAM technologies have evolved through generations like DDR3, DDR4, and DDR5, with each DIMM form factor specific to its DDR version. With DDR5, some motherboards offer additional features like dual-channel or quad-channel memory configurations, significantly boosting performance by allowing simultaneous access to multiple DIMMs.

The memory controller's capabilities and the number of physical slots determine the maximum amount of memory that can be installed.

Motherboard Storage Connectors

One or more fixed disks inside the PC case provide persistent storage for the operating system, software, and data files. These disks use either solid-state drive (SSD) or hard disk drive (HDD) technology.

Serial Advanced Technology Attachment Interface

The motherboard contains several Serial Advanced Technology Attachment (SATA) ports to connect fixed drives. SATA can also connect removable drives, such as tape drives and optical drives (DVD/Blu-ray). SATA devices are installed in a drive bay in the chassis and connected to a data port via a cable and to the power supply via a SATA power or Molex connector.

M.2 Interface

An SSD can be provisioned in an adapter card form factor, often using an M.2 interface. The M.2 port is oriented horizontally. The adapter card is inserted at an angle, pushed into place, and secured with a screw. M.2 adapters come in different lengths (42 mm, 60 mm, 80 mm, or 110 mm), so check your motherboard for compatibility. Labels indicate the supported adapter sizes. M.2 supplies power over the bus, eliminating the need for a separate power cable.

M.2 form factor SSD being inserted into a motherboard connector

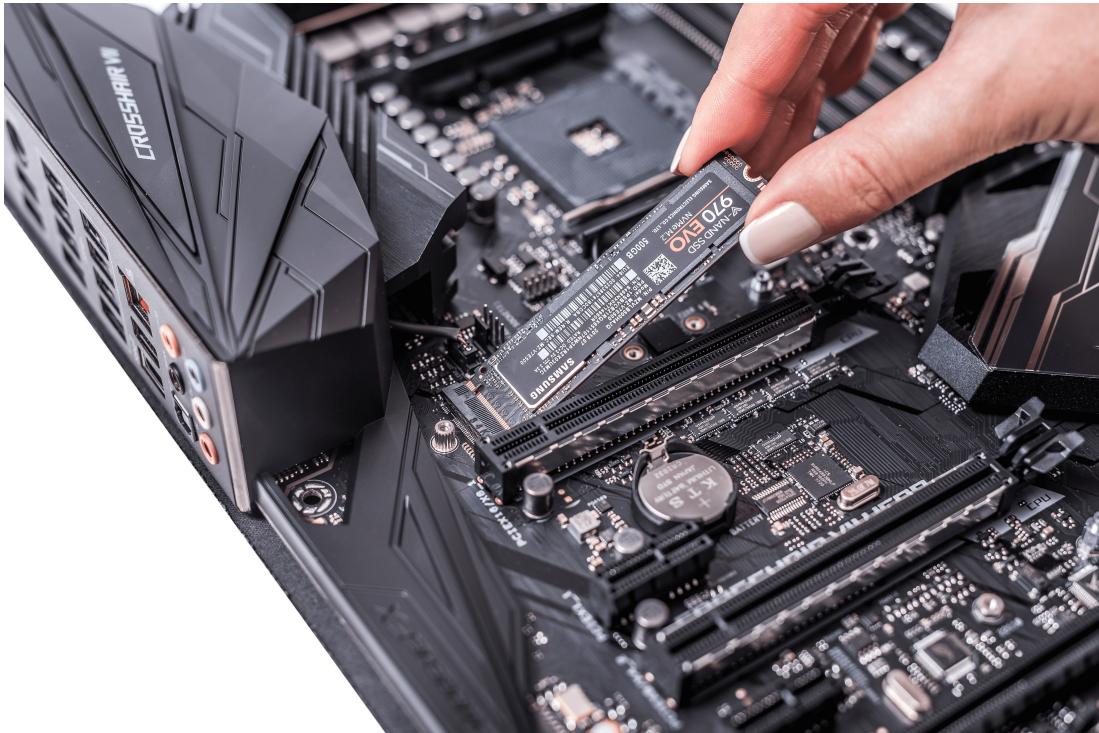


Image ©123RF.com

External SATA Interface

External SATA (eSATA) cables are designed for external connections, featuring better shielding than internal SATA cables to support longer lengths (up to 2 meters) and withstand external environments. Power over eSATA, or eSATAp, also known as "eSATA/USB Combo," combines eSATA and USB functionality in a single port, providing power to external devices, unlike standard eSATA. eSATA and eSATAp are less common today, as USB 3.x, Thunderbolt, and other high-speed connections offer higher speeds, greater versatility, and broader adoption.

Note: The main drawback of eSATA compared to USB or Thunderbolt is the lack of power supply over the cable. While this isn't an issue for 3.5-inch drives that require a separate power source, it limits the usefulness of eSATA for 2.5-inch portable drives.

Peripheral Component Interconnect Express Interface

Expansion slots accept plug-in adapter cards to extend the computer's functionality. There are two main types of expansion slot interfaces.

The [PCI Express](#) bus is the standard interface for modern adapter cards, using point-to-point serial communication to provide each component with a dedicated link to other components.

Motherboard PCI and PCI Express expansion slots

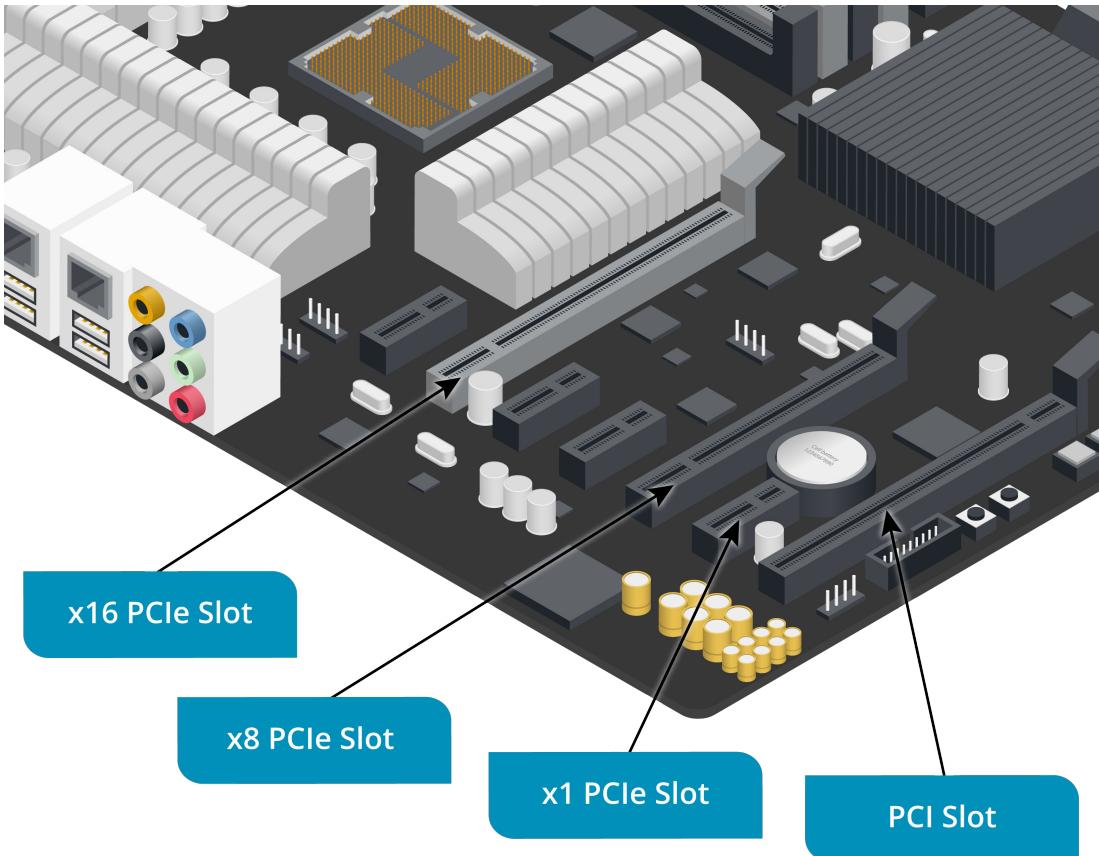
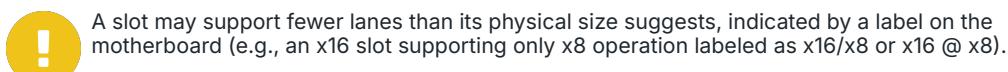


Image ©123RF.com

Each point-to-point connection is called a link, which can use one or more lanes. The raw transfer rate of each lane depends on the PCIe version and is measured in giga transfers per second (GT/s). Throughput in GB/s is the effective rate after accounting for encoding losses.

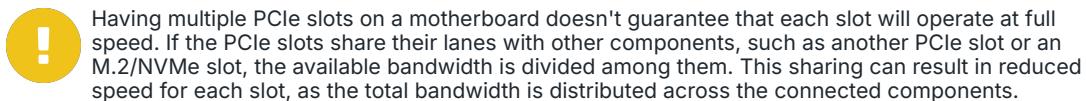
Version	GT/s	GB/s for x1	GB/s for x16
2	5	0.5	8
3	8	0.985	15.754
4	16	1.969	31.508
5	32	3.938	63.015
6	64	7.56	128

Adapter slots with more lanes are physically longer. Each PCIe adapter card supports a specific number of lanes, typically x1, x4, x8, or x16. Ideally, the card should be plugged into a port with the same number of lanes. However, if slots are limited, a card can fit into any port with an equal or greater number of lanes, known as up-plugging (e.g., an x8 card in an x8 or x16 slot). The card should work at x8 but may sometimes operate at x1. Down-plugging, fitting a longer card into a shorter slot, is possible if the card is not obstructed.



All PCIe versions are backward-compatible, meaning you can connect a PCIe version 2 adapter to a version 4 motherboard or a version 3 adapter to a version 2 motherboard, with the bus link operating at the speed of the lowest version component.

PCIe can supply up to 75W to a graphics card via a dedicated graphics adapter slot and up to 25W through other slots. An additional 75W can be supplied via a PCIe power connector.



Peripheral Component Interconnect Interface

Computers can support multiple expansion buses to accommodate older technologies. Peripheral Component Interconnect (PCI) is a legacy bus type that has been superseded by PCI Express (PCIe). PCIe is software-compatible with PCI, allowing PCI ports on a PCIe motherboard to support legacy adapter cards, but PCI cards cannot be fitted into PCIe slots.

PCI uses parallel communication and is typically 32-bit, operating at 33.3 MHz with a transfer rate of up to 133 MBps. Early PCI cards were designed for 5V signaling, but 3.3V and dual-voltage cards became more common. To prevent incompatible cards from being inserted into motherboard slots, different keying is used for 5V, 3.3V, and dual-voltage cards.

32-bit PCI sound card with dual voltage

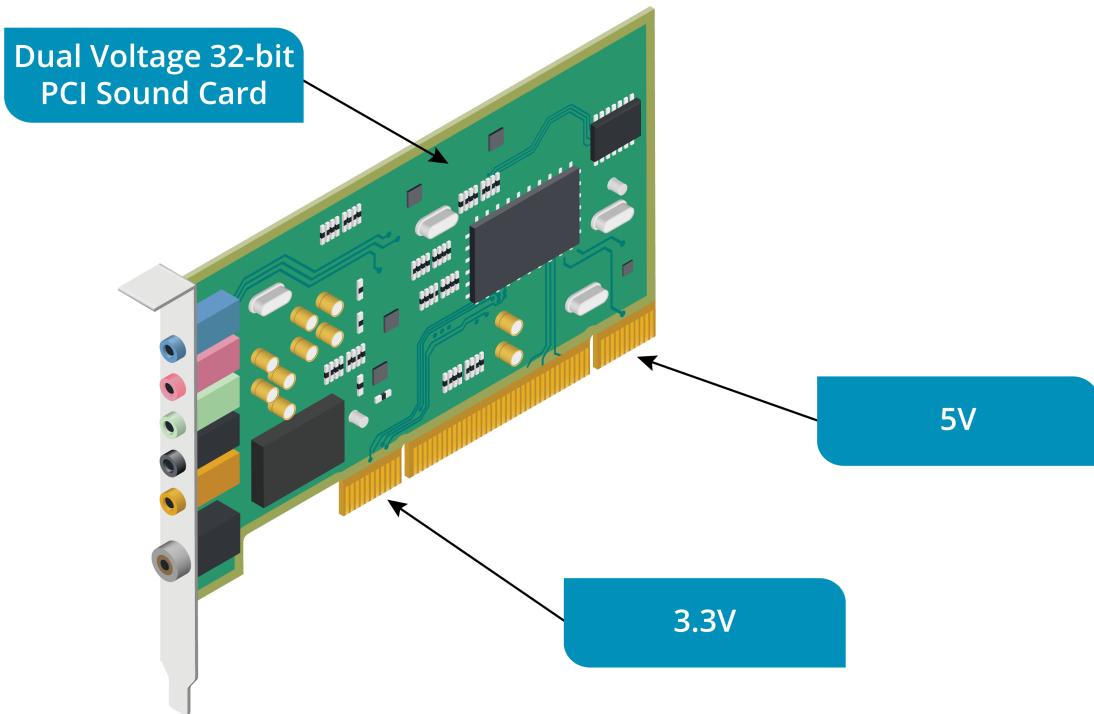


Image ©123RF.com

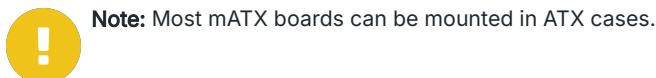
Motherboard Form Factors

The **motherboard form factor** defines its shape, layout, compatible case, power supply, and the number of adapter cards that can be installed.

Advanced Technology eXtended Form Factor

The [advanced technology extended](#) (ATX) specification is the standard form factor for most desktop PC motherboards and cases. Full-size ATX boards measure 12 x 9.6 inches (305 x 244 mm) and can have up to seven expansion slots.

The Micro-ATX (mATX) standard specifies a 9.6 x 9.6 inch (244 x 244 mm) square board, with a maximum of four expansion slots.

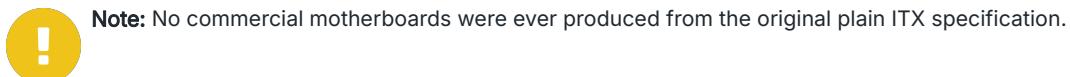


Note: Most mATX boards can be mounted in ATX cases.

Information Technology eXtended Form Factor

Small form factor (SFF) PCs are popular for home use and mini servers, often using Via's Mini-ITX ([information technology extended](#)) form factor.

Mini-ITX boards measure 6.7 x 6.7 inches (170 x 170 mm) and have one expansion slot. They are designed for small cases but can also be mounted in ATX cases. Smaller nano-, pico-, and mobile-ITX form factors are used for embedded systems and portables, not PCs.



Note: No commercial motherboards were ever produced from the original plain ITX specification.

Motherboard Installation

Installing a motherboard involves securing it inside the case and connecting various components. Follow these steps for a successful installation:

1. Review the Documentation:

- Familiarize yourself with the motherboard's installation procedure using the provided documentation.
- Check if any jumper settings need adjustment. Note that modern motherboards often handle configurations through the BIOS/UEFI rather than physical jumpers.



Protect the motherboard from electrostatic discharge (ESD) by using an anti-static wrist strap or grounding yourself before handling components.

2. Install the I/O Shield:

- If your motherboard doesn't come with a pre-installed I/O shield, align the shield with the rear I/O ports and snap it into place in the case.

3. Insert Standoffs:

- Place standoffs in the case to match the mounting holes on the motherboard. Ensure that standoffs are only positioned where the motherboard has corresponding holes to avoid short circuits.

4. Pre-install the CPU and Memory (Optional but recommended):

- Install the CPU, memory, and CPU cooler on the motherboard before securing the board in the case. This provides easier access and reduces the risk of damage.

5. Align and Secure the Motherboard:

- Carefully place the motherboard onto the standoffs, aligning it with the I/O shield and ensuring all standoffs line up with the holes.
- Secure the motherboard with the appropriate screws, ensuring it is firm and stable without overtightening.

Align the board with the I/O cut out (top left) and ensure that it is supported by standoffs at the edges and in the center

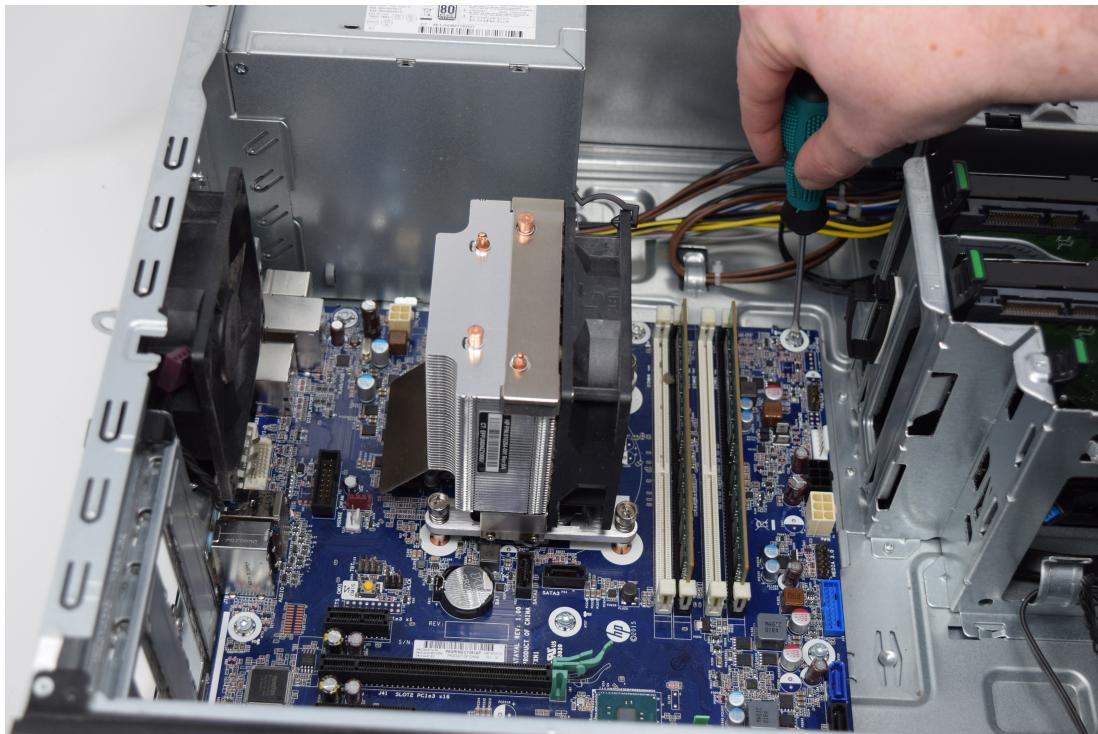


Image courtesy of CompTIA.

6. Final Assembly:

- Connect power supplies, disk drives, and any additional adapter cards to the motherboard.
- Attach all necessary data and power connectors.

7. Cable Management:

- Plan and route cables neatly to maintain airflow and prevent clutter inside the case.



Selection and installation of power, disk, system memory, and CPU devices are covered in detail in the next lesson.

Motherboard Headers and Power Connectors

In addition to slots and sockets for system devices, motherboards also include connectors for components such as case buttons, speakers, and fans.

Motherboard front panel, USB, and audio headers

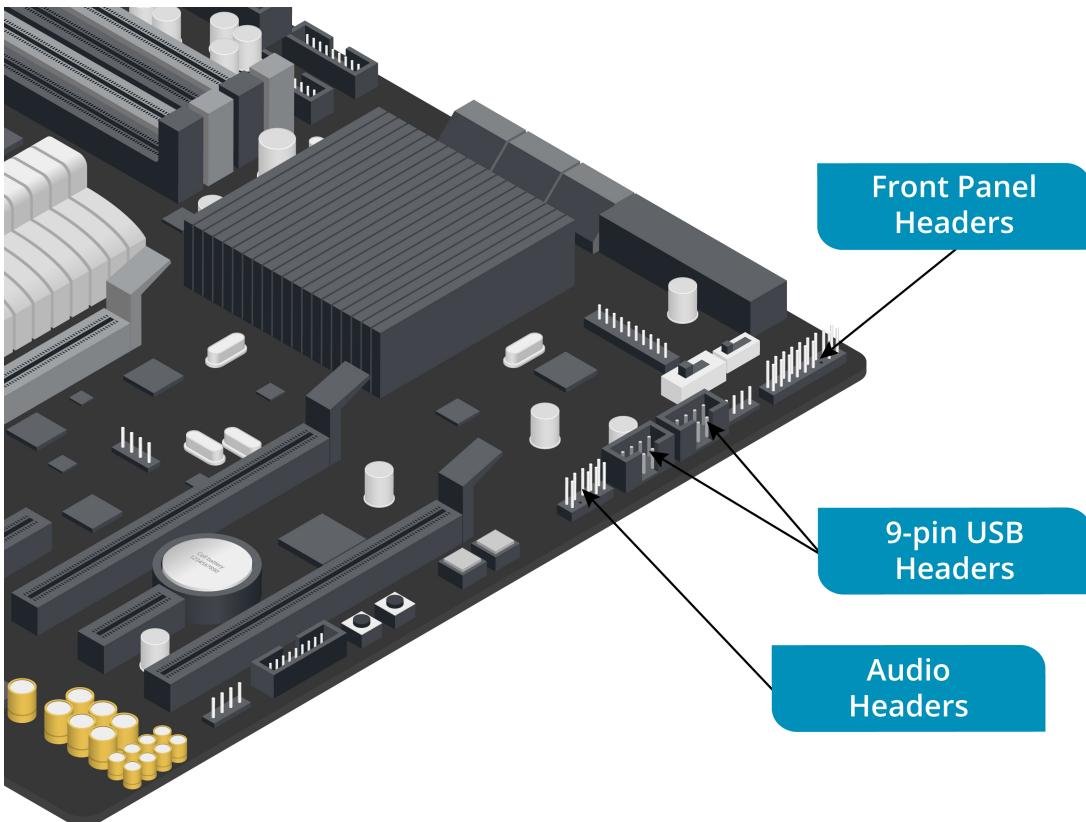


Image ©123RF.com

Headers

Components on the front and rear panels of the case connect to [header \(motherboard\)](#) on the motherboard:

- **Power button (soft power)**—Sends a signal that can be interpreted by the OS as a command to shut down rather than switching the PC off. Holding down the power button for a few seconds will cut the power, bypassing the OS.
- **Drive (HDD) activity lights**—Show when an internal hard disk is being accessed. The corresponding connector is usually labeled "HDD LED" or similar on the motherboard.
- **Audio ports**—Allow speakers and/or headphones and a microphone to be connected. The front panel audio ports typically connect to the motherboard via an HD Audio header, often labeled "HD Audio" (or "AC'97" for older systems).
- **USB ports**—Internal USB 2 connections are made via 9-pin headers. These headers can support up to two 4-pin USB ports, with the 9th pin used for correct cable orientation. USB 3 headers use a 20-pin (2×10) format and can connect to two USB 3.x ports, supporting faster data transfer rates compared to USB 2.0.

When disassembling the system, create a diagram or take photos to document the position and orientation of all header connectors. If no diagram is available, refer to the motherboard

documentation or the labels printed on the wires and headers. These labels can sometimes be small or difficult to interpret, making careful documentation important.

Power Connectors

The motherboard also contains various connection points for the power supply and fans.

- **Main Power Connector:**

- The primary P1 motherboard power connector is a distinctive 24-pin block (2 rows of 12 pins) with square pin receptacles.

- **Fan Connectors:**

- 3-pin Molex KK format connectors: Typically used for fans, these connectors control fan speed by varying the voltage.
- 4-pin fan Molex KK format connectors: These support precise fan-speed control via pulse width modulation (PWM), with the PWM signal carried by the blue wire. There will be one for the CPU and one or more for case fans and components such as memory and video adapters.

 **3-Pin Fans on 4-Pin Headers:** Fans with a 3-pin connector can usually be used with 4-pin headers, but the system may not be able to vary the fan speed without special configuration. **4-Pin Fans on 3-Pin Headers:** Fans with a 4-pin connector will generally work with a 3-pin header but will not be able to use PWM for speed control.

Video Cards

An **expansion card** enhances a motherboard by adding functions or ports not originally supported. It fits into a PCIe or PCI slot. Common types include sound, video, capture, and network cards.

The **video card** (or graphics adapter) generates the signal for a monitor or projector. Low-end graphics adapters, known as integrated or onboard graphics, are often built into the motherboard chipset or CPU. For tasks like 3D gaming, CAD, or digital artwork, a more powerful discrete graphics card is usually required and installed via a PCIe slot on the motherboard. Most graphics adapters use chipsets from AMD, NVIDIA, and Intel. Typical features of a video card include:

- **Graphics Processing Unit (GPU)**—A microprocessor optimized for rendering 2-D and 3-D images and effects on-screen. Key performance indicators include frame rate and support for advanced texture and lighting effects.
- **Graphics memory**—3-D graphics cards require substantial memory for processing and storing textures. High-end cards may have up to 24 GB of GDDR memory, while mid-range cards typically have 8–12 GB. Low-end cards may use shared memory from the system's RAM.
- **Video ports**—Modern graphics cards typically feature HDMI, DisplayPort, and sometimes USB-C with DisplayPort or Thunderbolt capabilities, determining the types and number of monitors or projectors that can be connected.



Graphics Double Data Rate (GDDR): GDDR memory is optimized for the high bandwidth needs of GPUs, similar to DDR memory used in system RAM.

Most modern graphics cards use a PCIe x16 slot, providing the necessary bandwidth for high-performance graphics. Some setups use multiple graphics cards in multiple PCIe slots, configured to work together.

A video/graphics card with DisplayPort, HDMI, and DVI-I ports

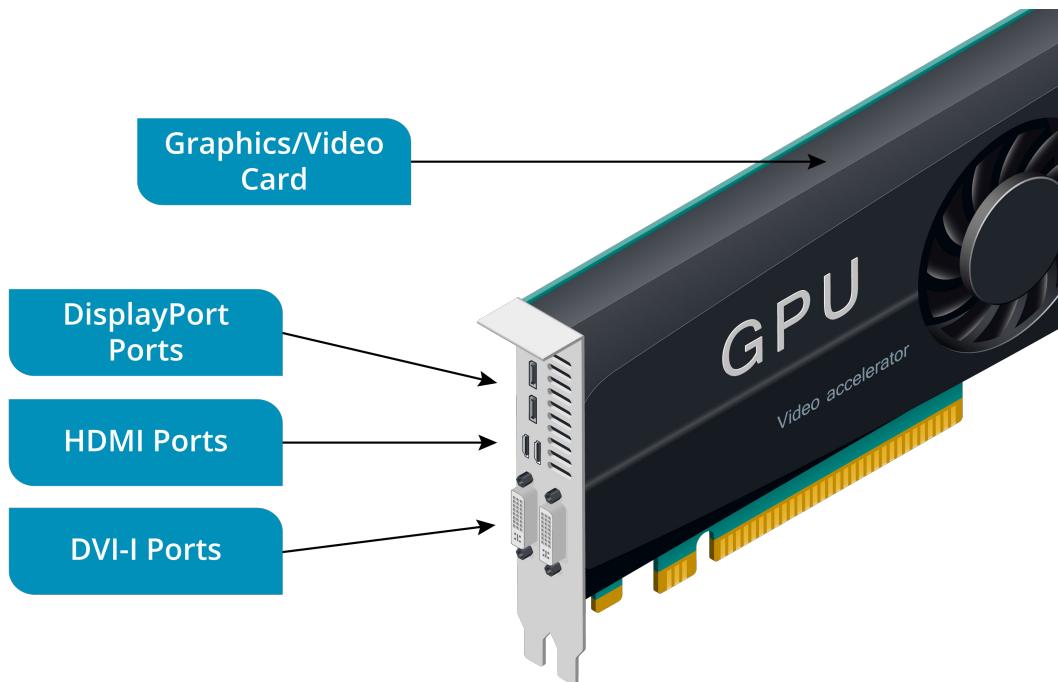


Image ©123RF.com

Capture Cards

Where a graphics card generates an output video signal to drive a monitor, a capture card records video input and saves it as a file or streams it live. Commonly used for recording or streaming gameplay, capture cards can also capture video from other sources.

Types of Capture Cards

- Game Capture Cards:
 - Designed to record or stream gameplay footage.
 - Can capture video from PCs or game consoles via HDMI.
- HDMI Capture Cards:
 - Record video from various HDMI sources, such as game consoles, camcorders, and security cameras.
 - Used for live streaming, video production, and content creation.
- TV Tuner Cards:
 - Receive and record video from broadcast TV sources.
 - Allow users to watch and record live TV on their computer.

Installation and Connectivity

- Internal Capture Cards:

- Installed inside the computer using a PCIe slot.
 - Offer lower latency and higher performance, suitable for professional use.
- External Capture Cards:
 - Connect to the computer via USB or Thunderbolt.
 - Portable and easy to install, ideal for casual users or those needing to use the card with multiple devices.

Sound Cards

Speakers or headphones connect to a [sound card](#) or the motherboard's integrated audio via a 3.5 mm (½ inch) audio jack, also known as a phone plug or mini TRS connector. These jacks support standard audio output and input for headphones, speakers, or microphones.

Audio jacks on a sound card

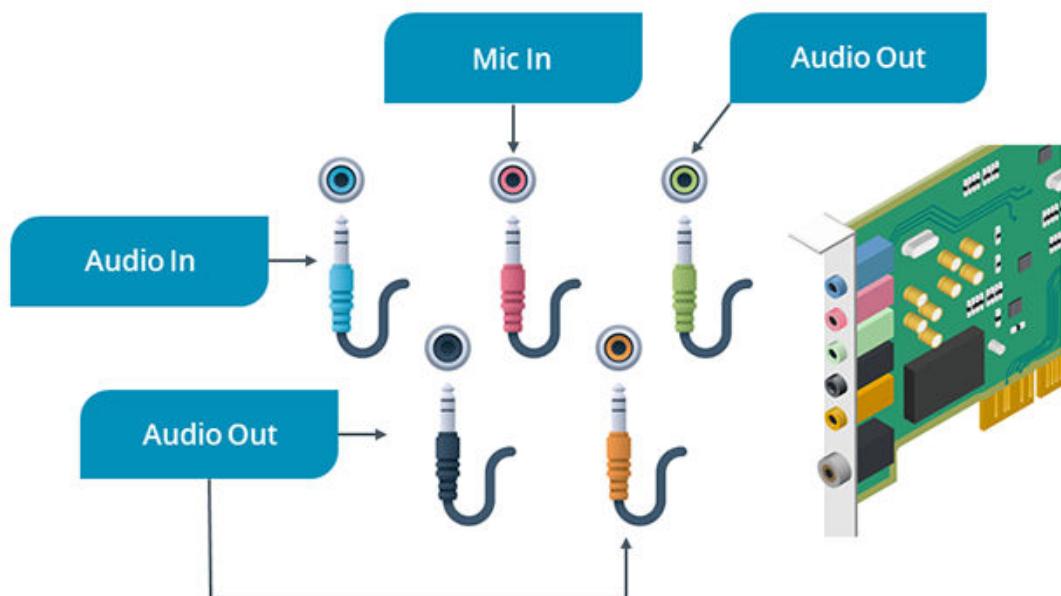


Image ©123RF.com

A basic sound chip may be provided as part of the motherboard chipset, but better-quality audio functions can be provided as a PCIe or PCI expansion card. Pro-level cards may also feature onboard memory, flash memory storing sound samples (wavetables), and additional jack types for different input sources.

Sound cards are used for both audio playback and recording input from a microphone, offering better sound quality and additional features compared to onboard audio.

Sound cards that support multiple output channels can deliver audio ranging from mono or stereo to advanced surround sound, creating an immersive cinematic experience with multiple speakers positioned around the listener.

Network Interface Cards

Most computers have an Ethernet network adapter integrated into the motherboard chipset. However, you may need to install an add-on [network interface card](#) to upgrade to a different type of network or cabling, such as copper versus fiber optic. A dedicated NIC can also provide multiple ports, which can be bonded into a single higher bandwidth link.

RJ45 ports on a Network Interface Card (NIC)

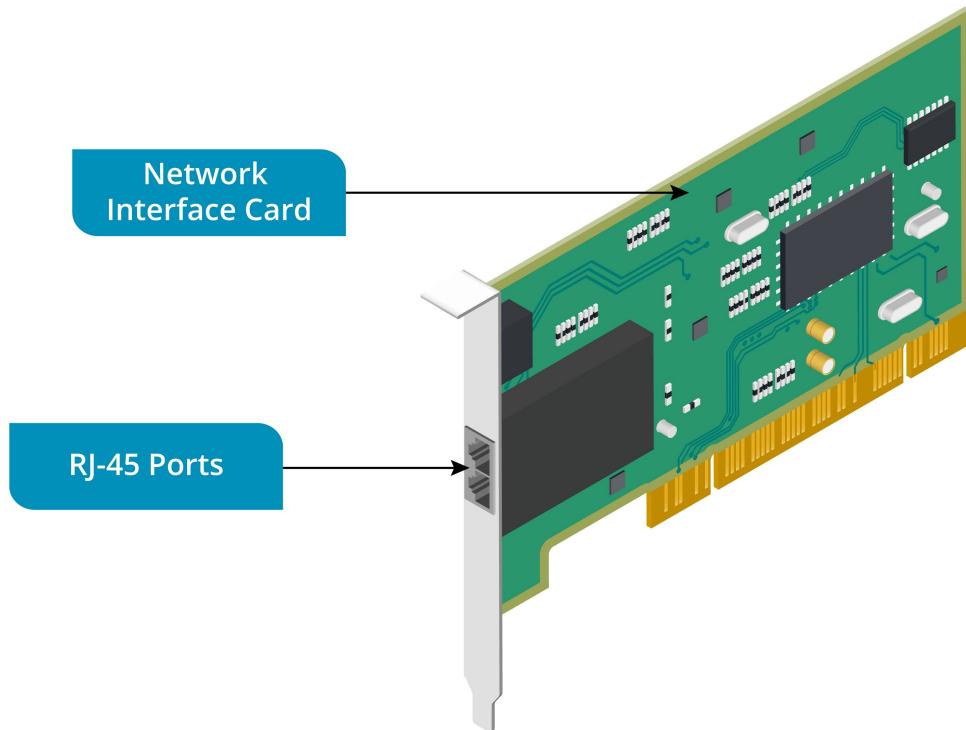


Image ©123RF.com

A Wi-Fi adapter can be added to connect to a wireless network, supporting various 802.11 standards. Some cards can also connect to cellular data networks.

Lesson 2C

Legacy Cables

Lesson Overview

As an IT professional, you are tasked with upgrading and integrating a mix of old and new technology in an office. The office has legacy devices that need to be connected to modern systems, and some older systems require upgrades to improve performance and compatibility.



Objectives Covered

3.2 Summarize basic cable types and their connectors, features, and purposes.

Learning Outcomes

As you study this lesson, answer the following questions:

- What type of adapter is needed to connect new computers to DVI monitors, and how do you ensure all connections are secure?
- How do you install a SCSI Host Bus Adapter (HBA) into an available PCIe slot on a new workstation?
- What is the process for accessing and transferring data from the IDE hard drives to the new systems?
- How do you connect an RS-232 serial cable to the console port on network equipment?
- What is the process for using USB hubs to expand the number of available USB ports on each workstation, allowing multiple devices to connect simultaneously?

DVI and VGA Video Cables

HDMI and DisplayPort interfaces are designed for digital flat-panel displays but can be adapted for analog devices. Older interfaces like VGA were used for cathode ray tube (CRT) monitors and projectors, which relied on analog signals.

DVI and VGA support only video, but not audio.



Digital Visual Interface

Digital video interface (DVI) supports both analog and digital outputs. Although popular after its 1999 introduction, DVI is no longer actively developed and is typically found on older display devices and video cards.

There are five types of DVI, each supporting different configurations for single and dual link (extra bandwidth) and analog/digital signaling. The connector's pin configuration indicates the type of DVI supported by a port.

DVI port and connector types

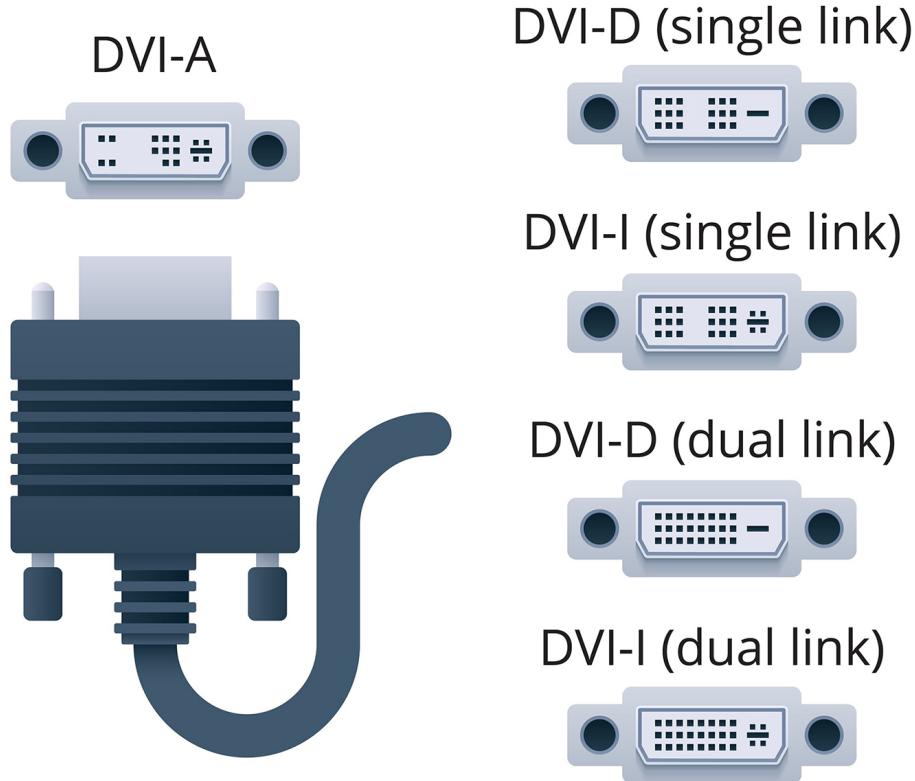


Image ©123RF.com

DVI-I supports both analog and digital outputs. DVI-A supports only analog output, while DVI-D supports only digital output.

Video Graphics Array Interface

The 15-pin [video graphics array](#) (VGA) port was the standard analog video interface for PCs for many years. Until recently, most video cards and monitors included a VGA port, though it is now being phased out. VGA typically supports resolutions up to Full HD (1920×1080), depending on cable quality. The connector is a D-shell type with screws for secure attachment.

A VGA connector and port

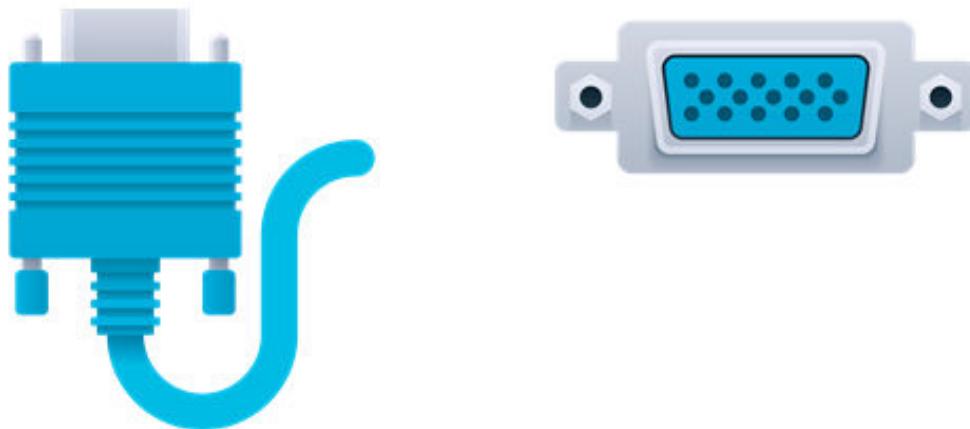
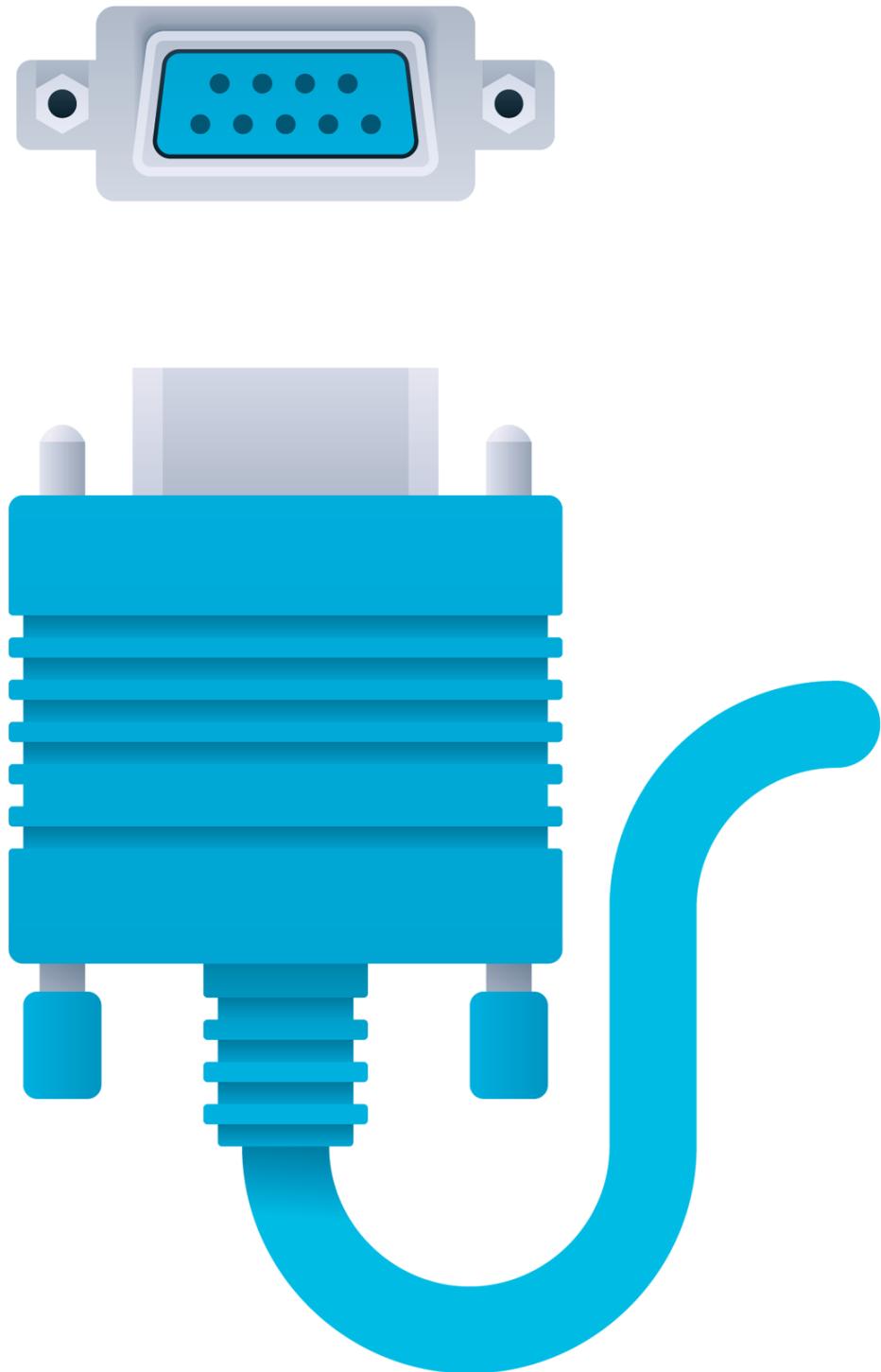


Image ©123RF.com

Serial Cables

The **serial** port is a legacy connection interface that transmits data one bit at a time over a single wire. Start, stop, and parity bits format and verify data transmission. This interface is also known as Recommended Standard #232 (RS-232). While modern interfaces like USB are also serial, RS-232 uses less sophisticated signaling, supporting data rates up to about 115 Kbps.

9-pin serial connector and port



Serial ports were commonly used to connect external modems for dial-up Internet, though USB has largely replaced this function. You may also find serial ports on network equipment for device management.

RS-232 specifies a 25-pin interface, but PC manufacturers typically use the cheaper 9-pin D-subminiature ([D-subminiature shell connector](#)) female port, commonly referred to as DB9, as shown above.

In Windows, the serial port is referred to as a Communications (COM) port.



You might also encounter PS/2 ports, used for connecting mice and keyboards. PS/2 ports use a 6-pin mini-DIN format, with green for mice and purple for keyboards.

Adapter Cables

Given the numerous cable and connector types available, a basic peripheral cable often won't directly connect a PC port to a peripheral device port. An adapter cable can solve this issue. An [adapter cable](#) has connectors for two different cable types at each end and comes in two types: **active adapters**, which use circuitry to convert signals (e.g., digital to analog), and **passive adapters**, which simply convert between connector types without changing the signal. Active adapters are necessary for converting signals that require different protocols, like digital HDMI to analog VGA. Passive adapters work when both connectors use the same signaling standard, such as different USB connector types.

Common types of adapter cables include:

- **Video adapters:** Convert between signaling types, such as **HDMI to VGA**, **HDMI to DisplayPort**, or **HDMI to DVI**.
- **USB adapters:** Convert between USB connector types, such as **USB-C to USB-A**.
- **USB hubs:** Provide additional USB ports, allowing multiple devices to connect to a single USB port.
- **USB adapters to various outputs:** Include adapters like **USB-C to HDMI** or **USB-C to Lightning**.

Module 3

Installing System Devices

Module Overview

The market for computer parts is complicated. There are many types of processors, memory modules, disk drives, and power supplies, each with different features. As a CompTIA A+ technician, you need to understand these features and know how they work together to build a computer that fits specific needs. You also need to solve compatibility problems and be confident in installing and removing these often expensive and delicate parts.

Module Summary

Prepare for A+ Core 1 by:

- Installing and configuring power supplies and cooling.
- Selecting and installing storage devices.
- Installing and configuring system memory.
- Installing and configuring CPUs.

Lesson 3A

Power Supplies and Cooling

Lesson Overview

You are tasked with setting up desktop and laptop computers in a repurposed office where heat and humidity are high-risk factors. The office will host client devices that require reliable cooling and humidity control to prevent overheating and moisture damage. You need to ensure that the cooling systems and dehumidifiers are adequate to support these devices and maintain a stable environment. Additionally, you must select components that can withstand higher temperatures and humidity levels to ensure continuous operation and system stability for everyday office tasks.



Objectives Covered

- 3.5 Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
- 3.6 Given a scenario, install or replace the appropriate power supply.

Learning Outcomes

As you study this lesson, answer the following questions:

- What are the key components of a power supply unit, and why is it important to ensure the PSU is compatible with the system case and motherboard?
- How do you calculate the total power requirements of a PC, and why is PSU efficiency important?
- What is a modular power supply, and how does it improve airflow and cooling within the chassis?
- What is the purpose of a heat sink and thermal paste, and how do they work together to cool the CPU?
- What are the components of an open-loop liquid cooling system, and what maintenance is required to keep it functioning properly?

Power Supply Units

The power supply unit (PSU) delivers low-voltage direct current (DC) power to PC components. It contains a rectifier to convert alternating current (AC) from the building to DC voltage, transformers to step down to lower voltages, and regulators to ensure consistent output with filters and regulators. The PSU also includes a fan to dissipate heat.

The PSU's size and shape determine its compatibility with the system case and motherboard, particularly regarding screw and fan locations and power connectors. Most desktop PC PSUs are based on the ATX form factor.

Ensure the PSU is compatible with the outlet's voltage before plugging it in. North American outlets typically provide 120 VAC (low-line), while UK outlets provide 230 VAC (high-line). Data centers often use high-line voltage for efficiency. Most PSUs are dual voltage and auto-switching, though some have a manual switch or are fixed to either low-line or high-line. Input operating voltages are marked on the PSU and its documentation.



AC voltage supply varies by country and distribution circuits, so PSUs have a wide tolerance range: **100-127 VAC** for low-line and **220-240 VAC** for high-line.

Autoswitching PSU



Image © 123RF.com

Wattage Rating

Power is the rate at which energy is generated or used, measured in watts (W), calculated as voltage multiplied by current ($V \cdot I$). A PSU must meet the combined power requirements of a PC's components, with its output capability measured in watts, known as its wattage rating. Standard desktop PSUs are typically rated at 400–500 W, while enterprise workstations and servers often have PSUs rated well over 300 W, sometimes exceeding 1000 W, especially in systems with multiple CPUs and GPUs. Gaming PCs may require 600 W or more due to high-spec CPUs and graphics cards.

It is crucial to correctly match the PSU wattage to the system's power requirements to prevent system instability or damage. An underpowered PSU can lead to several issues:

- **System Instability:** Insufficient power can cause random shutdowns, reboots, or crashes, as the PSU struggles to supply adequate power to all components.
- **Component Damage:** Consistently running a PSU at or beyond its capacity can lead to overheating, potentially damaging the PSU itself or other components.



Component power requirements vary widely. For example, CPUs can range from 17 W to over 100 W. Online calculators, such as coolermaster.com/power-supply-calculator, can help determine power needs.

When specifying a PSU for a system with high power requirements, assess the power distribution across [output voltage](#). Distribution refers to the power supplied over each rail, which is a wire providing current at a specific voltage. For modern computers, the +12 VDC rail is the most important due to its heavy usage.

Example Power Distribution:

Output Rail (VDC)	Maximum Load (A)	Maximum Output (W)
+3.3	20	130
+5	20	130
+12	33	396
-12	0.8	9.6
+5 (standby)	2.5	12.5



The +3.3 V and +5 V outputs have a combined limit. For modern computers, the +12 VDC rail is the most important, as it is the most heavily used.

Energy Efficiency

PSU efficiency is a critical factor in system performance and energy consumption. For example, a 300 W PSU operating at 75% efficiency draws 400 W from the outlet, with the excess 100 W lost as heat. This inefficiency not only increases energy costs but also contributes to additional heat generation, which can impact the cooling needs of the system.

To address these concerns, PSUs are often rated according to the 80 PLUS certification program, which signifies their efficiency levels. Some common efficiency ratings include:

- **80 PLUS Bronze:** At least 82% efficiency at 20% load, 85% at 50% load, and 82% at 100% load.
- **80 PLUS Silver:** At least 85% efficiency at 20% load, 88% at 50% load, and 85% at 100% load.
- **80 PLUS Gold:** At least 87% efficiency at 20% load, 90% at 50% load, and 87% at 100% load.

These ratings indicate how efficiently a PSU converts AC power from the outlet into DC power for the computer's components. More efficient PSUs, such as those with Gold or higher ratings, reduce the amount of wasted energy, thereby generating less heat. This reduction in heat generation can decrease the cooling requirements of the system, leading to quieter operation and potentially extending the lifespan of components by maintaining lower operating temperatures.

ENERGY STAR 80 PLUS compliant PSUs must be at least 80% efficient at 20–100% load, ensuring a baseline of energy efficiency and reliability for consumers. By choosing a PSU with

a higher efficiency rating, users can benefit from lower energy costs, reduced heat output, and improved overall system performance.

Power Supply Connectors

Each PSU has multiple power connectors that supply DC voltage to the motherboard and devices at 3.3 VDC, 5 VDC, and 12 VDC. Voltage regulators adjust the supplied voltage to match the component's requirements. The motherboard's power port is called the P1 connector or the 24-pin ATX power connector. A PSU also includes Molex and SATA power connectors, as well as 4/6/8/16-pin connectors for CPU and PCIe adapter card power ports.

20-pin to 24-pin Motherboard Adapter

The ATX PSU standard has undergone several revisions, specifying different connector form factors. In the original ATX specification, the P1 connector is 20-pin (2×10), with black wires for ground, yellow for +12 V, red for +5 V, and orange for +3.3 V.

Most systems use the 24-pin (2×12) P1 connector. Some PSUs include a **20+4-pin P1 adapter cable** for compatibility with older 20-pin motherboards.

A 24-pin main motherboard power cable and port

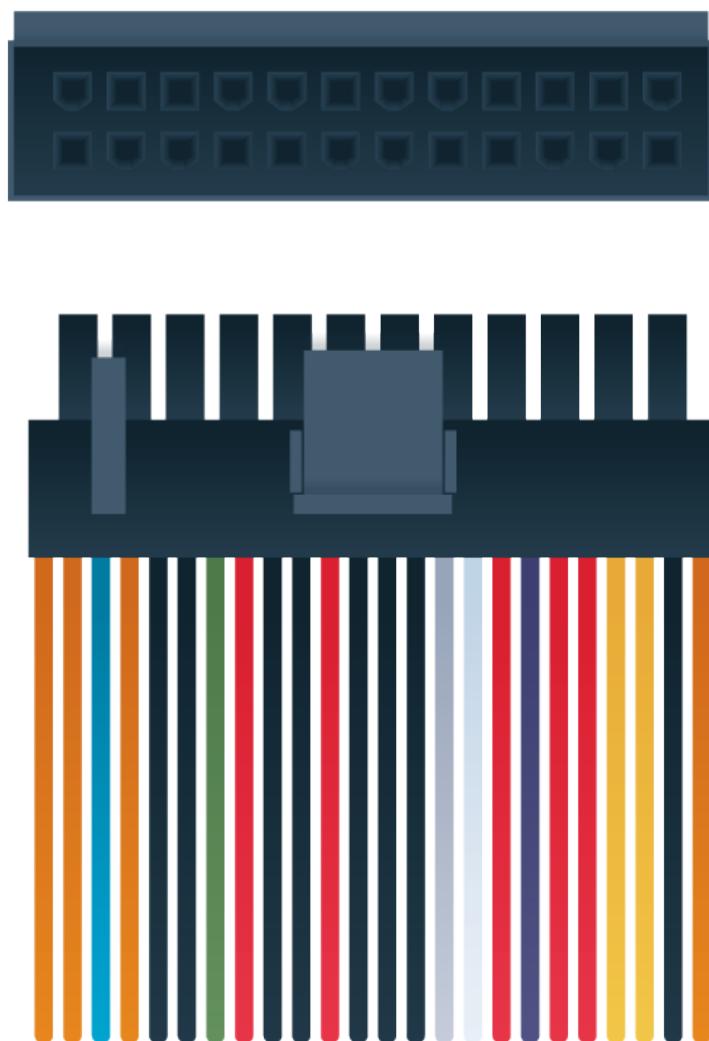


Image ©123RF.com

Modular Power Supplies

A [modular power supply](#) has detachable power connector cables, allowing you to use only the necessary ones. This reduces clutter within the chassis, improving airflow and cooling. For example, a non-modular PSU might have four or five Molex or SATA connectors, but the PC might only need two. With a modular PSU, you can remove the unnecessary cables.

Modular power supply with plugable cables



Image © 123RF.com

Redundant Power Supplies

Redundant power supplies are crucial in maintaining system uptime and preventing data loss, especially in enterprise environments where continuous operation is vital. A computer system may be equipped with two PSUs, with one serving as a failover redundant power supply. This setup ensures that if one PSU fails, the other can immediately take over, minimizing downtime and protecting against data loss.

This configuration is particularly critical in scenarios such as data centers or high-availability systems, where uninterrupted service is essential. In these environments, redundant power supplies help maintain system reliability and performance, even during power failures or PSU malfunctions.

In server setups, each PSU typically connects to a backplane, a circuit board that provides the electrical connections between different components. The backplane allows for hot-swappable PSUs, meaning faulty units can be replaced without opening the case or interrupting power to the system. This feature is invaluable in maintaining uptime and ensuring that critical services remain available.

Redundant power supplies are less common in desktop computers because desktops are generally not required to maintain the same level of uptime as servers. In server environments, however, the need for continuous operation and data integrity makes redundant PSUs a standard feature.

Fan Cooling Systems

Computer components emit heat due to resistance as the electrical current passes through. Without cooling, this heat raises the temperature of each component and the overall case, potentially causing malfunctions or damage. This is especially critical for CPUs. Despite efforts by Intel and AMD to improve thermal efficiency, all CPUs need **cooling** to maintain safe operating temperatures.

 Other components, like memory modules and graphics adapters, also require cooling solutions.

Heat Sinks and Thermal Paste

A heat sink is a copper or aluminum block with fins that increase surface area for better cooling of the component through convection. It is attached to the CPU chip using thermal paste/pad to eliminate air gaps and ensure efficient heat transfer. Thermal pads, which soften when heated, are easier to apply but may be less reliable than thermal paste.

CPU heat sink and fan assembly

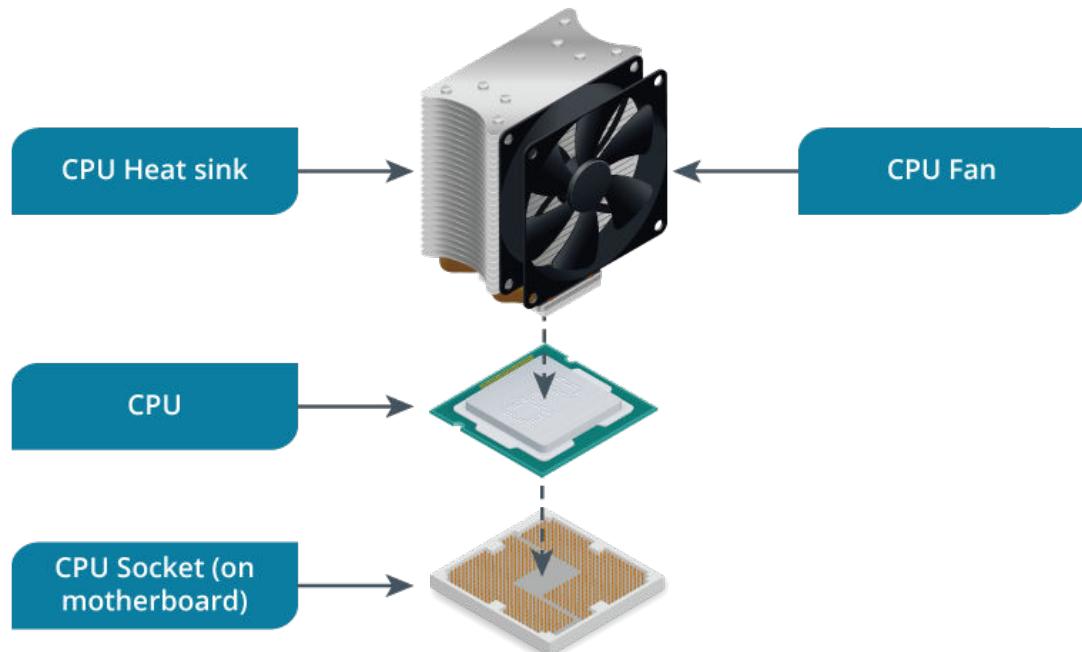


Image © 123RF.com

CPU heat sinks can be clamped to the motherboard using various mechanisms, such as retaining clips or push pins. Push pins can be released and reset with a half-turn of a screwdriver.

Fans

A heat sink is a passive cooling device that doesn't require electricity. For optimal performance, it needs good airflow, so minimize cable clutter and cover spare adapter slots with blanking plates.

Many PCs generate more heat than passive cooling can handle. Fans improve airflow and help dissipate heat. They are used in power supplies and chassis exhaust points, drawing cool air from front vents and expelling warm air from the back. Most heat sinks have fans to enhance cooling, which must be connected to a motherboard fan power port.

Thermometer sensors at each fan location set appropriate speeds and detect fan failures. Some chassis designs use plastic shrouds or baffles to channel airflow over the CPU, attached with plastic clips.

Both fans and heat sinks become less effective if dust accumulates. Clean these components and air vents periodically with a soft brush, compressed air, or a PC-approved vacuum cleaner.

Liquid Cooling Systems

High-end gaming PCs, high performance workstations, and those used in high ambient temperatures may require advanced cooling solutions.

A liquid-cooled PC

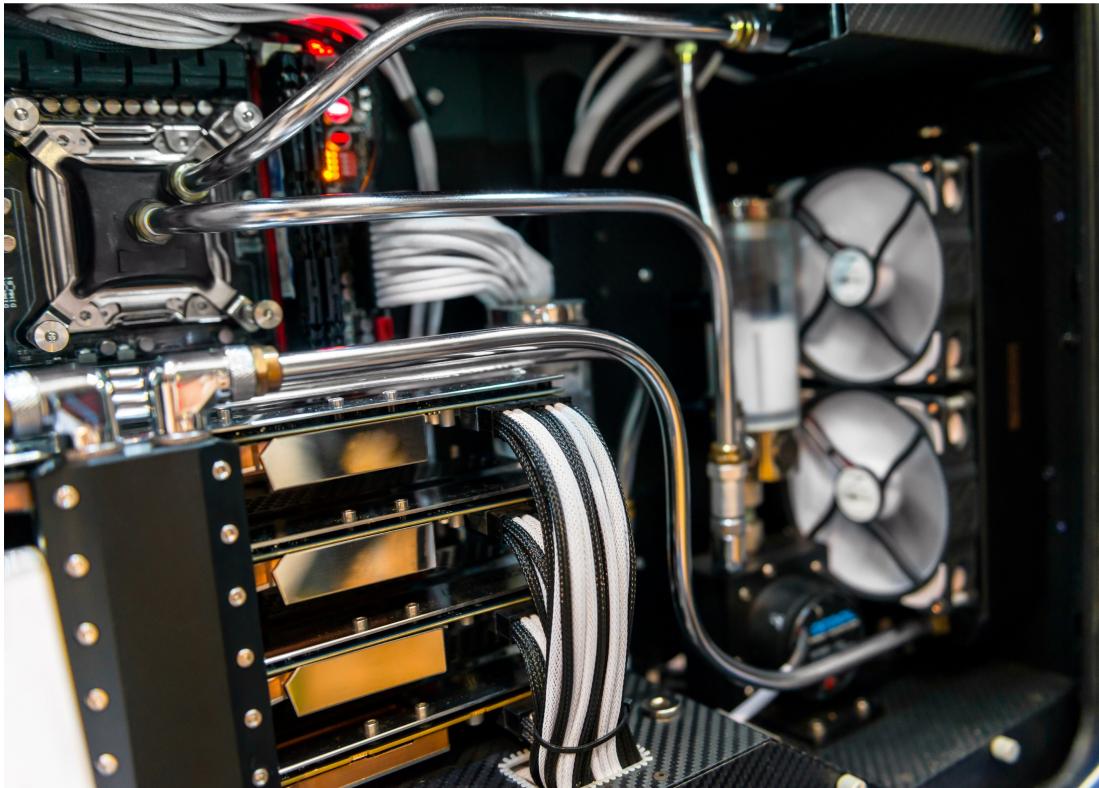


Image © 123RF.com

A [liquid cooling](#) system pumps water around the chassis, offering more effective cooling than air convection and often operating more quietly than multiple fans.

An open-loop liquid cooling system includes:

- **Water loop/tubing and pump:** Pushes coolant added via the reservoir around the system.
- **Water blocks and brackets:** Attached to each device to remove heat by convection, similar to heat sink/fan assemblies, and connected to the water loop.
- **Radiators and fans:** Positioned at air vents to dispel excess heat.



Simpler closed-loop systems (All-In-One coolers) are available for single components (CPU or GPU) only.

Maintenance for an open-loop system includes periodic draining, cleaning, and refilling. Fans and radiators must be kept dust-free, and the system should be drained before moving the PC to a different location.

Lesson 3B

Storage Devices

Lesson Overview

You need to build a server to store student assessments and coursework for a school. The server must ensure that student work is always available and safe from damage or loss. For administrators, reliable storage means the computer always starts up correctly. You will choose, install, and maintain the storage devices to meet these needs.



Objectives Covered

3.4 Compare and contrast storage devices.

Learning Outcomes:

As you study this lesson, answer the following questions:

- What are the advantages of using Solid State Drives over Hard Disk Drives, and how does wear leveling help extend the lifespan of a Solid State Drive?
- What is Redundant Array of Independent Disks (RAID), and how does RAID 5 differ from RAID 1 in terms of fault tolerance and performance?
- What are the benefits and drawbacks of using RAID 0 and RAID 1, and in what scenarios would each be appropriate?
- How does RAID 10 combine the features of RAID 0 and RAID 1, and why is it suitable for high-performance applications?
- What are the different types of secure digital (SD) cards, and how do their capacity and speed ratings differ?

Mass Storage Devices

Non-volatile storage devices, also known as mass storage, retain data even when the system is powered off. These devices use magnetic, optical, or solid-state technology. Internal mass storage devices are called fixed disks and come in standard widths of 5.25 inches, 3.5 inches, and 2.5 inches. Computer chassis have drive bays to fit these form factors, with 5.25-inch bays often featuring removable panels for devices like DVD drives and smart card readers.

Fixed disks are typically installed in drive bays using caddies, which allow for secure mounting and can adapt different drive sizes to fit various bays. For example, a 2.5-inch drive can be installed in a 3.5-inch bay using an adapter caddy. Some caddies use rails for easy removal without opening the case.

Motherboard Storage Drive Bays

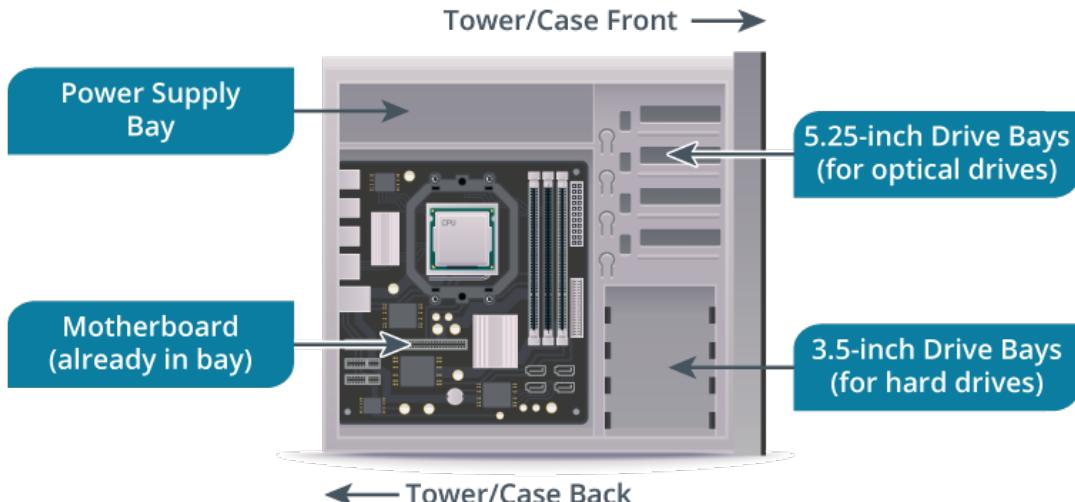


Image © 123RF.com

Removable mass storage devices and media enabled data archiving and transfer between PCs. External storage devices, such as external hard drives, are used for backup, data transfer, or providing additional drive types and typically connect via USB or Thunderbolt ports.

Several factors impact the choice of mass storage devices:

- **Reliability:** This includes the risk of total device failure and partial data corruption, rated by various statistics for each technology type.
- **Performance:** Evaluate based on the type of data transfer, considering read/write performance, sequential vs. random access, data throughput (MB/s or GB/s), and input/output operations per second (IOPS).
- **Use:** Consider reliability and performance in the context of specific use cases, such as running an OS, hosting a database, streaming audio/video, removable media, or data backup and archiving.

Major mass storage drive vendors include Seagate, Western Digital, Hitachi, Fujitsu, Toshiba, and Samsung.

Solid-State Drives

A solid state drive (SSD) uses flash memory technology for persistent mass storage, offering significantly better read performance than the mechanical components in hard disk drives (HDDs), especially in read operations. SSDs are less prone to failure from mechanical shock and wear, and their cost per gigabyte has decreased rapidly in recent years. However, SSDs can sometimes underperform compared to HDDs when handling multi-gigabyte file sizes.

A 2.5-inch form factor solid state drive with SATA interface



Image © 123RF.com

Flash memory in SSDs can degrade over many write operations. To mitigate this, drive firmware and operating systems use wear leveling routines to evenly distribute writing across all blocks, optimizing the device's lifespan.

! The NOT AND (NAND) flash memory used in SSDs comes in different types. Single-level-cell (SLC) is more reliable and expensive than multi-level cell types.

In modern desktop PCs, an SSD might serve as the sole internal drive or as a boot drive alongside a hard drive, with the SSD hosting the OS and applications and the HDD storing user data.

SSDs can be connected via different interfaces:

- **SATA:** SSDs may be packaged in a 2.5-inch caddy and connected using standard SATA data and power connectors. Alternatively, [mSATA](#) form factor SSDs plug into a combined data and power port on the motherboard. However, the 600 MBps SATA interface can bottleneck high-performing SSDs, which can achieve transfer rates up to 6.7 GB/s.
- **PCI Express (PCIe):** Modern SSDs often use the PCIe bus directly, utilizing the Non-Volatile Memory Host Controller Interface Specification (NVMHCl) or [non-volatile memory express](#) (NVMe) interface for better performance. NVMe SSDs can be installed in a PCIe slot as an expansion card or in an M.2 slot. M.2 SSDs are smaller and oriented horizontally, making them suitable for laptops and PC motherboards. M.2 slots provide power over the bus, eliminating the need for a separate power cable. M.2 adapters come in various sizes, indicated by labels such as M.2 2280 (22mm wide and 80mm long). PCIe 4.0, offers transfer rates up to 16 GT/s per lane, while PCIe 5.0 doubles this to 32 GT/s per lane, significantly enhancing SSD performance.
- **Serial Attached SCSI Small Computer System Interface (SAS):** SAS is another interface used for high-performance storage devices, often in enterprise environments. SAS drives offer faster data transfer rates and better reliability compared to SATA drives. SAS connects

multiple devices to a single controller using a point-to-point serial protocol, enabling high-speed data access and robust performance. They are commonly used in servers and workstations.

SSDs are vulnerable to electrostatic discharge (ESD), so always take anti-ESD precautions when handling and storing these devices.

mSATA SSD form factor



Image © 123RF.com



M.2 is a physical form factor. M.2 SSDs can use either the SATA/AHCI bus or the NVMe interface. NVMe-based M.2 SSDs typically outperform their SATA counterparts. Check your motherboard documentation to ensure compatibility with both types. SATA interface SSDs are usually B keyed, 2-lane PCIe SSDs are B/M keyed, and 4-lane SSDs are M keyed.

Hard Disk Drives

A [hard disk drive](#) (HDD) stores data on metal or glass platters coated with a magnetic substance. Each platter has a read/write head on both sides, moved by an actuator mechanism. The platters are mounted on a spindle and spin at high speeds. Each side of a platter is divided into circular tracks, which are further divided into sectors, each holding 512 bytes. This low-level formatting is known as drive geometry.

HDD with drive circuitry and casing removed showing 1) Platters; 2) Spindle; 3) Read/Write Heads; 4) Actuator

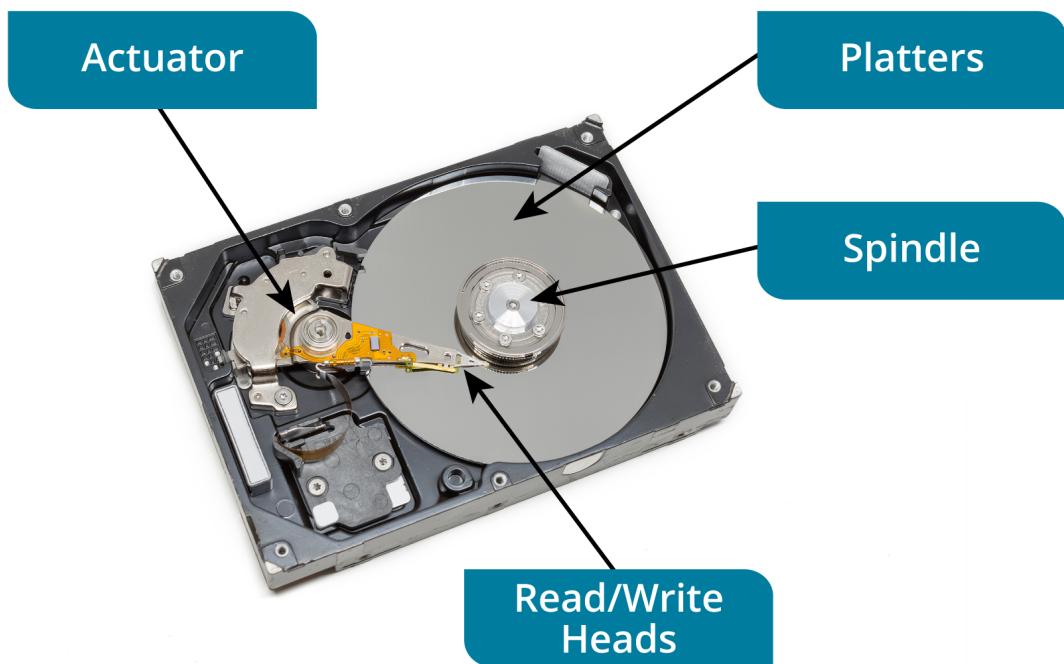


Image by mkphotoshu © 123RF.com

HDD performance is determined by the disk's spindle speed, measured in revolutions per minute (RPM). High-performance drives spin at **15,000** or **10,000** RPM, while average drives spin at **7,200** or **5,400** RPM. RPM affects access time, measured in milliseconds, which includes both access and seek time. Access time is the delay as the read/write head locates a track, while seek time is the time it takes to move to the data's position. High-performance drives have access times below 3 ms, while typical drives have around 6 ms.

The internal transfer rate (or data transfer rate) measures how fast read/write operations are performed on the platters. A 15,000 RPM drive supports up to 180 MBps, while a 7,200 RPM drive supports around 110 MBps.

Most HDDs use a SATA interface. HDDs come in two main form factors: 3.5-inch units for desktop PCs and 2.5-inch units for laptops and portable external drives. The 2.5-inch form factor can vary in height, with options including 15 mm, 9.5 mm, 7 mm, and 5 mm.

Redundant Array of Independent Disks

Both HDDs and SSDs store critical data, including system files for the OS and user-generated data files. If a boot drive fails, the system crashes. If a data drive fails, users lose access to files, potentially resulting in permanent data loss if not backed up. To mitigate these risks, disks can be configured as a [redundant array of independent/inexpensive disks](#) (RAID).

RAID works by distributing data across multiple disks to provide [fault tolerance](#) and improve performance. It sacrifices some disk capacity to achieve redundancy. To the OS, a RAID array appears as a single storage volume, which can be partitioned and formatted like any other drive.

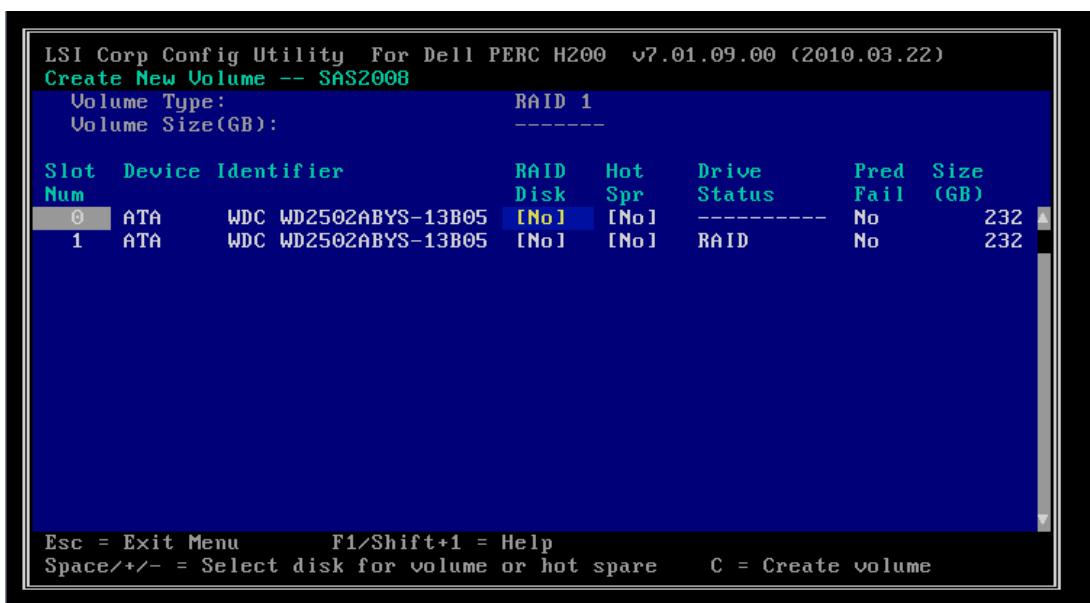
 RAID can also be said to stand for "Redundant Array of Independent Devices,"

RAID levels represent different **drive configurations** with specific types of fault tolerance, numbered from 0 to 6, with nested solutions like RAID 10 (RAID 1 + RAID 0). RAID can be implemented via software (software RAID) using OS features or via hardware (hardware RAID) using a dedicated controller installed as an adapter card. RAID disks connect to SATA ports on the RAID controller adapter card rather than the motherboard.

 As another option, some motherboards implement integrated RAID functionality as part of the chipset.

Hardware RAID solutions vary by the RAID levels they support. Entry-level controllers might support only RAID 0 or RAID 1, while mid-level controllers might add RAID 5 and RAID 10. Hardware RAID often allows for hot-swapping, meaning a damaged disk can be replaced without shutting down the OS.

Configuring a volume using RAID controller firmware



```

LSI Corp Config Utility For Dell PERC H200 v7.01.09.00 (2010.03.22)
Create New Volume -- SAS2008
  Volume Type: RAID 1
  Volume Size(GB): -----
Slot  Device Identifier          RAID   Hot   Drive   Pred   Size
Num      Disk     Spr    Status   Fail   (GB)
0       ATA      WD2502ABYS-13B05 [No]  [No]  -----  No    232
1       ATA      WD2502ABYS-13B05 [No]  [No]  RAID    No    232

Esc = Exit Menu      F1/Shift+1 = Help
Space/+/- = Select disk for volume or hot spare    C = Create volume

```

RAID 0 and RAID 1

When implementing RAID, selecting the appropriate RAID level is crucial. Factors to consider include the required fault tolerance, read/write performance, capacity, and cost.

 When building a RAID array, it's crucial to use disks that are identical in capacity, type, and performance to avoid issues with underutilization or potential performance bottlenecks. If disks differ in size, the smallest disk will indeed determine the maximum usable space across the array.

RAID 0 (Striping without Parity)

Disk striping divides data into blocks and distributes them across all disks in the array, improving performance by allowing multiple disks to service requests in parallel. [RAID 0](#), which requires at least two disks, uses this method. The logical volume size is the sum of the capacities of all drives, limited by the smallest disk in the array.

However, RAID 0 provides no redundancy. If any disk fails, the entire logical volume fails, causing a system crash and necessitating data recovery from backups. Therefore, RAID 0 is typically used only for non-critical cache storage.

RAID 0 (striping)—Data is spread across the array

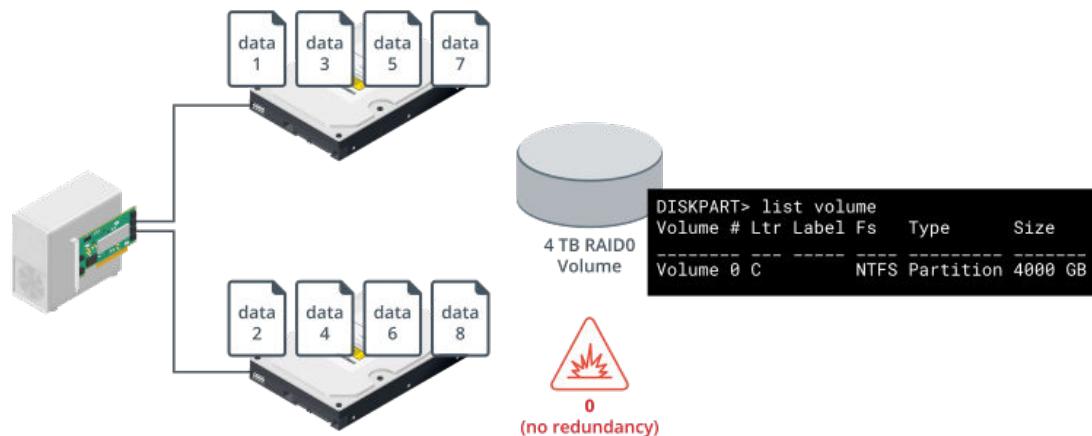


Image ©123RF.com

RAID 1 (Mirroring)

RAID 1 is a mirrored drive configuration using two disks. Each write operation is duplicated on the second disk, introducing a small performance overhead. Read operations can use either disk, slightly boosting performance. This setup is the simplest way to protect against single disk failure. If one disk fails, the other takes over with minimal performance impact, maintaining good availability. However, the failed disk should be replaced quickly to restore redundancy. When replaced, the new disk is populated with data from the remaining disk. Performance during rebuilding is temporarily reduced, though RAID 1 rebuilds faster than parity-based RAID levels.

RAID 1 (mirroring)—Data is written to both disks simultaneously

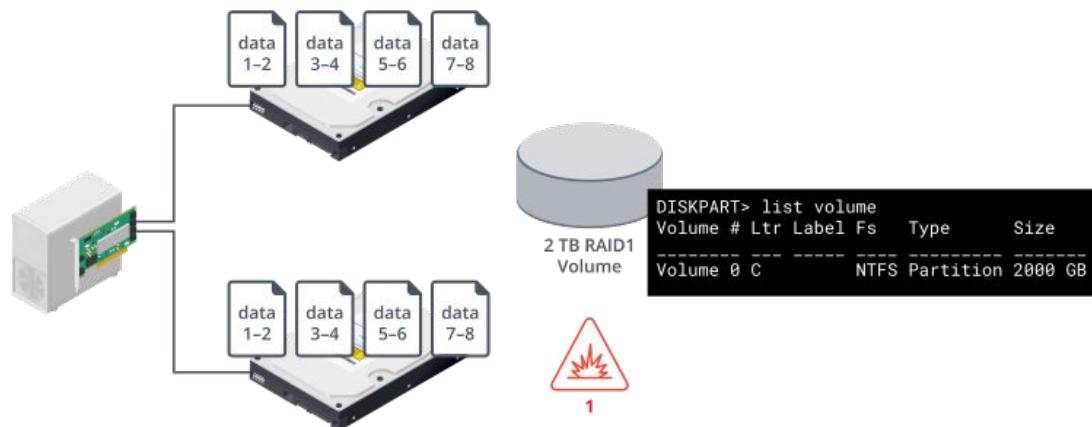


Image ©123RF.com

Disk mirroring is more expensive per gigabyte than other forms of fault tolerance because it utilizes only 50% of the total disk space.

RAID 5 and RAID 10

RAID 5 and RAID 10 offer better performance, disk utilization, and fault tolerance compared to basic mirroring, making them more suitable choices in many scenarios.

RAID 5 (Striping with Distributed Parity)

RAID 5 combines striping (like RAID 0) with distributed parity. Distributed parity means that error correction information is spread across all the disks in the array. Data and parity information are always on different disks. If a single disk fails, the data can be reconstructed using the information on the remaining disks. RAID 5 offers excellent read performance, but if a disk fails, read performance slows down because the system needs to use the parity information to recover data. Write operations are also slower due to the need to calculate parity.

RAID 5 (striping with parity)



Image ©123RF.com

RAID 5 requires at least three drives but can use more. This provides more flexibility in determining the array's overall capacity compared to RAID 1. The maximum number of drives is set by the controller or OS, but practical considerations like cost and risk usually determine the number of drives used. Adding more disks increases the chance of failure. If more than one disk fails, the entire logical storage unit (volume) becomes unavailable.

The level of fault tolerance and available disk space are inversely related. As you add more disks, fault tolerance decreases but usable disk space increases. For example, in a RAID 5 array with three disks, one-third of each disk is used for parity. With four disks, one-quarter of each disk is reserved for parity. In a three-disk configuration with 80 GB each, you would have 160 GB of usable space.

RAID 10 (Stripe of Mirrors)

RAID 10 combines features of RAID 0 and RAID 1. It is a striped volume (RAID 0) made up of mirrored arrays (RAID 1). This setup offers excellent fault tolerance, as one disk in each mirror can fail without losing data.

RAID 10—Either disk in each of the sub-volumes can fail without bringing down the main volume.



Image ©123RF.com

RAID 10 requires at least four disks and must have an even number of disks. It has a 50% disk overhead due to mirroring.

RAID 6 (Striping with Double Parity)

RAID 6 uses striping with dual distributed parity, spreading two sets of parity information across all disks. This allows RAID 6 to tolerate the simultaneous failure of two disks, providing greater fault tolerance than RAID 5. It's ideal for environments with higher disk failure risks, such as large arrays or critical systems. In the event of a disk failure, the array continues to operate with slightly reduced performance. Rebuilding a failed disk uses parity data from the remaining disks, a process that can be time-consuming based on disk size and system load.

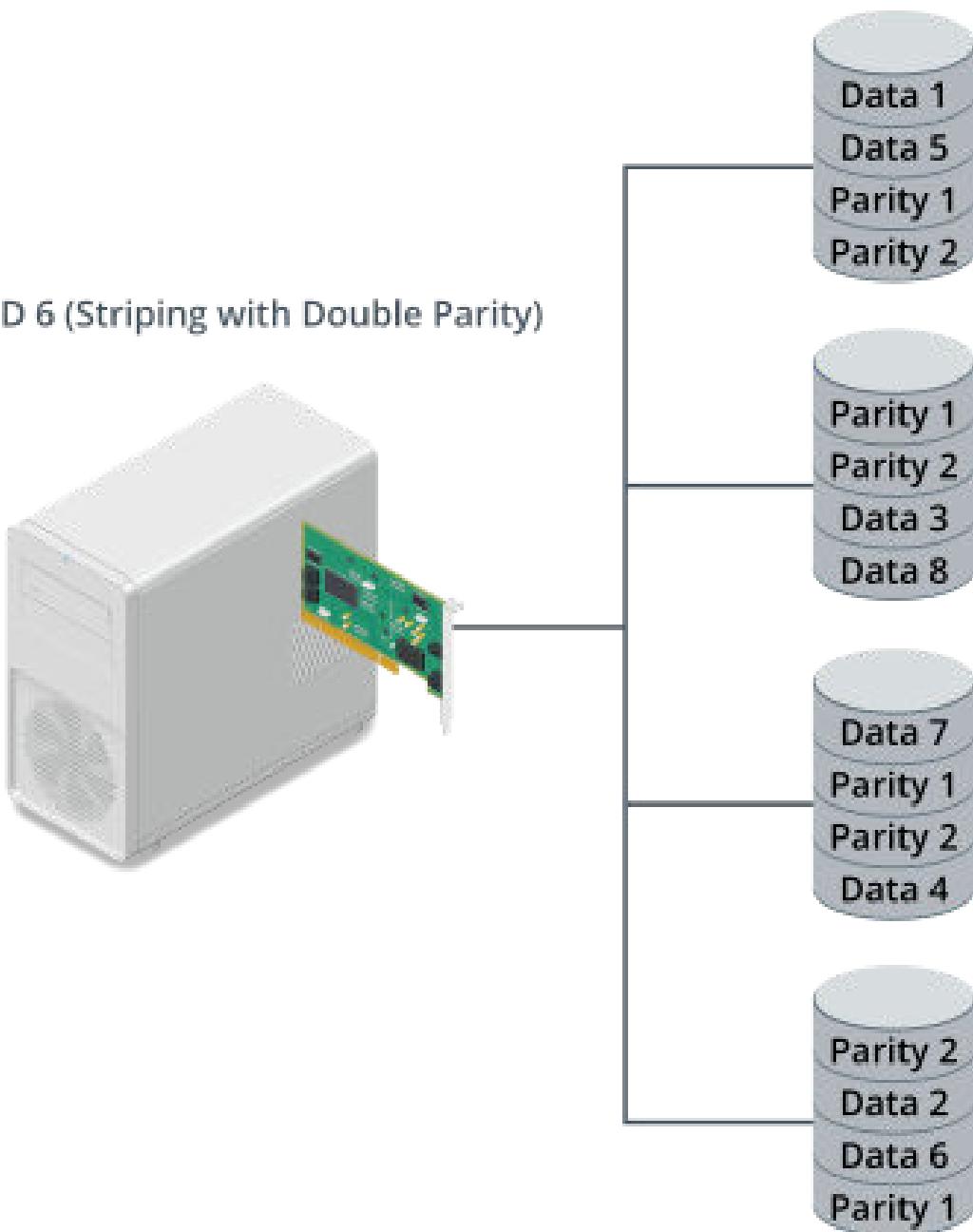
RAID 6 offers good read performance similar to RAID 5, but slower write performance due to the need to calculate and write two sets of parity data. The array remains operational even if one or two disks fail, though performance will degrade. A minimum of four disks is required, with two used for data storage and two for parity. RAID 6 is more suitable for larger arrays than RAID 5 due to its ability to tolerate two disk failures.

The usable capacity of a RAID 6 array is the total capacity minus the capacity of two disks for parity. For example, a four-disk array with 1 TB disks has 2 TB of usable capacity.

RAID 6 is more expensive than RAID 5 due to the need for additional disks and more powerful RAID controllers. Longer rebuild times and the write penalty are potential risks, so monitoring the array's health and planning for prompt disk replacements are essential.

RAID 6

RAID 6 (Striping with Double Parity)



Images © 123RF.com

Removable Storage Drives

Removable storage refers to devices that can be moved between computers without opening the case or to media that can be removed from its drive.

Drive Enclosures

HDDs and SSDs can be used as removable storage by placing them in an enclosure. The enclosure provides a data interface (such as USB, Thunderbolt, or eSATA), a power connector (if needed), and physical protection for the disk.

External storage device



Image ©123RF.com

Some enclosures, known as Network Attached Storage (NAS), can be connected directly to a network. Advanced enclosures can host multiple disks configured as a RAID array.

Some enclosures can be connected directly to a network rather than to a PC. This is referred to as network attached storage (NAS). Advanced enclosures can host multiple disk units configured as a RAID array.

Flash Drives and Memory Cards

SSDs (Solid State Drives) use flash memory, which can also be found in other forms like flash drives and memory cards. Also known as a USB drive, thumb drive, or pen drive, a [flash drive](#) consists of a flash memory board with a USB connector and a protective cover. You can plug it into any available USB port on your computer.

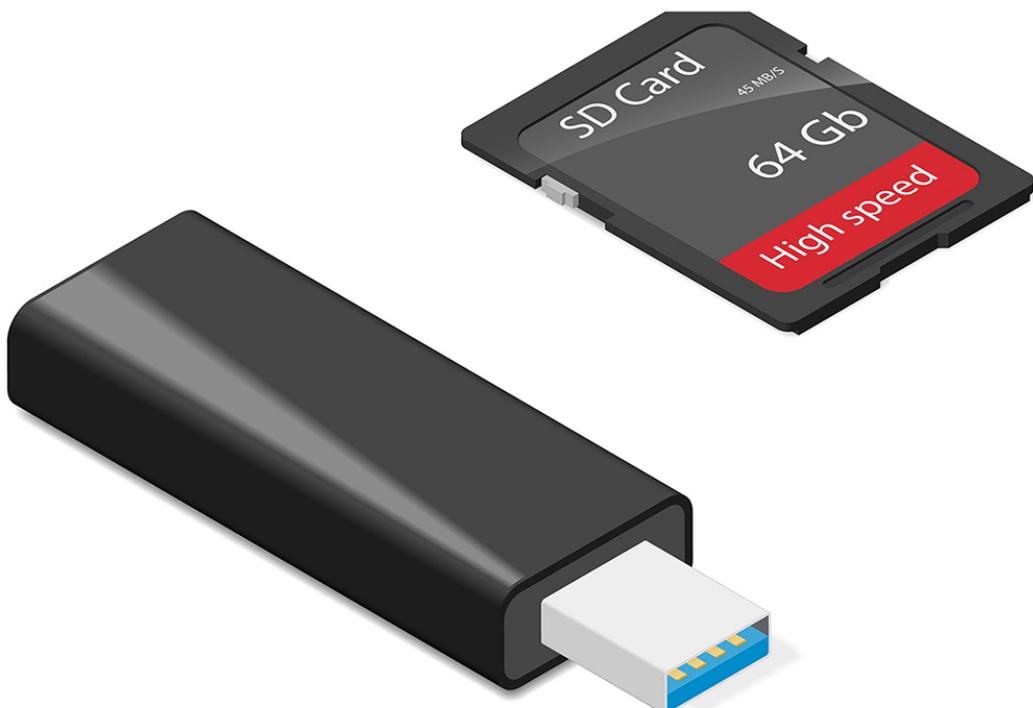
USB thumb drive (left) and SD memory card (right)

Image ©123RF.com

Commonly used in digital cameras, smartphones, and tablets to store photos, videos, and other data, a [memory card](#) requires a card reader to be used with a PC. These readers often fit into a front-facing drive bay of a PC and connect to the motherboard via a USB controller. Most motherboards have spare USB headers for these internal connections, or the reader might come with an expansion card.

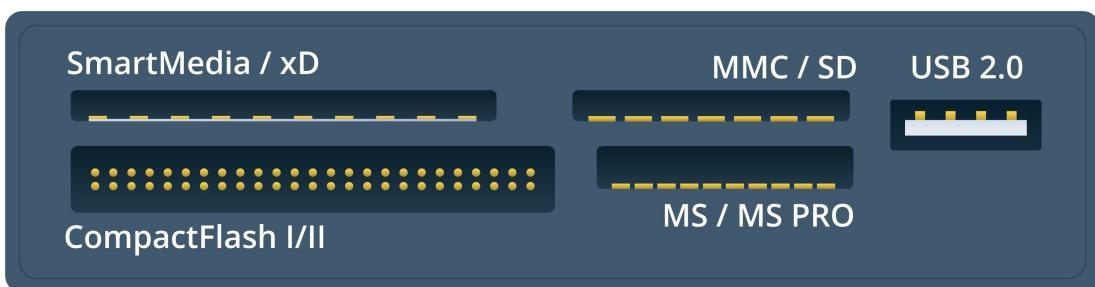
Multi-card reader

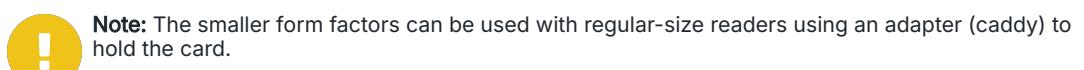
Image ©123RF.com

There are several proprietary types of memory cards, each with different sizes and performance levels. Most memory card readers can read multiple types of cards. For example, Secure Digital (SD) cards come in three capacity types:

- **SD:** Up to 2 GB.
- **SDHC (Secure Digital High Capacity):** Up to 32 GB.
- **SDXC (Secure Digital Extended Capacity):** Up to 2 TB.

SD cards also have different speed ratings:

- **Original SD:** Up to 25 MBps.
- **UHS (Ultra High Speed):** Up to 108 MBps.
- **UHS-II:** Up to 156 MBps full-duplex or 312 MBps half-duplex.
- **UHS-III:** Up to 312 MBps (FD312) or 624 MBps (FD624) full-duplex.
- **SD Express:** The latest variant, which combines the SD card form factor with PCIe and NVMe interfaces, offers speeds up to 985 MBps.



Note: The smaller form factors can be used with regular-size readers using an adapter (caddy) to hold the card.

Optical Drives

Compact Disc - Read Only Memory, **Digital Versatile Discs (DVDs)**, and **Blu-ray Discs (BDs)** are used for music and video retail. These optical media types use a laser to read data encoded on the disc surface. While marketed as durable, scratches can make them unreadable.

These discs can also store PC data and come in recordable and rewritable formats:

- **Basic Recordable Media:** Can be written to once in a single session.
- **Multisession Recordable Media:** Can be written to in multiple sessions, but data cannot be erased.
- **Rewritable Media:** Can be written and erased multiple times, up to a certain number of write cycles.

Capacity and Transfer Rates

Each optical disc type has different capacities and transfer rates:

- **CD:**
 - Capacity: Up to 700 MB.
 - Formats: Recordable (CD-R) and Rewritable (CD-RW).
 - Base Transfer Rate: 150 KBps.
- **DVD:**
 - Capacity: 4.7 GB (single-layer, single-sided) to about 17 GB (dual-layer, double-sided).
 - Formats: DVD+R/RW and DVD-R/RW (most drives support both, indicated by the ± symbol).
 - Base Transfer Rate: 1.32 MBps (equivalent to 9x CD speed).
- **Blu-ray:**
 - Capacity: 25 GB per layer.
 - Base Transfer Rate: 4.5 MBps, with a maximum theoretical rate of 16x (72 MBps).

Installation and Connectivity

- **Internal Optical Drive:** Installed in a 5.25-inch drive bay and connected to the motherboard via SATA data and power connectors.
- **External Optical Drive:** Connected via USB, eSATA, or Thunderbolt. These drives usually require an external power supply via an AC adapter. They may use either a tray-based or slot-loading mechanism.

Optical drive unit



Image ©123RF.com



Drives also feature a small hole that accesses a disc eject mechanism (insert a paper clip to activate the mechanism). This is useful if the standard eject button does not work or if the drive does not have power.

Drives are rated by their data transfer speeds, expressed as record/rewrite/read speeds (e.g., 24x/16x/52x). New drives are generally multi-format, but older drives may lack Blu-ray support.

Consumer DVDs and Blu-rays often include digital rights management (DRM) and region coding. Region coding restricts disc usage to players from the same region. On PCs, the region can be set via device properties but is usually limited to a few changes by the firmware.

Lesson 3C

System Memory

Lesson Overview

As an IT professional, you are tasked with upgrading and optimizing the memory of a high-performance workstation used by a financial analyst. The workstation needs to handle large datasets, run multiple applications simultaneously, and perform complex calculations efficiently. You must ensure that the system memory is configured correctly to meet these requirements.



Objectives Covered

3.3 Compare and contrast RAM characteristics.

Learning Outcomes

As you study this lesson, answer the following questions:

- What is the role of system RAM in a computer, and how does virtual memory help when system RAM is insufficient?
- What are the differences between DDR3, DDR4, and DDR5 RAM in terms of data rate, transfer rate, and maximum size?
- What is a memory module, and why is it important to match the DDR type with the motherboard?
- What is dual-channel memory, and how does it differ from single-channel memory in terms of performance?
- How do triple-channel and quadruple-channel memory configurations improve performance, and what are the requirements for these configurations?
- What is ECC RAM, and how does it help prevent data corruption and system crashes?

System RAM and Virtual Memory

The CPU processes software instructions through a pipeline, with the top instructions stored in its registers and cache. However, the CPU's cache is limited, necessitating support from additional storage technologies.

When executing a process or opening a data file, the image is loaded from the fixed disk into system memory (RAM). Instructions are then fetched from RAM into the CPU's cache and registers as needed, managed by a memory controller.

System memory, implemented as random-access memory (RAM), is faster than SSD flash memory and much faster than HDDs, but it is volatile, meaning it only stores data when powered

on. System memory is measured in gigabytes (GB), and the amount of RAM determines a PC's ability to handle multiple applications simultaneously and process large files efficiently.

Address Space

The bus, or communication system, connecting the CPU, memory controller, and memory devices has two main pathways: data and address.

- **Data Pathway:** Determines the amount of information transferred per clock cycle. In a single channel memory controller, this bus is typically 64 bits wide.
- **Address Pathway:** Determines the number of memory locations the CPU can track, thus limiting the maximum physical and virtual memory.
 - A 32-bit CPU with a 32-bit address bus can access up to 4 GB of memory.
 - A 64-bit CPU could theoretically use a 64-bit address space (16 exabytes), but most use a 48-bit address bus, allowing up to 256 terabytes of memory.

A 64-bit CPU can address more memory locations than a 32-bit CPU. The 64-bit data bus is the amount of memory that can be transferred between the CPU and RAM per cycle

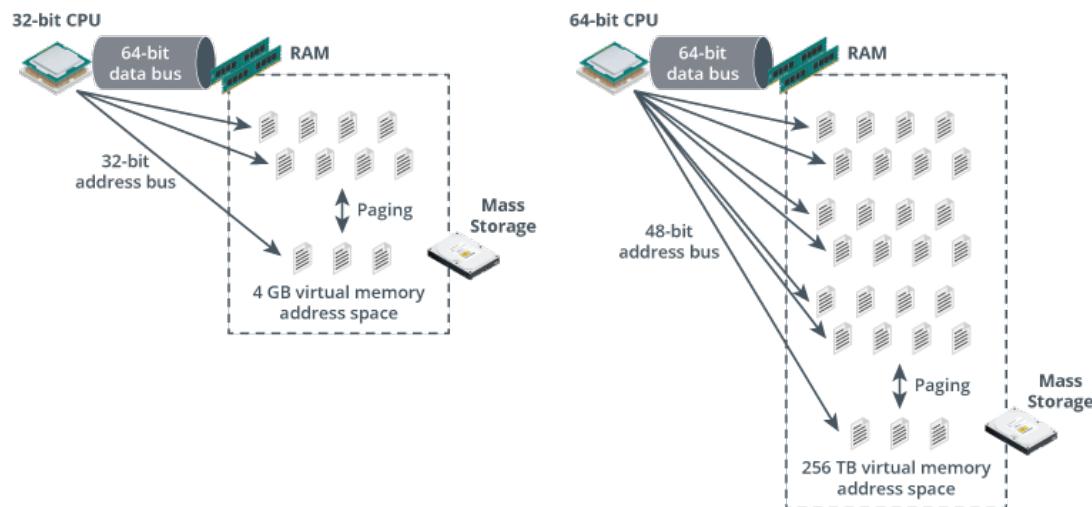


Image ©123RF.com

32-bit C P U is connected to a 64-bit data bus and RAM, uses a 32-bit address bus with a virtual memory address space of 4 G B, and includes paging to mass storage. 64-bit C P U is connected to a 64-bit data bus and RAM, uses a 48-bit address bus with a virtual memory address space of 256 T B, and includes paging to mass storage.

RAM Types

Modern system RAM is implemented as Double Data Rate Synchronous Dynamic Random Access Memory (DDR SDRAM), reflecting a progression of memory technologies from the 1990s to today:

- **Dynamic RAM (DRAM)** stores data bits as electrical charges in bit cells made of capacitors, that hold a charge, and transistors, that read the capacitor's contents. A charged capacitor represents 1, non-charged represents 0.
- **Synchronous DRAM (SDRAM)** is synchronized to the system clock, ensuring that memory operations are timed with the CPU's instructions.

- **DDR SDRAM (Double Data Rate SDRAM)** doubles data transfer by transmitting data on both the rising and falling edges of the clock cycle.

DDR memory modules are labeled by their maximum theoretical bandwidth, such as PC1600 or PC2100. Here's how these values are derived using DDR-200 (PC1600) as an example:

- **Clock Speed:** Both the internal memory device clock speed and the memory bus speed are 100 MHz.
- **Data Rate:** DDR performs two operations per clock cycle, resulting in a data rate of 200 megatransfers per second (MT/s), hence the DDR-200 designation.
- **Peak Transfer Rate:** The peak transfer rate is 1600 MBps (200 MT/s multiplied by 8 bytes per transfer), giving the PC-1600 designation. This is equivalent to 1.6 GBps.

Subsequent generations of DDR technology—DDR1, DDR2, DDR3, DDR4, and DDR5—increase bandwidth by multiplying the bus speed rather than the speed of the memory devices. This approach allows for scalable speed improvements without making the memory modules too unreliable or too hot. Design improvements also increase the maximum possible capacity of each memory module.

RAM Type	Data Rate	Transfer Rate	Maximum Size
DDR1	200 to 400 MT/s	1.6 to 3.2 GB/s	1 GB
DDR2	400 to 1066 MT/s	3.2 to 8.5 GB/s	4 GB
DDR3	800 to 2133 MT/s	6.4 to 17.066 GB/s	16 GB
DDR4	1600 to 3200 MT/s	12.8 to 25.6 GB/s	32 GB
DDR5	4800 up to 8000+	38.4 to 51.2+ GB/s	128 GB or higher

 MT/s stands for "megatransfers per second," where "mega" refers to one million. It is a measure of the data transfer rate, indicating how many million data transfers occur per second.

The transfer rate is the speed at which data is transferred by the memory controller. Memory modules also have internal timing characteristics that are expressed as values like 14-15-15-35 CAS 14. Lower values indicate better performance among RAM modules of the same type and speed. CAS latency, or Column Access Strobe latency, refers to the delay between the memory controller requesting data from the RAM and the moment it becomes available. It is measured in clock cycles. Lower CAS latency means the memory can access data more quickly, leading to better performance. This latency is a crucial factor in determining the overall speed and efficiency of RAM, especially when comparing modules of the same type and speed.

Architectural Improvements in DDR4 and DDR5:

- DDR4: Introduced improvements such as increased power efficiency and higher density, allowing for larger memory capacities. It also features a more efficient channel design, which enhances data throughput.
- DDR5: Further enhances power efficiency and introduces dual-channel architecture per module, effectively doubling the data paths and improving overall performance.

Memory Modules

A memory module is a printed circuit board that holds a group of RAM devices acting as a single unit. These modules come in various capacities, with each DDR generation setting an upper limit on maximum capacity. Desktop memory is packaged as a **Dual Inline Memory Module (DIMM)**. The notches on the module's edge connector identify the DDR generation (DDR3,

DDR4, DDR5) and prevent incorrect insertion. DIMMs often feature heat sinks due to high clock speeds.

DDR SDRAM packaged in DIMMs

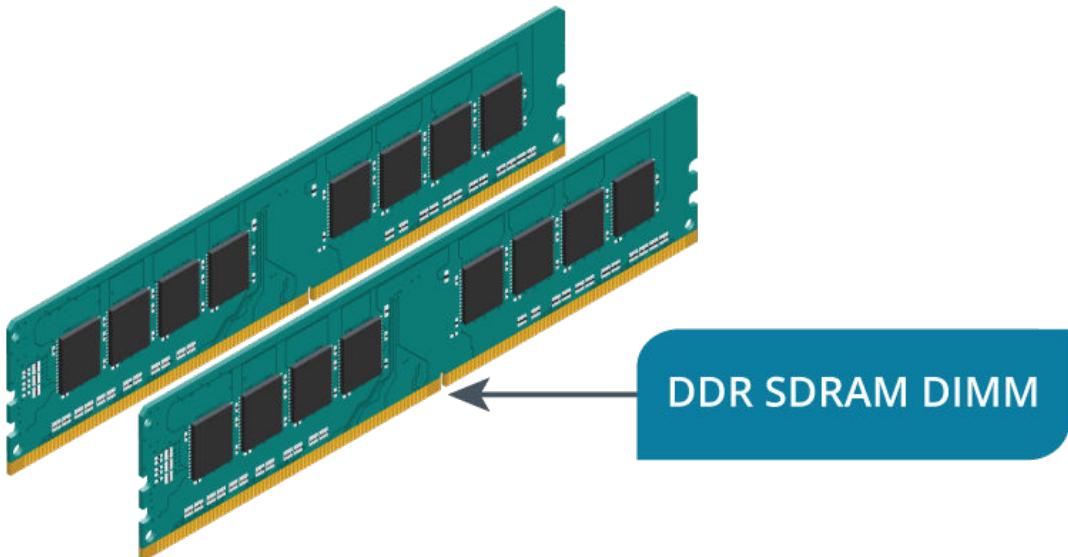


Image ©123RF.com

! Memory modules are vulnerable to electrostatic discharge (ESD). Always take anti-ESD precautions when handling and storing these devices.

DIMMs and SODIMMs are designed for different purposes based on their size and application. DIMMs, or Dual Inline Memory Modules, are primarily used in desktop computers. Their larger size allows for higher capacities and better performance, making them ideal for systems that require significant memory, such as gaming PCs and workstations. In contrast, [SODIMMs](#) (Small Outline DIMMs) are smaller and typically used in laptops and compact devices. Although they offer lower capacities and performance compared to DIMMs, SODIMMs are preferable in scenarios where space is limited. Typical SODIMM capacities range from 4 GB to 32 GB, making them suitable for portable devices and small form factor systems. In terms of use-case scenarios, DIMMs are favored in systems where performance and capacity are prioritized, such as gaming rigs, high-performance desktops, and servers. Conversely, SODIMMs are ideal for laptops, mini PCs, and other compact systems where space constraints are a consideration.

Installation and Compatibility

When installing memory modules, it is crucial to ensure that the DDR type matches the motherboard. For instance, DDR5 modules cannot be installed in DDR4 slots. For optimal performance, it is advisable to use modules rated at the same bus speed as the motherboard. While mixing different speeds is possible, it is not recommended, as the system will operate at the speed of the slowest component.

Memory slots resemble expansion slots but have catches on each end to secure the modules. SODIMMs are typically fitted into slots that pop up at a 45° angle for easy insertion or removal.

SODIMM

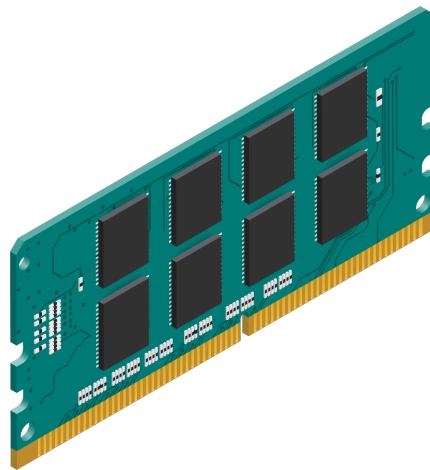


Image © 123RF.com

Multi-channel System Memory

In the 2000s, the increasing speed and architectural improvements of CPUs led to memory becoming a bottleneck in system performance. To address this, Intel and AMD developed dual-channel architecture for DDR memory controllers. Initially used in server-level hardware, dual-channel is now common in desktop systems and laptops.

Single-Channel vs. Dual-Channel Memory

- **Single-channel:** Features one 64-bit data bus between the CPU, memory controller, and RAM, which can limit data transfer rates.
- **Dual-channel:** Utilizes two 64-bit pathways, allowing 128 bits of data per transfer, effectively doubling the data bandwidth. This requires support from the CPU, memory controller, and motherboard, but not from the RAM modules themselves. Ordinary RAM modules are used; there are no specific "dual-channel" DDR memory modules.



Note: DDRx memory is sold in "kits" for dual-channel use, but the modules are identical to standard ones.

Motherboard DIMM slots (dual channel). Slots 1 and 3 (black slots) make up one channel, while slots 2 and 4 (grey slots) make up a separate channel

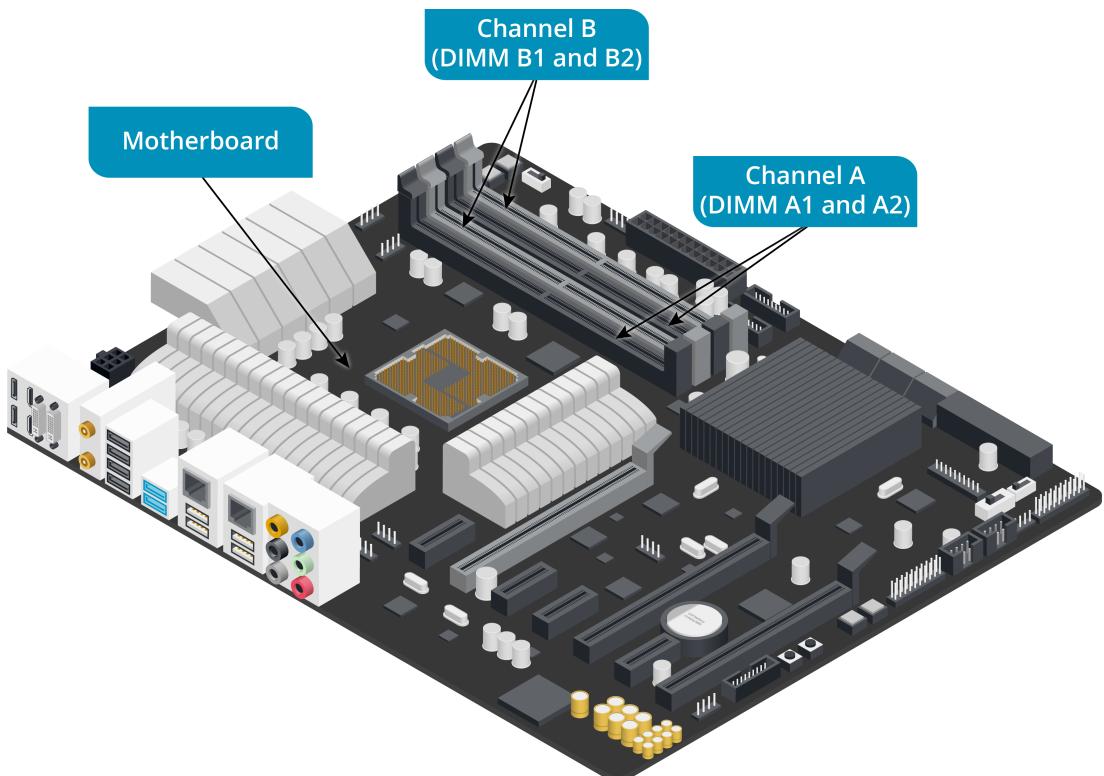


Image ©123RF.com

Configuring Dual-Channel Systems

- Slot Arrangement:** Dual-channel motherboards often have four DIMM slots arranged in color-coded pairs. Each pair represents one channel (e.g., channel A might be orange, and channel B might be blue).
- Installation:** To enable dual-channel, install identical modules in the corresponding slots of each channel (e.g., A1 and B1). The modules should match in clock speed, capacity, timings, and latency. Clock speed refers to the frequency at which the memory operates, affecting how quickly data can be processed. Timings and latency refer to the delay before data transfer begins, with lower values indicating faster performance. If the modules do not match, the system will default to the lowest (worst performing) values.
- System Setup:** Dual-channel mode may need to be enabled via the PC firmware's system setup program.



Note: Be aware that not all motherboards use consistent labeling or color-coding for their DIMM slots. Some may color-code each channel, while others color-code the socket numbers. Always consult the system documentation to ensure proper installation.

Mismatched Modules and Flex Mode

When adding an odd number of memory modules or modules with different clock speeds and sizes, several outcomes can occur. The system may default to single-channel mode, which limits data transfer rates compared to dual-channel configurations. Alternatively, the

system might enable dual-channel mode but disable the spare module, effectively ignoring the additional memory. In some cases, flex mode may be utilized. For instance, if slot A1 contains a 2 GB module and slot B1 contains a 6 GB module, dual-channel mode will be enabled for the 2 GB portion, while the remaining 4 GB in B1 will operate in single-channel mode. This configuration allows for some performance benefits of dual-channel operation while accommodating mismatched module sizes.

Triple-Channel and Quadruple-Channel Memory

Some CPUs and chipsets support [triple-channel](#) or [quadruple-channel](#) memory controllers. If the full complement of modules is not installed, the system will revert to as many channels as are populated.

 **Note:** DDR5 introduces a new data bus architecture. Each memory module has two 32-bit channels. When installed in a dual-channel memory controller configuration, this results in four 32-bit channels. This architecture distributes the load on each RAM device more effectively, supporting higher density (more gigabytes per module) and reducing latency. It also works better with the multi-core features of modern CPUs.

ECC RAM

[Error correction code](#) (ECC) RAM is primarily used in workstations and servers where high reliability is critical. It can detect and correct single-bit memory errors, preventing data corruption and system crashes. It can also detect (but not correct) multi-bit errors, generating an error message and halting the system if such an error occurs.

ECC RAM adds an 8-bit checksum to each data transfer, requiring a 72-bit data bus instead of the standard 64-bit bus. The memory controller calculates the checksum and compares it to the one stored by the RAM to detect errors.

Most ECC RAM is supplied as Registered DIMMs (RDIMMs), which include a register that reduces the electrical load on the memory controller, improving system stability when large amounts of memory are used. This comes with a slight performance penalty.

Unbuffered DIMMs (UDIMMs) are more common in consumer-grade systems and typically do not support ECC. However, some ECC RAM is available as UDIMMs, though this is less common.

Compatibility Considerations

- **Motherboard and CPU Support:** Both must support ECC for it to be enabled.
- **DIMM Type Compatibility:** Most motherboards support either UDIMMs or RDIMMs, not both. Mixing different types (e.g., UDIMMs with RDIMMs) will prevent the system from booting.
- **Mixing ECC and Non-ECC:** Mixing ECC and non-ECC UDIMMs is generally not supported and will likely result in system instability or failure to boot.

 **Note:** DDR5 RAM introduces an internal error-checking mechanism within the module itself, but this is not the same as traditional ECC. DDR5 still comes in both ECC and non-ECC varieties, with the latter providing full error correction via the memory controller.

Lesson 3D

CPUs

Lesson Overview

You are tasked with upgrading the computers for a security company. The company is rolling out more demanding analysis software and needs more powerful computers for its analysts. You need to choose and install new hardware that can handle the software while staying within the overall budget. The goal is to improve performance and ensure the new setup can support future needs.



Objectives Covered

3.5 Given a scenario, install and configure motherboards, CPUs, and add-on cards.

Learning Outcomes

As you study this lesson, answer the following questions:

- What are the four basic operations performed by the CPU on each instruction, and how can understanding these operations help in optimizing server performance?
- What are the key differences between ARM's RISC architecture and the CISC architecture used in x86/x64 CPUs, and how do these differences impact performance and power efficiency?
- What is Simultaneous Multithreading (SMT), and how does it enhance performance in multithreaded applications?
- What is the difference between Intel's Land Grid Array (LGA) and AMD's Pin Grid Array (PGA) socket types, and why is it important to match the CPU and motherboard socket types?
- What are the differences between Intel's Core i3/i5/i7/i9 processors and AMD's Ryzen 3/5/7/9 processors, and how do these differences impact the choice of desktop computers for office use?
- What are the key features of server-class CPUs like Intel Xeon and AMD EPYC, and why are these features important for data center operations?

CPU Architecture

The central processing unit (CPU), or simply the processor, executes program instruction code. When a software program runs (whether it be system firmware, an operating system, an antivirus utility, or a word-processing application), it is assembled into instructions using the CPU's fundamental instruction set and loaded into system memory. The CPU then performs the following basic operations on each instruction:

1. Fetch: The control unit fetches the next instruction in sequence from system memory to the pipeline.
2. Decode: The control unit decodes each instruction and either executes it or passes it to the arithmetic logic unit (ALU) or floating-point unit (FPU) for execution.
3. Execute: The ALU or FPU executes the instruction.
4. Write-back: The result of the executed instruction is written back to a register, cache, or system memory.
 - A register is a temporary storage area within the CPU that operates at the same clock speed as the CPU.
 - A cache is a small block of memory that operates at or near the speed of the CPU, depending on the cache level (L1, L2, L3). A cache enhances performance by storing frequently used instructions and data, reducing the time needed to access this information from the slower system memory. Together, registers and cache play a crucial role in optimizing CPU performance and efficiency.

x86 CPU Architecture

CPU architecture plays a crucial role in determining performance and suitability for different applications. Two primary architectures are RISC (Reduced Instruction Set Computing) and CISC (Complex Instruction Set Computing). RISC uses a small, optimized set of instructions for faster execution and efficiency, ideal for high-performance, power-efficient applications like mobile devices and embedded systems. Conversely, CISC, exemplified by the x86 architecture, employs a larger instruction set for more complex operations, simplifying programming and enhancing performance in general-purpose tasks, making it suitable for desktops and servers.

The x86 architecture, a CISC design, supports both **32-bit (IA-32)** and **64-bit** instruction sets and is primarily produced by **Intel** and **Advanced Micro Devices (AMD)**. These processors optimize the fetch, decode, execute, and write-back processes within the execution pipeline, allowing simultaneous processing of multiple instructions and improving throughput.

Key internal CPU components include the Arithmetic Logic Unit (ALU), which performs arithmetic and logical operations, and the Control Unit, which manages the fetch, decode, and execute cycles. Performance features such as multi-core processors enable parallel processing and improved multitasking, beneficial for applications requiring simultaneous task execution. Hyper-threading technology further boosts performance by allowing a single core to handle multiple threads, simulating additional cores.

Cache memory, a small, high-speed memory within the CPU, stores frequently accessed data and instructions. The cache hierarchy (L1, L2, L3) reduces access time to main memory, enhancing CPU efficiency. L1 cache is the smallest and fastest, integrated directly into CPU cores.

CPU families like Intel's Core series and AMD's Ryzen series utilize these architectural features for various use cases. Multi-core and hyper-threading capabilities make them ideal for demanding applications such as gaming, video editing, and data processing. Meanwhile, RISC architectures are preferred in environments prioritizing power efficiency and speed, such as mobile and embedded systems. Understanding these architectural differences helps users select the right CPU for their needs.

x64 CPU Architecture

The x86 architecture refers to the 32-bit instruction set, where each instruction can be up to 32 bits wide, and was the standard for CPUs through the 1990s. The x64 (or x86-64) architecture is the 64-bit extension of the x86 architecture, developed by Advanced Micro Devices (AMD) as AMD64 and adopted by Intel as Intel 64 or EM64T. This extension allows CPUs to handle 64-bit instructions, data paths, and memory addressing, enabling access to more than 4 GB of RAM.

64-bit CPUs can run both 32-bit and 64-bit software, whereas 32-bit CPUs cannot run 64-bit software. Software, including operating systems, device drivers, and applications, must be specifically designed and compiled to take advantage of the x64 architecture. Device drivers must match the operating system's architecture, meaning 64-bit drivers are required for a 64-bit OS. Modern operating systems like Windows 11 and most Linux distributions now require 64-bit versions, as modern OSs and applications are predominantly 64-bit, with 32-bit versions becoming obsolete.

The transition from 32-bit to 64-bit systems is evident in both hardware and software contexts. For example, Apple's shift to 64-bit began with the introduction of the 64-bit A7 chip in the iPhone 5s, and by macOS Catalina, support for 32-bit applications was completely dropped. In the software realm, many applications, such as Adobe Creative Cloud, have transitioned to 64-bit to leverage enhanced performance and memory capabilities.

The x64 architecture offers better performance, increased memory capacity, and support for more advanced computing tasks, making it the current standard for new hardware and software. Additionally, x64 architecture impacts virtualization and security by supporting hardware-based virtualization technologies, such as Intel VT-x and AMD-V, which enhance the performance and efficiency of virtual machines. It also supports Data Execution Prevention (DEP) for 64-bit systems, a security feature that helps prevent code execution from non-executable memory regions, thereby enhancing system security.

 A device driver is code that provides support for a specific model of hardware component for a given operating system.

ARM CPU Architecture

ARM ([Advanced RISC Machines](#)) provide CPU designs that are customized and manufactured by companies like Qualcomm, Nvidia, Apple, and Samsung. ARM processors are widely used in modern Apple hardware (like the M1 and M2 chips), most Android devices, Chromebooks, and some Windows tablets and laptops. A typical ARM design implements a system-on-chip (SoC), integrating components like video, sound, networking, and storage controllers into the CPU, making ARM ideal for mobile and fanless devices due to its power efficiency and compact size.

 ARM's architecture is based on Reduced Instruction Set Computing (RISC), which uses simpler, more efficient instructions compared to the Complex Instruction Set Computing (CISC) architecture used in x86/x64 CPUs from Intel and AMD. While RISC may require more instructions to perform certain tasks, each instruction typically completes in a single clock cycle, allowing for better performance-per-watt and increased battery life.

For an operating system and hardware drivers to run on an ARM-based device, they must be redesigned and compiled to use the ARM instruction set. While this task is typically within the reach of operating system developers, converting existing x86/x64 software applications to run on a different instruction set is an onerous task. Another option is support for emulation. This means that the ARM device runs a facsimile of an x86 or x64 environment. Windows 10 ARM-based devices use emulation to run x86 and x64 software apps. Emulation typically imposes a significant performance penalty, however.

Operating systems, drivers, and applications must be specifically compiled for the ARM instruction set to run on ARM-based devices. Apple's macOS and iOS are optimized for ARM-based chips, and Android apps are built primarily for ARM. Emulation, such as in Windows on ARM or Apple's Rosetta 2, allows x86 software to run on ARM, but typically with a performance penalty, although Apple has reduced this significantly. ARM's power efficiency and increasing performance, particularly demonstrated by Apple's M1 and M2 chips, have made it a strong competitor to x86/x64 architectures in both mobile and high-performance computing.

Physical Considerations for ARM-based SoCs

Integrating ARM-based SoCs into devices like mobile phones, tablets, or fanless laptops leverages their compact size and thermal efficiency. Unlike traditional CPUs, ARM SoCs are typically soldered directly onto the motherboard, saving space and enhancing durability. This design reduces the device's thickness and weight, making it ideal for portable or slim devices.

In fanless devices, ARM's low power consumption and efficient heat management allow for passive cooling solutions, such as heat sinks, instead of fans. This contributes to silent operation and longer battery life. Additionally, ARM SoCs integrate multiple functions, like GPU, networking, and storage controllers, reducing the number of components needed on the motherboard, which simplifies design and lowers production costs.

CPU Features

The speed at which a CPU runs (clock speed) is an important performance indicator when comparing processors with the same architecture but is less reliable for different architectures. Performance is also constrained by thermal and power limits, preventing CPUs from running indefinitely faster. Efficiency can be improved by optimizing the instruction pipeline to maximize work per clock cycle. Techniques like Simultaneous [multithreading](#) (SMT), known as HyperThreading by Intel, allows multiple instruction streams (threads) from software applications to be processed concurrently, reducing CPU idle time and enhancing performance in multithreaded applications. For example, Intel's Hyper-Threading Technology and AMD's Simultaneous Multithreading (SMT) allow each physical core to act like two virtual cores, enabling better performance in applications that can use multiple threads, such as video editing, gaming, or running virtual machines.

Another approach is SMP. Symmetric Multiprocessing (SMP) uses two or more physical CPUs in a system. An SMP-aware operating system can distribute tasks across available CPUs, regardless of whether applications are multithreaded. SMP is more common in servers and high-end workstations due to the cost of [multisocket](#) motherboards and CPUs in each socket must support SMP and be identical model and specifications.

Chip-level multiprocessing (CMP), or [multicore](#) CPUs, became possible with advancements in fabrication techniques. A multicore CPU places multiple processing units (cores) on a single chip, enabling better performance without the complexity of multisocket configurations. Each core has its own execution unit and cache, often with access to shared caches. The market has progressed beyond dual-core CPUs to models with eight or more cores, using the nC/nT notation to designate multicore and multithreading features. For example, an 8C/16T CPU has eight cores and can process 16 threads simultaneously, thanks to multithreading capabilities.

Finally, virtualization allows a single machine to run multiple operating systems (virtual machines or VMs) simultaneously. When building or specifying a machine for virtualization, look for CPUs with hardware-assisted virtualization technologies, or [virtualization support](#), such as Intel VT and AMD-V, which improve virtualization performance.

Additionally, second-generation virtualization features such as Second Level Address Translation (SLAT)—known as Extended Page Table (EPT) by Intel and Rapid Virtualization Indexing (RVI) by AMD—is critical for efficient virtual memory management, enabling VMs to run more smoothly. High core counts, multithreading (e.g., Intel Hyper-Threading or AMD SMT), and support for IOMMU (Input-Output Memory Management Unit) are also important for handling multiple VMs and resource-intensive virtualization tasks.

CPU Socket Types

CPU packaging refers to the form factor and connection method between the CPU and motherboard. Intel and AMD each use a different [pin grid array](#) and socket types, meaning that

AMD CPUs cannot be installed in Intel motherboards and vice versa. All CPU sockets feature a Zero Insertion Force (ZIF) mechanism, which allows CPUs to be installed without applying pressure, reducing the risk of damaging the pins.



CPU are vulnerable to electrostatic discharge (ESD). Always take anti-ESD precautions when handling and storing these devices.

Intel predominantly uses Land Grid Array (LGA) sockets, where the pins are located on the motherboard socket, and the CPU has contact pads. Popular Intel socket types include:

- LGA 1200: Used for the 10th and 11th generation Core processors, offering compatibility with Intel's Comet Lake and Rocket Lake CPUs.
- LGA 1700: Designed for the 12th generation Alder Lake CPUs, supporting Intel's latest architecture improvements.

Intel CPUs often feature Turbo Boost technology, which dynamically increases the processor's clock speed to enhance performance during demanding tasks.

GIGA-BYTE Z590 Gaming motherboard with IntelSocket 1200 LGA form factor CPU socket. Note that the socket is covered by a protective dust cap

Image used with permission from Gigabyte Technology.



When installing or removing a CPU, care must be taken to orient pin 1 on the CPU correctly with pin 1 on the socket to avoid bending or breaking any pins. When removing a CPU attached to a heat sink, gently twist the heat sink to avoid pulling the CPU from the socket. Release the latch securing the CPU before attempting to remove it. If reinstalling the same heat sink, clean old thermal paste and apply new thermal paste sparingly (such as in an "X" pattern) to ensure proper heat transfer. Do not apply too much—if it overruns, the excess could damage the socket.

AMD Socket Types and Features

AMD traditionally uses Pin Grid Array (PGA) sockets, where the pins are located on the CPU itself and fit into the motherboard socket. Key AMD socket types include:

- AM4: Widely used for AMD's Ryzen processors, providing compatibility across multiple generations.
- TR4: Designed for Threadripper CPUs, catering to high-performance desktop applications.
- SP3: Used for AMD's EPYC server processors, which utilize LGA sockets for enhanced durability and performance.

GIGA-BYTE X570S Gaming X motherboard with AMD Socket AM4 PGA form factor CPU socket



Image used with permission from Gigabyte Technology.

CPU Types and Motherboard Compatibility

The CPU market experiences rapid turnover, with vendors like Intel and AMD regularly releasing new models. Each new generation typically introduces architectural improvements and often a new socket design. Motherboards are designed specifically for either Intel or AMD CPUs, and compatibility is generally limited to CPUs from the same generation, requiring both the physical socket and the chipset to support the CPU.

Motherboard chipsets play a critical role in compatibility, as they determine which features (e.g., overclocking, PCIe lanes, or memory support) are available. For example, high-end chipsets like Intel's Z-series or AMD's X-series offer more advanced features compared to budget chipsets. Additionally, form factors such as ATX, microATX, and Mini-ITX impact the size of the motherboard and the number of components (e.g., RAM slots, PCIe slots) it can accommodate. For example, ATX boards typically offer more RAM slots and PCIe slots compared to smaller microATX or Mini-ITX boards, which are better suited for compact builds.

When installing a CPU and motherboard, follow these steps:

1. **Socket Alignment:** Ensure the CPU matches the motherboard socket type (e.g., LGA for Intel or AM4/AM5 for AMD). Align the CPU with the socket using the notches or triangle markers to avoid damaging the pins.
2. **Securing the CPU:** Gently place the CPU into the socket and secure it using the retention mechanism. Avoid applying excessive force.
3. **Thermal Paste Application:** Apply a small, pea-sized amount of thermal paste to the center of the CPU before attaching the cooler. This ensures proper heat transfer between the CPU and the cooler.
4. **Attach the Cooler:** Secure the CPU cooler to the motherboard, ensuring it is properly aligned and connected to the CPU fan header.
5. **Install the Motherboard:** Place the motherboard into the case, aligning it with the standoffs and securing it with screws.

Upgrading a CPU on the same motherboard is often limited, as new CPUs may require new sockets or chipsets. Even when upgrades are possible, they rarely offer significant performance improvements without replacing other components.

Both Intel and AMD release multiple CPU models within each generation, targeting different market segments such as desktop, server, and mobile processors.

Core Configurations and Performance Impacts

CPU performance is heavily influenced by its core configuration, which determines how efficiently it can handle tasks:

- **Single-Core vs. Multi-Core Processing:** Single-core CPUs process one task at a time, making them less efficient for multitasking. Multi-core CPUs can handle multiple tasks simultaneously, improving performance for modern applications. For example, a quad-core CPU can process four tasks at once, making it ideal for multitasking or running resource-intensive applications.
- **Hyper-Threading/Simultaneous Multithreading (SMT):** Technologies like Intel's Hyper-Threading and AMD's SMT allow each physical core to handle two threads, effectively doubling the number of tasks a CPU can manage at once. This is particularly beneficial for applications like video editing, virtualization, and 3D rendering.

Practical Scenarios: Core Configurations in Action

- **Gaming:** Most games rely on high single-core performance, as they are optimized to use fewer cores. A CPU with fewer, faster cores (e.g., Intel Core i5 or AMD Ryzen 5) is often sufficient for gaming.

- **Virtualization:** Virtualization benefits from CPUs with higher core counts and multithreading support, as running multiple virtual machines requires significant processing power. CPUs like AMD Ryzen 9, Threadripper, or Intel Core i9 are better suited for these tasks.
- **Workstations:** Tasks like video editing, 3D rendering, and software development require both high core counts and multithreading. Workstation-grade CPUs like AMD Threadripper or Intel Xeon are designed for these workloads.

Desktops

The term *desktop* refers to a basic PC used at home or in the office. Originally, computer cases sat horizontally on desks, but today most desktops come in tower or all-in-one configurations. The desktop segment includes a broad range of performance levels, from budget PCs to high-end gaming systems, reflected in both Intel and AMD CPU lineups.

Intel offers Core i3/i5/i7/i9 processors, with i3 being entry-level and i9 catering to enthusiasts and professionals. AMD offers Ryzen 3/5/7/9, ranging from budget to high-performance, and the high-end Threadripper series for workstation-grade performance. Intel also markets Pentium and Celeron CPUs as low-cost options for entry-level PCs.

Socket Types:

- **Intel:** Transitioned from older sockets like LGA 1151 and LGA 1200 to the current LGA 1700 socket, used for its 12th-gen (Alder Lake) and 13th-gen (Raptor Lake) processors, supporting DDR5 and PCIe 5.0.
- **AMD:** Used the AM4 socket for several Ryzen generations but has now shifted to AM5 for the Ryzen 7000 series, introducing support for DDR5 memory and PCIe 5.0. Most AMD CPUs historically used the PGA form factor (pins on the CPU), but newer platforms like AM5 are transitioning to LGA (pins on the motherboard), similar to Intel's design.

Workstations

The term *workstation* can refer to any business PC or network client. However, in PC sales, it typically means a high-performance PC used for tasks like software development or graphics/video editing. Workstation-class PCs often use components similar to those in server-class computers.

Servers

Server-class computers handle demanding workloads and require high reliability. These systems are designed with [multisocket](#) motherboards, allowing the installation of multiple CPU packages, each with multiple cores and support for multithreading, providing the necessary processing power for heavy workloads.

Key features of server-class motherboards include support for large amounts of ECC RAM (hundreds of gigabytes or more) and expanded cache memory. Intel Xeon and AMD EPYC CPUs, built for scalability and high performance, are typically paired with dedicated server-grade motherboards.

Recent Intel Xeon processors use sockets like LGA 4189 (for Xeon Scalable processors) and LGA 3647 (for older Xeon Scalable models), while older sockets like LGA 1150 and LGA 1151 are no longer used for modern Xeon CPUs. AMD EPYC processors use the Socket SP3 form factor, with newer models utilizing Socket SP5, introduced for AMD's Genoa and Bergamo series, supporting greater scalability, core counts, and memory capacity.

Mobiles

Mobile devices like smartphones, tablets, and laptops prioritize power efficiency, thermal management, and portability over raw performance. Many smartphones and tablets use ARM-

based CPUs for their superior energy efficiency. Both Intel and AMD have separate mobile CPU models within each generation of their platforms. Unlike desktops, mobile CPUs often use different form factors and are frequently soldered to the motherboard, making them non-replaceable or upgradeable.

Module 4

Troubleshooting PC Hardware

Module Overview

You have recently been hired as an IT support specialist for a large corporation. The company has been experiencing a range of hardware-related issues that are affecting employee productivity. Your task is to diagnose and resolve these issues, ensuring that all desktop, laptop, and client devices are functioning optimally. The problems include system firmware settings, power and disk issues, and system and display problems. Your goal is to systematically troubleshoot and fix these issues. Each lesson will have more specific tasks within this scenario that could be solved with the information found within that lesson.

Module Summary

Prepare for A+ Core 1 by:

- Applying troubleshooting methodology
- Configuring BIOS/UEFI
- Troubleshooting power and disk issues
- Troubleshooting system and display issues

Lesson 4A

BIOS and UEFI

Lesson Overview

As part of your role in diagnosing and resolving hardware issues, you have encountered several employees who have reported issues with booting their computers and accessing system settings after a recent upgrade to UEFI-based systems. Your task is to troubleshoot and resolve these BIOS/UEFI-related issues to ensure smooth operation.



Objectives Covered

3.5 Given a scenario, install and configure motherboards, CPUs, and add-on cards.

Learning Outcomes

As you study this lesson, answer the following questions:

- How can you access the UEFI (unified extensible firmware interface) setup program if you miss the key prompt during the boot process?
- What should you check if a computer is not booting from the correct device?
- How can you adjust the cooling settings in the system setup program?
- What is the purpose of Secure Boot in UEFI?
- What is the role of a Trusted Platform Module (TPM) in a computer system?

BIOS and UEFI

Firmware is special program code stored in flash memory, closely tied to the basic functions of specific hardware. Computer firmware helps initialize components on the motherboard so they can load the main operating system.

For many years, computers used **basic input/output system** (BIOS) firmware. Most motherboards now use **unified extensible firmware interface** (UEFI) instead. UEFI supports 64-bit CPU operation, has a graphical user interface (GUI) with mouse support, offers networking at boot, and provides better boot security. A computer with UEFI can also boot in legacy BIOS mode.

You can configure **system** settings through the firmware setup program, accessed by pressing a key during the boot process, usually when the computer vendor's logo appears. Common keys include **Esc**, **Del**, **F1**, **F2**, **F10**, or **F12**.

Bootup access to system firmware setup



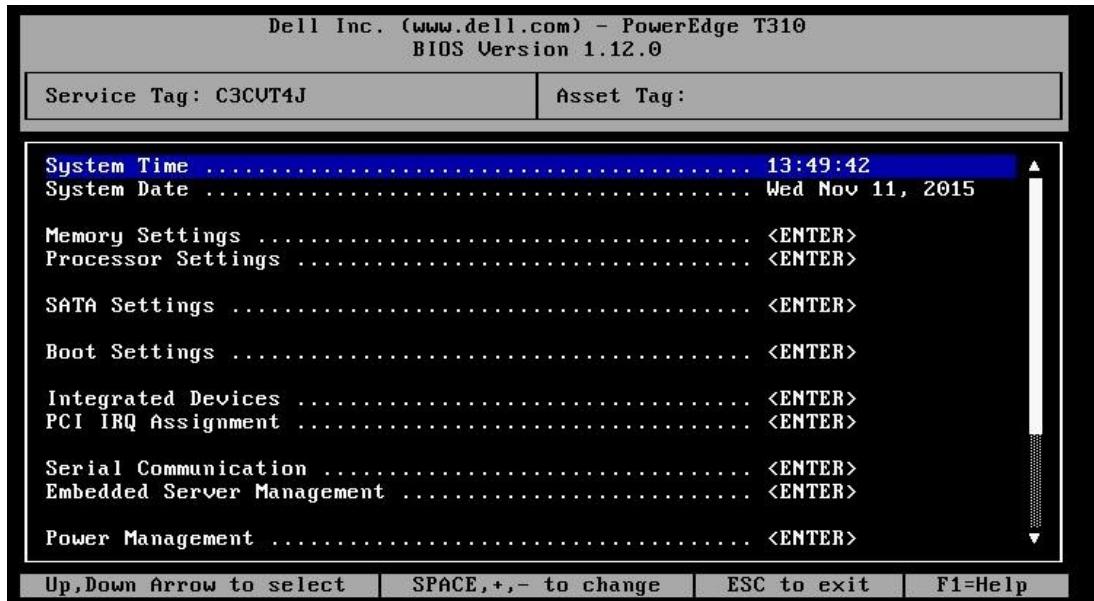
Reproduced with permission of Dell Copyright © Dell 2025 (2025). All Rights Reserved.

The options are as follows: F2: System Setup F10: System Services F11: BIOS Boot Manager F12: PXE Boot

! Modern computers can boot quickly. If you miss the key prompt, you can **Shift-click the Restart button** from the Windows logon screen to access UEFI boot options.

In a legacy BIOS setup program, you navigate using the keyboard arrow keys. Pressing **Esc** generally returns to the previous screen. When closing setup, you can choose to exit and discard changes or exit and save changes. Sometimes, this is done with a key (**Esc** versus **F10**, for instance), but more often, there is a prompt. You can also reload default settings if needed.

A BIOS setup program

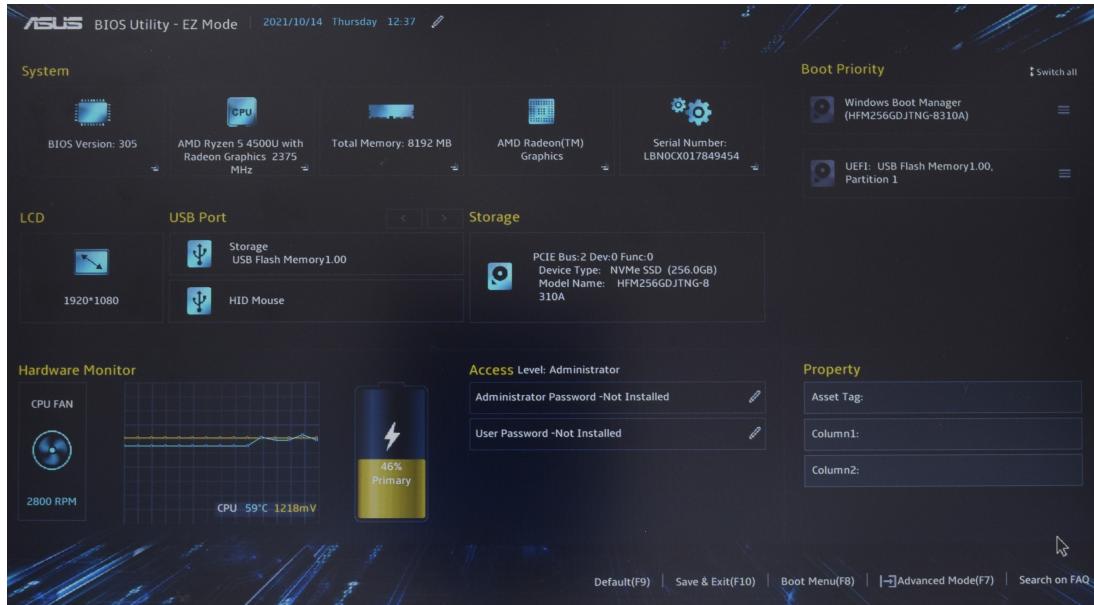


Reproduced with permission of Dell Copyright © Dell 2025 (2025). All Rights Reserved.

At the top, the Service Tag and Asset Tag fields are displayed. The menu includes options for: System Time (highlighted as 13:49:42). System Date (set to Wed Nov 11, 2015). Memory Settings. Processor Settings. SATA Settings. Boot Settings. Integrated Devices. PCI IRQ Assignment. Serial Communication. Embedded Server Management. Power Management. Instructions at the bottom specify navigation controls: up and down arrow to select, space, plus, minus to change, escape to exit, and F 1 equals help.

UEFI setup programs use a graphical interface and have mouse support, though some advanced menus may still require keyboard navigation.

A UEFI setup program

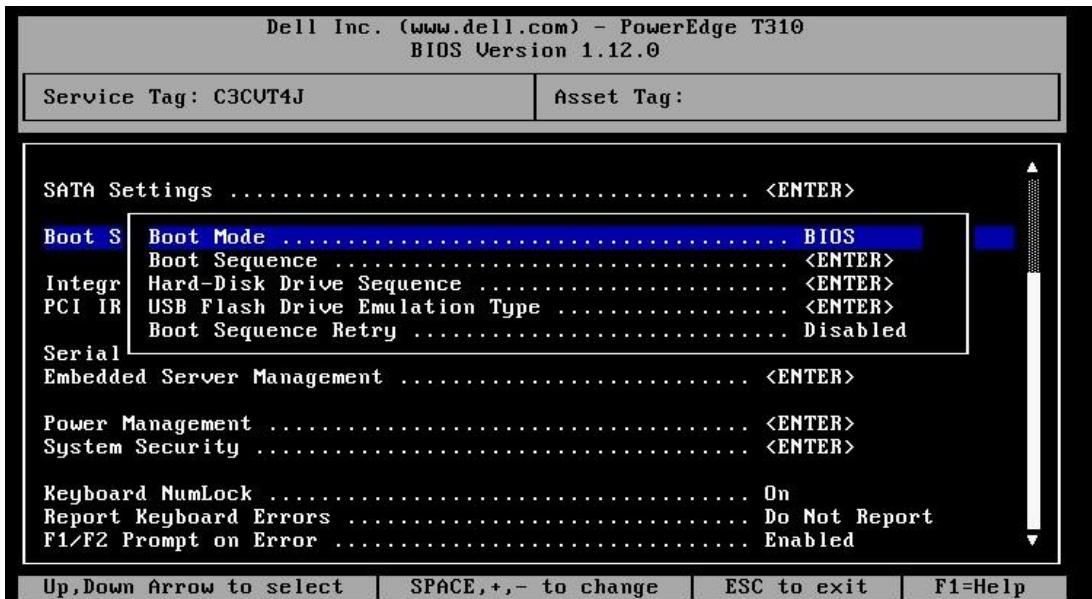


Screenshot used with permission from ASUSTek Computer Inc.

Boot and Device Options

One key system setup parameter is the boot option sequence or boot device priority, which determines the order in which the system firmware searches devices for a boot manager.

Boot parameters



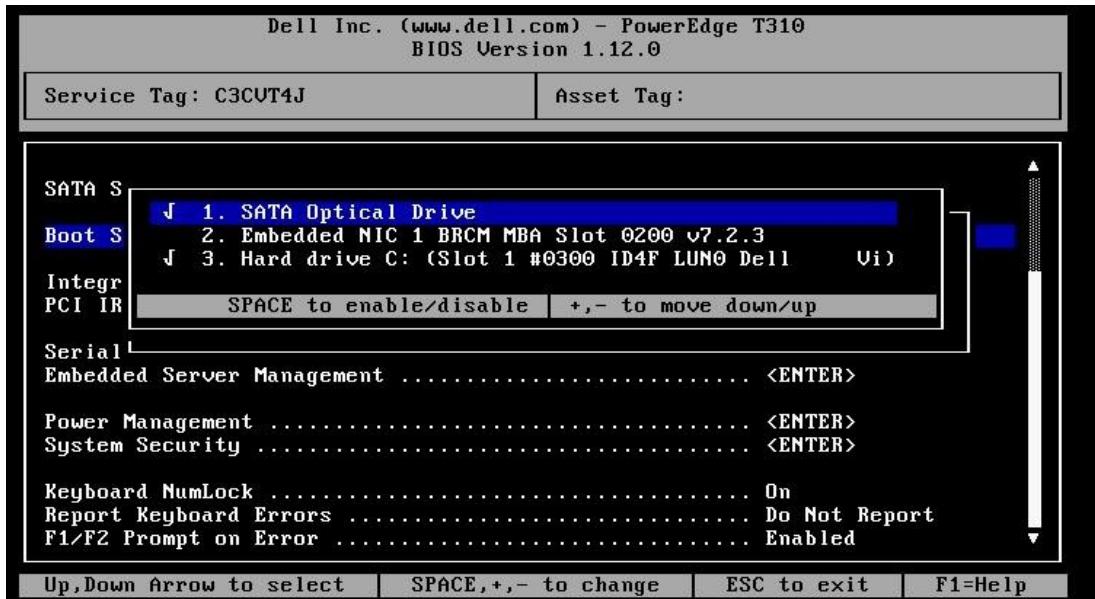
Reproduced with permission of Dell Copyright © Dell 2025 (2025). All Rights Reserved.

At the top, the Service Tag and Asset Tag fields are displayed. Boot settings is highlighted. Boot mode is set to BIOS. Other options include boot sequence, hard-disk drive sequence, U S B flash drive emulation type, and boot sequence retry (disabled). Menu options include SATA settings, integrated devices, PCI IRQ Assignment, Serial Communication, Embedded Server Management, Power Management, and system security. Keyboard settings include Num Lock: On. Report keyboard errors: Do not report. F 1 slash F 2 prompt on error: enabled. Instructions at the bottom specify navigation controls: up and down arrow to select, space, plus, minus to change, escape to exit, and F 1 equals help.

Typical choices include:

- **Fixed disk (Hard Disk Drive or Solid State Drive):** For drives connected via Serial Advanced Technology Attachment (SATA), it's recommended to connect the boot disk to the lowest-numbered port. In modern systems, SSDs using NVMe (Non-Volatile Memory Express) via the M.2 or PCIe (Peripheral Component Interconnect Express) interface are often used as boot drives, offering faster speeds than SATA SSDs.
- **Optical drive (CD/DVD/Blu-ray):** If performing a repair or installation from optical media, you may need to set the optical drive as the highest priority.
- **Universal Serial Bus:** Most modern systems can boot from a USB drive formatted as a boot device. USB booting is commonly used for operating system (OS) installations and recovery utilities.
- **Network/PXE (Preboot Execution Environment):** Boots via the network adapter by retrieving boot instructions from a configured server.

Boot order configuration



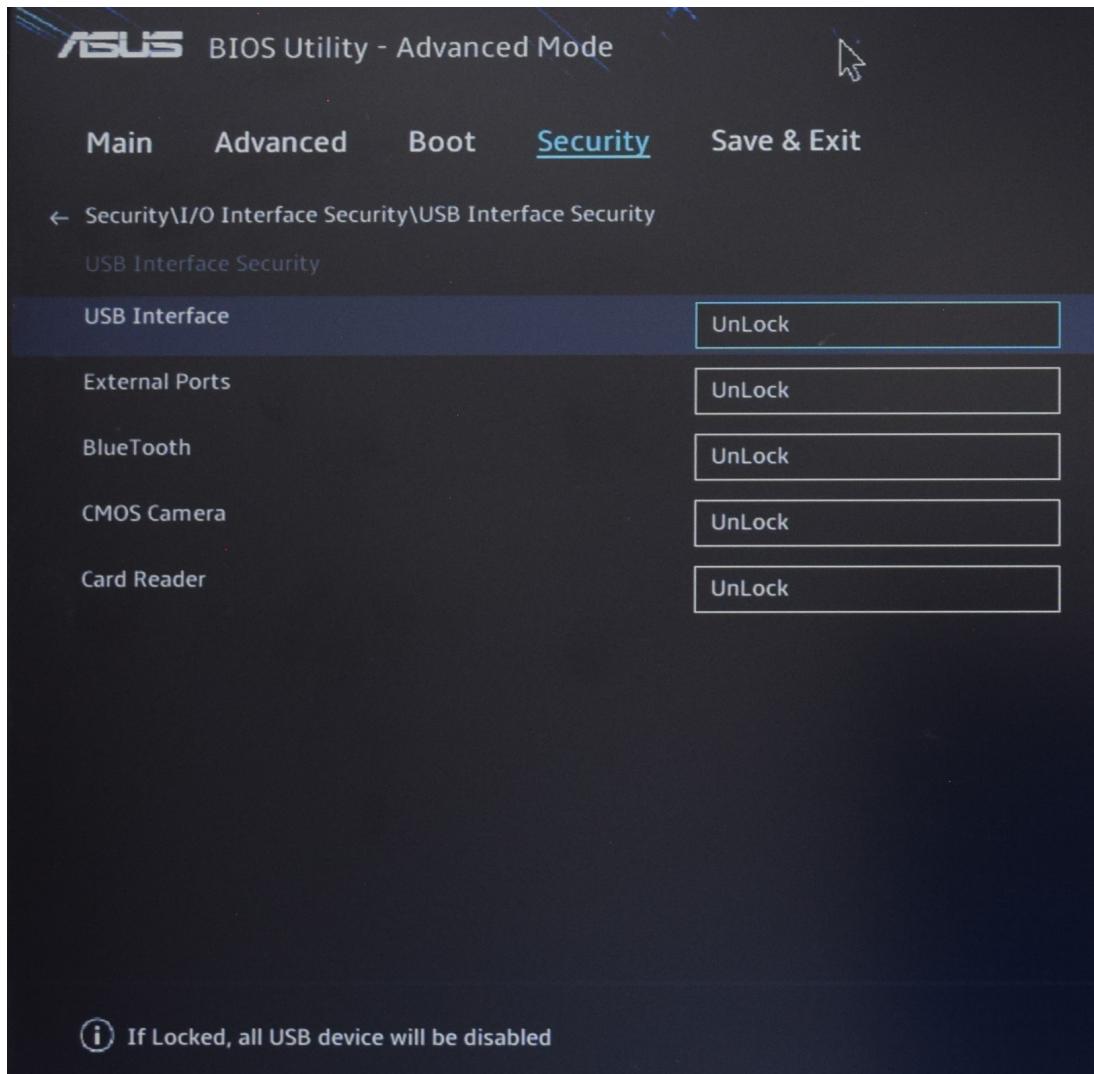
Reproduced with permission of Dell Copyright © Dell 2025 (2025). All Rights Reserved.

At the top, the Service Tag and Asset Tag fields are displayed. Boot settings is highlighted. Boot settings are as follows: SATA optical drive (Highlighted as the first priority). Embedded N I C 1 B R C M M B A Slot 0200 v 7.2.3 listed as the second priority. Hard Drive C (Slot 1, hash 0300 I D 4 F LUN0 Dell) listed as the third priority. Menu options include SATA settings, integrated devices, PCI IRQ Assignment, Serial Communication, Embedded Server Management, Power Management, and system security. Keyboard settings include Num Lock: On. Report keyboard errors: Do not report. F 1 slash F 2 prompt on error: enabled. Instructions at the bottom specify navigation controls: up and down arrow to select, space, plus, minus to change, escape to exit, and F 1 equals help.

USB Permissions

System firmware allows you to enable or disable controllers and adapters, including USB ports. Since USB connections can pose security risks, the firmware setup program may let you control USB permission by enabling or disabling individual or all USB ports.

Using UEFI setup to configure permissions for USB and other external interfaces



Screenshot used with permission from ASUSTek Computer Inc.

The navigation menu at the top includes tabs for Main, Advanced, Boot, Security, and Save and Exit. Options listed for security are as follows: U S B Interface: Unlock. External Ports: Unlock. Bluetooth: Unlock. C M O S Camera: Unlock. Card Reader: Unlock. A note at the bottom reads, If Locked, all U S B devices will be disabled.

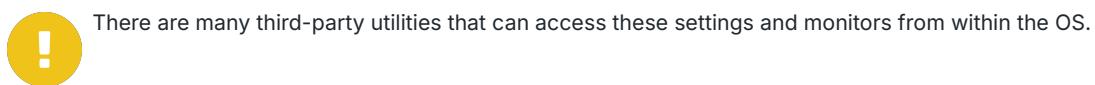
Fan Considerations

Proper maintenance and configuration of cooling fans are crucial for optimal system performance and longevity. Regularly clean fans to prevent dust accumulation, which can obstruct airflow and lead to overheating, potentially damaging components. Ensure that airflow is balanced, with an equal amount of air entering and exiting the system. Position fans to facilitate effective airflow based on thermodynamics, avoiding configurations that push hot air downward.

Most cooling fans can be controlled through system settings, typically found under menus like Cooling, Power, or Advanced. Options usually include:

- **Balanced:** A standard setting for general use.
- **Cool:** Runs fans at higher speeds for maximum cooling.
- **Quiet:** Reduces fan speed, allowing for higher temperatures.
- **Fanless:** Disables fans, relying on passive cooling.
- **Custom:** Allows for personalized fan speed settings.

You can also set the minimum temperature at which fans start to cool the system. Duty cycle settings control the frequency of power pulses to the fan; a higher percentage results in faster fan operation. The setup program will display the current temperature from probes near each fan connector.



There are many third-party utilities that can access these settings and monitors from within the OS.

Temperature Monitoring

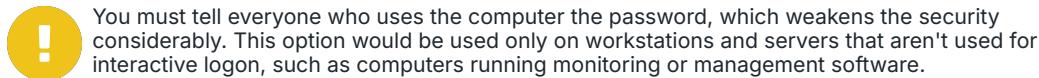
There are two ways to monitor a computer's temperature: manually or through a third-party application.

- **Manual Monitoring:** Restart your computer and enter the BIOS/UEFI settings by pressing a specific key during boot, usually F2, Delete, F12, or ESC. In the UEFI menu, look for an entry related to monitoring or sensors to view real-time readings, including CPU temperature.
- **Third-Party Applications:** These applications monitor computer temperatures through sensors that collect data. Many sensors have preset thresholds that trigger alerts when temperatures exceed safe limits.

Boot Passwords and Secure Boot

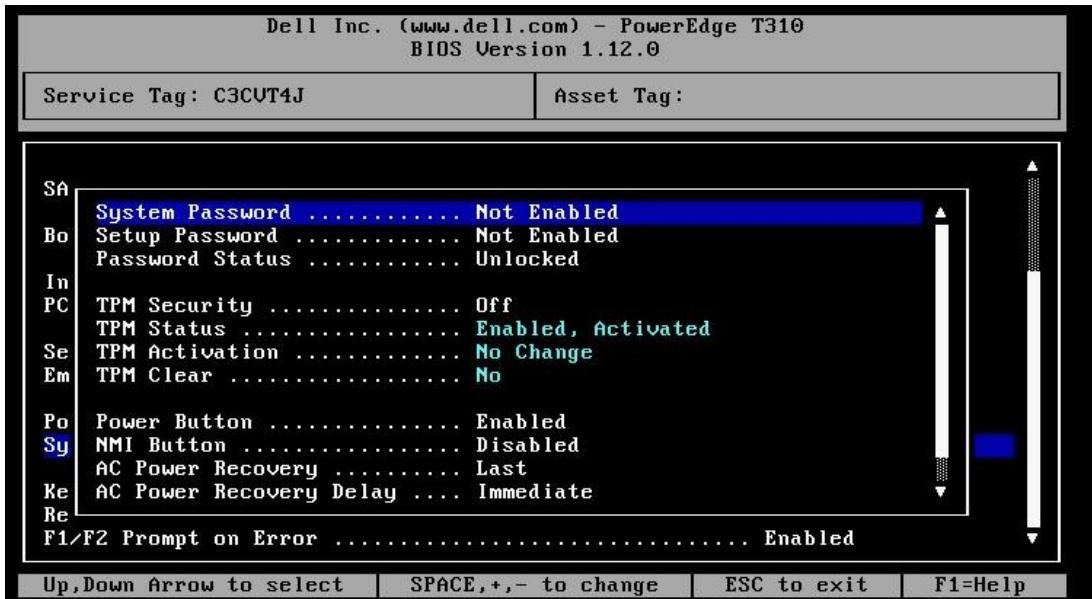
A boot password requires user authentication before the operating system loads. Different systems support various authentication methods, with typically two main passwords available:

- **Supervisor/Administrator/Setup/BIOS Password:** Restricts access to the system's BIOS/UEFI setup program.
- **User/System Password:** Locks the entire system until authentication is provided, preventing any actions until the firmware initializes the system.



You must tell everyone who uses the computer the password, which weakens the security considerably. This option would be used only on workstations and servers that aren't used for interactive logon, such as computers running monitoring or management software.

Configuring system security



Reproduced with permission of Dell Copyright © Dell 2025 (2025). All Rights Reserved.

At the top, the Service Tag and Asset Tag fields are displayed. The list below is as follows: System Password: Not Enabled. Setup Password: Not Enabled. Password Status: Unlocked. T P M Settings are as follows: T P M Security: Off. T P M Status: Enabled, Activated. T P M Activation: No Change. T P M Clear: No. Power Button: Enabled. N M I Button: Disabled. A C Power Recovery: Last. A C Power Recovery Delay: Immediate. Instructions at the bottom specify navigation controls: up and down arrow to select, space, plus, minus to change, escape to exit, and F 1 equals help.

Secure boot is a UEFI feature that protects against malware by ensuring only trusted, digitally signed bootloaders are used. The system firmware checks the operating system's bootloader against pre-loaded cryptographic keys to verify its integrity. If the bootloader is modified or unsigned, it will not be allowed to run. Many modern systems require UEFI (Unified Extensible Firmware Interface) with Secure Boot enabled for security and compatibility with newer operating systems.

! Keys from vendors like Microsoft (Windows and Windows Server) and Linux distributions (Fedora, openSUSE, and Ubuntu) are pre-loaded. You can add or remove keys for other bootloaders through the system setup software. Secure boot can also be disabled if needed.

Trusted Platform Modules

Encryption products secure data by scrambling it in such a way that it can only be decrypted using the correct decryption key. This security relies heavily on protecting the decryption key. UEFI-based systems provide secure storage for these keys, often using hardware-based solutions like the Trusted Platform Module (TPM).

! Encryption encodes data using a key to ensure confidentiality. Many cryptographic processes also use hashing. Hashing generates a unique code (hash) from data, allowing verification of data integrity without revealing the original data. Hashes are used to compare data, but unlike encryption, the original data cannot be recovered from the hash.

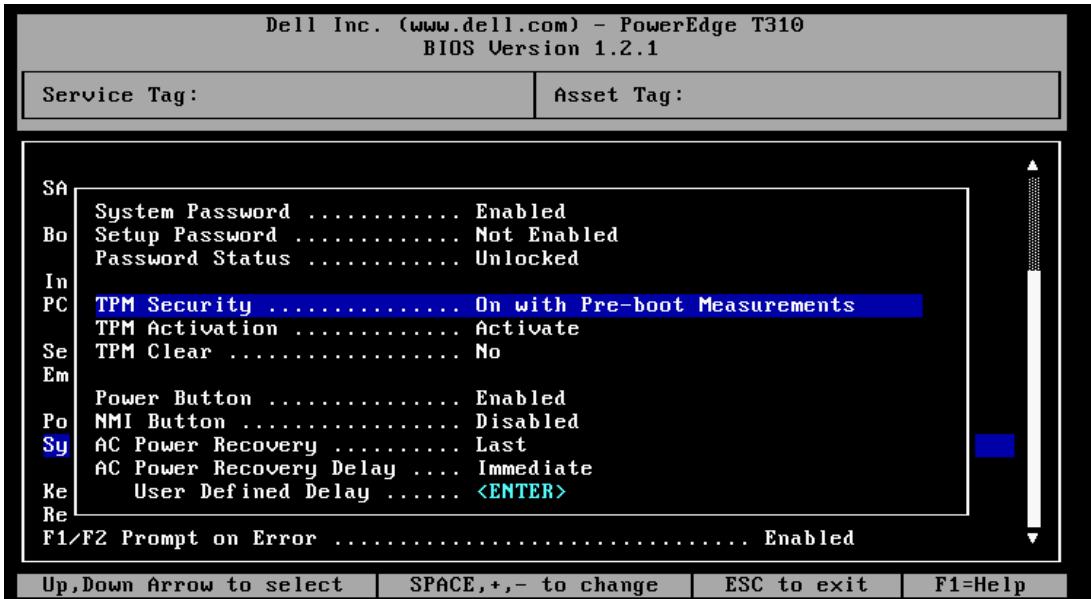
Trusted Platform Module

A [trusted platform module](#) (TPM) is hardware that securely stores digital certificates, cryptographic keys, and hashed passwords. Each TPM chip has a unique, unchangeable endorsement key, establishing a root of trust. During boot, the TPM compares hashes of key system data (such as firmware, boot loader, and OS kernel) to ensure they haven't been tampered with.

The TPM provides superior security by storing cryptographic keys in tamper-resistant hardware, isolating them from the OS and applications, which are more vulnerable to malware and unauthorized access. Its integration with firmware and the OS ensures secure boot processes and key protection, preventing extraction or compromise, unlike keys stored in ordinary apps or files.

The TPM's secure storage area can be used by disk encryption programs like Windows BitLocker to store their keys. TPMs can be enabled, disabled, or reset via the system setup program (BIOS/UEFI) and managed from the operating system.

Configuring a TPM



Reproduced with permission of Dell Copyright © Dell 2025 (2025). All Rights Reserved.

The settings are as follows: System Password: Enabled. Setup Password: Not Enabled. Password Status: Unlocked. T P M Settings are as follows: T P M Security: On with Pre-boot Measurements. T P M Activation: Activate. T P M Clear: No. Power Button: Enabled. N M I Button: Disabled. A C Power Recovery: Last.

Hardware Security Module

A removable USB thumb drive can be used to store cryptographic keys. This is useful if the computer does not support TPM, as a recovery mechanism if the TPM is damaged, or if a disk needs to be moved to another computer. A secure USB key or thumb drive used to store cryptographic material is referred to as a [hardware security module](#) (HSM). "Secure" means that the user must authenticate with a password, personal identification number (PIN), or fingerprint to access the keys stored on the module.

Lesson 4B

Power and Disk Issues

Lesson Overview

Continuing your role in diagnosing and resolving hardware issues, you now face reports from employees that their computers are either not starting at all, experiencing sudden shutdowns, or failing to detect bootable drives. Your task is to troubleshoot these power and disk-related issues to restore normal functionality.



Objectives Covered

- 5.1 Given a scenario, troubleshoot motherboards, RAM, CPU, and power
- 5.2 Given a scenario, troubleshoot drive and RAID issues

Learning Outcomes

As you study this lesson, answer the following questions:

- What steps would you take to diagnose a computer that won't start due to a power issue?
- What should you do if the computer powers on but does not start, showing a black screen with no beeps?
- What should you check if a fixed disk is not detected during boot?
- What are the two ways of formatting boot information, and how do they differ?
- What should you do if a Windows system displays a blue screen of death (BSOD)?
- What are common symptoms of a failing hard disk drive (HDD)?

Troubleshoot Power Issues

Computer components need a constant, stable supply of power to run. If the computer won't start, it is likely due to a power problem. If the PC suddenly turns off or restarts, power issues are a common cause.

When a computer is switched on, the power supply unit (PSU) converts AC input voltage (VAC) to DC voltage (VDC). DC voltage powers the motherboard components and peripheral devices. The PSU supplies 12V power immediately, causing the fans and hard disks to spin up. It then tests its 5V and 3.3V supplies. Once stable, it sends a power good signal to the processor.

To diagnose **no power** symptoms, check if the LEDs on the front panel are lit and if you can hear the fans. Power issues might arise from a faulty PSU, incoming electricity supply, power cables/connectors, or fuses. To isolate the cause of no power, try the following tests:

1. Check other equipment: Ensure other devices in the area are working to rule out a power circuit fault or a blackout.

2. Test the wall socket: Plug a known-good device, like a lamp, into the wall socket. If it doesn't work, the socket is faulty. Contact an electrician.
3. Verify PSU connections: Ensure the PSU is properly connected to the PC and wall socket, and all switches are in the "on" position.
4. Try another power cable: There may be an issue with the plug or fuse. Check the plug's wiring and fuse resistance with a multimeter or swap with a known good fuse.
5. Disconnect extra devices: Remove devices like a plug-in graphics card. If this solves the problem, the PSU may be underpowered, or one of the devices is faulty.
6. Test the PSU: If safe, use a multimeter or power supply tester to check the PSU.

Technician working with a power supply tester



Image by Konstantin Malkov @123RF.com



You must take appropriate safety measures before testing a live power supply. PC power supplies are NOT user serviceable. Never remove the cover of a power supply.

If you still cannot identify the fault, then the problem is likely to be a faulty motherboard or power supply. If you suspect the power supply, do not leave it on longer than necessary or unattended. Watch for external signs like smoke or fire and turn it off immediately if you notice any unusual sights, smells, or noises.

Troubleshoot POST Issues

Once the CPU has been given the power good signal, the system firmware performs a [power-on self-test](#). The POST is a diagnostic program implemented in the system firmware that checks the hardware components required to boot the computer.

 On modern computers, the POST happens very quickly to improve boot times, so you are unlikely to see any POST messages. The PC is likely to be configured to show a logo screen and will only display messages if there is an error.

If power is present (e.g., you hear the fans spinning) but the computer does not start, shows a **blank screen**, and there are no beeps from the internal speaker, it is likely either a display issue or the POST procedure is not executing. Assuming the display is not the issue, try the following:

1. **Ask what has changed**—If the system firmware has been updated and the PC has not booted since then, the system firmware update may have failed.
Use the reset procedure.
2. **Check cabling and connections**—Especially if maintenance work has just been performed, ensure all cables and adapter cards are correctly seated. An incorrectly oriented storage adapter cable or a poorly seated adapter card can stop POST from running.
Correct any errors, reset adapter cards, and then reboot the PC.
3. **Check for faulty interfaces and devices**—A faulty adapter card or device may halt POST. Remove one device at a time to identify the faulty component, or remove all non-essential devices and add them back one by one.
4. **Check the PSU**—Even if the fans are receiving power, there may be a fault preventing the power good signal from being sent to the CPU, stopping POST.
5. **Check for a faulty CPU or system firmware**—If possible, replace the CPU chip with a known good one or update the system firmware.



Some motherboards have jumpers to configure modes (such as firmware recovery) or processor settings. Incorrect jumper settings can prevent the computer from booting. If the computer does not work after being serviced, check that the jumpers have not been changed.

If POST runs but detects a problem, it generates an error message. If the fault prevents the computer from displaying anything on the screen, the error is often indicated by **beep codes**. Use resources such as the manufacturer's website to determine the meaning of the beep code.

The codes for the original IBM PC are listed in this table.

Code	Meaning
1 short beep	Normal POST -system is OK. Most modern PCs are configured to boot silently, however.
2 short beeps	POST error -error code shown on screen.
No beep	Power supply, motherboard problem, or faulty onboard speaker.
Continuous beep	Problem with system memory modules or memory controller.
Repeating short beeps	Power supply fault or motherboard problem.
1 long, 1 short beep	Motherboard problem.
1 long, 2 or 3 short beeps	Video adapter error.
3 long beeps	Keyboard issue (check that a key is not depressed).



Some PCs will not boot if a key is stuck. Check that nothing is resting on the keyboard. If the board is clogged with dust or sticky liquid, clean it using approved products, such as swabs and compressed air blowers.

Troubleshoot Boot Issues

After completing the POST, the system searches for boot devices in the order specified in the boot sequence. If the first device is not found, it attempts the next one, such as checking for a USB drive or network boot. If no bootable device is found, an error message is displayed, and the process halts.

If the system is booting from the wrong device, verify that removable drives do not have media interfering with the boot process, and ensure the boot order is correct.

If a fixed disk is not detected:

- Power Check: Ensure the drive is powered. Look for an activity LED, listen for the drive spinning up, or verify power connectors are secure.
- Data Connections: Inspect data cables for damage and verify they are properly connected.
- UEFI/BIOS Settings: Confirm the drive is enabled in UEFI/BIOS and that settings like Secure Boot or SATA mode (AHCI, RAID) are correctly configured.
- M.2/NVMe Drives: For modern drives, ensure they are properly seated and detected in UEFI/BIOS.

Troubleshoot Boot Sector Issues

If power and cabling issues are ruled out, suspect a problem with the device's boot sector and files. Corruption can occur due to disk faults, power failures, incorrect installation of multiple operating systems, or malware, preventing the disk from booting.

There are two ways of formatting boot information: MBR and GPT.

- In the legacy master boot record (MBR) scheme, the MBR is located in the first sector of the partition. Partitions divide the disk into multiple logical drives. The MBR holds information about these partitions and contains code that points to the active boot sector. The boot sector is either in the sector right after the MBR or in the first sector of each partition. It describes the partition's file system and contains code that helps boot the operating system. This is typically the Boot Configuration Data (BCD) for Windows or boot managers like GRUB or LILO for Linux. While each primary partition has a boot sector, only one can be marked as active for booting.
- GUID Partition Table (GPT) is not restricted to a single sector and serves to identify partitions and OS boot loaders. It offers more robust and flexible partitioning compared to MBR.

Damage to the MBR or GPT partition records can cause boot errors like "Boot device not found," "OS not found," or "Invalid drive specification." If malware caused the issue, the best solution is to use your antivirus software's boot disk option. This includes a scanner to detect the malware and tools to repair the boot sector.

If a recovery disk is unavailable, use the repair options provided by the OS setup trdisk.

When encountering boot issues, if power and cabling problems are ruled out, the device's boot sector and files may be at fault. Corruption can arise from disk faults, power failures, incorrect installation of multiple operating systems, or malware, preventing the disk from

booting. Additionally, a blank screen during boot can indicate issues with the boot process or display connections.

Boot Information Formatting: MBR and GPT

- Master Boot Record (MBR): In the legacy MBR scheme, the MBR is located in the first sector of the partitioned disk. It holds information about disk partitions and contains code pointing to the active boot sector. The boot sector, located immediately after the MBR or in the first sector of each partition, describes the partition's file system and contains code to boot the operating system. This includes Boot Configuration Data (BCD) for Windows or boot managers like GRUB or LILO for Linux. Only one primary partition can be marked as active for booting.
- GUID Partition Table (GPT): GPT is not limited to a single sector and provides more robust and flexible partitioning compared to MBR. It identifies partitions and OS boot loaders, offering enhanced reliability.

The troubleshooting steps include:

1. Check Display Connections: Ensure that the monitor is properly connected to the computer and powered on. A loose or faulty cable can result in a blank screen.
2. Inspect Boot Errors: Damage to the MBR or GPT partition records can cause boot errors such as "Boot device not found," "OS not found," or "Invalid drive specification."
3. Malware Solutions: If malware is suspected, use your antivirus software's boot disk option, which includes a scanner to detect malware and tools to repair the boot sector.
4. Repair Options: If a recovery disk is unavailable, utilize the repair options provided by the operating system setup disk to address boot sector issues.

Troubleshoot OS Errors and Crash Screens

If a boot device is found, the boot sector code is loaded into memory and takes over from the system firmware, loading the rest of the operating system files. Common symptoms of errors after this point are usually due to software or device driver issues rather than hardware problems.

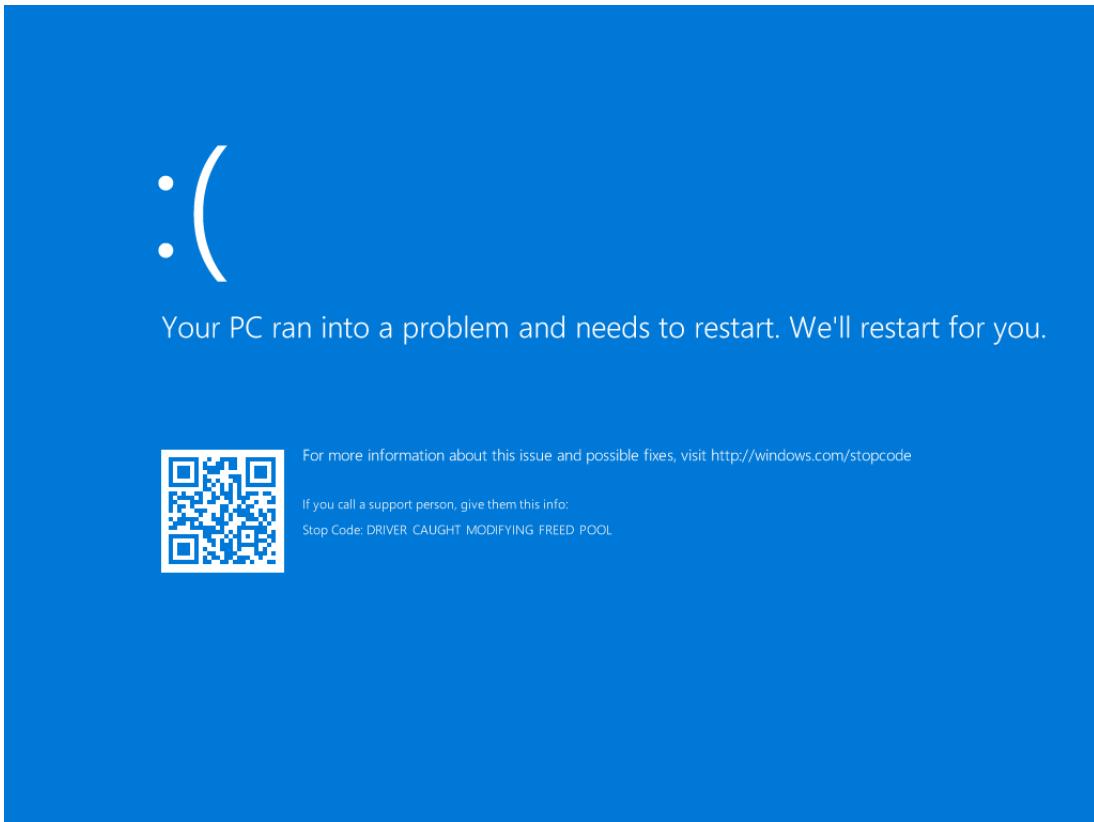
One of the most common symptoms of serious faults in a Windows system is the appearance of the [Blue Screen of Death \(BSOD\)](#). This proprietary crash screen indicates issues such as system memory faults, hardware device or driver problems, or OS file corruption. The BSOD can be caused by:

- Faulty or incompatible device drivers
- Corrupted system files
- Defective hardware components
- Overheating or power supply issues

To troubleshoot a BSOD:

- Use a camera to scan the QR code displayed on the screen for more information.
- The error is logged in the System log with "BugCheck" as the source. Use the first hex value (e.g., 0x0a) from the event description to search for more information online.
- If you have a support contract, a memory dump is generated for further analysis.

Blue screen of death (BSOD) preventing a Windows PC from booting



Screenshot courtesy of Microsoft.



A blue screen is a crash screen specific to Windows. macOS shows a spinning pinwheel (spinning wait cursor) for catastrophic failures. Linux displays a kernel panic or a "Something has gone wrong" message.

Troubleshoot Drive Availability

A hard disk drive (HDD) is more prone to mechanical failure either within the first few months or after several years of use (wear and tear). Solid-state drives (SSDs) are generally more reliable but have a limited lifespan due to the wear on memory cells from repeated writes. Power loss during write operations can cause data corruption or hardware damage for both types of drives.

When a drive is failing, it may exhibit these common symptoms:

- **Unusual noise (HDD):** A healthy HDD emits a low-level noise when accessing data. Loud grinding, clicking, or scraping sounds often indicate mechanical failure.
- **No light-emitting diode (LED) status/activity:** If disk activity lights are off, the system or the drive may not be powered. If the individual drive is faulty, check connections or power supply. For drives in RAID arrays, this could indicate a missing or failed array.
- **Constant LED activity (Disk Thrashing):** Continuous disk activity could indicate insufficient system RAM, causing excessive paging to the disk. It could also be a result of a faulty software process, malware, or a failing disk.

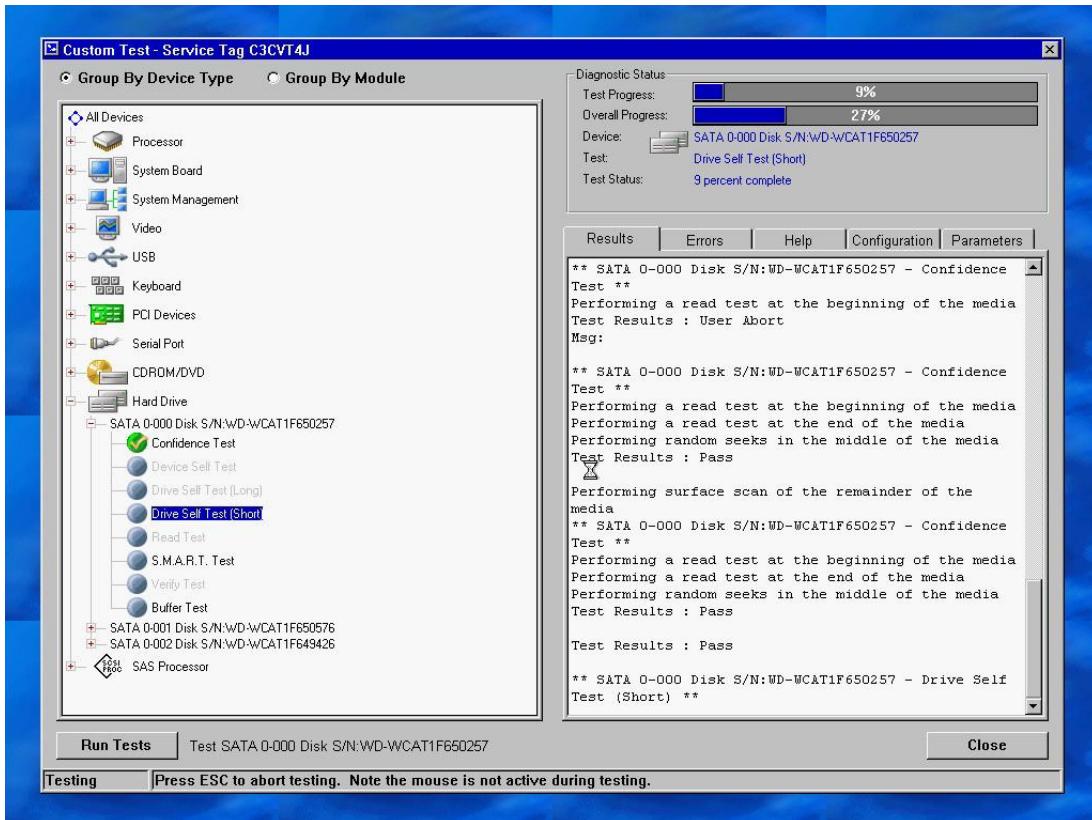
- **Bootable device not found:** If a system fails to boot, it might point to file corruption or a faulty drive. This may also occur if a RAID controller fails to detect one or more drives in the array, leading to the array going "missing."
- **Missing drives in OS:** If the drive doesn't appear in tools like File Explorer or command-line interfaces, check if it has been initialized, partitioned, and formatted. If not detected by tools like Windows Disk Management, suspect hardware or cable/connector faults.
- **Read/Write failure:** Errors like "Cannot read from the source disk" are signs of bad sectors on HDDs or bad blocks on SSDs. Running diagnostic tools like chkdsk can identify if bad sectors or blocks are increasing, indicating imminent failure.
- **Audible alarms:** Many enterprise-level drives and RAID controllers include audible alarms to alert users of drive or array failure. These alarms may indicate hardware issues or missing drives in an array, requiring immediate attention.
- **Blue screen of death (BSOD):** Severe drive issues can cause system crashes, particularly due to file corruption or read/write errors. This could result in a system stop error (BSOD).

If you encounter any of these symptoms, it's important to back up data immediately and replace the drive to prevent data loss.

Troubleshoot Drive Reliability and Performance

In addition to symptoms that you can detect by observing system operation, most fixed disks have a self-diagnostic program called [Self-Monitoring Analysis and Reporting Technology \(S.M.A.R.T.\)](#). S.M.A.R.T can alert the operating system if a **failure** is detected. If you suspect a drive is failing or experience performance issues like **extended read/write times**, run advanced diagnostic tests. Most disk vendors provide utilities for testing drives, and there may also be system diagnostics programs supplied with the computer.

Using system diagnostics software to test a hard drive

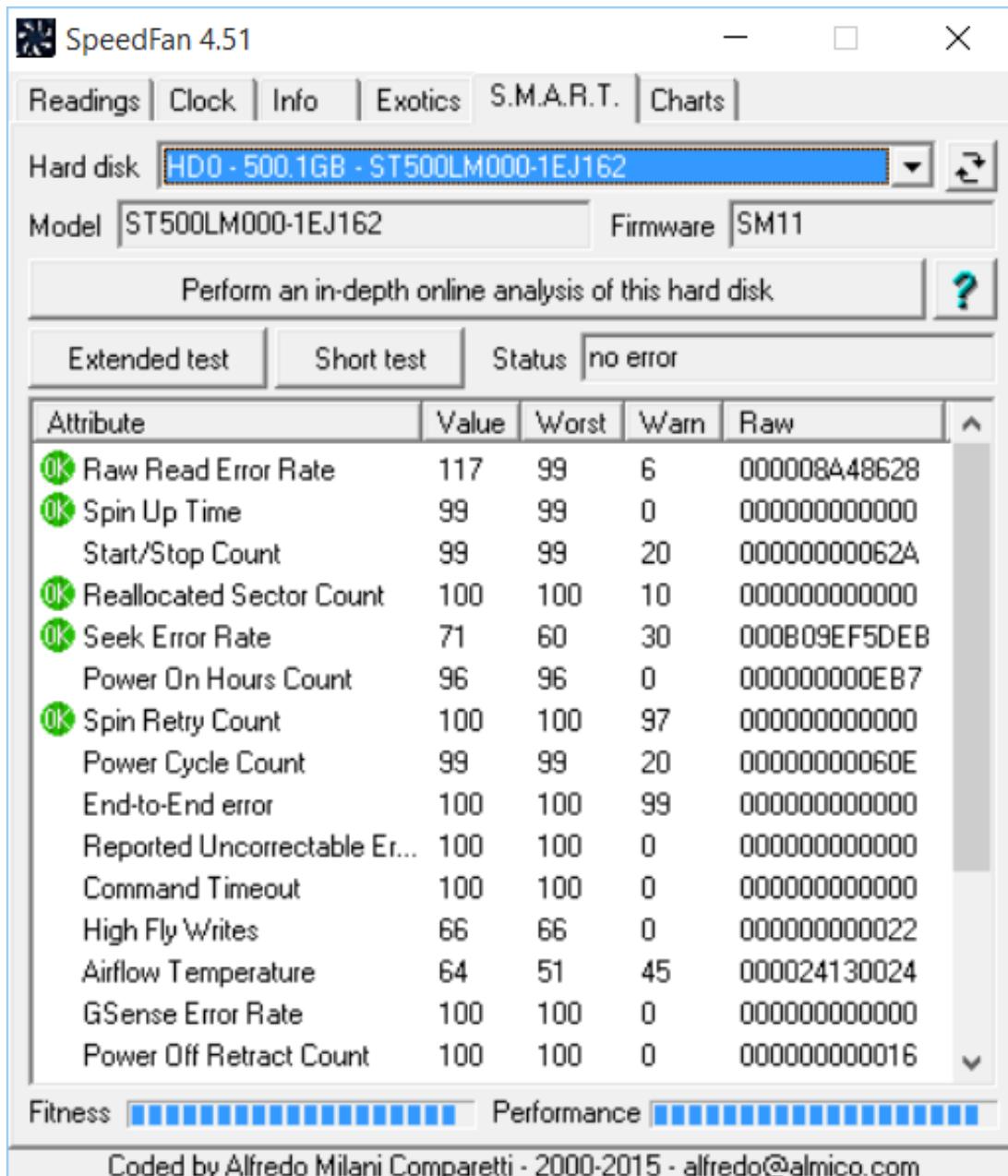


Screenshot courtesy of Microsoft.

The service tag is C 3 C U T 4 J. Drive Self Test (Short) is highlighted under the hard drive section on the left. Diagnostic status shows 9 percent test progress with 27 percent overall progress. Device: SATA 0-000 Disk S slash N W D-W C A T 1 F 650257. Test: drive self test (Short) Test Status: 9 percent complete The panel below has heads Results, Errors, Help, Configuration, and Parameters. Results is selected.

You can also use Windows utilities to query SMART and run manual tests.

Viewing SMART information via the SpeedFan utility



Screenshot courtesy of Microsoft.

The model and firmware are mentioned above. A table below lists the attribute, value, worst, warn, and raw. The fitness and performance is calculated at the bottom.

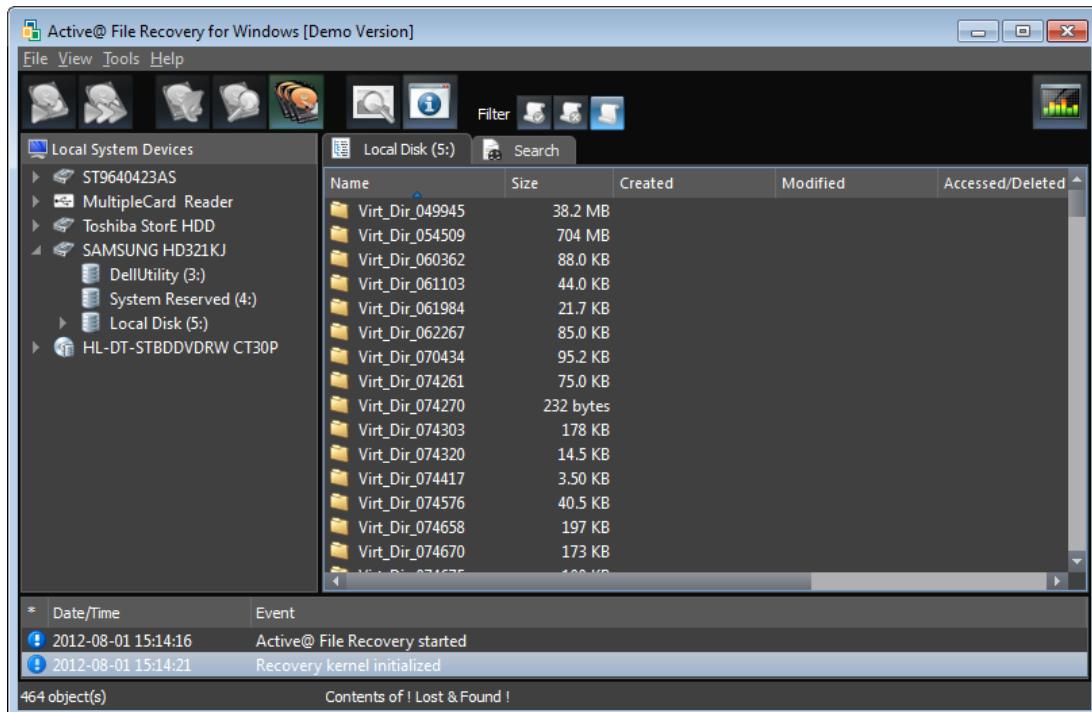
These tests can detect damage to the storage mechanisms and report statistics such as [input/output operations per second](#) (IOPS). If performance metrics are lower than the vendor's baseline measurements, the device is likely faulty. If metrics are similar to the benchmark, slow read/write access may be due to other system performance issues, such as:

- Application load and general system resource issues
- File fragmentation (on HDDs)
- Limited remaining capacity

Extended read/write times can also occur due to failing sectors (HDDs) or blocks (SSDs). **Data loss** or corruption means files stored in these locations cannot be opened or may disappear. When bad sectors or blocks are detected, the disk firmware marks them as unavailable for use.

If there is file corruption on a hard disk and no backup, you can attempt to recover data using a recovery utility.

Using file recovery software to scan a disk



Screenshot courtesy of Microsoft.

A table on the right lists the name, size, created, modified, and accessed or deleted details. Another table at the bottom lists the date, time, and event.

 File recovery from an SSD is not usually possible without highly specialized tools.

Troubleshoot RAID Failure

Redundant Array of Independent Disks (RAID) is configured to protect data against the failure of a single disk. Data is either mirrored to a second drive or recorded with parity information across multiple drives to enable recovery from a device failure. RAID can be implemented using hardware controllers or operating system features. The redundant storage is presented as a volume, which can be partitioned and formatted in the OS as one or more drives. There are two main scenarios for **RAID failure**:

- Device Failure:** If one of the devices in the array fails, the volume will be listed as "degraded," but the data will still be accessible, and it should continue to function as a boot device if configured to do so.



Note: Note: RAID 0 has no redundancy. If one of the disks fails, the volume will stop working. RAID 0 is used in scenarios where speed is prioritized over reliability.

- Array Failure:** Most desktop-level RAID solutions can tolerate the loss of only one disk, so it should be replaced as soon as possible. If the array supports hot swapping, the new disk can be inserted into the computer or disk chassis. The array can then be rebuilt using the RAID configuration utility (for hardware RAID) or an OS utility (for software RAID). The rebuilding process will likely severely affect performance as the controller writes multiple gigabytes of data to the new disk.

RAID errors using the configuration utility. This volume is missing one of its disks

```

LSI Corp Config Utility  For Dell PERC H200  v7.01.09.00 (2010.03.22)
View Volume -- SAS2008
  Volume           1 of 1
  Identifier
  Type            RAID 1
  Size(GB)        232
  Status          Inactive

  Manage Volume

Slot  Device Identifier          RAID   Hot     Drive   Pred   Size
Num   Disk      Spr    Status  Fail   (GB)
  1   ATA       WDC WD2502ABYS-13B05 Yes    No    Inactive  No    232
---                   Yes    No    Missing   ---   ----

Esc = Exit Menu      F1/Shift+1 = Help
Enter=Select Item   Alt+N=Next Volume

```



When hot swapping, ensure you do not remove a healthy disk, as this could cause the array to fail. Disk failure is usually indicated by a red LED. Always back up data beforehand.

Troubleshooting Steps

- Unavailable Volume or "array missing":** If the volume is not available, either more disks have failed than the array can tolerate, or the controller has failed. If the boot volume is affected, the OS will not start. Use the latest backup or file recovery solutions if too many disks have failed.
- Controller Failure:** If the controller fails, data on the volume should be recoverable, though there may be file corruption if a write operation was interrupted. Install a new controller or import the disks into another system.
- Boot Process Issues:** Use the RAID configuration utility to verify the status. If you cannot access the utility, the controller likely failed.

Boot message indicating a problem with the RAID volume. Press Ctrl+C to start the utility and troubleshoot

```
F10 = System Services  
F11 = BIOS Boot Manager  
F12 = PXE Boot  
One 2.40 GHz Quad-core Processor, Bus Speed:4.80 GT/s, L2/L3 Cache:1 MB/8 MB  
System Memory Size: 4.0 GB, System Memory Speed: 1067 MHz  
  
Broadcom NetXtreme II Ethernet Boot Agent v5.0.5  
Copyright (C) 2000-2009 Broadcom Corporation  
All rights reserved.  
Press Ctrl-S to Configure Device (MAC Address - 842B2B19E291)  
  
Dell PERC H200/6Gbps SAS HBA BIOS  
MPT2BIOS-7.01.09.00 (2010.03.22)  
Copyright 2000-2009 LSI Corporation.  
  
Integrated RAID exception detected:  
Volume (Hd1:079) is currently in state INACTIVE/OPTIMAL  
Enter the Dell PERC H200/HBA Configuration Utility to investigate!  
  
Press Ctrl-C to start Dell PERC H200/HBA Configuration Utility..
```

Lesson 4C

System and Display Issues

Lesson Overview

As you continue to address hardware issues within the company, you encounter employees experiencing various display issues, including no video output, incorrect color display, and intermittent shutdowns of projectors during presentations. Your task is to diagnose and resolve these system and display-related issues to ensure optimal performance.



Objectives Covered

- 5.1 Given a scenario, troubleshoot motherboards, RAM, CPU, and power
- 5.3 Given a scenario, troubleshoot video, projector, and display issues

Learning Outcomes

As you study this lesson, answer the following questions:

- What steps should you take to diagnose intermittent system lockups and shutdowns?
- How can you diagnose and correct overheating issues in a computer system?
- What should you check if a computer is experiencing sluggish performance after a new build or upgrade?
- What steps would you take to troubleshoot a monitor that shows no image?
- How can you rule out cable problems when troubleshooting a display issue?
- What steps should you take to troubleshoot intermittent shutdowns in projectors?

Troubleshoot Component Issues

Symptoms like system lockups, **random shutdowns**, continuous rebooting, OS blue screen/Kernel panic errors, and **application crashes** can be challenging to diagnose. These issues are often caused by software problems, disk/file corruption, or malware.

Diagnostic Steps:

1. Eliminate Software Issues: Ensure that software, disk/file corruption, and malware are not the causes.
2. Identify Patterns: Determine if the problem is truly intermittent or follows a pattern. For example, if errors occur after the PC has been running for a while, it could indicate a thermal issue.
3. Check Power Supply: Verify that the power supply is providing stable voltages to the system.

4. Suspect Hardware: If the power supply is not the issue, consider problems with memory, CPU, or the motherboard. Use diagnostic test programs provided by the vendor, which are often run from the firmware setup utility rather than the OS.
5. Observe Physical Symptoms: If no diagnostic utilities are available, look for physical symptoms to identify issues with the motherboard, RAM, or CPU.

Overheating

Excessive heat can easily damage the sensitive circuitry of a computer. If a system feels hot to the touch, check for **overheating** issues. Unusual odors, such as a **burning smell** or smoke, usually indicate overheating, likely from the power supply. Shut down the system immediately and investigate. Dust-clogged vents can also cause burning smells.



CPUs and other components heat up during operation. Handle internal components carefully to avoid burns.

Other techniques for diagnosing and correcting overheating issues include the following:

- **Temperature Sensors:** Most systems have internal temperature sensors accessible via driver or management software. Use vendor documentation to ensure the system operates within acceptable limits.
- **CPU Fan:** Ensure the CPU fan is working properly. Cooling is vital for processor performance and lifespan. Overheating can cause crashes or reboots. Check if the fan's power cable is connected, if the fan is jammed or clogged, or if it is too small. A fan from an older CPU may not be suitable for an upgraded processor.
- **Heat Sink:** Verify that the heat sink is properly fitted and snug against the processor. Clean and replace old thermal paste if necessary to help lower the processor's temperature.
- **Blanking Plates:** Use blanking plates to cover holes in the back or front of the PC case. Uncovered holes can disrupt airflow and reduce cooling effectiveness.
- **Environment:** Ensure the room is not unusually warm or dusty and that the PC is not near a radiator or in direct sunlight.

Thermal problems can also cause loose connectors, components to move in their sockets, or circuit board defects like hairline cracks to widen and break connections. Some faults can be detected by visual inspection.

Physical Damage

Actual Physical damage to a computer system typically affects peripherals, ports, and cables. Damage to other components is more likely if the unit has been in transit. Inspect the unit closely for case damage; even a small crack or dent may indicate a fall or knock that could have caused internal damage.

If a peripheral device is not working, examine the port and cable ends for bent, broken, or dirty pins and connectors. Check the cable length for any damage.

Motherboard issues are rare but possible. Be aware of the following:

- **Electrostatic Discharge (ESD), Electrical Spikes, or Overheating:** These can damage the motherboard's soldered chips and components.
- **Careless Insertion:** Pins on integrated connectors can be damaged by improper insertion of plugs and adapter cards.
- **Dirt and Chip Creep:** Errors may be caused by dirty contacts or chip creep, where an adapter works loose from its socket over time due to temperature changes.

Visible signs of damage include:

- **Liquid Spills:** Look for signs of liquid damage or dust clogging fans or the keyboard.
- **Schorch Marks and Capacitor Swelling:** A "blown" component may leave scorch marks. Swollen or bulging capacitors, which regulate electricity flow, may indicate damage or manufacturing defects.

If the motherboard shows physical damage, diagnostic software is essential to confirm the problem. Testing with "known good" components is often too time-consuming and expensive. Investigate any environmental issues or maintenance procedures that could be the root cause of the error.

Troubleshoot Performance Issues

Performance issues are challenging to diagnose due to their varied causes. Use a structured approach to identify the source of sluggish performance:

1. **Check for overheating**—High temperatures can cause the CPU and other components to throttle performance to avoid damage. Monitor temperature sensors and fan speeds. If they are high, consider cleaning the computer or upgrading the cooling system.
2. **Check for misconfigurations**—If sluggish performance occurs after a new build, upgrade, or maintenance, verify the compatibility of new components with the motherboard. For instance, a memory upgrade might disable dual-channel mode, reducing performance. Always ask, "What has changed?" when diagnosing issues.
3. **Verify the problem**—Performance issues can stem from compute, storage, or networking functions. Use diagnostic tests to compare the CPU, system memory, fixed disk, and network adapter performance against known baselines. Quantifying "sluggish" performance and isolating it to a specific subsystem helps identify the cause. If performance is insufficient, consider upgrading one or more subsystems.



A bottleneck occurs when an underperforming component slows down the entire system. For example, a PC with a fast CPU, dedicated graphics, and ample memory may still be sluggish if it's using an HDD, as SSDs provide much faster performance. While SSDs are now standard, modern bottlenecks can arise from improper NVMe drive configurations, latency issues, or bandwidth limitations, such as PCIe lanes not supporting optimal speeds (e.g., PCIe 3.0 vs. 4.0).

4. **Rule out software/configuration/networking issues**—Users might describe performance as sluggish due to configuration problems. For example, a computer might seem slow due to a faulty network login script, not a hardware issue. Rule out operating system and application issues before assuming hardware problems. Use built-in or third-party diagnostic tools to verify component performance. If diagnostics show no hardware issues, suspect a software or configuration problem.

Troubleshoot Inaccurate System Date/Time

Accurate timekeeping is crucial for computers, as incorrect date and time settings can disrupt network authentication and make scheduled tasks like backups unreliable. The **real-time clock (RTC)** tracks the date and time, powered by a coin-cell lithium battery (usually CR2032) when the computer is off.

RTC coin cell battery on the motherboard

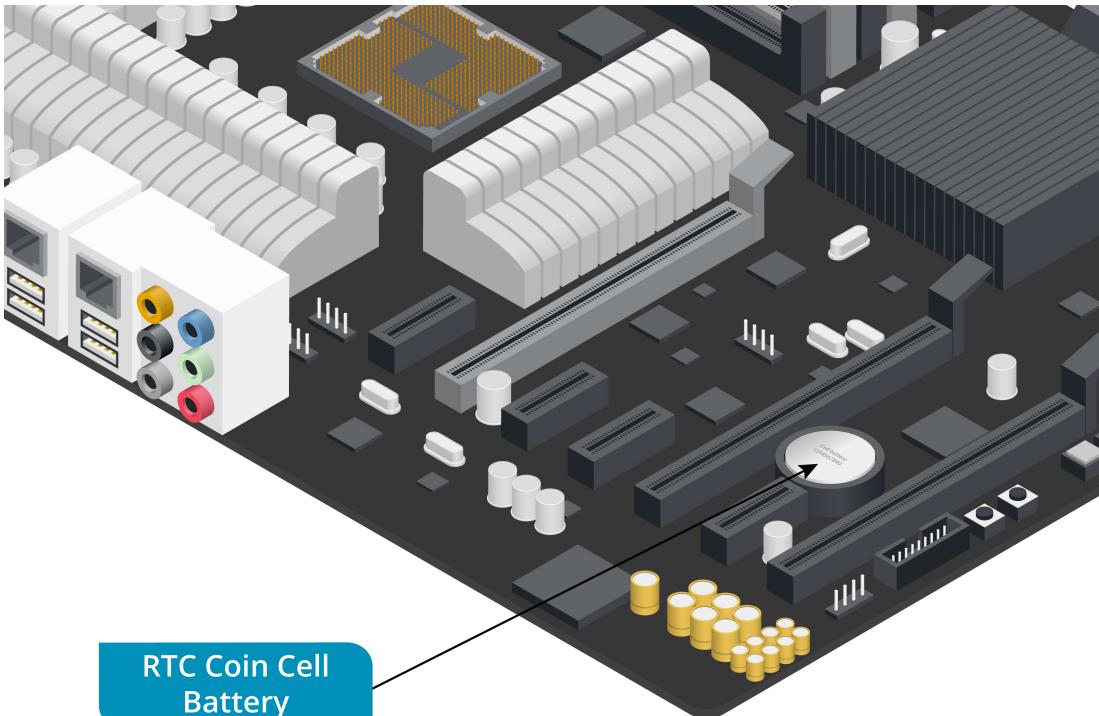


Image ©123RF.com

If the time in the system setup is incorrect, it may signal a failing RTC battery, which should be replaced with the same type. This battery is often called the "CMOS battery" because older systems stored settings in **CMOS (complementary metal-oxide semiconductor)** RAM. However, modern systems use **NVRAM (non-volatile random-access memory)** or flash memory for configuration data, so the battery mainly supports the RTC.

 Modern systems frequently use **Network Time Protocol (NTP)** to sync time with network clocks.

Troubleshoot Missing Video Issues

If no image is displayed on the monitor or projector, first ensure the display device is plugged in and turned on. Verify that the monitor is not in standby mode by pressing a key or cycling the power.

Use the monitor's controls to adjust the image or select the **correct input source**. An incorrect input source is a common issue; for example, if there is no image, make sure the monitor is set to the HDMI port connected to the computer, not an empty DVI port. These settings are accessible via the on-screen display (OSD) menus, operated by buttons on the monitor case, where you can also adjust brightness, color/contrast, and power-saving settings.

Physical Cabling Issues

If the display is powered on and the input source is not the issue, check the **cable and connectors** between the video card and monitor. Ensure the cable is securely connected at

both ends and is not loose, stretched, or crimped. Verify that the cable specification matches the application requirements; for instance, a basic HDMI cable may not support 4K resolution, which requires a High-Speed rated cable.

Another common issue is cable and port compatibility, especially with newer technologies like HDMI 2.1, DisplayPort 1.4, or USB-C. Using the appropriate cable and port can help avoid connection issues and ensure optimal display performance.

Note: To rule out cable problems, use the "known good" technique by substituting with another cable. Alternatively, test the monitor with a different PC to determine whether the issue lies with the display unit or the input source.

Burnt-Out-Bulb Issues

A video projector is a large-format display device used for presentations and meetings, projecting images onto a screen or wall through a lens system. Projectors use various imaging technologies such as cathode ray tube (CRT), liquid crystal display (LCD), and digital light processing (DLP). Unlike PC monitors that use small backlights or LED arrays, projectors rely on high-intensity bulbs to project images.

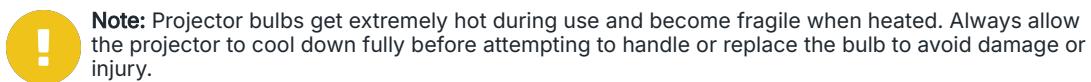
A DLP projector



Image ©123RF.com

Projector bulbs have a limited lifespan and will eventually need to be replaced. Signs of a failing bulb include dimming images and a possible bulb health warning on the projector. A completely

failed bulb, known as a "**burnt-out bulb**," may produce a popping sound and show visible scorch marks or a broken filament.



Modern projectors increasingly use **LED or laser light sources**, which last significantly longer and reduce the need for frequent bulb replacements, making "burned-out bulb" issues less common in newer models.

Intermittent Projector Shutdown Issues

Intermittent projector shutdown is typically caused by overheating. To troubleshoot, ensure the fan is working properly, verify that the ventilation system is clear of dust and debris, and confirm that the vents are not blocked. Also, check that the ambient temperature is within the projector's operating range.

If overheating is not the issue, check for loose connector cables that may disrupt power or signal, and ensure the bulb is securely installed, as an improperly installed bulb can cause unexpected shutdowns. Additionally, make sure the projector's firmware is up to date, as some models may have software-related shutdowns that can be resolved with updates.

Troubleshoot Video Quality Issues

Video quality issues, such as artifacts or glitches, can result from problems with the display or the input source (e.g., video card). Below are common issues and steps for troubleshooting:

- **Dim image:** Check the On-Screen Display (OSD) to adjust brightness and contrast. Power-saving modes or features like adaptive brightness or eye-saving mode may reduce brightness automatically, triggered by ambient light sensors or specific times of day. If the image is barely visible, the backlight may have failed, and the display may need repair or replacement.
- **Fuzzy image:** A fuzzy image is often due to a mismatch between the output resolution and the display's native resolution. For example, if a monitor's native resolution is 1920×1080 but the video card is set to 1024×768, the image will appear blurry. To resolve, adjust the resolution in the operating system or update the video driver.
- **Flashing screen:** Check the video cable and connectors to ensure they are securely attached. Flickering or flashing could also result from failing backlight components or internal circuitry. Other signs of failure include bands, lines, or bright spots. If so, the display may need repair.



A faulty or overheating video card can also cause flashing. Try connecting the monitor to another computer to isolate the issue.

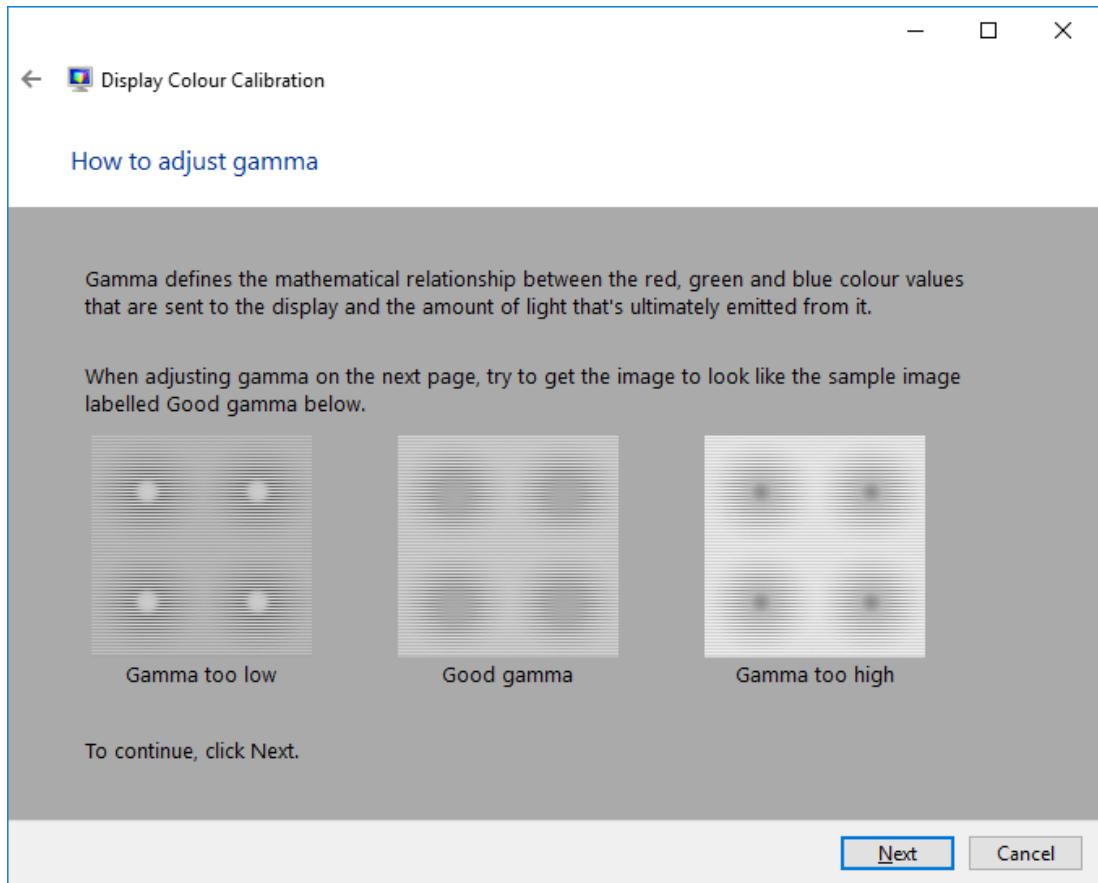
- **Dead pixels:** Stuck (constantly bright) or dead (black) pixels can occur in flat-panel displays. Stuck pixels may be fixed using pixel cycling software or by gently tapping the screen with a soft object. Dead pixels usually cannot be repaired. Check your warranty for replacement options.
- **Display burn-in:** Burn-in happens when a static image is displayed for too long, leaving a ghost image on the screen. OLED and plasma displays are more prone to burn-in than TFT/LED screens. Prevent burn-in by using a screen saver or enabling the display's auto-off function during inactivity.



A TFT/LED monitor uses an LED backlight to illuminate the image. In an OLED, each pixel provides its own illumination.

- **Incorrect color display:** For digital art production, it is crucial to calibrate the display to match scanning devices and print output. Color calibration involves adjusting screen and scanner settings to balance color input and output using a color profile. Utilize the Color Management applet in Control Panel, along with test card color patterns and spectrophotometers, to define and verify this profile.

Display Color Calibration utility in Windows 10



Screenshot courtesy of Microsoft.

The text reads, Gamma defines the relationship between red, green, and blue color values that are sent to the display and the amount of light that's ultimately emitted from it. When adjusting gamma on the next page, try to get the image to look like the sample image labelled Good gamma below. Three examples of gamma settings are shown: Gamma too low: The circles are faint with dark outer rings and visible shadows. Good gamma: The circles blend smoothly into the background with minimal visible shadows. Gamma too high: The circles are overly bright and fade into the background. Next and Cancel buttons are at the bottom. Users are instructed to click next to continue.

Color glitches, such as purple or green horizontal lines or unexpected color changes, are often caused by a faulty or loose connector or low-quality cabling. Try replacing the cable. If the issue persists, there may be a hardware fault in the monitor or graphics adapter.

- **Audio issues:** HDMI and DisplayPort can transmit both video and audio, while DVI and VGA do not. If you're not getting audio from built-in speakers, check power, connections, and

volume controls. Verify that the correct audio output is selected in the operating system and that volume settings are appropriate.

- **Sizing issues:** If the screen appears stretched, compressed, or has black bars around the edges, adjust the display settings on your computer to match the monitor's native resolution and use the monitor's on-screen display (OSD) menu to fit the image to the screen. Additionally, ensure that the correct video drivers are installed and updated.
- **Distorted image:** If the screen appears wavy or shows geometric warping, like pincushion effects, check for interference from nearby electronic devices, secure all cable connections, and ensure the display settings match the monitor's native resolution. For a CRT (Cathode Ray Tube), adjust the pincushion settings and consider replacing a potentially faulty cable.

Module 5

Comparing Local Networking Hardware

Module Overview

Network support is a great competency for IT technicians at all levels to possess. In today's environment, standalone computing is a rarity. Just about every digital device on the planet today is connected to external resources via a network, whether it is a small office/home office (SOHO) network, a corporate WAN, or to the Internet directly.

The ability to connect, share, and communicate using a network is crucial for running a business and staying connected to everything in the world. As a CompTIA® A+® support technician, if you understand the technologies that underlie both local and global network communications, you can play an important role in ensuring that the organization you support stays connected.

This module will help you understand how different types of networks are categorized and how to compare and contrast network cabling, hardware, and wireless standards.

Module Summary

Prepare for A+ Core 1 by:

- Comparing network types
- Comparing networking hardware
- Explaining network cable types
- Comparing wireless networking types

Lesson 5A

Network Types

Lesson Overview

As an IT professional, you have been tasked with configuring and setting up the network for a small business. The business has multiple offices throughout the area. You will be responsible for helping decide what is the best network type to use for the client. A network type categorizes the area over which the parts of the network are managed. Being able to use the correct terminology to classify the scope of a network and distinguish its specific requirements will enable you to assist with installation and support procedures.

In this lesson, you will learn the different types of networks and when each type will be used.



Objectives Covered

2.7 Compare and contrast Internet connection types, network types, and their characteristics

Learning Outcomes

As you study this lesson, answer the following questions:

- What is a network that covers the area equivalent to a city known as?
- A user has connected a smartwatch and earbuds to their cellphone over Bluetooth. What type of network have they created?
- You have been tasked with creating a network in which each segment of the network is designed as a modular function. What type of network are you creating?
- What is a whole site that is dedicated to provisioning server resources called?
- Which IEEE ethernet standards are most cabled LANs based on?

LANs and WANs

Local Area Network (LAN)

A [local area network](#) is a group of computers connected by cabling and one or more network switches that are all installed at a single geographical location. A LAN might span a single floor in a building, a whole building, or multiple nearby buildings (a campus). Any network where the nodes are within about 1 or 2 km (or about 1 mile) of one another can be thought of as "local." LAN cabling and devices are typically owned and managed by the organization that uses the network.

Most cabled LANs are based on the [Ethernet](#) standards maintained by the Institute of Electrical and Electronics Engineers (IEEE). The IEEE 802.3 standards are designated xBASE-Y, where x is the nominal data rate, and Y is the cable type. For example:

- 100BASE-T refers to Fast Ethernet over copper twisted pair cabling. Fast Ethernet works at 100 Mbps.
- 1000BASE-T refers to Gigabit Ethernet over copper twisted pair cabling. Gigabit Ethernet works at 1000 Mbps (or 1 Gbps). 1000BASE-T is the mainstream choice of standard for most LANs.
- 10GBASE-T refers to a copper cabling standard working at 10 Gbps.

The majority of LANs will use copper cabling, which uses electrical signaling to communicate data.

Oftentimes, the backbone of the LAN or some special Ethernet networks will transmit data over fiber optic cabling, which uses pulses of light to communicate data.

Wide Area Network (WAN)

Where a LAN operates at a single site, a [wide area network](#) spans multiple geographic locations. One example of a WAN is the Internet, a global network of networks. A company dedicated to facilitating access to the Internet from local networks is called an Internet Service Provider (ISP).

Most private or enterprise WANs use cabling and equipment leased from an ISP to interconnect two or more LAN sites. For example, a company might use a WAN to connect branch office sites to the LAN at its head office.

Wireless LANs

A [wireless local area network](#) (WLAN) uses radios and antennas for data transmission and reception. Most WLANs are based on the IEEE 802.11 series of standards. IEEE 802.11 is better known by its brand name, [Wi-Fi](#).

Wi-Fi and Ethernet technologies complement one another and are often used together as segments within the same local network. This allows computers with wired and wireless networking adapters on the same LAN to communicate with one another.

Metropolitan Area Networks

The term [metropolitan area network](#) (MAN) can be used to mean a specific network type covering an area equivalent to a city or other municipality. It could mean a company with multiple connected networks within the same metropolitan area - basically, a MAN will be larger than a LAN but smaller than a WAN.

Personal Area Networks

A [personal area network](#) (PAN) refers to using wireless connectivity to connect to devices at a range of a few meters. A PAN can be used to share data between a PC and mobile devices and wearable technology devices, such as smartwatches. It can also connect PCs and mobile devices to peripheral devices, such as printers, headsets, speakers, and video displays. The most common example of a PAN is wearable Bluetooth devices such as earbuds and smartwatches connected to the cellphone on a person.

As digital and network functionality continues to be embedded in more and more everyday objects (typically referred to as the Internet of Things or "IoT"), appliances, and clothing, the use of PANs will only grow.

Storage Area Network

A Storage Area Network (SAN) refers to a specialized network that is dedicated to storage devices. Servers can connect to the storage devices as if they are directly attached. The key characteristics of a SAN include:

- **Dedicated Network** - The SAN must be attached to a dedicated network that is independent of the LAN. This ensures that the SAN traffic does not interfere with other network operations.
- **Block-Level Access** - Data sent across the SAN is transferred in raw chunks of data with no file system structure called blocks. This allows for efficient data transfers and flexible storage management options.
- **Consolidated Storage** - Multiple types of storage, such as RAID arrays and tape drives, are joined together in the SAN, which sets up centralized storage resources for servers.
- **High Speed** - SANs will typically utilize high-speed connections such as Fibre Channel or Internet Small Computer System Interface (iSCSI) for data transfer.

SOHO and Enterprise Networks

A [small office/home office \(SOHO\)](#) LAN is a small network possibly using a centralized server, in addition to client devices and printers, but often using a single networking appliance to provide LAN and Internet connectivity. This is often referred to as a "SOHO router," "Internet router," or "broadband router." SOHO networks are typically designed to support a small number of users.

A typical SOHO network layout

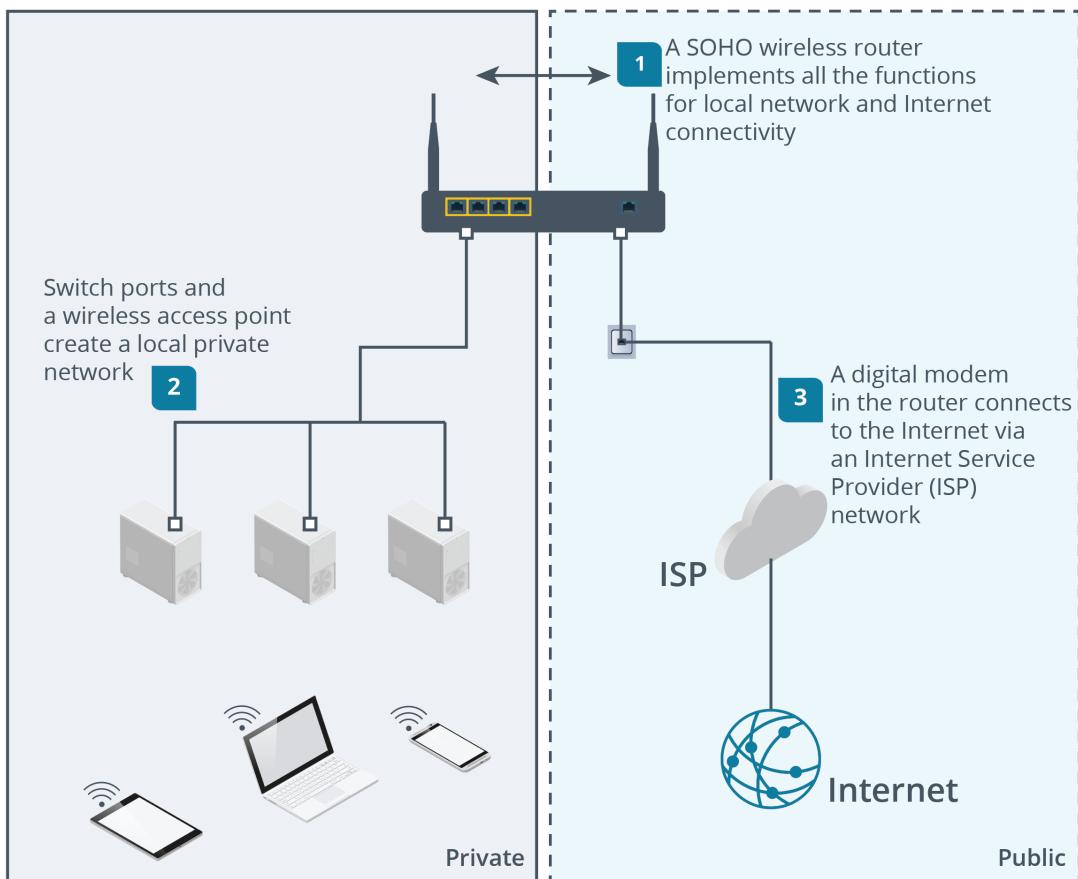


Image © 123RF.com.

The steps are as follows: Step 1 (Public): A SOHO wireless router implements all the functions for local network and internet connectivity. Step 2 (Private): Switch Ports and a wireless access point create a local private network. Step 3 (Public): A digital modem in the router connects to the internet via an internet service provider (ISP) network.

Networks supporting larger businesses or academic institutions have networking appliances with the same basic functions as a SOHO router, but because they must support more clients with a greater degree of reliability, each function is performed by a separate network device.

The following graphic illustrates how an enterprise LAN might be implemented. Each segment of the network is designed as a modular function. Client computers and printers are located in work areas and connected to the network by cabling running through wall conduit. Laptops and mobile devices connect to the network via wireless access points (APs). Network servers are separated from client computers in a server room. Workgroup switches connect each of these blocks to core/distribution switches, routers, and firewalls. These network appliances allow authorized connections between the clients and servers.

Positioning network components

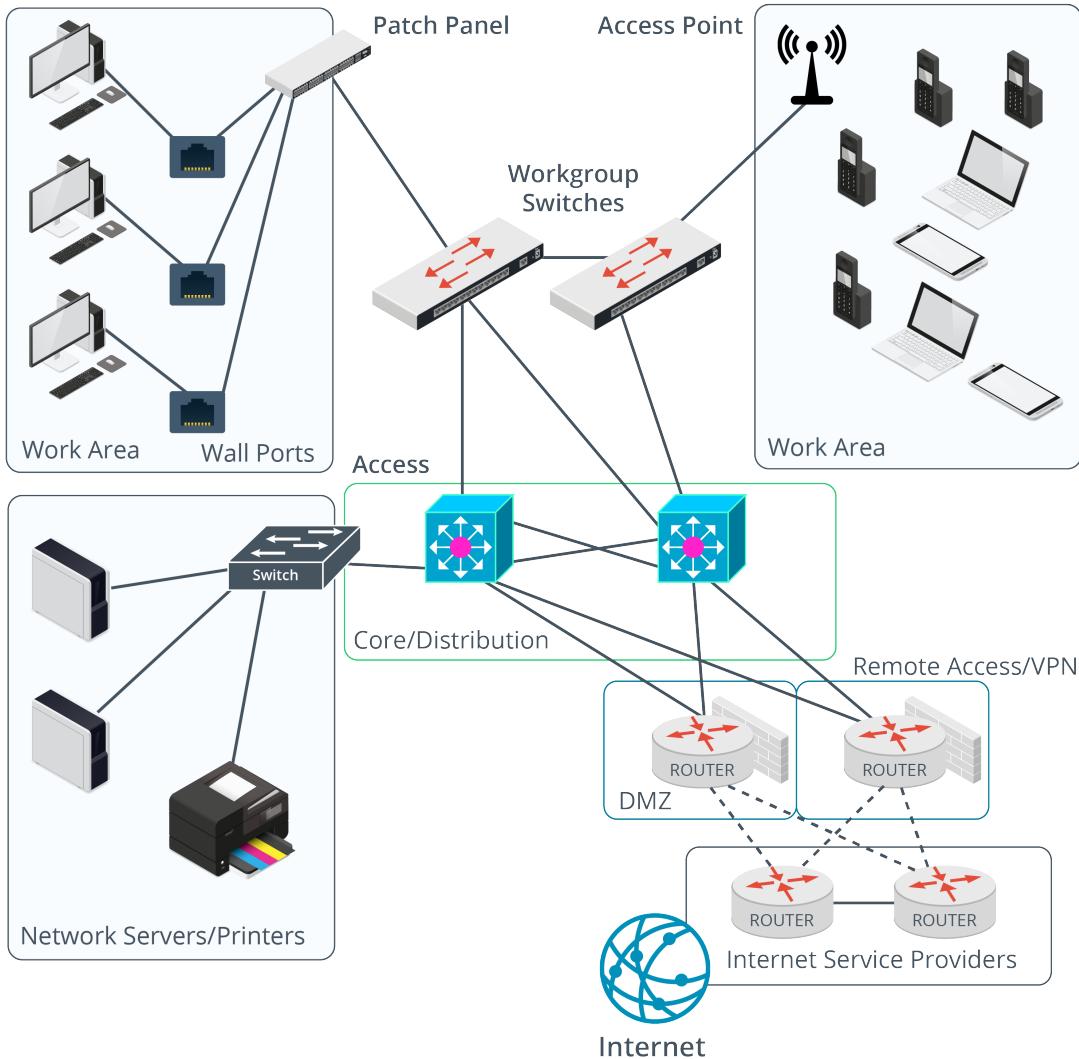


Image © 123RF.com.

On the top left, the Work Area is connected to Wall Ports. These devices are linked to a Patch Panel through cables. The Patch Panel connects to Workgroup Switches. On the right, there is another Work Area that includes wireless devices such as laptops, smartphones, and tablets. These devices communicate with the network wirelessly through an Access Point, which also links to the Workgroup Switches. The workgroup switches are connected to the core or distribution. The core or distribution further connects to the network servers or printers, D M Z, remote access or V P N, and internet service providers.

Internet services are placed in protected screened subnets, which represent a border between the private LAN and the public Internet. Traffic to and from this zone is strictly filtered and monitored. Network border services provide Internet access for employees, email and communications, remote access and WAN branch office links via virtual private networks (VPNs), and web services for external clients and customers.

Datacenters

Most networks distinguish between two basic roles for the computers:

- A server computer is dedicated to running network applications and hosting shared resources.
- A client computer allows end users to access the applications and resources to do work.

On an enterprise LAN, server computers are hosted in a separate area, referred to as a "server room."

A company with high server requirements might operate a datacenter, however. A [datacenter](#) is a whole site that is dedicated to provisioning server resources. Most datacenters are housed in purpose-built facilities. A datacenter has dedicated networking, power, climate control, and physical access control features all designed to provide a highly available environment for running critical applications.

Lesson 5B

Networking Hardware

Lesson Overview

Now that you have decided on the best network type to set up for the client, you are responsible for gathering the required hardware that will be needed to set up the network. In this lesson, you will learn the different components that make a network operate and how to set them up.



Objectives Covered

2.5 Compare and contrast common networking hardware devices

Learning Outcomes

As you study this lesson, answer the following questions:

- What computer component is responsible for establishing the physical connection to the network?
- What are the first 24 bits of a MAC address known as?
- What is the cable that runs from the wall port through the walls terminated into?
- Which type of switch can perform its function without requiring any sort of configuration?
- Which PoE standard provides approximately 51W of power?

Network Interface Cards

Ethernet communications are established by either electrical signaling over copper twisted pair cable or pulses of light transmitted over fiber optic cable. The physical connection to the cable is made using a transceiver port in the computer's network interface card (NIC). The majority of PC motherboards today have a built-in 1000BASE-T compatible adapter.

You might use a NIC adapter card to support other types of Ethernet, such as fiber optic. You can also purchase cards with multiple ports of the same type - two or four 1000BASE-T ports, for instance. The multiple ports can be bonded to create a higher-speed link. Four Gigabit Ethernet ports could be bonded to give a nominal link speed of 4 Gbps.

For the NIC to be able to process the electrical or light signals as digital data, the signals must be divided into regular units with a consistent format. There must also be a means for each node on the local network to address communications to other nodes. Ethernet provides a data link protocol to perform these framing and addressing functions.

Each Ethernet NIC port has a unique hardware/physical address, called the "media access control" (MAC) address. Each frame of Ethernet data identifies the source MAC address and destination MAC address in fields in a header.

Captured Ethernet frame showing the destination and source MAC addresses. The destination address is a broadcast address

No.	Time	Source	Destination	Protocol	Length	Info
3 2.3...	IntelCor_50:38:04	Broadcast	ARP	42 Who has 192.168.1.247? Tell 192.168.1.73		
4 2.9...	IntelCor_50:38:04	Broadcast	ARP	42 Who has 192.168.1.247? Tell 192.168.1.73		

```

> Frame 3: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
└Ethernet II, Src: IntelCor_50:38:04 (ac:72:89:50:38:04), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ↘ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
    Address: Broadcast (ff:ff:ff:ff:ff:ff)
      .... ..1. .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ..1. .... .... .... = IG bit: Group address (multicast/broadcast)
  ↘ Source: IntelCor_50:38:04 (ac:72:89:50:38:04)
    Address: IntelCor_50:38:04 (ac:72:89:50:38:04)
      .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
      .... ..0. .... .... .... = IG bit: Individual address (unicast)
  Type: ARP (0x0806)
  > Address Resolution Protocol (request)

0000  11111111 11111111 11111111 11111111 11111111 10101100 01110010  .....
0008  10001001 01010000 00111000 00000100 00001000 00000110 00000000 00000001  .P8.....
0010  00001000 00000000 00000110 00000100 00000000 00000001 10101100 01110010  .....
0018  10001001 01010000 00111000 00000100 11000000 10101000 00000001 01001001  .P8....I
0020  00000000 00000000 00000000 00000000 00000000 00000000 11000000 10101000  .....
0028  00000001 11110111  .....

Ethernet (eth), 14 bytes
  || Packets: 3521 · Displayed: 3521 (100.0%) || Profile: Default

```

Screenshot courtesy of Wireshark.

The interface at the top includes standard menu options like File, Edit, View, Capture, and others. Below the menu bar, there are filtering options and buttons for controlling the capture process. The table below includes the Number, Time, Source, Destination, Protocol, Length, and Info. Few lines of code are given below.

A MAC address consists of 48 binary digits, making it six bytes in size. A MAC address is typically represented as 12 digits of hexadecimal. Hexadecimal is a numbering system often used to represent network addresses of different types. A hexadecimal digit can be one of sixteen values: 0–9 and then A, B, C, D, E, F. Each hexadecimal digit represents half a byte (or four bits aka a nibble).

A MAC address is typically written out with a colon separating every two digits. They may occasionally use a hyphen or no separator - for example, 00:60:8C:12:3A:BC or 00608C123ABC.

A MAC address is broken into two distinct parts:

- The first 24 bits are known as the **Organizationally Unique Identifier (OUI)**. This identifies the manufacturer of the NIC.
- The last 24 bits are known as the **Network Interface Controller (NIC) Specific**. This is a unique identifier for each NIC.

Patch Panels

In most types of office cabling, the computer is connected to a wall port and via cabling running through the walls to a [patch panel](#). The cables running through the walls are terminated to insulation displacement connector (IDC) punchdown blocks at the back of the panel.

IDCs at the rear of a patch panel

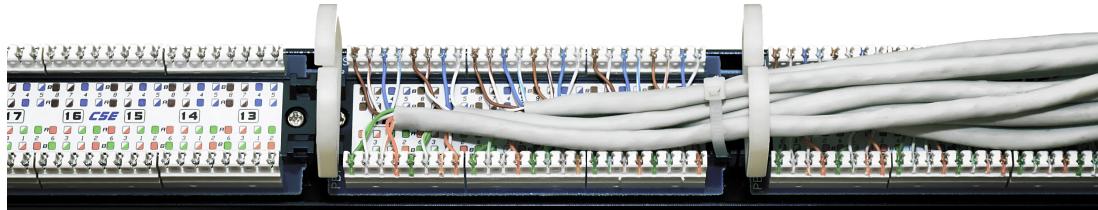


Image by plus69 © 123RF.com.

The other side of the patch panel has pre-wired RJ45 ports. A patch cord is used to connect a port on the patch panel to a port on an Ethernet switch. This cabling design makes it easier to change how any given wall port location is connected to the network via switch ports.

Patch panel with prewired RJ45 ports

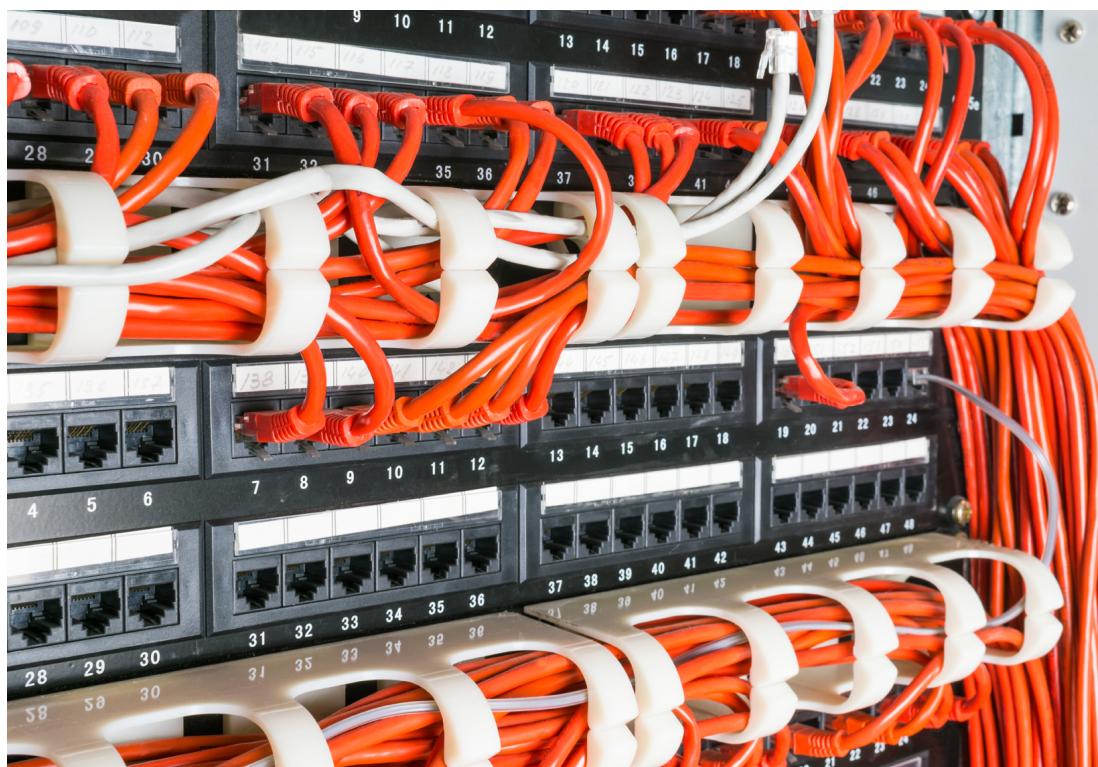


Image by Svetlana Kurochkina © 123RF.com.



It is vital to use an effective labeling system when installing structured cabling so that you know which patch panel port is connected to which wall port.

Switches

Ethernet switches are used to connect multiple devices inside of a network together. The switch provisions one port for each device that needs to connect to the network.

When a device is connected to the switch, it adds the device's MAC address to a table and keeps track of which port it connects to. When a frame comes in, the switch is able to decode each frame and identify the source and destination MAC addresses. The switch is able to intelligently forward it to the port that is a match for the destination MAC address.

Switch operation

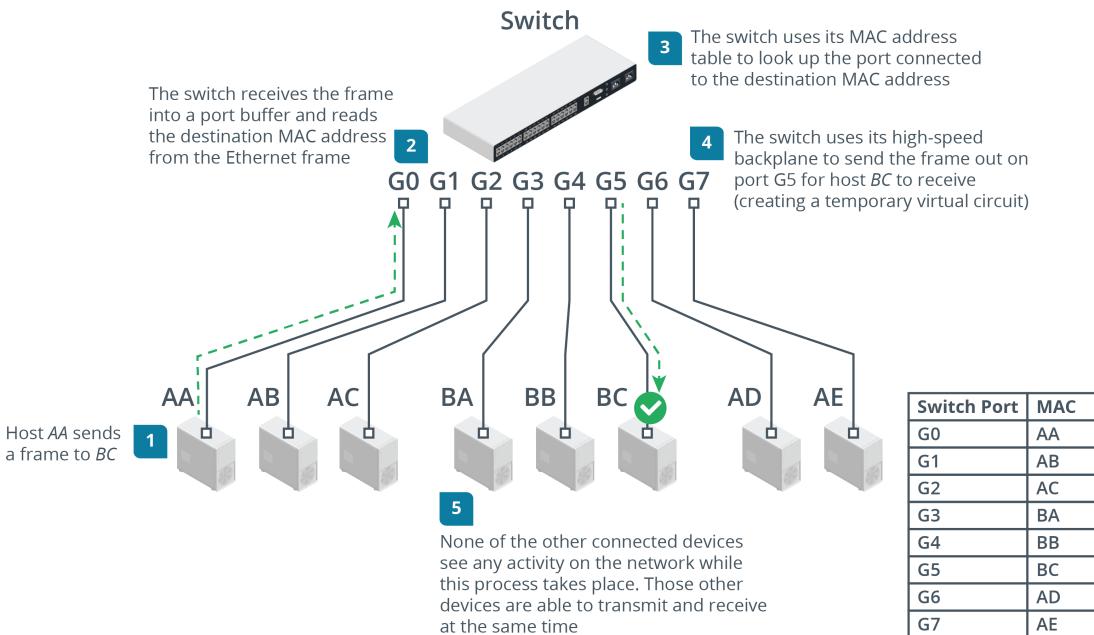


Image © 123RF.com.

The diagram includes a switch at the top, which has multiple ports labeled from G 0 to G 7. Several computers are connected to these ports, each assigned a unique MAC address. The steps are as follows: Step 1: Host AA sends a frame to BC. Step 2: The switch receives the frame into a port buffer and reads the destination MAC address from the Ethernet frame. Step 3: The switch uses its MAC address table to look up the port connected to the destination MAC address. Step 4: The switch uses its high speed backplane to send the frame out on port G5 for host BC to receive (creating a temporary virtual circuit). Step 5: None of the other connected devices see any activity on the network while this process takes place. Those other devices are able to transmit and receive at the same time. The table lists the switch port and MAC details as follows:

G0: AA G1: AB G2: AC G3: BA G4: BB G5: BC G6: AD G7: AE

This means that each switch port is considered a separate collision domain, and the negative effects of collisions are eliminated. Each computer has a full duplex connection to the network and can send and receive simultaneously at the full speed supported by the network cabling and NIC.

! When a computer sends a frame, the switch reads the source address and adds it to its MAC address table. If a destination MAC address is not yet known, the switch floods the frame out of all ports.

Unmanaged and Managed Switches

An **unmanaged** switch performs its function without requiring any sort of configuration. You just power it on and connect some hosts to it, and it establishes Ethernet connectivity between the

network interfaces without any more intervention. Common unmanaged switches will have four or eight ports, as they are typically used in small networks. There is an unmanaged four-port switch embedded in most of the SOHO router/modems supplied by Internet Service Providers (ISPs) to connect to their networks.

Larger workgroups and corporate networks require additional functionality in their switches. Switches designed for larger LANs are called a [managed switch](#). A managed switch will work as an unmanaged switch out-of-the-box, but an administrator can connect to it over a management port to configure security settings and then choose options for the switch's more advanced functionality. Most managed switches are designed to be bolted into standard network racks. A typical workgroup switch will come with 24 or 48 access ports for client PCs, servers, and printers. These switches have uplink ports allowing them to be connected to other switches.

A workgroup switch

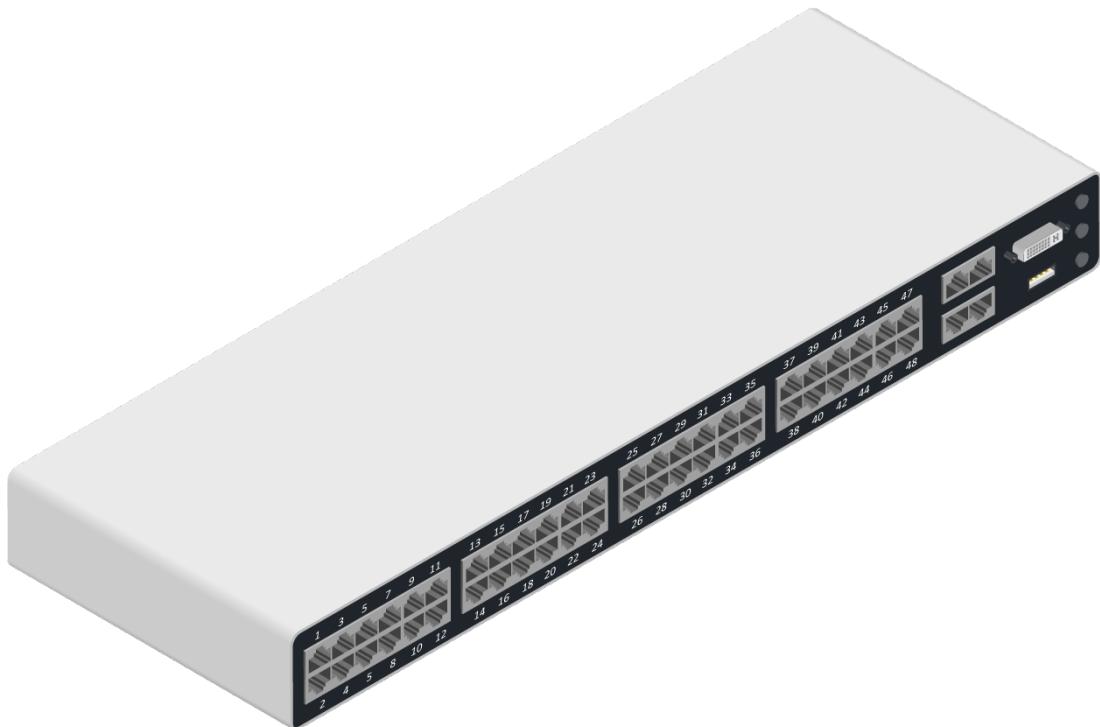


Image © 123RF.com.

An enterprise might also use modular switches. These provide a power supply and fast communications backplane to interconnect multiple switch units. This enables the provisioning of hundreds of access ports via a single compact appliance.

Modular chassis allows provisioning multiple access switches



Image © 123RF.com.

Configuring a managed switch can be performed over either a web or command line interface.

Viewing interface configuration on a Cisco switch

```
FastEthernet1/0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is f41f.c253.7103 (bia f41f.c253.7103)
    MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
      reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA, loopback not set
    Keepalive set (10 sec)
    Full-duplex, 100Mb/s, media type is 10/100BaseTX
    input flow-control is off, output flow-control is unsupported
    ARP type: ARPA, ARP Timeout 04:00:00
    Last input 00:00:51, output 00:00:00, output hang never
    Last clearing of "show interface" counters never
    Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
    Queueing strategy: fifo
    Output queue: 0/40 (size/max)
    5 minute input rate 0 bits/sec, 0 packets/sec
    5 minute output rate 0 bits/sec, 0 packets/sec
      18 packets input, 1758 bytes, 0 no buffer
      Received 4 broadcasts (2 multicasts)
      0 runts, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 watchdog, 2 multicast, 0 pause input
      0 input packets with dribble condition detected
      111 packets output, 13828 bytes, 0 underruns
      0 output errors, 0 collisions, 1 interface resets
      0 unknown protocol drops
```

Power over Ethernet

[Power over Ethernet](#) is a means of supplying electrical power from a switch port over ordinary data cabling to a powered device (PD), such as a voice over IP (VoIP) handset, camera, or wireless access point. PoE is defined in several IEEE **standards**:

- **802.3af (Type 1 PoE or 2-pair PoE)** allows powered devices to draw up to about 13 W. Power is supplied as 350mA@48V and limited to 15.4 W, but the voltage drop over the maximum 100m (328 feet) of cable results in usable power of around 13 W. Basic devices such as a VoIP handset, basic wireless access points, and basic security cameras will use this standard.
- **802.3at (PoE+ or Type 2 PoE)** allows powered devices to draw up to about 25 W, with a maximum current of 600 mA. Devices that require more power, such as advanced wireless access points, pan-tilt-zoom security cameras, and video IP phones, will use this standard.
- **802.3bt (PoE++, Type 3 and Type 4 PoE, 4PPoE)** supplies up to about 51 W (Type 3) or 73 W (Type 4) usable power. Devices such as LED lighting, digital signage, point-of-sale systems, and other high-power devices will use this standard.

PoE Switch

A **PoE-enabled switch** is referred to as endspan power sourcing equipment (PSE). When a device is connected to a port on a PoE switch, the switch goes through a detection phase to determine whether the device is PoE enabled. If so, it determines the device's power consumption and sets an appropriate supply voltage level. If not, it does not supply power over the port and, therefore, does not damage non-PoE devices.

Powering these devices through a switch is more efficient than using a wall-socket AC adapter for each appliance. It also allows network management software to control the devices and apply energy-saving schemes, such as making unused devices go into sleep states and power capping.

PoE Injector

If the switch does not support PoE, a device called a "power [injector](#)" (or "midspan") can be used. One port on the injector is connected to the switch port. The other port is connected to the device. The overall cable length cannot exceed 100m.

Lesson 5C

Network Cable Types

Lesson Overview

Once you have gathered and installed the appropriate switches and networking hardware, you will need to install and connect the appropriate network cables. In this lesson, you will learn the different types of network cables and when each one should be used. You will also learn how to properly construct and install network cables.



Objectives Covered

- 2.8 Explain networking tools and their purposes
- 3.2 Summarize basic cable types and their connectors, features, and purposes

Learning Outcomes

As you study this lesson, answer the following questions:

- What type of network cable should be used in environments with high levels of external interference?
- Which ethernet Cat standard can provide a maximum transfer rate of 25 Gbps over a maximum distance of 30 meters?
- What type of connector does a Cat 7 cable use?
- What is the order of wires in a T568B cable?
- Which tool is used to fix a RJ45 jack to a patch cord?
- Which cable type transfers data using light?

Unshielded Twisted Pair

The most popular type of **network cable** is of a **copper** wire construction called unshielded twisted pair (UTP). A UTP cable consists of four copper conductor wire pairs. Each pair of insulated conductors is twisted at a different rate from the other pairs, which reduces interference. The electrical signals sent over each pair are balanced. This means that each wire carries an equal but opposite signal to its pair. This is another factor helping to identify the signal more strongly against any source of interference. However, the electrical signaling method is still only reliable over limited range. The signal suffers from attenuation, meaning that it loses strength over long ranges. Most UTP cable segments have a maximum recommended distance of 100 m (328 feet).

UTP cable

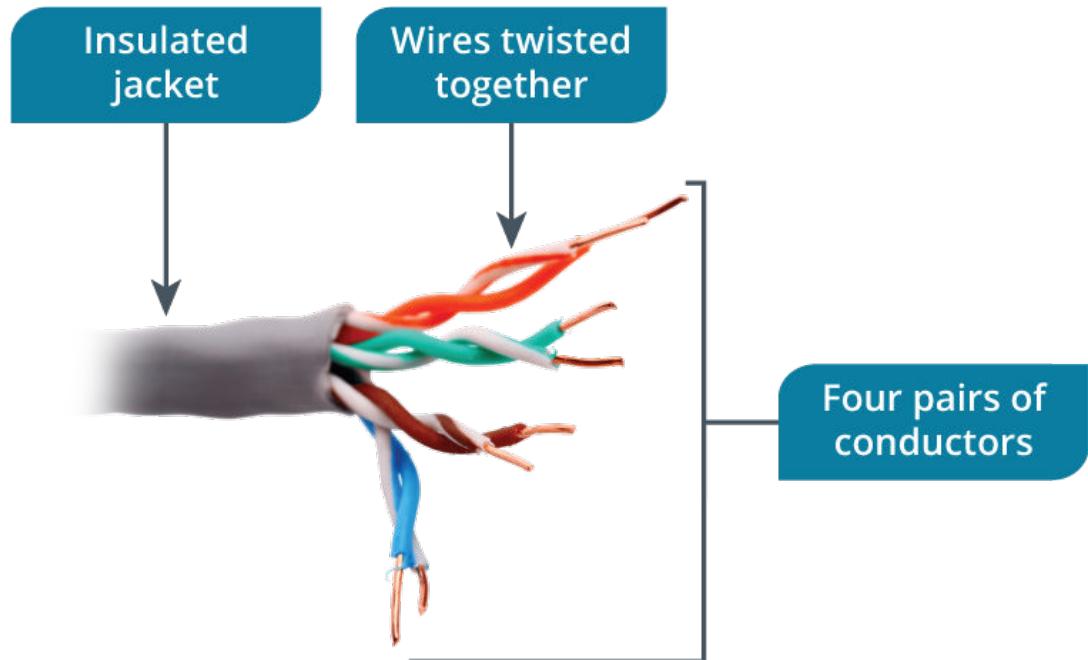


Image © 123RF.com.

Shielded Twisted Pair

Shielded Twisted Pair (STP) provides extra protection against interference. STP cables are typically a requirement in environments with high levels of external interference, such as cable that must be run in proximity to fluorescent lighting, power lines, motors, and generators.

Shielded cable can be referred to generically as "STP," but several types of shielding and screening exist:

- Foiled Unshielded Twisted Pair (F/UTP) cable has a single foil shield that surrounds all wires in the cable. This type of cable may also be called screened twisted pair (ScTP) or sometimes just foiled twisted pair (FTP). This type of cable provides decent protection against electromagnetic interference (EMI) and crosstalk at a reasonable cost.
- Shielded Foiled Twisted Pair (S/FTP) cabling has a braided outer screen and foil-shielded pairs. This type of cable provides the best protection against EMI and crosstalk but is expensive and less flexible. There are also variants with a foil outer shield (F/FTP).
- Unshielded with Foiled Twisted Pair (U/FTP) cable has no outer shield, but each pair of wires has a foil shield around them. This provides good protection against EMI and crosstalk.

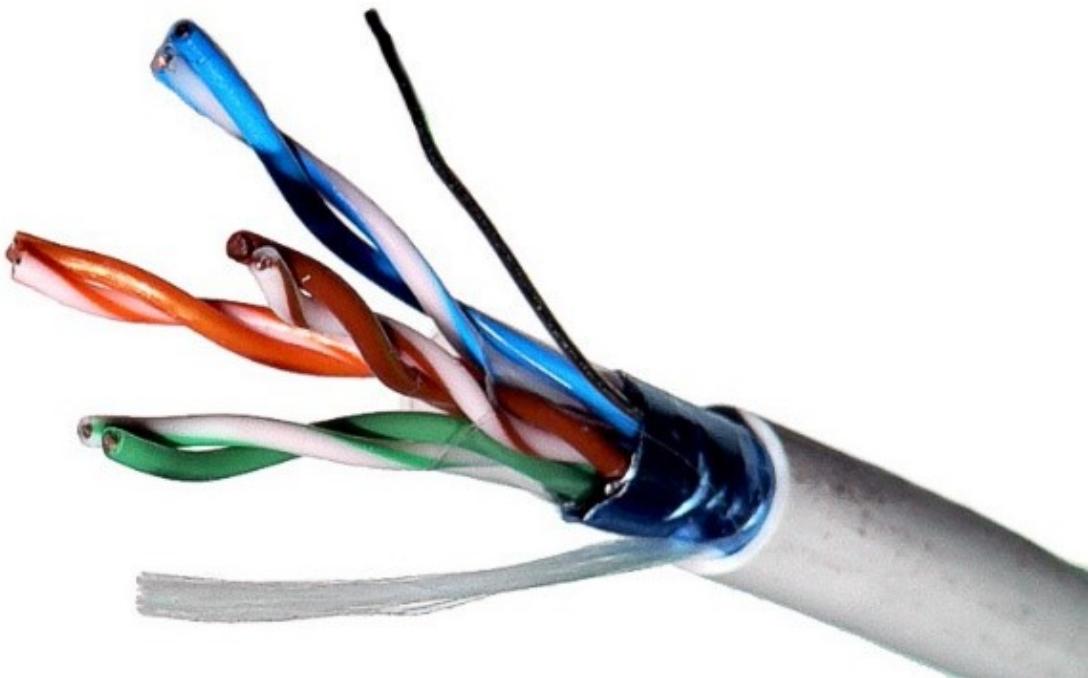
F/UTP cable with a foil screen surrounding unshielded pairs

Image by Baran Ivo and released to public domain.

The screening/shielding elements of shielded cable must be bonded to the connector to prevent the metal from acting as a large antenna and generating interference. Modern F/UTP and S/FTP solutions (using appropriate cable, connectors, and patch panels) facilitate this by incorporating bonding within the design of each element.

Category (Cat) Standards

A Category (Cat) standard defines the performance of twisted-pair cabling. Higher Cat specification cable is capable of higher data rates.

Cat specifications are defined in the TIA/EIA-568-C Commercial Building Telecommunications Cabling Standards.

Cat	Max. Transfer Rate	Max. Distance	Ethernet Standard Support
5	100 Mbps	100 m (328 ft)	100BASE-TX (Fast Ethernet)
5e	1 Gbps	100 m (328 ft)	1000BASE-T (Gigabit Ethernet)
6	1 Gbps	100 m (328 ft)	1000BASE-T (Gigabit Ethernet)
	10 Gbps	55 m (180 ft)	10GBASE-T (10G Ethernet)
6A	10 Gbps	100 m (328 ft)	10GBASE-T (10G Ethernet)

Cat	Max. Transfer Rate	Max. Distance	Ethernet Standard Support
7	10 Gbps	100 m (328 ft)	10GBASE-T (10G Ethernet)
	100 Gbps	15 m (50 ft)	100GBASE-T (100G Ethernet)
8	25 Gbps	30 m (100 ft)	25GBASE-T (25G Ethernet)
	40 Gbps	30 m (100 ft)	40GBASE-T (40G Ethernet)

The Cat specification is printed on the cable jacket along with the cable type (UTP or F/UTP, for instance). Cat 5 cable supports the older 100 Mbps Fast Ethernet standard. It is no longer commercially available. A network cabled with Cat 5 will probably need to be rewired to support Gigabit Ethernet.

Cat 5e would still be an acceptable choice for providing Gigabit Ethernet links for client computers, but most sites would now opt to install Cat 6 cable. The improved construction standards for Cat 6 mean that it is more reliable than Cat 5e for Gigabit Ethernet, and it can also support 10 Gbps, though over reduced range.

Cat 6A supports 10 Gbps over 100 m, but the cable is bulkier and heavier than Cat 5e and Cat 6, and the installation requirements are more stringent, so fitting it within pathways designed for older cable can be problematic. TIA/EIA standards recommend Cat 6A for healthcare facilities, with Power over Ethernet (PoE) 802.3bt installations, and for running distribution system cable to wireless access points.

Cat 7 and Cat 8 cables are not widely in use yet. These cables are mostly used in datacenters where shorter runs that require high bandwidth are needed. Cat 7 uses a special type of connector called a GG45, which is not compatible with an RJ45 port. Cat 8 cable can use either the GG45 or RJ45 connector.

Copper Cabling Connectors

Twisted pair cabling for Ethernet can be terminated using modular **RJ45** connectors. RJ45 connectors are also referred to as "8P8C," standing for eight-position/eight-contact. Each conductor in four-pair Ethernet cable is color-coded. Each pair is assigned a color (orange, green, blue, and brown). The first conductor in each pair has a predominantly white insulator with stripes of the color; the second conductor has an solid color.

Twisted pair RJ45 connectors

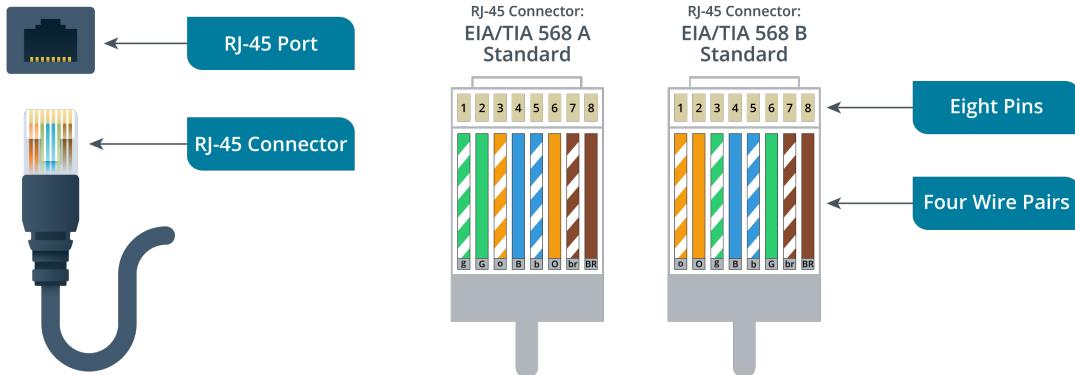


Image © 123RF.com.

RJ-45 connector: EIA/TIA 568 A standard and EIA/TIA 568 B standard has 8 pins and four wire pairs.

The EIA/TIA-568 standard defines two methods for terminating twisted pair: [T568A/T568B](#). In T568A, pin 1 is wired to green/white, pin 2 is wired to green, pin 3 is wired to orange/white, and pin 6 is wired to orange. In T568B, the position of the green and orange pairs is swapped over, so that orange terminates to 1 and 2 and green to 3 and 6. When cabling a network, it is best to use the same termination method consistently. A straight-through Ethernet cable is wired with the same type of termination at both ends.

Twisted-pair can also be used with **RJ11** connectors. Unlike the four-pair cable used with Ethernet, RJ11 is typically used to terminate two-pair cable, which is widely used in telephone systems and with broadband digital subscriber line (DSL) modems.

Copper Cabling Installation Tools

Data cable for a typical office is installed as a structured cabling system. With structured cabling, the network adapter port in each computer is connected to a wall port using a flexible **patch cord**. Behind the wall port, **permanent cable** is run through the wall and ceiling to an equipment room and connected to a patch panel. The port on the patch panel is then connected to a port on an Ethernet switch.

A structured cabling system uses two types of cable termination:

- Patch cords are terminated using RJ45 plugs crimped to the end of the cable.
- Permanent cable is terminated to wall ports and patch panels using insulation displacement connectors (IDC), also referred to as "**punchdown blocks**".



The 100 m distance limitation is for the whole link, referred to as "channel link." Each patch cord can only be up to 5 m long. Permanent link uses solid cable with thicker wires. Patch cords use stranded cable with thinner wires that are more flexible but also suffer more from attenuation.

Installing cable in this type of system involves the use of cable strippers, punchdown tools, and crimpers.

Cable Stripper and Snips

To terminate cable, a small section of outer jacket must be removed to expose the wire pairs. This must be done without damaging the insulation on the inner wire pairs. A [cable stripper](#) is designed to score the outer jacket just enough to allow it to be removed. Set the stripper to the correct diameter, and then place the cable in the stripper and rotate the tool once or twice. The score cut in the insulation should now allow you to remove the section of jacket.

A cable stripper

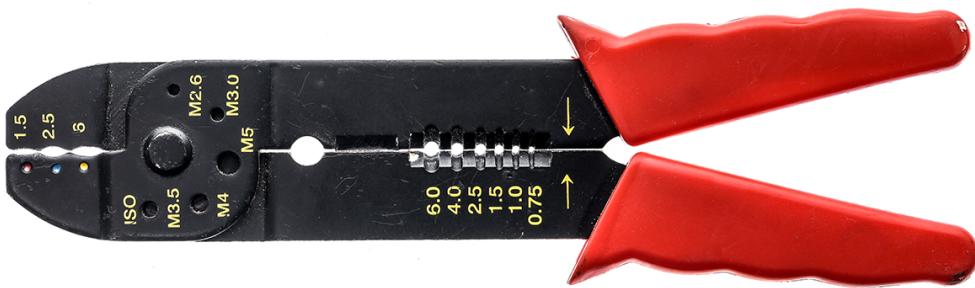


Image by gasparij © 123RF.com

Most Cat 6 and all Cat 6A cable has a plastic star filler running through it that keeps the pairs separated. You need to use electrician's scissors (snips) to cut off the end of this before terminating the cable. There will also be a nylon thread called a "ripcord." This can be pulled down the jacket to open it up more if you damaged any of the wire pairs initially. Snip any excess rircord before terminating the cable.

Punchdown Tool

A [punchdown tool](#) is used to fix each conductor into an IDC. First, untwist the wire pairs and lay them in the color-coded terminals in the IDC in the appropriate termination order (T568A or T568B). To reduce the risk of interference, no more than $\frac{1}{2}$ " (13 mm) should be untwisted. Use the punchdown tool to press each wire into the terminal. Blades in the terminal cut through the insulation to make electrical contact with the wire.

Connecting UTP cable to IDCs using a punchdown tool.



Image by dero2084 © 123RF.com.

Crimper

A crimper is used to fix a jack to a patch cord. Orient the RJ45 plug so that the tab latch is underneath. Pin 1 is the first pin on the left. Arrange the wire pairs in the appropriate order (T568A or T568B), and then push them into the RJ45 plug. Place the plug in the crimper tool, close it tightly to pierce the wire insulation at the pins, and seal the jack to the outer cable jacket.

A wire crimper.

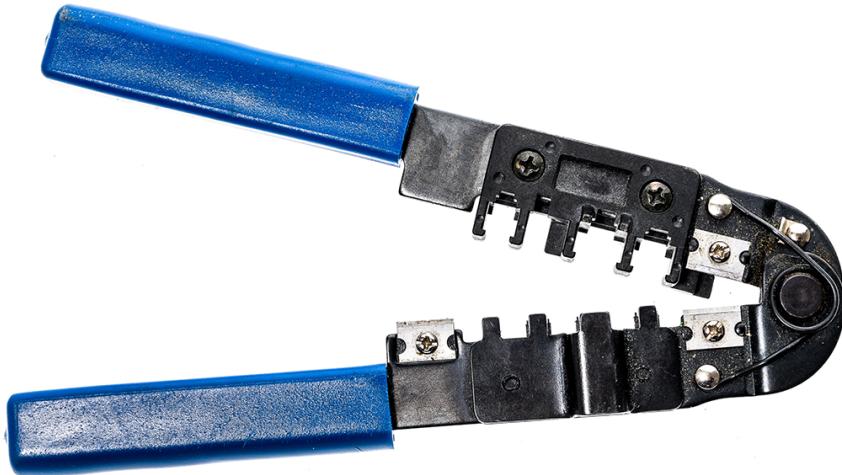


Image by gasparij © 123RF.com

Copper Cabling Test Tools

Once you have terminated cable, you must test it to ensure that each wire makes good electrical contact and is in the correct pin position. The best time to verify wiring installation and termination is just after you have made all the connections. This means you should still have access to the cable runs. Identifying and correcting errors at this point will be much simpler than when you are trying to set up enduser devices.

You can use several cabling and infrastructure troubleshooting devices to assist with this process.

Cable Tester

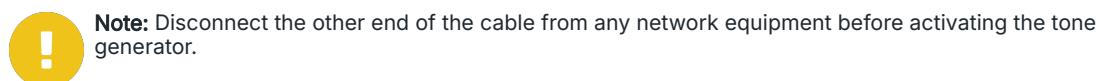
A [cable tester](#) is a pair of devices designed to attach to each end of a cable. It can be used to test a patch cord or connected via patch cords to a wall port and patch panel port to test the permanent link. The tester energizes each wire in turn, with an LED indicating successful termination. If an LED does not activate, the wire is not conducting a signal, typically because the insulation is damaged or the wire isn't properly inserted into the plug or IDC. If the LEDs do not activate in the same sequence at each end, the wires have been terminated to different pins at each end. Use the same type of termination on both ends.

Basic cable tester



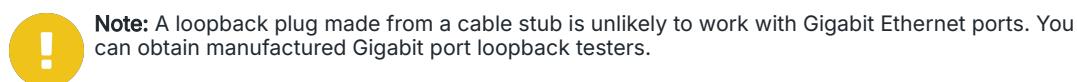
Toner Probe

Many cable testers also incorporate the function of a **toner probe**, which is used to identify a cable from within a bundle. This may be necessary when the cables have not been labeled properly. The [tone generator](#) is connected to the cable using an RJ45 jack and applies a continuous audio signal on the cable. The probe is used to detect the signal and follow the cable over ceilings and through ducts or identify it from within the rest of the bundle.

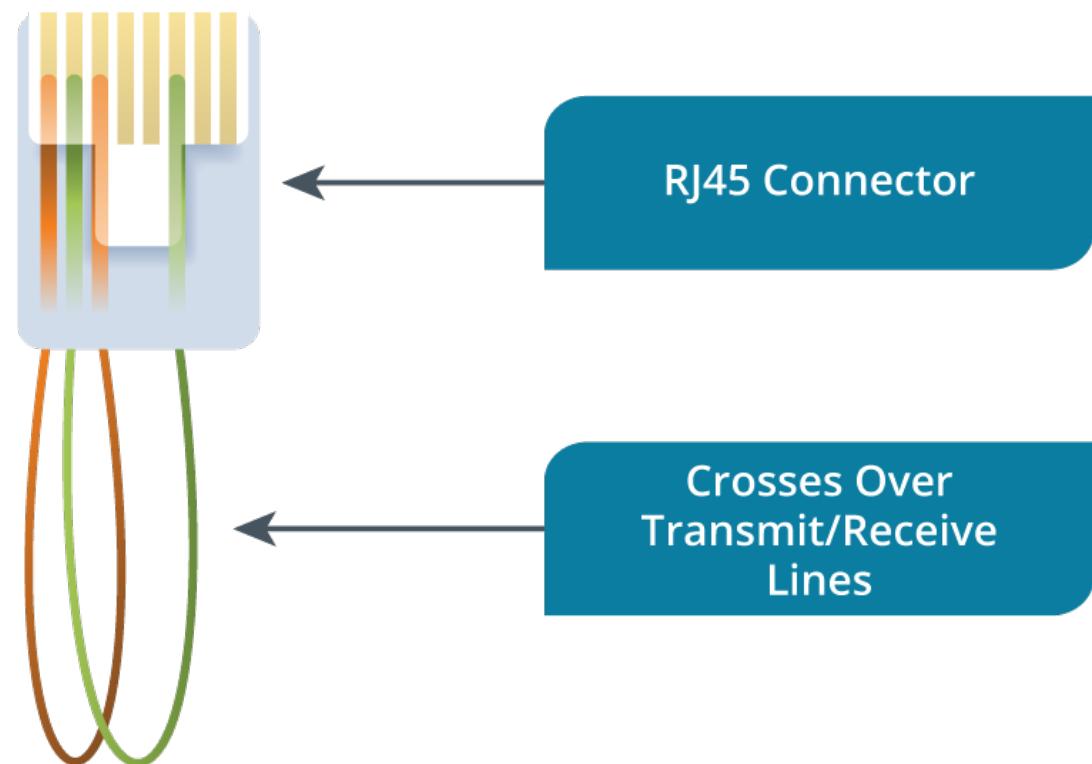


Loopback Plug

A [loopback adapter](#) is used to test a NIC or switch port. You can make a basic loopback plug from a 6" cable stub where the wires connect pin 1 to pin 3 and pin 2 to pin 6. When you connect a loopback plug to a port, you should see a solid link LED showing that the port can send and receive.



A loopback plug



Network Taps

A is used to intercept the signals passing over a cable and send them to a packet or protocol analyzer. Taps are either powered or unpowered:

- A **passive test access point (TAP)** is a box with ports for incoming and outgoing network cabling and an inductor or optical splitter that physically copies the signal from the cabling to a monitor port. No logic decisions are made, so the monitor port receives every frame regardless if it is corrupt or malformed or not and the copying is unaffected by load.
- An **active TAP** is a powered device that performs signal regeneration, which may be necessary in some circumstances. Gigabit signaling over copper wire is too complex for a passive tap to monitor, and some types of fiber links may be adversely affected by optical splitting. Because it performs an active function, the TAP becomes a point of failure for the links during power loss.



Network sniffing can also be facilitated using a [switched port analysis](#)/mirror port. This means that the sensor is attached to a specially configured port on a network switch. The mirror port receives copies of frames addressed to nominated access ports (or all the other ports).

Copper Cabling Installation Considerations

Installation of cable must be compliant with local building regulations and fire codes. This means that specific cable types must be used in some installation scenarios.

Plenum Cable

A [plenum](#) space is a void in a building designed to carry heating, ventilation, and air conditioning (HVAC) systems. Plenum space is typically a false ceiling, though it could also be constructed as a raised floor. As it makes installation simpler, this space has also been used for communications wiring in some building designs. Plenum space is an effective conduit for fire, as there is plenty of airflow and no fire breaks. If the plenum space is used for heating, there may also be higher temperatures. Therefore, building regulations require the use of fire-retardant plenum cable in such spaces. Plenum cable must not emit large amounts of smoke when burned, be self-extinguishing, and meet other strict fire safety standards.

General purpose (non-plenum) cabling uses PVC jackets and insulation. Plenum-rated cable uses treated PVC or fluorinated ethylene polymer (FEP). This can make the cable less flexible, but the different materials used have no effect on bandwidth. Data cable rated for plenum use under the US National Electrical Code (NEC) is marked as CMP on the jacket. General-purpose cables are marked as CMG or CM.

Direct Burial

Outside plant (OSP) is cable run on the external walls of a building or between two buildings. This makes the cable vulnerable to different types of weathering:

- Aerial cable is typically strung between two poles or anchors. The ultraviolet (UV) rays in sunlight plus exposure to more extreme and changing temperatures and damp conditions will degrade regular PVC.
- Conduit can provide more protection for buried cable runs. Such cable can still be exposed to extreme temperatures and damp conditions, however, so regular PVC cable should not be used.
- [Direct burial cable](#) is laid and then covered in earth or cement/concrete.

OSP cable types use special coatings to protect against UV and abrasion and are often gel-filled to protect against temperature extremes and damp conditions. Direct burial cable may also need to be armored to protect against chewing against rodents.

Optical Cabling

Copper wire carries electrical signals, which are sensitive to interference and attenuation. The light pulses generated by lasers and LEDs are not susceptible to interference and suffer less from attenuation. Consequently, **optical cabling** can support much higher bandwidth links, measured in multiple gigabits or terabits per second, and longer cable runs, measured in miles rather than feet.

A fiber optic strand



Image by atrush © 123RF.com

An **optical fiber** consists of an ultra-fine core of glass to convey the light pulses. The core is surrounded by glass or plastic cladding, which guides the light pulses along the core. The cladding has a protective coating called the "buffer." The **fiber optic cable** is contained in a protective jacket and terminated by a connector.

Fiber optic cables fall into two broad categories: single-mode and multi-mode:

- **Single-mode fiber (SMF)** has a small core (8–10 microns) and is designed to carry a long wavelength (1,310 or 1,550 nm) infrared signal, generated by a high-power, highly coherent laser diode. Single-mode cables support data rates up to 10 Gbps or better and cable runs of many kilometers, depending on the quality of the cable and optics.
- **Multimode fiber (MMF)** has a larger core (62.5 or 50 microns) and is designed to carry a shorter wavelength infrared light (850 nm or 1,300 nm). MMF uses less expensive and less coherent LEDs or vertical cavity surface emitting lasers (VCSELs) and consequently is less expensive to deploy than SMF. However, MMF does not support such high signaling speeds or long distances as single-mode and so is more suitable for LANs than WANs.

The core of a fiber optic connector is a ceramic or plastic ferrule that ensures continuous reception of the light signals. Several connector form factors are available:

- **Straight-tip connector (ST)** is a bayonet-style connector that uses a push-and-twist locking mechanism; it is used mostly on older multi-mode networks.
- **Subscriber connector (SC)** has a push/pull design that allows for simpler insertion and removal than fiber channel (FC) connector. There are simplex and duplex versions, though the duplex version is just two connectors clipped together. It can be used for single- or multi-mode.
- **Lucent connector (LC)** is a small form factor connector with a tabbed push/pull design. LC is similar to SC, but the smaller size allows for higher port density. This connector is also sometimes referred to as little-connector or local-connector.

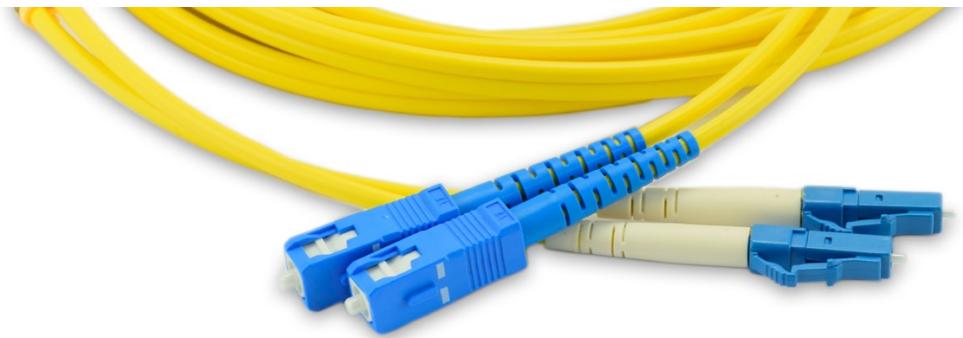
Patch cord with duplex SC format connectors (left) and LC connectors (right)

Image by YANAWUT SUNTORNKIJ © 123RF.com

Patch cords for fiber optic can come with the same connector on each end (ST-ST, for instance) or a mix of connectors (ST-SC, for instance). Fiber optic connectors are quite easy to damage and should not be repeatedly plugged in and unplugged. Unused ports and connectors should be covered by a dust cap to minimize the risk of contamination.

Coaxial Cabling

Coaxial cable is a different type of copper cabling that also carries electrical signals. Where twisted pair uses balancing to cancel out interference, coax uses two conductors that share the same axis. The core signal conductor is enclosed by plastic insulation (dielectric), and then a second wire mesh conductor serves both as shielding from EMI and as a ground.

Detailed layers of a coaxial cable

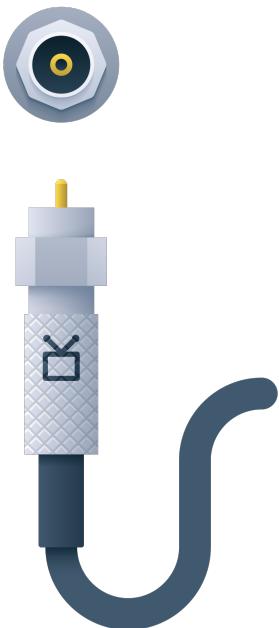


Image by destinacigdem © 123RF.com

Coax is now mostly used for CCTV installations and as patch cable for Cable Access TV (CATV) and broadband [cable modem](#). Coax for CATV installations is typically terminated using a screw-down [F-type connector](#).

F-type coaxial connector

Image © 123RF.com



Lesson 5D

Wireless Networking Types

Lesson Overview

As part of the network you have designed and configured, the client would like to incorporate wireless networking as well. You will need to decide what type of wireless network will work best in the offices and what hardware will be needed. In this lesson, you will learn the different types of wireless networking standards and how to install and configure wireless networks.



Objectives Covered

- 2.2 Explain wireless networking technologies
- 2.5 Compare and contrast common networking hardware devices
- 2.8 Explain networking tools and their purposes

Learning Outcomes

As you study this lesson, answer the following questions:

- What type of mode are most wireless networks configured in?
- What are the three main frequency bands used by wireless networks?
- You notice that your wireless network has been running slow lately. You perform a wireless analysis of the area and notice there are multiple wireless networks running on the same frequency. What would be the best solution to try to speed up your wireless network?
- What technology increases reliability and bandwidth by multiplexing signal streams from multiple antennas?
- Which wireless technology is primarily used for contactless payment?

Access Points

Wireless technologies use radio waves as transmission media. Radio systems use transmission and reception antennas tuned to a specific frequency for the transfer of signals. Most wireless LANs (WLANs) are based on the IEEE [802.11 standards](#), better known by the brand name Wi-Fi.

Most Wi-Fi networks are configured in what is technically referred to as "infrastructure mode." Infrastructure mode means that each client device (station) is configured to connect to the network via an [access point](#). In 802.11 documentation, this is referred to as an infrastructure "Basic Service Set" (BSS). The MAC address of the AP's radio is used as the [basic service set ID](#) (BSSID).

An access point can establish a wireless-only network, but it can also work as a bridge to forward communications between the wireless stations and a wired network. The wired network is referred to as the "distribution system" (DS). The access point will be joined to the network in

much the same way as a host computer is - via a wall port and cabling to an Ethernet switch. An enterprise network is likely to use Power over Ethernet (PoE) to power the AP over the data cabling.

An access point



Image © 123RF.com

Frequency Bands

Every Wi-Fi device operates on a specific radio frequency range within an overall frequency band.

Channels

Each wireless frequency band is split into a series of smaller ranges referred to as a [channel](#). These channels essentially act as lanes through the frequency band, allowing wireless networks to operate on the same wireless band without interfering with each other.

The width or size of each channel is determined by the frequency band and the access point configuration. All channels are the same width, but some wireless standards allow for channels to be bonded together, creating a wider channel. The larger the channel width, the more data that can flow down it.

Wireless Frequency Bands

The three main frequency bands in use by wireless networks are:

- The **2.4 GHz** standard is better at propagating through solid surfaces, giving it the longest signal range. However, the 2.4 GHz band does not support a high number of individual channels and is often congested with other Wi-Fi networks and even other types of wireless technology, such as Bluetooth®. Also, microwave ovens work at frequencies in the 2.4 GHz band. Consequently, with the 2.4 GHz band, there is increased risk of interference, and the maximum achievable data rates are typically lower than with 5 GHz.
- The **5 GHz** standard is less effective at penetrating solid surfaces, and so does not support the maximum ranges achieved with 2.4 GHz standards, but the band supports more individual channels and suffers less from congestion and interference, meaning it supports higher data rates at shorter ranges.
- The **6 GHz** standard is the latest wireless band that can be used by wireless networks. This standard is even less effective at penetrating solid surfaces than the 5 GHz band, so therefore does not achieve the longer ranges of the 2.4 GHz and 5 GHz bands. However, it is much faster than both of the other bands. Since this is a newer band, there is typically less congestion, which results in a more stable and reliable connection.

The nominal indoor range for Wi-Fi is 45 m (150 feet) over 2.4 GHz, 30 m (100 feet) over 5 GHz, and 15 m (50 feet) over 6 GHz. Depending on the wireless standard used, building features that may block the signal, and interference from other radio sources, clients are only likely to connect at full speed from a third to a half of those distances.

Frequency bands are typically regulated in terms of radio operation, and there is a restriction on power output, which is another factor in limiting range.

IEEE 802.11a

The **IEEE 802.11a** standard uses the 5 GHz frequency band only. The data encoding method allows a maximum data rate of 54 Mbps. The 5 GHz band is subdivided into 23 non-overlapping channels, each of which is 20 MHz wide.

The exact use of channels can be subject to different regulations in different countries. **Regulatory impacts** also include a limit on power output, constraining the range of Wi-Fi devices. Devices operating in the 5 GHz band must implement [dynamic frequency selection](#) to prevent Wi-Fi signals from interfering with nearby radar and satellite installations.

Unlicensed National Information Infrastructure (U-NII) sub-bands form the 20 MHz channels used in the 5 GHz frequency band. Each sub-band is 5 MHz wide, so the Wi-Fi channels are

spaced in intervals of four to allow 20 MHz bandwidth. Channels within the DFS range will be disabled if the access point detects radar signals

	U-NII-1		U-NII-2		U-NII-2 Extended										U-NII-3			
20 MHz	36 40 44 48		52 56 60 64		100 104 108 112 116 120 124 128 132 136 140										149 153 157 161			
Dynamic Frequency Selection (DFS) Range																		

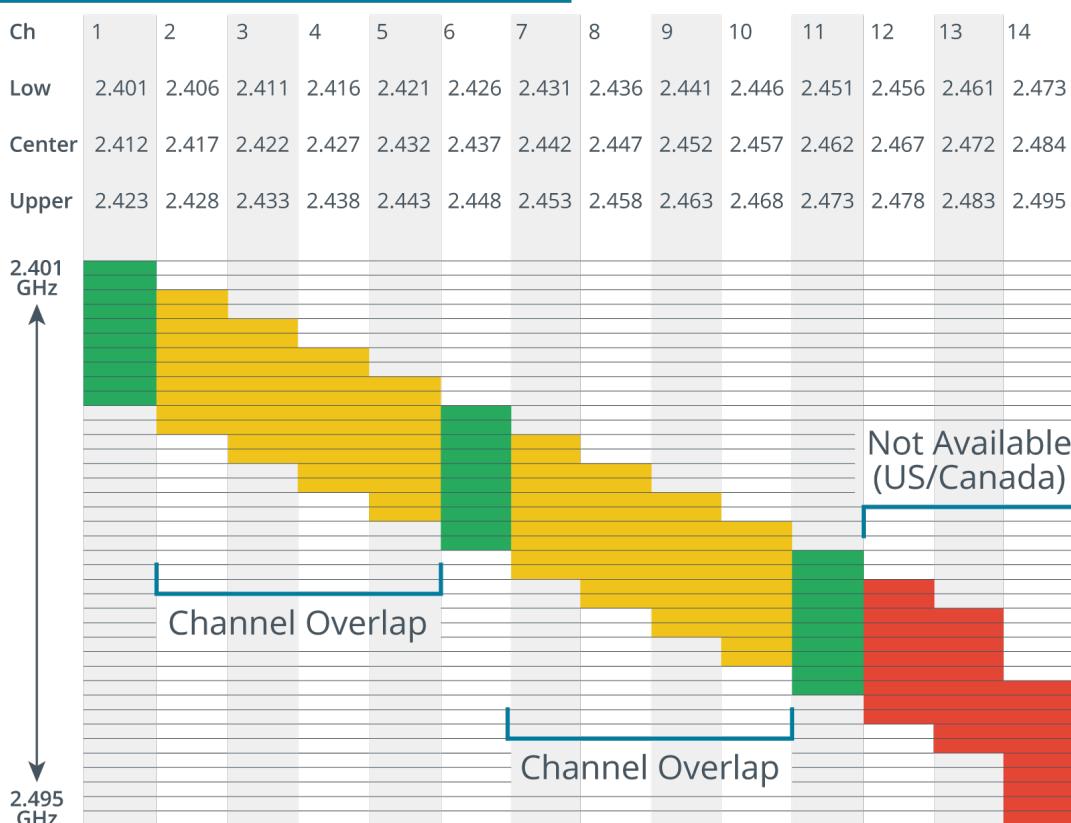
IEEE 802.11b/g

The **IEEE 802.11b** standard uses the **2.4 GHz** frequency band and was released in parallel with 802.11a. The signal encoding methods used by 802.11b are inferior to 802.11a and support a nominal data rate of just 11 Mbps.

The 2.4 GHz band is subdivided into up to 14 channels, spaced at 5 MHz intervals from 2,412 MHz up to 2,484 MHz. Because the spacing between each channel is only 5 MHz and 802.11b uses channels that are 22 MHz wide, 802.11b channels overlap quite considerably. This means that interference is going to occur unless you use one of the three non-overlapping channels (1, 6, and 11). Also, in the Americas, regulations permit the use of channels 1–11 only, while in Europe, channels 1–13 are permitted, and in Japan, all 14 channels are permitted.

Channel overlap in the 2.4 GHz band

2.4 GHz Wi-Fi Frequencies (in GHz)



The **IEEE 802.11g** standard offered a relatively straightforward upgrade path from 802.11b. 802.11g uses the same encoding mechanism and 54 Mbps rate as 802.11a but in the 2.4 GHz band used by 802.11b. This made it straightforward for vendors to design 802.11g devices that could offer backward support for legacy 802.11b clients.

One key difference between 802.11b and 802.11g is the channel width. 802.11b uses a 22 MHz channel width, whereas 802.11g uses a 20 MHz channel width. This is due to the modulation technique that each standard uses. Modulation is the process or technique used to modify a radio wave so it can carry data.

- 802.11b uses the Direct-Sequence Spread Spectrum (DSSS) modulation technique. DSSS spreads the signal across a wider channel (22 MHz) to improve resistance to interference.
- 802.11g uses the Orthogonal Frequency-Division Multiplexing (OFDM) modulation technique. OFDM is more efficient, which allows more data to be sent across a smaller channel (20 MHz).

Even though 802.11g uses a smaller channel width, the channel in the 2.4 GHz range is the same just to keep things compatible between the two standards.

IEEE 802.11n

The **IEEE 802.11n** standard introduced several improvements to increase bandwidth. It can work over both 2.4 GHz and 5 GHz. Each band is implemented by a separate radio. An access point or adapter that can support simultaneous 2.4 GHz and 5 GHz operation is referred to as "dual band." Some older client smartphone adapters support only a 2.4 GHz radio.

The 802.11n standard allows two adjacent 20 MHz channels to be combined into a single 40 MHz channel, referred to as "[channel bonding](#)." Due to the restricted channel layout of 2.4 GHz on a network with multiple APs, channel bonding is a practical option only in the 5 GHz band. However, note that 5 GHz channels are not necessarily contiguous, and the use of some channels may be blocked if the access point detects a radar signal.

802.11n 40 MHz bonded channel options in the 5 GHz band. The center channel number is used to identify each bonded channel

	U-NII-1				U-NII-2				U-NII-2 Extended								U-NII-3						
20 MHz	36	40	44	48	52	56	60	64	100	104	108	112	116	120	124	128	132	136	140	149	153	157	161
40 MHz	38	46	54	62					102	110	118	126	134				151	159					

Dynamic Frequency Selection (DFS) Range

The other innovation introduced with 802.11n increases reliability and bandwidth by multiplexing signal streams from 2–3 separate antennas. This technology is referred to as [multiple input multiple output](#) (MIMO). The antenna configuration is represented as 1×1 , 2×2 , or 3×3 to indicate the number of transmit and receive antennas available to the radio.

The nominal data rate for 802.11n is 72 Mbps per stream or 150 Mbps per stream for a 40 MHz bonded channel, and 802.11n access points are marketed using Nxxx designations, where xxx is the nominal bandwidth. As an example, an N600 2×2 access point can allocate a bonded channel to two streams for a data rate of 300 Mbps, and if it does this simultaneously on both its 2.4 GHz and 5 GHz radios, the bandwidth of the access point could be described as 600 Mbps.

In recent years, Wi-Fi standards have been renamed with simpler digit numbers; 802.11n is now officially designated as Wi-Fi 4.

Wi-Fi 5 and Wi-Fi 6

The Wi-Fi 5 (or **802.11ac**) and Wi-Fi 6 (**802.11ax**) standards continue the development of Wi-Fi technologies to increase bandwidth and support modern networks.

Wi-Fi 5 (802.11ac)

Wi-Fi 5 is designed to work only in the 5 GHz band. A dual-band access point can use its 2.4 GHz radio to support clients on legacy standards (802.11g/n). A tri-band access point has one 2.4 GHz radio and two 5 GHz radios. Wi-Fi 5 allows up to eight streams, though in practice, most Wi-Fi 5 access points only support 4×4 streams. A single stream over an 80 MHz channel has a nominal rate of 433 Mbps.

Wi-Fi 5 also allows wider 80 and 160 MHz bonded channels.

80 and 160 MHz bonded channel options for Wi-Fi 5

	U-NII-1	U-NII-2	U-NII-2 Extended					U-NII-3	
20 MHz	36	40	44	48	52	56	60	64	
40 MHz	38	46		54	62				
80 MHz		42			58				
160 MHz			50				114		
Dynamic Frequency Selection (DFS) Range									

Wi-Fi 5 access points are marketed using AC values, such as AC5300. The 5300 value is made up of the following:

- 1,000 Mbps over a 40 MHz channel with 2×2 streams on the 2.4 GHz radio.
- 2,166 Mbps over an 80 MHz bonded channel with 4×4 streams on the first 5 GHz radio.
- 2,166 Mbps on the second 5 GHz radio.

Note: You'll notice that, given 802.11n 150 Mbps per stream (40 MHz channels) and 802.11ac 433 Mbps per stream (80 MHz channels), none of those values can be made to add up. The labels are only useful as relative performance indicators.

Multiuser MIMO (MU-MIMO)

In basic 802.11 operation modes, bandwidth is shared between all stations. An AP can communicate with only one station at a time; multiple station requests go into a queue.

Wi-Fi 5 products partially address this problem using **multiuser MIMO**. In Wi-Fi 5, downlink MU-MIMO (DL MU-MIMO) allows the access point to use its multiple antennas to send data to up to four clients simultaneously.

Wi-Fi 6 (802.11ax)

Wi-Fi 6 improves the per-stream data rate over an 80 MHz channel to 600 Mbps. As with Wi-Fi 5, products are branded using the combined throughput of all radios. For example, AX6000 claims nominal rates of 1,148 Mbps on the 2.4 GHz radio and 4,804 Mbps over 5 GHz.

Wi-Fi 6 works in both the 2.4 GHz and 5 GHz bands. The Wi-Fi 6e standard adds support for a new 6 GHz frequency band. 6 GHz has less range but more frequency space, making it easier to use 80 and 160 MHz channels.

Where Wi-Fi 5 supports up to four simultaneous clients over 5 GHz only, Wi-Fi 6 can support up to eight clients, giving it better performance in congested areas. Wi-Fi 6 also adds support for uplink MU-MIMO, which allows MU-MIMO capable clients to send data to the access point simultaneously.

Wi-Fi 6 introduces another technology to improve simultaneous connectivity called [orthogonal frequency division multiple access](#). OFDMA can work alongside MU-MIMO to improve client density - sustaining high data rates when more stations are connected to the same access point.

Wi-Fi 7 (802.11be)

Wi-Fi 7 operates in the 2.4 GHz, 5 GHz, and 6 GHz bands. Wi-Fi 7 utilizes channels that are 320 MHz wide when operating the 6 GHz range, allowing for much faster data transfer speeds up to 46 Gbps.

Wi-Fi 7 provides support for Multi-Link Operation (MLO), which allows devices to connect and send data over multiple bands (2.4 GHz, 5 GHz, and 6 GHz) or channels to reduce latency and improve throughput.

Another key feature of Wi-Fi 7 is the ability to use Multi-Resource Units (MRUs). Each channel in the 6 GHz range is broken down into smaller channels called MRUs, which can all be different sizes based on the needs of the network. The access point dynamically allocates MRUs to different devices based on their data requirements. Devices with higher bandwidth needs may receive more MRUs, while devices with lower needs may receive fewer MRUs.

Wireless LAN Installation Considerations

Clients identify an infrastructure WLAN through the network name or [service set identifier](#) (SSID) configured on the access point. An SSID can be up to 32 bytes in length and, for maximum compatibility, should only use ASCII letters and digits plus the hyphen and underscore characters.

Configuring an access point

The screenshot shows the TP-LINK Archer VR900 configuration page. The top navigation bar includes tabs for Quick Setup, Basic, and Advanced, with Advanced selected. It also features language selection (English), Logout, and Reboot options, along with 2.4GHz and 5GHz frequency band toggles.

The left sidebar menu lists several options: Status, Operation Mode, Network, IPTV, Wireless (selected), Wireless Settings, WPS, MAC Filtering, Wireless Schedule, Statistics, and Advanced Settings.

The main content area is titled "Wireless Settings". It contains the following configuration fields:

- Wireless Radio:** Enable (checked)
- Wireless Network Name (SSID):** comptia_wlan (checkbox Hide SSID is unchecked)
- Security:** WPA/WPA2 Personal (Recommended) (dropdown menu)
- Version:** Auto (radio button)
- Encryption:** WPA2-PSK (radio button selected)
- Password:** 12345670
- Mode:** 802.11gn mixed (dropdown menu)
- Channel:** Auto (dropdown menu)
- Channel Width:** Auto (dropdown menu)
- Transmit Power:** Low (radio button)

A green "Save" button is located at the bottom right of the configuration section.

At the bottom of the page, there are footer links for Firmware Version (0.1.0 0.9.1 v0069.0 Build 160525 Rel.38143n), Hardware Version (Archer VR900 v2 00000000), and Support.

Screenshot courtesy of TP-Link.

The top bar has tabs Quick Setup, Basic, and Advanced. The top-right corner has options for Logout and Reboot with a dropdown for selecting the interface language, which is set to English. The upper-right section also displays toggles for 2.4 Giga Hertz and 5 Giga Hertz Wi-Fi bands.

The interface has a navigation menu on the left side with options like Status, Operation Mode, Network, I P T V, and Wireless. The options listed below the wireless are wireless Settings, W P S, MAC Filtering, Wireless Schedule, Statistics, and Advanced Settings. In the main section, Wireless Settings are being configured. The Wireless Radio is enabled, and the Wireless Network Name (S S I D) is set to CompTIA underscore w lan. There is an option to hide the S S I D, which is unchecked. The Security setting is set to W P A slash W P A 2 Personal (recommended). The version is set to W P A 2-P S K. The Encryption type selected is A E S, and a password field is visible, displaying 12345670. Other network settings include: Mode: 802.11 g n mixed, Channel: Auto, Channel Width: Auto. Transmit Power: Has 3 radio boxed labeled Low, Middle, High. At the bottom, there is a Save button.

When configuring an access point, you need to choose whether to use the same or different network names for both frequency bands. If you use the same SSID, the access point and client device will use a probe to select the band with the strongest signal. If you configure separate names, the user can choose which network and band to use.

For each frequency band, you also need to select the operation mode. This determines compatibility with older standards and support for legacy client devices. Supporting older devices can reduce performance for all stations.

Finally, for each frequency band, you need to configure the channel number and whether to use channel bonding. If there are multiple access points whose ranges overlap, they should be configured to use nonoverlapping channels to avoid interference. An access point can be left to autoconfigure the best channel, but this does not always work well. You can configure wide channels (bonding) for more bandwidth, but this has the risk of increased interference if there

are multiple nearby wireless networks. Channel bonding may only be practical in the 5 GHz band, depending on the wireless site design.



Along with the Wi-Fi frequency band and channel settings, you should also configure security parameters to control who is allowed to connect.

Wi-Fi Analyzers

To determine the best channel layout and troubleshoot wireless network performance, you need to measure the signal strength of the different networks using each channel. This can be accomplished using a [Wi-Fi analyzer](#). A Wi-Fi analyzer can be either hardware or software. A software Wi-Fi analyzer can be installed on a laptop or smartphone. It will record statistics for the AP that the client is currently associated with and detect any other access points in the vicinity.

Wireless signal strength is measured in [decibel](#) units. Signal strength is represented as the ratio of a measurement to 1 milliwatt (mW), where 1 mW is equal to 0 dBm. Because 0 dBm is 1 mW, a negative value for dBm represents a fraction of a milliwatt. For example, -30 dBm is 0.001 mW; -60 dBm is 0.000001 mW. Wi-Fi devices are all constrained by regulations governing frequency band use and output only small amounts of power.

When you are measuring signal strength, dBm values closer to zero represent better performance. A value around -65 dBm represents a good signal, while anything over -80 dBm is likely to suffer packet loss or be dropped.

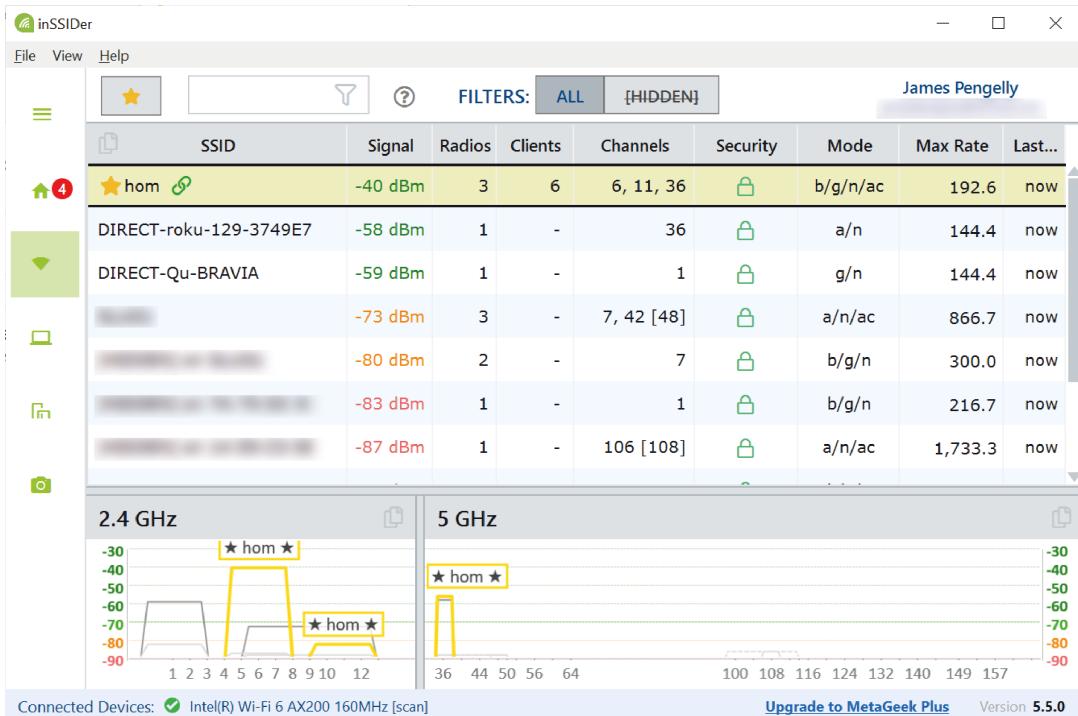


The dB units express the ratio between two values using a logarithmic scale. A logarithmic scale is nonlinear, so a small change in value represents a large change in the performance measured. For example, +3 dB means doubling, while -3 dB means halving.

The comparative strength of the data signal to the background noise is called the [signal-to-noise ratio](#). Noise is also measured in dBm, but here values closer to zero are less welcome, as they represent higher noise levels. For example, if signal is -65 dBm and noise is -90 dBm, the SNR is the difference between the two values, expressed in dB (25 dB). If noise is -80 dBm, the SNR is 15 dB and the connection will be much, much worse.

In the following screenshot, a Wi-Fi analyzer is being used to report nearby networks and channel configurations. The "home" network is supported by two access points using the same SSID for both bands. They are configured to use channels 6 and 11 on the 2.4 GHz band, with the stronger signal on channel 6, indicating the closer access point. On the 5 GHz band, only the signal on channel 36 is detected by this client. This is because 5 GHz has less range than 2.4 GHz. The blurred networks belong to other owners and have much weaker signals. Also, note from the status bar that the client adapter supports Wi-Fi 6 (ax), but the access points only support b/g/n/ac (shown in the mode column).

Metageek inSSIDer Wi-Fi analyzer software showing nearby access points



MetaGeek, LLC. © Copyright 2005-2025.

The top bar has a search tab, a filters option, and the user's account name. Below the top bar is a table with heads, S S I D, Signal, Radios, Clients, Channels, Security, Mode, Max rate, and Last modified. Graphs titled 2.4 Gigahertz and 5 Gigahertz are displayed at the bottom.

Long-Range Fixed Wireless

Wireless technology can be used to configure a bridge between two networks. This can be a more cost-effective and practical solution than laying cable. However, regulation of the radio spectrum means that the transmitters required to cover long distances must be carefully configured. These solutions are referred to as [long-range fixed wireless](#).

Point-to-point line-of-sight fixed wireless uses ground-based high-gain microwave antennas that must be precisely aligned with one another. "High-gain" means that the antenna is strongly directional. Each antenna is pointed directly at the other and can transmit signals at ranges of up to about 30 miles as long as they are unobstructed by physical objects. The antennas themselves are typically affixed to the top of tall buildings or mounted on tall poles to reduce the risk of obstructions.

Long-range fixed wireless can be implemented using licensed or unlicensed frequency spectrum. **Licensed** means that the network operator purchases the exclusive right to use a frequency band within a given geographical area from the regulator. The US regulator is the Federal Communications Commission (FCC). If any interference sources are discovered, the network operator has the legal right to get them shut down.

Unlicensed spectrum means the operator uses a public frequency band, such as 900 MHz, 2.4 GHz, and 5 GHz. Anyone can use these frequencies, meaning that interference is a risk. To minimize the potential for conflicts, **power** output is limited by **regulatory requirements**. A wireless signal's power has three main components:

- Transmit power is the basic strength of the radio, measured in dBm.
- Antenna gain is the amount that a signal is boosted by directionality - focusing the signal in a single direction rather than spreading it over a wide area. Gain is measured in [decibels per isotropic](#).
- [Effective isotropic radiated power \(EIRP\)](#) is the sum of transmit power and gain, expressed in dBm.

Lower frequencies that propagate farther have stricter power limits than higher frequencies. However, higher EIRPs are typically allowed for highly directional antennas. For example, in the 2.4 GHz band, each 3 dBi increase in gain can be compensated for by just a 1 dBm reduction in transmit power. This allows point-to-point wireless antennas to work over longer ranges than Wi-Fi APs.

Bluetooth, RFID, and NFC

Wi-Fi is used for networking computer hosts together, but other types of wireless technology are used to implement personal area networking (PAN).

Bluetooth

[Bluetooth](#) is used to connect peripheral devices to PCs and mobiles and to share data between two systems. Many portable devices, such as smartphones, tablets, wearable tech, audio speakers, and headphones, now use Bluetooth connectivity. Bluetooth uses radio communications and supports speeds of up to 3 Mbps. Adapters supporting version 3 or 4 of the standard can achieve faster rates (up to 24 Mbps) through the ability to negotiate an 802.11 radio link for large file transfers.

The earliest Bluetooth version supports a maximum range of 10 m (30 feet), while newer versions support a range of over 100 feet, though signal strength will be weak at this distance. Bluetooth devices can use a pairing procedure to authenticate and exchange data securely.

Bluetooth pairing



Image © 123RF.com

The Bluetooth option is toggled on, represented by a green slider. Below, there is a section titled, My Devices, listing a device P L T underscore B B FIT with a status of Not Connected. Below that, the section, other devices is displayed, with no devices listed.

Version 4 introduced a Bluetooth Low Energy (BLE) variant of the standard. BLE is designed for small battery-powered devices that transmit small amounts of data infrequently. A BLE device remains in a low-power state until a monitor application initiates a connection. BLE is not backward compatible with "classic" Bluetooth, though a device can support both standards simultaneously.

Bluetooth 5 is the latest Bluetooth standard. Bluetooth 5 offers a range of up to 240 m (800 ft) which is about 4 times the range for Bluetooth 4. Bluetooth 5 also provides twice the speed of Bluetooth 4 and 8 times the messaging capacity. This translates to quicker file transfers, smoother streaming, and improved responsiveness in applications that require real-time data exchange. Bluetooth 5 improves power consumption over other versions of Bluetooth.

Radio Frequency Identification (RFID)

[Radio Frequency ID](#) is a means of identifying and tracking objects using specially encoded tags. When an RFID reader scans a tag, the tag responds with the information programmed into it. A tag can be either an unpowered, passive device that only responds when scanned at close range (up to about 25 m) or a powered, active device with a range of 100 m. Passive RFID tags can be embedded in stickers and labels to track parcels and equipment. RFID is also used to implement some types of access badges to operate electronic locks.

Near Field Communications

[Near Field Communication](#) is a peer-to-peer version of RFID. In other words, an NFC device can work as both tag and reader to exchange information with other NFC devices. NFC normally works at up to two inches (6 cm) at data rates of 106, 212, and 424 Kbps.

NFC is mostly used for contactless payment readers, security ID tags, and shop shelf-edge labels for stock control. It can also be used to configure other types of connections such as pairing Bluetooth devices.

Module 6

Configuring Network Addressing and Internet Connections

Module Overview

You have just been assigned to work together with two colleagues on a project. The team has worked together before on a few projects, but this is the first time that the three of you are not in the same physical location. John is in Austin, Texas, Evan lives in London, and you are visiting Alice Springs, Australia. This remote location dynamic of the team will require time management from all members but also a reliance on technology solutions to facilitate meetings through a collaboration software application. To make this application work, your system needs to use a network address and several communication protocols. These communication protocols allow for a standard "language" to be used between devices across the Internet.

Several new hardware devices are used to make these Internet-wide communications occur. These include modems and radio antennas to connect to an internet service provider (ISP). The network addressing and forwarding function is performed by router devices and the Internet Protocol (IP).

This lesson will help you to compare the technologies that underpin Internet access and configure the main protocols in the Transmission Control Protocol/Internet Protocol (TCP/IP) suite that enable communications between networks and the Internet.

Module Summary

Prepare for A+ Core 1 by:

- Comparing Internet connection types
- Using basic TCP/IP concepts
- Comparing protocols and ports
- Comparing network configuration concepts

Lesson 6A

Internet Connection Types

Lesson Overview

As an IT professional, you are tasked with ensuring a reliable connection to the internet by using the ISP connection provided at your location. This connection will allow internal IT systems, including your gaming console, to connect to resources outside of the home or office. You will also ensure the different communication protocols are configured correctly. Ensuring all networking hardware is also connected, configured, and operational. In this lesson, you will also be able to identify various communication protocols and how they support network operations.



Objectives Covered

- 2.5 Compare and contrast common networking hardware devices
- 2.7 Compare and contrast Internet connection types, network types, and their characteristics

Learning Outcomes

As you study this lesson, answer the following questions:

- What are the various internet connection types provided by an ISP?
- What networking hardware components are used to connect to an ISP?
- What are IPv4 and IPv6, and how do they allow various networks to communicate?
- What are TCP and UDP communications protocols, and how are they different from one another?
- What ports and protocols are commonly found on SOHO and ISP networks?
- How do DNS and DHCP assist in the configuration of a network?

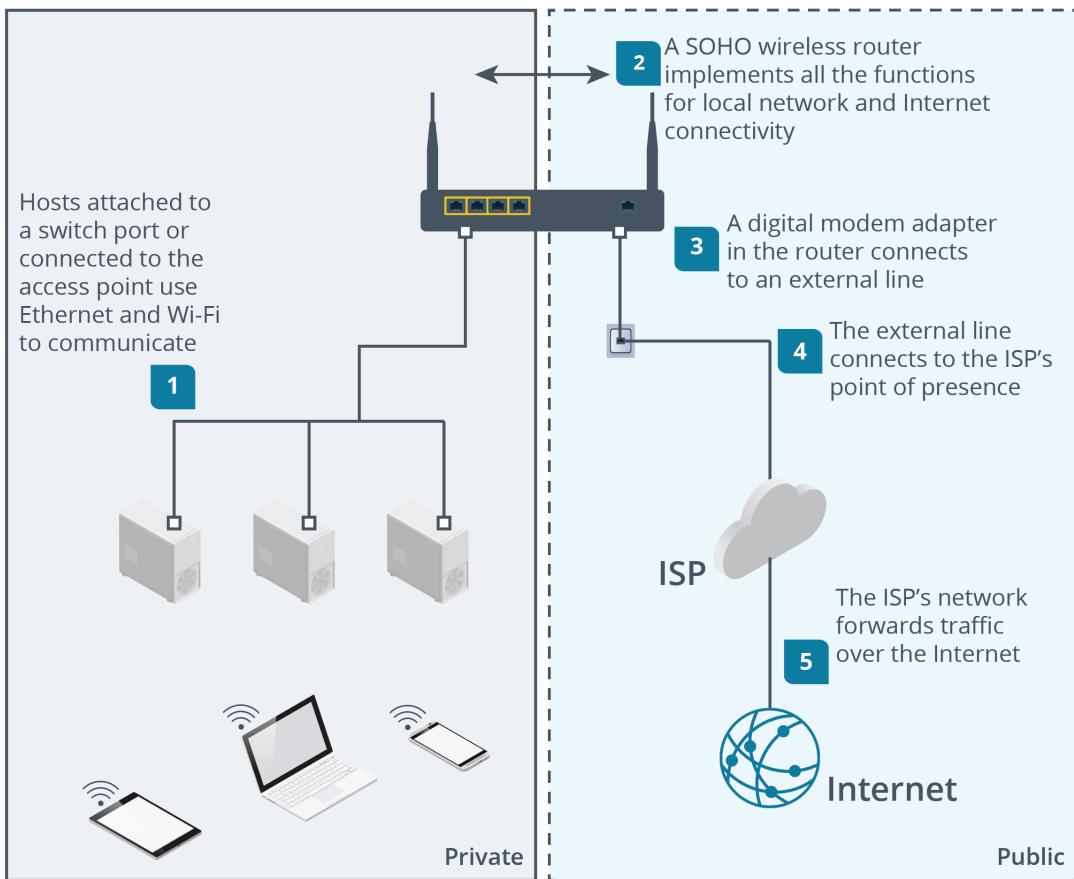
Internet Connection Types and Modems

The Internet is a global network of networks. The backbone of the Internet consists of high-bandwidth fiber optic links connecting [Internet exchange points](#) (IXPs). These trunk links and IXPs are mostly created by telecommunications companies and academic institutions. Within the datacenter supporting any given IXP, Internet [service providers](#) establish high-speed links between their networks, using transit and peering arrangements to carry traffic to and from parts of the Internet they do not physically own. There is a tiered hierarchy of ISPs that establishes to what extent they depend on transit arrangements with other ISPs.

Customers connect to the Internet via an ISP's network. The connection to the ISP's network uses its nearest point of presence (PoP), such as a local telephone exchange. An **Internet connection type** is the media, hardware, and protocols used to link the local network at a domestic residence or small office to the ISP's PoP. This WAN interface is typically a point-to-

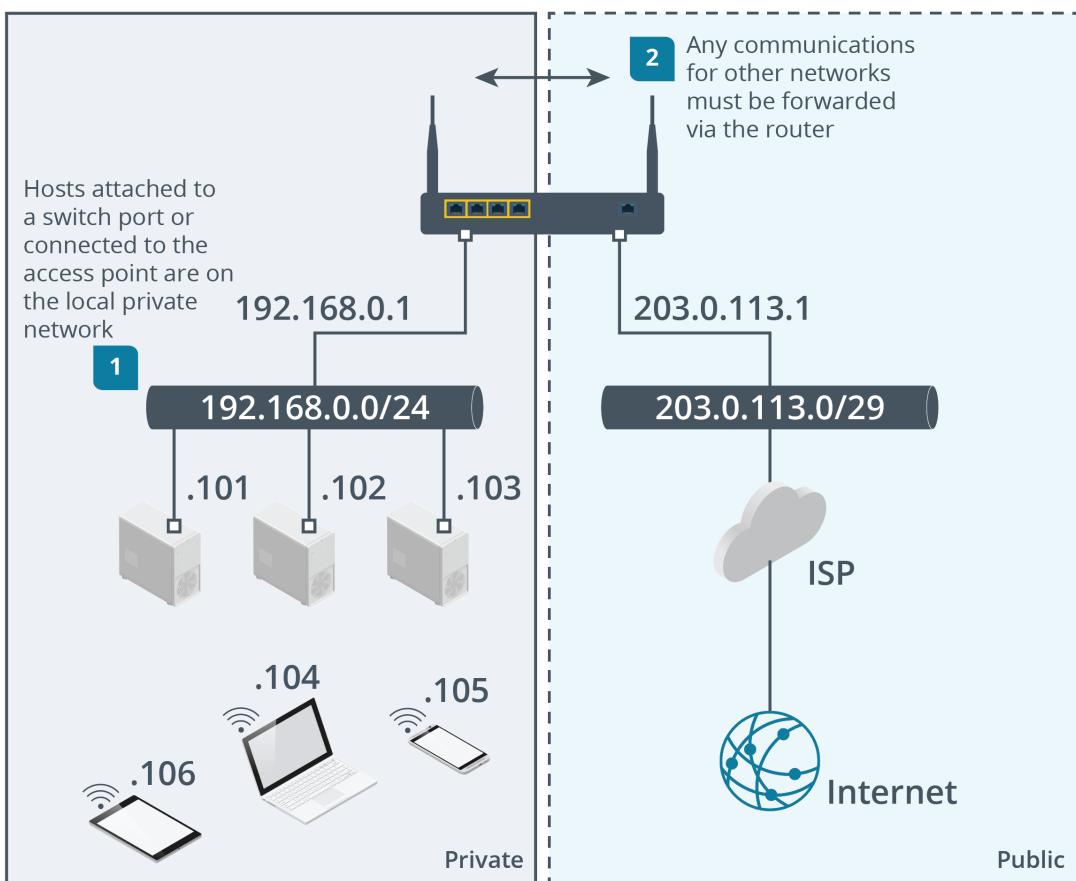
point connection. This means that there are only two devices connected to the media (unlike Ethernet). Where Ethernet connections are made using NICs and switches, the connection to a WAN interface is typically made by a type of digital modem.

Role of a digital modem to connect a local network to an ISP's network for Internet access



The modem establishes the physical connection to the WAN interface, but when interconnecting networks, there must also be a means of identifying each network and forwarding data between them. This function is performed by a router that implements the Internet Protocol (IP).

Role of the router and Internet Protocol (IP) in distinguishing logical networks



Digital Subscriber Line Modems

Many internet connection types make use of the national and global telecommunications network referred to as the [public-switched-telephone-network](#). The core of the PSTN is fiber optic, but at its edge, it is still often composed of legacy, two-pair copper cabling. This low-grade copper wire segment is referred to as the [plain-old-telephone-system](#), "local loop," or "last mile."

[Digital-subscriber-line](#) uses the higher frequencies available in these copper telephone lines as a communications channel. The use of advanced modulation and echo canceling techniques enables high-bandwidth, full-duplex transmissions.

There are various "flavors" of DSL, notably asymmetrical and symmetrical types:

- Asymmetrical DSL (ADSL) provides a fast downlink, but a slow uplink. There are various iterations of ADSL, with the latest (ADSL2+) offering downlink rates up to about 24 Mbps and uplink rates of 1.4 Mbps or 3.3 Mbps.
- Symmetric versions of DSL offer the same uplink and downlink speeds. These are of more use to businesses and for branch office links, where more data is transferred upstream than with normal Internet use.

The customer network is connected to the telephone cabling via a DSL modem. The DSL modem might be provisioned as a separate device or as an embedded function of a Small Office, Home Office (SOHO) router. On a standalone DSL modem, the RJ11 WAN port on the modem connects to the phone point. The RJ45 interface connects the modem to the router.

RJ11 DSL (left) and RJ45 LAN (right) ports on a DSL modem



Image © 123RF.com.

A filter (splitter) must be installed in each phone socket to separate voice and data signals. These can be self-installed on each phone point by the customer. Modern sockets are likely to feature a built-in splitter.

A self-installed DSL splitter

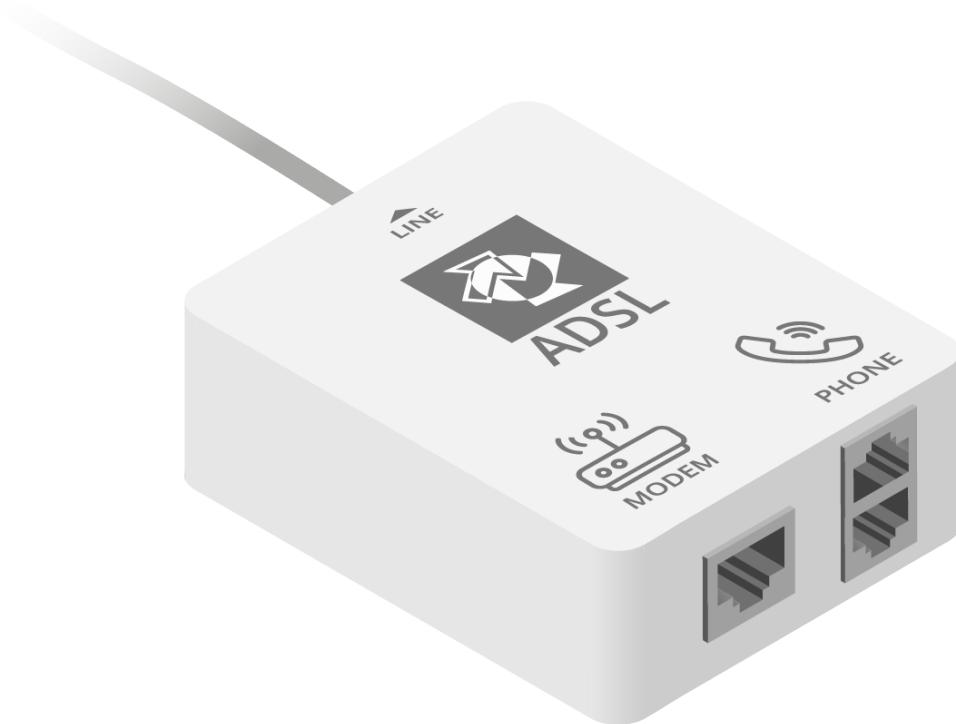


Image © 123RF.com.

Cable Modems

A cable Internet connection is usually available as part of a cable access TV (CATV) service. A CATV network is often described as a hybrid fiber coax (HFC), as it combines a fiber optic core network with copper coaxial cable links to customer premises equipment. It can also be described as broadband cable or just as cable. Cable based on the Data Over Cable Service Interface Specification (DOCSIS) supports downlink speeds of up to 42.88 Mbps (North America) or 55.62 Mbps (Europe) and uplinks of up to 30.72 Mbps. DOCSIS version 4 allows the use of multiplexed channels to achieve higher bandwidth with up to 10 Gbps downlink and up to 6 Gbps uplink.

Installation of a [cable modem](#) follows the same general principles as for a DSL modem. The cable modem is interfaced to the local router via an RJ45 port and with the access provider's network by a short segment of coax terminated using threaded F-type connectors. More coax then links all the premises in a street with a cable modem termination system (CMTS), which forwards data traffic via the fiber backbone to the ISP's point of presence and from there, to the internet.

A cable modem: The RJ45 port connects to the local network router, while the coax port connects to the service provider network



Image © 123RF.com.

An F-type connector is screwed down to secure it. Do not overtighten it.



Fiber to the Curb and Fiber to the Premises

The major obstacle to providing internet access that can perform like a LAN is bandwidth in the last mile, where the copper wiring infrastructure is often low-grade. The projects to update this wiring to use **fiber** optic links are referred to by the umbrella term fiber to the X (FTTx).

Fiber to the Curb and VDSL

A **fiber to the curb** (FTTC) solution retains some sort of copper wiring to the customer premises while extending the fiber link from the point of presence to a communications cabinet servicing multiple subscribers. The service providers with their roots in telephone networks use very high-speed DSL (VDSL) to support FTTC. VDSL achieves higher bit rates than other DSL types at the expense of range. It allows for both symmetric and asymmetric modes. Over 300 m (1,000 feet), an asymmetric link supports 52 Mbps downstream and 16 Mbps upstream, while a symmetric link supports 26 Mbps in both directions. VDSL2-Vplus specifies a very short range (250 m/820 feet) rate of 300 Mbps download and 100 Mbps upload.



Note: DSL modems are not interchangeable. An ADSL modem is unlikely to support VDSL, though most VDSL modems support ADSL.

Fiber to the Premises and Optical Network Terminals

A **fiber to the premise** (FTTP) Internet connection means that the service provider's fiber optic cable is run all the way to the customer's building. This full fiber connection type

is implemented as a passive optical network (PON). In a PON, a single fiber cable is run from an optical line terminal (OLT) to a splitter. The splitter directs each subscriber's traffic over a shorter length of fiber to an [optical network terminal](#)(ONT) installed at the customer's premises. The ONT converts the optical signal to an electrical one. The ONT is connected to the customer's router using an RJ45 copper wire patch cord or may contain the router within the same physical hardware device.

Optical network terminal—the PON port terminates the external fiber cable and the LAN ports connect to local routers or computers over RJ45 patch cords

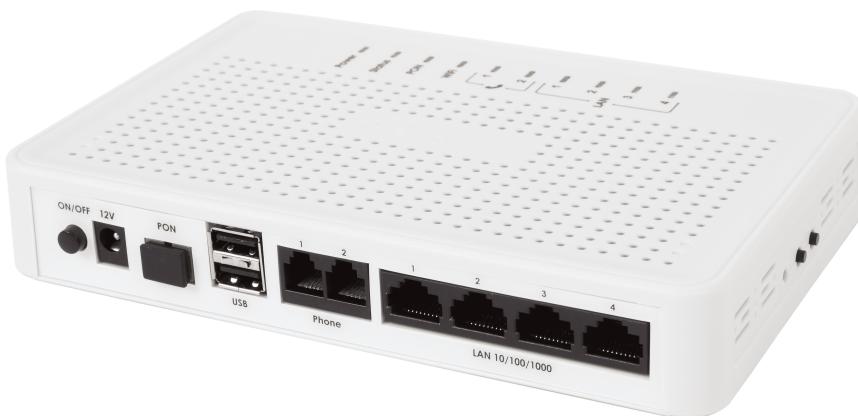


Image by artush © 123RF.com

Fixed Wireless Internet Access

Wired broadband internet access is not always available, especially in rural areas or older building developments, where running new cable capable of supporting DSL or full fiber is problematic. In this scenario, some sort of fixed wireless internet access might be an option.

Geostationary Orbital Satellite Internet Access

A [satellite](#)-based microwave radio system provides far bigger areas of coverage than can be achieved using other technologies. The transfer rates available vary between providers and access packages, but 2 or 6 Mbps up and 30 Mbps down would be typical.

One drawback of satellites placed in a high geostationary orbit is increased latency. The signal must travel over thousands of miles more than terrestrial connections, introducing a delay of many times what might be expected over a land link. For example, if accessing an internet web server over DSL involves a 10–20 ms round trip time (RTT) delay on the link, accessing the same site over a satellite link could involve a 600–800 ms RTT delay. This is an issue for real-time applications, such as video conferencing, VoIP, and multiplayer gaming.



Note: RTT is the two-way latency, or the time taken for a probe to be sent and a response to be received.

To create a satellite internet connection, the ISP installs a very small aperture terminal (VSAT) satellite dish antenna at the customer's premises and aligns it with the orbital satellite. The satellites are in high geostationary orbit above the equator, so in the northern hemisphere, the dish will be pointing south. Because the satellite does not move relative to the dish, there should be no need for any realignment. The antenna is connected via coaxial cabling to a Digital Video Broadcast Satellite (DVB-S) modem.

Low Earth Orbital Satellite Internet Access

A different type of service uses an array of satellites positioned in low Earth orbit (LEO). LEO satellites support better bandwidth (around 5–220 Mbps at the time of writing) and have lower latency (25–60 ms RTT). The drawback is that the satellites move relative to the surface of the Earth. The customer's premises antenna may be provisioned with a motor so that it can periodically realign with the array. The dish construction uses a technology called "phased array" to connect to different satellites as they pass overhead and minimize the amount of mechanical realignment required. The antenna must have a clear view of the whole sky. New providers have entered this market recently, and their systems utilize a flat panel-like antenna that does not require a motor. The user simply uses an application to point the panel in the correct direction. The plan is to provide global coverage to customers with a single service provider. These providers also use multiple constellations, or groups, of satellites to provide seamless coverage.

Wireless Internet Service Providers

A [wireless internet service provider](#) (WISP) uses ground-based, long-range, fixed-access wireless technology. The WISP installs and maintains a directional antenna to work as a bridge between the customer's network and the service provider. A WISP might use Wi-Fi type networking or proprietary equipment and licensed or unlicensed frequency bands.

A fixed-access wireless link is often low latency, or at least lower latency than a satellite. A disadvantage of fixed access wireless is that the actual unobstructed line of sight between the two antennas can be difficult to maintain. If the provider uses unlicensed frequencies, there are risks of interference from other wireless networks and devices.



Note: All types of microwave radio links can be adversely affected by snow, rain, high winds, and even solar flares from the sun.

Cellular Radio Internet Connections

The 2.4, 5, and 6 GHz frequency bands used by Wi-Fi have limited range, while fixed wireless internet requires a large dish antenna. [Cellular radio](#) wireless networking facilitates communications cover much larger distances using mobile devices. Cellular networking is also used by some Internet of Things (IoT) devices, such as smart energy meters. Cellular digital communications standards are described as belonging to a particular generation.

3G

A 3G cellular radio makes a connection to the closest base station. The area served by each base station is referred to as a "cell." Cells can have an effective range of up to 5 miles (8 km), though signals can be obstructed by building materials. A 3G cellular radio typically works in the 850 and 1,900 MHz frequency bands (mostly in the Americas) and the 900 and 1,800

MHz bands (rest of the world). These lower-frequency waves do not need so much power to propagate over long distances.

- With 3G cellular, there are two competing formats established in different markets: GSM or [global system for mobile communication](#)-based phones. GSM allows subscribers to use a removable subscriber identity module (SIM) card to use an unlocked handset with their chosen network provider.
- CDMA, or **code division multiple access**-based handsets. With CDMA, the handset is directly managed by the provider and there is no removable SIM card.

The type of data connection is represented by a code in the device's status bar. G, E, and 1X represent minimal service levels, with connection speeds of 50-400 Kbps only. The following codes represent 3G services:

- 3G—Universal Mobile Telecommunications Service (UMTS) on a GSM handset or Evolution-Data Optimized (EV-DO) on CDMA networks, working at up to around 3 Mbps.
- H/H+—High Speed Packet Access (HSPA) provides improved data rates on GSM networks. Nominally, HSPA+ can work at up to 42 Mbps, but real-world performance is likely to be lower.

4G

Long-Term Evolution (LTE) is a series of converged 4G standards supported by both the GSM and CDMA network providers. LTE devices must have a SIM card issued by the network provider installed. LTE cellular networks typically operate between 600 and 2500 MHz frequency bands in the Americas and 700 and 2600 MHz elsewhere.

5G

The 5G standard uses different spectrum bands from low (sub-6 GHz) to medium/high (20–60 GHz). Low bands have greater range and penetrating power; higher bands, also referred to as millimeter wave (mmWave), require close range (a few hundred feet) and cannot penetrate walls or windows. Consequently, design and rollout of 5G services is relatively complex. Rather than a single large antenna serving a wide area wireless cell, 5G involves installing many smaller antennas to form an array that can take advantage of multipath and beamforming to overcome the propagation limitations of the spectrum. This technology is referred to as massive multiple input multiple output (mMIMO).

As well as faster speeds for mobile device internet connections, 4G and 5G can be used as fixed-access wireless broadband solutions for homes and businesses and to support IoT networks.

Routers

The devices discussed so far enable physical links where the only type of addressing used identifies a host's hardware interface.

Ethernet switches and Wi-Fi access points forward frames using MAC addresses. A network segment is where hosts can send frames to one another using just their MAC addresses.

Digital modems, ONTs, and cellular radios transmit data over DSL, cable, fiber, satellite, and cellular links to connect a local network or device to an ISP. This is typically a point-to-point link and so does not require unique interface addressing. These network segments use different media types and have no physical or logical means of communicating with one another.

When you want to connect a local network to the internet, you need to use a protocol that can distinguish between the private LAN and public WAN and an intermediate system with

interfaces in both networks. The primary protocol used to implement this is the Internet Protocol (IP), and the intermediate system is a [router](#).

A router



Image © 123RF.com.

Whereas a switch forwards frames using MAC (hardware) addresses, a router forwards packets through the internet using IP addresses. A MAC address only identifies a hardware port. An IP address contains the identity of both the network and a single host within that network.

There are several types of routers and different uses for them. A SOHO router often simply routes between its local network interface and its WAN/Internet interface. An enterprise network is likely to use different router models to perform different routing tasks:

- A LAN router divides a single physical network into multiple logical subnetworks. Each logical subnetwork becomes a separate broadcast domain. Having too many hosts in the same broadcast domain reduces performance. There is also a security benefit because traffic passing from one logical network to another can be subject to filtering rules. This type of router generally has only Ethernet interfaces.
- A WAN or border router forwards traffic to and from the Internet or over a private WAN link. This type of router has an Ethernet interface for the local network and a digital modem interface for the WAN.

Firewalls

Once you have joined public and private networks using a router, you then need to control which computers are allowed to connect to them and which types of traffic you will accept. The role of filtering allowed and denied hosts and protocols is performed by a network [firewall](#). A basic firewall is configured with rules, referred to as a network access control list (ACL).

Each entry in the ACL lists source and/or destination network addresses and protocol types and whether to allow or block traffic that matches the rule.

Firewalls can also be deployed within a private network. For example, you might only want certain clients to connect to a particular group of servers. You could place the servers behind a local network firewall to enforce the relevant ACL.

Most routers can implement some level of firewall functionality. A firewall can also be implemented as a standalone appliance. These dedicated appliances can perform deeper analysis of application protocol data and use more sophisticated rules to determine what traffic is allowed. They are often implemented as unified threat management (UTM) appliances to perform multiple other security functions.

Sample ruleset configured on the OPNsense open-source firewall implementation

Firewall: Rules: WAN									Select category	Inspect
	Protocol	Source	Port	Destination	Port	Gateway	Schedule	Description		
									Automatically generated rules	
									Block bogon IPv4 networks from WAN	
									Block bogon IPv6 networks from WAN	
			10.0.0.0/8,127.0.0.0/8,100.64.0.0/10,172.16.0.0/12,192.168.0.0/16						Block private networks from WAN	
									Block private networks from WAN	
			fc00::/7						Allow ping to firewall interface	
			* ICMP		* This Firewall				Allow web access (unencrypted)	
			* IPv4 TCP		* SCREENED net		80 (HTTP)		Allow SMTP access from secure mail gateway	
			* IPv4 TCP MAILHOSTS		* SCREENED net		25 (SMTP)			
	pass	block	reject	log	in			first match		
	pass (disabled)	block (disabled)	reject (disabled)	log (disabled)	out			last match		

Lesson 6B

TCP/IP Concepts

Lesson Overview

The Transmission Control Protocol/Internet Protocol (TCP/IP) suite is used to perform logical addressing and data forwarding functions on most networks. As a CompTIA A+ technician, you must be able to configure these protocols on PCs and SOHO routers to implement fully functional local networks with Internet connectivity.



Objectives Covered

2.6 Given a scenario, configure basic wired/wireless small office/home office (SOHO) networks.

Learning Outcomes

As you study this lesson, answer the following questions:

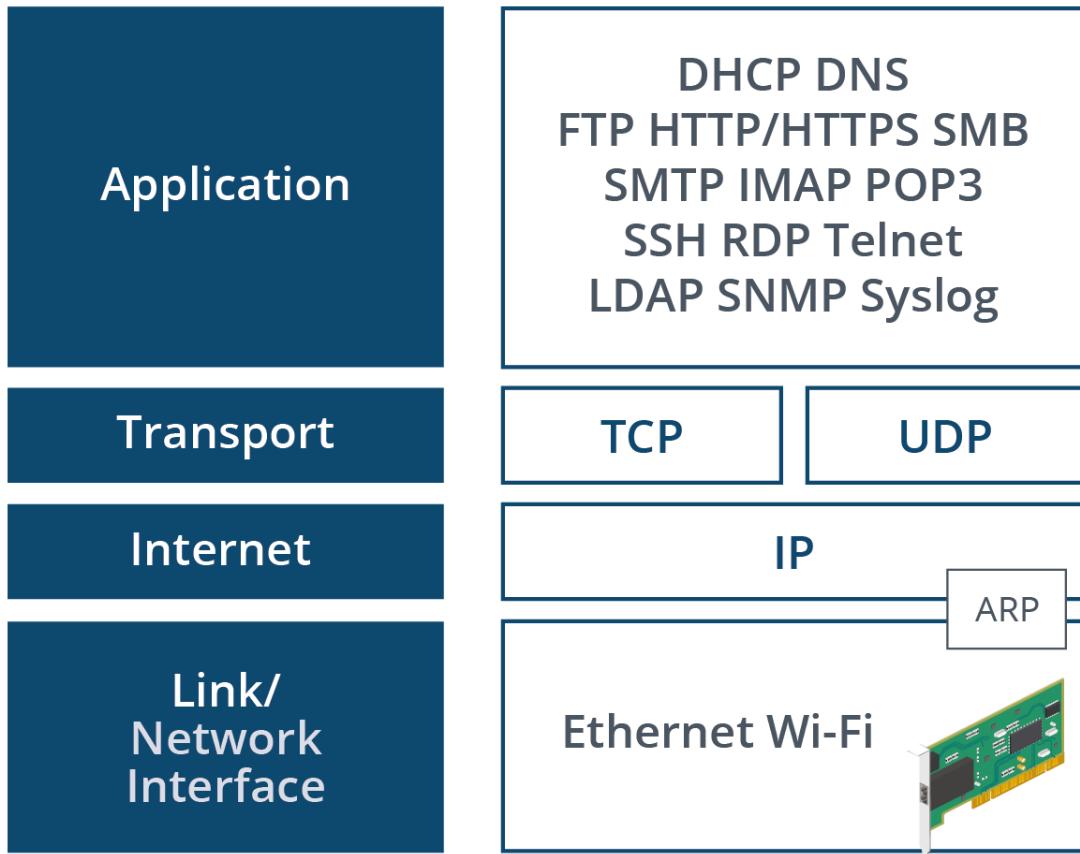
- What are the layers of the TCP/IP model?
- What are the differences in IPv4 and IPv6?
- What are the IPv4 classes of addresses?
- How does DHCP allocate IP addresses and what happens if it fails?

TCP/IP

A protocol is a set of rules that allows networked hosts to communicate data in a structured format. Often, several protocols used are designed to work together as a protocol suite. Most networks have converged on the use of the [Transmission Control Protocol Internet Protocol](#) suite. The function of each protocol can be better understood by dividing network functions into layers. Protocols operating at lower layers are said to encapsulate data from higher protocols. Each protocol adds its own header fields to data it is transporting from an upper-layer protocol.

The TCP/IP suite uses a model with four distinct layers.

TCP/IP model



Link or Network Interface layer

The Link layer is responsible for putting frames onto the physical network. This layer does not contain TCP/IP protocols as such. At this layer, different local networking products and media can be used, such as Ethernet or Wi-Fi. WAN interfaces, such as DSL and cable modems, also work at the Link layer.

Communications on this layer take place only on a local network segment and not between different networks. On an Ethernet or Wi-Fi segment, data at the link layer is packaged in a unit called a frame, and node interfaces are identified by a MAC address.

Internet Layer

The **internet protocol** provides packet addressing and routing within a network of networks. A PC, laptop, mobile device, or server that can communicate on an IP network is generically referred to as an "end system host." For data to be sent from one IP network to another, it must be forwarded by an intermediate system (a router).

When IP is being used with a physical/data link specification, such as Ethernet or Wi-Fi, there must be a mechanism to deliver messages from IP at the Internet layer to host interfaces addressed at the Link layer. This function is performed by the Address Resolution Protocol (ARP), which allows a host to query which MAC address is associated with an IP address.

IP provides best-effort delivery that is unreliable and connectionless. A packet might be lost, delivered out of sequence, duplicated, or delayed.

Transport Layer

Where the Internet layer deals with addressing, the Transport layer determines how each host manages multiple connections for different application layer protocols at the same time. The transport layer is implemented by one of two protocols:

- [Transmission control protocol](#) (TCP) guarantees connection-oriented forwarding of packets. TCP can identify and recover from lost or out-of-order packets, mitigating the inherent unreliability of IP. This is used by most TCP/IP application protocols, as failing to receive a packet or processing it incorrectly can cause serious data errors.
- [User datagram protocol](#) (UDP) provides unreliable, connectionless forwarding. UDP is faster and comes with less of a transmission overhead because it does not need to send extra information to establish reliable connections. It is used in time-sensitive applications, such as speech or video, where a few missing or out-of-order packets can be tolerated. Rather than causing the application to crash, they would just manifest as a glitch in video or a squeak in audio.

Application Layer

The Application Layer contains protocols that perform some high-level function, rather than simply addressing hosts and transporting data. There are numerous application protocols in the TCP/IP suite. These are used to configure and manage network hosts and to operate services, such as the web and email. Each application protocol uses a TCP or UDP port to allow a client to connect to a server.

 TCP/IP was originally developed by the US Department of Defense but is now an open standard to which anyone may contribute. Developments are implemented through the Internet Engineering Task Force (IETF), which is split into working groups. Standards are published as Request For Comments (RFCs). The official repository for RFCs is at rfc-editor.org.

IPv4 Addressing

The core protocol in TCP/IP is the [internet protocol](#), which provides network and host addressing and packet forwarding between networks. An IP packet adds some headers to whatever transport/application layer data it is carrying in its payload. Two of the most important header fields are the source and destination IP address fields.

There are two versions of IP: [IPv4](#) and [IPv6](#). An IPv4 address is 32 bits long. In its raw form, it appears as:

```
11000000101010000000000000000001
```

The 32 bits can be arranged into four groups of eight bits (one byte) known as "octets." The above IP address could therefore be rearranged as:

```
11000000 10101000 00000000 00000001
```

This representation of an IP address is difficult for a human to memorize or to enter correctly into configuration dialog. To make IP addresses easier to use, they are used in dotted decimal

notation. This notation requires each octet to be converted to a decimal value. The decimal numbers are separated using a period. Converting the previous number to this notation gives:

192.168.0.1

Dotted decimal notation

11000000

10101000

00000000

00000001

192

.

168

.

0

.

1

If all the bits in an octet are set to 1, the number obtained is 255 (the maximum possible value). Similarly, if all the bits are set to 0, the number obtained is 0 (the minimum possible value). Therefore, theoretically, an IPv4 address may be any value between 0.0.0.0 and 255.255.255.255. However, some addresses are not permitted or are reserved for special use.

Network Prefixes

An IPv4 address provides two pieces of information encoded within the same value:

- The network number (network ID) is common to all hosts on the same IP network.
- The host number (host ID) identifies a host within a particular IP network.

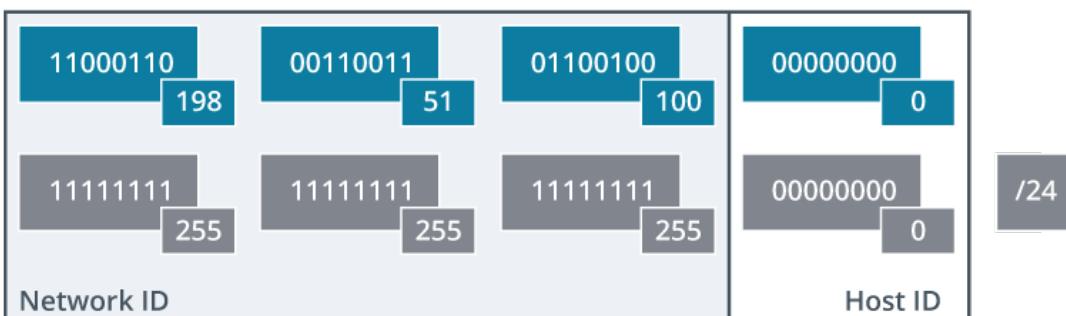
These two components within a single IP address are distinguished by combining the address with a network prefix. A prefix is a 32-bit value with a given number of contiguous bits all set to 1. For example, a prefix with 24 bits is the following binary value:

11111111 11111111 11111111 00000000

This can be written in slash notation in the form /24. The prefix can also be expressed in dotted decimal as a [network mask](#):

255.255.255.0

Network ID and Host ID



Network ID and host ID portions when using a 24-bit mask.

Note: The name "subnet mask" comes about because a single IP network can be divided into multiple logical subnetworks (subnets) using this method.

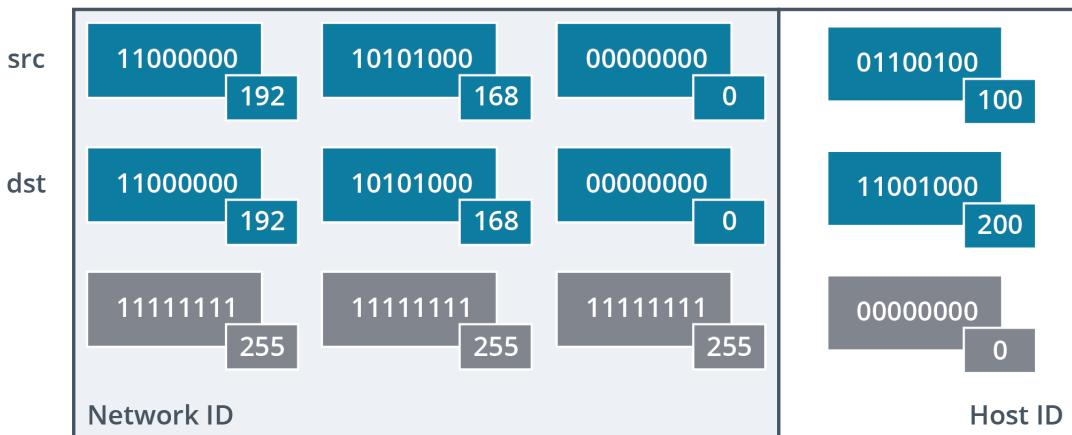
When combined with an IP address, the prefix masks the host ID portion to reveal the network ID portion. Where there is a binary 1 in the prefix, the corresponding binary digit in the IP address is part of the network ID.

Note: Slash notation is used to refer to network IDs, while the subnet mask is typically used in host configuration dialog. For example, 192.168.0.0/24 refers to an IP network, while 192.168.0.1/255.255.255.0 refers to a host address on that IP network.

IPv4 Forwarding

When a host attempts to send a packet via IPv4, the protocol compares the source and destination IP address in the packet against the sending host's subnet mask. If the masked portions of the source and destination IP addresses match, then the destination interface is assumed to be on the same IP network or subnet. For example:

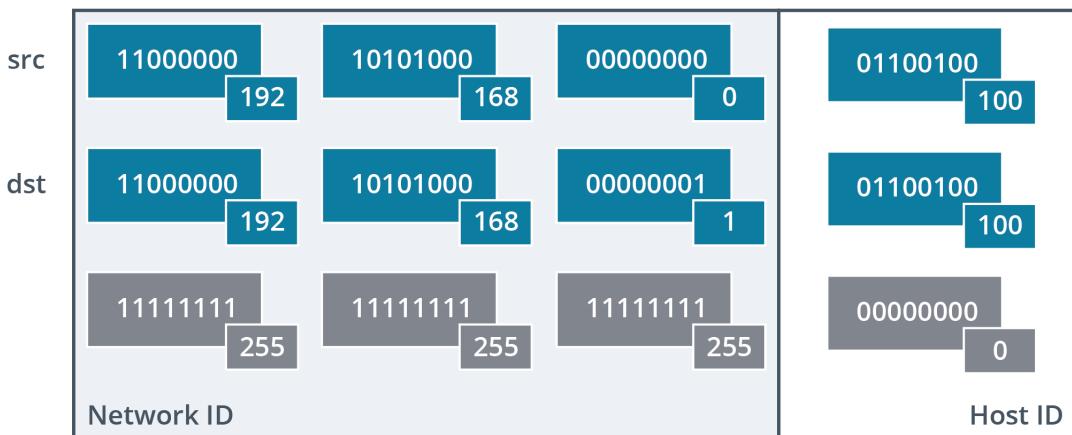
Matching source and destination network IDs



In the example, the host will determine that the destination IPv4 address is on the same IP network (192.168.0.0/24) and try to deliver the packet locally. On Ethernet, the host would use the address resolution protocol (ARP) to identify the MAC address associated with the destination IP address.

If the masked portion does not match, the host assumes that the packet must be routed to another IP network. For example:

Different source and destination network IDs



In this case, the source host 192.168.0.100 identifies that the destination IPv4 address is on a different IP network (192.168.1.0/24). Consequently, it forwards the packet to a router rather than trying to deliver it locally. Most hosts are configured with a default gateway parameter. The default gateway is the IP address of a router interface that the host can use to forward packets to other networks. The default gateway must be in the same IP network as the host.

Public and Private Addressing

To communicate on the Internet, a host must be configured with a unique **public**, versus a **private address**. Public addresses are allocated to customer networks by the ISP. Relatively few companies can obtain sufficient public IPv4 addresses for all their computers to communicate over the Internet, however. There are various mechanisms to work around the shortage of available public addresses.

Private Address Ranges

The IPv4 address scheme defines certain ranges as reserved for **private** addressing, often called "RFC 1918" addresses after the document in which they were published. Hosts with IP addresses from these ranges are not allowed to route traffic over the public Internet. Use of the addresses is confined to private LANs. There are three private address ranges:

- 0.0.0 to 10.255.255.255 (Class A private address range).
- 16.0.0 to 172.31.255.255 (Class B private address range).
- 168.0.0 to 192.168.255.255 (Class C private address range).

Address Classes and Default Subnet Masks

The address classes (A, B, and C) derive from the earliest form of IP. When first defined, IP did not include the concept of subnet masks. Hosts would identify the network ID just by using the address class. The subnet masks that align precisely with octet boundaries mirror this functionality. They are often referred to as the "default masks".

Class	1st Octet Range	Dotted Decimal Mask	Network Prefix	Binary Mask
A	0-127	255.0.0.0	/8	11111111 00000000 00000000 00000000
B	128-191	255.255.0.0	/16	11111111 11111111 00000000 00000000
C	192-223	255.255.255.0	/24	11111111 11111111 11111111 00000000



Note: There are two other classes not listed here, as they are reserved for special purposes. Class D is utilized for multicast groups and has a first octet range from 224-239. Class E IPv4 addresses are reserved for experimental and future use. Those addresses range from 240-255 in the first octet.

Internet Access Using Private Addressing

As a host configured with a private address cannot access the Internet directly, some mechanism must be used to allow it to forward packets. Internet access can be facilitated for hosts using a private addressing scheme in two ways:

- Through a router configured with a single or block of valid public addresses; the router uses [network address translation](#)(NAT) to convert between private and public addresses.
- Through a proxy server that fulfills requests for Internet resources on behalf of clients.

IPv4 Host Address Configuration

Each host must be configured with an IP address and subnet mask at a minimum to communicate on an IPv4 network. This minimum configuration will not prove very usable, however. Several other parameters must be configured for a host to make full use of an enterprise network or the Internet. There are also different ways to supply this configuration information to hosts.

An IPv4 address and subnet mask can be set manually in a static configuration:

- The IPv4 address is entered as four decimal numbers separated by periods, such as 192.168.0.100.
- The subnet mask is entered in dotted decimal notation, such as 255.255.255.0. When used with the IP address 192.168.0.100, this mask identifies 192.168.0 as the network ID, and means that the last octet (.100) is the host ID. Alternatively, this parameter might be entered as the mask length in bits.

Configuring a Windows 10 host to use a static IP address configuration. Note that this dialog uses a prefix length parameter rather than requiring the subnet mask in dotted decimal format.

IPv4



IP address

192.168.0.2

Subnet prefix length

24

Gateway

192.168.0.1

Preferred DNS

192.168.0.1

Alternative DNS

8.8.8.8

IPv6

Save

Cancel

Screenshot courtesy of Microsoft.

At the top, there is a toggle switch labeled IP v 4, which is turned on. Below, there are input fields for network configuration. IP address: 192.168.0.2. Subnet prefix length: 24 Gateway: 192.168.0.1. Preferred DNS: 192.168.0.1. Alternative DNS: 8.8.8.8 At the bottom of the interface, there are two buttons labeled Save and Cancel.



A host cannot be assigned either the first or last address in an IP network. For example, in the IP network 192.168.0.0/24, 192.168.0.0 is the first address and is used to identify the network itself. The last address 192.168.0.255 is used to broadcast to all hosts. Valid host addresses range from 192.168.0.1 to 192.168.0.254.

Two other parameters are typically configured to make the host fully functional:

- The default **gateway** parameter is the IPv4 address of a router, such as 192.168.0.1. This is the IP address to which packets destined for a remote network should be sent by default. This setting is not compulsory, but failure to enter a gateway would limit the host to communication on the local network only.
- One or more **domain name system (DNS)** server IPv4 addresses. These servers provide the resolution of host and domain names to their IP addresses and are essential for locating resources on the Internet. Most local networks also use DNS for name resolution. Typically, the primary DNS server address would be configured as the same as the gateway address. The router would be configured to forward DNS queries to a secure resolver. Often two DNS server addresses (preferred and alternate) are specified for redundancy.

Static Versus Dynamic Host Address Configuration

Using **static** addressing requires an administrator to visit each system to manually enter the configuration information for that host. If the host is moved to a different IP network or subnet, the administrator must manually reconfigure it. The administrator must keep track of which IP addresses have been allocated to avoid issuing duplicates. In a large network, configuring IP statically on each node can be very time-consuming and prone to errors that can potentially disrupt communication on the network.

Static addresses are typically only assigned to systems with a dedicated functionality, such as router interfaces or application servers that need to use a fixed IP address.

Dynamic Host Configuration Protocol

As an alternative to static configuration, a host can receive its IP address, subnet mask, default gateway, and DNS server addresses from a [Dynamic Host Configuration Protocol \(DHCP\)](#) server.

DHCP server configuration

The screenshot shows the TP-LINK Archer VR900 router's configuration interface. The top bar has tabs for Quick Setup, Basic, and Advanced. The top-right corner has Logout and Reboot options. The left sidebar shows a menu with Status, Operation Mode, Network (selected), Internet, LAN Settings (highlighted in blue), Interface Grouping, DSL Settings, Dynamic DNS, Advanced Routing, IPSec VPN, and IPTV. The main section is titled 'DHCP Server' and contains the following settings:

- IP Version: IPv4 (selected)
- MAC Address: 60:E3:27:CF:EA:CB
- LAN IPv4: 192.168.0.1
- Subnet Mask: 255.255.255.0
- IGMP Snooping: Enabled
- DHCP: Enabled
- DHCP Server (selected)
- IP Address Pool: 192.168.0.100 - 192.168.1.199
- Address Lease Time: 1440 minutes (1-2880)
- Default Gateway: 192.168.0.1 (Optional)
- Default Domain: (Optional)
- Primary DNS: 0.0.0.0 (Optional)
- Secondary DNS: 0.0.0.0 (Optional)

A green 'Save' button is located at the bottom right.

Screenshot courtesy of TP-Link.

The top bar has tabs Quick Setup, Basic, and Advanced. The top-right corner has options for Logout and Reboot. On the left sidebar, there is a menu with several options: Status, Operation Mode, Network (expanded to show LAN Settings, which is highlighted), Internet, Interface Grouping, D S L Settings, Dynamic D N S, Advanced Routing, I P Sec V P N, and I P T V. In the main section, the D H C P Server settings are displayed. The I P Version is set to I P v 4 (selected) with an option for I P v 6. The MAC Address of the router is shown as 60:E3:27:C F:E A:C B. The LAN I P v 4 address is 192.168.0.1, and the Subnet Mask is 255.255.255.0. There is an option for I G M P Snooping, which is enabled. The D H C P server is also enabled, as indicated by the checked box. The I P Address Pool for D H C P allocation is set from 192.168.0.100 to 192.168.1.199. The Address Lease Time is set to 1440 minutes (24 hours). The Default Gateway is 192.168.0.1 (optional). Other optional fields are Default Domain: Blank, Primary D N S: 0.0.0.0, and Secondary D N S: 0.0.0.0. At the bottom right, there is a Save button.

Automatic Private IP Addressing

Hosts have a failover mechanism for when the IP configuration specifies use of a DHCP server but the host cannot contact one. In this scenario, the computer selects an address at random from the range 169.254.0.1 to 169.254.255.254. Microsoft calls this **Automatic Private IP Addressing (APIPA)**. When a host is using an APIPA address, it can communicate with other hosts on the same network that are using APIPA but cannot reach other networks or communicate with hosts that have managed to obtain a valid DHCP lease.

Note: Other vendors and open-source products use the term "link local" rather than APIPA. Not all hosts use link-local addressing. Some may just leave the IP unconfigured or use the IP address 0.0.0.0 to indicate that the IPv4 address of the interface is not known.

SOHO Router Configuration

Unlike end-system host computers, a router has multiple interfaces. For example, a SOHO router has a public digital modem interface to connect to the ISP and a private Ethernet

interface on the LAN. Both interfaces must be configured with an IP address and subnet mask. The LAN interface is the address used by hosts as the default gateway parameter. It is also the address used to access the router's web management interface, such as <https://192.168.0.1> or <https://192.168.1.1>.

The router's public interface IP address is determined by the ISP. This must be an address from a valid public range, such as 203.0.113.1. Some Internet access packages assign a static IP or offer an option to pay for a static address. Otherwise, the public interface is dynamically configured using the ISP's DHCP server.

 In fact, 203.0.113.1 is not actually a valid public address. It is from a small range reserved for use as documentation and examples. However, in general terms, you can identify a public IPv4 address because it is *not* from a private range (10.x.y.z, 172.16–31.x.y, or 192.168.0–255.x), does not start with a zero, and is not a value of 224.x.y.z or above (the upper range of IP addresses is reserved for other types of addressing schemes).

To configure a SOHO router, first connect a computer to one of the device's RJ45 ports or join its wireless network using the default name (identified by a sticker on the back of the unit). Make sure the computer is set to obtain an IP address automatically. Wait for the DHCP server running on the router to allocate a valid IP address to the computer.

Use a browser to open the device's management URL, as listed in the documentation. This could be an IP address or a host/domain name:

<http://192.168.0.1>

<http://www.routerlogin.com>

It might use HTTPS rather than unencrypted HTTP. If you cannot connect, check that the computer's IP address is in the same range as the router's LAN IP.

Enter the default administrator username and password as listed in the documentation or printed on a sticker accompanying the router. The management software will prompt you to choose a new administrator password. Choose a strong password of at least 12 characters.

Most appliances use a wizard-based setup to connect to the Internet. The public IP address and DSL/cable link parameters are normally self-configuring. If manual configuration is required, obtain the settings from your ISP.

Configuring DSL modem settings

The screenshot shows the TP-LINK Archer VR900 management interface. The top navigation bar includes tabs for Quick Setup, Basic, and Advanced, with Advanced selected. On the far right are Logout and Reboot buttons. The left sidebar has a tree view with Status, Operation Mode, Network (selected), Internet (selected), LAN Settings, Interface Grouping, DSL Settings, Dynamic DNS, Advanced Routing, IPSec VPN, and IPTV. The main content area is titled 'WAN Interface' and contains a table with one row. The table columns are 'WAN Interface Name' (pppoe_ptm_101_0_d), 'VPI/VCI or VID' (101), 'Status' (Connected), 'Operation' (Disconnect), and 'Modify' (pencil icon). Below the table is the 'Internet Connection Setup' section. It shows 'DSL Modulation Type: VDSL', 'VLAN ID: 101', and 'Internet Connection Type: PPPoE'. The 'Username' field contains 'broadband.user@btbroa'. The 'Password' and 'Confirm password' fields are empty. Under 'Connection Mode', the radio button for 'Always on' is selected, while 'Connect on demand' and 'Connect manually' are unselected.

Screenshot courtesy of TP-Link.

The top bar has tabs Quick Setup, Basic, and Advanced. The top-right corner has options for Logout and Reboot. On the left sidebar, there is a menu with several options: Status, Operation Mode, Network (expanded to show Internet which is highlighted, L A N Settings, Interface Grouping, D S L Settings, Dynamic DNS, Advanced Routing, IPSec V P N), and I P T V. The main content area displays the WAN Interface. A table at the top lists a single WAN interface with a name V LAN I D as 101, status as Connected, and an option to Disconnect. There is also a Modify button represented by a small pencil icon. Below the table, the Internet Connection Setup section shows details for configuring the internet connection. It includes: D S L Modulation Type: V D S L V LAN I D: 101 Internet Connection Type: P P P o E Username: broadband dot user at the rate b t broad Password and Confirm Password fields are left blank. Connection Mode: Always on is selected, with options to Connect on demand or Connect manually also available.

You can also use the management console to view line status and the system log. These might be required by the ISP to troubleshoot any issues with the connection.

Viewing DSL line status

The screenshot shows the TP-LINK Archer VR900 configuration interface. The top navigation bar includes tabs for Quick Setup, Basic, and Advanced, along with Logout and Reboot options. On the left, a sidebar lists various settings: Status (selected), Operation Mode, Network, IPTV, Wireless, Guest Network, NAT Forwarding, USB Settings, and Parental Control. The main content area is titled 'DSL' and displays the following information:

	Upstream	Downstream
Current Rate(kbps)	9999	35428
Max Rate(kbps)	19294	41045
SNR Margin(dB)	12.9	7.8
Line Attenuation(dB)	0	31.6
Errors(pkts)	0	0

Screenshot courtesy of TP-Link.

The top bar has tabs Quick Setup, Basic, and Advanced. The top-right corner has options for Logout and Reboot. On the left sidebar, there is a menu with several options: Status, Operation Mode, Network, I P T V, Wireless, Guest network, N A T Forwarding, U S B settings, and Parental Control. The main content area is titled, D S L. The Line Status is shown as Connected, with D S L Modulation Type listed as V D S L 2 and Annex Type as Annex A slash L slash M. A table below lists the Upstream and Downstream values. Current Rate in k b p s: Upstream is 9999 and Downstream is 35428. Max Rate in k b p s: Upstream is 19294 and Downstream is 41045. S N R Margin in decibels: Upstream is 12.9 and Downstream is 7.8. Line Attenuation in decibels: Upstream is 0 and Downstream is 31.6. Errors in packets: Both Upstream and Downstream show 0.

IPv6 Addressing

The pool of available IPv4 public addresses is not very large compared to the number of devices that need to connect to the Internet. While private addressing and NAT provide a workable solution, IP version 6 (IPv6) is intended to replace IPv4 completely at some point. An [IPv6](#) address is a 128-bit number and so can express exponentially more address values than the 32-bit number used in IPv4.

IPv6 Notation

IPv6 addresses are written in hexadecimal notation. One hex digit can represent a four-bit binary value (a nibble). To express a 128-bit IPv6 address in hex, the binary address is divided into eight double-byte (16-bit) values delimited by colons. For example:

```
2001:0db8:0000:0000:0abc:0000: def0:1234
```

To shorten how this is written and typed in configuration dialogs, where a double-byte contains leading zeros, they can be ignored. In addition, one contiguous series of zeroes can be replaced by a double colon place marker. Thus, the address above would become:

```
2001:db8::abc:0:def0:1234
```

IPv6 Network Prefixes

An IPv6 address is divided into two main parts: the first 64 bits are used as a network ID, while the second 64 bits designate a specific interface.

In IPv6, the interface identifier is always the last 64 bits; the first 64 bits are used for network addressing



As the network and host portions are fixed size, there is no need for a subnet mask. Network addresses are written using prefix notation, where /nn is the length of the routing prefix in bits. Within the 64-bit network ID, the length of any given network prefix is used to determine whether two addresses belong to the same IP network.

Note: For example, most ISPs receive allocations of /32 blocks and issue each customer with a /48 prefix for use on a private network. A /48 block allows the private network to be configured with up to 65,336 subnets.

Global and Link-Local Addressing

In IPv4, hosts generally have a single IP address per interface. IPv6 interfaces are more likely to be configured with multiple addresses. The main types are global and link-local:

- A global address is one that is unique on the Internet (equivalent to public addresses in IPv4). In hex notation, a global address starts with a 2 or with a 3.
- Link-local addresses are used on the local segment to communicate with neighbor hosts. In hex notation, link-local addresses start with fe80::

While it is possible to configure IPv6 addresses statically, most hosts obtain a global and link-local address via the local router. This process is referred to as StateLess Address Auto Configuration (SLAAC). IPv6 hosts do not need to be configured with a default gateway. IPv6 uses a protocol called Neighbor Discovery (ND). ND is used to implement SLAAC, allows a host to discover a router, and performs the interface address querying functions performed by ARP in IPv4.

Dual Stack

While IPv6 is designed to replace IPv4, transitioning from IPv4 has proved enormously difficult. Consequently, most hosts and routers can operate both IPv4 and IPv6 at the same time. This is referred to as "dual stack." Typically, a host will default to attempting to establish an IPv6 connection and fall back to IPv4 if the destination host does not support IPv6.

Lesson 6C

Network Communications

Lesson Overview

Communication protocols are similar to different languages from around the world. To make communication easier, each protocol has a unique set of parameters that are defined to allow two or more systems to communicate. If you are attempting to use Spanish to communicate with another person who does not understand the language, they will not understand you. By establishing a common communication format, global communication is made easier.



Objectives Covered

2.1 Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes

Learning Outcomes

As you study this lesson, answer the following questions:

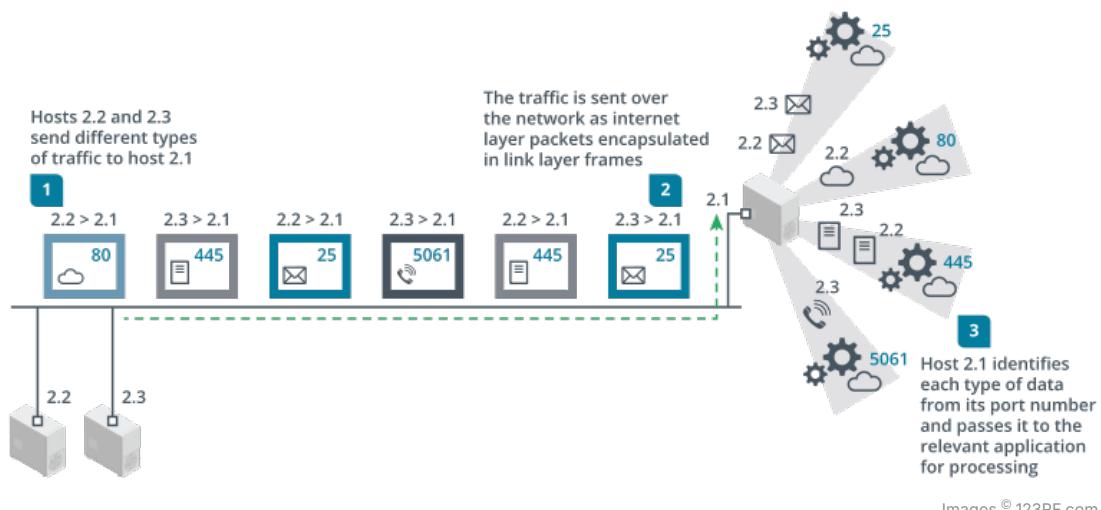
- What is the definition of TCP and UDP?
- How are TCP and UDP different as communication protocols?
- What are the standard communications protocols?
- What are the default port numbers configured for each protocol?

Protocols and Ports

The network hardware and protocols that we have covered to this point are primarily concerned with moving frames and packets between hosts and networks. At the Link layer, Ethernet allows hosts to send one another frames of data using MAC addresses. These frames would typically be transporting IP packets. At the Internet layer, IP provides addressing and routing functionality for a network of networks. The next layer up in the TCP/IP protocol stack is the Transport layer.

Any given host will be communicating with many other hosts using many different types of networking data. One of the functions of the Transport layer is to identify each type of network application. It does this by assigning each application a port number between 0 and 65535. For example, data addressed to the HTTP web browsing application can be identified as port 80, while data requesting an email transmission service can be identified as port 25. The host could be transmitting multiple HTTP and email segments at the same time. These are multiplexed using the port numbers onto the same network link.

Communications at the transport layer



Images © 123RF.com

! Each host assigns two port numbers. On the client, the destination port number is mapped to the service that the client is requesting (HTTP on port 80, for instance). The client also assigns a random source port number (47747, for instance). The server uses this client-assigned port number (47747) as the destination port number for its replies and its application port number (80 for HTTP) as its source port. This allows the hosts to track multiple "conversations" for the same application protocol.

In the TCP/IP suite, two different protocols implement this port assignment function: TCP and UDP.

Transmission Control Protocol

IP transmits a stream of application data as a series of packets. Any given packet could be damaged or fail to arrive due to faults or network congestion. TCP provides several mechanisms to overcome this lack of reliability. It is described as a "**connection-oriented**" protocol because it performs the following functions:

- Establishes a connection between the sender and recipient using a three-way handshake sequence of SYN, SYN/ACK, and ACK packets.
- Assigns each packet a sequence number so that it can be tracked.
- Allows the receiver to acknowledge (ACK) that a packet has been received.
- Allows the receiver to send a negative acknowledgment (NACK) to force retransmission of a missing or damaged packet.
- Allows the graceful termination of a session using a FIN handshake.

The main drawback is that this connection information requires multiple header fields. Using TCP can add 20 bytes or more to the size of each packet.

Observing the TCP handshake with the Wireshark protocol analyzer

Screenshot courtesy of Wireshark.

The top half of the screen shows a list of captured packets. Each row contains columns labeled Number, Time, Source, Destination, Protocol, Length, and Info. The middle section of the screenshot provides detailed information about the selected packet Packet 1. The analysis is divided into several layers: Internet Protocol Version 4 | IP v 4: Shows details like the source IP 10.1.0.101 and destination IP 10.1.0.2. Transmission Control Protocol T C P: Includes information about the source port 1624 and destination port 80. It lists the Sequence number

1, acknowledgment number 1, flags e.g., 0x010 for ACK, and window size 1024. The bottom section displays the raw hexadecimal and ASCII representation of the packet data. Hexadecimal values are displayed on the left, and the corresponding ASCII characters are shown on the right, where applicable.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.0...	10.1.0.101	10.1.0.2	TCP	66	1624 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256
2	0.0...	10.1.0.2	10.1.0.101	TCP	66	80 → 1624 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256
3	0.0...	10.1.0.101	10.1.0.2	TCP	54	1624 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
4	0.0...	10.1.0.101	10.1.0.2	HTTP	433	GET / HTTP/1.1
5	0.0...	10.1.0.2	10.1.0.101	TCP	54	80 → 1624 [ACK] Seq=1 Ack=380 Win=2102272 Len=0
6	0.2...	10.1.0.2	10.1.0.101	TCP	1514	80 → 1624 [ACK] Seq=1 Ack=380 Win=2102272 Len=1460 [HTTP/1.1 200 OK /index.html]
7	0.2...	10.1.0.2	10.1.0.101	HTTP	770	HTTP/1.1 200 OK /index.html


```

> Internet Protocol Version 4, Src: 10.1.0.101, Dst: 10.1.0.2
∨ Transmission Control Protocol, Src Port: 1624, Dst Port: 80, Seq: 1, Ack: 1, Len: 0
  Source Port: 1624
  Destination Port: 80
  [Stream index: 0]
  [TCP Segment Len: 0]
  Sequence number: 1    (relative sequence number)
  [Next sequence number: 1    (relative sequence number)]
  Acknowledgment number: 1    (relative ack number)
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x010 (ACK)
  Window size value: 1024
  [Calculated window size: 262144]
  [Window size scaling factor: 256]
0000 00 15 5d 01 ca 76 00 15 5d 01 ca 77 08 00 45 00  ..]..v... ]..w..E..
0010 00 28 16 49 40 00 80 06 00 00 0a 01 00 65 0a 01  ..( I@.... ....e..
0020 00 02 06 58 00 50 61 ff 66 ce 99 26 04 92 50 10  ..X.Pa. f...&P.
0030 04 00 14 83 00 00  ..... .

```

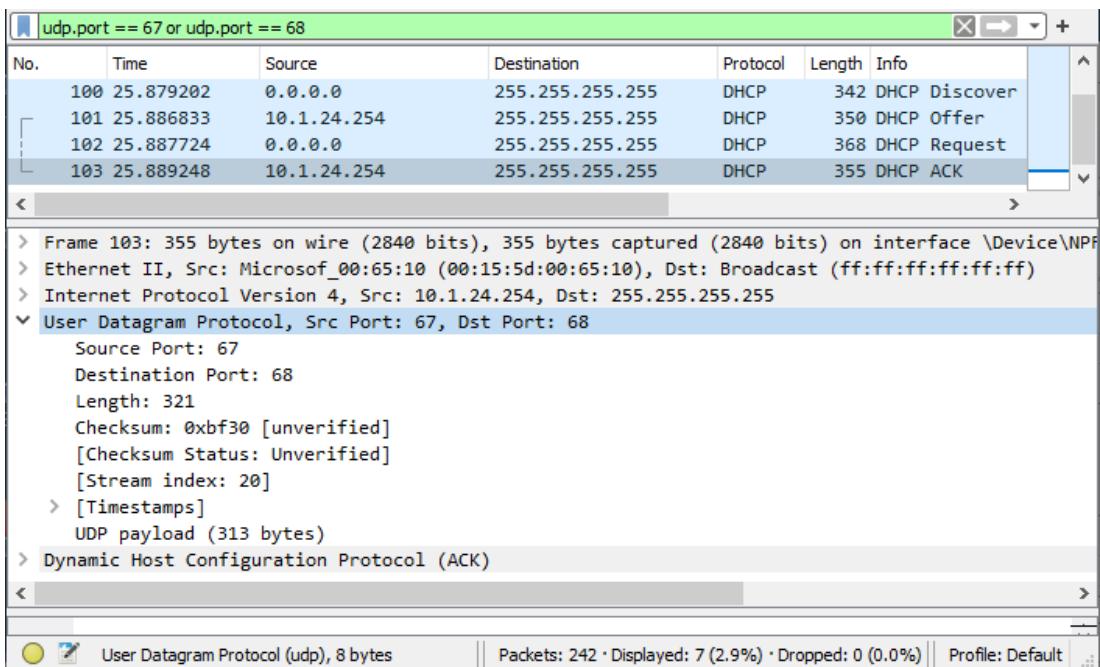
TCP is used when the application protocol cannot tolerate missing or damaged information. For example, the following application protocols must use TCP:

- **Hyper Text Transfer Protocol Secure (HTTPS)**— This protocol is used to deliver web pages and other resources. The secure version uses encryption to authenticate the server and protect the information that is being transmitted. A single missing packet would cause this process to fail completely.
- **Secure Shell (SSH)**— This protocol is used to access the command-line interface of a computer from across the network. It uses encryption to authenticate the server and user and protect the information that is being transmitted. This process would also fail if a data packet is not received.

User Datagram Protocol

Sometimes, it is more important that communications be faster than they are reliable. The connection-oriented process of TCP adds lots of header bytes to each packet. The **User Datagram Protocol (UDP)** is a **connectionless**, non-guaranteed method of communication with no sequencing or acknowledgments. There is no guarantee regarding the delivery of messages or the sequence in which packets are received.

Observing a UDP header in the final frame of the DHCP lease process with the Wireshark protocol analyzer



Screenshot courtesy of Wireshark.

The top section contains a list of captured packets with columns labeled No., Time, Source, Destination, Protocol, Length, and Info. The middle section displays detailed packet information for the selected D H C P A C K packet. It includes details such as: Frame size: 355 bytes captured on wire. Ethernet I I header: Source MAC address (Microsoft 00:65:10) and Destination MAC address as broadcast (f:f:f:f:f:f). I P v 4 header: Source I P address is 10.1.24.254, and Destination I P is 255.255.255.255. User Datagram Protocol (U D P) header: Source Port is 67, Destination Port is 68, Packet Length is 321 bytes, and Checksum value is displayed as unverified.

UDP is suitable for applications that do not require acknowledgment of receipt and can tolerate missing or out-of-order packets. It is often used by applications that transfer time-sensitive data but do not require complete reliability, such as voice or video, because missing data manifests as glitches rather than application errors or complete connection failures. The reduced overhead means that delivery is faster. If necessary, the application layer can be used to control delivery reliability.

Two other examples of protocols that use UDP are DHCP and TFTP:

- **Dynamic Host Configuration Protocol (DHCP)**—This protocol is used by clients to request IP configuration information from a server. It uses broadcast transmissions, which are not supported by TCP, so it must use UDP. The protocol is quite simple, so if a response packet is not received, the client just restarts the process and tries again repeatedly until timing out.
- **Trivial File Transfer Protocol (TFTP)**—This protocol is typically used by network devices to obtain a configuration file. The application protocol uses its own acknowledgment messaging, so it does not require TCP.

Well-Known Ports

Server port numbers are assigned by the Internet Assigned Numbers Authority (IANA). Some of the "well-known" port numbers and the functions of the application protocols they represent are listed in the following table.

Port#	TCP/UDP	Protocol	Purpose
20	TCP	File Transfer Protocol (FTP)—Data connection	Make files available for download across a network (data connection port)
21	TCP	File Transfer Protocol (FTP)—Control connection	Make files available for download across a network (control connection port)
22	TCP	Secure Shell (SSH)	Make a secure connection to the command-line interface of a server
23	TCP	Telnet	Make an unsecure connection to the command-line interface of a server
25	TCP	Simple Mail Transfer Protocol (SMTP)	Transfer email messages across a network
53	TCP/UDP	Domain Name System (DNS)	Facilitate identification of hosts by name alongside IP addressing
67	UDP	Dynamic Host Configuration Protocol (DHCP) Server	Provision an IP address configuration to clients
68	UDP	DHCP Client	Request a dynamic IP address configuration from a server
80	TCP	HyperText Transfer Protocol (HTTP)	Provision unsecure websites and web services
110	TCP	Post Office Protocol (POP)	Retrieve email messages from a server mailbox
137-139	UDP/TCP	NetBIOS over TCP/IP	Support networking features of legacy Windows versions
143	TCP	Internet Mail Access Protocol (IMAP)	Read and manage mail messages on a server mailbox
389	TCP	Lightweight Directory Access Protocol (LDAP)	Query information about network users and resources
443	TCP	HTTP Secure (HTTPS)	Provision secure websites and services
445	TCP	Server Message Block (SMB)	Implement Windows-compatible file and printer sharing services on a local network (also sometimes referred to as Common Internet File System [CIFS])
3389	TCP	Remote Desktop Protocol (RDP)	Make a secure connection to the graphical desktop of a computer

These application protocols will be covered in more detail over the course of the next topic and the next lesson.

Lesson 6D

Network Configuration Concepts

Lesson Overview

Configuration of four closely connected systems is an easy day. Now imagine configuring hundreds of systems across multiple locations to connect to your network. Walking to each system to manually set up the configuration will be time-consuming and cumbersome. Now, imagine you want to send communication packets to a computer named *Workstation-Three*, but you do not know its MAC address or its IP address. What if we had a system that allowed us to ask questions about the addresses of systems on our network, much like a phone book or contact list on our smartphones allow us to look up people and their phone numbers? Servers can be assigned various roles or jobs to provide services to the network of nodes it is connected to.



Objectives Covered

- 2.3 Summarize services provided by networked hosts
- 2.4 Explain common network configuration concepts

Learning Outcomes

As you study this lesson, answer the following questions:

- What is the purpose of Dynamic Host Configuration Protocol?
- What are the capabilities of DHCP?
- What is the purpose of Domain Name System?
- What is the purpose of VLANs?

DHCP Functions

When an interface is assigned a static configuration manually, the installer may make a mistake with the address information—perhaps duplicating an existing IP address or entering the wrong subnet mask—or the configuration of the network may change, requiring the host to be manually configured with a new static address. To avoid these problems, a **DHCP** server can be used to allocate an appropriate IP address and subnet mask (plus other settings) to any host that connects to the network and requests address information.

DHCP Scope

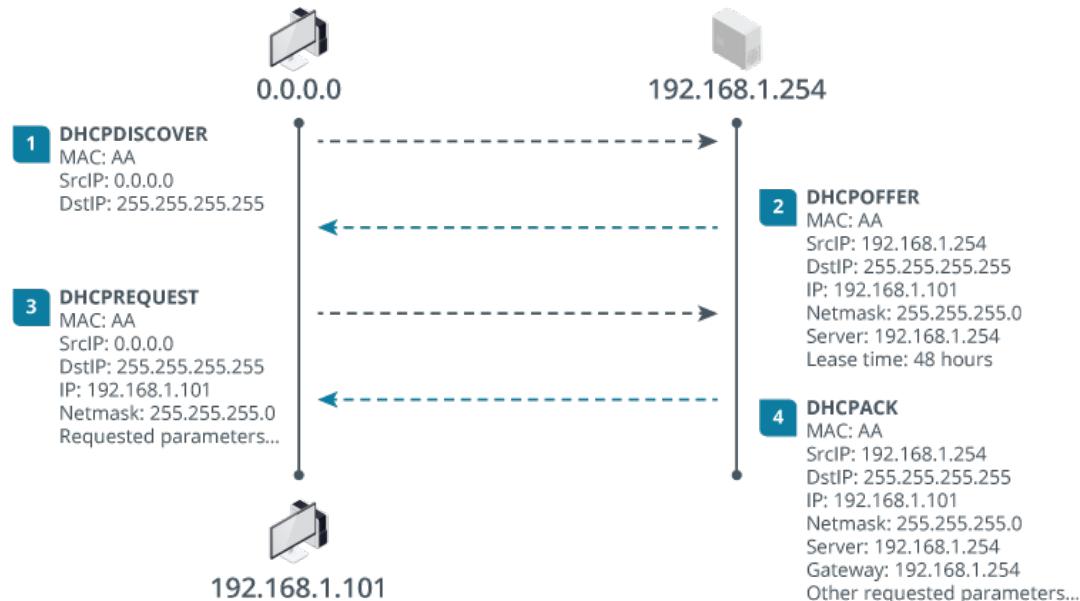
A **DHCP scope** is the range of IP addresses that a DHCP server can offer to client hosts in a particular subnet. The scope should exclude any addresses that have been configured statically. For example, the LAN address of a SOHO router is typically 192.168.0.1. This is

also the address used by the DHCP server running on the router. The scope must exclude this address. If the scope is defined as 192.168.0.100 to 192.168.0.199 , that allows for 100 dynamically addressed hosts on the local network.

DHCP Leases

A host is configured to use DHCP by specifying in its TCP/IP configuration that it should automatically obtain an IP address. When a DHCP client initializes, it broadcasts a DHCPDISCOVER packet to find a DHCP server. All communications are sent using UDP, with the server listening on port 67 and the client on port 68.

DHCP Discover, Offer, Request, Ack (Acknowledge) process



Images © 123RF.com.

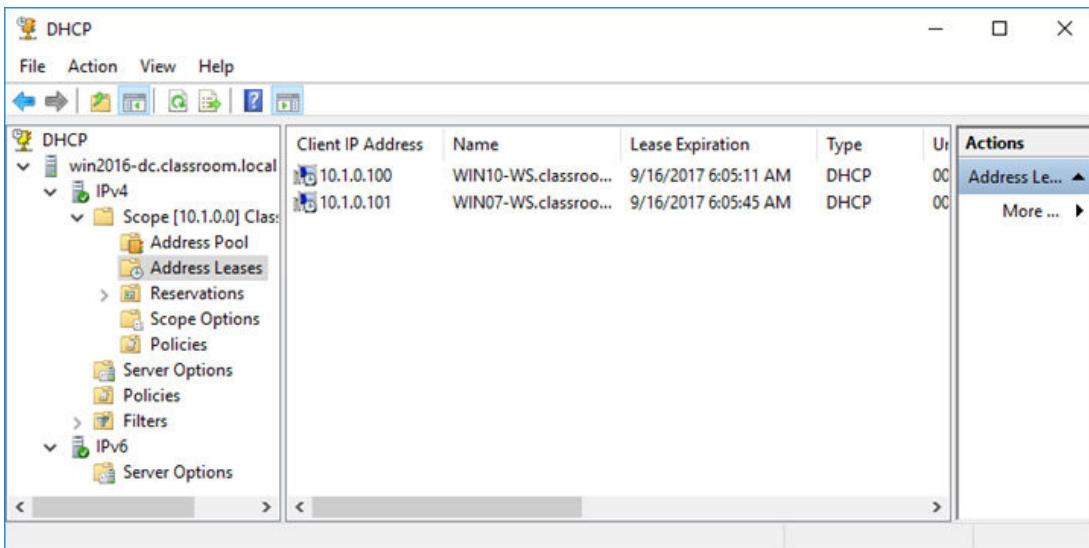
Note: The DHCP client communicates with the server using broadcast communications so there is no need to configure a DHCP server address in the client configuration. The DHCP server must be configured with a static IP address.

Presuming it has an IP address available, the DHCP server responds to the client with a DHCPOFFER packet, containing the address and other configuration information, such as default gateway and DNS server addresses. The client may choose to accept the offer using a DHCPREQUEST packet that is also broadcast onto the network.

Assuming the offer is still available, the server will respond with a DHCPACK packet. The client broadcasts an ARP message to check that the address is unused. If so, it will start to use the address and options; if not, it declines the address and requests a new one.

The IP address is leased by the server for a limited period only. A client can attempt to renew or rebind the [DHCP Lease](#) before it expires. If the lease cannot be renewed, the client must release the IP address and start the discovery process again.

Windows DHCP server showing address leases



Screenshot courtesy of Microsoft.

If the address information needs to change, this can be done on the DHCP server, and clients will update themselves automatically when they seek a new lease (or a new lease can be requested manually).

DHCP Reservations

It is often useful for a host to use the same IP address. Servers, routers, printers, and other network infrastructure can be easier to manage if their IP addresses are known. One option is to use static addressing for these appliances, but this is difficult to implement. Another option is to configure the DHCP server to reserve a particular IP address for each device using a [DHCP reservation](#). The DHCP server is configured with a list of the MAC addresses of hosts that should receive the same IP address each time they join the network. When it is contacted by a host with one of the listed MAC addresses, it issues a lease for the reserved IP address to the system.



Note: Some operating systems send a different unique identifier than a MAC address by default. The identification method should be configured appropriately on the client so that the server has the correct information.

Domain Name System

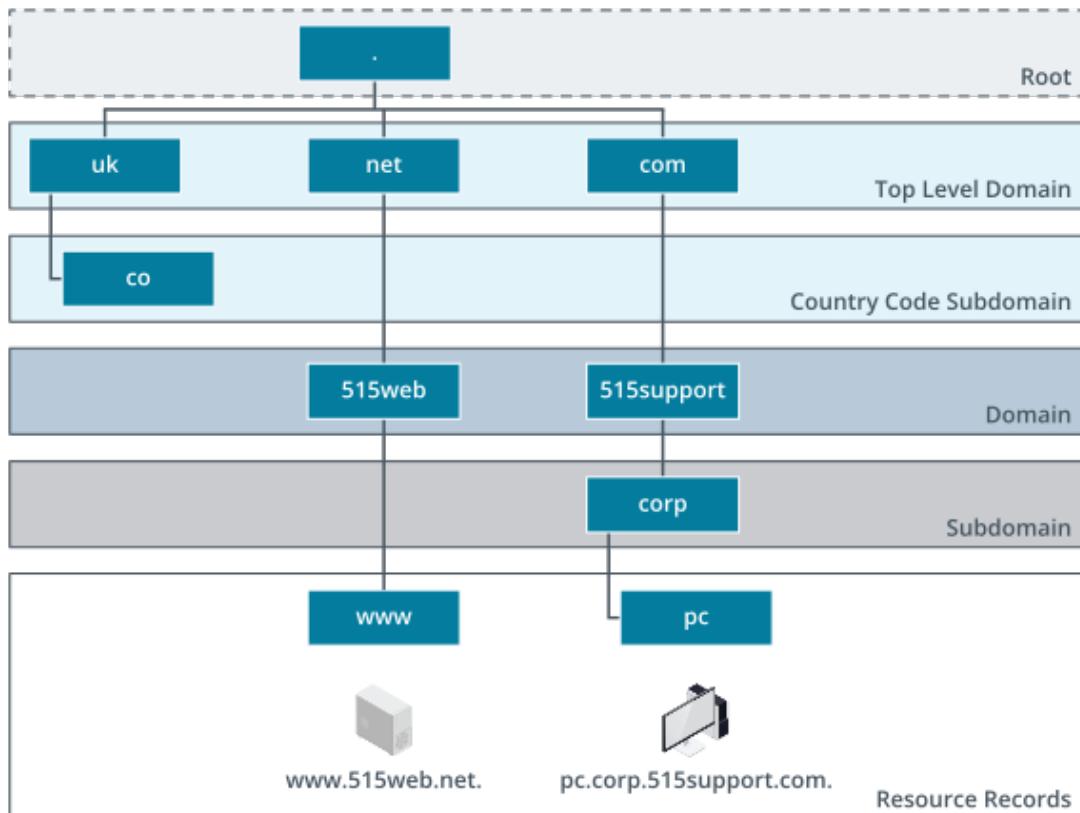
IP uses a binary address value to locate a host on an internetwork. The dotted decimal (IPv4) or hex (IPv6) representation of this IP address is used for configuration purposes, but it is not easy for people to remember or input correctly. For this reason, a "friendly" [host name](#) is also typically assigned to each host. The host name is configured when the OS is installed. The host name must be unique on the local network.

To avoid the possibility of duplicate host names on the Internet, the host name can be combined with a domain name and suffix. This is referred to as a [fully-qualified domain name](#) (FQDN). An example of an FQDN might be "nut.widget.example". The host name is `nut`, and the domain suffix is `widget.example`. This domain suffix consists of the domain name `widget` within the top-level domain (TLD) `.example`. A domain suffix could also contain subdomains between the host and domain name.

FQDNs are assigned and managed using **DNS**. DNS is a global hierarchy of distributed name server databases that contain information about each domain and the hosts within those domains. At the top of the DNS hierarchy is the root, which is represented by the null label, consisting of just a period (.). There are 13 root-level servers (A to M).

Immediately below the root lie the top-level domains (TLDs). There are several types of TLDs, but the most prevalent are generic (such as .com, .org, .net, .info, .biz), sponsored (such as .gov, .edu), and country code (such as .uk, .ca, .de). DNS is operated by ICANN (icann.org), which also manages the generic TLDs. Country codes are generally managed by an organization appointed by the relevant government.

DNS hierarchy



Images © 123RF.com

Each FQDN reflects this hierarchy, from most specific on the left (the host name) to least specific on the right (the TLD followed by the root). For example: `pc.corp.515support.com`.

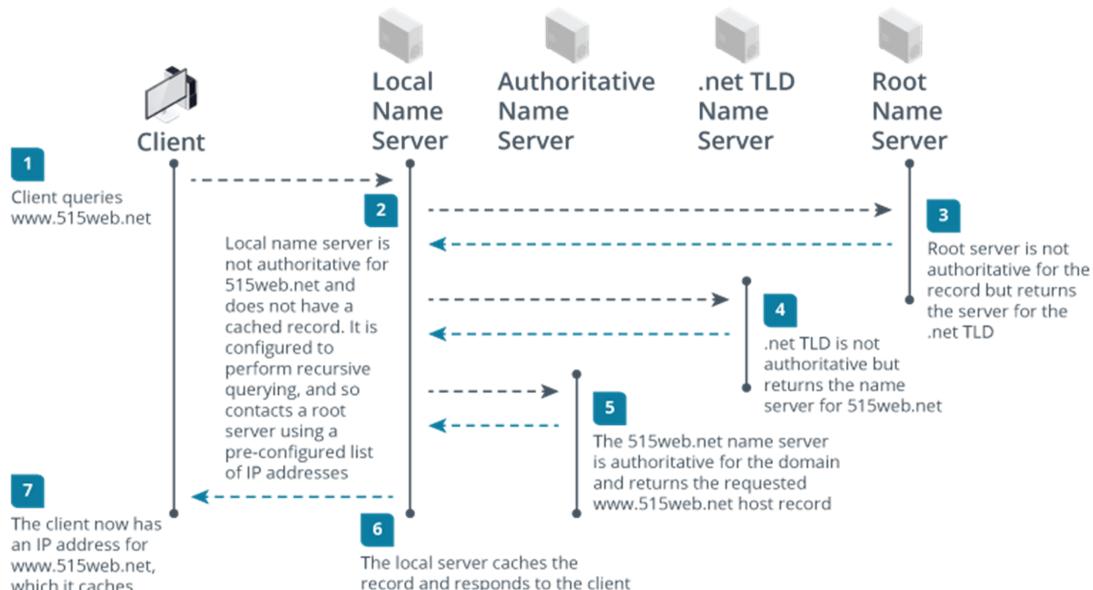
Note: The trailing period at the end of a URL can safely be omitted when querying for a resource, as it is assumed to be a resource in the root zone of the domain name system.

DNS Queries

To resolve a host name or FQDN to an IP address, the client must obtain the appropriate record from a DNS server. For example, a user might type an FQDN into the address bar of a web

browser client application. The client app, referred to as a "stub resolver," checks its local cache for the mapping. If no mapping is found, it forwards the query to its local DNS server. The IP addresses of one or more DNS servers that can act as resolvers are usually set in the TCP/IP configuration. The client communicates with a DNS server over **port 53**. The resolution process then takes place as follows:

DNS name resolution process



Images © 123RF.com.

The steps are as follows: Step 1: Client queries `www.515web.net`. Step 2: Local name server is not authoritative for `515web.net` and does not have a cached record. It is configured to perform recursive querying, and so contacts a root server using a pre-configured list of IP addresses. Step 3: Root server is not authoritative for the record but returns the server for the `.net` TLD. Step 4: Dot net TLD is not authoritative but returns the name server for `515web.net`. Step 5: The `515web.net` name server is authoritative for the domain and returns the name server for `515web.net`. Step 6: The local server caches the record and responds to the client. Step 7: The client now has an IP address for `www.515web.net`, which it caches.

DNS Record Types

The DNS server IP addresses configured on a client machine are used to resolve the client's queries for hosts and domains across the Internet. At least one DNS server also needs to be configured to act as an authoritative store of information about each domain. These name servers are normally installed separately from the ones used as client resolvers.

The DNS server responsible for managing a zone will contain numerous resource records. These records allow the name server to resolve queries for names and services hosted in the domain into IP addresses. Resource records can be created and updated manually (statically), or they can be generated dynamically from information received from client and server computers on the network.

Address (A) and Address (AAAA) Resource Records

An **address (A)** record is used to resolve a host name to an IPv4 address. An **AAAA** record resolves a host name to an IPv6 address.

Both types of host records (A and AAAA) in Windows Server DNS

The screenshot shows the Windows Server DNS Manager window. The left pane displays a navigation tree with sections for DNS, DC10, Forward Lookup Zones, Reverse Lookup Zones, Trust Points, and Conditional Forwarders. Under Forward Lookup Zones, the 'corp.515support.com' zone is selected. The main pane lists resource records in a table with columns: Name, Type, Data, and Timestamp. The table contains the following data:

Name	Type	Data	Timestamp
BACKUP	Host (A)	10.1.16.13	4/10/2021 3:00:00 AM
BACKUP	IPv6 Host (AAAA)	fdf0:2413:6d1c:0020:7b88:f308:ff44:7991	4/10/2021 3:00:00 AM
ca	Alias (CNAME)	DC10.corp.515support.com.	static
CS01	Host (A)	10.1.16.17	4/10/2021 3:00:00 AM
CS01	IPv6 Host (AAAA)	fdf0:2413:6d1c:0020:bf79:db95:594e:018e	4/10/2021 2:00:00 AM
dc10	Host (A)	10.1.16.1	static
dc10	IPv6 Host (AAAA)	fdf0:2413:6d1c:0020:0000:0000:0000:0001	static
dc10	IPv6 Host (AAAA)	fdf0:2413:6d1c:0020:41f3:89dd:42ad:92ae	static
git	Host (A)	10.1.16.9	8/4/2021 2:00:00 AM
mail	Host (A)	10.1.16.2	static

Screenshot courtesy of Microsoft.

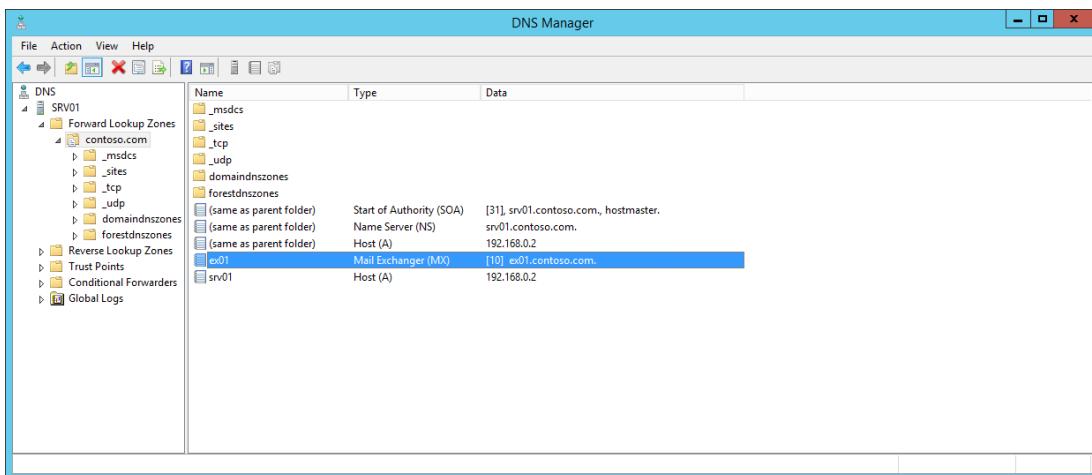
Left Pane has a navigation tree with sections for Forward Lookup Zones, Reverse Lookup Zones, Trust Points, and Conditional Forwarders. Under Forward Lookup Zones, there is a selected zone: corp dot 515 support dot com. Main Pane has a table listing D N S resource records for the selected zone. Columns are titled, names, types, data, and timestamps.

CNAME Records

A CNAME record, or canonical name record, is used to link one domain name to another domain name. For example, Company A acquires another company, Company B. Instead of maintaining two websites, www.companyA.com and www.companyB.com, Company A can simply make a CNAME record entry that links www.companyB.com to www.companyA.com. This allows users who type in www.companyB.com to be redirected to www.companyA.com and prevents a user who may not be aware of the acquisition and change in the URL.

Mail Exchanger (MX) Resource Records

A Mail Exchange (MX) record is used to identify an email server for the domain so that other servers can send messages to it. In a typical network, multiple servers are installed to provide redundancy, and each one will be represented by an MX-record. Each MX record is given a preference value, with the lowest numbered entry preferred. The host name identified in an MX record must have an associated A or AAAA record.



Screenshot courtesy of Microsoft.

The File, Action, View, and Help tabs are on the top. The left pane has a navigation tree that shows DNS zones. Under Forward Lookup Zones, the contoso dot com zone is expanded to display subfolders like underscore m s d c s. The main pane shows a table titled, Name, Type, and Data.

DNS Spam Management Records

A [TXT-record](#) is used to store any free-form text that may be needed to support other network services. A single domain name may have many TXT records, but they are most commonly used to verify email services and block the transmission of spoofed and unwanted messages, referred to as [spam](#).

Sender Policy Framework

Sender Policy Framework (SPF) uses a TXT resource record published via DNS by an organization's hosting email service. The SPF record—there must be only one per domain—identifies the hosts authorized to send email from that domain. An SPF can also indicate what to do with mail from servers not on the list, such as rejecting them (`-all`), flagging them (`~all`), or accepting them (`+all`).

DomainKeys Identified Mail

DomainKeys Identified Mail (DKIM) uses cryptography to validate the source server for a given email message. This can replace or supplement SPF. To configure DKIM, the organization uploads a public encryption key as a TXT record in the DNS server. Organizations receiving messages can use this key to verify that a message derives from an authentic server for the domain.

Domain-Based Message Authentication, Reporting, and Conformance

The [Domain-Based Message Authentication, Reporting, and Conformance](#) (DMARC) framework ensures that SPF and DKIM are being utilized effectively. A DMARC policy is published as a DNS TXT record. DMARC can use SPF or DKIM or both. DMARC specifies a more robust policy mechanism for senders to specify how DMARC authentication failures should be treated (flag, quarantine, or reject), plus mechanisms for recipients to report DMARC authentication failures to the sender.

Virtual LANs

All hosts connected to the same unmanaged switch are said to be in the same broadcast domain. This does not present any problems on a small network. However, the switching fabric on an enterprise network can provide thousands of ports. Placing hundreds or thousands of hosts in the same broadcast domain reduces performance. To mitigate this, the ports can be divided into groups using a feature of managed switches called [virtual local area network](#) (VLAN). This allows the large network of systems to be logically divided to increase performance, and in some cases the security, of that network is also increased.

The simplest means of assigning a node to a VLAN is by configuring the port interface on the switch with a VLAN ID in the range 2 to 4094. For example, switch ports 5 through 8 could be configured as a VLAN with the ID 100, and ports 9 through 12 could be assigned to VLAN 200. Host A connected to port 2 would be in VLAN 100, and host B connected to port 12 would be in VLAN 200.

Cumulus VX switch output showing switch ports swp 5–8 configured in VLAN 100 and ports 9–12 in VLAN 200

```
interface swp5
    bridge-access 100

interface swp6
    bridge-access 100

interface swp7
    bridge-access 100

interface swp8
    bridge-access 100

interface swp9
    bridge-access 200

interface swp10
    bridge-access 200

interface swp11
    bridge-access 200

interface swp12
    bridge-access 200

interface bridge
    bridge-ports swp5 swp6 swp7 swp8 swp9 swp10 swp11 swp12
    bridge-vids 10 100 200
    bridge-vlan-aware yes
```

! The VLAN with ID 1 is referred to as the "default VLAN." Unless configured differently, all ports on a managed switch default to being in VLAN 1.

When hosts are placed in separate VLANs, they can no longer communicate with one another directly, even though they might be connected to the same switch. Each VLAN must also be configured with its own subnet address and IP address range as well. Communications between VLANs must go through an IP router. Each VLAN must also be provisioned with its own DHCP and DNS services.

As well as reducing the impact of excessive broadcast traffic, from a security point of view, each VLAN can represent a separate zone. Traffic passing between VLANs can easily be filtered and monitored to ensure it meets security policies. VLANs are also used to separate nodes based on traffic type, such as isolating devices used for voice traffic so that they may be prioritized over data passing over other VLANs.

Virtual Private Networks

A [virtual private network](#) (VPN) enables hosts to connect to the LAN without being physically installed at the site. Rather than attach to a switch or AP, the host connects to the local network via a remote access server that accepts connections from the Internet. Because the Internet is a public network, it is important for the VPN connection to be secure.

A secure VPN configures a protected tunnel through the Internet. It uses special connection protocols and encryption technology to ensure that the tunnel is protected against snooping and that the user is properly authenticated. Once the connection has been established, to all intents and purposes, the remote computer becomes part of the local network, though it is still restricted by the bandwidth available over the Internet connection.

A typical remote access VPN configuration

The VPN client host connects to a VPN gateway using any type of Internet subscriber access method

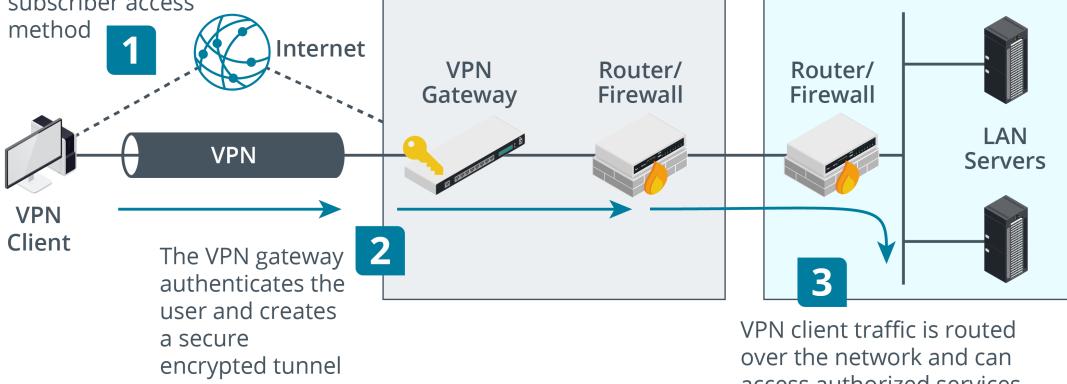


Image © 123RF.com.

The process includes three main steps: Step 1: The VPN client host connects to a VPN gateway using any type of internet subscriber access method. Step 2: The VPN gateway authenticates the user and creates a secure encrypted tunnel. Step 3: VPN client traffic is routed over the network and can access authorized services.

The VPN described above is for remote access to the LAN by teleworkers and roaming users. VPNs can also be used to connect sites over public networks, such as linking branch offices to a head office, or within a local network as an additional security mechanism.



Module 7

Supporting Network Services

Module Overview

Application protocols implement services such as web browsing, email, and file sharing. As well as computer server roles, modern networks use a variety of Internet security appliances and smart devices. Some networks are integrated with embedded system devices that underpin industrial technologies. While you will not have responsibility for configuring the devices and servers that run these applications, being able to summarize the functions and purposes of server roles will help you assist other technicians.

Being able to summarize the function of protocols up the network stack is also a prerequisite for troubleshooting network issues. When you are diagnosing connectivity problems with a host, you need to determine whether the issue is with a cable or adapter that you can resolve or whether there is a wider network or application server issue that you will need to escalate to senior support staff.

Module Summary

Prepare for A+ Core 1 by:

- Summarizing services provided by networked hosts
- Comparing Internet and embedded appliances
- Troubleshooting networks

Lesson 7A

Networked Host Services

Lesson Overview

Networks today are used for much more than just email and Internet web browsing. Take a remote employee for example. They must have the ability to access the files and enterprise systems from their off-site location. Your sales team needs to access the price listings and check inventory of stock while visiting customers, and your on-site employees need to be able to do all of this and more while still at the primary work site. Without networked systems and services, all of this would be difficult to make happen, and doing so safely and securely could be difficult.



Objectives Covered

- 2.1 Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purpose
- 2.3 Summarize services provided by networked hosts

Learning Outcomes

As you study this lesson, answer the following questions:

- What services are commonly found on modern networks?
- What port numbers are associated with the various services found on modern networks?
- How does a web server function?
- What are the services utilized by email systems and servers?
- How do remote access and monitoring services assist system administrators?

File/Print Servers

One of the core network functions is to provide shared access to disk and print resources. Like many network protocols, resource sharing is implemented using a client/server architecture. The machine hosting the disk or printer is the **server**. A server disk configured to allow clients to access it over the network is a **file share**. Machines accessing those resources are the clients.

The file share and print server roles may be implemented on a local network using proprietary protocols, such as File and Print Services for Windows Networks. A file server could also be implemented using TCP/IP protocols, such as File Transfer Protocol (FTP).

Server Message Block

Server Message Block (SMB) is the application protocol underpinning file and printer sharing on Windows networks. SMB usually runs directly over the TCP/445 port.

SMB has gone through several updates, with SMB3 as the current version. SMB1 has very serious security vulnerabilities and is now disabled by default on current Windows versions (docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3). Support for SMB in UNIX- or Linux-based machines and network attached storage (NAS) appliances is provided by using the Samba software suite, which allows a Windows client to access a Linux host as though it were a Windows file or print server.

SMB is sometimes referred to as the Common Internet File System (CIFS), though technically that should only be used to refer to a specific dialect of SMB version 1.

Print servers assist in managing printer and print jobs across the network. They can be implemented through hardware or software configurations. Providing centralized management of printing leads to more efficient handling of the high volume of print requests large enterprise networks may experience. A print server also allows you to queue print jobs and in some cases hold the print job until a user releases the print job to a printer for processing. This can prevent a print job from printing and not being collected by a user.

Network Basic Input/Output System

The earliest Windows networks used a protocol stack called the [NetBIOS](#) rather than TCP/IP. NetBIOS allowed computers to address one another by name and establish sessions for other protocols, such as SMB. As the TCP/IP suite became the standard for local networks, NetBIOS was re-engineered to work over the TCP and UDP protocols, referred to as NetBIOS over TCP/IP (NetBT). NetBT uses UDP/137 for name services, UDP/138 for UDP connections, and TCP/139 for TCP session services.

Modern networks use IP, TCP/UDP, and DNS for these functions, so NetBT is obsolete. NetBT should be disabled on most networks, as it poses a significant risk to security. It is only required if the network must support file sharing for Windows versions earlier than Windows 2000.

File Transfer Protocol

The File Transfer Protocol (FTP) allows a client to upload and download files from a network server. It is often used to upload files to websites. FTP is associated with the use of port TCP/21 to establish and maintain a connection and either port TCP/20 to transfer data in "active" mode or a server-assigned port in "passive" mode.

 **Note:** Plain FTP is unencrypted and so poses a high-security risk. Passwords for sites are submitted in plaintext. There are ways of encrypting FTP sessions, such as FTP-Secure (FTPS) and FTP over Secure Shell (SFTP), and it is the encrypted services that is most widely used today.

Database Servers

Data needs to be stored, organized, and managed in a way that makes it easy for users to retrieve the information when needed. **Database servers** provide a method to store large amounts of structured and unstructured data. While you may think a spreadsheet is easy to store data, there is only so much a flat file will allow you to do with that data. Databases allow the same data to be queried for reports, modified for special purposes, and used to make business decisions.

There are several common types of databases, with relational databases being the most popular. Relational databases link different data points together based on their relationships to one another. Relational databases are also known as SQL databases because a user can utilize the Structured Query Language to interact with the database, and they store data in tables using columns and rows. Examples of relational databases include Oracle, MySQL, and MariaDB.

Non-relational databases store data in a flexible manner using graphs, documents, or key-value pairs. This database type is more aligned for more flexibility when storing various types of data and is best used for large amounts of data. Examples of non-relational databases include MongoDB, CouchDB, and Amazon SimpleDB.

Web Servers

A **web server** is one that provides client access using HTTP or its secure version (HTTPS). Websites and web applications are perhaps the most useful and ubiquitous of network services. Web technology can be deployed for a huge range of functions and applications, in no way limited to the static pages of information that characterized the first websites.

HyperText Transfer Protocol

HTTP enables clients (typically web browsers) to request resources from an HTTP server. A client connects to the HTTP server using port **TCP/80** (by default) and submits a request for a resource (GET). The server either returns the requested data if it is available or responds with an error code.

Inspecting the HTTP requests and response headers

The screenshot shows the Mozilla Firefox developer tools interface with the Network tab selected. The main pane displays a list of network requests made to the website <https://www.comptia.org>. The table includes columns for Status, Mimetype, Domain, File, Initiator, Type, Transferred, and Size. The right pane shows the detailed response for the main page request (Status: 200 OK, Version: HTTP/2, Transferred: 17.26 KB (73.65 KB size)). It also lists Response Headers, including cache-control, content-encoding, content-length, content-type, date, expires, and feature-policy.

Status	Mimetype	Domain	File	Initiator	Type	Transferred	Size	
200	GET	scatec.io	/	collect	app.js:1 (...	browsing...	html	17.26 KB ... 7...
304	GET	code.jquery.com	jquery-latest.min.js		script	js	cached	0 B
200	GET	www.comptia.org	jquery.validate.min.js		script	js	6.96 KB	2...
200	GET	www.comptia.org	jquery.validate.unobtrusive.min.js		script	js	3.03 KB	5....
200	GET	www.comptia.org	mvcfoolproof.unobtrusive.js		script	js	2.39 KB	7....
200	GET	www.comptia.org	project.min.js?v=3.6.0		script	js	183.71 KB	1....
200	GET	kit.fonts.com	df896256a0.js		script	js	4.62 KB	1...
304	GET	www.google-analytics.com	js?id=UA-113138049-1		script	js	cached	1...
301	GET	www.comptia.org	js.cookie-2.2.0.min.js		script	js	1.75 KB (...	1....
200	GET	cdn.rangle.io	featherlight.min.js		script	js	4.54 KB	9 ...

Response Headers (722 B)

- cache-control: no-cache
- content-encoding: gzip
- content-length: 16951
- content-type: text/html; charset=utf-8
- date: Wed, 04 Aug 2021 12:43:22 GMT
- expires: -1
- feature-policy: self

Screenshot courtesy of Mozilla.

A browser's developer tools window analyzing network activity for the CompTIA website. Key elements include the website's header with the CompTIA logo and URL. Developer Tools Panel: The Network tab is selected, displaying a table of HTTP requests. The table includes columns titled status, domain, file, initiator, type, transferred, and size. The right pane with headers tab selected lists the following: Status: 200 OK Version: HTTP/2 Transferred: 17.26 KB (73.65 KB size) Response headers include the cache-control, content-encoding, content-length, content-type, date, expires, and feature-policy.

HyperText Markup Language, Forms, and Web Applications

HTTP is usually used to serve HTML web pages, which are plain text files with coded tags describing how the document should be formatted. A web browser can interpret the tags and display the text and other resources associated with the page (such as pictures or sound files). Another powerful feature is the ability to provide hyperlinks to other related documents. HTTP also features mechanisms (POST) whereby a user can submit data from the client to the server.

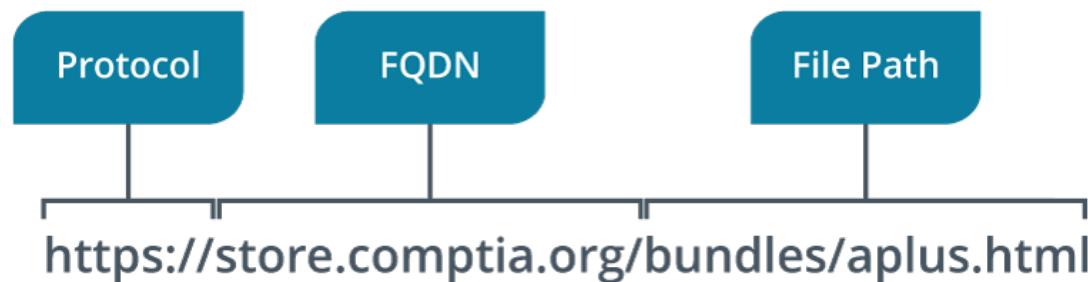
The functionality of HTTP servers is often extended by support for scripting and programmable features (web applications).

Uniform Resource Locators

Resources on the Internet are accessed using an addressing scheme known as a URL, such as <http://www.microsoft.com>. A URL contains all the information necessary to identify and access an item. For example, a URL for an HTTP resource might contain the following elements:

- The protocol describes the access method or service type being used.
- The host location is usually represented by a FQDN. The FQDN is not case-sensitive. The host location can also be an IP address; an IPv6 address must be enclosed in square brackets.
- The file path specifies the directory and file name location of the resource (if required). The file path may or may not be case-sensitive, depending on how the server is configured.

URL for an HTTPS website. The site is identified by the FQDN `store.comptia.org` and the requested resource is in the file path `/bundles/aplus.html` from the site root.



Web Server Deployment

Typically, an organization will lease a web server or space on a server from an ISP. Larger organizations with Internet-connected datacenters may host websites themselves. Web servers are not only used on the public Internet, however. Private networks using web technologies are described as "intranets" (if they permit only local access) or "extranets" (if they permit remote access).

Hypertext Transfer Protocol Secure

One of the critical problems for the provision of early websites was the lack of security in HTTP. Under HTTP, all data is sent unencrypted, and there is no authentication of client or server. Secure Sockets Layer (SSL) was developed by Netscape in the 1990s to address these problems. SSL proved very popular in the industry. [Transport Layer Security](#) was developed from SSL and ratified as a standard by the IETF.

When TLS is used with the HTTP application, it is referred to as **HTTPS**. Encrypted traffic between the client and server is sent over port **TCP/443** (by default), rather than the open and

unencrypted port 80. TLS can also be used to secure other TCP application protocols, such as FTP, POP3/IMAP, SMTP, and LDAP. If the "S" for secure is at the end of the acronym (HTTPS, SMTPS, LDAPS, etc.), the security is being provided through SSL or TLS.

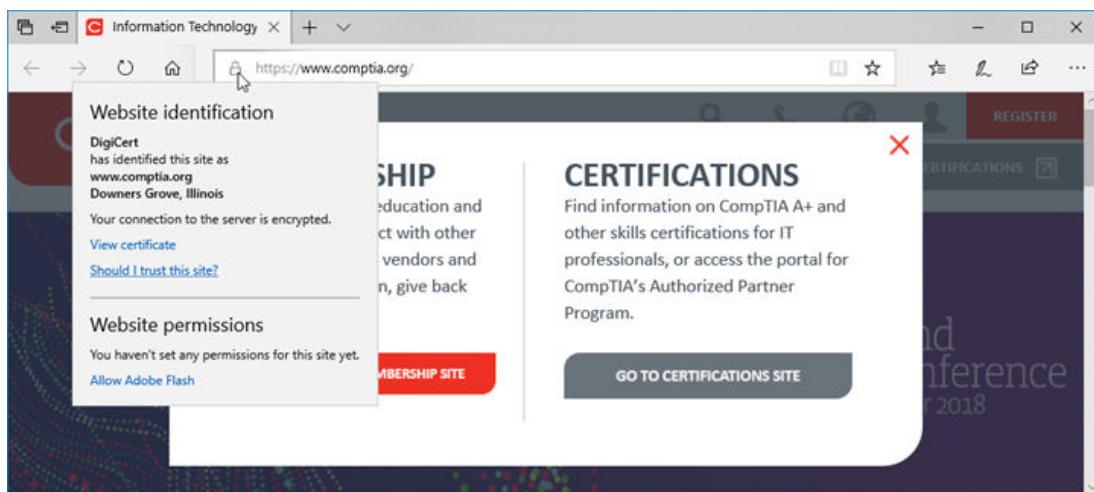
 TLS can also be used with UDP, referred to as Datagram Transport Layer Security (DTLS), most often in virtual private networking (VPN) solutions.

To implement HTTPS, the web server is installed with a digital certificate issued by some trusted certificate authority or CA. The certificate uses encrypted data to prove the identity of the server to the client, assuming that the client also trusts the CA. The system uses a public/private encryption key pair. The private key is kept a secret known only to the server; the public key is given to clients via the digital certificate.

The server and client use the key pair in the digital certificate and a chosen cipher suite within the TLS protocol to set up an encrypted tunnel. Even though someone else might know the public key, they cannot decrypt the contents of the tunnel without obtaining the server's private key. This means that the communications cannot be read or changed by a third party.

A web browser will open a secure session to an HTTPS server by using a URL starting with https:// and it will also show a padlock icon in the address bar to indicate that the server's certificate is trusted and that the connection is secure. A website can be configured to require a secure session and reject or redirect plain HTTP requests.

HTTPS padlock icon

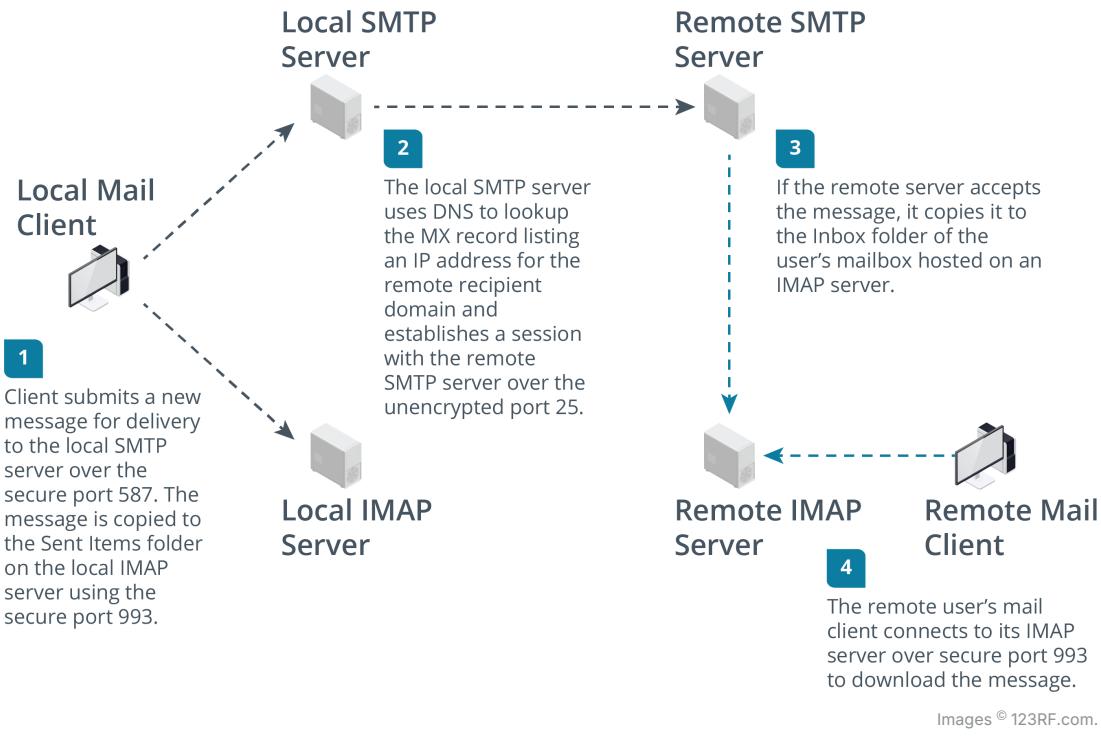


Screenshot courtesy of Microsoft.

Mail Servers

Electronic mail enables a person to compose a message and send it to another user on their own network (intranet) or anywhere in the world via the Internet. Two types of **mail servers** and protocols are used to process **email**: mail transfer and mailbox access protocols:

Operation of delivery and mailbox email protocols



Images © 123RF.com.

The steps are as follows: Step 1: Client submits a new message for delivery to the local S M T P server over the secure post 587. The message is copied to the Sent Items folder on the local I M A P server using the secure port 993. Step 2: The local S M T P server uses D N S to lookup the M X record listing an I P address for the remote recipient domain and establishes a session with the remote S M P T server over the unencrypted port 25. Step 3: If the remote server accepts the message, it copies it to the Inbox folder of the user's mailbox hosted on an I M A P server. Step 4: The remote user's mail client connects to its I M A P server over secure port 993 to download the message.

Internet email addresses follow the mailto URL scheme. An Internet email address comprises two parts—the username (local part) and the domain name, separated by an @ symbol. The domain name may refer to a company or an ISP; for example, `david.martin@comptia.org` or `david.martin@aol.com`.

The Simple Mail Transfer Protocol (SMTP) specifies how email is delivered from one mail domain to another. The SMTP server of the sender discovers the IP address of the recipient SMTP server by using the domain name part of the recipient's email address. The SMTP servers for the domain are registered in DNS using Mail Exchange (MX) and host (A/AAAA) records.

Typical SMTP configurations use the following ports and secure services:

- **Port TCP/25** is used for message relay between SMTP servers, or message transfer agents (MTAs). Transmissions over port 25 are usually insecure.
- **Port TCP/587** is used by mail clients—message submission agents (MSAs)—to submit messages for delivery by an SMTP server. Servers configured to support port 587 should use encryption and authentication to protect the service.

Mailbox Servers

SMTP is used only to deliver mail to server hosts that are permanently available. When an email is received by an SMTP server, it delivers the message to a mailbox server. The mailbox server could be a separate machine or a separate process running on the same computer. A mailbox access protocol allows the user's client email software to retrieve messages from the mailbox.

Post Office Protocol 3

The **Post Office Protocol** (POP) is an early example of a mailbox access protocol. POP is often referred to as POP3 because the active version of the protocol is version 3. A POP client application, such as Microsoft Outlook® or Mozilla Thunderbird®, establishes a connection to the POP server on port TCP/110 or over the secure port TCP/995. The user is authenticated (by username and password), and the contents of the mailbox are downloaded for processing on the local PC. With POP3, the messages are typically deleted from the mailbox server when they are downloaded, though some clients have the option to leave messages on the server.

Configuring an email account

The screenshot shows the 'Add Account' dialog box. At the top, it says 'POP and IMAP Account Settings' and 'Enter the mail server settings for your account.' There is a close button (X) and a help icon (mousing over it shows a cursor icon).

User Information

- Your Name: David Martin
- Email Address: david@davidmartin.me

Server Information

- Account Type: POP3
- Incoming mail server: pop3.myisp.net
- Outgoing mail server (SMTP): smtp.myisp.net

Logon Information

- User Name: david
- Password: [REDACTED]
- Remember password
- Require logon using Secure Password Authentication (SPA)

Test Account Settings

We recommend that you test your account to ensure that the entries are correct.

Automatically test account settings when Next is clicked

Deliver new messages to:

- New Outlook Data File
- Existing Outlook Data File

At the bottom are buttons: < Back, **Next >**, and Cancel.

Screenshot courtesy of Microsoft.

An Add Account dialog box. POP and IMAP account settings. Enter the mail server settings for your accounts. The data are as follows:

User Information: Your Name: David Martin Email Address: David at the rate David martin dot me Server Information: Account Type: P O P 3 (selected from a dropdown menu) Incoming Mail Server: pop 3 dot my i s p dot net Outgoing Mail Server (S M T P): s m t p dot my i s p dot net Logon Information: Username: David Password: Hidden (with Remember password checkbox checked). Additional Options: Checkbox for Require logon using Secure Password Authentication (S P A) is checked. Test Account Settings: We recommend that you test your account to ensure that the entries are correct. A test accounts settings button is below. Automatically test account settings when Next is clicked checkbox is selected. Deliver new messages to: New Outlook Data File (selected) or an Existing Outlook Data File (not selected). A more settings button is below. At the bottom, Back, Next and Cancel buttons allow navigation. Next button is selected.

Internet Message Access Protocol

The **Internet Message Access Protocol** (IMAP) addresses some of the limitations of POP. IMAP is a mail retrieval protocol, but its mailbox management features lack the features associated with POP mail management. IMAP supports permanent connections to a server and connecting multiple clients to the same mailbox simultaneously. It also allows a client to manage the mailbox on the server (to organize messages in folders and to control when they are deleted, for instance) and to create multiple mailboxes.

A client connects to an IMAP server over port TCP/143, but this port is insecure. Connection security can be established using TLS. The default port for IMAP-Secure (IMAPS) is TCP/993.

Directory and Authentication Servers

DHCP allows a network client to request an IP configuration, and DNS allows it to request resources using plain names. Most networks must also authenticate and authorize clients before allowing them to connect to fileshares and mail servers.

This security requirement is met by configuring an access control system to prevent unauthorized users (and devices) from connecting. In a Windows workgroup, for example, the access control method is a simple password, shared with all authorized users. Enterprise networks use directory servers to maintain a centralized database of user accounts and authenticate the subjects trying to use those accounts. These protocols allow a user to authenticate once to access the network and gain authorization for all the compatible application servers running on it. This is referred to as single sign-on (SSO).

Lightweight Directory Access Protocol

Network resources can be recorded as objects within a directory. A directory is a type of database, where an object is like a record and things that you know about the object (attributes) are like fields. Most directories are based on the X.500 standard. The **Lightweight Directory Access Protocol** (LDAP) is a TCP/IP protocol used to query and update an X.500 directory. It is widely supported in current directory products—Windows Active Directory or the open-source OpenLDAP, for instance. LDAP uses TCP and UDP port 389 by default but can use TLS (LDAPS) to impose security through encryption by using port TCP/636.

Authentication, Authorization, and Accounting

Network clients can join the network using multiple types of access devices, including switches, access points, and remote access VPN servers. Storing copies of the network directory and authentication information on all these access devices would require each device to do more processing and have more storage. It also increases the risk that this confidential information could be compromised.

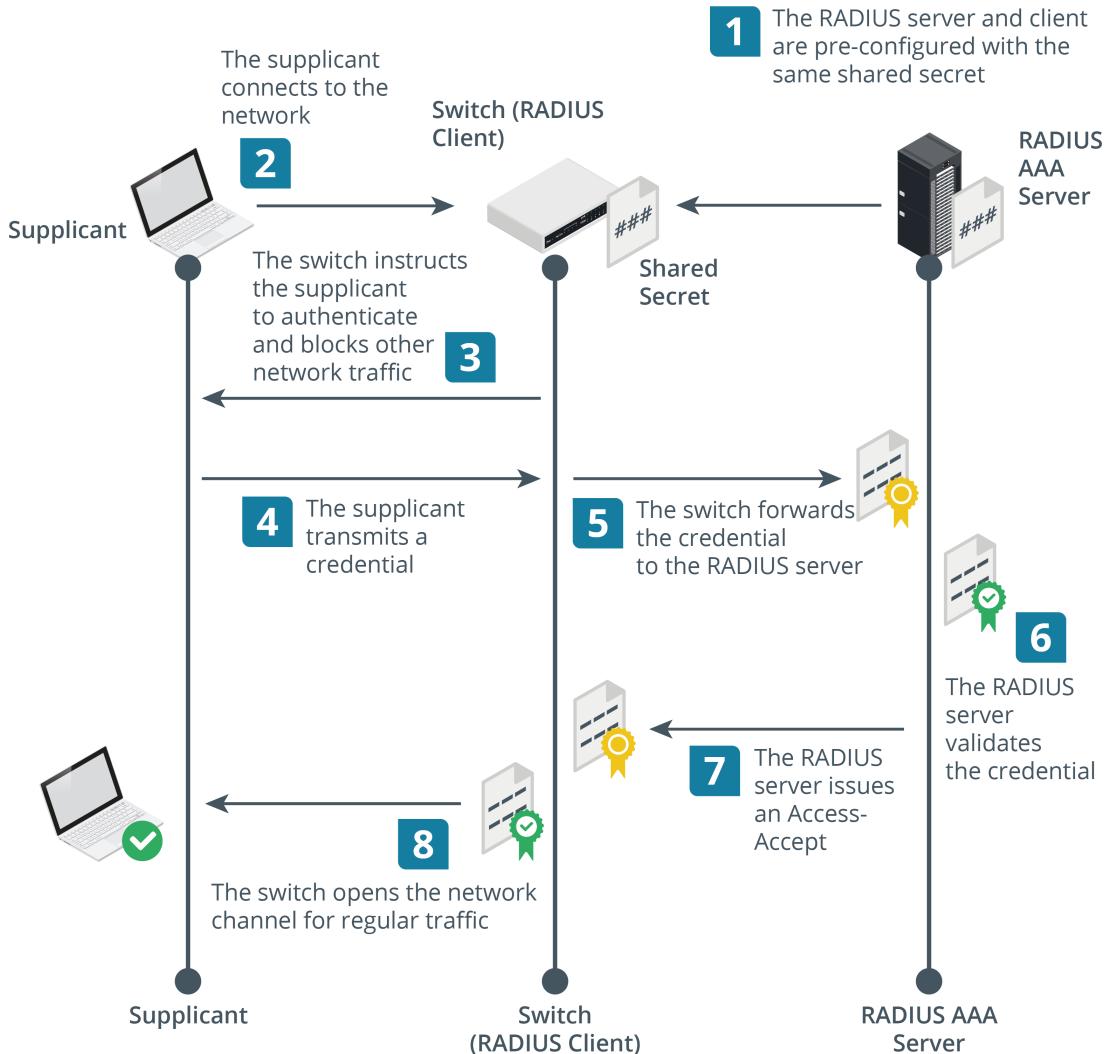
An authentication, authorization, and accounting (AAA) server is one that consolidates authentication services across multiple access devices. AAA uses the following components:

- **Supplicant**—The device requesting access, such as a user's PC or laptop.
- **Network access server (NAS) or network access point (NAP)**—Network access appliances, such as switches, access points, and VPN gateways. These are also referred to as "AAA clients" or "authenticators."
- **AAA server**—The authentication server, positioned within the local network.

With AAA, the network access appliances do not have to store any authentication credentials. They simply act as a transit to forward this data between the AAA server and the supplicant. AAA is often implemented using a protocol called **Remote Authentication Dial In User Service** (RADIUS) on port TCP/UDP 1812/1813 or as **Terminal Access Controller Access Control System**

Plus (TACACS+) using TCP/49. RADIUS is commonly used to authenticate users to a network, whereas TACACS is commonly used to authenticate devices such as routers and switches.

Communications between RADIUS server, client, and supplicant in AAA architecture



Images © 123RF.com.

The steps are as follows: Step 1: The RADIUS server and client are pre-configured with the same shared secret. Step 2: The supplicant connects to the network. Step 3: The switch instructs the supplicant to authenticate and blocks other network traffic. Step 4: The supplicant transmits a credential. Step 5: The switch forwards the credential to the RADIUS server. Step 6: The RADIUS server validates the credentials. Step 7: The RADIUS server issues an Access Accept. Step 8: The switch opens the network channel for regular traffic.

Remote Terminal Access Servers

A remote terminal server allows a host to accept connections to its command shell or graphical desktop from across the network. The name "terminal" comes from the early days of computing where configuration was performed by a teletype (TTY) device. The TTY is the terminal or endpoint for communication between the computer and the user. It handles text input and output between the user and the shell, or command environment. Where the terminal accepts input and displays output, the shell performs the actual processing.

A **terminal emulator** is any kind of software that replicates this TTY input/output function. A given terminal emulator application might support connections to multiple types of shells. A remote terminal emulator allows you to connect to the shell of a different host over the network.

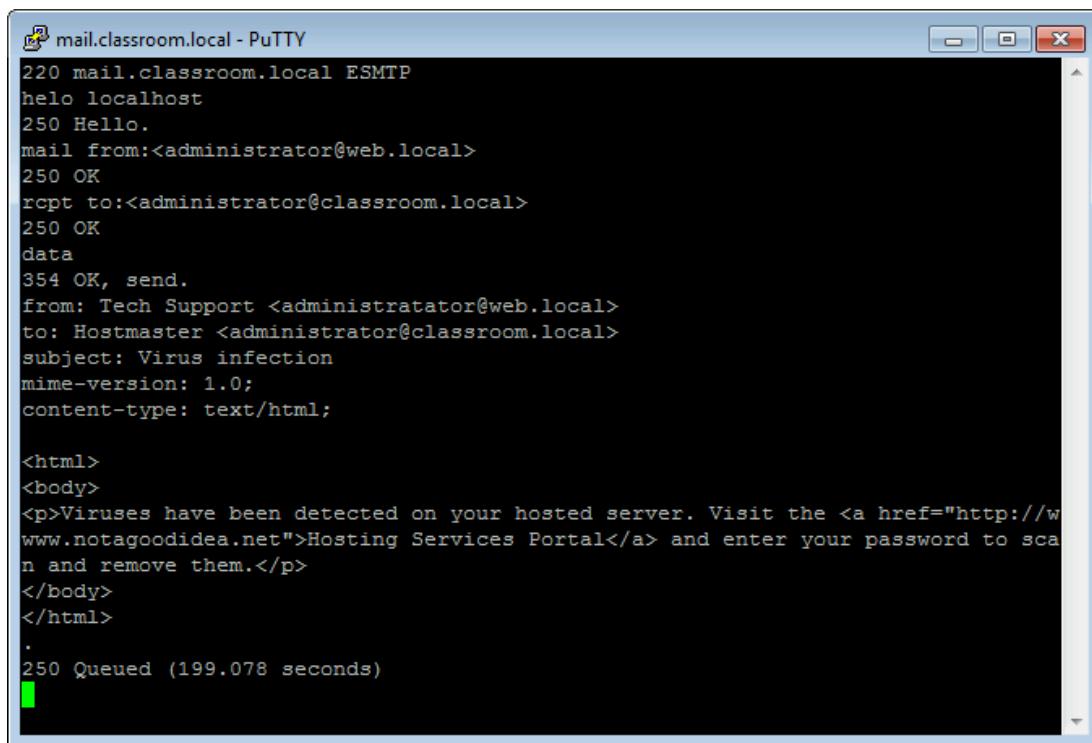
Secure Shell

Secure Shell (SSH) is the principal means of obtaining secure remote access to UNIX and Linux servers and to most types of network appliances (switches, routers, and firewalls). As well as encrypted terminal emulation, SSH can be used for SFTP and to achieve many other network configurations. Numerous commercial and open-source SSH servers and terminal emulation clients are available for all the major NOS platforms (UNIX®, Linux®, Windows®, and macOS®). The most widely used is OpenSSH (openssh.com). An SSH server listens on port TCP/22 by default.

Telnet

Telnet is both a protocol and a terminal emulation software tool that transmits shell commands and output between a client and the remote host. A Telnet server listens on port TCP/23 by default.

PuTTY Telnet client.



```
mail.classroom.local - PuTTY
220 mail.classroom.local ESMTP
hello localhost
250 Hello.
mail from:<administrator@web.local>
250 OK
rcpt to:<administrator@classroom.local>
250 OK
data
354 OK, send.
from: Tech Support <administratator@web.local>
to: Hostmaster <administrator@classroom.local>
subject: Virus infection
mime-version: 1.0;
content-type: text/html;

<html>
<body>
<p>Viruses have been detected on your hosted server. Visit the <a href="http://www.notagoodidea.net">Hosting Services Portal</a> and enter your password to scan and remove them.</p>
</body>
</html>
.
250 Queued (199.078 seconds)
```

Screenshot courtesy of PuTTY.

A Telnet interface can be password protected, but the password and other communications are not encrypted and therefore could be vulnerable to packet sniffing and replay. Historically, Telnet provided a simple means to configure switch and router equipment, but only secure access methods, like SSH, should be used for these tasks now.

Remote Desktop Protocol

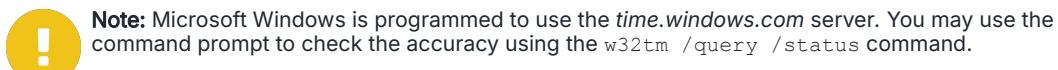
Telnet and SSH provide terminal emulation for command-line shells. This is sufficient for most administrative tasks, but where users want to connect to a desktop, they usually prefer to work with a graphical interface. A GUI remote administration tool sends screen and audio data from the remote host to the client and transfers mouse and keyboard input from the client to the remote host. **Remote Desktop Protocol** (RDP) is Microsoft's protocol for operating remote GUI connections to a Windows machine. RDP uses port TCP/3389. The administrator can specify permissions to connect to the server via RDP and can configure encryption on the connection.

RDP clients are available for other OSs, including Linux, macOS, iOS, and Android so you can connect to a Windows desktop remotely using a non-Windows device. There are also open-source RDP server products, such as xrdp (xrdp.org).

Time Servers

Network Time Protocol (NTP) allows networked systems to sync their clocks to a common source. This ensures network log entries have accurate time stamps for events. Some communication protocols also rely on an accurate clock to control the transmission of data across the network.

There are different levels of accuracy when it comes to a clock. The official term we utilize to differentiate the accuracy is through the use of Stratum levels. The most accurate clock source would be an atomic clock and this would be considered Stratum-0. NTP servers that sync their clocks to this source would be considered a Stratum-1 level of accuracy. Furthermore, NTP servers that sync their clocks to a Stratum-1 system are considered at a Stratum-2 degree of accuracy.



NTP servers operate on port UDP/123. Newer secure NTP servers are being introduced to protect the time servers. Imagine if all the clocks in the world were inaccurate! Network Time Security (NTS) was approved in 2020 and uses TLS encryption to protect the time data transfer on port TCP/4460.

Network Monitoring Servers

SSH and RDP allow administrators to log on and manage hosts and switches/routers/firewalls remotely. For a network to run smoothly, it is also important to gather information regularly from these systems. This type of remote monitoring can identify an actual or possible fault more quickly.

Simple Network Management Protocol

The **Simple Network Management Protocol** (SNMP) is a framework for management and monitoring network devices. SNMP consists of three components: a network management system, managed devices, and agents.

The agent is a process running on a switch, router, server, or other SNMP-compatible network device. This agent maintains a database called a management information base (MIB) that holds statistics relating to the activity of the device. An example of such a statistic is the number of frames per second handled by a switch. The agent is also capable of initiating a trap operation where it informs the network management system of a notable event (port failure, for instance). The threshold metric for triggering traps can be set for each value.

SNMP agents and management system

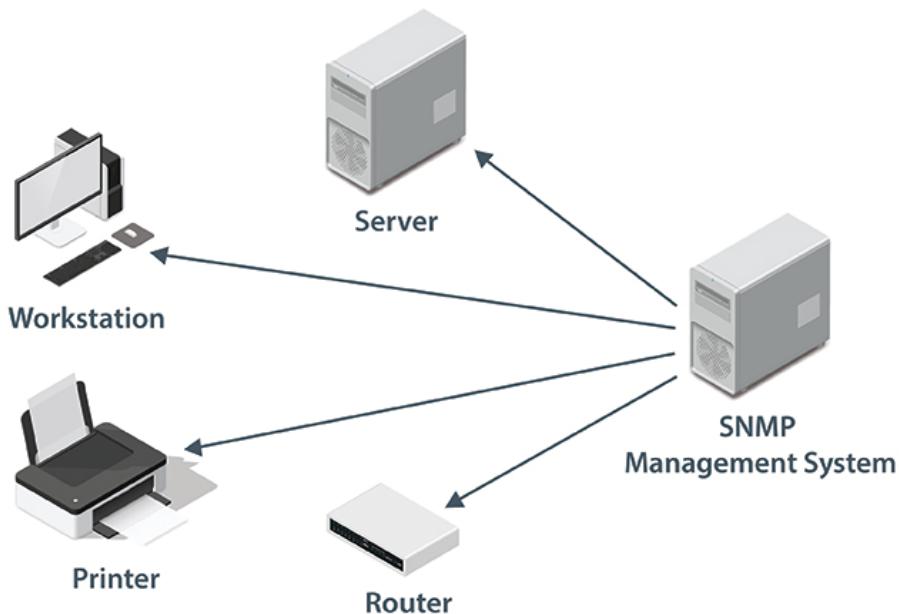


Image © 123RF.com.

The network management system monitors all agents by polling them at regular intervals for information from their MIBs and displays the information for review. It also displays any trap operations as alerts for the network administrator to assess and act upon as necessary.

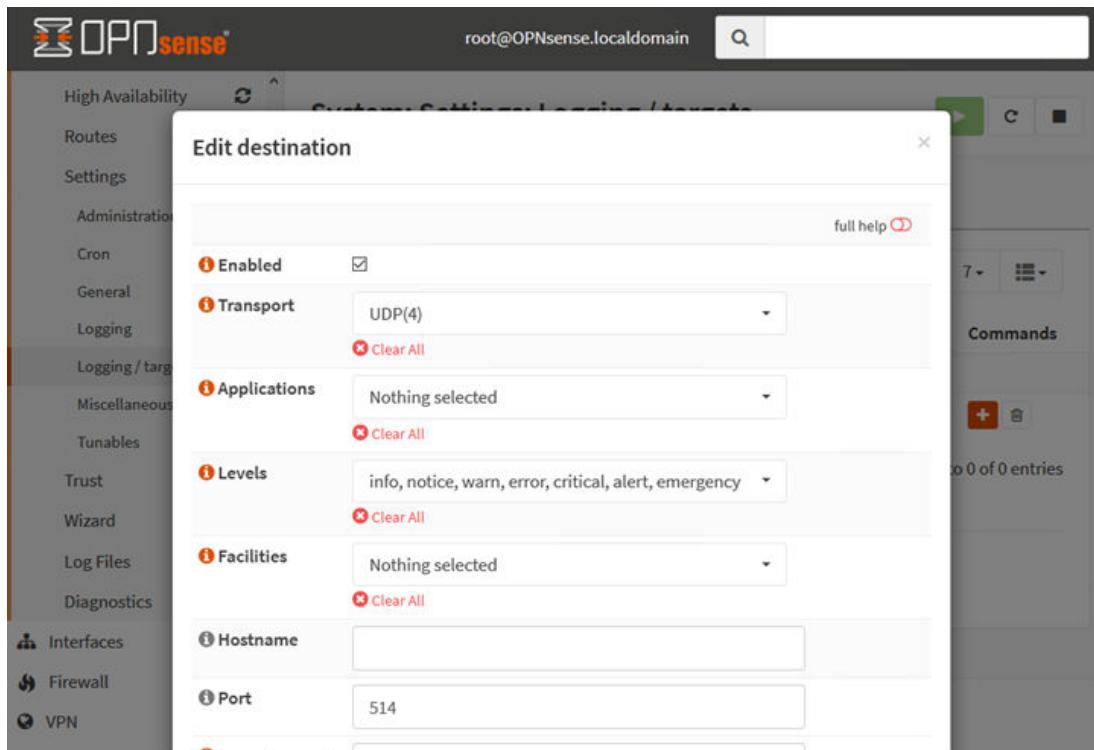
SNMP device queries take place over port UDP/161; traps are communicated over port UDP/162. While SNMP is available in three versions, SNMPv1 and v2 should not be used due to security concerns. SNMPv3 is preferred as it supports authentication between the management system and enrolled devices.

Syslog

Effective network management often entails capturing logs from different devices. It is more efficient to review logs and respond to alerts if the logs are consolidated on a single system. A log collector aggregates event messages from numerous devices to a single storage location. As well as aggregating logs, the system can be configured to run one or more status and alerting dashboards.

Syslog is an example of a protocol and supporting software that facilitates log collection. It has become a de facto standard for logging events from distributed systems. For example, syslog messages can be generated by routers and switches, as well as UNIX or Linux servers and workstations. A syslog collector usually listens on port UDP/514.

Configuring an OPNsense security appliance to transmit logs to a remote syslog server



Screenshot courtesy of OPNsense.

At the top, there is an option to enable or disable the configuration using a checkbox. The transport protocol can be selected from a dropdown menu, with UDP being one of the available options. Users can specify applications to log, although none are currently selected in this instance. Logging levels are customizable, with options such as info, notice, warn, error, critical, alert, and emergency. Facilities for logging can also be chosen, but none are selected in this setup. Fields are provided for entering the hostname and port of the logging server, with the default port set to 514.

As well as a protocol for forwarding messages to a remote log collector, syslog provides an open format for event data. A syslog message comprises a PRI code, a header containing a timestamp and host name, and a message part. The PRI code is calculated from the facility and the severity level. The message part contains a tag showing the source process plus content. The format of the content is application-dependent.

Lesson 7B

Internet and Embedded Appliances

Lesson Overview

Today's modern networks also include devices that are designed to help manage the security of the network in addition to adding convenience to our lives. For example, you may have an embedded computer in an automobile that allows interaction with a social media account and to share your music library for those long road trips. You also will find IoT devices being used to monitor the temperature or security of your home or business. Furthermore, we now see devices being deployed to appliances such as refrigerators or dishwashers. A camera in the refrigerator might allow you to remotely connect to see just how much milk is left while you are at the store. These "computers" are now connected to your network and will need to be managed while providing security and modern convenience, but you may also come across older systems that are kept around for a dedicated purpose.



Objectives Covered

2.3 Summarize services provided by networked hosts

Learning Outcomes

As you study this lesson, answer the following questions:

- How does a proxy server work?
- How does a spam gateway function?
- How does a load balancer increase the availability of resources?
- What is the purpose of a unified threat management system?
- What are several examples of IoT devices?

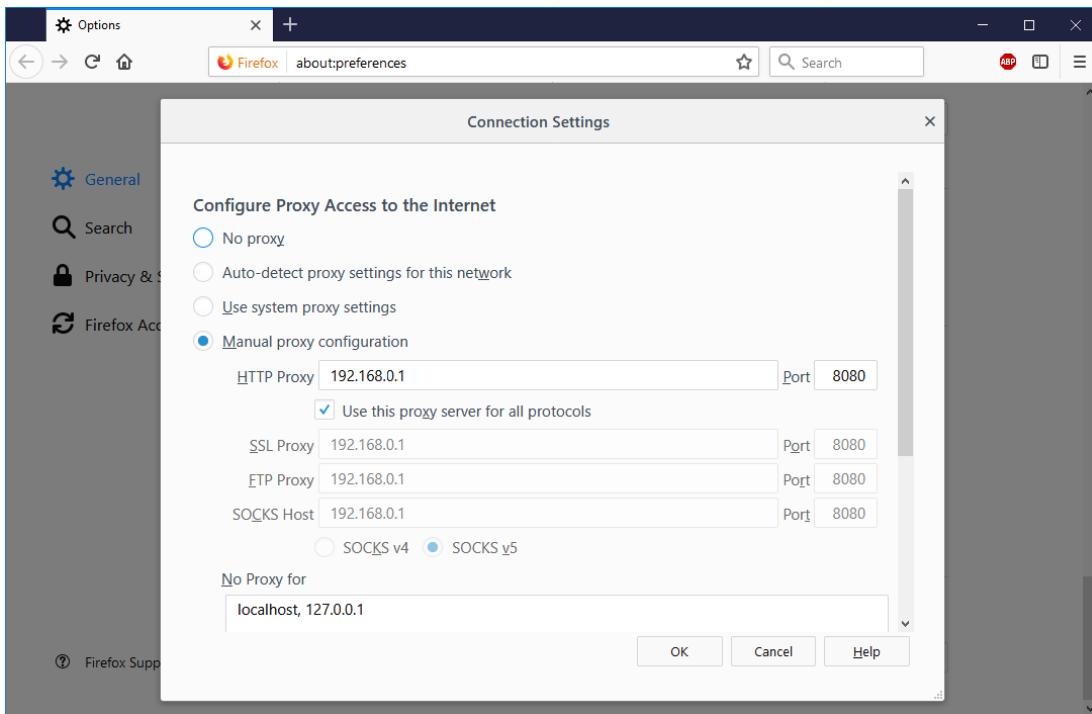
Proxy Servers

On a SOHO network, devices on the LAN access the Internet via the router using a type of network address translation (NAT), specifically port-based or overloaded NAT. Port-based NAT translates between the private IP addresses used on the LAN and the publicly addressable IP address configured on the router's WAN interface. Whereas, overloaded NAT, also known as PAT, is where a single IP address is shared amongst several nodes and they are differentiated by the port number for each connection.

Many enterprise networks also use some sort of NAT, but another option is to deploy a **proxy server**. A proxy server does not just translate IP addresses. It takes a whole HTTP request from a client, checks it, and then forwards it to the destination server on the Internet. When the reply

comes back, it checks it and then shuttles it back to the LAN computer. A proxy can be used for other types of traffic too (email, for instance).

Configuring the Firefox web browser to use a proxy server at 192.168.0.1 to connect to the Internet



Screenshot courtesy of Mozilla.

The user has selected the Manual proxy configuration option. In this configuration, the H T T P Proxy field is set to 192.168.0.1 with the port number 8080. The checkbox labeled Use this proxy server for all protocols is selected, causing the same proxy and port to populate the fields for S S L Proxy, F T P Proxy, and SOCKS Host. There are options to choose between SOCKS v 4 and SOCKS v 5 protocols, with SOCKS v 5 currently selected. Additionally, the No Proxy field includes localhost and 127.0.0.1. At the bottom, there are buttons for O K, Cancel, and Help.

A proxy server can usually operate either as a transparent service, in which case, the client requires no special configuration, or as non-transparent. For a nontransparent proxy, the client must be configured with the IP address and service port (often 8080 by convention) of the proxy server.

A proxy can perform a security function by acting as a content filter to block access to sites deemed inappropriate. It can also apply rules to access requests, such as restricting overall time limits or imposing time-of-day restrictions. As well as managing and filtering outgoing access requests, a proxy can be configured to cache content to improve performance and reduce bandwidth consumption.

Spam Gateways and Unified Threat Management

Networks connected to the Internet need to be protected against malicious threats by various types of security scanners. These services can be implemented as software running on PC servers, but enterprise networks are more likely to use purpose-built Internet security appliances. The range of security functions performed by these appliances includes the following:

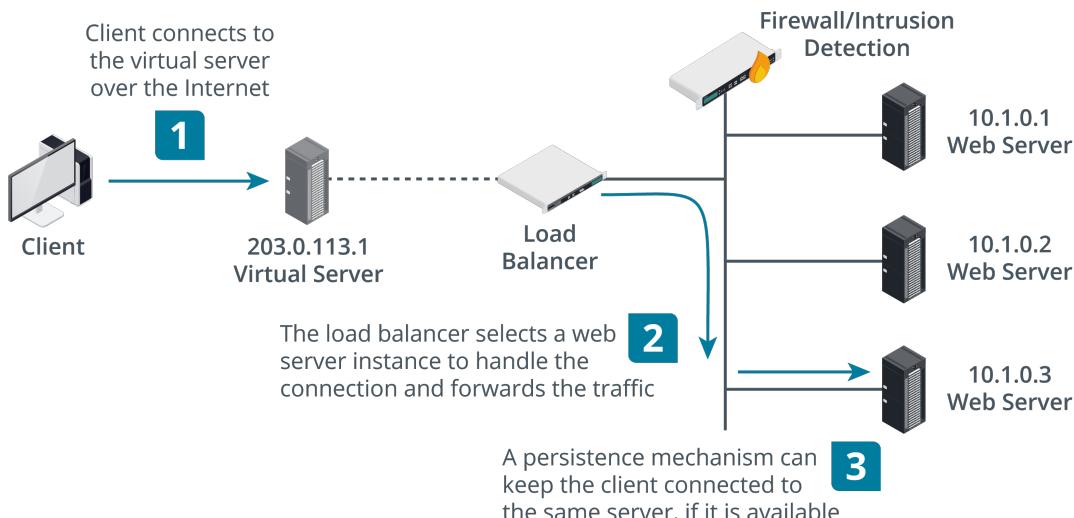
- Firewalls allow or block traffic based on a network access control list specifying source and destination IP addresses and application ports.
- Intrusion detection systems (IDS) are programmed with scripts that can identify known malicious traffic patterns. An IDS can raise an alert when a match is made. An intrusion prevention system (IPS) can additionally take some action to block the source of the malicious packets.
- Antivirus/antimalware solutions scan files being transferred over the network to detect any matches for known malware signatures in binary data.
- Spam gateways use SPF, DKIM, and DMARC to verify the authenticity of mail servers and are configured with filters that can identify spoofed, misleading, malicious, or otherwise unwanted messages. The spam gateway is installed as a network server to filter out these messages before it is delivered to the user's inbox.
- Content filters are used to block outgoing access to unauthorized websites and services.
- Data leak/loss prevention (DLP) systems scan outgoing traffic for information that is marked as confidential or personal. The DLP system can verify whether the transfer is authorized and block it if it is not.

These security functions could be deployed as separate appliances or server applications, each with its own configuration and logging/reporting system. A **unified threat management** (UTM) appliance is one that enforces a variety of security policies and controls, combining the work of multiple security functions. A UTM centralizes the threat management service, providing simpler configuration and reporting compared to isolated applications spread across several servers or devices.

Load Balancers

A **load balancer** can be deployed to distribute client requests across server nodes in a farm or pool. You can use a load balancer in any situation where you have multiple servers providing the same function. Examples include web servers, email servers, web conferencing servers, and streaming media servers. The load balancer is placed in front of the server network and distributes requests from the client network or Internet to the application servers. The service address is advertised to clients as a virtual server. This is used to provision high-availability services that can scale from light to heavy loads.

Topology of basic load balancing architecture.



The steps are as follows: Step 1: Client connects to the virtual server over the internet. Step 2: The load balancer selects a web server to handle the connection and forwards the traffic. Step 3: A persistence mechanism can keep the client connected to the same server, if it is available.

Legacy Systems

A **legacy system** is one that is no longer directly supported by its vendor. This might be because the vendor has gone out of business or formally deprecated use of the product. A product that is no longer supported is referred to as **end-of-life** (EOL). Networks often need to retain hosts running legacy OSs and applications software or old-style mainframe computers to run services that are too complex or expensive to migrate to a more modern platform.

Legacy systems usually work well for what they do—which is why they don't get prioritized for replacement—but they represent severe risks in terms of security vulnerabilities. If attackers discover faulty code that they can use to try to exploit the device, the vendor will not be available to develop a software patch to block the exploit. It is important to isolate them as far as possible from the rest of the network and to ensure that any network channels linking them are carefully protected and monitored.

Embedded Systems and SCADA

An **embedded system** is an electronic device that is designed to perform a specific, dedicated function. These systems can be as small and simple as a microcontroller in an intravenous drip-rate meter or as large and complex as an industrial control system managing a water treatment plant. Embedded systems might typically have been designed to operate within a closed network, where the elements of the network are all known to the system vendor and there is no connectivity to wider computer data networks. Where embedded systems need to interact within a computer data network, there are special considerations to make in terms of network design and support, especially regarding security.

Workflow and Process Automation Systems

An industrial control system (ICS) provides mechanisms for workflow and process automation. An ICS controls machinery used in critical infrastructure, such as power suppliers, water suppliers, health services, telecommunications, and national security services.

An ICS comprises plant devices and equipment with embedded programmable logic controllers (PLCs). The PLCs are linked by a cabled network to actuators that operate valves, motors, circuit breakers, and other mechanical components, plus sensors that monitor some local state, such as temperature. An embedded system network is usually referred to as an **operational technology network** to distinguish it from an IT network. Output and configuration of a PLC is performed by a human-machine-interface (HMI). An HMI might be a local control panel or software running on a computing host. PLCs are connected within a control loop, and the whole process automation system can be governed by a control server. Another important concept is the data historian, which is a database of all the information generated by the control loop.

Supervisory Control and Data Acquisition

A **supervisory control and data acquisition** (SCADA) system takes the place of a control server in large-scale, multiple-site ICSs. SCADAs typically run as software on ordinary computers, gathering data from and managing plant devices and equipment with embedded PLCs, referred to as "field devices." These embedded systems typically use WAN communications, such as cellular or satellite, to link the SCADA server to field devices.

Note: Both legacy and embedded systems represent a risk in terms of maintenance and troubleshooting as well as security because they tend to require more specialized knowledge than modern, off-the-shelf, computing systems. Consultants with expertise in such systems can become highly sought after.

Internet of Things Devices

The term **Internet of Things** (IoT) is used to describe the global network of wearable technology, home appliances, home control systems, vehicles, and other items that have been equipped with sensors, software, and network connectivity. These features allow these types of objects to communicate and pass data between themselves and other traditional systems, such as computer servers. Smart devices are used to implement home automation systems. An IoT smart device network will generally use the following types of components:

- **Hub/control system**—IoT devices usually require a communications hub to facilitate wireless networking. There must also be a control system, as many IoT devices are headless, meaning they cannot be operated directly using input and output devices. A hub could be implemented as a smart speaker operated by voice control or use a smartphone/PC app for configuration.
- **Smart device**—IoT endpoints implement the function, such as a smart lightbulb, refrigerator, thermostat/heating control, or doorbell/video entry phone that you can operate and monitor remotely. These devices are capable of computer, storage, and network functions that are all potentially vulnerable to malicious code. Most smart devices use a Linux or Android kernel. Because they're effectively running mini-computers, smart devices are vulnerable to some of the standard attacks associated with web applications and network functions. Integrated peripherals, such as cameras or microphones, could be compromised to facilitate surveillance.

While the control system is typically joined to the Wi-Fi network, smart devices may use other wireless technologies, such as Z-Wave or Zigbee, to exchange data via the hub. These protocols are designed for operation on low-power devices without substantial CPU or storage resources.

Lesson 7C

Troubleshoot Networks

Lesson Overview

As an IT specialist, you will find much of your time on the clock will be spent troubleshooting issues with the networks and systems that facilitate communications for the business or client. From wired network cable issues that require a new cable to be terminated or a switch that has a misconfigured port, troubleshooting these network issues will require a technician to think quickly about the issue and find a solution to restore the services and systems needed. Modern networks also require a technician to understand the physical and logical operations of the network to understand where the issue is and its effects on the organization.



Objectives Covered

5.5 Given a scenario, troubleshoot network issues

Learning Outcomes

As you study this lesson, answer the following questions:

- What are common issues found on wired networks and how are they resolved?
- What are the common issues found in wireless networks and how are they resolved?
- What unique problems stem from the use of VOIP systems on a network?

Troubleshoot Wired Connectivity

A client-wired connectivity issue means that either the network adapter does not establish a network link at all (no connectivity) or the connection is unstable or intermittent. Assuming that you can establish that the problem affects a single host only, you need to isolate the precise location of the physical issue.

Troubleshoot Cable and Network Adapter Issues

A typical Ethernet link for an office workstation includes the following components:

- NIC port on the host.
- RJ45 terminated patch cord between the host and a wall port.
- Structured cable between the wall port and a patch panel, terminated to insulation displacement connector (IDC) blocks (the permanent link).
- RJ45 terminated patch cord between the patch panel port and a switch port.
- Network transceiver in the switch port.

 **Note:** The link LEDs on network adapter and switch ports will indicate whether the link is active and possibly at what speed the link is working. The LEDs typically flicker to show network activity.

1. The first step in resolving a no or intermittent connectivity issue is to check that the patch cords are properly terminated and connected to the network ports. If you suspect a fault, substitute the patch cord with a known good cable. You can verify patch cords using a cable tester.
2. If you cannot isolate the problem to the patch cords, test the transceivers. You can use a loopback tool to test for a bad port.
3. If you don't have a loopback tool available, another approach is to substitute known working hosts (connect a different computer to the link or swap ports at the switch). This method may have adverse impacts on the rest of the network, however, and issues such as port security may make it unreliable.
4. If you can discount faulty patch cords and bad network ports/NICs, use a cable tester to verify the structured cabling. The solution may involve installing a new permanent link, but there could also be a termination or external interference problem. An advanced type of cable tester called a "certifier" can report detailed information about cable performance and interference.
5. If there is no issue in the structured cabling, verify the Ethernet speed/duplex configuration on the switch interface and NIC. This should usually be set to auto-negotiate. You might also try updating the NIC's device driver software.

Troubleshoot Port Flapping Issues

Intermittent connectivity might manifest as [port flapping](#), which means that the NIC or switch interface transitions continually between up and down states. This is often caused by bad cabling, external interference, or a faulty NIC at the host end. You can use the switch configuration interface to report how long a port remains in the up state.

Troubleshoot Network Speed Issues

The transfer speed of a cabled link could be reduced by mismatched duplex settings on the network adapter and switch port. With Gigabit Ethernet, both should be set to autonegotiate. Check the configuration of the network adapter driver on the client OS and the setting for the switch port via the switch's management software.

If there is no configuration issue, **slow network speeds** can be caused by a variety of other problems and are difficult to diagnose. Apply a structured process to investigate possible causes:

1. If a user reports slow speed, establish exactly what network activity they are performing (web browsing, file transfer, authentication, and so on). Establish that there is a link speed problem by checking the nominal link speed and using a utility to measure transfer rate independent of specific apps or network services.
2. If you can isolate the speed issue to a single cable segment, the cabling could be affected by interference. External interference is typically caused by nearby power lines, fluorescent lighting, motors, and generators. Poorly installed cabling and connector termination can also cause a type of interference called "crosstalk." Check the ends of cables for excessive untwisting of the wire pairs or improper termination. If you have access to a network tap, the analyzer software is likely to report high numbers of damaged frames. You can also view error rates from the switch interface configuration utility. You may also need to use shielded cables to reduce interference.
3. If the cabling is not the issue, there could be a problem with the network adapter driver.

Install an update if available. If the latest driver is installed, check whether the issue affects other hosts using the same NIC and driver version.

4. Consider the possibility that the computer could be infected with malware or have faulty software installed.

Consider removing the host from the network for scanning. If you can install a different host to the same network port and that solves the issue, identify what is different about the original host.

5. Establish the scope of the problem: are network speeds an issue for a single user, for all users connected to the same switch, or for all users connecting to the Internet, for instance? There may be congestion at a switch or router or some other network-wide problem.

This might be caused by a fault or by user behavior, such as transferring a very large amount of data over the network.

Troubleshoot Wireless Issues

When troubleshooting wireless networks, as with cabled links, you need to consider problems with the physical media, such as interference, and configuration issues.

The radio frequency (RF) signal from radio-based devices weakens considerably as the distance between the devices increases. If you experience **intermittent wireless connectivity**, slow transfer speeds, or inability to establish a connection, as a first step, try moving the devices closer together. If you still cannot obtain a connection, check that the security and authentication parameters are correctly configured on both devices. Authentication failures usually result from entering the incorrect network password or selecting the wrong security standard.

Troubleshooting Wireless Configuration Issues

If a user is looking for a network name that is not shown in the list of available wireless networks (SSID not found), the user could be out of range or the SSID name broadcast might be suppressed. In the latter scenario, the connection to the network name must be configured manually on the client.

Another factor to consider is standards mismatch. If an access point is not operating in compatibility mode, it will not be able to communicate with devices that only support older standards. Also, when an older device joins the network, the performance of the whole network can be affected. To support 802.11b clients, an 802.11b/g/n access point must transmit legacy frame preamble and collision avoidance frames, adding overhead. If possible, upgrade 802.11b devices rather than letting them join the WLAN. Both 802.11g and 802.11n/ac/ax are more compatible in terms of negotiating collision avoidance.

Also, consider that not all clients supporting 802.11n have dual-band radios. If a client cannot connect to a network operating on the 5 GHz band, check whether its radio is 2.4 GHz-capable only.

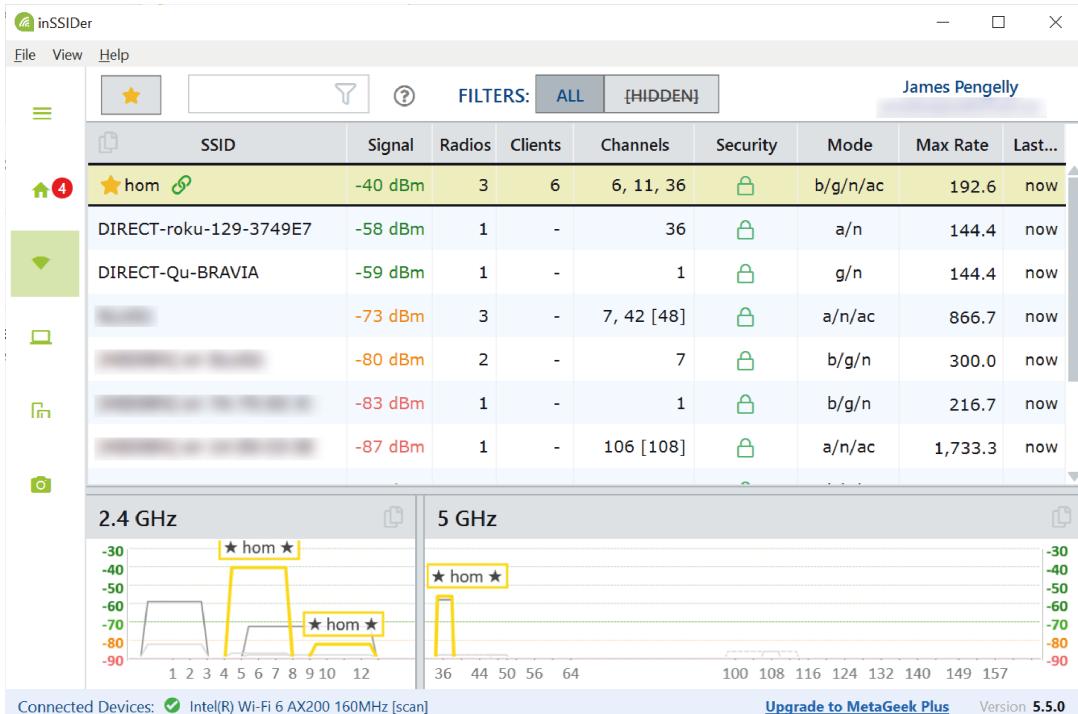
Received Signal Strength Indicator

A wireless adapter will reduce the connection speed if the **received signal strength indicator** is not at a minimum required level. The RSSI is an index level calculated from the signal strength level. For example, an 802.11n adapter might be capable of a 144 Mbps data rate with an optimum signal, but if the signal is weak, it might reduce to a 54 Mbps or 11 Mbps rate to make the connection more reliable. If the RSSI is too low, the adapter will drop the connection entirely and try to use a different network. If there are two weak networks, the adapter might "flap" between them. Try moving to a location with better reception.

Troubleshooting Wireless Signal Issues

If a device is within the supported range but the signal is weak or you can only get an **intermittent connection**, there is likely to be interference from another radio source broadcasting at the same frequency. If this is the case, try adjusting the channel that the devices use. Another possibility is interference from a powerful electromagnetic source, such as a motor, or a microwave oven. Finally, there might be something blocking the signal. Radio waves do not pass easily through metal or dense objects. Construction materials, such as wire mesh, foil-backed plasterboard, concrete, and mirrors, can block or degrade signals. Try angling or repositioning the device or antenna to try to get better reception.

Surveying Wi-Fi networks using inSSIDer



Screenshot courtesy of MetaGeek, LLC. © Copyright 2005-2021.

The top bar has a search tab, a filters option, and the user's account name. Below the top bar is a table with heads, S S I D, Signal, Radios, Clients, Channels, Security, Mode, Max rate, and Last modified. Graphs titled 2.4 Gigahertz and 5 Gigahertz are displayed at the bottom.

Wi-Fi analyzer software is designed to identify the signal strength of nearby networks on each channel. It shows the signal strength, measured in dBm, and expressed as a negative value, where values close to zero represent a stronger signal. The analyzer will show how many networks are utilizing each channel. Setting the network to use a less congested channel can improve performance.

Troubleshoot VoIP Issues

While slow network speeds are a problem for all types of network traffic, there are other performance characteristics that affect real-time network protocols and devices. "Real time" refers to services such as voice and video. One example is **voice over internet protocol (VOIP)** protocols. These use data networks to implement voice calling. The symptoms of poor VoIP service quality are dropouts, echo, or other glitches in the call.

With "ordinary" data, it might be beneficial to transfer a file as quickly as possible, but the sequence in which the packets are delivered and variable intervals between packets arriving do not materially affect the application. This type of data transfer is described as "bursty." Network protocols, such as HTTP, FTP, or email, are sensitive to packet loss but tolerant of delays in delivery. The reverse is applicable to real-time applications. These can compensate for some amount of packet loss but are very sensitive to delays in data delivery or packets arriving out of sequence.

Problems with the timing and sequence of packet delivery are defined as latency and jitter:

- **Latency** is the time it takes for a signal to reach the recipient, measured in milliseconds (ms). Latency increases with distance and can be made worse by processing delays at intermediate systems, such as routers. VoIP can support a maximum one-way latency of about 150 ms. Round trip time (RTT) or two-way latency is the time taken for a host to receive a response to a probe.
- **Jitter** is the amount of variation in delay over time and is measured by sampling the elapsed time between packets arriving. VoIP can use buffering to tolerate jitter of up to around 30 ms without a severe impact on call quality. Jitter is typically caused by network congestion affecting packet processing on routers and switches.

VoIP call quality can only really be established by using a **quality of service** (QoS) mechanism across the network. QoS means that switches, access points, and routers are all configured to identify VoIP data and prioritize it over bursty data. Enterprise networks can deploy sophisticated QoS and traffic engineering protocols on managed switches and routers. However, it is difficult to guarantee QoS over a public network, such as the Internet.

On a SOHO network, you may be able to configure a QoS or bandwidth control feature on the router/modem to prioritize the port used by a VoIP application over any other type of protocol. This will help to mitigate issues if, for example, one computer is trying to download a Windows 11 feature update at the same time as another set of computers is trying to host a video conference.

The Bandwidth Control feature on this router/modem provides a basic QoS mechanism

TP-LINK Archer VR900

Quick Setup Basic Advanced English Logout Reboot

NAT Forwarding USB Settings Parental Controls **Bandwidth Control** ?

Bandwidth Control

Bandwidth Control: Enable

Line Type: ADSL Other

Current Upstream Rate: 36333 Kbps

Current Downstream Rate: 100013 Kbps

Total Upstream Bandwidth: 36333 Kbps

Total Downstream Bandwidth: 100013 Kbps

IPTV Bandwidth Guarantee: Enable

Save

Controlling Rules

	Description	Priority	Up (min/max)	Down (min/max)	Enable	Modify
<input type="checkbox"/>	--	--	--	--	--	--

Firmware Version: 0.1.0 0.9.1 v0069.0 Build 160525 Rel.38143n Hardware Version: Archer VR900 v2 00000000 Support

Screenshot courtesy of TP-Link.

The top bar has tabs Quick Setup, Basic, and Advanced. The top-right corner has options for Logout and Reboot. On the left sidebar, there is a menu with several options: NAT Forwarding, USB Settings, Parental Controls, Bandwidth Control, Security, and System Tools. The main content area is titled, the Bandwidth Control. The page includes a section for enabling bandwidth control, with a checkbox labeled Enable that is currently selected. The Line Type is set to ADSL, with fields displaying the current upstream rate as 36333 kilo bytes per second and the current downstream rate as 100013 kilo bytes per second. Users can configure the total upstream and downstream bandwidth, which are set to the same values. There is also an option for enabling IPTV bandwidth guarantees, which is currently disabled. A save button is below. A table below is titled, Controlling Rules. An add and delete button is above the table. The column headers are blank, description, priority, up (min/max), down (min/max), enable, and modify.

You should also be able to use the management interface to report connection latency and possibly jitter too. If not, you can use a speed test site to measure latency and bandwidth. If latency is persistently higher than an agreed service level, contact your ISP to resolve the issue.

Troubleshoot Limited Connectivity

In Windows, a **limited connectivity** message specifically means that the host can establish a physical connection to the network but has not received a lease for an IP configuration from a DHCP server. The host will be configured with an address in the automatic private IP addressing (APIPA) 169.254.x.y range. A Linux host might also use APIPA, set the IP address to unknown (0.0.0.0), or just leave the IP unconfigured.

- **Establish the scope of the issue**—If the issue affects multiple users, the problem is likely to be the DHCP server itself. Remember that DHCP leases take time to expire, so a problem

with the DHCP server might take a few hours to manifest as different clients try to renew their leases over time. The DHCP server could be offline, it could have run out of available leases, or forwarding between the server and clients could be improperly configured.

- **Check the configuration of patch cords**—Verify that the wall port is connected to an appropriate port on a switch via the patch panel. If the computer is not connected to an appropriate switch port, it is unlikely to connect to the expected services, such as its default gateway, DHCP, and DNS.
- **Check the VLAN configuration**—If the switch port is not configured with the correct VLAN ID, it can have the same effect as connecting the host to the wrong switch port.

Windows may also report that a network adapter has no Internet access. This means that the adapter has obtained an IP configuration (or is configured statically) but cannot reach the Microsoft test site to download a test file. This error indicates that there is an issue with either Internet access at the gateway router or name resolution. On a SOHO network, access the router management interface and verify the Internet connection via a status update page. If the link is down, contact your ISP. The router may also have tools to test connectivity. Verify that it can connect to the servers configured for DNS.

Module 8

Summarizing Virtualization and Cloud Concepts

Module Overview

You work at a mid-sized law firm that is transitioning to a more virtualized and cloud-based infrastructure. Your role involves managing client devices, supporting desktop and laptop users, and ensuring the smooth operation of virtualized environments and cloud services. The firm is looking to improve its hardware utilization, enhance security, and provide flexible, scalable solutions for its employees.

Module Summary

Prepare for A+ Core 1 by:

- Summarizing client-side virtualization
- Summarizing cloud concepts

Lesson 8A

Client-Side Virtualization

Lesson Overview

To support the development and testing of new legal software applications at the law firm, you need to set up a client-side virtualization environment on the existing desktop computers. This will allow developers to test applications in isolated environments without affecting the host system. By doing so, you will ensure that the development process is efficient and secure, while also maintaining the stability of the primary operating systems used by employees.



Objectives Covered

4.1 Explain virtualization concepts

Learning Outcomes

As you study this lesson, answer the following questions:

- What are the differences between Type 1 and Type 2 hypervisors, and which would be more suitable for client-side virtualization on employee workstations?
- How can client-side virtualization be used to support legacy software and provide sandbox environments for testing?
- What are the key resource requirements for setting up a client-side virtualization workstation?
- How does the amount of system memory affect the performance of virtual machines on a client-side virtualization setup?
- How does container virtualization differ from traditional virtual machine (VM) virtualization, and what are the benefits of using containers?

Hypervisors

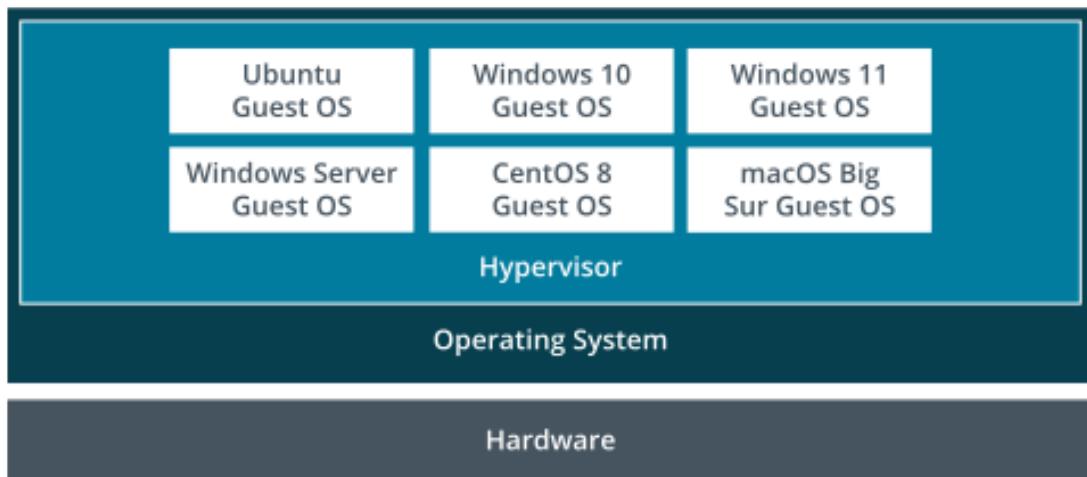
A typical computer is designed to run a single operating system (OS) at a time, meaning all applications on that machine share the same OS environment. However, advances in CPU and memory technology now allow most computers, except entry-level models, to support **virtualization**—the ability to run multiple OSs simultaneously on one system.

The software that enables this is called a *hypervisor*. It manages **virtual machines** (VMs), also known as guest OSs, by emulating hardware resources such as the CPU, memory, storage, and peripherals, allowing each guest OS to function as if it has exclusive access to the system. To function properly, VMs require drivers for the emulated hardware. Hypervisors may have limits on the types of guest OSs they can support.

There are two main types of hypervisors:

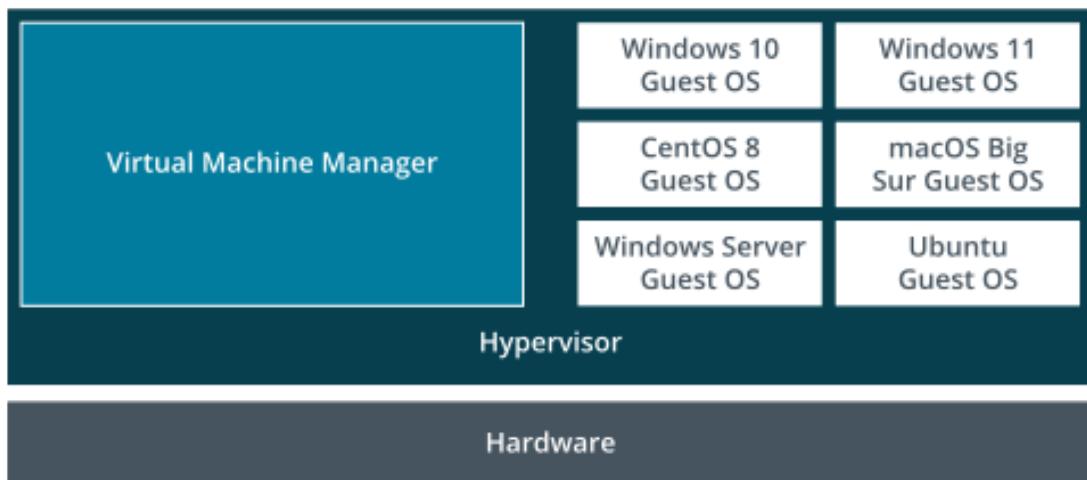
- **Type 2 (Host-based Hypervisors):** These are installed on top of an existing host OS. Examples include VMware Workstation™, Oracle® Virtual Box, and Parallels® Workstation. The system must have enough resources to run both the host OS and the guest OSs through the hypervisor.

Guest OS virtualization (Type II hypervisor)



- **Type 1 (Bare Metal Hypervisors):** These are installed directly onto the hardware, bypassing a host OS. Examples include VMware ESXi® Server, Microsoft's Hyper-V®, and Citrix's XEN Server. The hardware only needs to meet the system requirements of the hypervisor and the guest OSs.

Type I bare metal hypervisor



Uses for Virtualization

There are many different **purposes** for deploying virtualization.

Client-Side Virtualization

Client-side virtualization refers to solutions designed to run on standard desktops or workstations, where each user interacts directly with the virtualization host. Desktop virtual platforms, typically based on a guest OS hypervisor, are commonly used for **testing and development**:

- **Sandboxing:** Create an isolated environment, or sandbox **sandbox**, to analyze malware (viruses, worms, Trojans). Containing malware within the guest OS prevents it from infecting the researcher's computer or network.
- **Supporting legacy software and OSs:** If host computers are upgraded, older software may not be compatible with the new OS. The old OS can be installed as a VM, allowing access to the legacy software.
- **Cross-platform virtualization:** Test software applications under different OSs and resource constraints.
- **Training:** Set up lab environments for students to practice using a live OS and software without affecting the production environment. Changes to the VM can be discarded after the lab, restoring the original environment for the next student.

Server-Side Virtualization

Server-side virtualization involves deploying a server role as a virtual machine (VM). The primary benefit is improved hardware utilization through server consolidation. Typically, a hardware server may only utilize about 10% of its resources. By virtualizing, you can run 8-9 additional server instances on the same hardware without compromising performance.

Desktop Virtualization

Virtual desktop infrastructure (VDI) uses VMs to provision corporate desktops, replacing traditional desktop computers with low-spec thin clients. A thin client is a computer that uses a centralized server for most of its resources, instead of a hard drive.

When a thin client starts, it boots a minimal OS, allowing the user to log on to a VM stored on the company server or cloud infrastructure. The user connects to the VM using a remote desktop protocol, such as Microsoft Remote Desktop or Citrix ICA (Independent Computing Architecture). The thin client locates the correct VM image and uses an appropriate authentication mechanism, which may involve a 1:1 mapping based on machine name or IP address or be managed by a connection broker.

In this **desktop virtualization** setup, all application processing and data storage occurs on the server. The thin client only needs to display the screen image, play audio, and transfer mouse, keyboard, video, and audio information over the network.

The virtualization server hosting the virtual desktops can be **on-premises** (on the same local network as the client) or in the **cloud**. Centralizing data simplifies backups, and desktop VMs are easier to support, troubleshoot, and secure. Any changes to the VM can be easily overwritten from the template image, and IT infrastructure can be offloaded to a third-party services company.

The main disadvantage is that users have no local processing ability during server or network failures, potentially leading to costly downtime.



Provisioning VDI as a cloud service is often referred to as **Desktop as a Service (DaaS)**.

Application Virtualization

[Application virtualization](#) allows clients to access or stream applications from a server, ensuring they always run the latest version without local installation. This simplifies updates and maintenance for administrators.

Most solutions are based on Citrix Virtual Apps (formerly XenApp), while Microsoft offers App-V within its Windows Server range, and VMware provides ThinApp.

Container Virtualization

Container virtualization eliminates the need for a hypervisor by isolating resources at the OS level. Containers run processes through the host OS kernel, with each container allocated CPU and memory. While containers can run different OS distributions, they must use the same OS kernel (e.g., you cannot run Windows in a Linux container).

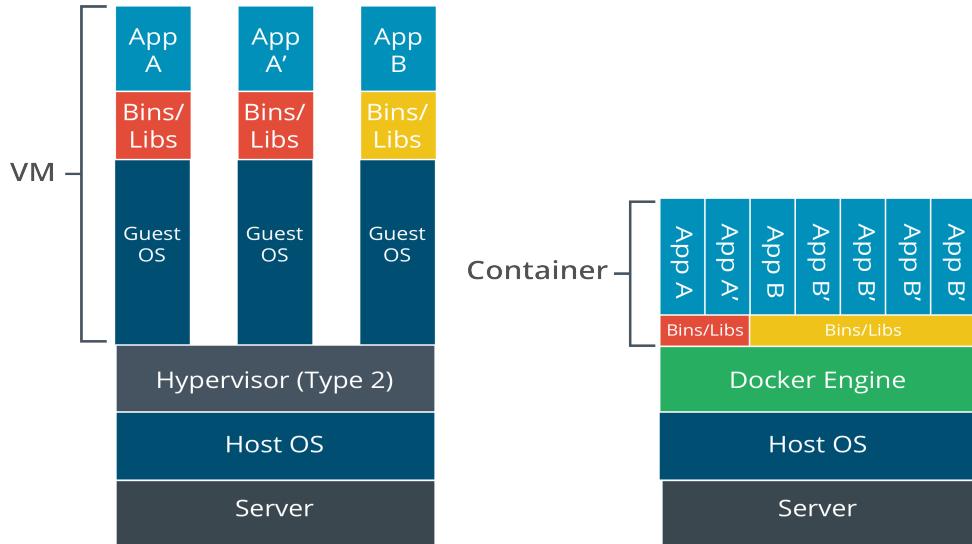
Containers often encapsulate specific application processes, along with the necessary libraries and environment variables. This makes them lightweight compared to virtual machines.

One of the best-known container virtualization products is Docker ([docker.com](https://www.docker.com)).

[Containerization](#) is also being widely used to implement corporate workspaces on mobile devices.

Comparison of virtual machines versus containers

Container vs. VMs



Virtualization Resource Requirements

To deploy a client-side virtualization workstation, identify the **resource requirements** for both the hypervisor and each guest OS you plan to install.

CPU and Virtualization Extensions

CPU vendors have developed special instruction sets to enhance virtualization performance. Intel's technology is called "VT-x" (Virtualization Technology), while AMD's is "AMD-V". Additionally, most virtualization products benefit from "Second Level Address Translations" (SLAT), which improves virtual memory performance when multiple VMs are installed. Intel's SLAT implementation is "Extended Page Table" (EPT), and AMD's is "Rapid Virtualization Indexing" (RVI).

Most virtualization software requires a CPU with virtualization support enabled. Even if not mandatory, VM performance will suffer without hardware-assisted virtualization. Some cheaper CPUs lack this feature, and it may be disabled in the system firmware. When choosing a computer for virtualization, ensure the CPU supports Intel VT-x or AMD-V and SLAT, and verify these features are enabled in the system setup.

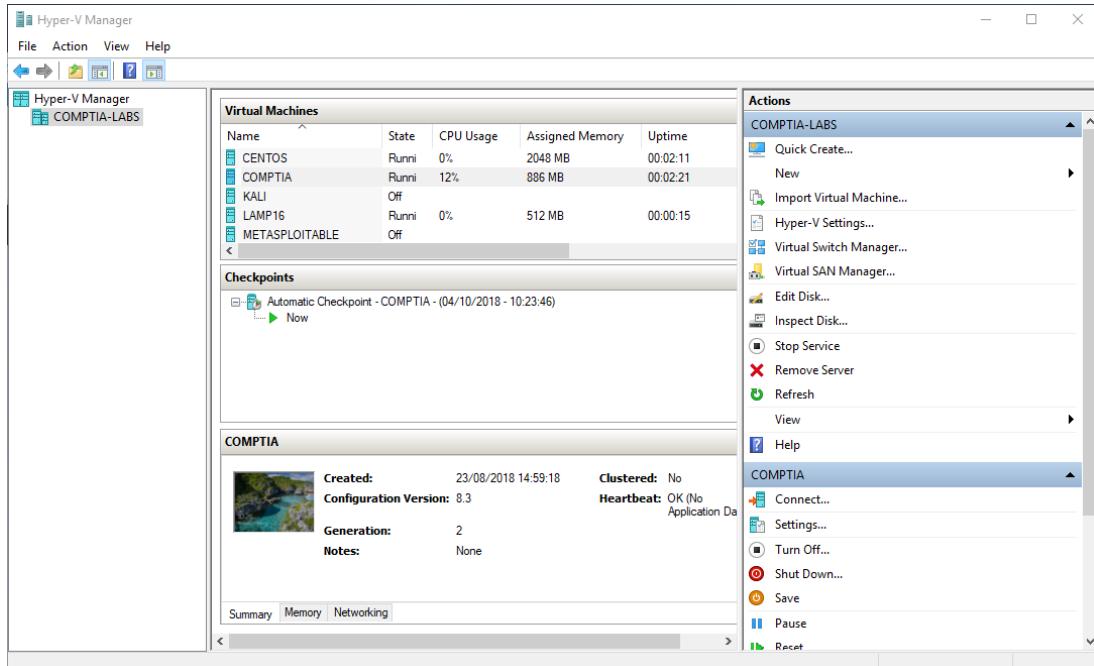
Apart from virtualization extensions, multiple CPU resources—whether through multiple physical processors, multi-core, or HyperThreading—greatly enhance performance, especially when running multiple guest OSs concurrently.

Note: A 64-bit hypervisor can support 32-bit guest OSs if the hypervisor allows it. However, 32-bit hypervisors cannot support 64-bit guest OSs

System Memory

Each guest OS requires additional system memory beyond what the host OS/hypervisor needs. For example, Windows 11 requires at least 4 GB of memory. Therefore, a virtualization workstation must have at least 8 GB of RAM to run the host and a single Windows 11 guest OS. Running multiple guest OSs concurrently will increase memory demands. If the VMs are used only for development and testing, performance may be less critical, allowing for lower memory specifications.

Microsoft Hyper-V hypervisor software



Screenshot courtesy of Microsoft.

The main pane lists several virtual machines, including centos, CompTIA, kali, L A M F 16, and meta S P L O I table. Each virtual machine entry displays its current state such as, Running or Off, C P U usage, assigned memory, and uptime. Below the virtual machine list is a section for Checkpoints, showing an automatic checkpoint for the CompTIA virtual machine with a timestamp. A detailed pane at the bottom provides information about the selected virtual machine, including its creation date, configuration version, generation, notes, clustered, and heartbeat.

On the right, the Actions pane for COMPTIA-LABS offers management options, such as quick create, New, Import Virtual Machine, Hyper-V Settings, Virtual Switch Manager, Virtual SAN Manager, Edit Disk, Inspect Disk, Stop Service, Remove Server, Refresh, View, and Help. The pane for COMPTIA has options, Connect, Settings, Turn Off, Shut Down, Save, Pause, and Reset.

Mass Storage

Each guest OS requires significant disk space, with the VM's "hard disk" stored as an image file on the host. Most hypervisors use dynamically expanding disk images that grow as more data is added to the guest OS. For example, a typical Windows installation might require around 20–30 GB of space, depending on the version and installed applications.

Snapshots, which capture the VM's disk state at a specific point in time, can increase storage demands. They are useful for rolling back changes during testing or system modifications but consume additional space, as each snapshot preserves a different disk state.

 In an enterprise environment, you are not limited by the local disk space of the host machine. Disk images can be stored in a high-speed storage area network (SAN).

Networking

A hypervisor can create a virtual network allowing communication between VMs, the host, and other hosts. Enterprise virtualization platforms also support configuring virtual switches and routers.

Virtualization Security Requirements

Like any computing technology, deploying a virtualization solution comes with **security requirements** and challenges.

Guest OS Security

Each guest OS requires regular patching and protection against malware, just like a physical OS. However, patching individual VMs can impact performance. To mitigate this, many environments use a template [image](#) that is patched, tested, and then deployed to production.

Running security software, such as antivirus or intrusion prevention, on every guest OS can degrade performance. Modern virtualization-aware security solutions allow security to be managed at the hypervisor or host level, reducing the overhead on individual VMs.



Note: Standard antivirus software on the host cannot detect malware inside guest OSs. Scanning virtual disks from the host can cause severe performance issues.

Uncontrolled deployment of unauthorized VMs, known as rogue VMs, leads to [virtual machine sprawl](#), complicating security and resource management. System management tools can detect and control rogue builds.

Security management should include strict controls over VM template development, ensuring they are free from unnecessary services, malware, or unauthorized code. One of the major

risks is rogue developers or contractors inserting backdoors or malicious code, such as "logic bombs", into VM images.

Host Security

In virtualization, the host is a **single point of failure** for multiple guest OS instances. If the host goes down (e.g., due to power loss or hardware failure), all guest VMs and their applications go offline simultaneously.

Modern virtualization environments mitigate this risk with high availability solutions, which automatically restart VMs on another host in case of failure, and power redundancy, such as using uninterruptible power supplies (UPS) or backup generators.

Hypervisor Security

In addition to securing guest OSs and the host, the hypervisor itself must be monitored for vulnerabilities. One critical threat is [virtual machine escaping](#), where malware on a guest OS can access other guest VMs or the host. To mitigate this, it's essential to keep the hypervisor patched with updates for critical vulnerabilities, just like any other software.

Lesson 8B

Cloud Concepts

Lesson Overview

In your efforts to implement a virtualized environment at the law firm and to ensure high availability and scalability, you need to explore cloud solutions that can complement the virtualized environment. This includes evaluating different cloud deployment models and service models to determine the best fit for the company's needs.



Objectives Covered

4.2 Summarize cloud computing concepts

Learning Outcomes

As you study this lesson, answer the following questions:

- What are the key characteristics of cloud computing that distinguish it from traditional on-premises IT infrastructure?
- Which cloud deployment model would you recommend for a company that needs high availability and data security, and why?
- How can Infrastructure as a Service (IaaS) and Software as a Service (SaaS) benefit a company in terms of resource provisioning and software deployment?
- What are some key advantages of using cloud file storage services like Microsoft OneDrive, Dropbox, Apple iCloud, and Google Drive for file synchronization and collaboration?
- What are the three layers defined in the Software-Defined Networking (SDN) model by IETF, and what is the primary function of each layer?

Cloud Characteristics

Cloud characteristics distinguish cloud provisioning from on-premises or hosted client/server network architecture.

From the consumer's perspective, [cloud computing](#) provides on-demand resources—such as server instances, file storage, databases, or applications—over a network, typically the Internet. Users don't manage the underlying infrastructure and pay only for what they use, a model known as [metered utilization](#). Metering is based on resource types like storage, processing, bandwidth, or active users. This includes charges for [ingress](#) (data entering the cloud) and [egress](#) (data leaving the cloud). The metering mechanism is accessible via a reporting dashboard for transparency.

From the provider's perspective, cloud infrastructure operates like any large-scale datacenter, using virtualization to allocate resources efficiently.

Key cloud computing benefits include:

- **High Availability:** Minimal downtime, with services like "Five Nines" (99.999%) availability, equating to only 5 minutes and 15 seconds of annual downtime.
- **Scalability:** Costs involved in supplying the service to more users are linear. For example, if the number of users doubles in a scalable system, the costs to maintain the same level of service would also double (or less than double). If costs are more than double, the system is less scalable. Scalability can be achieved by adding nodes (horizontal/scaling out) or by adding resources to each node (vertical/scaling up).
- **Rapid Elasticity:** The ability to handle real-time demand changes without loss of service or performance. Systems can also reduce costs when demand is low.

Cloud providers meet these requirements through automatic provisioning and de-provisioning of resources, achieved via pooling **shared resources** and virtualization. Shared resource pooling means datacenter hardware is not dedicated to a single customer. Virtualization allows providers to manage resources like CPU, memory, disk, or network through software, rather than manual hardware adjustments.

Common Cloud Deployment Models

Cloud deployment models can be categorized based on ownership and access arrangements:

- **Public (Multitenancy):** Offered over the Internet by a cloud service provider (CSP) to multiple tenants. This model often includes subscription or pay-as-you-go options, and sometimes free lower-tier services. As a shared resource, it carries performance and security risks. Multicloud architectures involve using services from multiple CSPs.
- **Private:** Cloud infrastructure exclusively owned and managed by an organization. A dedicated business unit typically manages the cloud, while other units use it. This model offers greater control over privacy and security, making it ideal for banking and governmental services requiring strict access control.
- **Community:** Several organizations share the costs of a hosted private or fully private cloud to pool resources for common concerns, such as standardization and security policies.
- **Hybrid:** Combines public, private, and/or community cloud elements. For example, a travel organization might use a private cloud for most of the year but switch to a public cloud during peak times. Alternatively, a hybrid deployment might use a public cloud for some functions while keeping sensitive data and applications on-premises.

Common Cloud Service Models

A **cloud service model** is differentiated by the level of complexity and preconfiguration provided, in addition to the deployment model (public, private, community, or hybrid). The most common models are Infrastructure, Software, Platform, and Desktop.

Infrastructure as a Service (IaaS) allows organizations to provision and manage IT resources like virtual servers, storage, networking, and load balancers from a cloud provider, without needing to purchase and maintain physical hardware. These resources can be deployed quickly and scaled as needed. Popular IaaS platforms include Amazon Elastic Compute Cloud (aws.amazon.com/ec2), Microsoft® Azure® Virtual Machines (azure.microsoft.com/services/virtual-machines), and OpenStack® (openstack.org).

Software as a Service (SaaS) delivers software applications over the internet on a subscription or pay-as-you-go basis, eliminating the need for businesses to purchase and install software locally. Developers can provision, test, and deploy applications quickly using cloud

infrastructure without installing them on client machines. Popular SaaS platforms include Microsoft 365® (support.office.com), Salesforce® (salesforce.com), and Google Workspace™ (workspace.google.com).

Platform as a Service (PaaS) provides a development environment that includes infrastructure like servers and storage (similar to IaaS) but also offers tools for building, testing, and deploying applications. This platform could be based on Oracle®, MS SQL, PHP, or MySQL™. Examples of PaaS platforms include Oracle Cloud (cloud.oracle.com/paas), Microsoft Azure SQL Database (azure.microsoft.com/services/sql-database), and Google App Engine™ (cloud.google.com/appengine).

Unlike SaaS, PaaS does not come with a pre-built application. Developers are responsible for creating, securing, and managing the software they deploy on the platform, while the provider ensures the platform's availability and infrastructure integrity.

Dashboard for Amazon Web Services Elastic Compute Cloud (EC2) IaaS/PaaS

The screenshot shows the AWS EC2 Dashboard. The left sidebar has sections for EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES (with sub-options Instances, Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Scheduled Instances), IMAGES (AMIs, Bundle Tasks), ELASTIC BLOCK STORE (Volumes, Snapshots), and NETWORK & SECURITY. The main content area is titled 'Resources' and displays a summary of resources in the US East (N. Virginia) region: 0 Running Instances, 0 Dedicated Hosts, 0 Volumes, 0 Key Pairs, 0 Placement Groups, 0 Elastic IPs, 0 Snapshots, 0 Load Balancers, and 1 Security Groups. Below this is a callout box with a link to 'Learn more about the latest in AWS Compute from AWS re:Invent 2017 by viewing the [EC2 Videos](#)'. To the right, under 'Account Attributes', it lists Supported Platforms (EC2, VPC), Resource ID length management, and Additional Information links (Getting Started Guide, Documentation, All EC2 Resources, Forums, Pricing, Contact Us). At the bottom, there are buttons for 'Launch Instance', 'Service Health', and 'Scheduled Events'. The footer includes links for Feedback, English (US), Privacy Policy, Terms of Use, and a note about copyright (© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.).

Screenshot courtesy of Amazon.

On the left sidebar, there are navigation options for managing EC2 services, such as Instances, Images, Elastic Block Store, and Network. The central section provides a summary of available resources, such as running instances, dedicated hosts, volumes, key pairs, placement groups, elastic IPs, snapshots, load balancers, and security groups, all of which currently show zero usage. Below this, there is a section labeled Create Instance with a Launch Instance button. The right-hand section includes account attributes, additional information links such as, Getting Started Guide, Documentation, All EC2 Resources, Pricing, and contact us. The AWS marketplace section is below the additional information.

Desktop as a Service (DaaS) is a cloud computing solution that delivers virtual desktops to end-users over the internet, allowing them to access their desktop environment and applications from any device, anywhere. This service is managed by a third-party provider.

Cloud File Storage

Cloud storage is a type of Software as a Service (SaaS) that allows users to store and sync files across multiple devices. Services like Microsoft OneDrive, Dropbox, Apple iCloud, and Google Drive offer **file synchronization**, enabling seamless access and collaboration across PCs, smartphones, and other devices. One key advantage is automated file syncing, allowing multiple users to collaborate on the same document, with features like change tracking and commenting.

To ensure fast access and reliability, cloud providers replicate files across multiple datacenters. Content delivery networks (CDNs) are often used to store files closer to where they will be downloaded, speeding up access times. Additionally, cloud storage is available in different cost tiers based on factors like replication speed and geographical distribution.

Module 9

Supporting Mobile Devices

Module Overview

This lesson focuses on mobile devices and how they differ from desktop systems in terms of features, upgrade/repair procedures, and troubleshooting. As a certified CompTIA® A+® technician, you will be expected to configure, maintain, and troubleshoot laptops, smartphones, and tablets. With the proper information and the right skills, you will be ready to support these devices as efficiently as you support their desktop counterparts.

Module Summary

Prepare for A+ Core 1 by:

- Setting up mobile devices and peripherals.
- Configuring mobile device apps.
- Installing and configuring laptop hardware.
- Troubleshooting mobile device issues.

Lesson 9A

Mobile Devices and Peripherals

Lesson Overview

You have been hired as an IT technician by a small construction firm. One of your first assignments is to research and present management with different options for mobile devices for their field techs. The field techs do most of their work on job sites and need appropriate devices to fill out their reports. Each technician is given a laptop and you need to make sure they have the appropriate accessories and a way to connect to the internet while in the field.

In this lesson, you will learn the different types of mobile device accessories, different options for mobile networking and, how to configure devices to use these mobile network options.



Objectives Covered

- 1.2 Compare and contrast accessories and connectivity options for mobile devices.
- 1.3 Given a scenario, configure basic mobile device network connectivity and provide application support.

Learning Outcomes

As you study this lesson, answer the following questions:

- What is the little nub that is embedded into the keyboard on some laptops that controls the mouse cursor called?
- What option on a mobile device disables some or all of the wireless features (cellular data, Wi-Fi, GPS, Bluetooth, and NFC), depending on the device type and model?
- What is the small card that is used to identify the mobile device on the mobile network called?
- You are in a remote location and want to use your mobile device's cellular connection on your laptop wirelessly. What option do you need to enable and configure on the mobile device?
- When you make a purchase using contactless payment on your cell phone, what technology is being used?
- A field technician returns to the office and plugs their laptop into a special device that provides a full complement of ports for devices such as keyboards, monitors, mice, and network connections for their laptop. What is this device called?

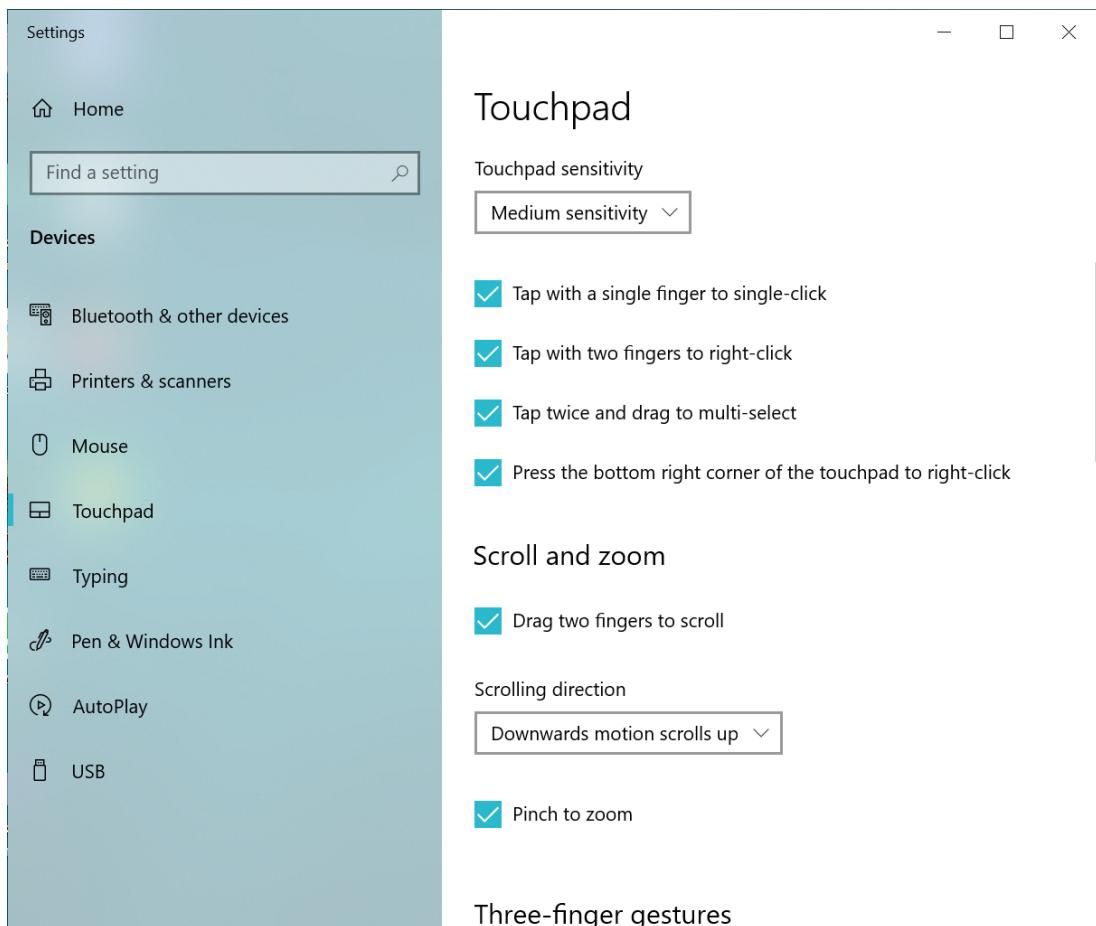
Mobile Device Accessories

Some popular accessories and peripheral options for mobile devices include the following:

Input Devices

The digitizer touch and gesture support built into touchscreens can be deployed in a variety of other form factors:

- Touchpad usually refers to the embedded panel on a laptop computer that is used for pointer control. Most touchpads now support multitouch and gestures.
Use the Settings app in Windows 10 to configure touchpad settings, such as sensitivity, tap events, and gestures.



Screenshot courtesy of Microsoft.

The left sidebar titled 'Settings' has an 'Home' option at the top. A search bar below reads, 'Find a setting'. The other options listed below under the heading 'Devices' are 'Bluetooth & other devices', 'Printers & scanners', 'Mouse', 'Touchpad', 'Typing', 'Pen & Windows Ink', 'Autoplay', and 'USB'. The main section allows users to configure touchpad behavior, starting with a dropdown to set 'Touchpad sensitivity', which is currently set to 'Medium sensitivity'. Below, several gesture options are enabled, such as tap with a single finger to single-click, tap with two fingers to right-click, tap twice and drag to multi-select, and press the bottom-right corner of the touchpad to right-click. In the 'Scroll and zoom' section, options include 'Drag two fingers to scroll' (enabled) and selecting the 'scrolling direction', set to 'Downwards motion scrolls up'.

Additional settings, such as 'pinch-to-zoom' and 'three-finger gestures', are available further down the page.

- Trackpad** can be used to mean the same thing as *touchpad*, but it is often used to mean a larger-format device attached as a peripheral.
- Drawing pad also refers to a large-format touch device attached as a peripheral. These are also called graphics tablets as they are most widely used for sketching and painting in a digital art application.

- A track point is a little nub that is embedded into the keyboard on some laptops. This pressure-sensitive nub can be used to control the mouse cursor. The harder you press the nub, the faster the cursor will move.

A touch device may require careful configuration to set up gesture support, calibrate to the screen area, and adjust sensitivity. This might be performed via OS settings or an application for the device.

Stylus

Most drawing pads and some touchscreens can be used with a [touch pen](#) or stylus rather than fingers. A stylus allows for more precise control and can be used for handwriting and drawing. This functionality is often referred to as natural input.

Touch pens are available in a wide range of sizes, from small styluses designed for use with smartphones to full-size pens designed for use with tablet touchscreens and dedicated graphics pads. Touch pens designed for use with drawing pads have removable and changeable nibs for use as different pen/brush types with digital art applications.

Microphone, Speakers, and Camera/Webcam

Mobile devices also feature integrated audio/video input and output devices. A **microphone** is used to record audio and for voice calling, while **speakers** produce audio output. A [digital camera](#) allows for video recording or **web conferencing** and can also be used to take still pictures.

On a laptop, the **microphone** is exposed by a small hole in the top bezel next to the camera lens and an LED to illuminate the subject.

Smartphones and tablets have both front-facing and rear-facing camera lenses, both of which can function either as a still camera or for video recording and streaming. The microphone and speakers are usually positioned on the bottom edge of the device.

An external [headset](#) or earbud set provides both a speaker microphone and headphone speakers. Wired headsets use either the 3.5 mm audio jack or a USB/Lightning connector. If no audio jack is supported on the mobile device, an adapter cable can be used. Wireless headsets are connected via Bluetooth. These connections can also be used for more powerful external speakers.

Mobile Device Wired Connection Methods

Although mobile devices are designed to be self-contained, they still need to support a variety of connection methods. These cabled and wireless interfaces allow the user to attach peripheral devices, share data with a PC, or attach a charging cable.

Laptop Ports

Laptops ship with standard wired ports for connectivity. The ports are usually arranged on the left and right edges or along the back.

There will typically be at least one video port for an external display device, typically HDMI or DisplayPort/Thunderbolt, but possibly VGA or DVI on older laptops. There will also be a few Universal Serial Bus (USB) Type A ports and one or more USB Type C ports on a modern laptop, some of which may also function as Thunderbolt ports.

Other standard ports include microphone and speaker jacks and RJ45 (Ethernet) for networking. Finally, a laptop might come with a memory card reader.

Smartphone and Tablet Connectors

Modern Android and Apple smartphones and tablets use the **USB-C** connector for wired peripherals and charging. The **Micro-B** USB and **Mini-B** connector form factors are only found on old devices.

Older Apple iPhone and iPad models use the proprietary **Lightning** connector, but the latest models have moved to using the USB-C connector.

Port Replicators and Docking Stations

Mobile devices do not always provide sufficient connection methods. Port replicators and docking stations allow the connection of more peripheral devices so that a mobile device can be used at a desk in a similar manner to a PC.

Port Replicator

A [port replicator](#) either attaches to a special connector on the back or underside of a laptop or is connected via USB. It provides a full complement of ports for devices such as keyboards, monitors, mice, and network connections. A replicator does not normally add any other functionality to the laptop.

A port replicator



Image by Elnur Amikishiyev © 123RF.com

Docking Station

A [docking station](#) is a sophisticated port replicator that may support add-in cards or drives via a media bay. When docked, a portable computer can function like a desktop machine or use additional features, such as a full-size expansion card.

A laptop docking station

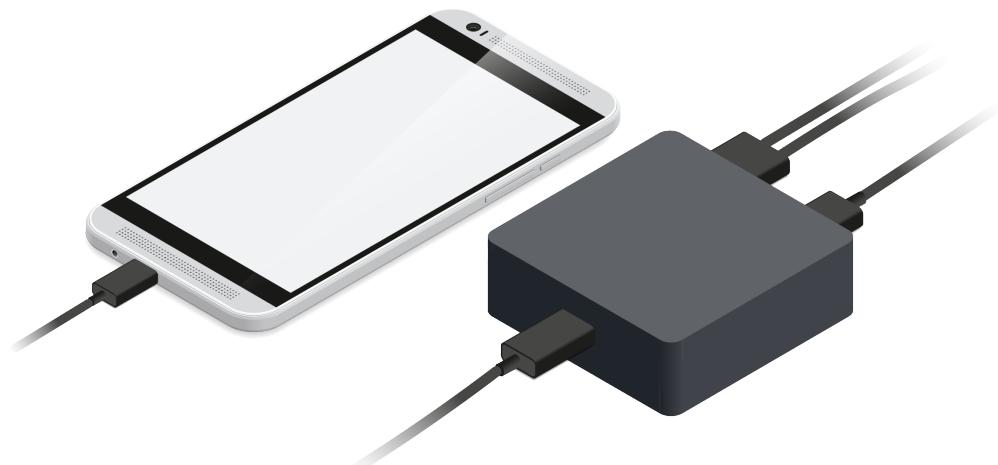


Image by Luca Lorenzelli © 123RF.com

Smartphone and Tablet Docks

As modern smartphones develop, manufacturers have been able to include processing power to rival some desktops and sometimes even replace them altogether. A smartphone/tablet dock connects the device to a monitor, external speakers, and keyboard/mouse input devices via the mobile's USB or Lightning port.

Example of a smartphone dock



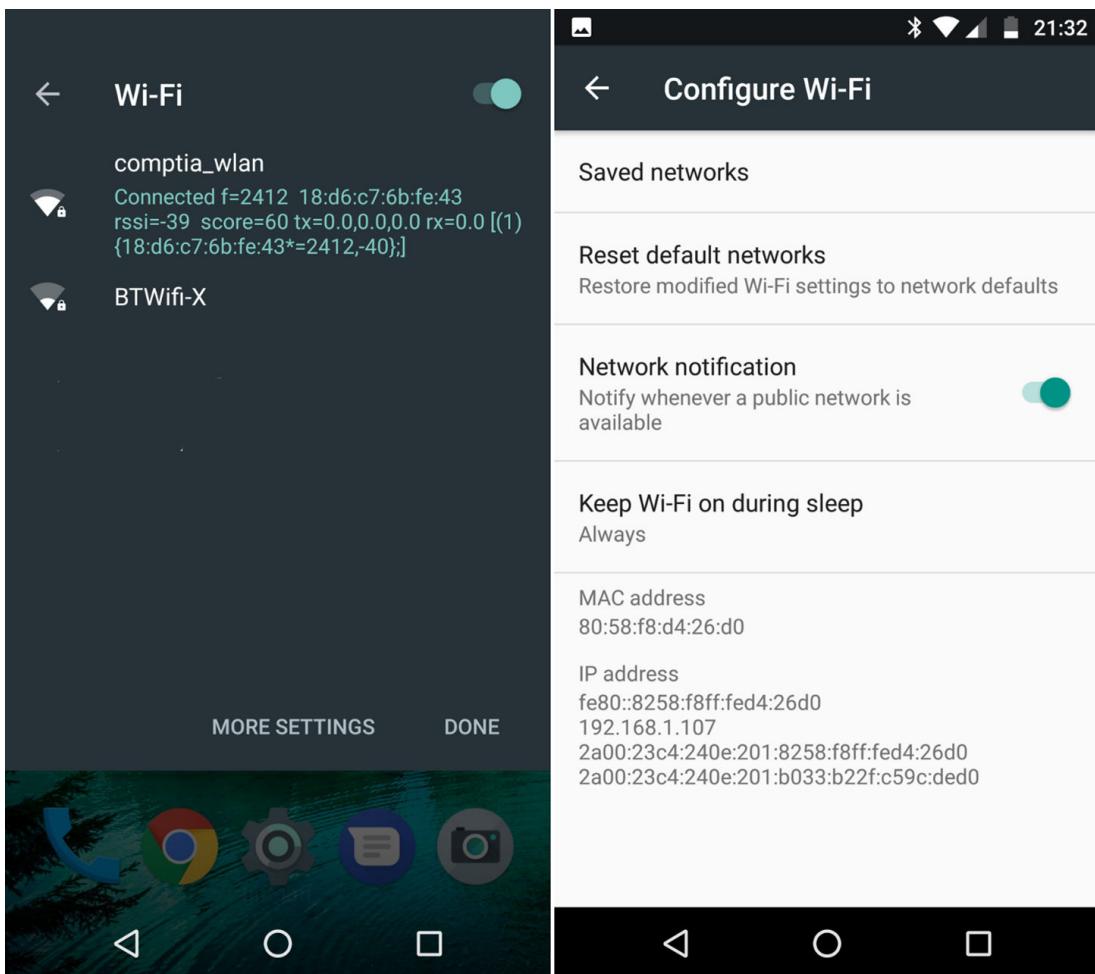
Wi-Fi Networking

Every laptop, smartphone, and tablet today supports a Wi-Fi radio. On a smartphone or tablet, the indicator on the status bar at the top of the screen shows the data link in use as the current Internet connection method. A device will usually default to Wi-Fi if present and show a signal strength icon.

Enabling and Disabling Wi-Fi

Each type of wireless radio link can be toggled on or off individually using the Control Center (swipe up from the bottom in iOS) or notification shade (swipe down from the top in Android). For example, you could disable the cellular data network while leaving Wi-Fi enabled to avoid incurring charges for data use over the cellular network. You can use the Settings menu to choose which network to connect to or to configure a manual connection to a hidden SSID.

Using Android to join a Wi-Fi network (left) and confirming the device's network address in the Advanced Settings (right).



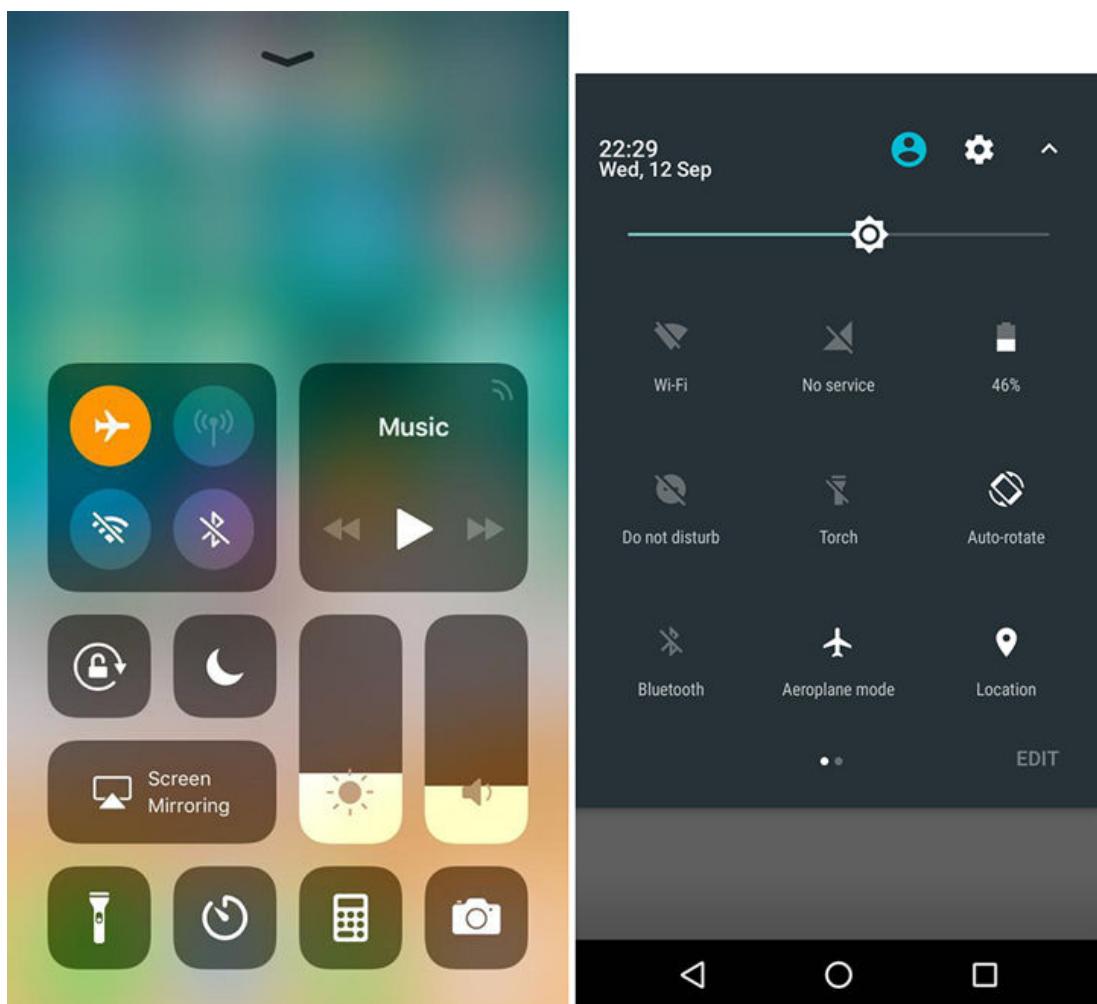
Screenshot courtesy of Android platform, a trademark of Google LLC.

On the left, the Wi-Fi menu displays available networks. CompTIA underscore w Lan is connected. Another network, B T Wi-Fi-X, is listed but not connected. At the bottom, options for More Settings and Done are visible, along with the navigation bar showing app icons for phone, chrome, settings, messages, and camera. The screen on the right is titled, configure Wi-Fi. Features include Saved networks, Reset default networks, and a toggle for Network notification, which is enabled to notify when public networks are available. The Keep Wi-Fi on during sleep option is set to Always. Technical details, such as the MAC address and IP address are displayed below.

Airplane Mode

Most airlines prohibit passengers from using radio-based devices while on board a plane. A device can be put into [airplane mode](#) to comply with these restrictions, though some carriers insist that devices must be switched off completely at times, such as during take-off and landing. Airplane mode disables some or all of the wireless features (cellular data, Wi-Fi, GPS, Bluetooth, and NFC), depending on the device type and model. On some devices, some services can selectively be re-enabled while still in airplane mode.

iOS iPhone (left) and Android phone (right) with Airplane (AeroPlane) mode enabled



Screenshots reprinted with permission from Apple Inc., and Android platform, a trademark of Google LLC.

On the left, the iOS Control Center provides toggles for Airplane mode, cellular data, Wi-Fi, and Bluetooth in the top row, followed by music playback controls with a play button at the center. Below are options for screen mirroring, brightness, and volume sliders, along with quick-access buttons for the flashlight, timer, calculator, and camera. The interface features a translucent background with blurred colors.

from the underlying screen. On the right, the Android Quick Settings panel displays the time, date, and a gear icon for settings access. A brightness adjustment slider is positioned at the top of the panel. The panel includes toggles for Wi-Fi, No service, Battery, Do not Disturb, Torch, Auto-Rotate, Bluetooth, Airplane mode, and Location. An edit button is at the bottom right.

Wi-Fi Antenna Connector/Placement

On mobile devices, the Wi-Fi antenna typically consists of two wires that are connected to the Wi-Fi chip and then run around the edges of the device display. This allows the device to pick up the strongest wireless signal possible.

Cellular Data Networking

Cellular data networking means connecting to the Internet via the device's cellular radio and the handset's network provider. The data rate depends on the technology supported by both the phone and the cell tower (4G or 5G, for instance). When a mobile device uses the cellular provider's network, there are likely to be charges based on the amount of data transferred. These charges can be particularly high when the phone is used abroad (referred to as *international roaming*), so it is often useful to be able to disable mobile data access.

Cellular Networking Technologies

Cellular networking technologies have evolved over the years through several different generations. Each new generation offers faster speeds and more features:

- 3rd Generation (**3G**) technology was used in the first iPhones and Android smartphones. 3G speeds could reach up to approximately 7.2 Mbps.
- 4th Generation (**4G**) introduced the Long-Term Evolution (**LTE**) technology which supports download speeds of up to 300 Mbps.
- 5th Generation (**5G**) builds on the previous generations and offers download speeds up to 10 Gbps.



Note: Keep in mind that the above speeds are all theoretical and would only ever be achieved in a lab environment. Actual speeds will be much slower and will vary based on factors like network coverage, signal strength, device capabilities, and network congestion.

Subscriber Identity Module (SIM / eSIM)

A Subscriber Identity Module (SIM) card is a small card that is used to identify the mobile device on the mobile network. The SIM card allows the device to connect to the correct service and access functions such as making calls, texting, and using mobile data.

A SIM card may also be used to store contacts and a limited number of text messages, but this data is typically now stored in the phone's memory or in cloud services.

The SIM card is tied to the mobile device's phone number. If the user gets a new phone, the SIM card can typically be inserted into the new phone and then activated on the network.

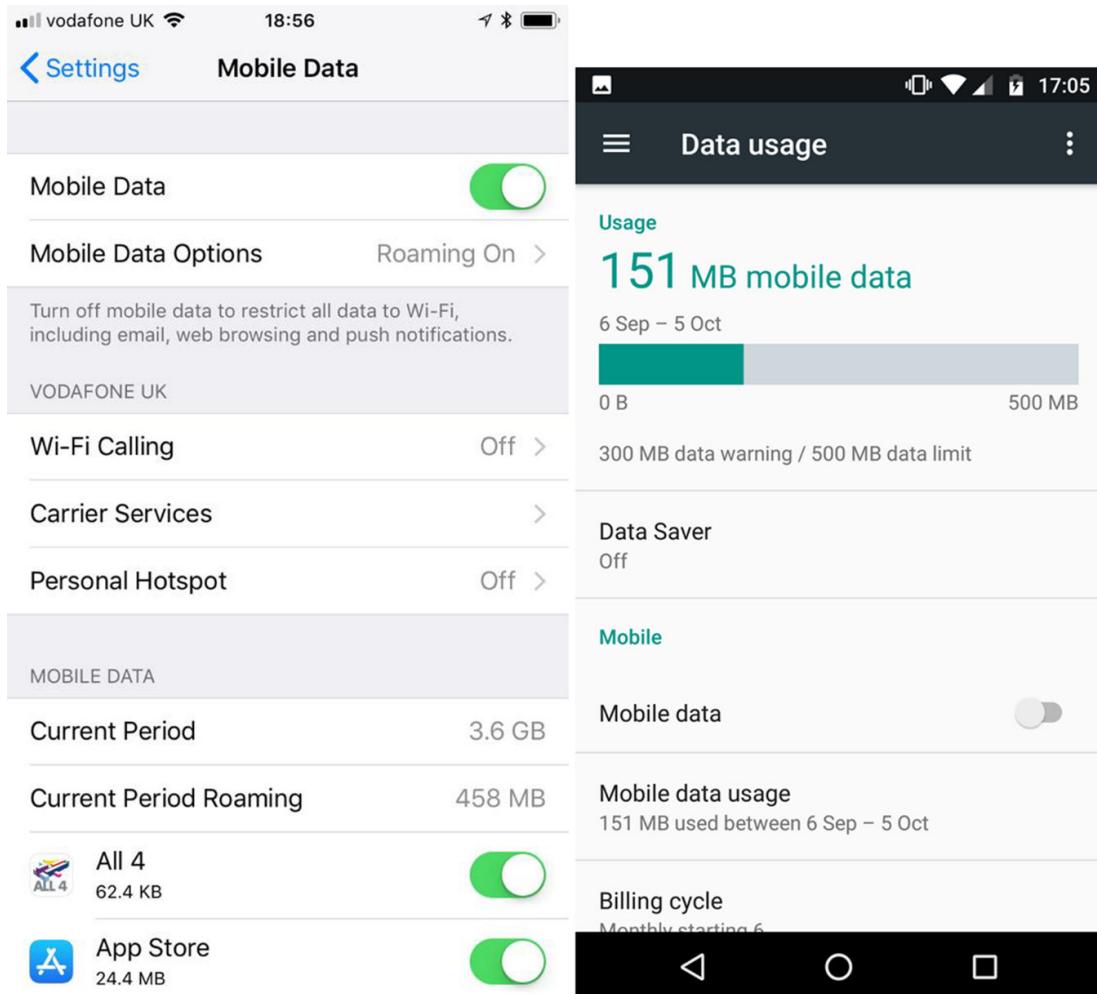
An embedded SIM (eSIM) performs the same functions as a physical SIM card, but instead of a small card, the eSIM is a small chip that is embedded inside the mobile device. The information for the eSIM can be downloaded and activated over the air which allows for quicker and easier setup of a new device.

Many devices that support eSIM allow for multiple eSIM profiles to be stored on a single device. This would allow a user to have multiple phone numbers or data plans on the same device.

Enabling and Disabling Cellular Data

The cellular data connection can usually be enabled or disabled via the notification shade, but there will also be additional configuration options via the Settings menu. You can usually set usage warnings and caps and prevent selected apps from using cellular data connections. Some handsets support the use of two SIMs, and you can choose which one to use for data networking.

Configuring cellular data options in iOS (left) and Android (right)



Screenshots reprinted with permission from Apple Inc., and Android platform, a trademark of Google LLC.

On the left, the iOS Mobile Data settings screen shows a toggle to enable or disable mobile data, with Mobile Data Options set to Roaming On. Below, additional options include Wi-Fi Calling, Carrier Services, and Personal Hotspot, all of which are turned off. The Mobile Data section displays the current period as 3.6 GB and current period roaming as 458 MB. Specific app data usage is listed, such as All 4 using 62.4 KB and App Store using 24.4 MB, with toggles to restrict their mobile data access. On the right, the Android Data Usage screen provides an overview of mobile data usage, showing 151 MB used between September 6 and October 5. A bar graph visualizes the usage against a data limit of 500 MB, with a warning set at 300 MB. The Data Saver feature is shown as off, and there is an option to toggle mobile data on or off. Additional details include the mobile date usage and current billing cycle.

Mobile Hotspots and Tethering

Tethering refers to connecting another device (such as a laptop) to a mobile device so that it can share its cellular data connection. Tethering can occur using a USB cable, Bluetooth, or Wi-Fi connection.

Configuring tethering on an Android phone

Screenshot courtesy of Android platform, a trademark of Google LLC.

At the top, U S B tethering is enabled, indicated by the toggle switched on and the status showing Tethered. Below, the Mobile Wi-Fi hotspot option is available but currently disabled. The Set up Wi-Fi hotspot section shows the configured hotspot name, CompTIA-mobile-hotspot, with W P A 2 P S K mobile Wi-Fi hotspot. At the bottom, Bluetooth tethering is also disabled.

The screenshot shows the "Tethering & mobile hotspot" settings screen on an Android device. The top status bar displays icons for signal strength, battery level, and the time (20:14). The title bar says "Tethering & mobile hotspot..." with a back arrow and a three-dot menu icon.

USB tethering
Tethered

Mobile Wi-Fi hotspot

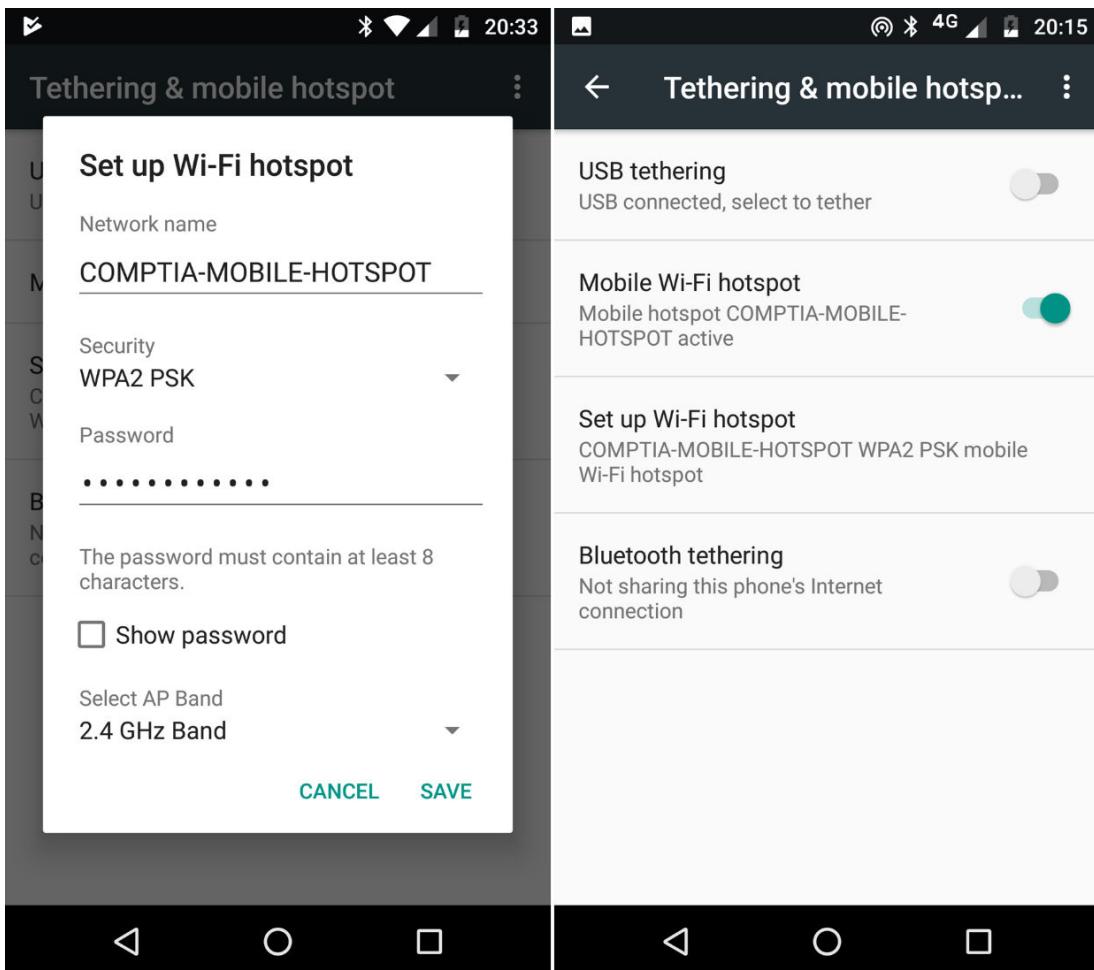
Set up Wi-Fi hotspot
COMPTIA-MOBILE-HOTSPOT WPA2 PSK mobile
Wi-Fi hotspot

Bluetooth tethering
Not sharing this phone's Internet connection

Hotspot

Tethering over a Wi-Fi connection is called a hotspot. To enable a mobile **hotspot**, configure the device with the usual settings for an access point (network name, security type, and passphrase), and then other devices can connect to it as they would with any other Wi-Fi access points.

Configuring mobile hotspot settings (left), then enabling it (right)



Screenshot courtesy of Android platform, a trademark of Google LLC.

The first screen is titled Set up Wi-Fi hotspot. It displays the network name as CompTIA-mobile-hotspot and the security type set to W P A 2 P S K. A password field is shown with a hidden password of at least eight characters. The show password checkbox is available to reveal the entered password. Additionally, there is an option to select the access point band, set to 2.4 Giga Hertz Band in this case. At the bottom, buttons for Cancel and Save allow the user to discard or save the configuration. The second screen is titled Tethering and mobile hotspot. U S tethering is disabled, Mobile Wi-Fi hotspot is enabled. A set up Wi-Fi hotspot is CompTIA-MOBILE-HOTSPOT WPA2 PSK mobile Wi-Fi hotspot. Bluetooth tethering is disabled.

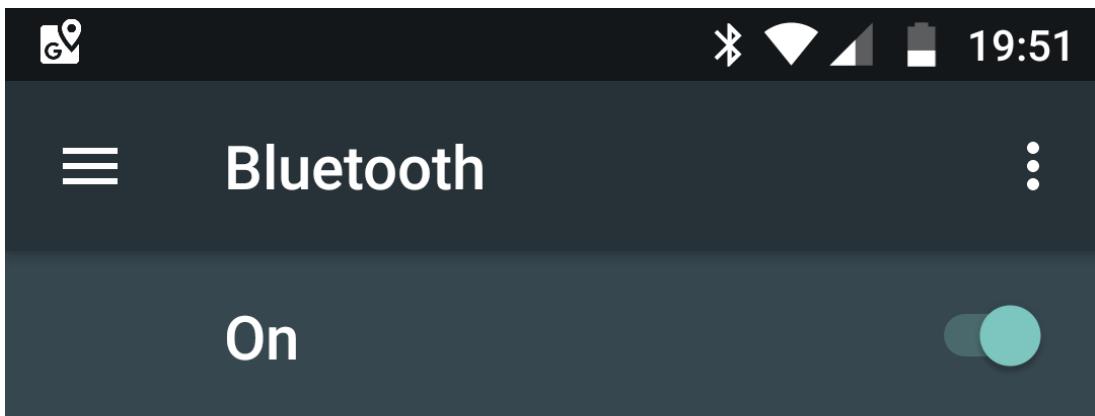
Bluetooth Wireless Connections

A **wireless connection for accessories** is often a better option for mobile devices than a cable. A **Bluetooth** wireless radio creates a short-range personal area network (PAN) to share data with a PC, connect to a printer, use a wireless headset, and so on.

Enabling Bluetooth

Bluetooth needs to be **enabled** for use via device settings. You may also want to change the device name since this is displayed publicly.

Enabling Bluetooth on an Android device. In this figure, the Android device is named "COMPTIA-MOBILE." "COMPTIA" is a nearby Windows PC with Bluetooth enabled.



Available devices



COMPTIA-MOBILE is visible to nearby devices while Bluetooth Settings is open.

Screenshot courtesy of Android platform, a trademark of Google LLC.

Bluetooth is switched on, as indicated by the active toggle in the top-right corner. The screen lists Available devices, showing a nearby device named CompTIA with an icon representing its type. A message states that CompTIA-MOBILE is visible to nearby devices while Bluetooth Settings is open.

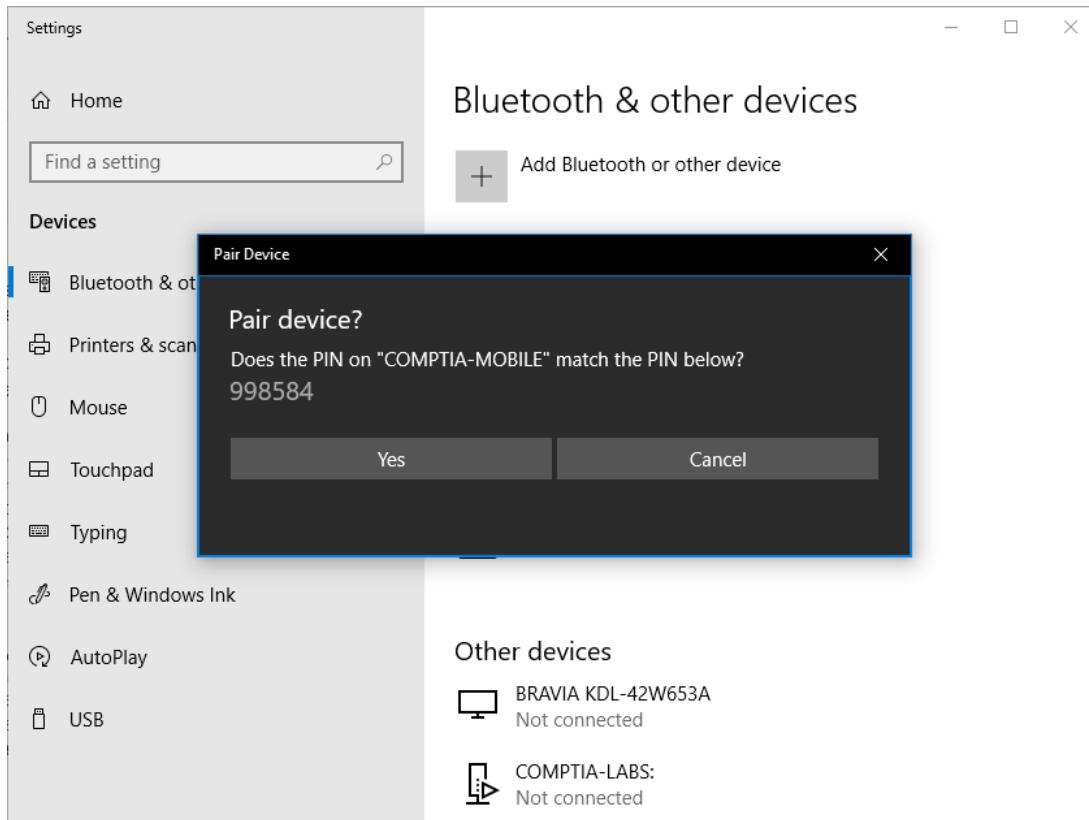
Enable Pairing

To connect via Bluetooth, the Bluetooth radio on each device must be put into discoverable or pairing mode. Bluetooth discoverability may be toggled within settings.

- In iOS, Bluetooth devices are configured via Settings → General → Bluetooth (or Settings → Bluetooth, depending on the iOS version).
- In Android, you can access Bluetooth settings via the notification shade.
- In Windows, you can manage Bluetooth Devices using the applet in Control Panel or Windows Settings and the Bluetooth icon in the notification area.

The settings page will show a list of nearby Bluetooth-enabled devices that are also in discoverable mode. Select a device to proceed. The pairing system should automatically generate a passkey or **PIN code** when a connection request is received. Input or confirm the key on the destination device, and accept the connection.

Pairing a Windows 10 computer with a smartphone



Screenshot courtesy of Microsoft.

The pop-up dialog, titled Pair Device, prompts the user to confirm a pairing attempt with CompTIA-mobile. It asks, Does the PIN on CompTIA-mobile match the PIN below and displays the PIN 998584. Two options, Yes and Cancel are provided below.

Test Bluetooth Connection

To **test** the connection, you can simply try using the device - for example, check that music plays through Bluetooth headphones. If you are connecting a device and a PC, you can use the Bluetooth icon to try to send a file.

If you cannot connect a device, check that both have been made discoverable. If you make a computer or mobile device discoverable, check the pairing list regularly to confirm that the devices listed are valid.

Near-Field Communication Wireless Connections

An increasing range of mobile devices have **near-field communication (NFC)** chips built in. NFC allows for very short-range data transmission (up to about 20 cm/8 in) to activate a receiver chip in the contactless reader. The data rates achievable are very low, but these transactions do not require exchanging large amounts of information.

NFC mobile payment



Image © 123RF.com

On the left, a payment terminal with a keypad and display screen emits a wireless signal icon, indicating it is ready to accept a payment. On the right, a hand holding a smartphone is shown, also emitting a wireless signal icon. The smartphone displays a credit card interface.

NFC allows a mobile device to make payments via contactless point-of-sale (PoS) machines. To configure a payment service, the user enters their credit card information into a wallet app on the device. The wallet app does not transmit the original credit card information, but a one-time token that is interpreted by the card merchant and linked back to the relevant customer account. There are three major wallet apps: Apple Pay, Google Pay (formerly Android Pay), and Samsung Pay. Some PoS readers may only support a particular type of wallet app or apps.

On an Android device, NFC can be enabled or disabled via settings. With most wallets, the device must be unlocked to initiate a transaction over a certain amount.

NFC can also be used to configure other types of connection, such as pairing Bluetooth devices. For example, if a smartphone and headset both support NFC, tapping the headset will automatically negotiate a Bluetooth connection.

Lesson 9B

Mobile Apps and Data

Lesson Overview

Now that all field technicians have been supplied with the appropriate mobile devices, management decided that they will now provide field technicians with their own mobile devices to use for company purposes. Part of your job will be to manage these devices, including configuring email, installed apps, and security features.

In this lesson, you will learn about managing permissions on mobile platforms, synchronizing data, configuring email accounts, and managing mobile devices in an enterprise environment.



Objectives Covered

1.3 Given a scenario, configure basic mobile device network connectivity and provide application support.

Learning Outcomes

As you study this lesson, answer the following questions:

- Where can users download apps for Android devices from?
- What type of account do Apple devices require?
- What are the common types of data that need to be synced?
- What are the common server addresses that will need to be input when configuring a corporate email account?
- A user needs to supply a PIN and use an authenticator to login to an app. What type of authentication is being used?

Mobile Apps

An app is an installable program that extends the functionality of the mobile device. An app must be written and compiled for a particular mobile operating system. For example, an app written for Apple iOS cannot directly be installed on Android. The developer must make a version for each OS.

iOS Apps

In iOS, apps are distributed via Apple's [app store](#). Apps must be submitted to and approved by Apple before they are released to users. This is also referred to as the *walled garden model* and is designed to prevent the spread of malware or code that could cause faults or crashes. Apps

can use a variety of commercial models, including free to use, free with in-app purchases, or paid-for.

Third-party developers can create apps for iOS using Xcode, which is Apple's integrated development environment (IDE), and the programming language Swift. Xcode can only be installed and run on a computer using macOS.

Apple's App Store and app permission settings



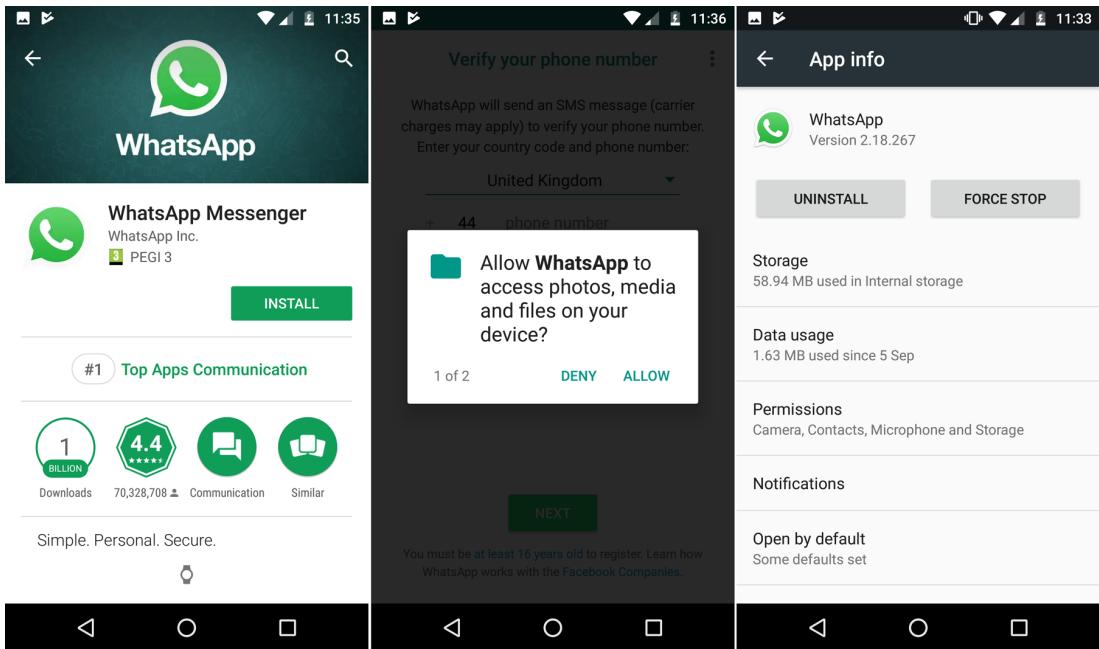
Screenshot reprinted with permission from Apple Inc., and WhatsApp.

On the left, the App Store page for WhatsApp Messenger is shown, featuring the app's logo, name, and description: Simple. Reliable. Secure. The page indicates that an update is available, with a blue Update button prominently displayed. The app has a rating of 4.7 stars based on 834K ratings and is categorized as No 1 Social Networking with an age rating of 12 plus. Below, the What's New section highlights recent updates, including features like 3D Touch and media previews. The right screen shows the settings for WhatsApp. It displays toggles for enabling access to features such as Contacts, Photos (set to Read and Write), Microphone, and Camera, all of which are turned on. Additional settings include Siri and Search preferences, Notifications, Background App Refresh, and Mobile Data, each enabled.

Android Apps

Android's app model is more relaxed, with apps available from both Google Play Store and third-party sites, such as Amazon's app store. The Java-based IDE, Android Studio, is available on Linux, Windows, and macOS.

Play Store to install an app (left), grant the app permissions (middle), and review permissions and other settings (right)



Screenshots courtesy of Android platform, a trademark of Google LLC., and WhatsApp.

The first screen displays the Google Play Store page for WhatsApp Messenger, showing the app's logo, name, and the developer. An Install button is on the right. The app is 1 Top Apps Communication. It has over 1 billion downloads and has a rating of 4.4 stars. The app's tagline, Simple. Personal. Secure. is at the bottom. The second screen shows a pop up that reads, Allow WhatsApp to access photos, media, and files on your device? with options to Deny or Allow. The third screen displays the WhatsApp App Info page in the Android settings. The version of WhatsApp is 2.18.267. An install and force stop button is below. The storage usage is 58.94 M B and data usage is 1.63 M B. It also lists the permissions granted, including access to the camera, contacts, microphone, and storage. The notifications and default settings are shown.

Permissions

On both iOS and Android, apps are supposed to run in a sandbox and have only the privileges granted by the user. An app will normally prompt when it needs to obtain permissions. If these are not granted, or if they need to be revoked later, you can do this via the app's Settings page.

Account Setup

Most smartphones are designed to be used by a single user. The owner's user account is configured when the device is used for the first time (or re-initialized). This account is used to manage the apps installed on the device by representing the user on the app store. iOS requires an Apple ID, while an Android device requires either a Google Account or a similar vendor account, such as a Samsung Account. This type of account just requires you to select a unique ID (email address) and to configure your credentials (pattern lock, fingerprint, face ID, and so on). Accounts can also be linked to a cellphone number or alternative email address for verification and recovery functions.

As well as managing the app store, the owner account can be used to access various services, such as an email account and cloud storage. However, the device owner might want to use multiple other accounts or digital identities in conjunction with different apps. These accounts allow app settings and data to be **synchronized between multiple devices**. For example, a user

can access their contacts list from both their mobile device and their laptop computer. Some examples of these services include:

- [Microsoft 365](#) - A Microsoft digital identity is used to access cloud subscriptions for the Office productivity software suite and the OneDrive cloud storage service. Microsoft identities use the @outlook.com domain by default but can be registered with a third-party address also.
- [Google workspace](#) - A Google Account (@gmail.com) grants free access to Google's Workspace productivity software and the free storage tier on Google Drive.
- [iCloud](#) - An Apple ID (@icloud.com) grants free access to Apple's productivity software and the free storage tier on iCloud.

The device owner can set up sub-accounts for services not represented by their Apple ID or Google Account, such as a corporate email account. Each app can set up a subaccount too. For example, the device might have accounts for apps such as Facebook or LinkedIn.

Account settings allow you to choose which features of a particular account type are enabled to synchronize data with the device. You can also add and delete accounts from here.

iOS supports a single Apple ID account per device

The screenshot shows the 'Apple ID' settings screen. At the top, there is a circular placeholder for a profile picture. Below it, three main sections are listed: 'Name, Phone Numbers, Email', 'Password & Security', and 'Payment & Shipping'. Underneath these, two service-specific sections are shown: 'iCloud' and 'iTunes & App Store'. At the bottom right, there is a red 'Sign Out' button.

vodafone UK 18:57

Settings Apple ID

Name, Phone Numbers, Email >

Password & Security >

Payment & Shipping >

iCloud Off >

iTunes & App Store >

Sign Out

Screenshot reprinted with permission from Apple Inc.

At the top, there is a blurred profile photo placeholder, with the user's Apple ID details such as name, phone numbers, and email listed as the first option. Below that, options for Password and Security and Payment and Shipping are visible. Further down, there are toggles for services like iCloud, which is shown as off, and iTunes and App Store. At the bottom, a Sign Out option is available.

Types of Data to Synchronize

Mobile device synchronization (sync) refers to copying data back and forth between different devices. This might mean between a PC and a smartphone or between a smartphone, a tablet, and a PC. Syncing data can also occur between a device and a cloud service (such as Google Drive). Many people have multiple devices and need to keep information up to date on all of them. If users edit contact records on a phone, they want the changes to appear when they next log into email on their PC.

There are many different types of information that users might synchronize and many issues you might face dealing with synchronization problems.

 **Note:** One thing to keep in mind is that some data plans implement data caps. This means that there is a limited amount of data the user can use each month. Syncing certain data, such as media files, may cause the user to go over the data cap resulting in additional fees. If the user has a data cap, you should ensure the mobile device is connected to Wi-Fi before syncing data.

Contacts

A **contact** is a record with fields for name, address, email address(es), phone numbers, notes, and so on. One issue with contacts is that people tend to create them on different systems and there can be issues matching fields or phone number formats when importing from one system to another using a file format such as comma separated values (CSV).

vCard represents one standard format and is widely supported now. Maintaining a consistent, single set of contact records is challenging for most people, whatever the technology solutions available.

Calendar

A **calendar** item is a record with fields for appointment or task information, such as subject, date, location, and participants. Calendar records have the same sort of sync issues as contacts whereas people create appointments in different calendars and then have trouble managing them all.

Calendar items can be exchanged between different services using the iCalendar (ICS) format.

Mail

Most email systems store messages on the server, and the client device is used to manage them. There can often be sync issues, however, particularly with deletions, sent items, and draft compositions.

Media Files and Documents

The main sync issue with media files such as **photos** tends to be the amount of space they take up. There might not be enough space on one device to sync all the files the user has stored.

There can also be issues with file formats; not all devices can play or show all formats.

Users editing a document on different devices may have trouble with version history unless the changes are saved directly to the copy stored in the cloud.

Apps

An app will be available across all devices that the account holder signs in on, as long as they are on the same platform. If you have a Windows PC and an Apple iPhone, you will find yourself managing two sets of apps. Most of them will share data seamlessly, however (the social media ones, for instance).

Passwords

Both iOS and Android will prompt you to save passwords when you sign in to apps and websites. These passwords are cached securely within the device file system and protected by the authentication and encryption mechanisms required to access the device via the lock screen.

These cached passwords can be synchronized across your devices using cloud services. You must remember that anyone compromising your device/cloud account will be able to access any service that you have cached the password for.

Password managers can also be used to store and sync passwords across multiple devices.

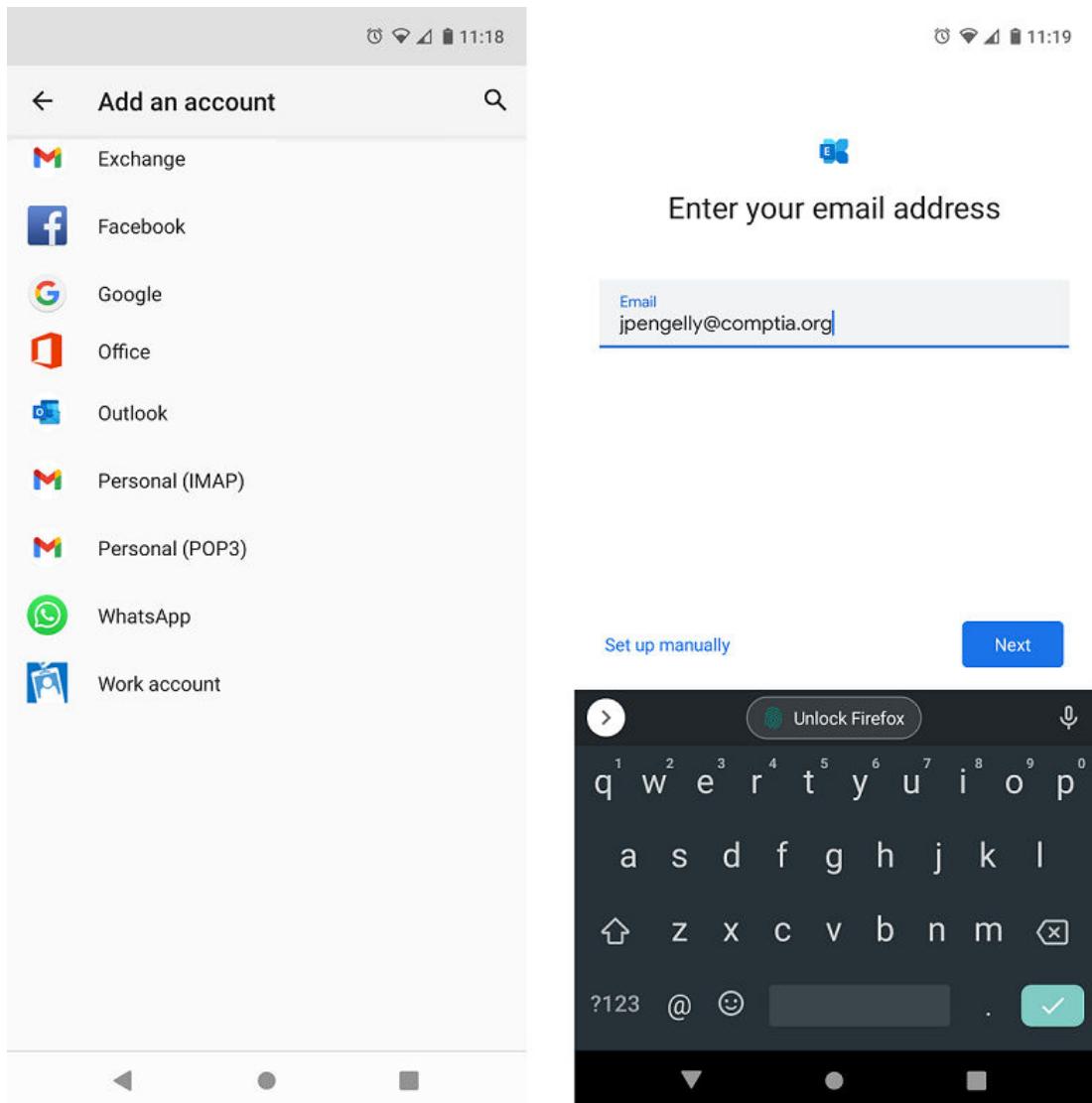
Email Configuration Options

With email being one of the main forms of communication, especially in today's enterprise environments, the ability to compose and receive emails on a mobile device is incredibly important. Knowing how to configure email clients on mobile devices is a critical skill for today's technicians.

Commercial Provider Email Configuration

Most commercial email providers allow the OS to autodiscover connection settings. *Autodiscover* means that the mail service has published special DNS records that identify how the account for a particular domain should be configured. To connect to an autodiscover-enabled account, simply choose the mail provider (Exchange, Gmail, Yahoo, Outlook.com, iCloud, and so on) then enter your email address and credentials.

Configuring an autodiscover-enabled Exchange mail account in Android



Screenshot courtesy of Android platform, a trademark of Google LLC.

The first screen displays a menu titled Add an account, listing various account types available for setup. These include options like Exchange, Facebook, Google, Office, Outlook, Personal (I M A P), Personal (P O P 3), WhatsApp, and Work account. The second screen has a field to enter the email address. A text field is partially filled with the email jpengelly at the rate comptia dot o r g. A set up manually option on the left and a next button on the right is followed by a virtual keyboard at the bottom.

Corporate and ISP Email Configuration

Many institutions use Microsoft's Exchange mail server for corporate email. Exchange is usually an integrated provider option and clients can autodiscover the correct settings. To manually configure an Exchange ActiveSync account, you need to enter the email address and username (usually the same thing) and a host address (obtain this from the Exchange administrator) as well as a password and the choice of whether to use Transport Layer Security (TLS). There is often also a field for domain, but this is usually left blank.

! If there is a single "Domain\Username" field, prefix the email address with a backslash: \me@company.com.

If you are connecting to an internet service provider (ISP) email host or **corporate mail gateway** that does not support autodiscovery of configuration settings, you can enter the server address manually by selecting **Other**, then inputting the appropriate server addresses such as:

- Incoming mail server - the FQDN or IP address of the Internet Mail Access Protocol (IMAP) or Post Office Protocol (POP3) server.



Choose **IMAP** if you are viewing and accessing the mail from multiple devices. POP3 will download the mail to the device, removing it from the server mailbox. Note that Exchange doesn't use either POP3 or IMAP (though it can support them) but a proprietary protocol called Exchange ActiveSync (EAS).

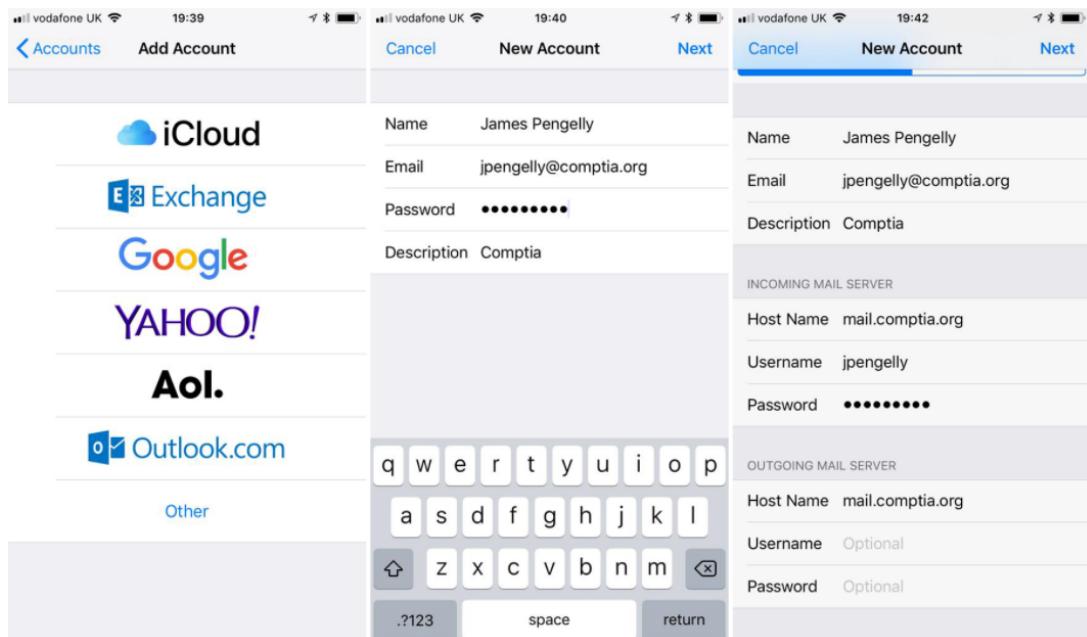
- Outgoing mail server - the address of the Simple Mail Transfer Protocol (SMTP) server.
- Enable or disable Transport Layer Security (TLS).



Note: TLS protects confidential information such as the account password and is necessary if you connect to mail over a public link (such as an open Wi-Fi "hotspot"). Note that you can only enable TLS if the mail provider supports it.

- Ports - the secure (TLS enabled) or insecure ports used for IMAP, POP3, and SMTP would normally be left to the default ports. If the email provider uses custom port settings, you would need to obtain those and enter them in the manual configuration.

Configuring an email account manually in iOS



Screenshot reprinted with permission from Apple Inc.

The first screen, titled Add Account, presents a list of email service providers such as iCloud, Exchange, Google, Yahoo!, AOL, Outlook dot com, and an Other option for manual configuration. The second screen, titled New Account, is part of the manual configuration process. It includes fields for entering the user's name, email address, password, and a description of the account. The example shows James Pengelly as the name, the email address jpengelly at comptia dot o rg, and CompTIA as the account description. A virtual keyboard is visible below. The third screen continues the setup process, displaying additional configuration options for a New Account. It shows

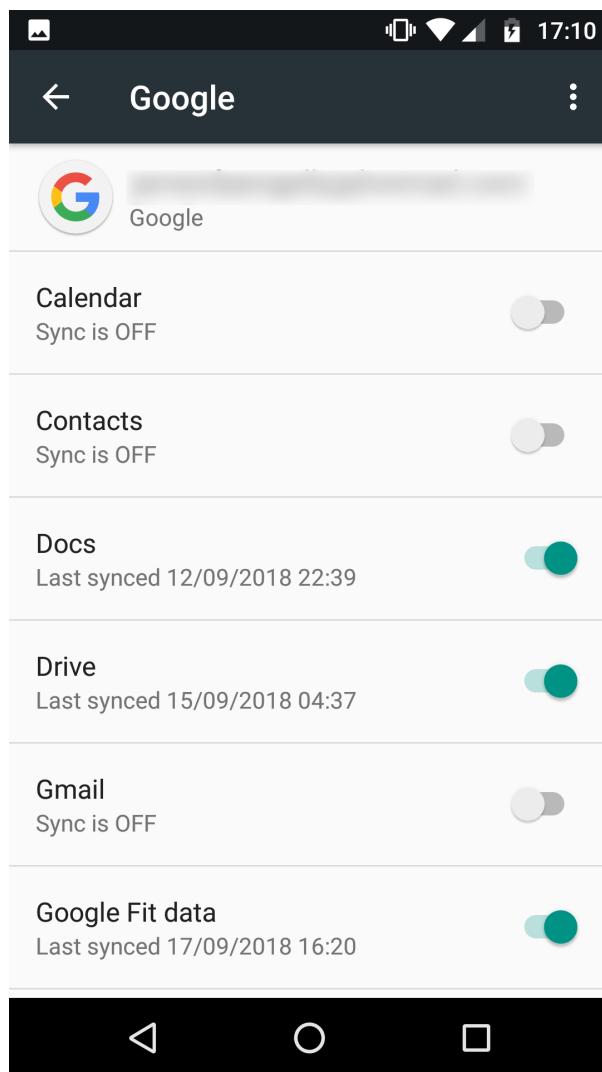
fields for the incoming mail server settings, such as the host name, mail dot comptia dot org, username, j pengelly, and password.

Similarly, the outgoing mail server section lists the same host name, with the username and password fields marked as optional.

Synchronization Methods

Before cloud services became prevalent, data on a smartphone or tablet would typically be manually synchronized with a desktop PC. You might use the PC to back up data stored on the smartphone, for instance, or to sync calendar and contact records. Nowadays, it is much more likely for devices to be connected via cloud services. If given permission, the device OS and apps can back up data to the cloud service all the time. When you sign in to a new device, it syncs the data from the cloud seamlessly.

Account settings for the Google master account on an Android smartphone



Screenshot courtesy of Android platform, a trademark of Google LLC.

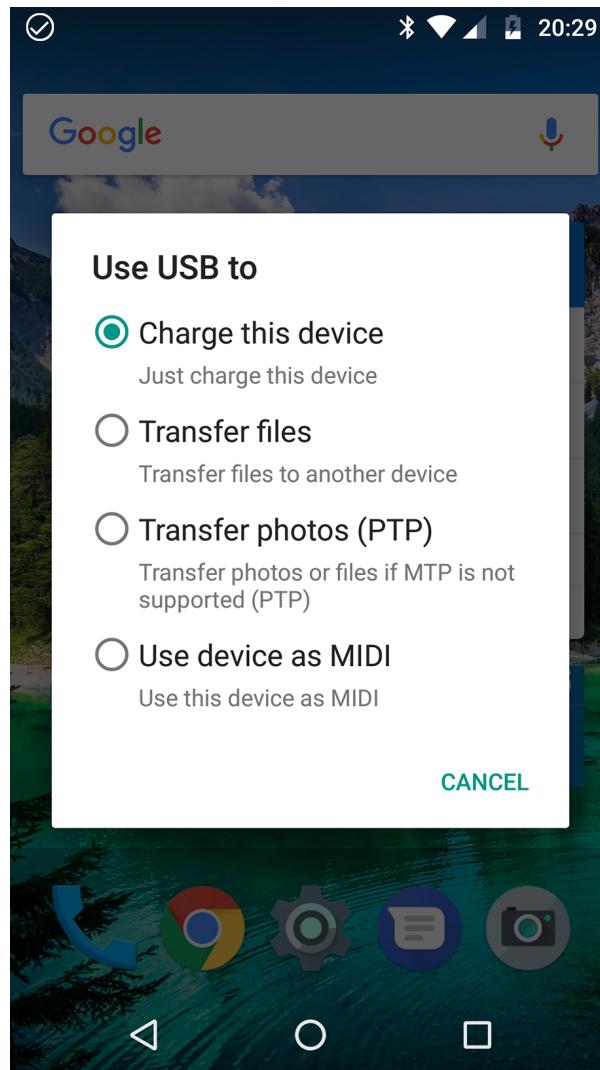
When synchronizing large amounts of data, you should account for different types of [data cap](#):

- The account will have an overall storage limit. Most accounts are issued with 5 GB of free tier storage. Additional storage needs to be purchased.
- If synchronizing over a cellular data network, there will be a monthly data allowance and a rate for any transfers exceeding the allowance. To avoid incurring unwanted charges, you can configure the device to warn and/or cap cellular data transfers. Most apps can be configured to sync over Wi-Fi only.

Synchronizing to PCs

If synchronizing via a cloud service is not an option, you can usually view an Android phone or tablet from Windows over USB or Bluetooth and use drag-and-drop for file transfer.

Connecting an Android smartphone to a Windows PC over USB



Screenshot courtesy of Android platform, a trademark of Google LLC.

Synchronizing to Automobiles

Most new automobiles come with in-vehicle entertainment and navigation systems. The main part of this system is referred to as the head unit. If supported, a smartphone can be used to "drive" the head unit so the navigation features from your smartphone will appear on the display (simplified for safe use while driving), or you could play songs stored on your tablet via the vehicle's entertainment system. The technologies underpinning this are Apple CarPlay and Android Auto.

Enterprise Mobility Management

Enterprise mobility management (EMM) is a class of management software designed to apply security policies to the use of mobile devices and apps in the enterprise. The challenge of identifying and managing all the devices attached to a network is often referred to as visibility.



Enterprises use different deployment models to specify how mobile devices and apps are provisioned to employees. One example is bring your own device (BYOD), where employees are allowed to use a personally owned device to access corporate accounts, apps, and data.

There are two main functions of an EMM product suite:

- **Mobile device management** (MDM) sets device configuration policies for authentication, policy enforcement, feature use (camera and microphone), and connectivity. MDM can also allow device resets and remote wipes.
- **Mobile application management** (MAM) sets policies for apps that can process corporate data and prevent data transfer to personal apps. This type of solution configures an enterprise-managed container or workspace.

Examples of EMM solution providers include [Omnissa ONE](#), [Microsoft Intune](#), [Broadcom](#), and [Citrix Endpoint Management](#).

When a device is enrolled with the MAM software, it can be configured into an enterprise workspace mode in which only a certain number of authorized **corporate applications** can run. For example, the app(s) used for corporate email, calendar, cloud storage, and contacts would store settings and data separately from the app used for personal email. Messages and attachments sent from the account might be subject to data loss prevention (DLP) controls to prevent unauthorized forwarding of confidential or privacy-sensitive data.

Endpoint management software such as Microsoft Intune can be used to approve or prohibit apps

The screenshot shows the Microsoft Azure portal interface for device configuration. On the left, there's a sidebar with various icons. The main area has a breadcrumb navigation path: Device configuration - Profiles > Create profile > Device restrictions > Restricted Apps. The 'Create profile' step is active, showing fields for Name (gtlearning EMM Default Android Policy), Description (Enter a description...), Platform (Android), and Profile type (Device restrictions). The 'Configure' button is at the bottom. The 'Device restrictions' step is active, showing categories: General (11 settings available), Password (10 settings available), Google Play Store (1 setting available), Restricted Apps (2 settings available, currently selected), Browser (5 settings available), Allow or Block apps (3 settings available), and Cloud and Storage (4 settings available). The 'Restricted Apps' step is active, with a sub-section titled 'Type of restricted apps list' set to 'Not configured'. It includes fields for App URL, App Bundle ID, App Name, and Publisher, each with an 'Import' and 'Export' button. A table below lists these fields with placeholder values like 'e.g. https://play.google.com' and 'Not configured'. The table has columns for APP URL, APP BUNDLE ID, APP NAME, and PUBLISHER, with a header row. The table is currently empty with the message 'No apps'.

Screenshot courtesy of Microsoft.

The create profile has fields for name, description, platform, profile type. The settings tab is at the bottom. A create button is on the bottom left. The device restrictions has an option to select a category to configure settings. The settings are as follows: General: 11 settings available Password: 10 settings available Google Play Store: 1 setting available Restricted Apps: 2 settings available Browser: 5 settings available Allow or Block Apps: 3 settings available Cloud and Storage: 4 settings available The restricted app shows the type of restricted apps list. It also lists the app URL, app bundle ID, app name, and publisher.

Apple operates enterprise developer and distribution programs to allow private app distribution via [Apple Business Manager](#). Google's Play store has a private channel option called [Managed Google Play](#). Both of these options allow a MAM suite to push apps from the private channel to the device.

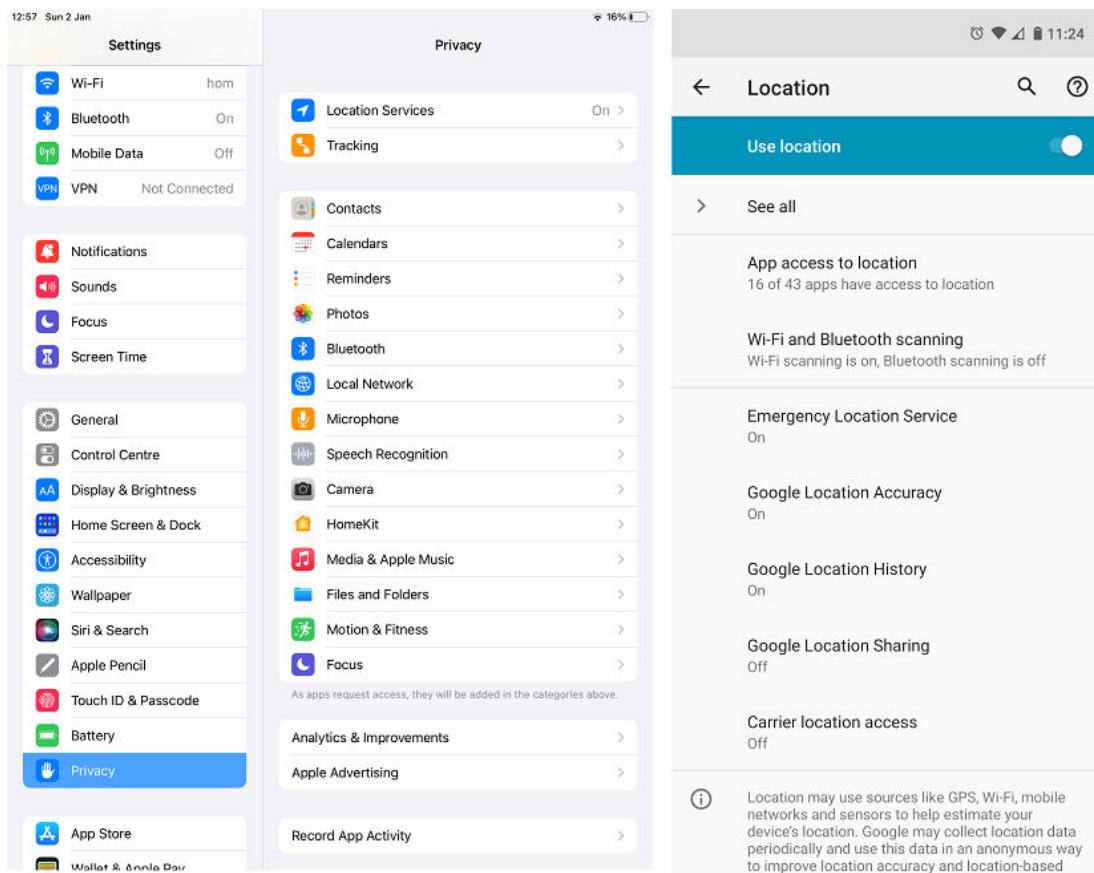
Location Services

Geolocation is the use of network attributes to identify (or estimate) the physical position of a device. A mobile device operates a [location service](#) to determine its current position. The location service can make use of two systems:

- [Global Positioning System](#) is a means of determining the device's latitude and longitude based on information received from orbital satellites via a GPS sensor. Note that not all mobile devices are fitted with GPS sensors.
- [Indoor positioning system](#) works out a device's location by triangulating its proximity to other radio sources, such as cellular radio towers, Wi-Fi access points, and Bluetooth/RFID beacons.

As the location service stores highly personal data, it is only available to an app where the user has granted specific permission to use it.

Configuring location services in iOS (left) and Android (right)



Screenshots reprinted with permission from Apple Inc., and Android platform, a trademark of Google LLC.

The first tab titled settings has the following options: Wi-Fi, Bluetooth, Mobile Data, VPN, Notifications, Sounds, Focus, Screen Time, General, Control Centre, Display and Brightness, Home Screen and Dock, Accessibility, Wallpaper, Siri and Search, Apple Pencil, Touch ID and Passcode, Battery, and Privacy (selected). The second tab titled privacy lists, location services, tracking, contacts, calendars, reminders, photos, Bluetooth, Local network, microphone, speech recognition, camera, HomeKit, media and apple music, files and folders, motion and fitness, and focus.

The analytics and improvements and apple advertising are listed below. The record app activity is at the bottom. The third tab is titled location.

The use location toggle is enabled. The see all option is below. Further the options list app access to location, Wi-Fi and Bluetooth scanning, Emergency Location Service, Google Location Accuracy, Google Location History, Google Location Sharing, and Carrier Location access.

! Some mobile devices are additionally fitted with a magnetometer sensor. This enables more accurate compass directions.

Lesson 9C

Laptop Hardware

Lesson Overview

Some of the laptops that have been assigned to the field technicians have been damaged. Management has tasked you with diagnosing and repairing these laptops when possible.

In this lesson, you will learn which laptop components can typically be replaced or upgraded and how to perform these repairs.



Objectives Covered

1.1 Given a scenario, monitor mobile device hardware and use appropriate replacement techniques.

Learning Outcomes

As you study this lesson, answer the following questions:

- What are some of the concerns you should be aware of when working on laptops?
- What types of batteries are typically used in laptops?
- Where are the antenna wires for a Wi-Fi adapter card in a laptop routed to?
- What type of Solid State Drive (SSD) usually interfaces with the PCI Express bus?

Laptop Disassembly Processes

Laptops have specialized hardware designed especially for use in a portable chassis and can run on battery or AC power. Laptops use the same operating systems as desktop PCs, and unlike smartphones and tablets, typically have some upgradeable or replaceable components.

Distinctive features of a laptop computer

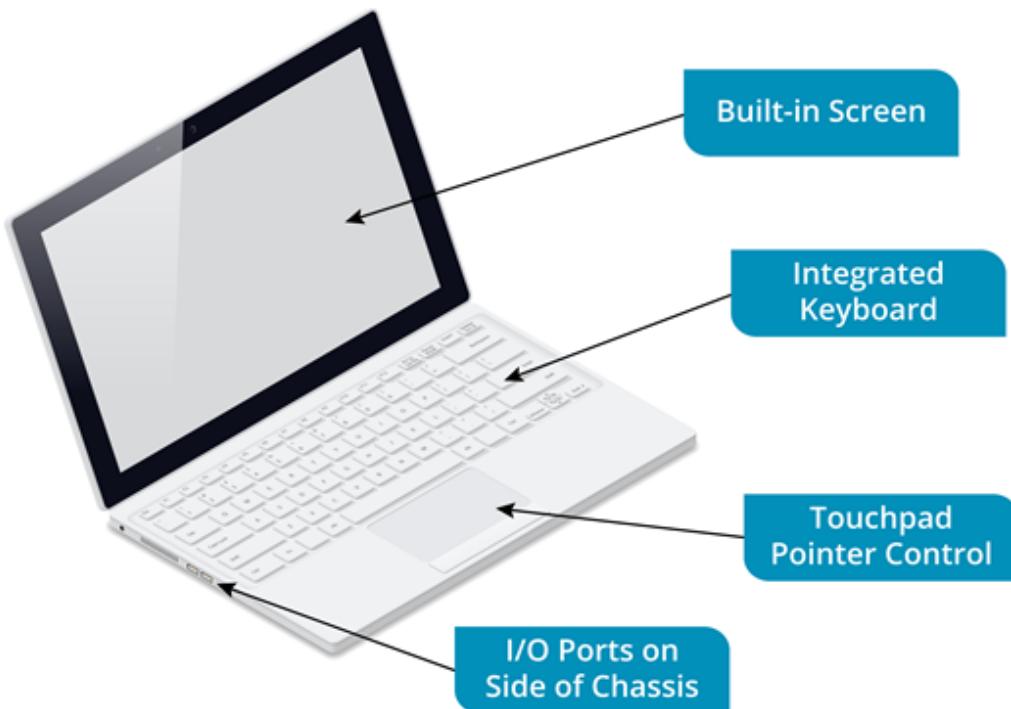


Image © 123RF.com

When it comes to performing upgrades or replacing parts, there are some issues specific to laptops that you should be aware of.

Hand Tools and Parts

Laptops use smaller screws than are found on desktops. You may find it useful to obtain a set of precision screwdrivers and other appropriate hand tools. It is also much easier to strip the screws (remove the notch for the screwdriver) so you should take care to use an appropriately sized screwdriver!

Laptops will typically use different sized screws throughout the machine. You need to document the location of screws of a specific size and the location and orientation of ribbon cables and other connectors. It can be very easy to remove them quickly during disassembly and then face a puzzle during reassembly.

! A useful tip is to take a photo of the underside of the laptop and print it out. As you remove screws, tape them to the relevant point in your picture. This ensures you will not lose any and will know which screw goes where. Photograph each stage of disassembly so you know where to re-fit cables and connectors.

As with a desktop, organize parts that you remove or have ready for installation carefully. Keep the parts away from your main work area so that you do not damage them by mistake. Keep static-sensitive parts, such as the Solid State Drives (SSDs), memory modules, and adapter cards, in antistatic packaging.

Form Factors and Plastics/Frames

The laptop chassis incorporates the motherboard, power supply, display screen, keyboard, and touchpad. The plastic or aluminum frames are the hard surfaces that cover the internal components of the laptop. They are secured using either small screws or pressure tabs. Note that screws may be covered by rubber or plastic tabs.

Make sure you obtain the manufacturer's service documentation before commencing any upgrade or replacement work. This should explain how to disassemble the chassis and remove tricky items, such as plastic bezels, without damaging them. You should only perform this work if a warranty option is not available.

Battery Replacement

Portable computers can work off both AC power and battery operation.

AC Adapters

To operate from building power, the laptop needs a power supply to convert the AC supply from the power company to the DC voltages used by the laptop's components. The power supply is provided as an external AC adapter. AC adapters are normally universal (or auto-switching) and can operate from any 110 - 240 VAC 50/60 Hz supply, though do check the label to confirm.

A laptop AC adapter



Image by Olga Popova © 123RF.com



Note: Plugging a fixed-input 220 - 240 V adapter into a 110 - 120 V supply won't cause any damage (though the laptop won't work), but plugging a fixed-input 110 - 120 V adapter into a 220 - 240 V supply will likely cause damage.

AC adapters are also rated for their power output (ranging from around 65–120 W). Again, this information will be printed on the adapter label. The AC adapter connects to the laptop via a DC jack or a USB port.

Battery Power

Laptop computers use removable, rechargeable Lithium-ion (Li-ion) [battery](#) packs. Li-ion batteries are typically available in 6-, 9-, or 12-cell versions, with more cells providing for a longer charge. The connector and battery-pack form factor are typically specific to the laptop vendor and a range/model.

Before inserting or removing the battery pack, you must turn the machine off and unplug it from the AC wall outlet. A portable battery is usually removed by releasing catches on the back or underside of the laptop.

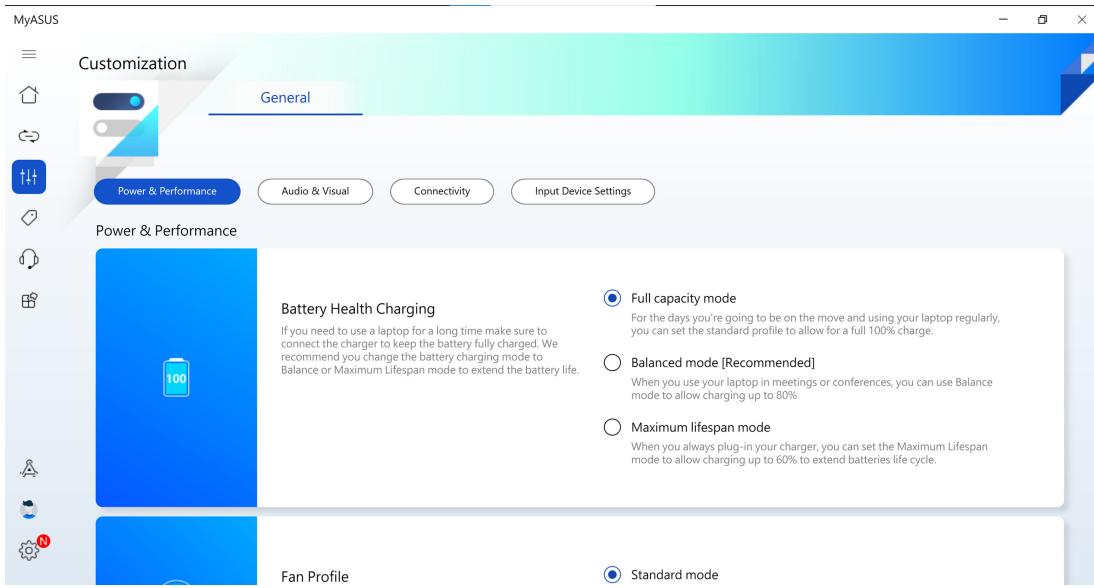
A removable laptop battery pack



Image by cristil180884 © 123RF.com

The battery recharges when the laptop is connected to the AC adapter and is connected to power. When the laptop is in use, the battery is trickle-charged. A laptop should come with a power management driver to ensure a proper charging regime and prevent repeated trickle charging from damaging it. Li-ion battery life is affected by being fully drained of charge and by being held continually at 100% charge. Balanced power charging stops trickle charging at 80%. Li-ion batteries are also sensitive to heat. If storing a Li-ion battery, reduce the charge to 40% and store below 20°C.

Customization in MyASUS V3.1.0.0



Screenshot used with permission from ASUSTek Computer Inc.

It highlights a Battery Health Charging section with three modes: Full capacity mode, Balanced mode (recommended), and Maximum lifespan mode. Each mode offers different options for battery usage and charging optimization. The full capacity mode is selected.



Note: Li-ion batteries hold less charge as they age and typically have a maximum usable life of around 2–3 years. If you charge a battery and the run time is substantially decreased, you may need to purchase a new battery.

RAM and Adapter Replacement

Laptops have fewer field-replaceable units (FRU) than desktops. That said, laptop components and designs have become better standardized. Using components sourced from the laptop vendor is still recommended, but basic upgrade options, such as system memory and fixed disks, have become much simpler.

Some FRUs can be accessed easily by removing a screw plate on the back cover (underside) of the laptop. This method generally provides access to the fixed disk, optical drive, memory modules, and possibly adapter card slots for components such as Wi-Fi cards and cellular radios.

Upgrading RAM Modules

Laptop **RAM** is packaged in Small Outline Dual In-line Memory Modules (SODIMMs). As with DIMMs, a given SODIMM slot will only accept a specific type of DDR. For example, you cannot install a DDR4 SODIMM in a DDR3 slot. The slots are keyed to prevent incompatible modules from being installed.

Two SODIMM RAM modules. The modules stack one over the other. When the side catches are released, the modules pop up at an angle for easy removal.



Image courtesy of CompTIA.

A SODIMM slot pops-up at a 45° angle to allow the chips to be inserted or removed. Sometimes one of the memory slots is easily accessible via a panel, but another requires more extensive disassembly of the chassis to access.

Note: There are a couple of other laptop memory module form factors, including Mini-DIMM and Micro-DIMM. These are smaller than SODIMM and are used on some ultraportable models. Always check the vendor documentation before obtaining parts for upgrade or replacement.

Upgrading Adapter Cards

Depending on the design, adapters for modems, **wireless cards**, and SSD storage cards may be accessible and replaceable via screw-down panels. Note that there are several adapter formats, notably Mini PCIe, mSATA, and M.2, none of which are compatible with one another.

You can obtain mini PCIe or M.2 adapters for laptops that will provide some combination of Wi-Fi, Bluetooth, and/or cellular data connectivity. Remember that when upgrading this type of adapter, you need to re-connect the antenna wires used by the old adapter or install a new antenna kit. The antenna wires are usually routed around the screen in the laptop's lid. The antenna connections can be fiddly to connect and are quite delicate, so take care.

Wi-Fi adapter installed as a mini PCIe card. Note the antenna wire connections.



Image courtesy of CompTIA.

If installing an adapter with GSM or LTE cellular functionality, remember to insert the SIM card as well.

Disk Upgrades and Replacement

A laptop typically supports one internal mass storage device only, with extra storage attached to an external port. This means that to upgrade the fixed disk, there must be a plan for what to do with existing data:

- **Migration** means using backup software to create an image or clone of the old drive and store it on USB media. When the new drive has been installed, the system image can be restored to it. A system image is technology neutral, so an image of a Hard Disk Drive (HDD) can be applied to an SSD. However, the new drive must be the same size or larger than the old one, unless using a cloning tool that can shrink the source image.



As an alternative to using a third USB drive to store the image, a disk enclosure allows you to connect an internal drive temporarily as an external drive. You can then migrate the image directly to the SSD before removing the old drive and installing the new one.

- **Replacement** means that only data is backed up from the old drive. The new drive is then fitted to the laptop and an OS plus apps are installed. User data can then be restored from backup.

The fixed disk can be accessed via a panel, but you may have to open the chassis on some models.

Laptop HDDs are usually 2.5" form factor, though sometimes the 1.8" form factor is used. Compared to 3.5" desktop versions, magnetic 2.5" HDDs tend to be slower (usually 5400 rpm models) and have lower capacity. Within the 2.5" form factor, there are also reduced height units designed for ultraportable laptops. A standard 2.5" drive has a z-height of 9.5 mm; an ultraportable laptop might require a 7 mm (thin) or 5 mm (ultrathin) drive.

A laptop HDD with SATA interface



Magnetic drives use ordinary SATA data and power connectors, though the connectors on the drive mate directly to a port in the drive bay, without the use of a cable. Drive bays measuring 1.8" might require the use of the micro SATA (μ SATA or uSATA) connector.

An SSD flash storage device can also use the SATA interface and connector form factors but is more likely to use an adapter card interface:

- mSATA - An SSD might be housed on a card with a Mini-SATA (mSATA) interface. These cards resemble Mini PCIe cards but are not physically compatible with Mini PCIe slots. mSATA uses the SATA bus, so the maximum transfer speed is 6 Gb/s.
- M.2 - An M.2 SSD usually interfaces with the PCI Express bus, allowing much higher bus speeds than SATA. M.2 adapters can be different lengths (42 mm, 60 mm, 80 mm, or 110 mm), so you should check that any given adapter will fit within the laptop chassis. The most popular length for laptop SSDs is 80 mm (M.2 2280).



The specific M.2 form factor is written as xxxyy, where xx is the card width and yy is the length. For example, 2280 means a card width of 22 mm and a length of 80 mm.

Keyboard and Security Component Replacement

As mechanical devices, components such as the keyboard, touchpad, and biometric sensors can easily be damaged. If parts can be obtained from the vendor, it can be more cost-effective to replace damaged components than buy a new laptop.

Keyboard and Touchpad Replacement

When you are replacing components such as the **keyboard** and **touchpad**, you will almost always need to use the same part as was fitted originally. Accessing the parts for removal and replacement might require complete disassembly of the chassis or might be relatively straightforward – check the service documentation.

Each part connects to the motherboard via a data cable, typically a flat ribbon type. The cable is held in place by a latch that must be released before trying to remove the cable and secured after insertion.

When replacing an input device, use the OS/driver settings utility or app to configure it. A keyboard should be set to the correct input region. Touchpads need to be configured to an appropriate sensitivity to be comfortable for the user.

Key Replacement

In some circumstances, it might be economical to lift a single key for cleaning or replacement. Carefully pry off the plastic key cap with a flat blade to expose the retainer clip. The retainer clip can also be removed for cleaning, but it is fragile so take care. To replace, line up each component carefully and then push to snap it back into place.

Biometric Security Components

A **biometric** sensor allows users to record a template of a feature of their body that is unique to them. On a laptop, this is typically implemented as a fingerprint scanner, though the camera can also be used to make facial scans or to scan an iris eye pattern. A fingerprint sensor might be installed as a separate component or might be a feature of the keyboard or touchpad.

A fingerprint reader board is attached to the motherboard by a flat ribbon cable in the same way as the keyboard and touchpad.

Camera and Microphone

The camera is typically integrated into the display assembly which will require extensive disassembly to access and replace the camera. The connections for the camera will run through the display assembly and connect to the motherboard.

Many users will use magnetic or sliding camera privacy shades to block the camera lens when it is not supposed to be used. When replacing a camera, make sure to carefully remove the privacy shade and see if it can be reused.

The microphone assembly is often connected right next to the camera assembly but will have separate connections.

Near-Field Scanner

A **near-field communication (NFC) scanner** on a laptop is primarily used to pair peripheral devices or to establish a connection to a smartphone. This is configured via the vendor's app.

NFC might be implemented as a feature of the keyboard, touchpad, or fingerprint reader. As well as the data connection to the motherboard, the NFC sensor must be connected to its antenna.

Lesson 9D

Troubleshoot Mobile Devices

Lesson Overview

Field technicians have been bringing you their mobile devices to troubleshoot and fix different issues. As the lead technician, part of your job is to handle these issues and make sure the mobile devices remain in proper working order.

In this lesson, you will learn how to identify and troubleshoot common issues with mobile devices including power and battery, hardware failure, screen and calibration, connectivity, and malware issues.



Objectives Covered

5.4 Given a scenario, troubleshoot common mobile devices issues.

Learning Outcomes

As you study this lesson, answer the following questions:

- What are the steps that should be taken if a mobile device is not working with AC power?
- What are common causes of overheating in a laptop?
- Why would a port be physically damaged?
- What troubleshooting steps should be taken when dealing with a possible digitizer issue?
- What are some of the signs of a potential malware issue?

Power and Battery Issues

If you experience problems working from AC power, first test the outlet with a "known good" device (such as a lamp). Next, check that the LED on the AC adapter is green. If there is no LED, check the fuse on the plug, and if available, try testing with a known good adapter.



Sometimes AC adapters can get mixed up. If an underpowered adapter is used - for example, a 65 W adapter is plugged into a 90 W system - the laptop will display a warning at boot time.

If a mobile device will not power on when disconnected from building power, first check that the battery is seated properly in its compartment. Also, check whether the battery contacts are dirty. You can clean them using swabs and isopropyl alcohol (90% or higher).

If the battery is properly inserted and the mobile device does not switch on or only remains on for a few seconds, it is most likely completely discharged. A battery exhibiting **poor health** will

not hold a charge. This means that the battery is at the end of its useful life. You can test this by using a known good battery. If a known good battery does not work, then there is something wrong with the power circuitry on the motherboard.

While laptop batteries are replaceable, few smartphones or tablets come with removable battery packs. Most vendors try to design their devices so that they will support "typical" usage for a full day without charging. As the battery ages, it becomes less able to hold a full charge. If it is non-removable, the device will have to be returned to the vendor for battery replacement.

Mobile handset with cover removed - the battery is accessible but not designated as user-removable

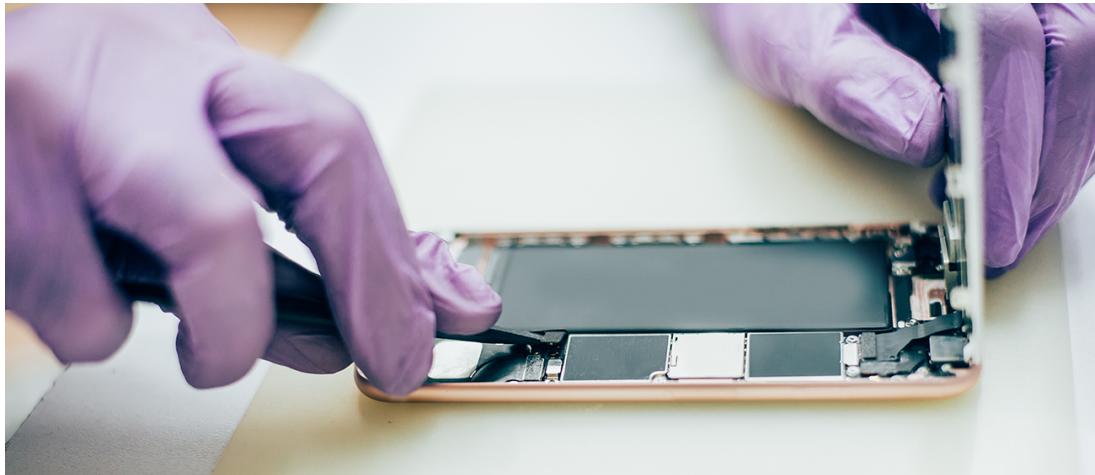


Image by guruxox © 123RF.com

Improper Charging Symptoms

Properly caring for the battery not only prolongs battery life but also mitigates health and safety risks. Use the battery charger provided by the manufacturer or an approved replacement charger. Using an incorrect battery charging cable or exposing a battery to extreme heat carries risks of fire or even explosion.



Note: Exercise caution when leaving batteries to recharge unattended (for example, overnight). Do not leave a battery charger close to flammable material, and ensure there is plenty of ventilation around the unit.

An **improper charging** routine will reduce the usable life of a battery. Follow manufacturer instructions on the proper charging and discharging of the battery. Make use of power management features included with your device/OS to prolong battery life. A Li-ion battery should not be allowed to fully discharge regularly or be kept persistently at 100% charge, as this reduces battery life.

As batteries age, the maximum charge they can sustain decreases, so short battery life will usually indicate that the battery needs replacing. If the battery is not old or faulty, you could suspect that an app is putting excessive strain on the battery. You can use an app to check battery utilization.

Battery status and notifications in iOS (left) and Android (right)



Screenshot reprinted with permission from Apple Inc., and Android platform, a trademark of Google LLC.

The battery settings for iOS has toggles for low power mode and battery percentage. The battery usage for last 24 hours is shown as follows:

Facebook: 37 percent Home and Lock Screen: 11 percent MailOnline: 10 percent WhatsApp: 9 percent The settings for Android are: Battery Saver: Off or Never turn on automatically 84 percent, Approx 59 minutes left. Usage since last full charge: Screen, Mobile standby, and Chrome.

Swollen Battery Symptoms

If you notice any **swelling** from the battery compartment, discontinue use of the mobile device immediately. Signs that the battery has swollen can include a device that wobbles when placed flat on a desk or a deformed touchpad or keyboard. A swollen battery indicates some sort of problem with the battery's charging circuit, which is supposed to prevent overcharging. If a device is exposed to liquid, this could also have damaged the battery.

Li-ion batteries are designed to swell to avoid bursting or exploding, but great care must be taken when handling a swollen battery to avoid further damage. A swollen battery is a fire hazard and could leak hazardous chemicals - do not allow these to come into contact with your skin or your eyes. If the battery cannot be released safely and easily from its compartment, contact the manufacturer for advice. You should also contact the manufacturer for specific disposal instructions. A swollen battery should not be discarded via standard recycling points unless the facility confirms it can accept batteries in a potentially hazardous state.



Note: Manufacturing defects in batteries and AC adapters often occur in batches. Make sure you remain signed up to the vendor's alerting service so that you are informed about any product recalls or safety advisories.

Hardware Failure Issues

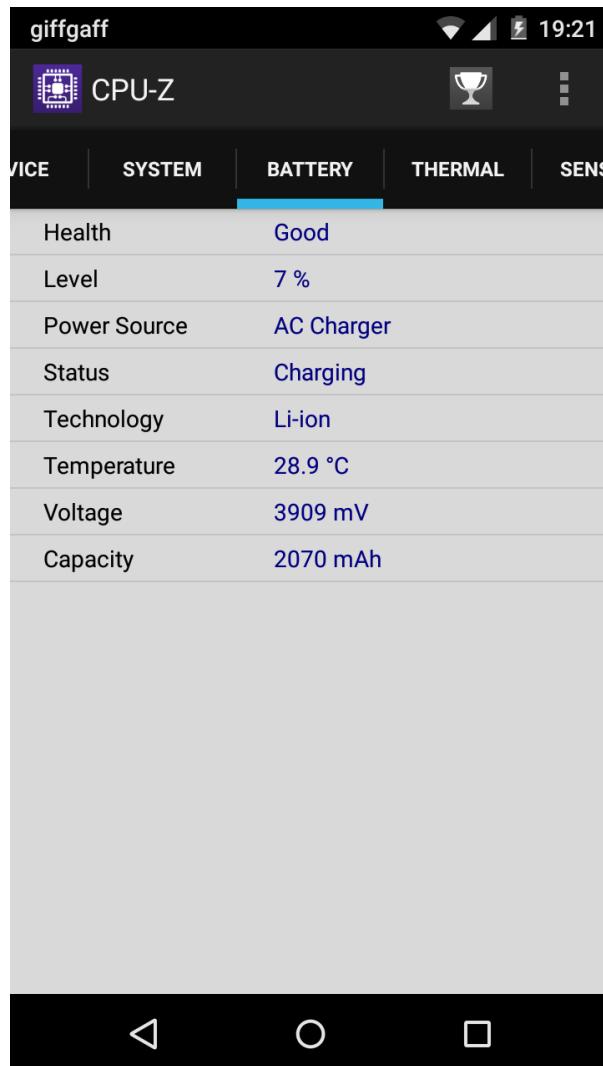
Mobile devices are more susceptible to mechanical problems than most desktop PCs, so you should be alert to the symptoms of hardware failure.

Overheating Symptoms

The compact design of mobile devices makes them vulnerable to **overheating**. The bottom surface of a laptop becomes hot when not properly ventilated. This can easily happen when laptops are put on soft surfaces, on people's laps, or in places where there is not enough room between the vents and a wall. Laptop cooling (or chiller) pads are accessories that are designed to sit under the laptop to maximize airflow and protect a user from getting a burn from a device overheating.

Dust trapped in vents acts as an insulator and can prevent proper cooling. Handheld devices use passive cooling and therefore can become quite warm when used intensively. High screen brightness and use of the flashlight function will rapidly increase heat. A mobile device will start to overheat quickly when exposed to direct sunlight. Devices have protective circuitry that will initiate a shutdown if the internal temperature is at the maximum safe limit. You can also use an app to monitor the battery temperature, and then compare that to the operating limits. Generally speaking, approaching 40°C is getting too warm.

CPU-Z app showing the device's battery status



Liquid Damage Symptoms

Some mobile device cases provide a degree of waterproofing. Waterproofing is rated on the Ingress Protection (IP) scale. A case or device will have two numbers, such as IP67. The first (6) is a rating for repelling solids, with a 5 or 6 representing devices that are dust-protected and dust-proof, respectively. The second value (7) is for liquids, with a 7 being protected from immersion in up to 1 m and 8 being protected from immersion beyond 1 m.



Note: If dust protection is unrated, the IP value will be IPX7 or IPX8.

If a mobile device is exposed to **liquid damage**, there may be visible signs of water under the screen. The screen might display graphics artifacts or not show an image. Even if there is no visible sign, power off the device immediately if you suspect liquid damage. Dry as much excess liquid as possible. If you suspect that the internal components have been exposed, the

device must be disassembled to fully dry. Once dry, clean the circuit boards and contacts. The battery will usually need to be replaced.

Physically Damaged Port Symptoms

Improper insertion and removal of connectors can easily **damage the external ports** of a mobile device. If a port is damaged, the connector may be loose or may no longer fit. There may be no data connection at all, or it might be intermittent. The device may fail to charge properly.

Educate users to remove a connector by holding the connector and pulling it straight. A connector should not be jiggled to remove it. USB-C and Lightning connectors are reversible. Make sure users take care to orient other connector types properly before plugging them in.

Screen and Calibration Issues

When you are troubleshooting a mobile display issue, you will often need to take into account the use of the integrated display and/or an external display and how to isolate a problem to a particular component, such as the graphics adapter, display panel, backlight, and digitizer.

If there is no image on the screen, check that the video card is good by using an external monitor. Alternatively, there should be a very dim image on the display if the graphics adapter is functioning, but the backlight has failed. Most screens use LED backlights. Older laptops might use an inverter component to power a fluorescent backlight.



As well as the display itself, it is common for the plastics around a laptop case to get cracked or broken and for the hinges on the lid to wear out. The plastics are mostly cosmetic (though a bad break might expose the laptop's internal components to greater risks), but if the hinges no longer hold up the screen, they will have to be replaced.

Broken Screen Issues

Mobile devices are very easy to drop, and while the glass is designed to be tough, impacts on a hard surface from over 1m in height will usually result in cracking or shattering. If only the glass layer is damaged, the digitizer and display may remain usable, to some extent. A **broken screen** is likely to require warranty or professional services to repair it, however.



Note: If there are no visible cracks, the screen or digitizer circuitry may have been damaged by liquid.

Digitizer Issues

Symptoms such as the touch screen not responding to input or the stylus not working can indicate a problem with the digitizer. If you can discount shock and liquid damage, try the following tests:

- Verify that the touchscreen and the user's fingers are clean and dry.
- If a screen protector is fitted, check that it is securely adhered to the surface and that there are no bubbles or lifts.
- Check that there is not a transitory software problem by restarting the device.
- Try using the device in a different location in case some source of electromagnetic interference (EMI) is affecting the operation of the digitizer.
- If the device has just been serviced, check that the right wires are still connected in the right places for the digitizer to function. Remember to ask, "What has changed?"

Cursor Drift / Touch Calibration Issues

On a laptop, if touchpad sensitivity is too high, typing can cause vibrations that move the cursor. Examples include the pointer drifting across the screen without any input or a "ghost cursor" jumping about when typing. Install up-to-date drivers and configure input options to suit the user. Many laptops now come with a Fn key to disable the touchpad.

If you can rule out simple hardware causes, unresponsive or inaccurate touch input can be an indication of resources being inadequate (too many open apps) or badly written apps that hog memory or other resources. A soft reset will usually fix the problem in the short term. If the problem is persistent, either try to identify whether the problem is linked to running a particular app or try freeing space by removing data or apps. Windows devices and some versions of Android support re-calibration utilities, but if you cannot identify another cause, then you are likely to have to look at warranty repair.

Connectivity Issues

Wi-Fi and Bluetooth **connectivity** issues on a mobile can be approached in much the same way as on a PC. Problems can generally be categorized as either relating to "physical" issues, such as interference, or to "software" configuration problems.

Consider these guidelines when you are troubleshooting issues with communication and connectivity:

- Verify that the adapter is enabled. Check the status of function key toggles on a laptop, or use the notification shade toggles on a mobile device to check that airplane mode has not been enabled or that the specific radio is not disabled.
- If a laptop has been serviced recently and wireless functions have stopped working, check that the antenna connector has not been dislodged or wrongly connected.
- If a wireless peripheral such as a Bluetooth mouse or keyboard that has been working stops, it probably needs a new battery.
- If you experience problems restoring from hibernate or sleep mode, try cycling the power on the device or reconnecting it and checking for updated drivers for the wireless controller and the devices.

If you are experiencing intermittent connectivity issues:

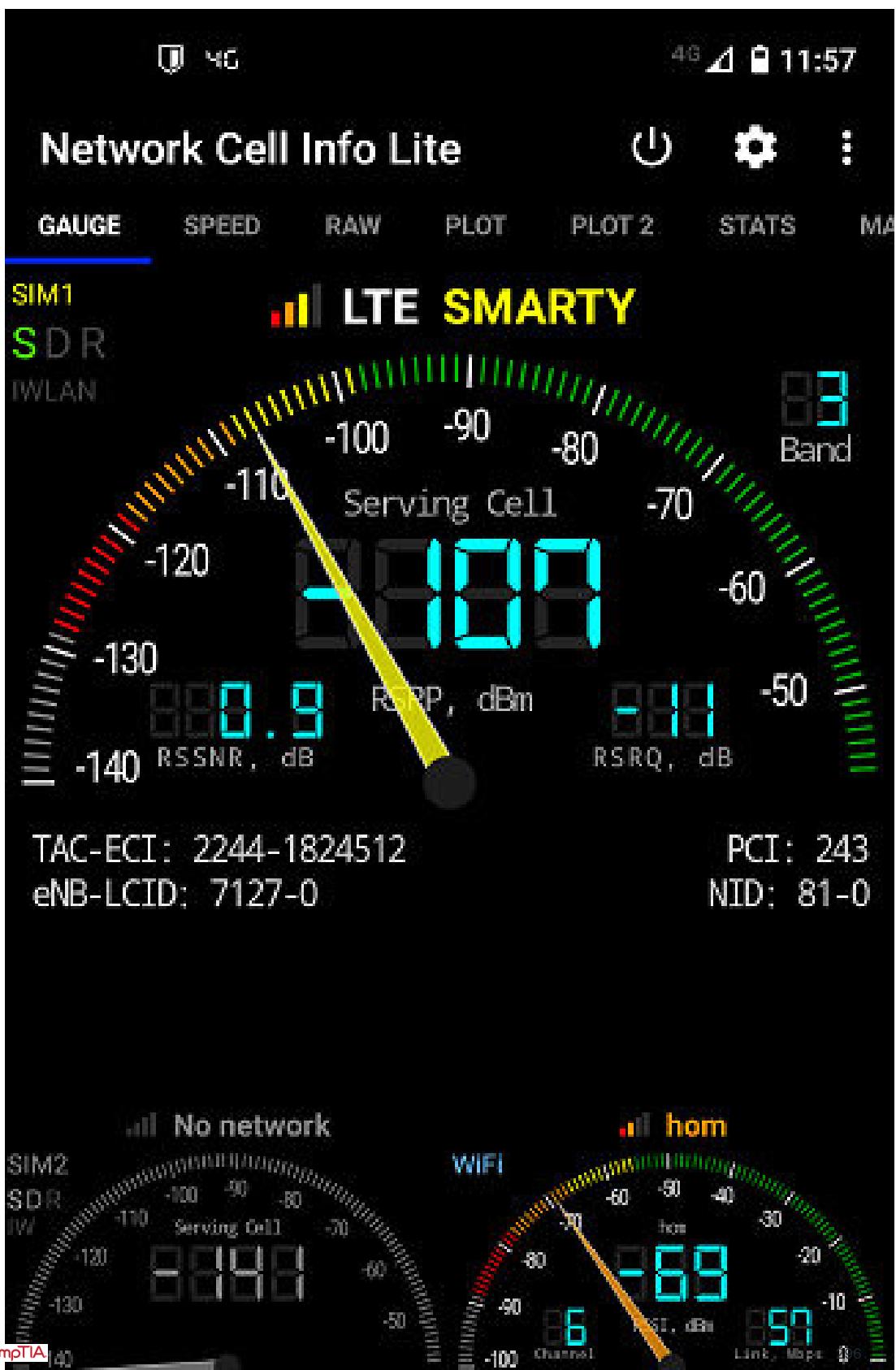
- Try moving the two devices closer together.
- Try moving the devices from a side-to-side or up-and-down position to a different position or changing how the device is held.



The radio antenna wire for a mobile will be built into the case (normally around the screen). On some devices, certain hand positions can stop the antenna from functioning as well as it should.

- Consider using a Wi-Fi analyzer to measure the signal strength in different locations to try to identify the source of interference.

Network Cell Info Lite showing cell tower connection status in the top gauge and Wi-Fi in the lower gauge



Screenshot used with permission from M2Catalyst, LLC

A similar utility (Cell Tower Analyzer or GSM Signal Monitor) can be used to analyze cellular radio signals, which use different frequencies than Wi-Fi uses. An app might combine both functions.

Malware Issues

Whenever a device does not function as expected, you should assess whether it could be infected with malware. Consider the following scenarios:

- Malware or rogue apps are likely to try to collect data in the background. They can become unresponsive and might not shut down when closed. Such apps might cause excessive power drain and high resource utilization, potentially leading to overheating problems.
- This excessive background usage will also lead to degraded performance. This is a common sign of a malware infection.
- Another tell-tale sign of a hacked device is reaching the data transmission overlimit unexpectedly. Most devices have an option to monitor data usage and have limit triggers to notify the user if the limit has been reached. This protects from large data bills but should also prompt the user to check the amount of data used by each application to monitor their legitimacy.
- Malware may try to use the camera or microphone to record activity. Check that the camera LED is not activated.
- The user also may not be able to install new applications. Malware may block new applications to prevent security software from being installed or the malware may use up so much free space that there is not enough space left to install new applications.

Module 10

Supporting Print Devices

Module Overview

You work for a graphic design firm that specializes in creating marketing materials, including brochures, posters, and digital content for various clients. The firm relies heavily on a range of print devices, including multifunction printers, laser printers, inkjet printers, and 3-D printers, to produce high-quality outputs for client presentations and proofs. Your task is to ensure that all print devices are functioning optimally, are well-maintained, and that any issues are quickly resolved to minimize downtime and maintain productivity.

Module Summary

Prepare for A+ Core 1 by:

- Deploying printer and multifunction devices
- Replacing print device consumables
- Troubleshooting print device issues

Lesson 10A

Printers and Multifunction Devices

Lesson Overview

The design team at your firm is preparing for a major client presentation and needs to print high-quality mock-ups of their designs. They require guidance on selecting the right printer for their needs and ensuring it is set up correctly in their workspace.



Objectives Covered

3.7 Given a scenario, deploy and configure multifunction devices/printers and settings.

Learning Outcomes

As you study this lesson, answer the following questions:

- What environmental factors should be considered when setting up a printer to ensure optimal performance and longevity?
- Why is it important to regularly update the firmware on multifunction devices and printers?
- How do you confirm that a printer with USB connectivity is properly installed and functioning?
- How can you configure default settings for a printer using the Printer Properties dialog in Windows?
- How can you configure a printer to be shared across a network in a Windows environment?
- What measures can be implemented to ensure the security of a networked printer?

Printer Unboxing and Setup Location

Printer types or technologies create images on paper using various technologies. The most common for home and office use are inkjet and laser printers. Major print device vendors include HP, Epson, Canon, Xerox, Brother, OKI, Konica/Minolta, Lexmark, Ricoh, and Samsung.



The term "printer object" or "logical printer" refers to the software representation of the printer, while "print device" or "physical printer" denotes the actual hardware.

Selecting a Printer

Consider the following criteria when choosing a printer:

- **Speed:** Measured in pages per minute (ppm). Monochrome text prints faster than color photos.

- **Resolution:** Measured in dots per inch (dpi). Higher dpi means better quality. Vertical and horizontal resolutions may differ (e.g., 2400×600 dpi).
- **Paper Handling:** Types and sizes of paper the printer can handle, including labels, envelopes, and card stock. Also, consider paper tray capacity to avoid jams.
- **Options:** Additional features like an automatic [duplex unit](#) for double-sided printing and finishing units for folding, stapling, and hole punching.

Setup Location

When choosing a location for your printer, consider:

- **Power and Network:** Ensure access to a power outlet and network data port. Avoid trip hazards with cables.
- **Environment:** Place the printer on a stable, flat surface away from direct sunlight. Ensure good ventilation to disperse fumes and store consumables in a dry, temperature-controlled area.
- **Accessibility:** The printer should be easily accessible but not disruptive. For confidential printing, consider an access-controlled area.

Unboxing

After selecting an installation location, follow the manufacturer's instructions to unbox and set up the printer. Keep these general factors in mind:

- **Lifting:** Many printers are heavy and may require two people to lift safely. Use safe lifting techniques, bend at the knees, and grip only the designated handle locations. Ensure the path is free from trip hazards.
- **Packing Materials:** Remove all packing strips and supports before switching on the printer. Check for strips on removable components concealed by panels.
- **Acclimation:** Allow the printer to acclimate after unboxing. Leave it powered off for a few hours to prevent condensation issues if it has moved from a cold to a warm environment. Similarly, store printer paper for a day or more to adjust to the installation location's temperature and humidity.

Firmware Management in MFDs and Printers

Firmware in multifunctional devices (MFDs) and printers controls functions like printing, scanning, and network connectivity. Regular updates improve performance, fix bugs, and address security vulnerabilities, which is crucial for networked printers handling sensitive data.

Firmware ensures compatibility with drivers and operating systems and provides access to advanced settings such as IP addresses, DNS configurations, security features, and network scanning options.

Checking and Updating Firmware

To check the firmware version:

- Use the control panel under System Information.
- Access the device's web interface by entering its IP address in a browser.

To update firmware:

- Download and install updates via the control panel, web interface, or manufacturer tools like HP Web Jetadmin or Canon imageWARE.

Regular updates ensure devices remain secure, compatible, and perform optimally.

Resetting and Reflashing Firmware

Outdated or corrupted firmware can cause malfunctions. Learning to reset or reflash firmware is a key troubleshooting skill:

- **Resetting:** Use the control panel to navigate to Settings or Maintenance, then select Reset or Restore Factory Defaults.
- **Reflashing:** Access the web interface, go to the Firmware Update or Maintenance section, upload the latest firmware file from the manufacturer's website, and follow the prompts.



Note: Reflashing the firmware should only be done when necessary, as it could potentially cause issues if interrupted.

Best Practices

Always back up configurations before performing updates. Additionally, test new firmware on a single device before deploying it across multiple devices to ensure compatibility and stability.

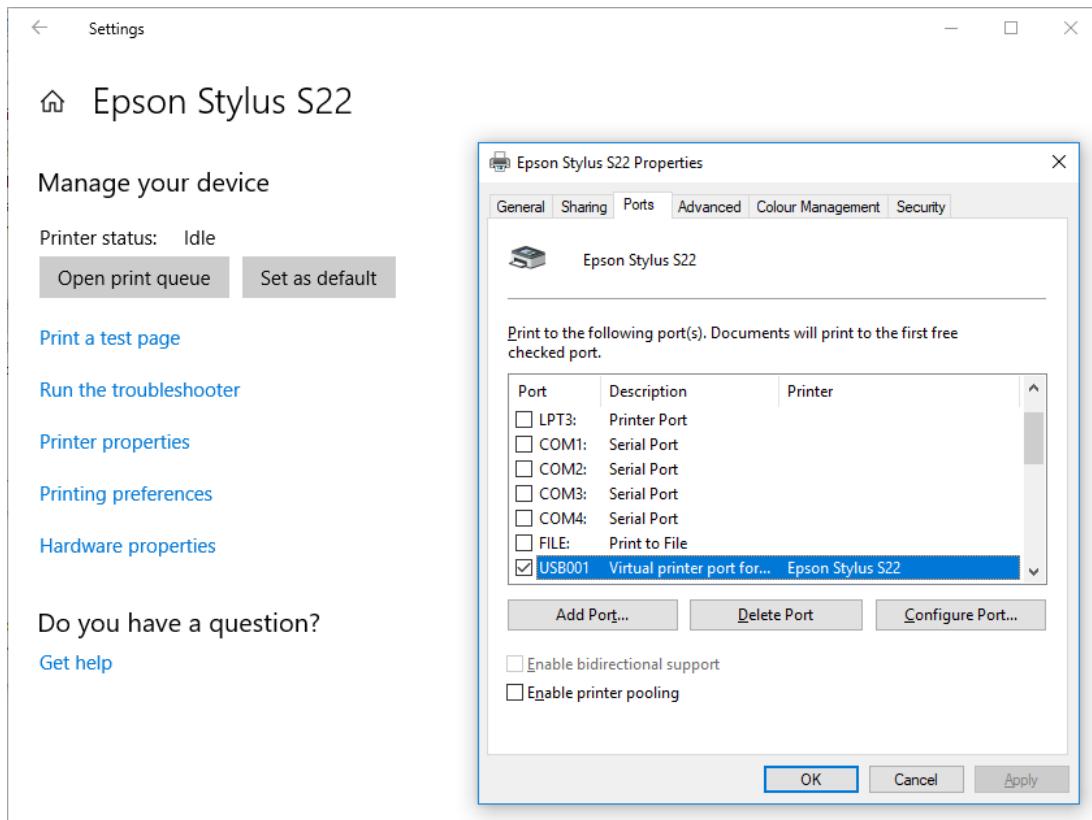
Print Device Connectivity

Each print device supports a range of wired and wireless connection interfaces.

USB Print Device Connectivity

To install a printer with **USB connectivity**, connect the Type B plug to the printer and the Type A plug to a USB port on the computer. If a computer only has USB C ports, a USB B to USB C adapter may be needed. The operating system will typically detect the printer automatically through Plug and Play and install the necessary driver. To confirm the installation, you can print a test page using the driver or an OS utility.

Using Windows Settings to verify printer installation to the USB port



Screenshot courtesy of Microsoft.

The printer status is Idle. Open print queue and Set as default buttons are at the top left. The options below are as follows: Print a test page, Run the troubleshooter, Printer properties, Printing Properties, Hardware properties. The text below reads, Do you have a question? Get help link is given below. A pop-up window titled Epson Stylus S 22 Properties shows the Ports tab. A table below lists the ports, their descriptions, and printers. The active port U S B 001: Virtual printer port for Epson Stylus S 22 is highlighted. An option to add port, delete port, and configure port is below the table. The checkboxes to enable bidirectional support and enable printer pooling are on the bottom left. Ok, cancel, and apply buttons are at the bottom.

Ethernet Print Device Connectivity

Most printers come with an Ethernet adapter and RJ45 port. They can obtain an Internet Protocol (IP) address automatically from a DHCP server or be manually configured. The printer's IP address can also be registered on a DNS server for easier client connections via a fully qualified domain name (FQDN).

Printers typically offer local network configuration through an LCD menu system with buttons or a touchscreen.

Setting the IP address configuration method via the printer's control panel

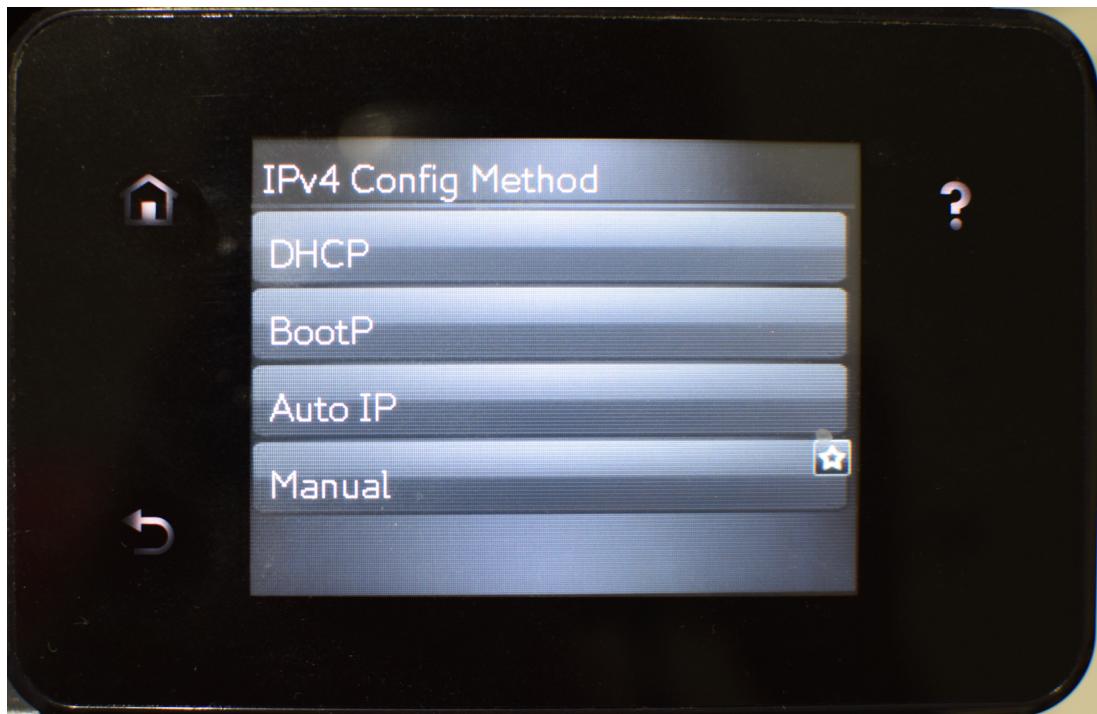


Image courtesy of CompTIA.

Icons and navigation buttons surround the display for further settings access.

This method is useful for small offices with few printers or for troubleshooting when the printer is inaccessible over the network. For broader management, vendors usually provide web-based utilities, and many newer printers also offer mobile apps or cloud-based portals for remote configuration and monitoring.

Managing a printer using a browser

The screenshot shows a web browser window with the URL 192.168.1.250/info_deviceStatus.html?tab=Home&menu=DevStatus. The title bar indicates the device is a **LaserJet 200 color MFP M276 NPID1F933** with IP address **192.168.1.250**. The main content area is titled **Device Status** and includes sections for **Device Status** and **Supplies Summary**. Under **Supplies Summary**, it lists four cartridges with their names, current levels, and model numbers:

Cartridge	Level (%)	Model Number
Black Cartridge	10%	(CF210X)
Cyan Cartridge	95%	(CF211A)
Magenta Cartridge	32%	(CF213A)
Yellow Cartridge	60%	(CF212A)

A **Supplies Detail** button is located at the bottom right of the supplies summary section.

Ensure the printer can communicate over the necessary TCP or UDP ports and verify that these ports are not blocked by firewalls or security software.

Wireless Print Device Connectivity

Wireless printers primarily use Bluetooth and Wi-Fi interfaces. For Bluetooth connections on a Windows client, make the printer discoverable via its control panel, then add the device through the **Bluetooth** settings in Windows.

Wi-Fi connectivity can be established in two ways:

- **Infrastructure mode:** Connect the printer to a Wi-Fi access point, making it available to clients on the network via an IP address or FQDN. Ensure the printer's wireless adapter supports the same 802.11 standard as the access point.
- **Wi-Fi Direct:** Set up a software-implemented access point on the printer to allow direct connections from client devices.

Using the printer control panel to verify Wi-Fi connection status in infrastructure mode



Image courtesy of CompTIA.

The printer is connected to the network with an IP address of 192.168.1.247. The SSID of the connected Wi-Fi network is comptia underscore w Lan, and it is operating on Channel 1. The hardware address of the printer is displayed as 1 c:3 e:84:04:8 f:c 2. The screen includes options such as Wireless Menu and an OK button for navigation. Icons and navigation buttons surround the display for further settings access.

Additionally, mobile printing features like Apple AirPrint, Mopria, and cloud-based solutions such as HP ePrint are now commonly used for wireless printing, complementing traditional Bluetooth and Wi-Fi options.

Printer Drivers and Page Description Languages

Applications that support printing typically follow the "what you see is what you get" (WYSIWYG) principle, ensuring the screen and print output are identical. Printer drivers serve as the interface between the print device and the operating system. For networked printers used by clients with different operating systems, each client must have a suitable driver installed. Note that 64-bit operating systems require 64-bit drivers.

! Many older printers have become unusable because vendors have not developed 64-bit drivers for them. If an up-to-date driver is not available from Microsoft, download it from the printer vendor's website, extract it to a folder on your PC, and use the "Have Disk" option in the Add Printer Wizard to install it.

Typically, the appropriate print driver is selected and installed automatically when the printer is detected, a process known as Plug and Play (PnP). However, you might need to manually add the driver or choose a version that supports a specific [page description language \(PDL\)](#).

To manually select a driver based on PDL:

1. Download the driver from the printer vendor's website.

2. Open the "Add Printer Wizard" in your operating system.
3. Choose the "Have Disk" option and navigate to the folder where the driver is extracted.
4. Select the driver that matches the desired PDL (e.g., PCL, PostScript, or XPS).
5. Complete the installation process.

A PDL converts print commands from software applications into a raster file, which is a dot-by-dot description of where the printer should place ink. PDLs generally support the following features:

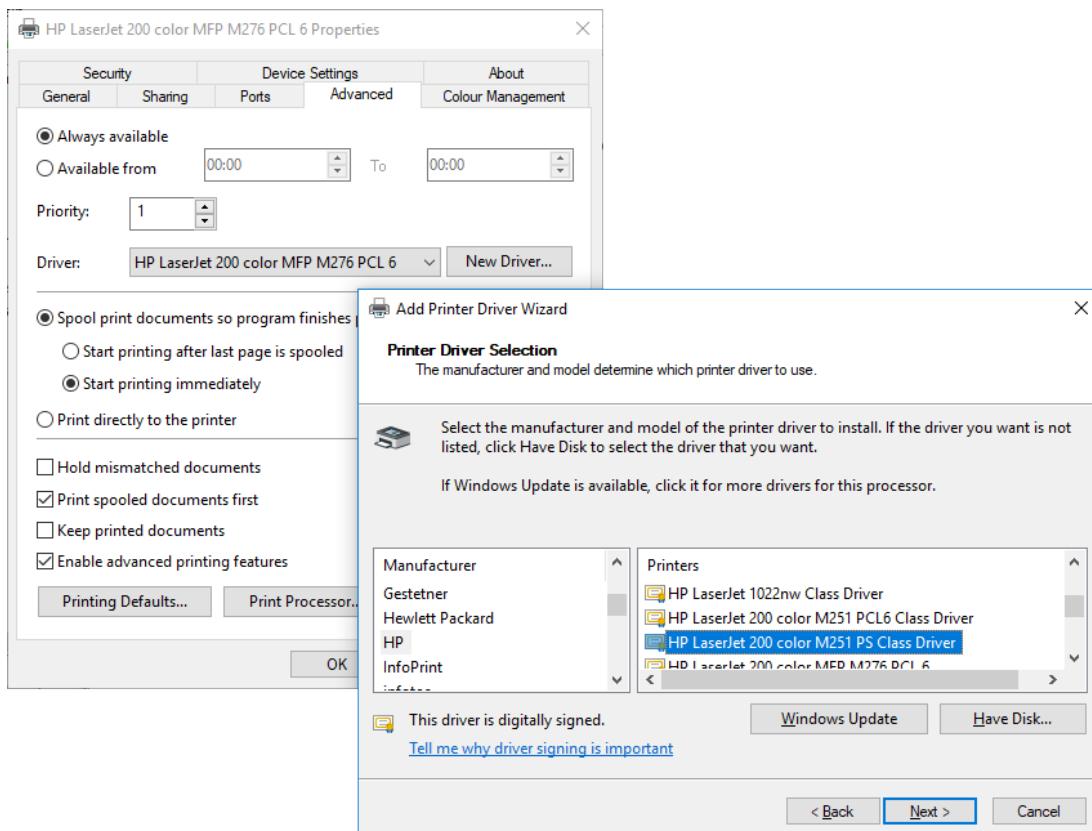
- **Scalable fonts:** Unlike bitmap fonts, which are fixed-size dot-by-dot images, scalable fonts are described by vectors and can be resized. All Windows printers support scalable TrueType or OpenType fonts.
- **Vector graphics:** Similar to scalable fonts, vector graphics describe how lines should be drawn, rather than providing a pixel-by-pixel description.
- **Color printing:** PDLs support color models to ensure accurate translation between on-screen colors and print output. Printers use the CMYK (cyan, magenta, yellow, black) color model, which differs from the RGB (red, green, blue) model used by computer displays.

 The "K" in CMYK is usually explained as standing for "key," as in a key plate used to align the other plates in the sort of offset print press used for professional color printing in high volumes. It might be more helpful to think of it as "black," though.

The choice of PDL is often driven by software compatibility. Adobe [PostScript](#) is device-independent and commonly used for professional desktop publishing and graphic design. It ensures consistent output across different devices but may be slower than other PDLs. HP's [Printer Control Language \(PCL\)](#) is more closely tied to specific printer models and may vary in output depending on the device, but it is usually faster than PostScript. Many Windows printers default to using Microsoft's XML Paper Specification (XPS) PDL, which offers better integration with Microsoft applications and faster performance than PostScript in some cases. However, it may lack the widespread compatibility of PCL and PostScript.

In an office setting where speed is critical, such as printing large volumes of text documents, PCL is often preferred due to its faster processing. Conversely, a graphic designer working on high-quality print materials, such as brochures or posters, would choose PostScript for its superior consistency and precision across devices.

A print device might support more than one PDL—this HP printer supports both Printer Control Language (PCL) and PostScript (PS)



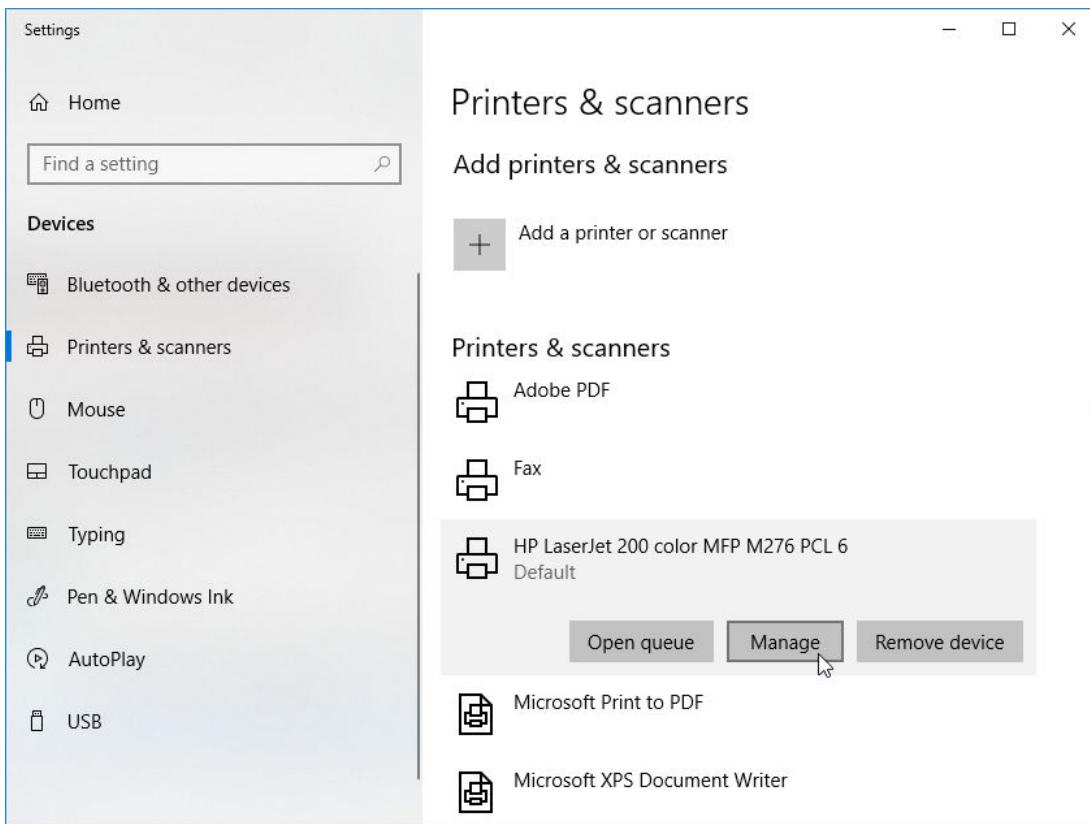
Screenshot courtesy of Microsoft.

The first window shows the properties for an HP LaserJet 200 color MFP M276 PCL 6 printer. The advanced tab at the top is selected. The second dialog box is part of the Add Printer Driver Wizard, allowing users to select the printer driver. It lists available drivers, including the HP LaserJet 200 series. The window update and have disk buttons are on the bottom right. The back, next, and cancel buttons are at the bottom.

Printer Properties

Each logical printer object can be set up with default **configuration settings** via its driver or app.

Viewing the print queue and configuring preferences through the Printers and Scanners Settings app page



Screenshot courtesy of Microsoft.

The left panel displays a field to find a setting at the top. The options under the head devices are Bluetooth and other devices, Printers and Scanners, Mouse, Touchpad, Typing, and Pen and Windows Ink. The page lists installed printers and scanners, including H P LaserJet 200 color M F P M 276 P C L 6, which is marked as the default device. The interface provides options to Open queue, Manage, or Remove device for the selected printer. Other devices like Adobe P D F, Fax, and Microsoft Print to P D F are also listed.

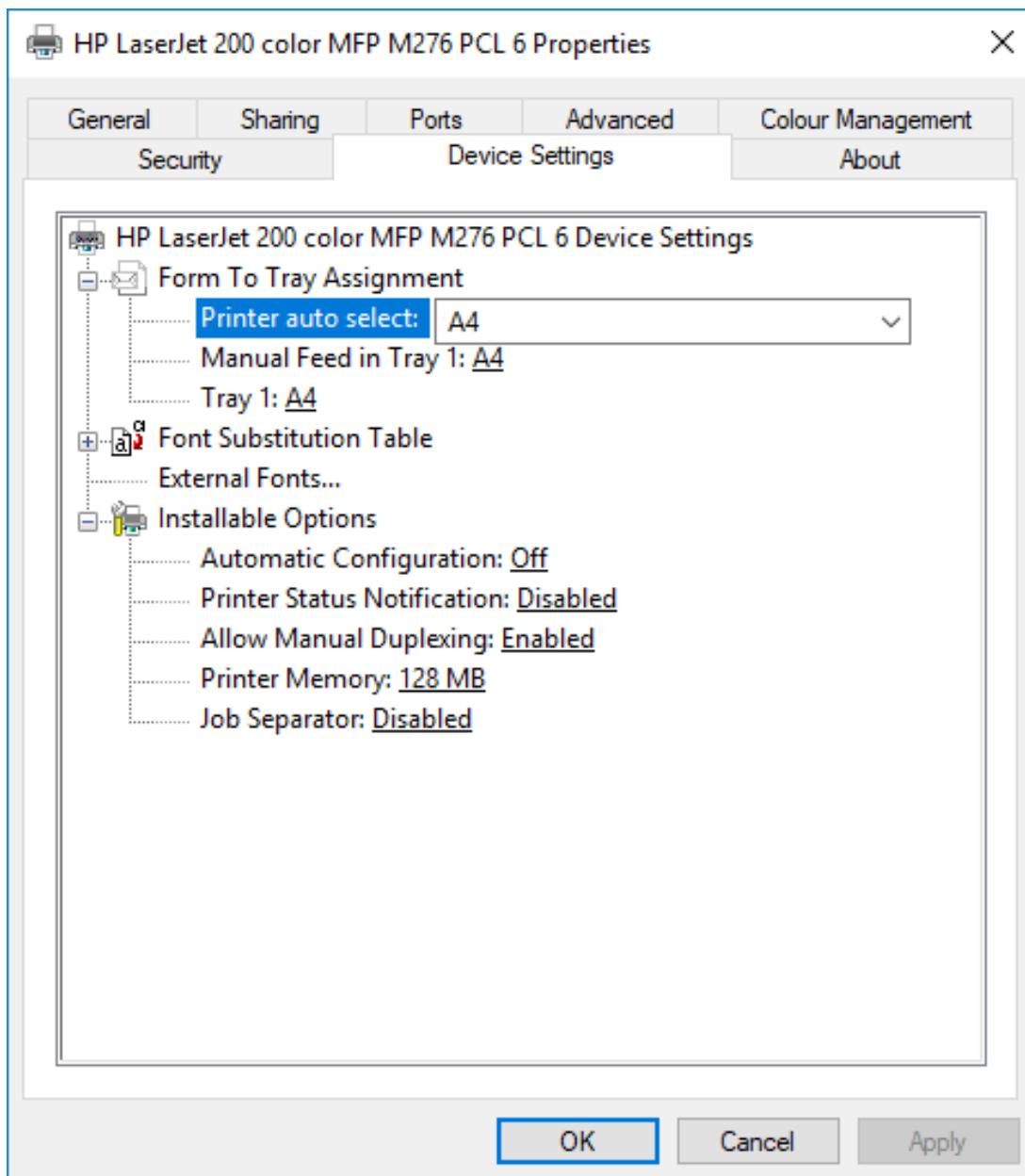
In Windows, there are two main configuration dialogs for a local printer: **Printer Properties** and **Printing Preferences**.

The **Printer Properties** dialog allows you to manage settings for the printer object and hardware, such as updating the driver, changing the port, sharing and permissions, installing a duplex unit or configuring a finisher unit. A duplex unit, which enables automatic double-sided printing, is a printer component that can be installed or configured through this dialog. Additionally, you can set default paper types for different trays.

Printer properties—this HP printer allows defaults and installable options to be configured here

Screenshot courtesy of Microsoft.

The tab displays the following information: HP LaserJet 200 Color M F P M 276 P C L 6 Device Settings. Form to tray Assignment. Printer auto select: A4 Manual Feed in Tray: A4 Tray: A4 Font Substitution Table External Fonts Installable Options Automatic Configuration: Off Printer Status Notification: Disabled Allow Manual Duplexing: Enabled Printer Memory: 128 M B Job Separator: Disabled Ok, Cancel, and Apply buttons are at the bottom.

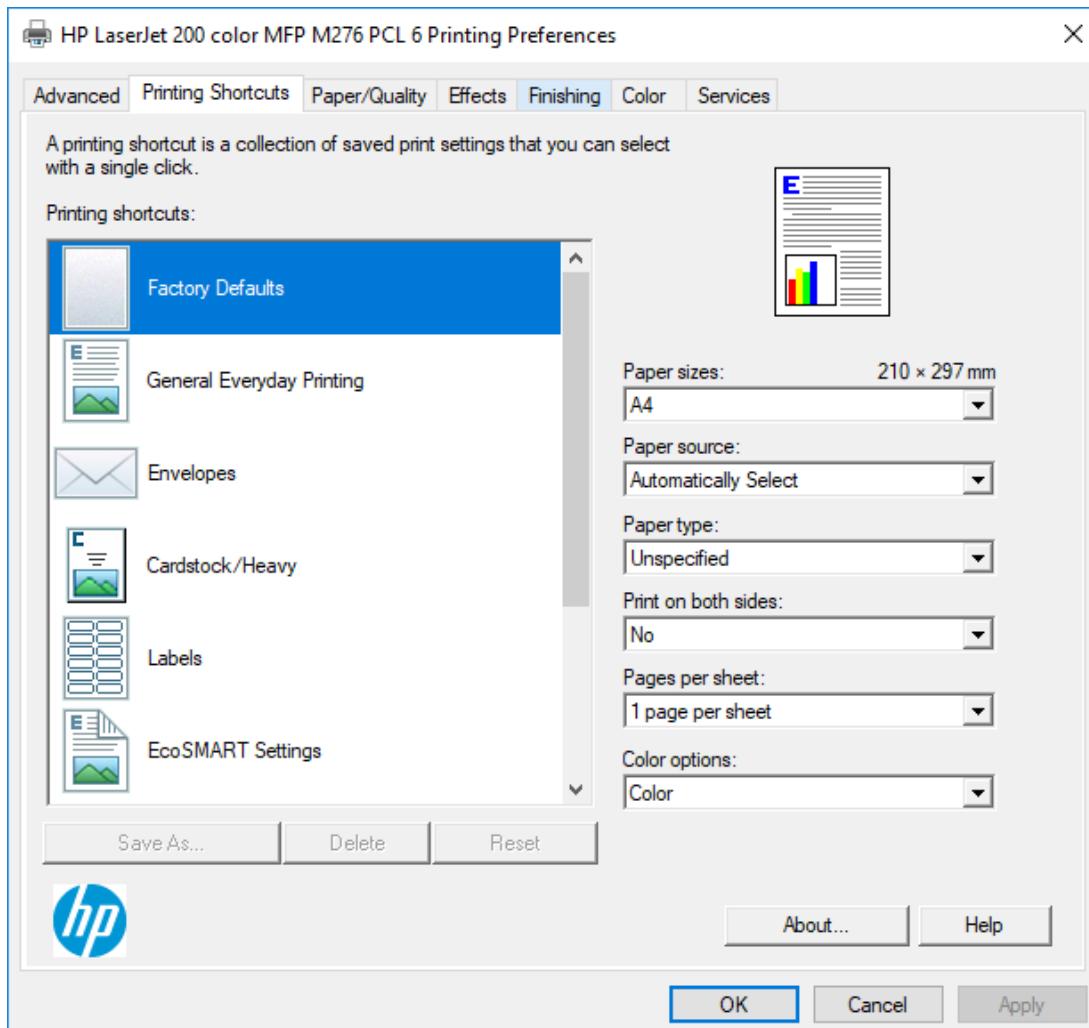


The **About** tab contains information about the driver and the printer vendor and may include links to support and troubleshooting resources.

Printing Preferences

The Printing Preferences dialog sets default print job options, such as paper type, **orientation**, and color or black-and-white printing. These settings can be adjusted per job by selecting the Properties button in the application's Print dialog. Alternatively, the printer may include management software for changing these settings.

Printing Preferences dialog box—this shortcuts tab lets you select from preset option templates



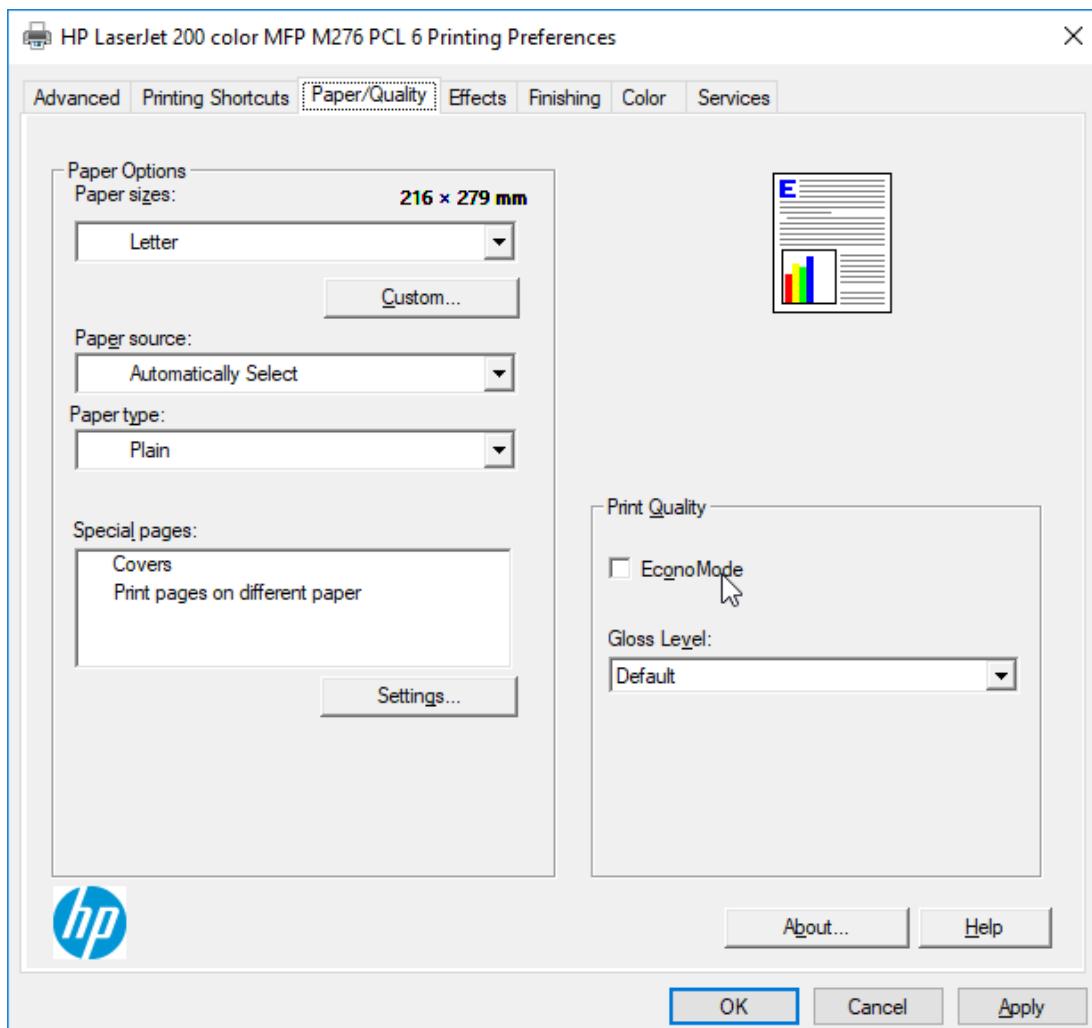
Screenshot courtesy of Microsoft.

The bar at the top has tabs advanced, printing shortcuts, paper and quality, effects, finishing, color, and services. Printing shortcuts is selected. The window includes a sidebar with various printing shortcuts like Factory Defaults, General Everyday Printing, Envelopes, Cardstock or Heavy, Labels, and Eco SMART Settings. The save as, delete, and reset buttons are at the bottom. On the right, options like paper sizes, source, type, print on both side, pages per sheet, and color options. The about and help buttons are at the bottom followed by ok, cancel, and apply buttons below them.

Paper/Quality

The **Paper/Quality** tab lets you select the paper size and type and choose economy or draft mode to save ink or toner. The **Color** tab allows you to switch between color and grayscale printing.

Use the Paper/Quality tab to configure the paper type and whether to use a reduced ink/toner economy mode



Screenshot courtesy of Microsoft.

The bar at the top has tabs advanced, printing shortcuts, paper and quality, effects, finishing, color, and services. Paper and quality is selected.

It includes settings for paper options such as size, source, and type, with additional features for special pages. Print quality adjustments like Econo Mode and gloss level settings are also visible on the right side. The about and help buttons are at the bottom followed by ok, cancel, and apply buttons below them.

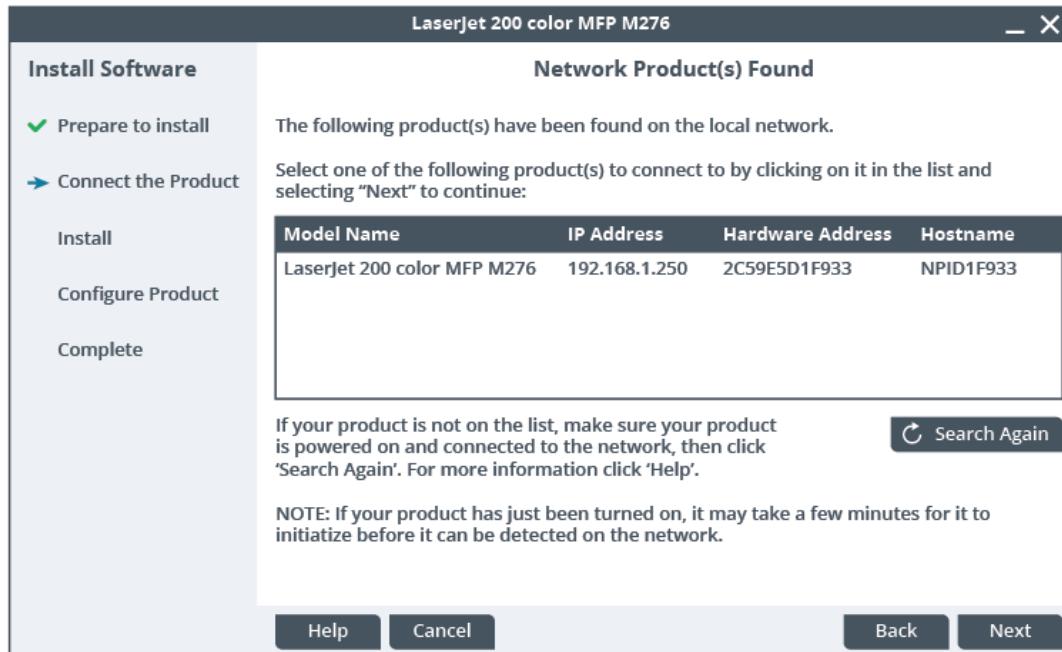
Finishing

The **Finishing** tab lets you select output options such as whether to print on both sides of the paper (duplex), print multiple images per sheet, and/or print in portrait or landscape orientation.

Printer Sharing

Printer interfaces determine how print devices connect to the network, while the **sharing** model describes how multiple clients access the printer. Some printers have integrated print servers, allowing direct network connections without a server computer.

Installing a network printer using a vendor tool



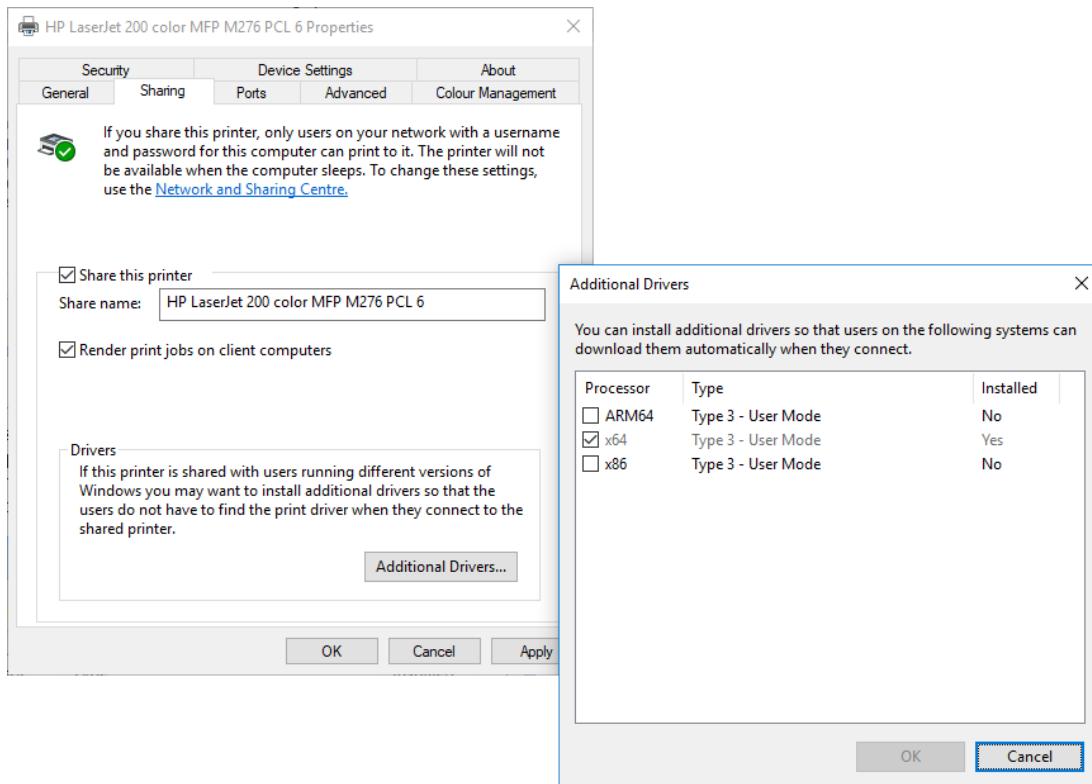
A **public** printer has no access controls, allowing any guest to use it. However, even guest printing today often includes some security measures like network segmentation, user authentication, or guest Wi-Fi networks.

Windows Print Server Configuration

Instead of allowing clients to connect directly to a printer, any computer with an installed printer can share it with other clients. The print server can connect to the printer via USB or over the network, providing more administrative control over client access. Permissions can be set to allow only authenticated users to submit print jobs.

In Windows, configure sharing using the **Sharing** tab in the printer's **Properties** dialog. Drivers for different operating systems can be made available so clients can download and install the appropriate driver when they connect to the print share.

Sharing a printer via the Printer Properties dialog box



Screenshot courtesy of Microsoft.

The Sharing tab is active, allowing users to configure printer sharing options, such as sharing the printer on the network and assigning a share name. A check box to render print jobs on client computers is checked. An additional driver button at the bottom is followed by ok, cancel, and apply buttons below them. A second window titled Additional Drivers displays a list of processors, their types and the status of installed drivers, including x 86 and x 64 types. Buttons for O K and Cancel are available at the bottom of the windows.

For networks with mixed operating systems, ensure printer drivers are available for each supported client. For "Type 3" drivers, add x86 (32-bit) and/or x64 (64-bit) Windows support. "Type 2" drivers require specific versions for each Windows release.

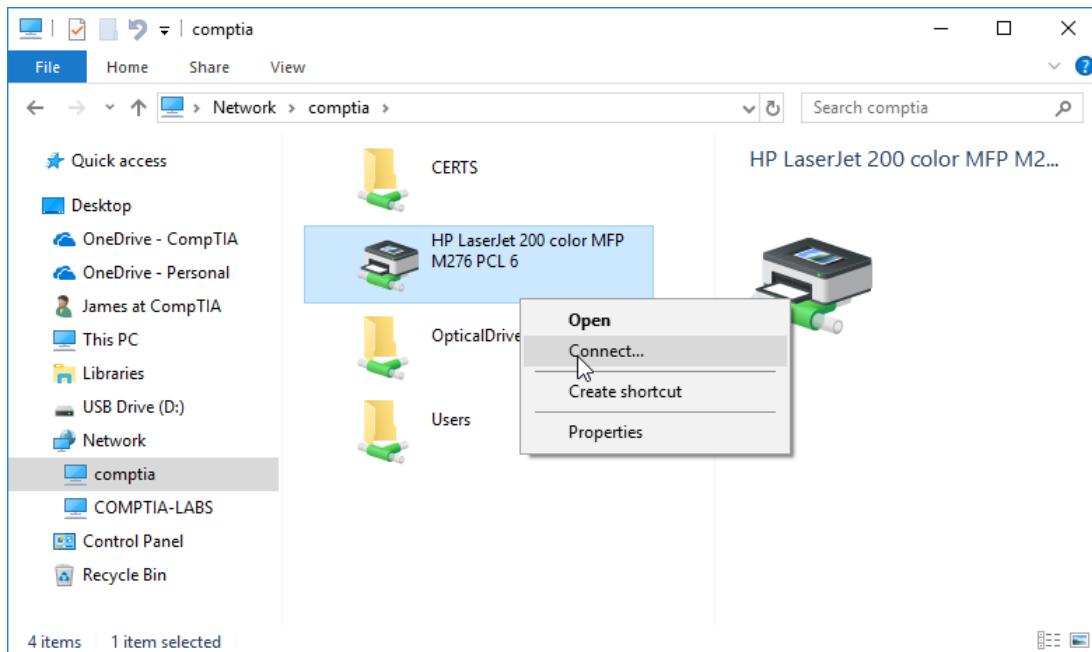


Windows 10 added support for "Type 4" drivers, which aim to create a print class driver framework where a single driver works with multiple devices. If a specific driver is needed, the client can obtain it from Windows Update rather than the print server.

Shared Printer Connections

Ordinary users can connect to a network printer if they have the necessary permissions. To do this, browse network resources using the **Network** object in **File Explorer**, open the server hosting the printer, right-click the desired printer, and select **Connect**.

Connecting to a network printer via File Explorer



Screenshot courtesy of Microsoft.

In the window, multiple items, including folders and a network printer, are visible. The highlighted item is an HP LaserJet 200 color MFP M276 PCL 6 printer. A context menu is open for this printer, showing options such as Open, Connect, Create shortcut, and Properties. The Connect option is selected.

Printer Security

Using printers raises security concerns, including access to print services and the confidentiality of printed output.

User Authentication

To prevent unauthorized use of a network printer, user authentication ensures that only authorized accounts can submit print jobs. In Windows, configure user or group permissions in the Sharing and Security tabs of the printer's Properties dialog.



Note: Windows shares, permissions, and authentication are covered in more detail in the Core 2 course.

Printers may also support direct user authentication. Local authentication stores valid usernames and passwords on the printer, while network authentication communicates with a directory server to verify users.

Secured Print and Badging

Secured print holds a print job on the device until the user authenticates, reducing the risk of confidential information being intercepted from the output tray. Authentication methods include:

- **PIN entry:** The user inputs a password or code via the device control panel.

- **Badging:** The device has a smart card reader, and the user presents their ID badge to release the print job.

Secured print can be set as a default or configured per job. Print jobs may be cached for a limited time and deleted if not printed. The device might need a memory card or storage to cache encrypted print jobs.

Audit Logs

A print share server or print device can **log** each job, creating an **audit** record of documents printed by specific users and devices. This helps track missing documents or unauthorized information release. If the log is generated on the print device, tools like syslog can transmit logs to a centralized server.

Scanner Configuration

Many office printers are multi-function devices (MFDs) that typically combine printing, scanning, copying, and faxing. [Scanners](#) in MFDs create digital files from physical flat objects like documents, receipts, or photos. [Optical character recognition](#) (OCR) software can convert scanned text into editable digital documents.

An MFD that can scan, print, and fax documents

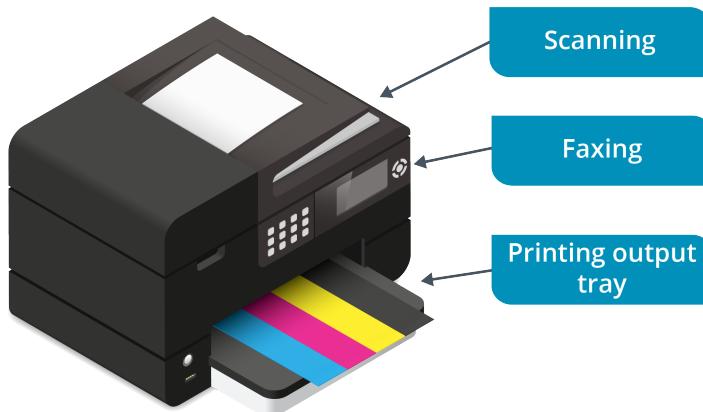


Image © 123RF.com

Scanner Types

Scanners are available in two basic formats:

- **Flatbed Scanner:** Shines a bright light on the object placed on a glass surface. Mirrors reflect the image onto a lens, which either splits it into RGB colors with a prism or focuses it onto imaging sensors with color filters. This creates a bitmap file of the object.
- **Automatic Document Feeder (ADF):** Passes paper over a fixed scan head, efficiently scanning multi-page documents.

Network Scan Services

An MFD or standalone scanner can be configured as a network device, similar to a printer. Network scan services direct scan output to specific media:

- [Scan to email](#): The scan is sent as an email attachment. The MFD must be configured with the IP address of an SMTP server, which typically authenticates the user before sending the email.
- [Server Message Block \(SMB\)](#): The scan is saved to a shared network folder. The MFD must be configured with the path to a file server and shared folder, and users must have write permissions to share.
- [Scan to cloud](#): The scan is uploaded to a cloud storage service like OneDrive or Dropbox. The MFD may offer these options or allow custom configurations via a template. Users authenticate to their cloud accounts through the scan dialogs.

Lesson 10B

Print Device Maintenance

Lesson Overview

The graphic design firm has noticed a decline in print quality and an increase in paper jams across several departments. Your task is to implement a maintenance schedule and perform necessary repairs to restore optimal performance.



Objectives Covered

3.8 Given a scenario, perform appropriate printer maintenance

Learning Outcomes

As you study this lesson, answer the following questions:

- How does a duplexing assembly work, and what are its benefits?
- What steps should be taken when replacing a toner cartridge to ensure proper installation and disposal?
- What components are typically included in a printer maintenance kit, and when should they be replaced?
- What routine maintenance tasks are necessary to keep an inkjet printer in good working condition?
- What are the key maintenance tasks for a direct thermal printer?

Laser Printer Imaging Process

Laser printers are popular for office use due to their affordability, quiet operation, speed, and high-quality output. They are available in both grayscale and color models. The laser printing process involves several stages:

The laser print process

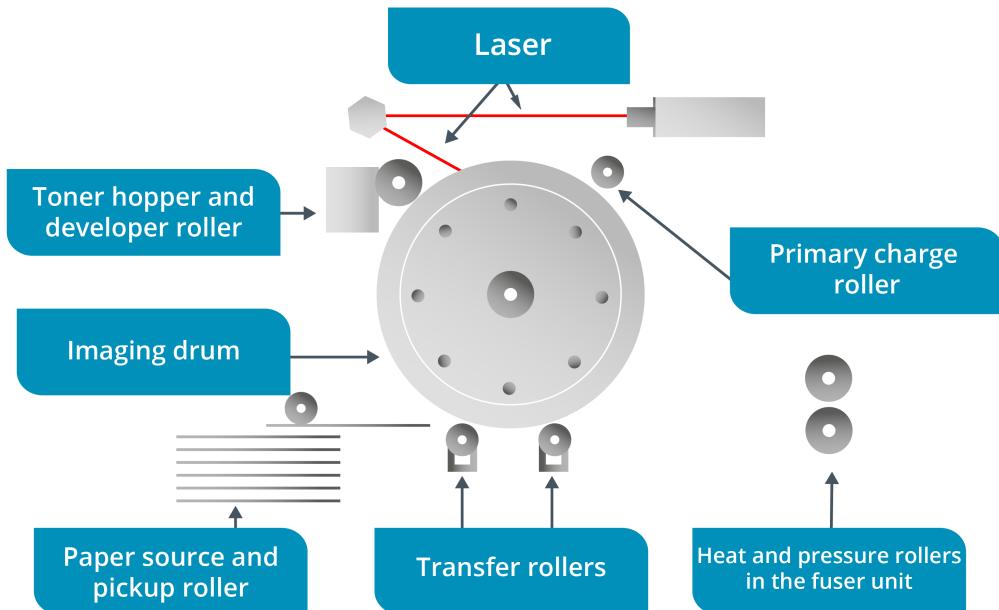


Image © 123RF.com

Key components are laser, toner hopper and developer roller, imaging drum, primary charge roller, paper source and pickup roller, transfer rollers, and heat and pressure rollers in the fuser unit.

Processing Stage: The OS driver encodes the page and sends it to the printer, where it's processed into a bitmap and stored in RAM.

Charging Stage: The primary charge roller (PCR) applies a uniform negative charge to the photosensitive imaging drum.

Exposing Stage: The photosensitive imaging drum loses charge when exposed to light. The laser fires light pulses for each raster dot, neutralizing the PCR charge and forming an electrostatic latent image on the drum.

Developing Stage: Toner is attracted to the neutralized areas on the drum, forming the image to be printed.

Transferring Stage: The paper is guided through the printer, receiving a positive charge to attract toner from the drum.

Pickup, feed, and separation rollers on an HP 5Si laser printer



Image courtesy of CompTIA.

Fusing Stage: The paper passes through the fuser, where heat and pressure bond the toner to the paper.

Cleaning Stage: The drum is cleaned of residual toner and charge, readying it for the next print cycle.

! The entire laser printing cycle occurs in one smooth sequence. However, since the drum's circumference is smaller than a sheet of paper, the early stages must be repeated 2–4 times to process a single page.

Duplex Printing and Paper Output Path: After the paper passes through the fuser, it is flipped and returned to the developer unit to print the second side of a **duplexing assembly** unit is installed. Otherwise, the paper is directed to the selected output bin via the exit rollers.

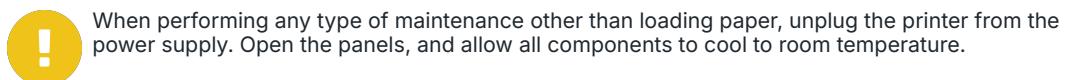
For printers without an automatic duplexer, manual duplexing is often an option. Instructions vary by model, but printers typically provide on-screen prompts for reloading the paper. For example, typically in manual duplex mode, the printer pauses after printing the first side. The user then returns the printed pages to the input tray without changing the orientation to resume printing the second side.

Color Laser Printers: Color laser printers use separate toner cartridges for each CMYK color. They employ different processes to create images: some use four passes to apply each color sequentially, while others combine all colors on a **transfer roller/belt** and print in a single pass.

Laser Printer Maintenance

When performing any type of maintenance other than loading paper, unplug the printer from the power supply. Open the panels, and allow all components to cool to room temperature.

Printers require more maintenance than most IT devices due to their mechanical parts and consumables. They create debris like paper dust and toner spills, necessitating regular cleaning. Under heavy use, consumables such as toner cartridges, fusers, and rollers need frequent replacement. Maintaining a laser printer requires a regular maintenance schedule and proper user training.



When performing any type of maintenance other than loading paper, unplug the printer from the power supply. Open the panels, and allow all components to cool to room temperature.

Loading Paper

When a tray runs out of paper, the printer will notify you. Follow these guidelines when loading new paper:

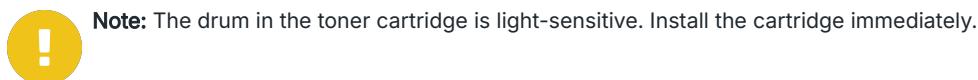
- Use high-quality paper designed for your printer model and the required output type (e.g., documents or photos).
- Position the media guides at the edges of the paper stack. The printer uses these guides to detect the paper size. Different trays may support various types, sizes, and thicknesses of media. Avoid adding unsupported media or overloading the tray.
- Do not use creased, dirty, or damp paper. Store paper in a climate-controlled environment, free from excessive humidity, temperature, or dust.

Replacing the Toner Cartridge

Keep a supply of the correct **toner cartridges** for your printer model. When toner is low, the printer will display a status message. Frugal departments may continue printing until output quality declines. Gently rocking the cartridge from front to back can extend its life. Color laser printers typically have four separate cartridges for different colors.

To replace a toner cartridge:

1. Open the service panel and remove the old cartridge, placing it in a bag to prevent toner spills.
2. Take the new cartridge, remove the packing strips, and gently rock it from front to back to distribute the toner evenly.
3. Insert the new cartridge, close the service panel, turn on the printer, and print a test page.



Note: The drum in the toner cartridge is light-sensitive. Install the cartridge immediately.

Cleaning the Printer

Consult and follow the manufacturer's specific recommendations for **cleaning** and maintenance. The following guidelines generally apply:

- Use a damp cloth to clean exterior surfaces.
- Wipe dust and toner away from the printer interior or exterior with a soft cloth, or use a toner-safe vacuum.



Do not use compressed air to clean a laser printer, as it can disperse toner dust into the air, creating a health hazard. Avoid using a domestic vacuum cleaner, as toner can damage the motor and pass through the dust collection bag.

- If toner is spilled on skin or clothes, wash it off with cold water.
- Use 99% Isopropyl Alcohol (IPA) and non-scratch, lint-free swabs to clean rollers and electronic contacts, taking care not to scratch the rollers.
- Replace the printer's dust and ozone filters regularly, as per the manufacturer's recommendations.

Replacing the Maintenance Kit

A [maintenance kit](#) typically includes replacement feed rollers, a transfer roller, and a fuser unit. The printer will display a "Maintenance Kit Replace" message based on its internal page count. To replace the maintenance kit:

1. Remove the old fuser and rollers.
2. Clean the printer.
3. Install the new fuser and rollers, remove packing strips, and follow the instructions carefully. Dispose of the fuser unit and old rollers through a recycling program to ensure environmental responsibility.

Calibrating a Printer

Calibration determines the appropriate print density or color balance (basically, how much toner to use) for the printer. Most printers perform this automatically. If print output is not as expected, you can manually invoke the calibration routine from the printer's control panel or software driver.

Inkjet Printer Imaging Process

[Inkjet printers](#) are often used for good-quality color output, such as photo printing. They are typically inexpensive to purchase but costly to operate due to expensive ink cartridges and high-grade paper. Compared to laser printers, inkjets are slower and noisier, making them less popular in office environments, except for low-volume, high-quality color printing.

Inkjet Printer Imaging Process

Inkjet printers create high-quality images by spraying tiny ink droplets onto paper, with optimal results on treated paper. There are two main print head types:

1. Thermal Method (HP, Canon, Lexmark): Heats ink to form a bubble that bursts, spraying ink. These are cost-effective but have a shorter lifespan.
2. Piezoelectric Method (Epson): Uses a piezoelectric element to push ink through the nozzle. Both technologies are licensed to other manufacturers, resulting in re-branded printers.

The inkjet printing process.

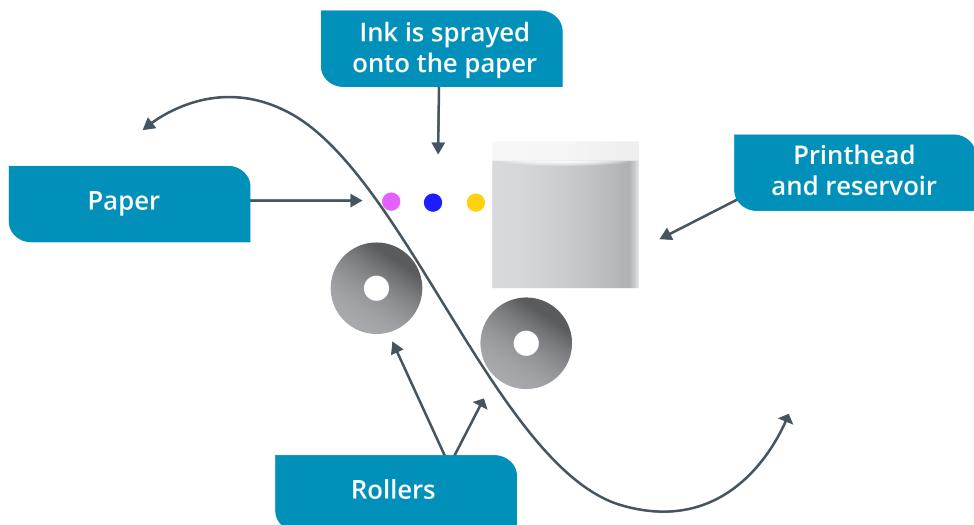


Image © 123RF.com

Carriage System

Inkjet printers build images line by line by moving the print head back and forth over the paper using a **carriage system**. Some printers apply ink only in one direction, while bidirectional models apply ink on both the outward and return passes, increasing speed.

Some printers feature a platen gap adjustment, which controls the distance between the print head and the paper. This can be adjusted manually or automatically, allowing the printer to accommodate thicker media like cardstock or photo paper.

The carriage mechanism in an inkjet printer



Image by Erik Bobeldijk © 123RF.com

Inkjet Printer Maintenance

Maintenance for inkjet printers primarily involves stocking paper and replacing ink cartridges, as they can deplete quickly due to being designed for high-quality graphics and lower page yields than laser printers.

Avoid cleaning the inside of the inkjet printer to prevent damage. Use a soft, damp cloth to clean the exterior.

Paper Handling and Duplex Assembly

Most inkjet printers support a single paper path with one input and output tray, though some feature automatic duplexers and accessory trays. Printers are generally categorized into two types: those that load paper from the top and output at the bottom, and those with both input and output bins at the bottom, using an "up-and-over" path.

1. The paper pickup mechanism is similar to that of a laser printer. A load roller moves the top sheet while a separation roller prevents multiple sheets from entering.
2. A sensor detects the paper once it is sufficiently advanced. The stepper motor then advances the paper as the print head completes each pass until printing is finished.
3. Eject rollers deliver the paper to the duplexing assembly (if installed and duplex printing is selected) or the output bin. Some inkjets with a curved paper path may have a "straight-through" rear panel for bulkier media.

Inkjets typically have smaller paper trays than laser printers, requiring more frequent restocking. While most inkjets can use regular copier/laser printer paper, better results are achieved with

premium, less absorbent paper designed for inkjet use. This type of paper is often intended for single-sided printing, so ensure it is correctly oriented when loading the printer.

Replacing Inkjet Cartridges

Inkjet print heads are often considered consumable items, especially when built into the **ink cartridge**, as with most thermal print heads. However, Epson's piezoelectric print heads are non-removable and designed to last as long as the printer.

Cartridge reservoirs have sensors to detect ink levels. A color printer requires at least four reservoirs for CMYK inks. These can be in a single cartridge, separate cartridges for black and color, or individual cartridges for each ink. Some inkjets also use light cyan and light magenta inks for a wider color gamut.

Ink cartridges

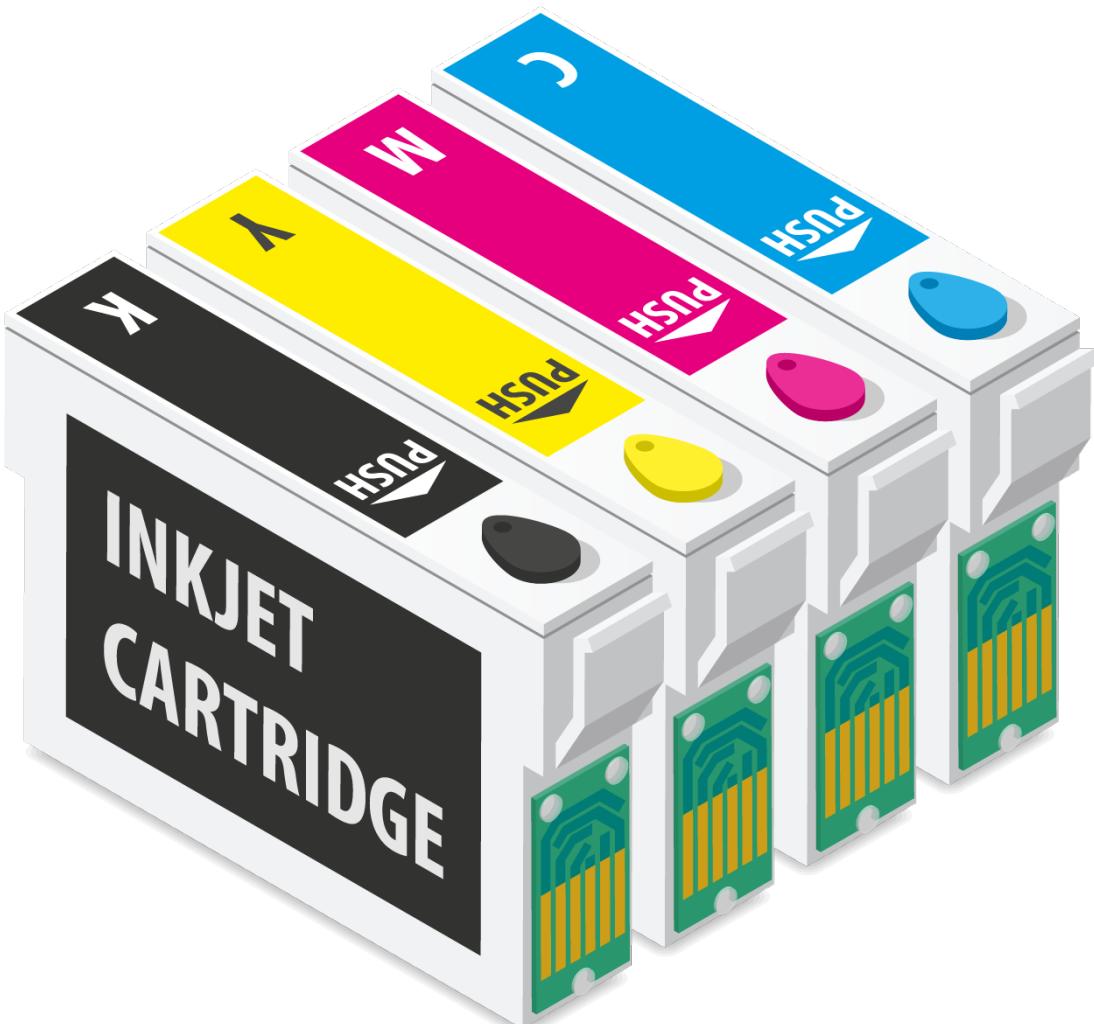


Image © 123RF.com

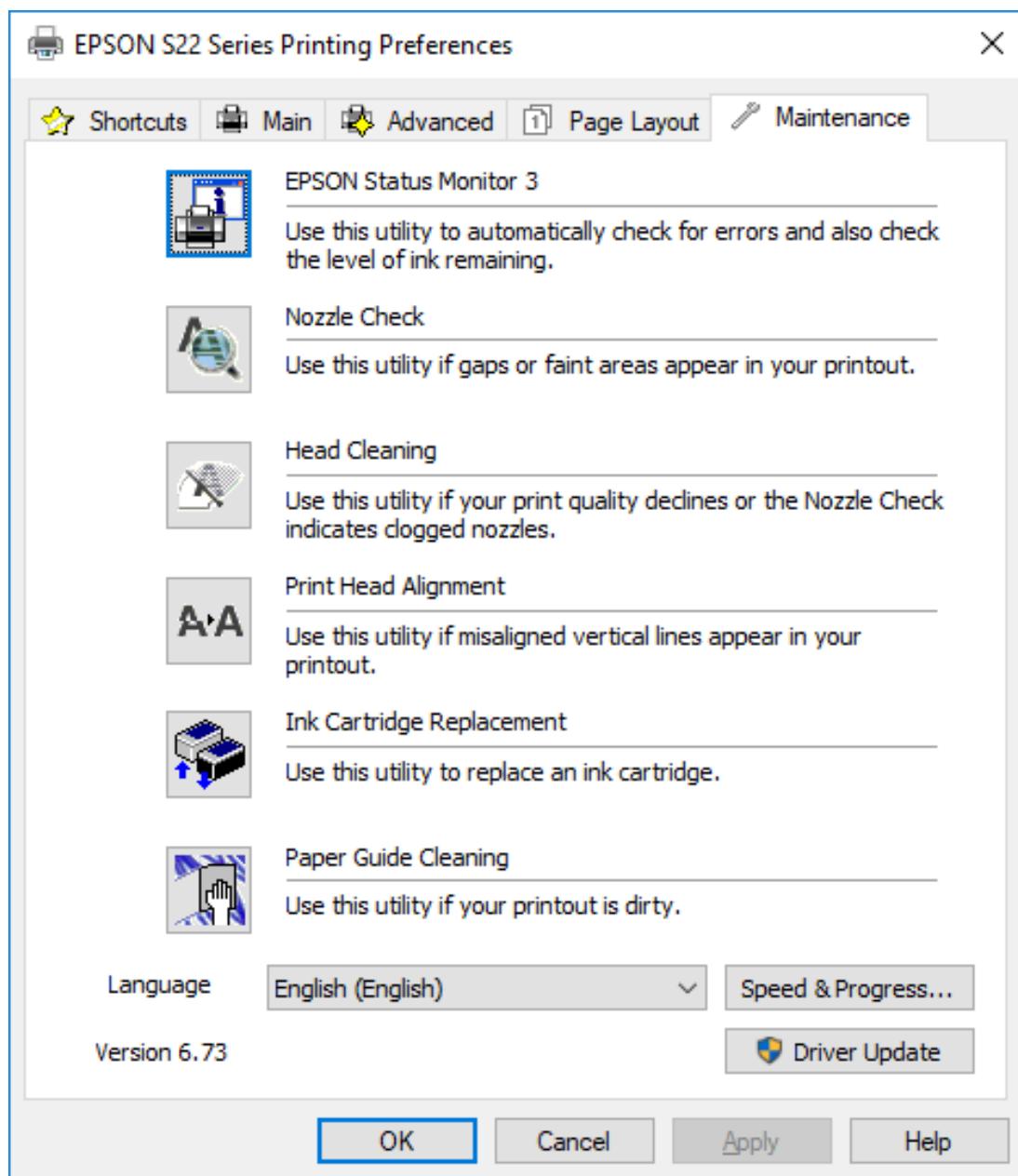
When the driver software detects an empty cartridge, it will prompt you to replace it. Refer to the printer's instruction manual for the correct procedure.

Other Inkjet Maintenance Operations

Three other maintenance operations may be required periodically:

- **Print head alignment:** If output is skewed, use the print head alignment function from the printer's property sheet to **calibrate** it. This is typically done automatically when you replace the ink cartridges.
- **Print head cleaning:** A blocked or dirty nozzle will result in missing lines on the output. Use the printer's cleaning cycle (accessible via the property sheet or control panel) to resolve the issue. If this doesn't work, consider using inkjet cleaning products available on the market.
- **Clearing Paper Jams:** Paper jams can occur when paper is misfed or stuck inside the printer. To clear jams, carefully open the printer's access panel and gently remove the jammed paper, ensuring no torn pieces are left behind. Refer to the printer's manual for specific instructions if needed. Avoid using excessive force to prevent damaging internal components.

Use the Maintenance or Tools tab on an inkjet printer's property sheet to access cleaning routines and calibration utilities



Screenshot courtesy of Microsoft.

It includes options like Epson Status Monitor 3, Nozzle Check, Head Cleaning, Print Head Alignment, Ink Cartridge Replacement, and Paper Guide Cleaning. The language is English. A speed and progress button is on the right followed by Driver Update button below it. The ok, cancel, apply, and help buttons are at the bottom.

Thermal Printer Maintenance

[Thermal printers](#) use a heating element to create images on paper. The most common type you'll support is the direct thermal printer, used for high-volume barcode, label printing, and receipts. These portable or small form factor printers typically support 200-300 dpi resolution, with some models capable of printing in one or two colors. Print speeds are measured in inches per second (IPS).

A direct thermal receipt printer



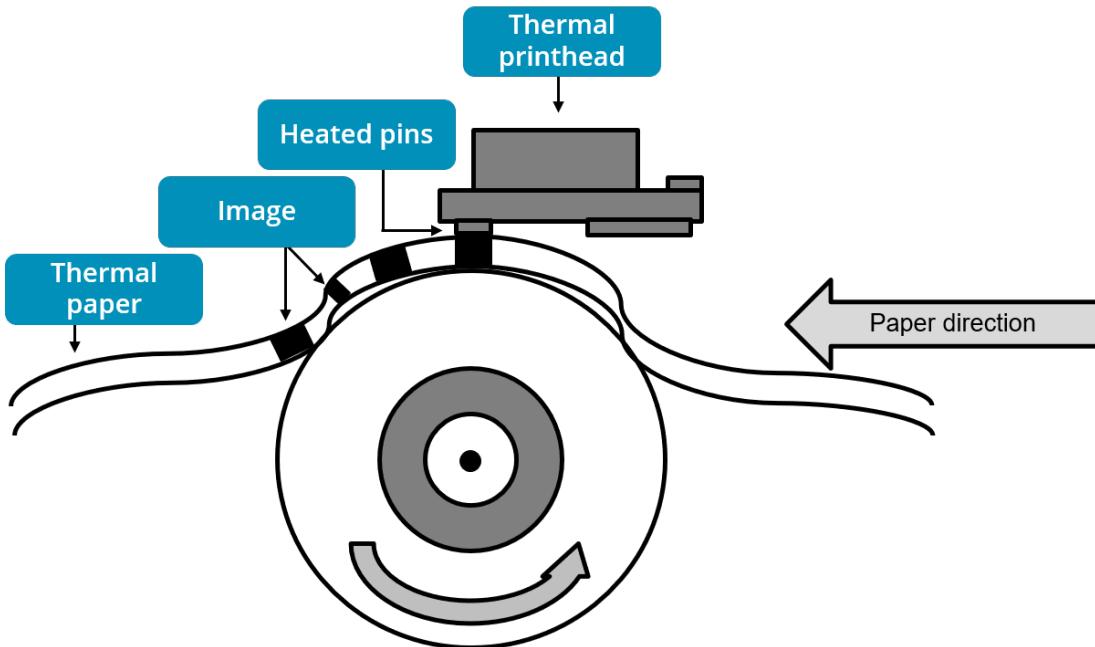
Image © 123RF.com

Direct Thermal Printer Imaging Process

Most direct thermal print devices require special **thermal paper** that contains chemicals designed to react and change color as it is heated by the **heating element** within the printer to create images.

In the feed assembly, a stepper motor turns a rubber-coated roller to friction-feed the paper through the print mechanism. Paper and labels can be in fanfold or roll format.

Direct thermal print process



Direct Thermal Printer Maintenance Tips

When **replacing the paper roll**, use the specific size and type for your thermal printer model. The process is simple: open the printer case, insert the roll with the shiny, **heat-sensitive** side facing outward, and ensure the paper end is held by the print head when closing the case.

Receipts are separated by tearing across serrated teeth, which can create **paper dust and debris**. Use a vacuum or soft brush to remove any buildup.

Label printers may accumulate sticky residue if labels are not loaded correctly and separate from the backing. Ensure users know how to load labels properly and clean any stuck labels. Use a swab with isopropyl alcohol (IPA) to clean the print head and remove sticky residue. Alternatively, use cleaning cards to safely clean the print head.

Impact Printer Maintenance

Impact printers strike an inked ribbon against paper to create marks. A common type is the dot matrix printer, which uses a column of pins in the print head to strike the ribbon. While desktop dot matrix printers are less common for general document printing, they are still used for specialized tasks like printing invoices, pay slips, and multipart forms. **Multipart paper** consists of multiple layers of paper with carbon or carbonless coating between them, allowing the printer to create duplicate or triplicate copies of a document in a single pass. These forms are typically used with continuous, tractor-fed paper.

Example of a dot matrix printer

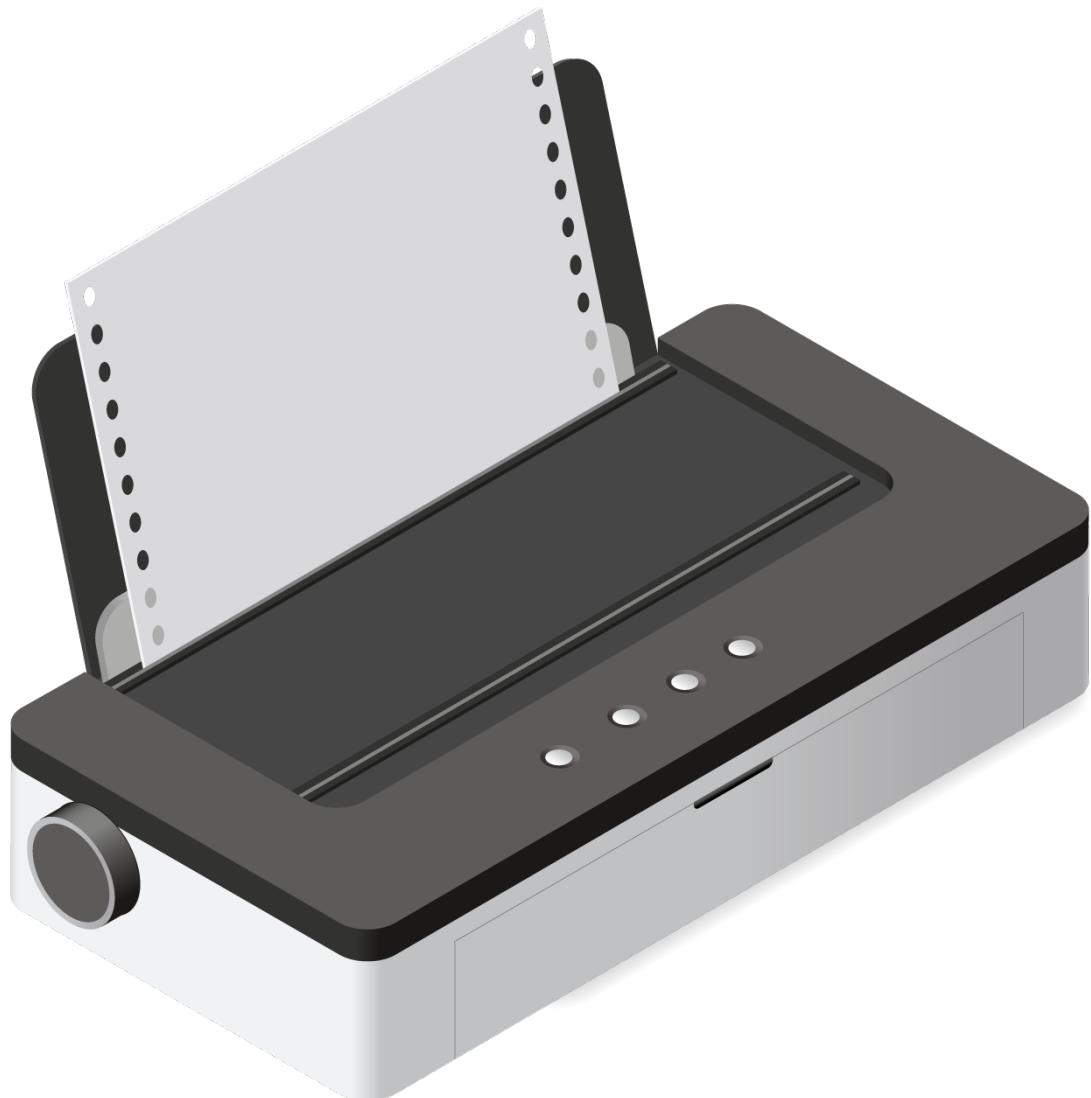


Image © 123RF.com

Impact Printer Paper

Impact printers can use plain, carbon, or tractor-fed paper:

- **Plain Paper:** Held against the moving roller (platen) and pulled through by friction as the platen rotates. Some printers can add a cut sheet feeder to automate page feeding.
- **Carbon Paper (or impact paper):** Used for making multiple copies in one pass. A sheet of carbon paper is placed between each plain paper sheet, transferring the print head's mark to all sheets.
- **Tractor-Fed Paper:** Features removable, perforated side strips with holes that fit over studded rollers at each end of the platen. This setup reduces skewing and slippage, making it ideal for multi-part stationary.

When **loading a tractor-fed impact printer**, ensure the paper holes engage with the sprockets and the paper feeds cleanly. Set the lever to the correct position for friction or tractor feed, depending on the media used.

Impact Printer Components

Impact printers have **replaceable ribbons**. Modern printers use cartridge ribbons that slot over or around the print head carriage, forming a continuous loop moving in one direction. Older models used two-spool ribbons, requiring a sensor and reversing mechanism.

When print quality deteriorates, replace the ribbon holder and contents as an integrated component. Some printers use reusable cartridges.

Follow the manufacturer's instructions to **replace the print head** and be cautious as it may become very hot during use.

Lesson 10C

Troubleshoot Print Devices

Lesson Overview

Several departments at the firm have reported issues with print devices, including connectivity problems, print quality defects, and unrecognized trays. Your task is to troubleshoot and resolve these issues to restore full functionality.



Objectives Covered

5.6 Given a scenario, troubleshoot printer issues

Learning Outcomes

As you study this lesson, answer the following questions:

- What basic checks should be performed when a printer is reported as offline or unavailable?
- What steps should be taken to troubleshoot issues with cloud printing, such as when a printer is not responding to print jobs sent from a cloud service?
- What steps can be taken to resolve paper feed issues in a printer?
- How can you troubleshoot a backed-up print queue in Windows?
- How can you clear a frozen print queue to restore printing functionality?

Printer Connectivity Issues

Printer connectivity issues can occur when the device cannot be located during installation or when the OS reports an installed device as offline or unavailable. Here are steps to troubleshoot and resolve these issues:

1. Basic Checks:

- Ensure the printer is switched on and online. Printers can easily be taken offline accidentally via the control panel.
- Verify all components and cartridges are correctly installed, service panels are closed, and at least one tray is loaded with paper.
- Print a test page using the printer's control panel. If successful, the issue lies with the connection to the computer/network.
- Cycle the power on the printer. If this doesn't resolve the issue, consider performing a factory reset.

- Inspect the USB/Ethernet cable and connectors. Replace with a known good cable to test for cable or connector problems. If possible, try a different connection type (e.g., USB or Ethernet if wireless is not working).

2. Wireless Printer Connectivity:

- Ensure the printer is connected to the correct Wi-Fi network. Wireless printers may attempt to connect to different networks if multiple routers are in range.
- Check for interference from other wireless devices or obstacles like walls.
- Restart the router or access point, as the issue may lie in the network rather than the printer.

3. Firmware and Driver Updates:

- Update printer firmware and drivers, as outdated software can cause connectivity issues, especially after an OS update. Modern printers often offer automatic firmware updates, but this feature may need to be manually enabled.
- Ensure the computer's OS is up-to-date and compatible with the printer's drivers.

4. Cloud Printing:

- If the printer is configured for cloud printing, verify it is correctly registered with the cloud service and that there are no account-related issues preventing access.



Remember to ask: "What has changed?" Determine whether the issue is with something that never worked (indicating an installation error) or something that stopped working (suggesting a configuration change or maintenance issue).

Print Feed Issues

If there is connectivity with the print device but multiple jobs do not print, there is likely to be a mechanical problem with the printer.

Paper Jam Issues

A **paper jam** occurs when a sheet of paper becomes lodged in the paper path. To address a paper jam, gain proper access to the stuck page without using force to avoid further damage. Most sheets can be pulled free, but if a page is stuck in the fuser unit of a laser printer, use the release levers. Forcibly pulling paper through the fuser can damage the rollers and leave debris.

The printer control panel should identify the location of the paper jam

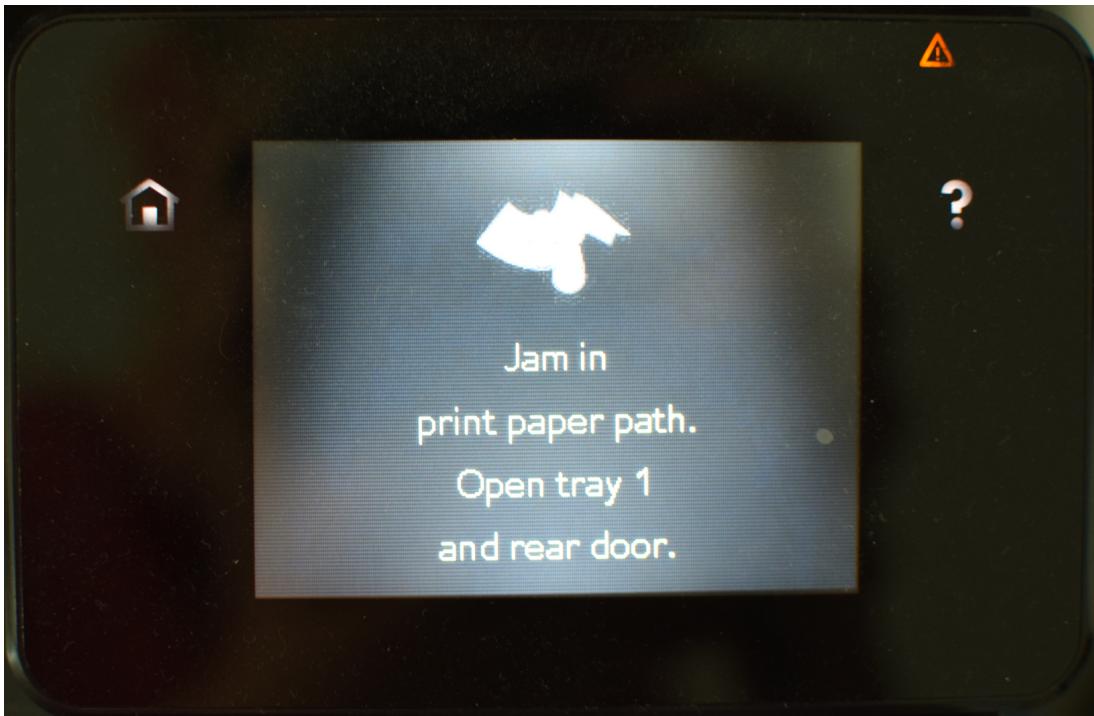


Image courtesy of CompTIA.

Frequent jams often result from unsuitable media (paper or labels), creased or improperly loaded sheets, or faulty rollers. Identify if the jam occurs in the same place each time and perform preventive maintenance, such as cleaning or replacing parts.

If jams occur within the drum assembly but before the image is fused, a faulty static eliminator may be the cause. This part removes the high static charge from the paper as it leaves the transfer unit. If it fails, the paper may stick to the drum or curl entering the fuser unit.

Note: Always check the media and pickup rollers. If they are in good condition and jams persist, further investigation into specific components may be necessary.

In inkjet printers, it is usually easy to see where the paper has jammed. If the sheet won't come out easily, refer to the instruction manual to release any components preventing removal.

Paper Feed Issues

If paper is **not feeding** into the printer or if a **multipage misfeed** occurs (where feed rollers insert two or more sheets instead of one), follow these steps:

- Verify that the **paper size and weight are compatible** with the print tray options and that it is loaded properly with the media guides set correctly.
- Ensure the paper is not creased, damp, or dirty.



Fan the edge of a paper stack with your thumb to separate the sheets before loading the tray, but avoid overdoing it to prevent generating a static charge that holds the sheets together.

- If the media is not the issue, try changing the pickup rollers. In a laser printer, these are part of the maintenance kit.

Grinding Noise Issues

In a laser printer, a **grinding noise** usually indicates a problem with the toner cartridge, fuser, or gears/rollers. Identify the noise source, ensure all components are seated correctly, and check the paper path for jams and debris. If the issue persists, replace the printer cartridge, maintenance kit, or both.

In an inkjet printer, a grinding noise typically points to a fault in the carriage mechanism. Consult the vendor documentation for instructions on re-engaging the clutch mechanism with the gear that moves the cartridge.

Print Quality Issues

If a print job results in smudged, faded, or marked output, the issue is likely due to printer hardware or media faults. Print defects are often specific to the imaging technology used. Always consult the manufacturer's documentation and troubleshooting notes.

Laser Printer Print Defects

Common print defects in laser printers include:

- **Faded or faint prints:** Likely indicates the toner cartridge needs replacing unless a low-density (draft) option was selected.
- **Blank pages:** Usually, an application or driver issue, or the toner cartridge packing seals were not removed. It could also indicate a damaged transfer roller (the image transfer stage fails).
- **White stripes:** Indicates poorly distributed toner (gently shake the cartridge) or a dirty/damaged transfer roller.
- **Black stripes or whole page black:** Suggests a dirty or damaged primary charge roller or a malfunctioning high-voltage power supply. Try a known good toner cartridge.
- **Speckling on output:** Loose toner may be contaminating the paper. Clean the printer interior with an approved toner vacuum.
- **Vertical or horizontal lines:** Repetitive marks often result from dirty feed rollers (note that there are rollers in the toner cartridge and fuser unit too) or a damaged/dirty photosensitive drum.
- **Toner not fused to paper:** Smudging output indicates the fuser needs replacing.
- **Double/echo images:** Indicates the photosensitive drum is not properly cleaned. Try printing different images; if the issue persists, replace the drum/toner cartridge.
- **Incorrect chroma display:** Ensure toner cartridges are installed in the correct slots and have sufficient toner, if prints display incorrect colors (e.g., a magenta tint). Misalignment of the transfer belt or cartridges can cause color casts or shadows. Reseat components, run the calibration utility, and print a test page.
- **Color missing:** Replace the cartridge. If the issue persists, clean the contacts between the printer and cartridge.

Inkjet Print Defects

- **Lines through printouts:** Indicate a dirty print head or blocked ink nozzle. Run a cleaning cycle to fix this.
- **Smearing, wavy, or blurry output:** Likely a media problem. Persistent marks suggest a dirty feed roller.

- **Print head jams:** The printer will display a status message or a flashing LED. Turn the printer off, unplug it, then turn it back on.
- **Inconsistent color output:** Indicates a low ink reservoir or a completely blocked print head for one of the colors.
- **No color printing:** Ensure color printing is selected.

Dot Matrix Print Defects

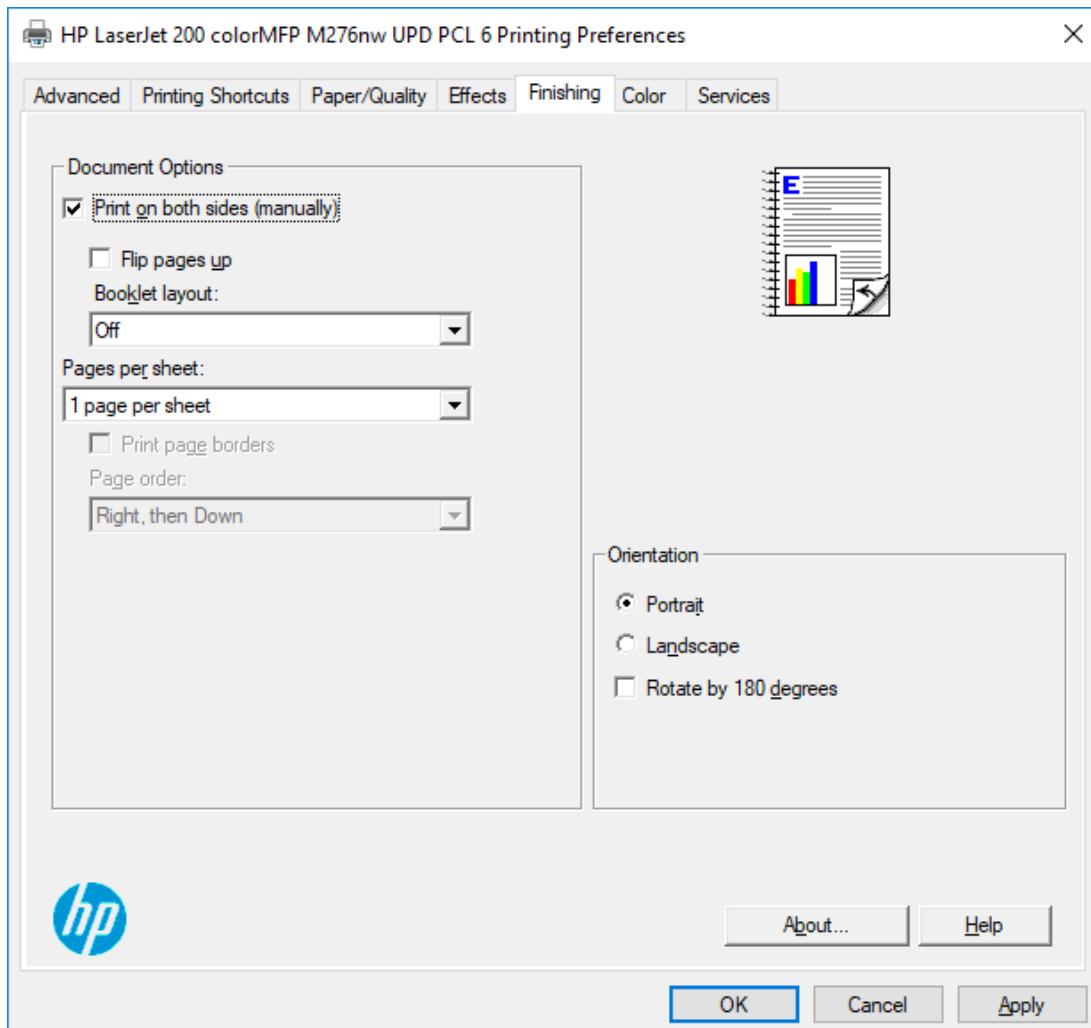
Lines in the output of a dot matrix printer indicate a stuck pin in the print head. The platen position, which adjusts the gap between the paper and the print head to accommodate different paper types, can also affect output. An incorrect gap can cause faint printing if too wide or smudging if too narrow.

Finishing Issues

A **finisher unit** on laser printers and MFDs can perform functions like stapling pages or punching holes for binders. Ensure printer settings are configured to select the finisher as an installed output option. However, several issues can arise with finisher units that require troubleshooting:

- **Incorrect page orientation:** Set the correct paper size and orientation for the print job to ensure proper finishing/binding. Users may find it tricky to paginate and select the correct output options, especially for booklet printing which applies staples to the middle of the sheet. The printing preferences dialog icon shows the binding edge. Test settings on a short document first.

The Finishing tab in Printing Preferences



Screenshot courtesy of Microsoft

The document options include a check box to print on both sides manually, which is ticked. Another checkbox to flip pages up is not ticked. The booklet layout is off. Pages per sheet is listed as 1 page per sheet. The orientation can be portrait, landscape, or rotate by 180 degrees.

Portrait is selected. The about and help button at the bottom is followed by ok, cancel, and apply buttons below them.

- **Hole punch:** Exceeding the maximum number of sheets can cause jams. Send print jobs in batches within the permissible sheet count for the finisher unit. Note that the maximum sheet count may vary based on paper weight.
- **Staple jam:** An excessive number of sheets can cause staple jams, bending and sticking a staple within the punch mechanism. Remove the staple cartridge and release the catch to remove stuck staples.

Print Job Issues

If there is no hardware or media issue, investigate the OS print queue and driver settings.

Print Monitors

In Windows, display and print functions are handled by the Windows Presentation Foundation (WPF) subsystem. A WPF print job is formatted using the Page Description Language (PDL) and spooled in the logical printer's spool folder within %SystemRoot%\System32\Spool\Printers\.

The [print monitor](#) transmits the print job to the printer and provides status information. If a problem occurs, the printer sends a status message back to the print monitor, which displays a desktop notification.

For networked printers, a redirector service on the local computer passes the print job from the local spool file to the spooler on the print server, which then transmits it to the printer.

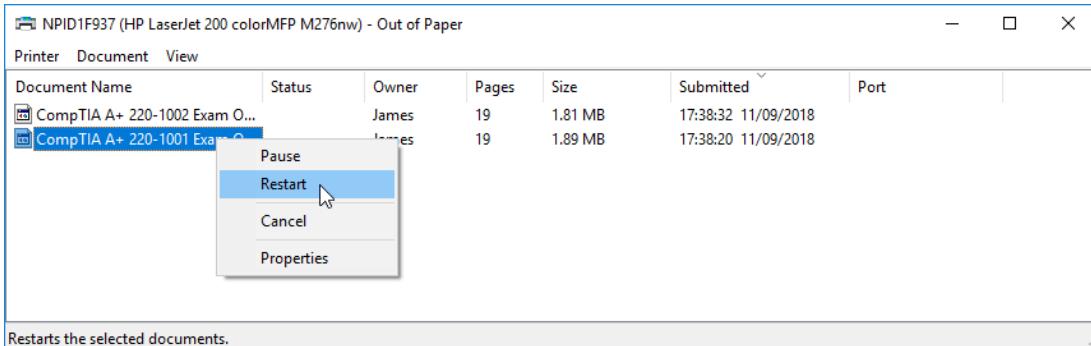
Print Queue and Spooler Troubleshooting

A backed-up print queue indicates multiple pending print jobs. This can occur if the printer is offline, out of paper, low on ink/toner, or due to an error processing a specific job.

In Windows, access the printer through Windows **Settings** and open its print queue. Try restarting the job by right-clicking the document name and selecting **Restart**. If that doesn't work, delete the print job and try printing again. If you cannot delete a job due to a backed-up or stalled queue, stop and restart the Print Spooler service.

 **Note:** The same steps apply to a shared printer. The server's print queue will hold jobs from multiple users.

Use the print queue to manage jobs



Screenshot courtesy of Microsoft.

The printer, document, and view tabs are at the top. The table below includes the document name, status, owner, pages, size, and submitted.

Tray Not Recognized

An unrecognized paper tray can prevent jobs from printing or cause failures.

- Driver issues: Ensure the driver is configured to recognize all installed trays. Check for driver updates from the printer manufacturer's website.
- Physical connection: Ensure the tray is properly seated in the printer. Reseat the tray or ensure it's loaded with the correct paper.
- Printer settings: Verify the correct tray is selected in both the printer settings and print driver settings. In multi-tray systems, jobs may fail if an unrecognized tray is assigned as the default.
- Restart: Power cycle the printer and computer to refresh settings.

Frozen Print Queue

A frozen print queue can prevent new jobs from processing.

- Stop and Restart the Print Spooler Service as mentioned above.
- Clear the Spooler Cache:
 - Stop the Print Spooler service.
 - Navigate to the spool folder (%SystemRoot%\System32\Spool\Printers\) and delete all files inside.
 - Restart the Print Spooler service.
- Check for Corrupt Print Jobs: Sometimes a particular print job may be corrupt and cause the entire queue to freeze. Deleting the problematic job can restore functionality.

Garbled Print Issues

A **garbled print**, where the printer emits many pages with a few characters or blank pages, typically results from a fault in rendering the print job. To troubleshoot, cancel the print job, clear the print queue, power cycle the printer (leaving it off for 30 seconds to clear memory), and try printing again.

Print a test page using the OS. If successful, the issue is likely with a specific application. Try printing a different file from the same application to confirm. If the test page fails, print a test page directly from the printer's control panel. If this works, there is a communication problem between the printer and Windows.

If the problem persists, update the printer driver and ensure the printer uses a supported Page Description Language (PDL) like PCL or PostScript. If characters appear incorrectly or strange characters print, check that the specified fonts are available on the PC and/or printer. The application should indicate if it is substituting fonts.

