Specialized Network Connectivity Router Devices

by Sophia

WHAT'S COVERED

In this lesson, you will examine additional network continuity devices.

Specifically, this lesson will cover the following:

1. Other Specialized Devices

While switches and routers are the primary devices that enable network connectivity, there are other devices that actively participate in moving or securing network data.

Here is a list of devices covered in this tutorial:

- Encryption devices
- Multilayer switch
- Load balancer
- DNS server
- Proxy server

1a. Encryption Devices

Encryption is the process of obscuring information to make it unreadable without special knowledge, key files, or passwords. There are dedicated appliances that can perform encryption. The advantage of using these devices is that they normally provide choices of encryption methods and very strong encryption options. They also offload the process from other devices like routers and servers, which is a good thing since the encryption/decryption process is very processor intensive and may interfere with other functions that those routers and servers might be performing.

Sometimes these devices are called **encryption gateways**. They can either sit in line with a server or a local network, encrypting and decrypting all traffic, or function as an application server, encrypting any file sent to them within a network. Examples of encryption appliances are shown in the photograph below.

While an encryption appliance is dedicated to encryption, a **content filtering appliance** scans the content of what goes through it and filters out specific content or content types. Dedicating a device to this process offloads the work from servers or routers that could do this but at a cost of greatly slowing the devices. Also, there is usually more functionality and tighter control available with a dedicated appliance.

> EXAMPLE Email is a good example of what you might run through one of these devices to filter out spam and objectionable content before the email is delivered. Another example of the use of a content filter might be to block websites based on the content of the web pages rather than on the basis of the URL or IP address.

An example of a dedicated content/URL filtering appliance is shown below.

TERMS TO KNOW

Encryption

The process of obscuring information to make it unreadable without special knowledge, key files, or passwords.

Encryption Gateway

A network device dedicated to encrypting data.

Content Filtering Appliance

A device that scans network traffic and filters out specific content or content types.

1b. Multilayer Switch

A **multilayer switch (MLS)** is a networking device that switches on Layer 2 like an ordinary network switch but also provides routing. The major difference between the packet-switching operation of a router and that of a Layer 3 or multilayer switch lies in the physical implementation.

In routers, **packet switching**, a means of directing digitally encoded information in a communication network from its source to its destination, in which messages may be divided into smaller entities called packets, each of which travels independently through the network in paths based on moment-to-moment routing decisions made by the nodes through which they pass, takes place using a microprocessor, whereas a Layer 3 switch handles this by using **application-specific integrated circuit (ASIC)** hardware. The term “multilayer switch” is also known as a Layer 3 switch, which was introduced in a previous lesson.

TERMS TO KNOW

Multilayer Switch (MLS)

A device that provides both Layer 2 switching and Layer 3 routing functions.

Packet Switching

A means of directing digitally encoded information in a communication network from its source to its destination, in which messages may be divided into smaller entities called packets, each of which travels independently through the network in paths based on moment-to-moment routing decisions made by the nodes through which they pass.

Application-Specific Integrated Circuit (ASIC)

An integrated circuit (IC) chip designed for a particular use.

1c. Load Balancer

A router delivers incoming packets to the destination IP address on the network, but a **load balancer** can actually send incoming packets to multiple machines hidden behind one IP address. Today's load-balancing routers follow various rules to determine specifically how they will route network traffic. Depending on your needs, you can set rules based on the least load, the fault tolerance, the fastest response times, or just by dividing up (balancing) outbound requests for smooth network operations. The fault tolerance, or redundancy, as well as the scalability may be vital to large networking environments and e-commerce sites.

IN CONTEXT

Consider a website where customers place orders for the stuff you have for sale. Obviously, the orders placed will vary in size and the rate at which they come. You definitely would not want your servers becoming so overloaded that they freeze up and crash your site causing you to lose lots of money, would you? That is where balancing the load of traffic between a group of servers comes to the rescue, because even if one of them freezes, your customers will still be able to access your site and place orders.

TERM TO KNOW

Load Balancer

A device that distributes network traffic to a number of servers.

1d. DNS Server

A **Domain Name Service (DNS)** server is one of the most important servers in your network and on the internet because without a **DNS server**, you would have to type http://34.197.217.64 instead of simply entering www.sophia.org. Think of the DNS system as the phone book of the internet that matches, or resolves, names to IP addresses.

HINT

A hostname is typically the name of a device that has a specific IP address; on the internet, it is part of what is known as a **fully qualified domain name (FQDN)**. An FQDN consists of a hostname and a domain name.

The process of finding the IP address for any given hostname is known as **name resolution**, and it can be performed in a number of ways. DNS is the most popular process today and is the resolution method you really need to know.

On the internet, domains are arranged in a hierarchical tree structure. The top level domain is the one at the end of the FQDN, representing the highest (that is, the most general) level. The following list includes some of the top-level domains currently in use:

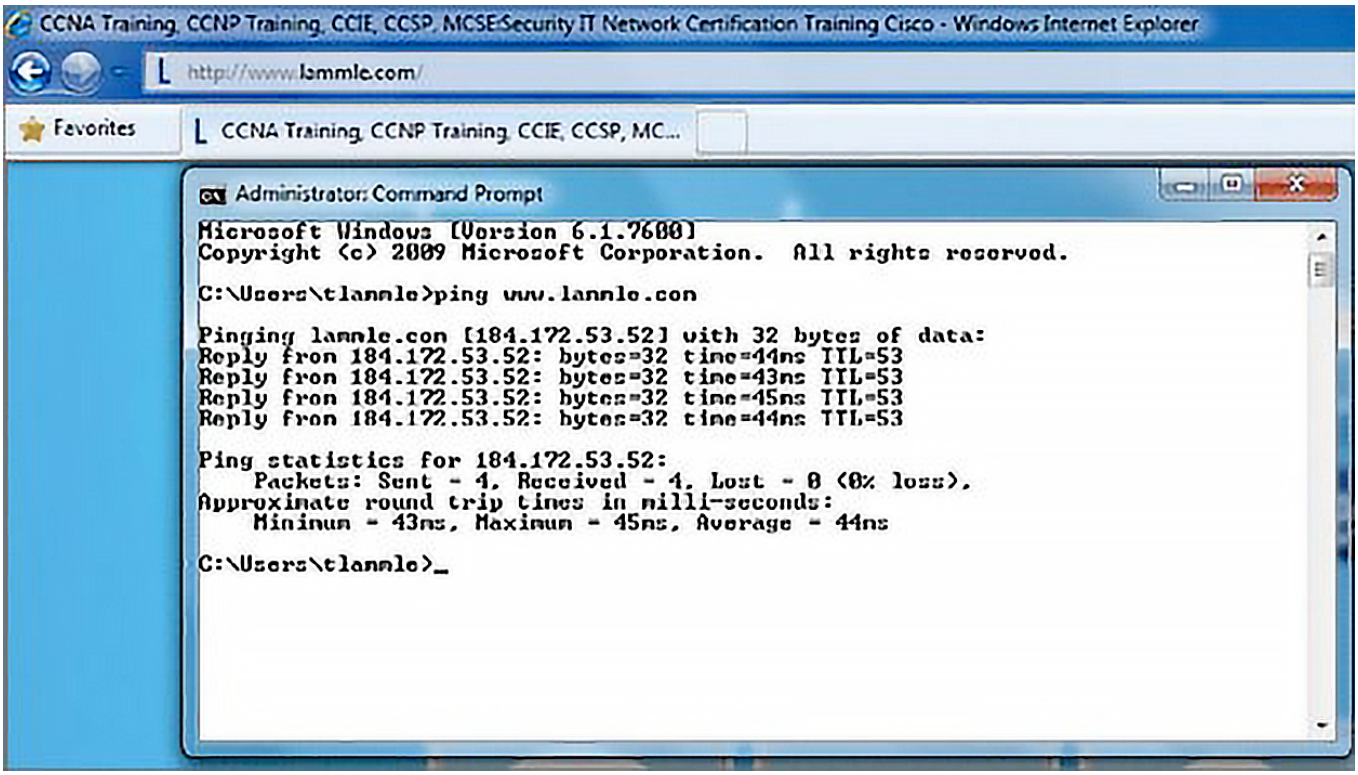
- .com: A commercial organization
- .edu: An educational establishment, such as a university

- .gov: A branch of the U.S. government
- .int: An international organization, such as NATO or the United Nations
- .mil: A branch of the U.S. military
- .net: A network organization
- .org: A nonprofit organization

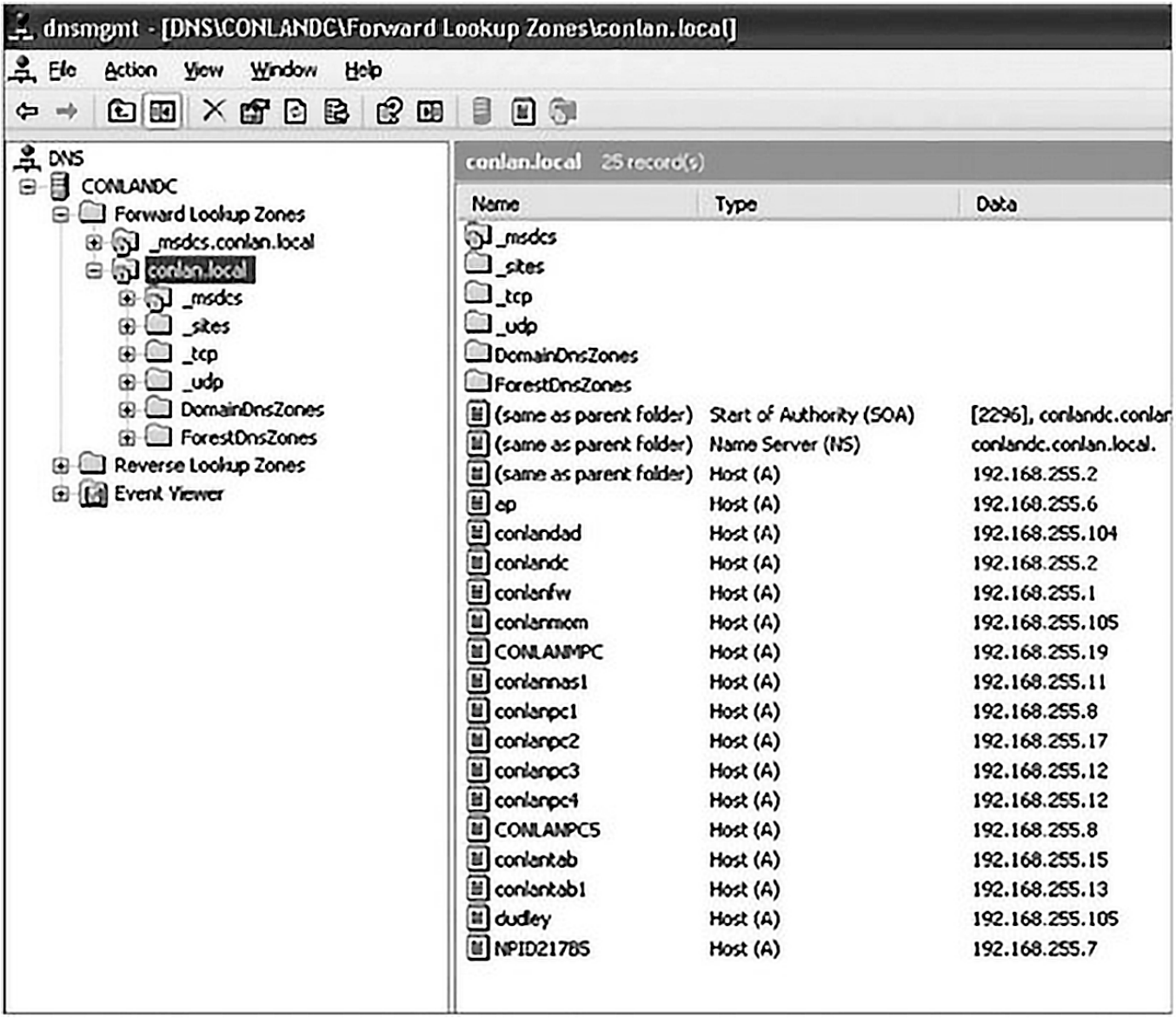
IN CONTEXT

The .com domain is by far the largest, followed by the .edu domain. Some new domain names are becoming popular, however, because of the increasing number of domain-name requests. These include .firm for businesses and companies, .store for businesses selling goods rather than services, .arts for cultural and entertainment organizations, and .info for informational services. The domains .cc, .biz, .travel, and .post are also in use on the internet.

The screenshot below shows how, when you type in a domain name, the DNS server resolves it, allowing the host to send the HTTP packets to the server.



This screenshot shows how the DNS server can resolve the human name to the IP address of the Lammle.com server when we ping the server by the name instead of the IP address. Imagine how hard life would be without DNS translating human names to IP addresses, routing your packet through the internet or internetwork to get to your servers. The screenshot below gives you an example of a Windows server configured as a DNS server.



The DNS server will resolve hostnames to correct IP addresses. This is a mission-critical service in today's networks. As shown above, if we ping from a host to CONLAND, the host will send the name-resolution request to the DNS server and translate this name to IP address 192.168.255.8. Host (A) is called an **A record** and is what gives you the IP address of a domain or host. In IPv6, it is called a quad-A or **AAAA record**. You can see that each name has an A record, which is associated with an IP address. So, A records resolve hostnames to IP addresses, but what happens if you know the IP address and want to know the hostname? There is a record for this, too! It is called the **pointer record (PTR)**.

Other typical records found on DNS servers are **mail exchanger (MX) records**, which are used to translate mail records. The MX record points to the mail exchanger for a particular host. DNS is structured so that you can actually specify several mail exchangers for one host. This feature provides a higher probability that email will arrive at its intended destination. The mail exchangers are listed in order in the record, with a priority code that indicates the order in which they should be accessed by other mail-delivery systems. There are many other types of records the DNS server keeps as well, as indicated below.

Record Type	Explanation
AAAA	Used to map hostnames to an IPv6 address of the host
TXT (SPF)	Used to provide authentication of mail sent and received by the same email system
TXT (DKIM)	Used to provide authentication of mail sent and received by the same email system
SRV	Generalized service location record, used for newer protocols instead of creating protocol-specific records such as MX
NS	Represents DNS server

If the first-priority mail exchanger does not respond in a given amount of time, the mail-delivery system tries the second one, and so on. Here are some sample mail-exchange records:

```
host.compant.com.   IN   MX   10   mail.company.com.
host.compant.com.   IN   MX   20   mail2.company.com.
host.compant.com.   IN   MX   30   mail3.company.com.
```

In this example, if the first mail exchanger, mail.company.com, does not respond, the second one, mail2.company.com, is tried, and so on.

Another important record type on a DNS server is the **canonical name (CNAME) record**. This is also commonly known as the **alias record**, and it allows hosts to have more than one name. For example, suppose your web server has the hostname www and you want that machine to also have the name ftp so that users can use **file transfer protocol (FTP)** to access a different portion of the file system as an FTP root. You can accomplish this with a CNAME record. Given that you already have an address record established for the hostname www, a CNAME record that adds ftp as a hostname would look something like this:

```
www.company.com.   IN   A       204.176.47.2
ftp.company.com.   IN   CNAME   www.company.com.
```

When you put all these record types together in a DNS table, it might look like this:

mail.company.com.	IN	A	204.176.47.9
mail2.company.com.	IN	A	204.176.47.21
mail3.company.com.	IN	A	204.176.47.89
yourhost.company.com.	IN	MX	10 mail.company.com.
yourhost.company.com.	IN	MX	20 mail2.company.com.
yourhost.company.com.	IN	MX	30 mail3.company.com.
www.company.com.	IN	A	204.176.47.2
ftp.company.com.	IN	CNAME	www.company.com.

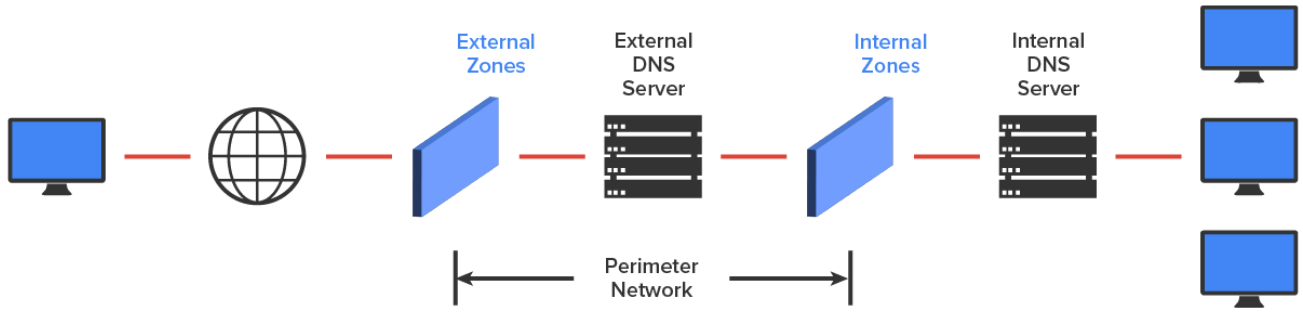
DNS is a Layer 7 (Application) protocol. DNS queries are made on UDP port 53.

Dynamic DNS

At one time, all DNS records had to be manually entered into the DNS server and edited manually when changes occurred. Today, DNS is dynamic and works in concert with the DHCP function. Hosts register their names with the DNS server as they receive their IP address configuration from the DHCP server. This does not mean that manual records cannot be created if desired. In fact, some of the record types we have discussed can only be created manually. These include MX and CNAME records.

Internal and External DNS

DNS servers can be located inside the intranet, as shown below:



When located in the DMZ, the DNS server should contain only the records of the devices within the DMZ. Implementing separate internal and external DNS servers might require you to include external resource records in the internal DNS zone.

Third-Party/Cloud-Hosted DNS

Some smaller organizations find that it makes more sense to outsource the DNS function. Rather than hire and train staff to set up, configure, and maintain the infrastructure required to keep name resolution up and secure, they might find it more cost effective to utilize a third-party vendor who makes it their business to provide this service. Cloud providers can provide you with cloud-based storage, and these same vendors can also provide you with reliable DNS service.

TERMS TO KNOW

Domain Name Service (DNS)

The services provided by the Domain Name System.

DNS Server

A computer that responds to a client's DNS request.

Fully Qualified Domain Name (FQDN)

A domain name that specifies the exact location of a host computer.

Name Resolution

The DNS process of translating a domain name to an IP address.

A Record

DNS record of the IPv4 address of a domain or host.

AAAA Record

DNS record of the IPv6 address of a domain or host.

Pointer Record (PTR)

A DNS record that indicates IP address to name mapping records.

Mail Exchanger (MX) Record

A DNS record that points to the email server for a particular host.

Canonical Name (CNAME) Record

DNS record that enables hosts to have more than one name.

Alias Record

DNS record that enables hosts to have more than one name.

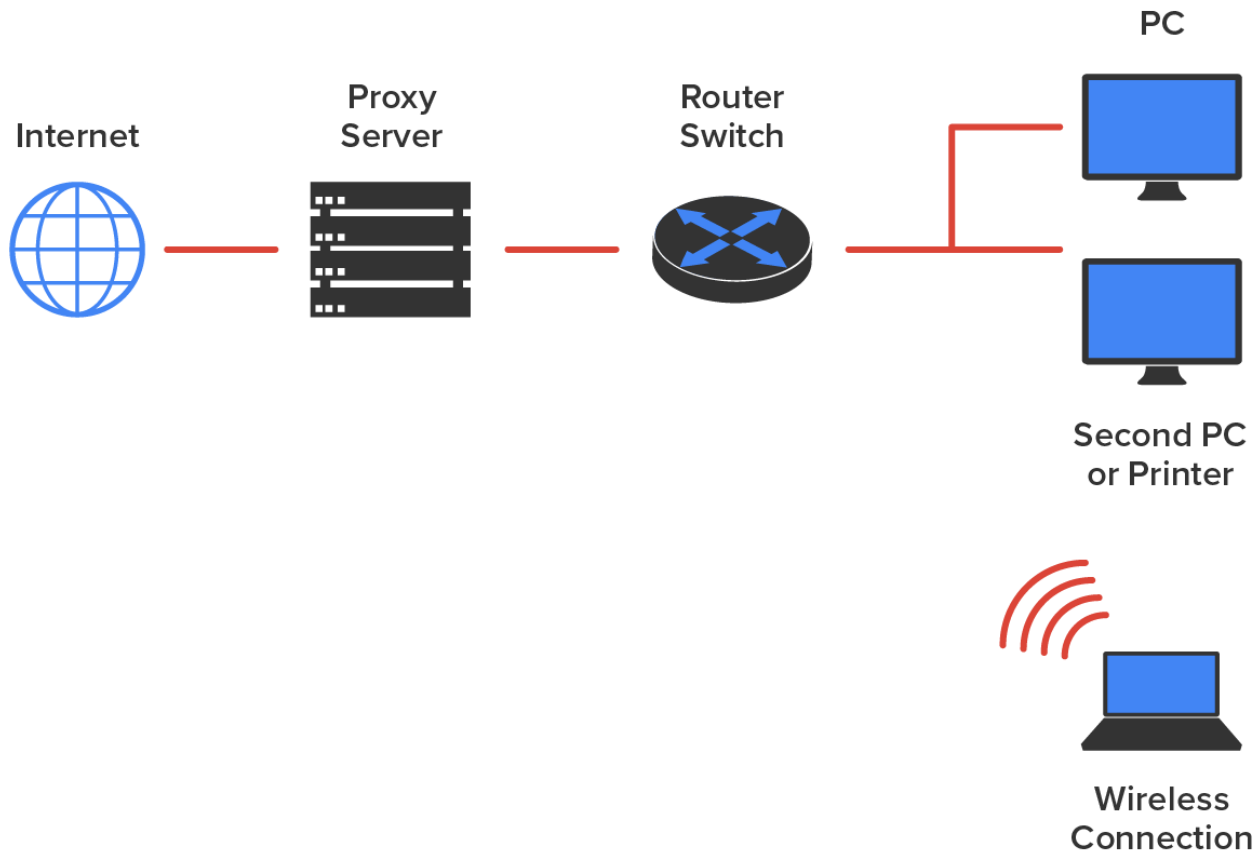
File Transfer Protocol (FTP)

A technology for transferring files over a network.

1e. Proxy Server

A **proxy server** is a type of server that handles its client-machine requests by forwarding them on to other servers while allowing a high degree of control over the traffic between the local LAN and the internet. When it receives a request, the proxy will then connect to the specific server that can fulfill the request for the client that wants it. A proxy server operates at Layer 7.

The diagram below shows where a proxy server would typically be found in a small-to-medium network.



There are two main types of proxy servers you will typically find working in present-day networks: web proxy server and caching proxy server.

Web Proxy Server
A web proxy server is usually used to create a web cache. You experience this when you Google a site you have visited before. The web proxy "remembers" you, and the site not only loads faster, it sometimes even recalls your personal information by automatically filling in your username, or even your billing/shipping information when you place another order.

Caching Proxy Server
A caching proxy server speeds up the network's service requests by recovering information from a client's earlier request. Caching proxies keep local copies of the resources requested often, which really helps minimize the upstream use of bandwidth. These servers can greatly enhance network performance.

A **reverse proxy server** takes requests from the internet and forwards them to servers in an internal network, whereas the forward proxy we discussed in this section takes client requests and sends them to the internet.

TERMS TO KNOW

Proxy Server
A server that acts as an intermediary between a user and another server, usually on the internet.

Reverse Proxy Server

A server that takes requests from the internet and forwards them to servers in an internal network.

SUMMARY

In this lesson, you learned about **other specialized network devices**, including, encryption devices, multilayer switches, load balancers, DNS servers, and proxy servers. You will continue to explore additional network devices in our next lesson.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

A Record
DNS record of the IPv4 address of a domain or host.

AAAA Record
DNS record of the IPv6 address of a domain or host.

Alias Record
DNS record that enables hosts to have more than one name.

Application-Specific Integrated Circuit (ASIC)
An integrated circuit (IC) chip designed for a particular use.

Canonical Name (CNAME) Record
DNS record that enables hosts to have more than one name.

Content Filtering Appliance
A device that scans network traffic and filters out specific content or content types.

DNS Server
A computer that responds to a client's DNS request.

Domain Name Service (DNS)
The services provided by the Domain Name System.

Encryption
The process of obscuring information to make it unreadable without special knowledge, key files, or passwords.

Encryption Gateway
A network device dedicated to encrypting data.

File Transfer Protocol (FTP)

A technology for transferring files over a network.

Fully Qualified Domain Name (FQDN)

A domain name that specifies the exact location of a host computer.

Load Balancer

A device that distributes network traffic to a number of servers.

Mail Exchanger (MX) Record

A DNS record that points to the email server for a particular host.

Multilayer Switch (MLS)

A device that provides both Layer 2 switching and Layer 3 routing functions.

Name Resolution

The DNS process of translating a domain name to an IP address.

Packet Switching

A means of directing digitally encoded information in a communication network from its source to its destination, in which messages may be divided into smaller entities called packets, each of which travels independently through the network in paths based on moment-to-moment routing decisions made by the nodes through which they pass.

Pointer Record (PTR)

A DNS record that indicates IP address to name mapping records.

Proxy Server

A server that acts as an intermediary between a user and another server, usually on the Internet.

Reverse Proxy Server

A server that takes requests from the Internet and forwards them to servers in an internal network.