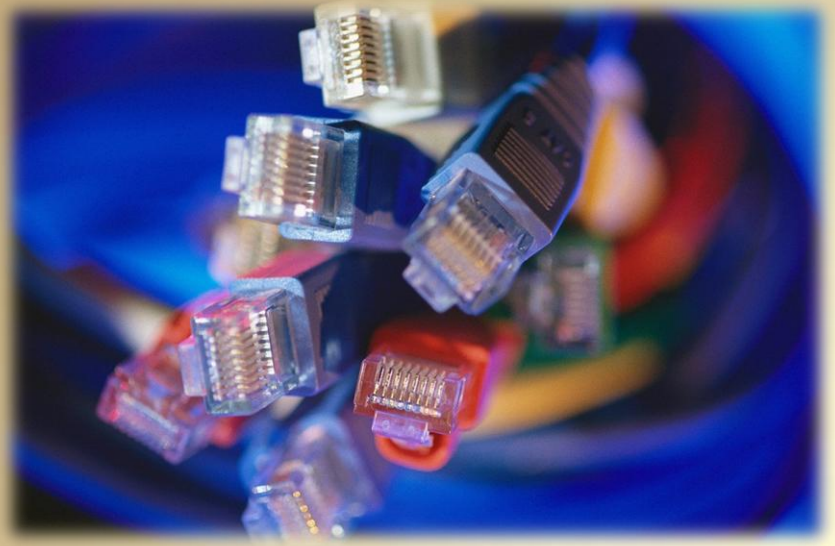
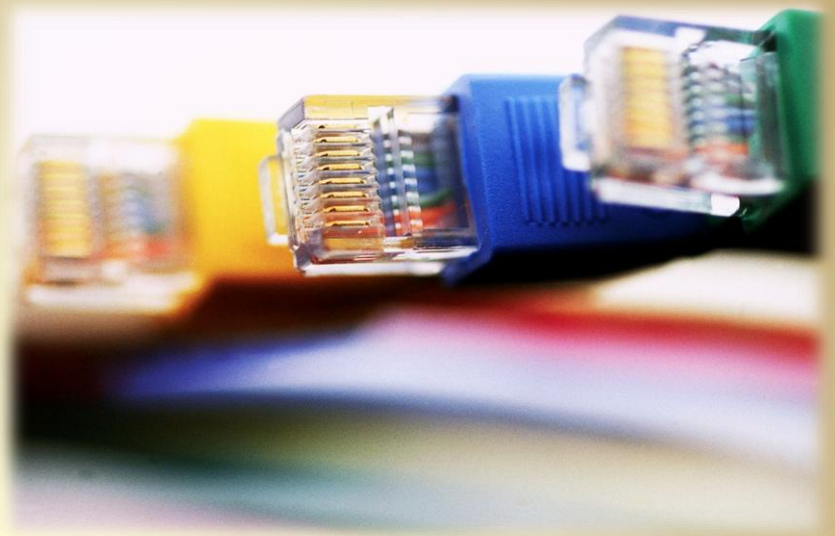


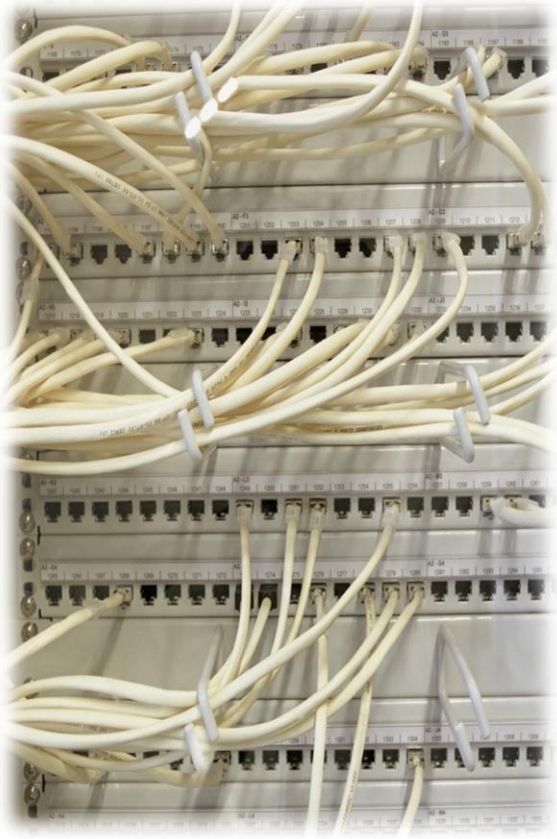


Networking Overview (GUI)

This material is based upon work supported by the National Science Foundation under Grant No. 0802551

Lesson Overview

One of the reasons computers are so powerful is their ability to communicate and share information with other computers. One computer sitting in a basement may communicate with other computers on the Internet, or with another computer in the same house using a wired connection such as an Ethernet network cable, or a wireless connection (Wi-Fi or a cell phone connection).



To communicate, computers must speak the same language, or have access to a translator to ensure each computer can understand the other and respond appropriately.

In this lesson, you will be learning about computer networks in a Linux environment. This lesson is important because proper networking skills are essential to any administrator managing multiple computer systems that must communicate with each other to function properly. In other words, you cannot be a good Linux administrator if you lack networking skills.

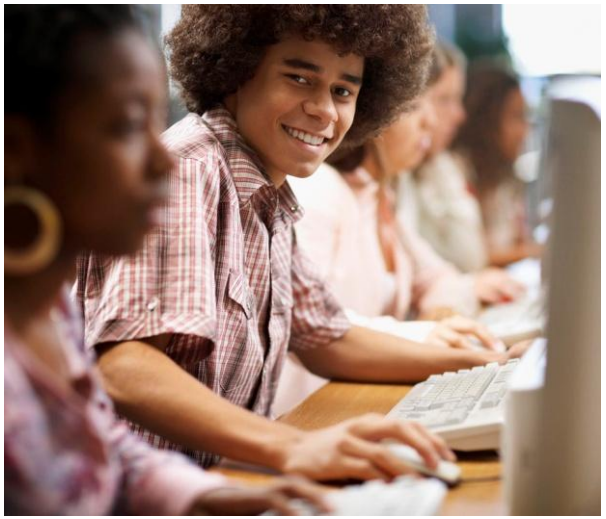
Student Expectations

You should know what will be expected of you when you complete this lesson. These expectations are presented as objectives.

Objectives are short statements of expectations that tell you what you must be able to do, perform, learn, or adjust after reviewing the lesson.

Objective

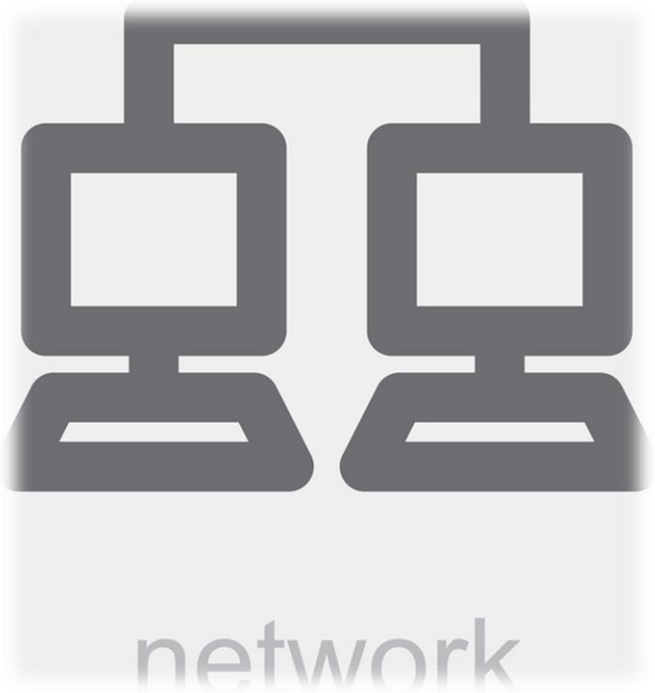
Given an installation of Linux that lacks network access, students will be able to establish and configure appropriate networking protocols in a GUI environment to allow for external communication as required.



Lesson Outline

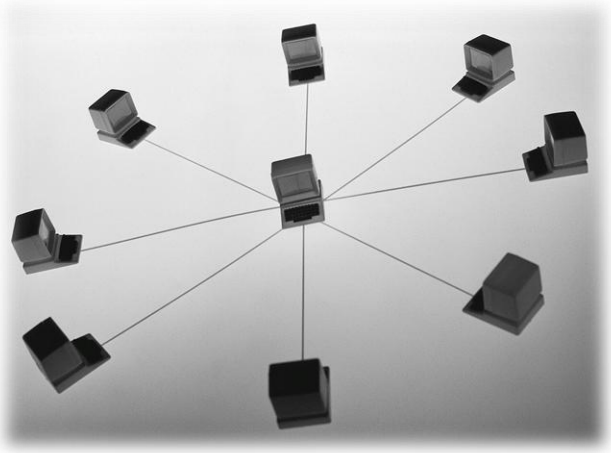
During this lesson, you will explore:

- Network Configuration
- IP Addressing
- Testing with CLI Tools
- Introduction to Firewalls
- Network Managers
- Remote Access



Network Configuration

In today's technology dependent society, the use of a computer is not complete without a network connection. Networking allows you to communicate with billions of other computers on the Internet, or to other network-capable machines nearby or far away. To network your computer, you need to follow specific steps that will differ depending on the type of operating system your computer uses or the type of network you wish to use.

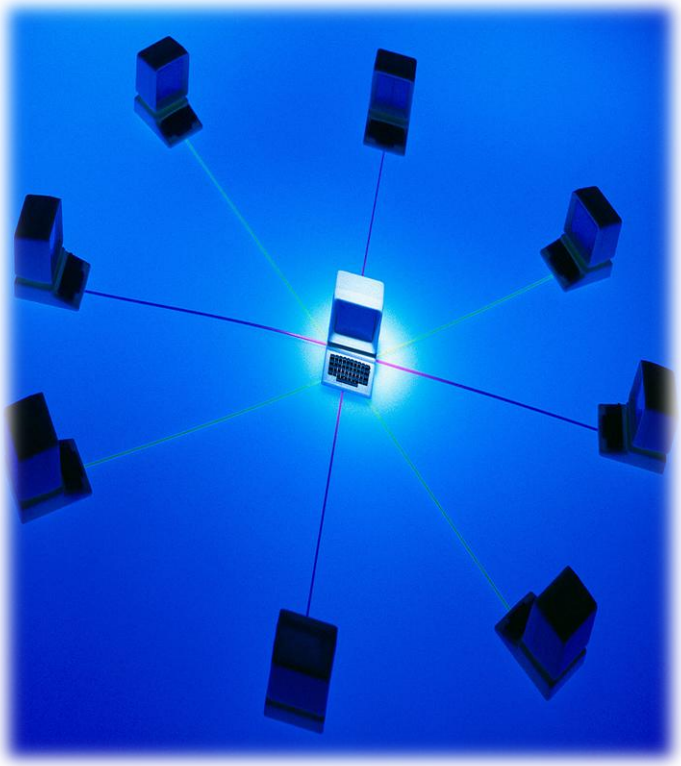


Before networking or connecting one computer to others, you need to make certain decisions. What connection will you use? Will the computers communicate through physical connections such as wired Ethernet cables connected to each other, or will computers communicate wirelessly?

Wired connections generally provide faster, more reliable connections, but may require drilling through walls or partitions to connect multiple cables. Wireless connections communicate via radio waves, satellite, infrared or other wireless signals. They do not require much cabling, but can be affected by other devices communicating on the same channel or by physical boundaries such as walls that block or limit their signal strength.

Networking

The topic of networking is extensive and takes several weeks to digest. Throughout this lesson, you will learn some introductory and basic networking concepts. You will also be introduced to the most familiar and common networking tools used in the Unix/Linux environment.



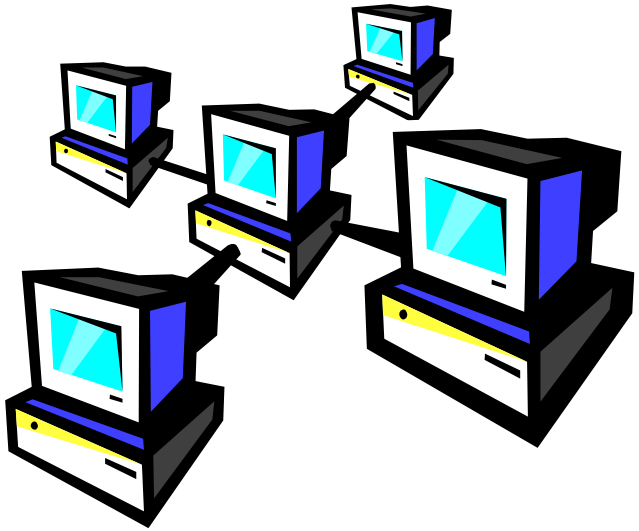
Before communicating with other computers, a networked computer must know the location of other machines. One way to locate a computer is through the use of an IP address. Some computers live at the same address for a long time and are given static IP addresses. Other computers change addresses frequently and are assigned dynamic IP addresses. IP addresses are written as a series of four numbers separated by a period. Humans often find complicated numbers difficult to remember, so a DNS server is used to translate between IP addresses and web site names. Finally, a DHCP server is used to assign IP addresses to computers automatically.

TCP/IP

A common language allows two people to communicate with each other. Similarly, TCP/IP is a communication protocol that allows two or more computers to send and receive data.

TCP/IP is considered a protocol suite (TCP is one protocol and IP is another). The IP protocol is generally used to assign addresses to computers on a TCP/IP network. There are two types of IP addresses—static and dynamic.

A static IP address is an address assigned to a device that needs to be "found." For example, a web server, a router or email server would typically need to have an address that does not change (static IP). On the other hand, a dynamic address changes frequently. A user may receive a new address each time he/she logs in. This arrangement allows one IP address to be reused by different users at different times.



TCP/IP: Dynamic

A dynamic IP address is assigned to a device that needs to be on a network but does not necessarily need to be "found." For example, a personal computer at home or work will generally have a dynamic address that it receives from a DHCP (Dynamic host Configuration Protocol) server.

You can see an example of each of these type of addresses on the right.

Lo = Loopback interface
etho = First Ethernet interface card
wlano = First wireless network interface

Static IP

```
auto lo
iface lo inet loopback

auto etho
iface etho inet static
        address 209.86.43.106
        netmask 255.255.255.248
        broadcast 209.86.43.111
        network 209.86.43.104
        gateway 209.86.43.110
```

Dynamic IP

```
auto lo
iface lo inet loopback

auto etho
iface etho inet dhcp

auto eth1
iface eth1 inet dhcp

auto eth2
iface eth2 inet dhcp

auto wlano
iface wlano inet dhcp
```

IP Addressing

Unix/Linux network configurations support multiple network devices. A device can be identified by using either a network name, IP address and/or MAC address. Network identification also depends on the operating system and/or protocol used.

In a Unix/Linux environment, you would most likely use the TCP/IP protocol suite. However, you may choose to use other protocols which are beyond the scope of this course and would require you to seek additional training in this area as needed.

Computers can be connected by physical cables using Ethernet cards or NICs (Network Interface Cards). In a Linux system, the first Ethernet card is labeled "eth**0.**" If a second Ethernet card is present, it will be labeled "eth**1,**" and a third card would be labeled "eth**2.**" In the example on the right, the computer system has six (6) NICs.

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet dhcp

auto eth1
iface eth1 inet dhcp

auto eth2
iface eth2 inet dhcp

auto eth3
iface eth0 inet dhcp

auto eth4
iface eth1 inet dhcp

auto eth5
iface eth2 inet dhcp
```

IP Addressing: Mac Address

MAC address - the MAC address is also referred to as the hardware network address. This address is generally displayed using hexadecimal numbers. In the example on the right, the hardware address (or MAC address) for eth**o** is 00:08:C7:10:74:A8. It is possible to change the MAC address of a NIC card, though it is highly recommended that you do not.

A MAC address is used to identify the device within a LAN (Local Area Network). If the data leaves the LAN, then the device needs an IP address (assuming we are using TCP/IP) for communication and identification.

```
[root@sales tmp]# ifconfig -a

etho Link encap:Ethernet HWaddr 00:08:C7:10:74:A8
BROADCAST MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
Interrupt:11 Base address:0x1820

lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:787 errors:0 dropped:0 overruns:0 frame:0
TX packets:787 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:82644 (80.7 Kb) TX bytes:82644 (80.7 Kb)

[root@sales tmp]#
```

IP Addressing: Numbering

An IP address consists of 4 octets. Each octet represents 8 bits of data (or 1 Byte). Therefore, an IP version 4 (or IPv4) IP address (as displayed in figure 4) is 32 bits long or 4 bytes long. The IP address (or inet address) for wlan**0** is 192.168.1.100.

Note: There is also an IP version 6 (or IPv6). This IP address configuration is different from IPV4. It is based on hexadecimal numbers.

```
wlan0 Link encap:Ethernet HWaddr 00:06:25:09:6A:B5
inet addr:192.168.1.100 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:47379 errors:0 dropped:0 overruns:0 frame:0
TX packets:107900 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:4676853 (4.4 Mb) TX bytes:43209032 (41.2 Mb)
Interrupt:11 Memory:c887a000-c887b000

[root@sales tmp]#
```

Broadcast address – This is a reserved address used to send a message to all the devices within a network. In figure 4 - The broadcast address for wlan0 is 192.168.1.255 where the 255 is the host portion of the address and it will send the message to all the devices from within this network segment.

IP Addressing: Subnet Mask

The subnet mask is what determines which portion of the IP address is the network portion and which is the host portion of the address. In figure 4 the subnet mask (or mask) for wlano is 255.255.255.0. since the IP address (inet address) is 192.168.1.100 this means that the network portion of the address is 192.168.1 and the host portion of the address is 100.

Frequently network administrators use a subnet calculator to visualize the range of numbers that can be assigned to a network. Loopback address – In figure 4 the loopback address (lo link) is 127.0.0.1. The default loopback address of any computer is 127.0.0.1. Although, any 127.0.0.(1 – 254) address can be used as a loopback address. The entire 127.0.0.0/8 subnet is reserved for Internet host loopback addresses..

```
wlano Link encap:Ethernet HWaddr 00:06:25:09:6A:B5
inet addr:192.168.1.100 Bcast:192.168.1.255
Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500
Metric:1
RX packets:47379 errors:0 dropped:0 overruns:0
frame:0
TX packets:107900 errors:0 dropped:0 overruns:0
carrier:0
collisions:0 txqueuelen:100
RX bytes:4676853 (4.4 Mb) TX bytes:43209032 (41.2
Mb)
Interrupt:11 Memory:c887a000-c887b000

[root@sales tmp]#
```

Firewalls

Network security is a very important task for a Network Administrator. Though Unix/Linux systems are considered very secure operating systems, you must configure your firewall appropriately to minimize unauthorized use and / or access.

A firewall (software or hardware based) will prevent unauthorized users from entering and using your network. A firewall's effectiveness will depend on its location on your network. For example, a firewall located at the computer level protects only the computer. If the firewall is located at the router level, it protects the network segment that is serviced by the router.

Firewalls: Configuring

You can configure your software-based firewall during the installation process or at a later time. Whichever option you choose, it is critical that you configure the firewall to allow or limit various activities on the network. Failure to use a firewall or configure it properly is similar to leaving your front door unlocked while you sleep.

After the NIC has been configured, you will be prompted to select which network traffic is allowed on your network. For example, you may wish to prevent outside intruders sending ping packets to your server by blocking ICMP packets at the firewall level.

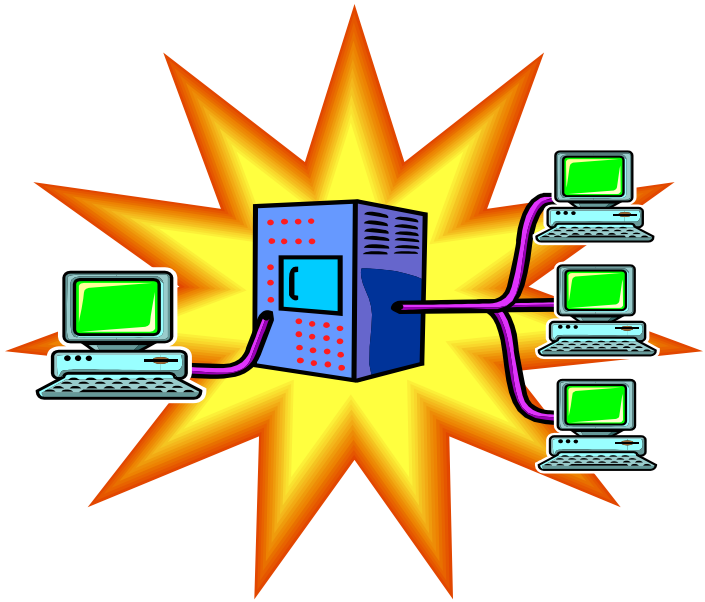
You can also block unused ports that are open by default and you can also block ports that often used by unauthorized intruders. For example, if you do not want anyone in your network using SSH you should block port 22.

Select **PLAY** below to view a video on the use of ping.

View Video VideoLesson6UsingPing(C1L7S23).mp4

Network Managers

A network manager is a set of tools that allow you to monitor your network and the allocated resources. It aids in the monitoring of devices, set alarms if needed, and could even notify the administrator of any problems that may arise. These networks can be used either with wireless, cable, or Bluetooth based networks.



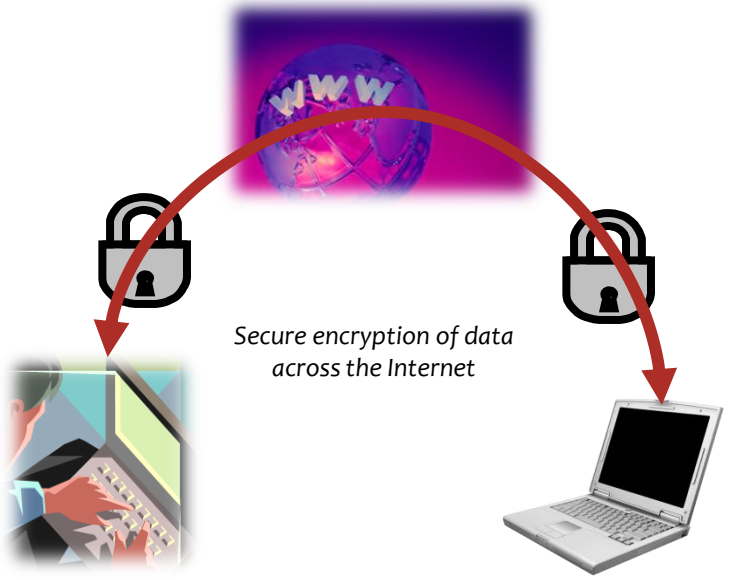
There is an array of monitoring tools available including: bandwidth monitoring tools, open source monitoring tools, network analyzers/sniffers (i.e. Wireshark), and SNMP tools.

Additional Reading
Overview of Wireshark

Remote Access

Many network administrators service networks that are not located at their work site. In these instances, administrators connect remotely to these networks. Sometimes, administrators need to access their networks remotely while on the road on personal or business trips. Fortunately, Unix/Linux systems provide very capable remote login options.

Some of the tools you may need for remote access include SSH, Telnet, Webmin (GUI based), and VNC® Remember, tools that offer greater convenience for remote access generally have lower security options. Consequently, you should be very careful when logging on to your network remotely. Check your surroundings and verify your security settings.



Review VNC and cross-platform remote connection

Summary

A Linux Administrator has an important task in configuring a network for optimal data communications with adequate security safeguards to limit access to unauthorized users and activities.

Before configuring a network, Linux administrators must decide what technologies, systems, protocols, servers, ports, and addresses will be used on the network, and each must be configured according to the procedures or rules for each operating system. Additionally, a Linux Admin must install a firewall and other network security tools to monitor the network, detect unauthorized intrusions, and limit security breaches.

Finally, an administrator may need remote access to a network so that he or she can fix, review, monitor, install, and troubleshoot problems without having to be physically present at the installation site. Linux provides many powerful tools to handle the myriad tasks that Network Administrators face.