

CCNA

Mega Guide

Prepare With Confidence

This PrepLogic Mega Guide was written by certified subject matter experts and published authors to provide you accurate, in-depth exam coverage. All exam objectives are covered in detail, giving you the knowledge and confidence you need to pass your exam.



PrepLogic

Be Prepared. Be Confident. Get Certified.



Jeremy Cioara - Author
Sean Wilkins - Technical Editor

Domain 1 – The Benefits of Cisco Certification

Since the CCENT and CCNA Cisco certifications are typically how most people begin their journey into Cisco networking, let's take a moment to talk about some of the benefits of obtaining this certification.

1. **Credibility** – Cisco certifications are considered by many to be some of the most real-world applicable certification paths in the industry. Obtaining Cisco certification is no easy feat, so when you do become certified, the certification acronyms you place after your name (such as CCENT, CCNA or CCNP) actually means something to other IT professionals!
2. **Marketability** – Organizations are looking for Cisco-certified individuals! Cisco has structured their partner program in such a way that it *requires* organizations to hire certified individuals to move to higher levels in their partner relationship with Cisco. The higher the partner relationship, the bigger discount on Cisco equipment (along with many other benefits). So, an organization can actually *save* money by hiring you. Nice!
3. **Sense of Accomplishment** – When you take a Cisco certification exam, regardless of the pass or fail mark, you will know that the exam is fair. Cisco does not attempt to mislead you in their exam questions or ask questions that are looking for the "Cisco answer" rather than "how it really works." There's nothing like passing the exam and then thinking to yourself, "Wow. There's no way I could have passed that test without *really* knowing what I was doing."

With that in mind, let's move into the material that will help you get there.

Domain 2 – Network Foundations

The Purpose and Pieces of Networking

When you move into the realm of Cisco networking, you have entered a world of building the roads that makes business possible. Most of the time, users and other network administrators take these roads for granted, just like you take them for granted when you drive a car. You simply assume that the roads will be there and that they'll carry you through to your destination. However, a poorly timed construction project (network maintenance) or unscheduled road closure (network outage) will bring the entire infrastructure crumbling down. The goal of a network is to establish communications throughout an organization. Let's take a look at the core building blocks that make this communication possible:

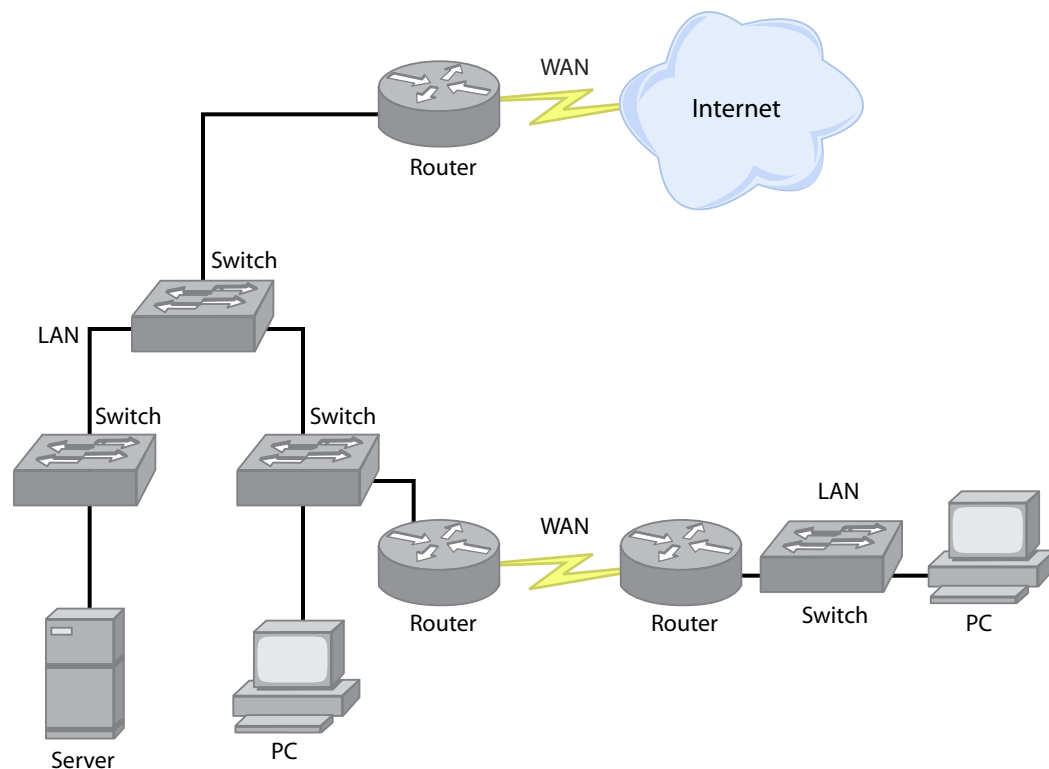
- **Personal Computers (PCs) and Servers** – these devices serve as the endpoints in the network and are responsible for sending and receiving data to and from the network.
- **Network Connections** – you must have a way to attach a device to the network; this building block includes the network interface card (NIC), cabling and connectors.
- **Hubs and Switches** – these devices provide points on which all the end systems of a network can attach.
- **Routers** – routers connect multiple networks together and find the best way to reach each network.

These components can build a network within a local area (LAN) or across a wide area (WAN). In recent years, the lines between a LAN and WAN have begun to blur, since Wireless and Fiber Optic technology can extend the reach of a LAN much further than older technology ever could. Regardless, the following definitions still stand strong:

- **Local Area Network (LAN)** – a computer network covering a small geographic area such as a home, office or group of buildings.
- **Wide Area Network (WAN)** – a computer network covering a large geographic area such as a city, state, nation or globe.

Interpreting a Network Diagram

The following figure shows the placement of each of the core network components:



Types of Network Communication

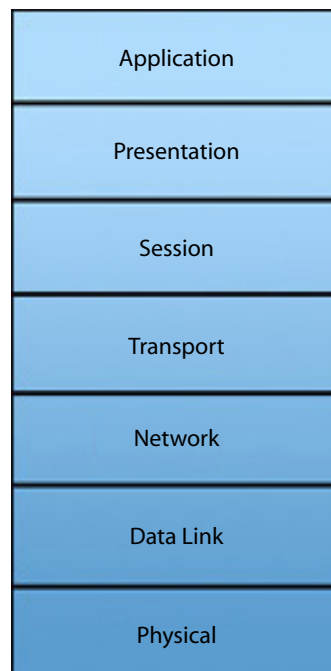
Not that long ago, network communication was solely restricted to data: internal corporate data or external Internet data. Nowadays, the network has evolved to support all types of communication. Organizations have begun to merge their telephone system with the network, creating Voice over IP (VoIP) network traffic. Users have begun to mount video cameras on their computers and in conference rooms to create streaming video traffic. What's more, the network has begun to become so entirely saturated with different application types, network administrators now require a way to divide the different traffic types into application classes, some of which are far more important than others. Because of this, all of Cisco's newer equipment supports Quality of Service (QoS) features allowing you to manage the priorities of data crossing the network. For example, at a major bottleneck in the network (such as the transition from the high-speed LAN to the low-speed WAN), you could set up a system stating that the VoIP traffic is sent first, followed by the streaming video, followed by the business-critical applications and so on.

Using the OSI Model

With all of this network communication occurring, trying to understand the network can become very complex, very quickly. In order to try to make sense of it all, you can use the handy OSI Model. It's a little known fact that the OSI Model was never meant to be just a model that describes network communication. There is also an OSI protocol (technically called the "OSI Networking Suite") that was designed to compete with TCP/IP. We now know the end of the story: TCP/IP wins. However, the OSI Model is still used today as an excellent way to describe and fully understand network communication. You will find that a deep understanding of the OSI Model is critical to your networking success in the Cisco world. This is not one of those models that you learn in order to pass the exam and then never use again. With that foundation, let's begin.

The Layers of the OSI Model

The OSI Model is comprised of 7 layers, each of which describes a specific aspect of network communication:

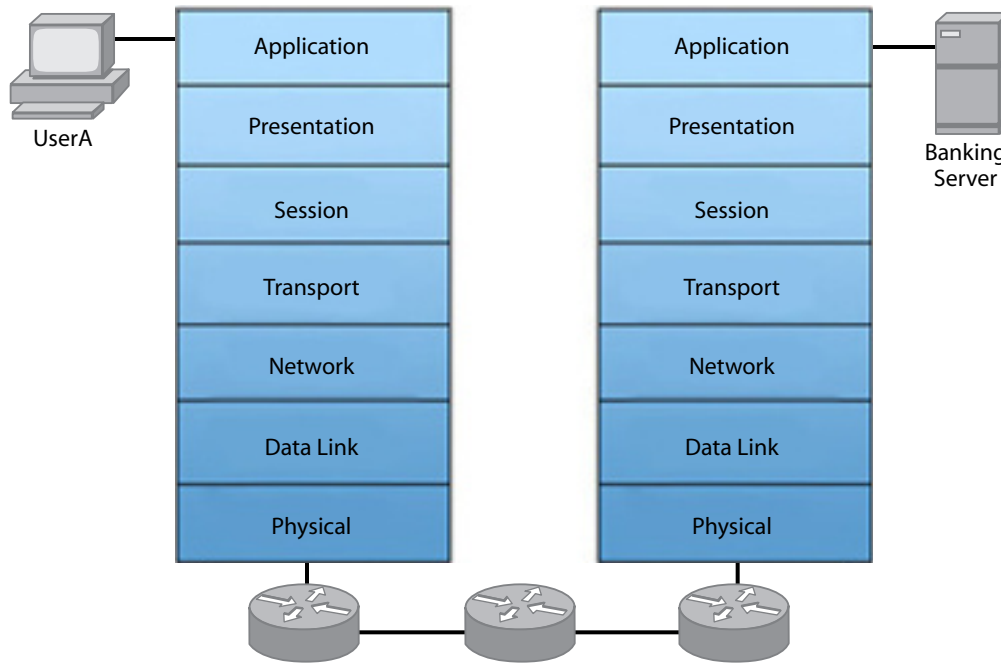


Your first job will be to memorize the layers and their order. There are two handy memorization tips you can use to remember the layers: **All People Seem To Need Data Processing**, where each word contains the first letter of the layers from the top-down, or you can use **Please Do Not Throw Sausage Pizza Away**, where each word contains the first letter of the layers from the bottom-up. I personally love sausage pizza, so I prefer the latter.

Once you've got the layers down, you now need to know what each of them accomplishes. I'll present this to you in two ways. First, we'll look at the cold, hard facts about each layer, and then we'll look at a practical example of how the OSI Model is used in real-world network communication. So, here are the facts:

- **Application Layer:** This layer interfaces directly with the network-aware application, giving it access to network resources. Without this layer, no user application would be able to get access to the network.
- **Presentation Layer:** Encodes the data being sent or received into a generic format that will be understood by both devices. For example, a web browser might receive data in HTML format or a picture in JPG format, which are generic and well understood standards.
- **Session Layer:** Begins, ends, and manages the sessions between devices.
- **Transport Layer:** Handles the reliability of the connection and logical separation of applications. For example, if a computer is surfing the Internet with a web browser and at the same time listening to Internet-radio, this layer ensures the correct data arrives to the correct application. In addition, this layer handles flow-control (ensuring one side does not send information faster than the other can receive) and data integrity (ensuring the data is not corrupt). The most common Transport Layer protocol is TCP.
- **Network Layer:** Provides logical addressing services allowing a device to dictate the source and destination address used for end-to-end communication. This layer is also responsible for routing the packet from its source to its destination. The most common Network layer protocol is IP.
- **Data Link Layer:** Provides physical addressing services allowing a device to dictate the source and destination address used for local network communication. This layer permits communication between devices connected to the same network. This layer is also responsible for error detection.
- **Physical Layer:** Defines the physical standards used for network communication.

Now that we've seen the facts, let's put them together into a practical example of network communication. On the next page is a network diagram representing a task many people do frequently: using online banking to manage finances. In this case, UserA (shown to the left) has used a web browser to issue a request to transfer \$100.00 from his checking account to his savings account. Let's follow this network request step-by-step as it passes through the layers of the OSI Model.



Step 1: The Application Layer (Layer 7)

The user is operating in a web browser. For this example, we'll say he's using Internet Explorer (IE). While the user is interacting with IE, this application doesn't represent function of the OSI Application Layer. The Application Layer is invoked when IE attempts to communicate over the network. The operating system (Microsoft Windows in this case) sees the request and captures it from the application. It then takes the \$100.00 transfer request and passes it down to the Presentation Layer.

Step 2: The Presentation Layer (Layer 6)

The job of the Presentation Layer is to take the user data (the \$100.00 transfer request) and format it into a generic language understandable by industry standard applications. Here's what that means in English: I mentioned above that the user was using Internet Explorer (IE) to perform the transfer request. However, IE is not the only web browser on the market. The user could have been using Mozilla Firefox, Opera, Apple Safari or Netscape Navigator, just to name a few. Likewise, the web server for online banking could have been running on Microsoft's Internet Information Server (IIS), IBM's Websphere or Apache. How do you ensure that the online bank is able to understand the \$100.00 transfer request from the user? What if the user is using Firefox and the web server is running IIS? That's the job of the Presentation Layer. It will format the request in a generic format (such as HTML). It also secures the connection using generic encryption that any standards-compliant web browser is able to support. Once the data has been formatted correctly, it is then passed down to the session layer.

Step 3: The Session Layer (Layer 5)

The Session Layer has a simple function: starting, ending and managing sessions between devices. At any one time, your PC may have numerous network connections going to and from it. Likewise, busy network servers can have hundreds or even thousands of network connections occurring at any one time. The Session Layer is responsible for managing all of these active sessions, as long as the device can keep them all straight. The \$100.00 transfer example we are working through already has an active session with the online bank that started when the user first logged into the online banking website. Once the user closes the web browser (or navigates to a different website), the Session Layer will close down the session.