# **Objectives**

After completing this chapter, you should be able to answer the following questions:

- What are the various roles of help desk and installation technicians?
- What levels of support do help desk technicians provide?
- What are the seven layers of the OSI model, and how is the OSI model used to troubleshoot network issues?
- What common tools and diagnostic procedures do help desk technicians use?
- What onsite procedures are used to help resolve issues?

# **Key Terms**

This chapter uses the following key terms. You can find the definitions in the glossary.

help desk 20	transport layer 25
escalation 21	network layer 25
outsourcing 21	data link layer 25
frequently asked questions (FAQ) 21	physical layer 25
remote desktop sharing 22	upper layers 25
managed services 22	lower layers 25
customer premises equipment (CPE) 22	protocol stack 26
service-level agreement (SLA) 22	bottom-up approach 30
incident management 23	top-down approach 30
trouble ticket 23	divide-and-conquer approach 31
Open Systems Interconnection (OSI) model 24	Domain Name System (DNS) 33
application layer 25	link-local address 35
presentation layer 25	Automatic Private IP Addressing (APIPA) 35
session layer 25	loopback address 36

Providing Internet service is a highly competitive business, and poor service can cause the ISP to lose customers to competing ISPs. Having a good help desk ensures that problems are resolved quickly and to the customer's satisfaction. Whether a technician is employed inside the organization as a help desk technician or as an onsite support technician, that person represents the ISP to the customer.

# **Help Desk Technicians**

The help desk function is critical to maintaining the network and supporting end users and business functions. ISP technicians staff the help desk to resolve user problems and keep the network up and running.

This section describes the job of the help desk network technician and how this person interacts with customers.

# **ISP Help Desk Organization**

Connecting to the local network, as well as the Internet, is critical to most business operations. When people cannot access the Internet or local network resources, their productivity can suffer. Solving network problems is a top priority for businesses and ISPs.

Because ISPs provide the Internet connection for businesses, they also provide support for problems that occur with that connectivity. This support usually includes assistance with customer equipment problems. ISP support typically is provided through the ISP *help desk*.

It is important to distinguish between a help desk technician who works within a business to support that organization's own users and a technician who works for an ISP supporting many users from different companies. The internal technician usually deals with a wider variety of issues, including local PC applications support. The internal help desk usually has more direct face-to-face contact with the end user. The ISP technician may provide some of the same support as the internal help desk. However, this person usually focuses only on the services the customer has purchased from the ISP and the access to the resources the ISP provides.

ISP help desk technicians have the knowledge and experience to fix problems and get users connected. ISP help desk technicians provide solutions to customer problems with the goal of network optimization and customer retention. Whether the problem is connecting to the Internet or receiving e-mail, the ISP help desk is usually the first place a user or business turns to for help.

A good help desk team ensures that problems are resolved quickly and to the customer's satisfaction. A typical conversation between a help desk employee and a customer is shown in Figure 2-1.

### Figure 2-1 Help Desk Technician and Customer Conversation



An ISP usually has three levels of customer support:

- Level 1 is for immediate support handled by junior-level help desk technicians.
- Level 2 handles calls that are escalated to more experienced telephone support.
- Level 3 is for calls that cannot be resolved by phone support and require a visit by an onsite technician.

In addition to ISPs, many other types of medium-to-large businesses employ help desk or customer support teams within the company. The titles assigned to the technicians may vary from those described here, but the three-level hierarchy is the most common structure.

The process of raising a problem from one level to the next if the previous level cannot solve it is called *escalation*. Figure 2-2 shows the process of escalating a help desk call. Depending on the size of the organization, the help desk can consist of one person who performs all three levels of support, or it can be a comprehensive call center with elaborate call routing facilities and escalation rules. Some ISPs and businesses contract out their help desk functions to a third-party call center company, which provides the services of Level 1 and Level 2 technicians. This is called *outsourcing*.

#### Figure 2-2 Levels of Customer Support Escalation



## **Roles of ISP Technicians**

When a user initially contacts the help desk to resolve an issue, the call or message is usually directed to a Level 1 support technician. Level 1 support is usually an entry-level position that provides junior technicians with valuable experience. The duties and responsibilities of the Level 1 technician include the following:

- Diagnose basic network connectivity issues.
- Diagnose and document the symptoms of hardware, software, and system problems.
- Resolve and document any basic user issues.
- Answer frequently asked questions (FAQ).

- Help customers complete online order forms to attain various systems, services, hardware, software, reports, and entitlements.
- Escalate any issues that cannot be resolved to the next level.

The majority of customer issues can be resolved by the Level 1 support technician. Level 2 support typically has fewer agents available, but they have a higher skill level. The duties and responsibilities of the Level 2 technician are similar to that of the Level 1 technician. These agents are expected to solve problems that are more challenging and that require more problem-solving abilities than normal end-user issues.

The duties and responsibilities of the Level 2 technician include the following:

- Diagnose and solve more difficult network problems.
- Use diagnostic tools and *remote desktop sharing* tools to identify and fix problems.
- Identify when an onsite technician must be dispatched to perform repairs.

Some smaller ISPs and businesses may combine Level 1 and Level 2 support, requiring that all technicians have the higher technical capabilities.

Many larger service providers have expanded their businesses to include *managed services* or onsite support of a customer network. Organizations that provide managed services sometimes are referred to as managed service providers (MSP). Managed services can be provided by ISPs, telecommunications service providers, or other types of computer and network support organizations. When an ISP provides managed services, it often requires technicians to visit customer sites for the purpose of installation and support. This represents Level 3 support.

The duties and responsibilities of the Level 3 onsite installation and support technician include the following:

- Diagnose and resolve problems that have been escalated by Level 1 and Level 2 technicians.
- Survey network conditions for analysis by a senior network technician for more complex problems.
- Install and configure new equipment, including *customer premises equipment (CPE)* upgrades, when necessary.

Level 3 support is usually provided in accordance with a *service-level agreement (SLA)*. An SLA is like an insurance policy, because it provides coverage, or service, in the case of a computer or network problem.



#### Interactive Activity 2-1: Identify Technician Support Level Responsibilities (2.1.2)

In this interactive activity, you identify the responsibilities of each level of network technician. Use file d2ia-212 on the CD-ROM that accompanies this book to perform this interactive activity.

# Interacting with Customers

Help desk technicians may be required to provide phone support, e-mail support, web-based support, online chat support, and possibly onsite support. They are often the first point of contact for frustrated and anxious customers. Until the problem is solved, help desk technicians may continue to get calls and correspondence asking for status updates and time estimates to resolve the issue.

The help desk technician must be able to stay focused in an environment with frequent interruptions and perform multiple tasks efficiently and accurately. It can be difficult to consistently maintain a positive attitude and provide a high level of service. The help desk technician must have excellent interpersonal and communication skills, both oral and written. The technician must also be able to work independently as well as part of a team.

It is also important for the help desk technician to be able to handle customer issues with speed, efficiency, and professionalism.

Basic *incident management* procedures should be followed every time a help desk technician receives a call and begins troubleshooting issues. Incident management includes techniques such as opening a *trouble ticket* and following a problem-solving strategy. Problem-solving techniques include using troubleshooting flowcharts, addressing questions in a template format, and maintaining proper ticket escalation procedures.

The help desk technician uses a help desk script to gather information and cover the important facts about a customer incident.

In addition to technical ability, help desk technicians need other skills to be successful. Customer service and interpersonal skills are important when handling difficult clients and incidents. Help desk technicians must greet customers pleasantly and maintain a professional and courteous demeanor, as shown in Figure 2-3, throughout the call until the customer request is resolved or escalated. Technicians must also know how to relieve customer stress and respond to abusive customers. Here are some of the skills that are consistently used in successful help desk communication:

- Preparing with adequate training
- Offering a courteous greeting
- Opening a trouble ticket
- Listening to the customer
- Adapting to the customer's temperament
- Correctly diagnosing a simple problem
- Logging the call

#### Figure 2-3 Technician Following the Customer Service Policy

Be prepared to answer the customer call in accordance with the company customer service policies. Answer the call in a courteous manner and immediately identify yourself and the company.



Opening trouble tickets and logging information on the tickets are critical to help desk operation. When many calls relate to a single problem or symptom, it is helpful to have information on how the problem was resolved in the past. It is also important to relay to the customer what is being done to solve the problem. Good information on open trouble tickets helps communicate accurate status, to both the customer and other ISP personnel.

Although many issues can be handled remotely, some problems require an onsite visit to the customer premises to install and troubleshoot equipment. When a technician goes on site, it is important to represent the organization in a professional manner. A professional knows how to make the customer feel at ease and confident in the technician's skills.

On the first visit to a customer location, it is important for the technician to make a good first impression. Personal grooming and how the technician is dressed are the first things the customer notices. If the technician makes a bad first impression, it can be difficult to change that impression and gain the confidence of the customer. Many employers provide a uniform or have a dress code for their onsite technicians.

The language and attitude of the technician also reflect on the organization that the technician represents. A customer might be anxious or concerned about how the new equipment will operate. When speaking with a customer, the technician should be polite and respectful and answer all customer questions. If the technician does not know an answer to a customer question, or if additional information is required, the technician should write down the customer inquiry and follow up on it as soon as possible.



#### Interactive Activity 2-2: Determine the Customer Support Process (2.1.3)

In this interactive activity, you examine statements and decide to which part of the customer support process they belong. Use file d2ia-213 on the CD-ROM that accompanies this book to perform this interactive activity.

# **OSI Model**

The OSI model can be very helpful in troubleshooting network problems. An understanding of the OSI model layers and their functions provides a good foundation for categorizing and analyzing network issues.

This section describes the layers of the OSI model and some troubleshooting techniques that make use of it, including top-down, bottom-up, and divide-and-conquer. It also describes the protocols, the types of problems, and tools available for troubleshooting at each layer of the OSI model.

# **Using the OSI Model**

When a network connectivity problem is reported to the help desk, many methods are available to diagnose the problem. One common method is to troubleshoot the problem using a layered approach. Using a layered approach requires that the network technician be familiar with the various functions that occur as messages are created, delivered, and interpreted by the network devices and hosts on the network.

The process of moving data across a network is highly structured. It is best visualized using the seven layers of the *Open Systems Interconnection (OSI) model*, commonly called the OSI model. The OSI model breaks network communications into multiple processes. Each process is a small part of the larger task.

For example, in a vehicle manufacturing plant, one person does not assemble the entire vehicle. The vehicle moves from station to station, or levels, where specialized teams add various components. Each station adds its assigned components and then passes the vehicle to the next station. The complex task of assembling a vehicle is made easier by breaking it into more manageable and logical tasks. When a problem occurs in the manufacturing process, it is possible to isolate the problem to the specific task where the defect was introduced and then fix it.

In a similar manner, the OSI model can be used as a reference when troubleshooting to identify and resolve network problems. All aspects of network communication between two hosts can be described and classified using the OSI model. The basic functions of each OSI layer are as follows:

- Layer 7: *Application layer* 
  - Defines interfaces between application software and network communication functions.
  - Provides standardized services such as file transfer between systems.
- Layer 6: *Presentation layer* 
  - Standardizes user data formats for use between different types of systems.
  - Encodes and decodes user data. Encrypts and decrypts data. Compresses and decompresses data.
- Layer 5: Session layer
  - Manages user sessions and dialogues.
  - Maintains logical links between systems.
- Layer 4: Transport layer
  - Manages end-to-end message delivery over the network.
  - Can provide reliable and sequential packet delivery through error recovery and flow control mechanisms.
- Layer 3: Network layer
  - Defines logical host addressing.
  - Routes packets between networks based on network Layer 3 device addresses.
- Layer 2: *Data link layer* 
  - Defines procedures and frame formats for operating the communication links.
  - Detects and compensates for frame transmit errors.
- Layer 1: *Physical layer* 
  - Defines physical means of sending data over network devices.
  - Interfaces between the network medium (physical cables and wireless) and devices.
  - Defines optical, electrical, and mechanical characteristics of both wired and wireless media.
  - Includes all forms of electromagnetic transmission such as light, electricity, infrared, and radio waves.

The seven layers of the OSI model can be divided into two groups: *upper layers* and *lower layers*.

The upper layer is any layer above the transport layer. The upper layers of the OSI model deal with application functionality and generally are implemented only in software. The highest layer, the application layer, is closest to the end user.

The lower layers of the OSI model handle data transport functions. The physical and data link layers are implemented in both hardware and software. The physical layer is closest to the physical network medium, or network cabling. The physical layer actually places information on the medium.

End stations, such as clients and servers, usually work with all seven layers. Each host runs a network *protocol stack* that it uses to send and receive messages, as shown in Figure 2-4. Networking devices are concerned with only the lower layers. Hubs operate at Layer 1; LAN switches at Layers 1 and 2; routers at Layers 1, 2, and 3; and firewalls at Layers 1, 2, 3, and 4. Figure 2-5 shows the seven layers of the OSI model and identifies some of the more important protocols, technologies and terminology associated with each layer.



Figure 2-4 Layers of the OSI Model Enable Communication Between Networked Hosts

Figure 2-5 OSI Model Layer Chart

Group	No.	Layer Name	Common Protocols and Technologies	Common Network Components Associated with This Layer
	7	Application	DNS, NFS, DHCP, SNMP, FTP, TFTP, SMTP, POP3, IMAP, HTTP, Telnet	Network-Aware Applications, E-mail, Web Browsers and Servers, File Transfer, Name Resolution
Upper Layers	6	Presentation	SSL, Shells and Redirectors, MIME	
5	5	Session	NetBIOS, Application Program Interfaces, Remote Procedure Calls	
	4	Transport	TCP and UDP	Video and Voice Streaming Mechanisms, Firewall Filtering Lists
	3	Network	IP, IPv6, IP NAT	IP Addressing, Routing
Lower Layers	2	Data Link	Ethernet Family, WLAN, Wi-Fi, ATM, PPP	Network Interface Cards and Drivers, Network Switching, WAN Connectivity
	1	Physical	Electrical Signaling, Light Wave Patterns, Radio Wave Patterns	Physical Medium (Copper Twisted Pair, Fiber-Optic Cable, Wireless Transmitters), Hubs and Repeaters

# **OSI Model Protocols and Technologies**

When using the OSI model as a framework for troubleshooting, it is important to understand which functions are performed at each layer. You also need to understand what network information is available to the devices or software programs performing these functions. For example, many processes must occur for e-mail to successfully travel from the client to the server. The OSI model breaks the common task of sending and receiving e-mail into separate and distinct steps:

- **Step 1.** Upper layers create the data.
- Step 2. Layer 4 packages the data for end-to-end transport.
- **Step 3.** Layer 3 adds the network IP address information.
- **Step 4.** Layer 2 adds the data link layer header and trailer.
- Step 5. Layer 1 converts the data into bits for transmission.

## Step 1: Upper Layers Create the Data

When a user creates an e-mail message, the alphanumeric characters entered are converted into digital bits within the computer's RAM. When the message is sent, the information in the message is converted into data that can travel across the network. Upper Layers 7, 6, and 5 are responsible for ensuring that the message is formatted in a way that can be understood by the application running on the destination host. This process is called encoding. The upper layers then send the encoded messages to the lower layers for transport across the network. Figure 2-6 shows some of the functions that the upper layers can perform. Transporting the e-mail to the correct server relies on the configuration information provided by the user. Problems that occur at the application layer are often related to errors in the configuration of the user software programs.





## Step 2: Layer 4 Packages the Data for End-to-End Transport

The data that comprises the e-mail message is packaged for network transport at Layer 4. Layer 4 breaks the message into smaller segments. A header is placed on each segment, indicating the TCP or UDP port number that corresponds to the correct destination application. Examples of application layer destination port numbers include port 80 for HTTP and port 21 for FTP session control. When

e-mail is sent, the destination application port is 25, which corresponds to Simple Mail Transport Protocol (SMTP). Functions in the transport layer indicate the type of delivery service. E-mail uses TCP segments, so the destination e-mail server acknowledges packet delivery. Layer 4 functions are implemented in software that runs on the source and destination hosts. Firewalls often use the TCP and UDP port numbers to filter traffic. Therefore, problems that occur at Layer 4 can be caused by improperly configured firewall filter lists. The process of adding a transport header to each user data segment is called *encapsulation*. As the user data moves down through the protocol stack, each layer encapsulates the next, until the bits are transmitted onto the medium.

## Step 3: Layer 3 Adds the Network IP Address Information

The segments of e-mail data received from the transport layer are put into packets. Each packet contains a header with the source and destination logical IP addresses. Routers use the destination address to direct the packets across the network along the appropriate path. Incorrectly configured IP address information on the source or destination hosts can cause Layer 3 problems. Because routers also use IP address information, router configuration errors can also cause problems at this layer.

## Step 4: Layer 2 Adds the Data Link Layer Header and Trailer

Each network device in the path from the source to the destination, including the sending host, encapsulates the packet into a frame. The frame header contains the physical or hardware address of the next directly connected network device on the link. Each device in the chosen network path requires framing for it to connect to the next device. In addition to the header, a trailer is added to the end of the packet to complete the frame. The trailer contains a checksum to help ensure that the frame content received by a device is the same as that which was sent by the previous device in the series.

As data travels through a network, it may pass through many different types of devices. The frame type and physical addressing can change at each device, but the internal contents of the frame do not change. For example, a package that is sent to someone may go from a car to a truck to an airplane to another truck before it reaches the end user. The type of carrier and vehicle identification changes at each step, but the contents of the package being carried do not. Switches and network interface cards (NIC) use the information in the frame to deliver the message to the correct destination device. Incorrect NIC drivers, interface cards themselves, or hardware problems with switches can cause Layer 2 issues.

## Step 5: Layer 1 Converts the Data into Bits for Transmission

The frame is converted into a pattern of 1s and 0s (bits) for transmission on the medium. A clocking or timing function enables the devices to distinguish these bits as they travel across the medium. The medium can change along the path between the source and destination. For example, the e-mail message can originate on an Ethernet LAN, cross a fiber-optic campus backbone, and cross a serial WAN link until it reaches its destination on another remote Ethernet LAN. Layer 1 problems can be caused by loose or incorrect cables, malfunctioning interface cards, or electrical interference.

Figure 2-7 shows a completed Ethernet frame ready for transmission over the network to the e-mail server. It takes many of these frames to carry the entire message. A portion of the user e-mail data is encapsulated in a TCP segment. The TCP segment is encapsulated in an IP packet, and the IP packet is encapsulated in the Ethernet frame. On its way to the e-mail server, this Ethernet frame may pass through multiple switches and one or more routers. As the frame passes through each router, the exiting frame header is stripped and replaced with another header. This could be an Ethernet header or a WAN link encapsulation header, depending on the link type to which it is being forwarded.



#### Figure 2-7 Encapsulated Components Within an Ethernet Frame

At the receiving e-mail server, the process described in Steps 1 through 5 is reversed, with the message traveling back up the layers to the appropriate application. The Ethernet frame header is stripped, followed by the IP header and then the TCP header. After all TCP segments have been received and reassembled on the e-mail server, the e-mail message is stored on the server's hard disks. When the e-mail recipient retrieves the message from the server, it starts the process of encapsulation again to transmit the message over the network to the final recipient host. There the frames are de-encapsulated so that the user can read them.



#### Interactive Activity 2-3: Identify OSI Layer Protocols and Technologies (2.2.2)

In this interactive activity, you identify the layer to which the protocol or technology belongs. Use file d2ia-222 on the CD-ROM that accompanies this book to perform this interactive activity.

# **Troubleshooting Using the OSI Model**

As a theoretical model, the OSI model defines the functions that take place at the seven layers. These then can be associated with the protocols, hardware, and other specifications that operate at these layers.

The OSI model also provides a systematic basis for troubleshooting a network. In any troubleshooting scenario, the basic problem-solving procedure includes the following steps:

- **Step 1.** Define the problem.
- Step 2. Isolate the cause of the problem.
- **Step 3.** Solve the problem:
  - Identify and prioritize alternative solutions.
  - Select one alternative as the solution.
  - Implement the solution.
  - Evaluate the solution.
  - Document the solution.

If an identified solution does not fix the problem, undo any changes, and proceed to the next possible solution. Loop through the steps until a solution works.

In addition to the basic problem-solving procedures, the OSI model can be used as a troubleshooting guide. In any troubleshooting situation, it is usually best to start with the easiest items to check. Using the OSI model as a guide, the help desk technician can query the customer to help define the problem and isolate the cause. The OSI model can be used to analyze and troubleshoot a problem when accessing a website. Different problems at each layer can contribute to the symptoms being experienced. For example, as shown in Table 2-1, you can ask the following questions to help isolate the problem to a specific layer or group of layers.

Table 2-1 OSI Model Layers and Related Issues

Layer	Question
Layers 5 through 7: Upper layers	Can your browser open this website?
Layer 4: Transport	Do you have a firewall configured on your PC?
Layer 3: Network	Can you ping your default gateway?
Layer 2: Data link	Is the link light on your NIC on?
Layer 1: Physical	Is your network cable plugged in and secure?

When troubleshooting a problem using the OSI model, you have three basic troubleshooting approaches:

- Bottom-up
- Top-down
- Divide-and-conquer

### Bottom-Up Approach

The *bottom-up approach* to troubleshooting a networking problem starts with the network's physical components and works up the layers of the OSI model. Bottom-up troubleshooting is an effective and efficient approach for situations when the problem is suspected to be physical. Physical problems are usually fairly easy to rule out and can save you time troubleshooting other higher-level issues. For example, if the cable is unplugged, it does not make sense to spend time trying to analyze upper-layer problems.

### Top-Down Approach

When you apply a *top-down approach* to troubleshooting a networking problem, you start with the user application and work your way down the layers of the OSI model. The top-down approach is usually the simple route and typically affects only one or a few users. Lower layers, or network infrastructure, usually affect more than a few users.

For example, if a user cannot get to a website, the technician can start at the top of the OSI model and try accessing a different website. If the other website can be accessed, the problem is probably with the first website. If the second site is also inaccessible, the technician can move down the OSI model and check for a firewall blocking ports at the transport layer. The technician could then check IP settings on the host and try pinging the default gateway or the DNS servers to determine if the problem is at the network layer.

## **Divide-and-Conquer Approach**

The *divide-and-conquer approach* is generally used by more experienced network technicians. The technician makes an educated guess targeting the problem layer and then moves up or down the OSI layers based on the observed results.

## Help Desk Troubleshooting Example

The help desk technician usually has a standard checklist or script to follow when troubleshooting a problem. Often the script takes a bottom-up approach to troubleshooting because physical problems usually are the simplest to diagnose and repair, and the bottom-up approach starts with the physical layer.

### Layer 1 Troubleshooting

The technician should start with Layer 1 issues. Remember, Layer 1 deals with the physical connectivity of the network devices. Layer 1 problems often involve cabling and electricity and are the cause of many help desk calls. Some of the more common Layer 1 problems include the following:

- Device power is off
- Device power is unplugged
- Loose network cable connection
- Incorrect cable type
- Faulty network cable

To troubleshoot at Layer 1, check that all devices have the proper electrical supply and that they are turned on. This seems obvious, but many times a device within the network path from source to destination may be overlooked by the person reporting the problem. If any LEDs display the status of the connectivity, verify with the customer that they are indicating correctly. If the technician is onsite at the customer location, the next step is to visually inspect the network cabling and reconnect cables to ensure a proper connection. Figure 2-8 shows the back of a router with various connections, including an Ethernet cable, console cable, serial cable, and power cord. Any of these can cause Layer 1 problems that might prevent network communication.

#### Figure 2-8 Cables and Connections



When remotely troubleshooting a problem, talk the caller through each step. Tell the person what to look for and what to do if an error is found. If it is determined that all Layer 1 issues have been addressed, it is time to travel up the OSI model to Layer 2.

#### Layer 2 Troubleshooting

Network switches and host NICs perform Layer 2 functions. Layer 2 problems can be caused by faulty equipment, incorrect device drivers, or an improperly configured switch. When remotely troubleshooting a problem, it may be difficult to isolate a Layer 2 problem.

An onsite technician can check whether the NIC is installed and working properly. Reseating the NIC, or replacing a suspected faulty NIC with a known good NIC, helps isolate the problem. The same process can be done with any network switch.

#### Layer 3 Troubleshooting

At Layer 3, the technician needs to investigate the logical addressing used in the network, such as the IP addressing scheme. If the network is using IP addressing, the technician verifies that the device has the proper settings, such as

- IP address within the assigned network
- Correct subnet mask
- Correct default gateway
- Other settings as required, such as DHCP or DNS

Most network problems usually can be resolved using Layer 1, 2, and 3 troubleshooting techniques. At Layer 3, several utilities can assist with the troubleshooting process. Three of the most common Windows command-line tools are **ipconfig**, **ping**, and **tracert**. Linux and UNIX hosts use **ifconfig**, **ping**, and **traceroute**. Cisco network devices such as switches and routers can also use **ping** and **traceroute**. Examples of the output from the Windows versions of these tools follow.

ipconfig shows IP settings on the computer, as shown in Example 2-1.

#### Example 2-1 Sample ipconfig Output

**ping** tests basic network connectivity, as shown in Example 2-2. If the IP address 192.168.1.1 is on the same local Ethernet network as the host that issued the ping, the ping demonstrates that the target host is up and configured correctly and that any switches in between are functioning properly. If the two hosts are on different networks, separated by routers and perhaps one or more WAN links, the ping demonstrates that the host is configured correctly with a default gateway. It also shows that the gateway and any other routers or WAN links between the two hosts are functioning properly.

Example 2-2 Sample ping Output

```
C:\> ping 192.168.1.1
```

Pinging 192.168.1.1 with 32 bytes of data: Reply from 192.168.1.1: bytes=32 time<1ms TTL=64

```
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms</pre>
```

**traceroute** or **tracert** determines whether the routing path between the source and destination is available, as shown in Example 2-3. This example illustrates a Windows PC issuing the command. If this were a Linux or UNIX host or a Cisco networking device, such as a router, the command used would be **traceroute**.

Example 2-3 Sample tracert Output

```
C:\> tracert www.cisco.com
Tracing route to www.cisco.com [198.133.219.25]
over a maximum of 30 hops:
<some output omitted>
 1
      <1 ms
             <1 ms
                       <1 ms 192.168.1.1
 2
                      7 ms 10.44.192.1
       8 ms
                9 ms
 3
       7 ms
                7 ms
                       10 ms gig5-2.rtr3.cisco.com [172.18.234.57]
 4
       9 ms
                9 ms
                        10 ms www.cisco.com [198.133.219.25]
Trace complete
```

### Layer 4 Troubleshooting

If Layers 1 through 3 all appear to be operating normally and the technician can successfully ping the IP address of the remote server, it is time to check the higher layers. For example, if a network fire-wall is used along the path, it is important to check that the application TCP or UDP port is opened and that no filter lists are blocking traffic to that port.

### Layer 5 Through 7 Troubleshooting

The technician should also check the application configuration. For example, if troubleshooting an email issue, ensure that the application is configured with the correct sending and receiving e-mail server information, as shown in Figure 2-9. In the figure, the e-mail server name is specified. If the wrong server name is specified, the e-mail client cannot send or receive e-mail. Because the server name must be resolved to an IP address before e-mail can be sent or received, it is also necessary to ensure that *Domain Name System (DNS)* resolution is occurring as expected. This can be done by pinging the e-mail server by name and IP address. If the technician can ping the server by IP address but not by name, there could be a problem with DNS. Further testing can also be performed by pinging the primary and secondary DNS servers to see if they are up. Remote technicians can check higherlayer issues by using other network utility tools, such as a packet sniffer, to view traffic as it crosses the network. A network application, such as Telnet, can also be used to view configurations remotely.

E-mail Accounts	X
Email Server Settings	
You can enter the required inf	ormation to connect to your Email server.
Type the name of your Email Ser	ver computer. For information, see your system administrator.
Email Server:	emailsvr.academy.cisco.com
	🗹 Use Cached Email Mode
Type the name of the mailbox set your user name.	tup for you by your administrator. The mailbox name is usually
User Name:	John Smith (jsmith) Check Name
	More Settings
	<back next=""> Cance</back>

#### Figure 2-9 E-mail Account Settings

#### Note

Just because you cannot ping a server or telnet to it does not mean that the server is down or inaccessible. Firewalls and server OS settings may prevent ping and telnet as a protection measure for the server.

The bottom-up approach works for many situations, but the top-down approach can also be used. The top-down approach simply reverses the order in which things are checked, starting with the application layer.

The divide-and-conquer approach can also be used. With this technique the technician may choose to start the troubleshooting process at a middle layer, such as the network layer. The technician then works up or down the OSI model, depending on the troubleshooting results from that layer.



#### Interactive Activity 2-4: Identify Network Issues at OSI Layers (2.2.3)

In this interactive activity, you identify whether a network issue occurs at Layer 1, Layer 2, Layer 3, Layer 4, or Layers 5 through 7. Use file d2ia-223 on the CD-ROM that accompanies this book to perform this interactive activity.

# **ISP Troubleshooting**

Network help desk personnel must be prepared for various types of potential end-user problems, but most can be categorized as either e-mail-related or an inability to access a network resource due to connectivity issues. Problems can usually be resolved remotely but may require an onsite visit by the technician. This section covers the use of help desk records, remote diagnostics, and onsite customer procedures.

# Help Desk Troubleshooting Scenarios

The number and types of calls received by the help desk can vary considerably. Some of the most common calls include e-mail and connectivity issues.

## E-mail Issues

Common e-mail issues include the following:

- You can receive but not send
- You can send but not receive
- You cannot send or receive
- Nobody can reply to your messages

A very common cause of many e-mail problems is using the wrong POP, IMAP, or SMTP server name. It is best to check with the e-mail administrator to confirm the proper name of the e-mail server and SMTP server. In some cases, the same server name for both POP/IMAP and SMTP are used. Also, confirm that the username and password are correct.

When troubleshooting these issues over the phone, it is important to step the customer through the configuration parameters carefully. Many customers are unfamiliar with both the terminology and the values of the various configuration parameters. If possible, connecting to the customer device via remote management software, using in-band management, is preferred. Examples of remote desktop management software include PC Anywhere, LogMeIn, and GoToMyPC. Use an Internet search engine with the keywords "remote desktop management software" to see many others. When the technician uses remote desktop tools, the end user must allow the remote application to access his or her PC. This allows the technician to take control of the customer's PC and perform the necessary steps for the customer.

Another problem that can affect application functionality is a failure of DNS to correctly resolve server names. This can be checked with the command-line **ping** or **nslookup**. A simple web browser check for DNS operation can prevent needless troubleshooting steps.

## Host Configuration Issues

A common issue that can prevent connectivity to the Internet or other network resources is improperly configured host addressing information. This can include an incorrect IP address, subnet mask, or default gateway, or a combination of these.

In environments where the IP addressing information is manually configured, it is possible that the IP configuration was simply entered incorrectly. In environments where hosts are configured to dynamically receive an IP address from an assignment server, such as a DHCP server, the DHCP server may fail or become unreachable due to network issues.

If a Windows host is configured to receive an address dynamically, and an assignment server, such as a DHCP server, is unavailable or unreachable, the operating system will automatically assign a *link-local address* to the local host. IPv4 addresses in the address block 169.254.0.0 to 169.254.255.254 (169.254.0.0/16) are designated as link-local addresses. A link-local process will randomly select an IP address within the 169.254.0.0/16 range. But what prevents two hosts from randomly selecting the same IP address?

When the link-local process selects an IP address, it sends an ARP query with that IP onto the network to see if any other devices are using that address. If there is no response, the IP address is assigned to the device; otherwise, another IP address is selected and the ARP query is repeated. Microsoft refers to link-local addresses as *Automatic Private IP Addressing (APIPA)*.

If multiple hosts on the same network obtain a link-local address, client/server and peer-to-peer applications between those hosts will work properly. However, because link-local addresses are in the private Class B address space, communication outside the local network is not possible. When troubleshooting both manually and dynamically configured hosts, use the host command **ipconfig /all** to verify that the host is using the appropriate IP configuration.

In Figure 2-10, the DHCP server on Network A is down. All Microsoft OS hosts on this network receive an APIPA link-local address. They are able to communicate locally but are unable to access other hosts on other networks. The DHCP server on Network B is up and all hosts on that network receive normal IP addressing. These hosts can communicate with each other and with hosts on the Internet.

#### Figure 2-10 APIPA Addressing Issues



### **Customer Connectivity Issues**

Connectivity problems are more common with new customers trying to connect for the first time; however, sometimes existing customers encounter connectivity issues. First-time customers usually have a problem with the hardware as well as software settings. Existing customers notice connectivity problems when they cannot open a web page or connect to instant messaging or e-mail.

There can be many reasons why a customer has no connectivity:

- Billing account issues
- Hardware failure
- Physical layer problems
- Application settings
- Application plug-in is missing
- Missing applications

In many cases, the problem is a faulty cable, or even a cable plugged in to an incorrect port. These types of issues can be resolved by checking the cable connection or replacing the cable.

Other problems, such as software issues, may be more difficult to detect and might require researching similar issues on FAQs or a knowledge base. One example is an incorrectly loaded TCP/IP stack, preventing IP from operating correctly. The TCP/IP stack can be tested and verified using a *loopback address*. The loopback is a special address, the reserved IPv4 address 127.0.0.1, which hosts use to direct traffic to themselves.

The loopback address creates a shortcut method for TCP/IP applications and services that run on the same device to communicate.

You can ping the loopback address to test the configuration of TCP/IP on the local host. If you are unable to get a response when pinging the loopback address, suspect an improperly configured or installed TCP/IP stack.

Addresses 127.0.0.1 through 127.255.255.254 are reserved for testing purposes. Any address within this block will loop back within the local host. No address within this block should ever appear on any network. Despite the fact that the entire 127.0.0.0/8 network range is reserved, the only address typically used for loopback testing is the 127.0.0.1 address.

Packet Tracer

#### **Troubleshoot and Resolve Network Connectivity Issues (2.3.1)**

In this activity, you troubleshoot and resolve a network connectivity issue. Use file d2-231.pka on the CD-ROM that accompanies this book to perform this interactive activity.

# Creating and Using Help Desk Records

When a Level 1 help desk technician receives a call, he or she follows a certain process in gathering information and using a system to store and retrieve relevant information. This is extremely important in case a call has to be escalated to Layer 2, or even needs an onsite visit.

The information gathering and recording process starts as soon as the technician answers the phone. When the customer identifies himself or herself, the technician accesses the relevant customer information. Typically, a database application is used to manage the customer information. Examples of help desk software include Autotask, Help Desk, and HelpSTAR. Use an Internet search engine with the keywords "help desk management software" to see many others.

The information is transferred to a trouble ticket, or incident report. This document can be a piece of paper in a filing system or an electronic tracking system designed to follow the troubleshooting process from beginning to end. Each person who works on the customer's problem is expected to record in the trouble ticket what was done. When an onsite call is required, the trouble ticket information can be converted to a work order, as shown in Figure 2-11, that the onsite technician can take to the customer site.



Company Address: <u>204 N</u> Company Phone: <u>1-866-5</u>	Company Address: 204 N, Main Street Company Phone: 1-866-555-0998	
	Generating a New Tick	tet
Category: <u>Hardware</u>	Closer Code	Status <u>Open</u>
Туре:	Escalated Yes	Pending
Item	Р	Pending Until Date
E	Business Impacting? X Ye	es O NO
Summary The computer	will not start up. The comp	outer beeps constantly.
Priority 2 User Platform Windows X	P Pro	nent
Problem Description: <u>Con</u> manufacturer of the BIOS. not hear any strange soun purning electronics.	nputer will not boot. Custo Cannot identify error from ds from the computer. Cus	mer does not know the n beep sequence. Customer did stomer does not smell smoke or
Problem Solution		

When a problem is resolved, the solution is documented on the customer work order or trouble ticket and in a knowledge-base document for future reference.

Occasionally, the help desk technician may receive a call that cannot be resolved quickly. In this case, the technician is responsible for passing the call to someone who is more qualified to resolve the issue. This is the process of call escalation, in which the call is passed to a Level 2 technician.

Level 1 and Level 2 help desk technicians attempt to solve customer problems using the telephone, web tools, and possibly even remote desktop-sharing applications.

If the help desk technicians cannot remotely fix the problem, it is often necessary to dispatch a mobile onsite technician to the customer premises. It is the job of the onsite technician to visit the customer premises to physically work on the problem equipment. The help desk technician can make an appointment with the customer for the onsite technician to perform the repairs, or it may be the responsibility of the onsite technician to arrange the appointment.

To properly troubleshoot the problem, the onsite technician reviews the trouble ticket to see what was previously done. This review gives the technician some background information, as well as a logical starting point. It also helps the technician decide which tools and supplies to bring, rather than having to leave the customer site to obtain supplies.

Onsite technicians typically work on the network at the customer location. But sometimes the technician is unable to make the needed repairs and must bring the damaged equipment back to the ISP site for repair. In many cases, the technician can install a replacement unit to get the customer up and running. The onsite technician can bring a number of tools to help with the job, such as those shown in Figure 2-12. These can include, but are not limited to, the following:

- **Crimpers:** Used to crimp the connector to the cable.
- **Cable:** Used to run new cable or replace old cable.
- Cable tester: Used to determine cable length and whether a cable is good or bad.
- **Connectors:** Used to make new cables or replace broken connectors.
- Multimeter: Used to check an electric circuit.
- Laptop: Used to test the network through various utility programs.
- Hub or small switch: Used to connect multiple computers to a single network.
- Floppy disk: Used for boot disks.
- **CD-ROM:** Used to boot and store troubleshooting utilities.
- USB flash drive: Used to store files and troubleshooting utilities.
- Cell phone: Used to call the office and set up and confirm appointments with customers.

Figure 2-12 Troubleshooting Tools



# **Customer Site Procedures**

An onsite technician should follow four steps before beginning any troubleshooting or repair at the customer site:

- **Step 1.** Provide proper identification to the customer.
- **Step 2.** Review the trouble ticket or work order with the customer to verify that the information is correct.
- **Step 3.** Communicate the current status of any identified problems or issues, as well as the actions the technician expects to take at the customer site that day.
- Step 4. Obtain permission from the customer to begin the work.

The technician must verify all items on the trouble ticket. As soon as the technician is familiar with all the issues, the work can begin. The technician checks all device and network settings and runs any necessary utilities. When necessary, the technician may have to swap out suspected faulty hardware with known good hardware to determine if a hardware problem exists. After the technician determines the cause of the problem, he or she can attempt the repair and observe the results.

When performing any troubleshooting tasks on site, especially when installing new or replacing existing equipment, it is important to minimize the risk of injury by following good safety practices. Many employers offer safety training as part of their employee services.

Different equipment and workspaces require you to take special care while troubleshooting, as follows:

- Ladders: Use ladders to reach high locations to install networking cable and to install or troubleshoot wireless access points in places that are difficult to reach. To reduce the risk of falling off the ladder or dropping equipment while climbing on the ladder, work with a partner whenever possible.
- High or dangerous locations: Sometimes network equipment and cables are located in high and dangerous places that are not accessible by a ladder, such as on the side of a building, on rooftops, or in an internal structure such as an elevator shaft. Work performed at this type of location must be done very carefully. Using a safety harness reduces the risk of falling.
- Electrical equipment: If there is a risk of damaging or coming in contact with any electrical lines when handling hardware, consult with the customer's electrician about measures that can be taken to reduce the risk of electrical shock. Coming in contact with electrical equipment can result in serious personal injury.
- Awkward spaces: Network equipment is often located in narrow and awkward spaces. Ensure that the work area is properly lighted. Determine the best way to lift, install, and remove equipment to minimize the risks.
- Heavy equipment: Networking devices can be large and heavy. Plan to have the correct equipment and trained personnel when heavy equipment needs to be installed or moved at a customer site.

When finished, the technician communicates to the customer the nature of the identified problem, what solution was applied, and any follow-up procedures. Before the problem can be considered fully resolved, the technician must obtain the customer's acceptance. The technician can then close the trouble ticket and document the solution.

The customer receives a copy of the documentation. The document includes the original help desk call problem and the actions taken to solve it. The technician records the final solution, and the customer acceptance is indicated on the trouble ticket. For future reference, the technician should also record the problem and the solution in the help desk documentation and FAQs.

In some cases, an onsite technician can uncover network problems that require upgrades or reconfiguration of the network devices. When this occurs, it may be outside the scope of the original trouble ticket. These issues usually are communicated to both the customer and the ISP network personnel for further action.

# Summary

Help desk technicians provide solutions to customers' network problems. Help desk user support usually exists at three levels. Incident management is the basic procedure followed when a help desk technician initiates the standard problem-solving processes. Help desk operation relies on opening trouble tickets and logging information.

Customer service and interpersonal skills are important when handling difficult clients and incidents. Some of the skills that are consistently used in successful help desk communication include

- Preparation
- Courteous greeting
- Listening to the customer
- Adapting to the customer's temperament
- Correctly diagnosing a simple problem
- Logging the call

A layered approach is used for troubleshooting. The layered OSI model breaks the task of network communication into multiple processes. Each process is a small part of the larger task. The seven layers of the OSI reference model can be divided into two categories: upper and lower layers. Upper layers consist of any layer above the transport layer and are implemented in software. Lower layers consist of the transport, network, data link, and physical layers and handle data transport functions. Using the OSI model, the help desk technician can troubleshoot using a bottom-up, top-down, or divide-and-conquer approach.

Information gathered from the customer is transferred to the trouble ticket, or incident report. Some of the most common customer service calls are about e-mail and connectivity issues.

Level 1 and Level 2 help desk technicians attempt to solve customer problems over the telephone or web or by using remote desktop-sharing applications. Sometimes it is necessary to dispatch a mobile onsite technician, or Level 3 technician.

It is important to document the solution on the customer work order, on the trouble ticket, and in a knowledge-base document for future reference.

# **Activities and Labs**

This summary outlines the activities you can perform to help reinforce important concepts described in this chapter. You can find the activity and Packet Tracer files on the CD-ROM accompanying this book.



### Interactive Activities on the CD:

Interactive Activity 2-1: Identify Technician Support Level Responsibilities (2.1.2) Interactive Activity 2-2: Determine the Customer Support Process (2.1.3) Interactive Activity 2-3: Identify OSI Layer Protocols and Technologies (2.2.2) Interactive Activity 2-4: Identify Network Issues at OSI Layers (2.2.3)



#### Packet Tracer Activity on the CD:

Troubleshoot and Resolve Network Connectivity Issues (2.3.1)

Chapter 2 does not have a Hands-on Lab in Part II of this book.

# **Check Your Understanding**

Complete the review questions to test your understanding of the topics and concepts in this chapter. Appendix A, "Check Your Understanding and Challenge Questions Answer Key," lists the answers.

- 1. Indicate whether the network function is associated with the transport or network layer by placing a T or N next to it:
  - A. Packages data in segments for transmission: \_\_\_\_
  - B. Routes packets between networks: \_\_\_\_
  - C. Encapsulates data in packets for transmission:
  - D. Uses UDP for real-time data streaming:
  - E. Adds port numbers: \_\_\_\_
  - F. Adds IP addresses to data packets: \_\_\_\_
- 2. Using a systematic troubleshooting approach, a help desk technician suspects a problem at Layer 3 of the OSI model. Which two questions could the technician ask to isolate the problem to Layer 3?
  - A. Is your PC configured for DHCP?
  - B. Can you browse to http://www.cisco.com?
  - C. Is your network cable plugged in?
  - D. Can you ping your default gateway?
  - E. Do you see a link light on your network card?
- **3.** Indicate the OSI layer that each question is associated with if a help desk technician is using a bottom-up approach to troubleshooting. Place the OSI model layer number next to each question to indicate the order in which the technician would troubleshoot. For the application layer, use Layers 5 through 7.

Is your network cable securely connected?

What mail server is listed in the outgoing server setting?

Is your Windows firewall blocking port 25? \_

Do you see a link light on your network card? \_\_\_\_

What is the subnet mask on Local Area Connection 2? \_\_\_\_\_

- **4.** A customer call has been escalated to an onsite technician because the Level 1 and 2 technicians could not determine the problem. Which three tasks would the onsite technician perform?
  - A. Open the trouble ticket and enter the customer's information.
  - B. Replace faulty cables or connections.
  - C. Check to see if the ISP's e-mail server is working.
  - D. Correct PC network settings, and run any necessary utilities.
  - E. Swap out suspected faulty hardware with known good hardware.
  - F. Check the customer's account payment status.
- 5. Which two actions should be taken after a customer problem is resolved by the ISP help desk?
  - A. Delete the trouble ticket from the database.
  - B. Document the solution in the trouble ticket or work order.
  - C. Escalate the trouble ticket to Level 2 for future reference.
  - D. File a work order for customer notification.
  - E. Copy the solution into a knowledge-base document for future reference.
- 6. Which two scenarios are common causes of physical network connectivity problems?
  - A. The monitor is unplugged
  - B. The Ethernet cable is plugged into the wrong port
  - C. Incorrect default gateway
  - D. Unassigned IP address
  - E. Faulty Ethernet cable
- 7. Indicate whether each network component or function is associated with the physical, data link, or network layer by placing a P, D, or N next to it:
  - A. Twisted-pair cable: \_\_\_\_
  - B. IP address: \_\_\_\_
  - C. Routing: \_\_\_\_
  - D. Switching: \_\_\_\_
  - E. MAC address: \_\_\_\_
  - F. Hub: \_\_\_
- **8.** What two tasks should an onsite technician perform before beginning any troubleshooting or repair at the customer site?
  - A. Review the trouble ticket with the customer to verify that the information is correct.
  - B. Take damaged equipment to the ISP site for repair.
  - C. Document the troubleshooting task performed and the solution.
  - D. Provide identification, including name and place of employment.
  - E. Examine cabling to determine if it is faulty or connected to the wrong port.

9. Match the technical skill on the left to the appropriate help desk activity on the right:

Skill	Help Desk Activity
Make notes about the resolution of a help desk case	Providing a courteous greeting
Answer calls in a friendly, professional manner	Adapting to the customer's temperament
Speak in a calm, reassuring manner	Logging the call
Get all relevant information from the customer	Diagnosing a problem correctly
Use analytical tools to provide a problem resolution	Listening to the customer

10. An ISP customer calls to report that the web server web-s1.cisco.com cannot be reached through a web browser. The technician uses command-line utilities to verify the problem and to begin the troubleshooting process. Based on the results shown in the following sample output, what can you determine about the problem? (Choose two.)

```
C:\> ping web-s1.cisco.com
```

Ping request could not find host web-s1.cisco.com. Please check the name and try again. C:\> ping 192.168.0.10

```
Pinging 192.168.0.10 with 32 bytes of data:
Reply from 192.168.0.10: bytes=32 time<10ms TTL=64
Ping statistics for 192.168.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 10ms, Average = 10ms
```

- A. The web server at 192.168.0.10 can be reached from the source host.
- B. A problem is occurring with the web server software on web-s1.cisco.com.
- C. A router is down between the source host and the server web-s1.cisco.com.
- D. DNS cannot resolve the IP address for the server web-s1.cisco.com.
- E. The default gateway between the source host and the server at 192.168.0.10 is down.
- **11.** A network technician is unable to telnet to a remote server from her workstation. She tries pinging the server and is successful. Next she checks to see if a firewall is blocking Telnet port 23. Finally, she checks to see if the Telnet service is running on the remote server. What troubleshooting approach is she using?
  - A. Top-down approach
  - B. Divide-and-conquer approach
  - C. Bottom-up approach
  - D. Substitution

- **12.** A technician uses the **nslookup** command to troubleshoot a problem when none of the users at a customer's location can access remote websites. What type of problem can this command help diagnose?
  - A. The firewall is blocking port 23.
  - B. An Ethernet cable to one of the customer's hosts is disconnected.
  - C. DNS is not resolving names to IP addresses.
  - D. Wireless connectivity issues are occurring.
- **13.** When a Microsoft computer is configured as a DHCP client and a DHCP server is unavailable, what type of address does the client receive?
- 14. The TCP/IP software stack on the local machine can be tested using what type of address?

# **Challenge Questions and Activities**

These questions require a deeper application of the concepts covered in this chapter. You can find the answers in Appendix A.

- **1.** In your role as an internal organization help desk technician, you receive a call from a user stating that she cannot access a file server that she normally works with.
  - A. Would you employ the top-down, bottom-up, or divide-and-conquer troubleshooting approach?
  - B. What questions would you ask the user to help identify the problem?
  - C. What other steps could you take to help resolve the problem?
- 2. In your role as an ISP help desk technician, you receive a call from a DSL/cable customer stating that he cannot access any websites.
  - A. Would you employ the top-down, bottom-up, or divide-and-conquer troubleshooting approach?
  - B. What questions would you ask the customer to help identify the problem?
  - C. What other steps could you take to help resolve the problem?
- 3. Help desk person interview activity (optional).

In this activity you will contact a help desk person and, using the following form, ask him a few questions about his job. This will help you better understand the background that a help desk employee has and the nature of his work. This person can be an internal help desk person or one who works for an ISP.

Use your help desk skills to interview the person. Tell him that you are a networking student and would like a few minutes of his time. Be sure to thank him when the interview is complete.

Organization:
Person's name:
Position/title:
Length of time with the company:
Number of years as a help desk support person:
Support level provided:
Training/background/preparation:

Primary desktop management software used:

Help desk problem resolution software used:

Most common types of problems encountered:

Most challenging problem solved:

Compare your notes with those of other students to try to develop a profile of a help desk technician.