Chapter 1

Enterprise Network Design

IN THIS CHAPTER, YOU WILL LEARN HOW TO DO THE FOLLOWING:

✓ Compare methodologies used to design a network
✓ Identify network requirements to support the organization
✓ Describe the Enterprise Composite Network Model
✓ Describe the Cisco Services-Oriented Network Architecture
I start off by showing you the components and practices that will allow you to design and implement a network—not just any network, but the perfect network for a given situation. It will be properly sized and have high availability features throughout. All of the devices will be chosen with the proper resources for the load they will carry. I introduce some design models to help you understand how to connect those devices together and help you ensure that it can grow and remain stable in the future. Basically, you will find out how to make a network that is high speed, low drag, and leaves you the hero. Hopefully with a raise!

For up-to-the-minute updates on this chapter, check out www.sybex.com/go/CiscoProGuidetoInternetworking or www.lammle.com.

The Three-Layer Hierarchical Design Model

For years, the three-layer model has been used to design and evaluate networks with a good amount of success. The three-layer model, as shown in Figure 1.1, provided you with three design areas. The three layers are the access, distribution, and core layers. Using a layered approach allows a network designer to logically define the network in terms of functions and devices. The result is a network that can be easily managed and has deterministic failure built in.

**Concept: Deterministic Failure**

Although no one wants a device or link to fail, every seasoned network administrator knows that failures occur. Deterministic failure allows you to implement secondary or standby devices to take over for a failed primary or permits a redundant link to relieve the traffic load for a downed link. Deterministic failure allows you to predict exactly how a network will respond when a device or link fails.
Access Layer  The access layer connects all of the hosts and user workstations. This layer uses switches with high port density or the lowest cost per port device. The switch devices in this layer should also have the ability to make or use higher speed uplinks to the other layers. Depending on the switch platform that is used, there might be built-in uplink ports that have greater bandwidth capacity. It may also be necessary to create and use EtherChannel links from the access layer to the other layers. Those uplinks should be redundant so that the loss of any one link does not prevent the traffic from getting out of the access layer. Normally, the redundant connections in the access layer are Layer 2 connections, which means Spanning Tree Protocol (STP) controls the forwarding and blocked links preventing loops in this area of the network. I discuss STP in Chapter 3, “Spanning Tree Protocol.”

Concept: EtherChannel

EtherChannel is a feature that allows you to bind together more than one interface, which gives the switch a higher bandwidth connection between devices. I cover EtherChannel later in Chapter 2, “Switching.”

Distribution Layer  The distribution layer serves as the aggregation point for all of the access layer networks and devices. Filtering and security are implemented here. It is the point in the network where routing and filtering decisions are made. Features such as quality of service (QoS) policies, access control lists (ACLs), and route filtering should also be placed at this layer.
Distribution layer devices must have the capacity to process and forward traffic from all of the connected devices. Here, you will find all the redundant connections from access layer devices, as well as redundant connections to the core layer.

Core Layer  The core layer primarily provides high-speed transport for data. There should be very little manipulation of the data in this layer. No filtering or access lists are found here. All of the connections in and out of the core layer should be redundant for high availability. The redundant links in the core layer and down to the distribution layer devices are usually routed or Layer 3 links. Having a routing protocol determine which links are used makes the time to transition from the primary link to the secondary link much shorter than when STP is being used. I discuss this difference later in the chapter.

You might be asking right now, “What if my network isn’t large enough for all of those layers?”

Well, that is a very good point. Not all networks require all three layers. In fact, many small- and medium-sized networks are designed with only two. The functions of all three layers still exist and are still necessary. In these networks, the distribution and core layers are pushed together in what is called a collapsed core design. The collapsed core design allows for a simplified and cost effective network.

The three-layer model has been very successful due to its simplicity. However, the requirements for networks today have increased tremendously and require a more detailed and feature-rich model for design. This complexity has brought about the Enterprise Composite Network Model.

Enterprise Composite Network Model

The Enterprise Composite Network Model was introduced to provide a more detailed strategy for designing networks. Previous design models did not define how to make specific connections or how the network should expand over time. Networks, therefore, grew with no direction. Network administrators had little control over the way networks reacted to change.

To ensure that this doesn’t happen to your network, I’m going to show you some design practices and components that will give you a scalable and highly available network for years to come. We all need job security and these techniques will make you the rock star of your network!

The Enterprise Composite Network Model is based on the three-layer model. The new model is broken into more pieces, so we can more easily define their function and physical connections. Figure 1.2 shows the areas of the model that I’ll cover.

In the Figure 1.2, you can see that the design model has three main pieces or modules.

- Enterprise Campus
- Enterprise Edge
- Service Provider Edge
Each of these pieces is further divided to define specific distinct functions for the network.

**FIGURE 1.2** Enterprise Composite Network Model

The Enterprise Campus section of the network is the real meat and potatoes in the design. It houses all of the local area networks (LANs). LANs start by connecting the users and end devices. Connecting LANs gives a path through the network to the core or backbone, which provides a central connection point for everything in the network. In the following sections, I’ll introduce you to each of the components that make up this area of the network. Figure 1.3 shows the components in the Enterprise Campus Module.
Campus Infrastructure Module

The Campus Infrastructure Module is really made up of two primary building blocks for a network: the switch block and the campus core.

A switch block is often referred to as a building switch block because a campus with multiple buildings often has a separate switch block for each building. The switch block is a combination of the access layer and the distribution layer for a particular part of the network. The part of the network that a switch block represents depends on a couple of things, first of which is the number of users or end devices in the switch block. The second major factor is the type and amount of traffic that will be transmitted through it. I’ll cover the different types of traffic and the effects on the network in much greater detail later in the book.

The second piece of the Campus Infrastructure Module is the campus backbone. Like the core block described in the three-layer model, the campus backbone is in place to transport data as quickly and efficiently as possible. It is the central point in the network and carries all of the traffic from the building switch blocks, edge block, and server farm block. Since it will carry all of that traffic, the backbone must be sized to handle at least the sum of traffic that all of the distribution switches carry. The backbone of a network today is often implemented as a Layer 3 (the network layer in the open-systems interconnection (OSI) model) or routed core. With the vast improvements in multilayer switches in recent years, there is not the huge performance loss using a routed solution. I’ll tell you about the benefits of multilayer switches in Chapter 2, “Switching.” A routed core provides link redundancy and failover. Routing protocols have the ability to load balance across multiple links and utilize whatever path may be left after a failure. The benefit of using multiple links is not the only thing a Layer 3 core provides. Routing protocols give much more control in determining what links will be used when
a failure occurs, and the time a routing protocol takes to fail over the link is much shorter than what spanning tree protocol (STP) can provide in a Layer 2 solution.

**Network Management Block**

The next component in the Enterprise Campus is the Network Management Block. Enterprise networks today, with their vast number of devices and services, must be managed with a management tool or an entire suite of tools and applications. In the past, a management network or virtual local area network (VLAN) that spanned the entire network was setup for monitoring and management. In today’s networks, however, spanning a single network or VLAN across the entire network is considered poor practice. It provides no way to control the amount of traffic that would be going across every layer of the enterprise. To prevent this practice, it is now recommended that management addresses and subnets be assigned to all of the devices being monitored. Some devices can be configured specifically with the addresses and names of the management devices that will be monitoring them. Others though will have to be configured with access lists and filtering so that they only allow management devices from a specific subnet to access them. This allows all of the management applications to be located within the management block and still be capable of monitoring the devices across the enterprise. Some of the most common items included in the management block are:

- Monitoring applications
- Security management, policy, and intrusion detection
- Alarm and logging servers
- AAA servers (for authentication, authorization, and accounting)

**Server Farm Block**

The Server Farm Block allows for the physical collocation and consolidation of most, if not all, of the servers and applications that the vast majority of users in the enterprise will access. The Server Farm Block, like the other blocks, needs redundant connections between the access switches and the distribution switches, and between the distribution switches and the core switches. However, with the high availability of the servers and applications in this block, the hosts, which are the servers in this case, will also have redundancy built in. Most servers today can be multihomed. A multihomed server has at least two separate connections to the network. In this case, the server could have a separate connection to two different switches in the block, allowing it to have redundant paths should any one device fail.

**Enterprise Edge**

The Enterprise Edge is truly another switch block. It connects to the campus core in the Enterprise Infrastructure with redundant links and redundant distribution switches, just as any other switch block in the network would. The difference between this block and the other blocks is in the devices that you put into the Enterprise Edge. The Enterprise Edge provides connections out of the Enterprise network. Those connections fall into a few different categories and each category defines the type of device that will be placed
there. Let’s take a look at each of the different categories that make up the foundation for this block.

**Internet Connection** The first and most common type of connection in and out of the enterprise is an Internet connection. This connection provides access for all enterprise users to external web servers, e-mail, and any other public service. Depending on the importance and the amount of traffic going in and out to the Internet this connection can be redundant. The amount of bandwidth that you get for this connection is most often determined by the amount of money that you are willing to spend. The bandwidth of a connection is determined by the service provider and usually comes in increments—the more you pay, the wider the bandwidth.

**WAN Connection** The wide area network (WAN) connection provides access to other locations throughout the enterprise. Branch offices and other remote sites, located too far away to install and maintain your own cables, will have WAN connections installed between them and the rest of your enterprise. Again, bandwidth and connection types vary based on the amount of money that you want to spend, but they can also differ based on the type of connection available from a service provider in the city where the branch office is located. Many types of WAN connections can be purchased today; some of them have been around for a very long time. They can include frame relay, asynchronous transfer mode (ATM), leased lines, integrated services digital network (ISDN), and multi-protocol label switching (MPLS). I tell you about MPLS in Chapter 11, “WAN and Teleworker Connections.” I don’t spend a lot of time describing the other technologies, but you should have learned about frame relay and leased lines when you were studying for the Cisco Certified Network Associate (CCNA) certification.

**Remote Access Connections** The remote access connections usually refer to dial-up connections that can be made into the network. These connections allow remote workers to gain access to enterprise resources while away from the office. This type of connection is made over the public switched telephone network (PSTN).

**VoIP Connections** Since I am talking about telephone lines and connections made to a phone company, it is important to realize that the internal enterprise phone system still requires external phone line connections. External phone connections will be made at this location in the network if you have a voice over IP phone (VoIP) system. The VoIP system still requires you to have outside lines connecting it to the outside world. These lines allow calls made to a number that is not internal or on the enterprise phone system.

**VPN Connections** The last type of connection I want to mention is hopefully replacing most of the dial-up connections that users have made for years. Virtual private network (VPN) connections provide a secure tunnel in which to pass data from a remote site or user to the enterprise edge. The secure tunnel is carried over an unsecure or untrusted network. Most often, that network is the Internet. Using a VPN, a simple and cheap connection can be made to the office. The flexibility it gives users is also a huge benefit. Almost anywhere a user can get a connection to the Internet, they can have a secure tunnel back to the office to access e-mail and other resources. Now, whether they view this ability as a benefit or a leash connecting them 24/7 to work, that is up for discussion.
Service Provider Edge

The service provider edge is often a network engineer’s favorite part of the entire network design. This piece of the design model is here to signify where the physical connections to various service providers terminate. There is very little or no equipment in this module that must be maintained by you or your enterprise network engineering team. Other than the occasional disagreement with a service provider about whose fault an outage was, there shouldn’t be anything that you have to do or maintain here.

IIN and SONA

IIN or Intelligent Information Network is more of a vision for future design and implementation strategy in a network. IIN combines the functions of applications and the network, allowing the network to make better and smarter decisions about how to move and direct traffic. By placing some of the intelligence in the network, it reduces the amount of influence any one application has to have on the network. The enterprise composite model is the basis for the IIN to be built on. The IIN adds functionality to what the network already does. IIN is described in a three-phase approach.

Phase 1  Integrated system describes the intelligent movement of data, voice, and video across a system of networks. It is where the underlying composite designed network is used.

Phase 2  Integrated services describe virtualized networking resources. Their usefulness has become apparent in the shift to using virtual servers and storage. It also extends past just the use of virtualized servers and moves into network devices. You can already begin to see single devices such as routers and firewalls with the ability to appear and operate as multiple virtual instances, replacing what would have been a group of many individual devices.

Phase 3  Integrated applications or application-aware networks and services are the parts of phase 3. We can already witness the beginning of where this exciting idea can go. Through the use of Network Admission Control (NAC), the network can detect a host machine attaching to the network. From the point of connections, NAC can authenticate; scan the host for antivirus software, which can be checked to make sure it is up to date; and then configure the physical port to access the appropriate VLAN to which the device should be connected. This process enables the network devices to grant and authorize access only when a device authenticated. All of those functions can be controlled through central policies. In the past, each of those functions would have been controlled and configured separately, making their management an administrative nightmare.

SONA or Services-Oriented Network Architecture is the true implementation strategy for IIN. SONA has three layers of implementation that correlate to the three phases on IIN. Those layers are listed here in order respective to phase 1 through 3 of the IIN.

- Network system layer
- Integrated network service layer
- Application layer
Case Study: FutureTech Corporation

In today’s networks, you have to know many different technologies and functions. Keeping track of where in the network items are used and deployed can become difficult. Many of the functions have dependencies, so you’ll need to track those relationships to each function. Some of the processes you run can be on independent devices, and keeping track of the fact that they may not play well with other devices can be a real pain in the neck. To aid you in keeping track of where in the network you plan to deploy and implement all of the technologies covered in this book, I’m going to use a single enterprise network example. For this purpose, I created a fictional company named FutureTech Corporation. The name and all examples of this company are entirely fictitious and do not in any way represent a real company, named or otherwise.

FutureTech will serve as the basis of our case study. As I move you through each topic in the book, I will relate back to this overall network example to better show you where in a real network a technology can be used and for what specific purpose.

I am going to ask you, the reader, to put yourself in the place of a senior network engineer for FutureTech. As I move through the technologies in this book, you can think about designing this network, basically from the ground up. The design process that I am going to take you through will be somewhat of a parallel path using two design guides everyone should be now familiar with. I am going to use the OSI model as the first guide, starting off at Layers 1 and 2, then moving through the layers to add applications and new technologies to the network.

As I start building the network with the OSI model, the second guide will be the Enterprise Composite Network Model. Since the fundamental building block of the enterprise model is the switch block, my discussion starts there. I’ll show you how the different types of switch blocks will be built layer by layer.

Book Organization

With that in mind, this book begins with the OSI model. I start with switching (Layer 2) that has Layer 1 connections and cables scattered through it. Then, I go through the routing and all of the routing protocols. The routing chapters help tie the layers of a switch block, allow me to show you how the switch blocks will be linked, and ultimately bring you into the core of the network.

Following the routing protocols, I cover a couple of other Layer 3 functions that, if not now, will soon be placed into all enterprise networks. These topics include Internet Protocol version 6 (IPv6) and multicast routing. I immediately follow those protocols with WANs, VPNs, and remote access connections. This will tie another switch block, the Enterprise Edge, into the network. You will see how all of those services are provided and brought into the enterprise.

After all of the switch blocks have been built, I continue up the OSI model, adding services and higher layer functions into the network. Some of the later topics may actually reside or use protocols in lower layers of the OSI; however, you need a good foundation in the network design before you can add them into your network.
At this point, you will add security to the network. Most of the network’s framework will be constructed, and you need to make sure that it is secure and protected from possible attack. I cover securing Layer 2 and the associated devices followed by the same for Layer 3 and the devices found there. You will learn how to configure the internetwork operating system (IOS) Firewall and intrusion prevention system (IPS) services on a router.

Once your security is in place, I take you through some network convergence and traffic management topics. Many of you have or soon will be adding voice traffic and applications to your network and you will have to understand the effects of that traffic to properly finish the design.

Finally, I round out the book with wireless local area network (WLAN) functions. I discuss WLAN last not because it is a higher layer protocol or function, but because again not everyone uses or implements wireless technologies. However, a lot of new and exciting enhancements can be made to networks today with the use of wireless devices.

**FutureTech Company Background**

FutureTech is a globally scaled, advanced, technology company. The company designs, develops, and distributes thousands of products for businesses and government agencies all over the world.

Figure 1.4 gives you an overall view of where the company headquarters, primary offices, branch offices, manufacturing plants, and remote offices are located. Notice that the FutureTech enterprise network includes:

- VPN connections for branch offices and remote users
- Multi-protocol label switching (MPLS) connections for its WAN connections
- Redundant connections to separate Internet service providers (ISP) that provide high availability to the enterprise

**Enterprise Network Design Details**

From that broad overview, the company can be broken into smaller pieces with the different technologies applied. By technologies, I mean all of the concepts I cover through the course of this book. I start at the bottom of the OSI model and in the Enterprise Campus module of the composite design model. The enterprise network will have multiple switch blocks, but most of them have similar design topics and all of them have access and distribution layer devices and protocols.

**Layers 1 and 2**

Using a global company gives the ability to use and see just about every technology that a network administrator could want. I start out by showing you a small single piece of the network. That small piece is typically called a switch block. Remember that a switch block is usually a single building on a campus setting or a whole floor in a large building. It might even be a branch office or department-size piece of the network.
Starting in this small setting, you will be able to explore access and distribution layer devices. I can also begin showing you Layer 2 functions, since the access layer is primarily made up of Layer 2 switches. I’ll show you the protocols and functions that you can use to connect them and provide resiliency and availability. Through the course of the book, I will cover the most common network devices in detail and show you how to configure them.

In the access layers of the network, port density—meaning the number and amount of users and data that can be taken into the network—is the issue that most concerns network administrators. Many different types of switches can be used to address this issue.

Each of the different parts of the network has different numbers of users. The headquarters building, for instance, could have as many as 25,000 users. With that number of people, a network could have between 10 and 50 switch blocks depending on how you break up the users. Moving through the other size buildings, offices, and the branch offices, the number of users is obviously going to be different. Each could have as few as 100 to 500 users; with this number of users the network may require only a single switch block to connect the entire building.
As you go through the book, I show you how to configure even these Layer 2 devices for security, quality of service (QoS), redundancy, voice, and other types of converged traffic conditions. You will see how these devices handle different types of traffic, as well as the effects on all of the other devices you implement. You will also have to think about the load each device will have to accommodate.

**Layer 3**

Moving from the access layer specifically into the distribution layer brings other challenges and more protocols to explore. Most common will be the wide range of routing protocols. Routing protocols allow you to connect all of the networks and VLANs in the access layer. I will walk you through the most common routing protocols, starting off with distance vector protocols such as routing information protocol (RIP) and interior gateway routing protocol (IGRP). You will see how they can be used in smaller networks or in places where you need to keep the overhead on a router's processor down.

In areas of the network where administrators have to plan for much larger deployments with more routers and more connected networks, I show you how to use enhanced interior gateway routing protocol (EIGRP), open shortest path first (OSPF), and integrated intermediate system to intermediate system (IS-IS). Each of these protocols has distinct benefits and drawbacks. For example, EIGRP has the ability to provide fast convergence and loop-free operation, as well as routing for multiple network layer protocols. However, it is a Cisco proprietary protocol and can only be run in a homogeneous Cisco environment.

**Core Layer or Backbone**  

The backbone of the network is supposed to move data as fast as possible without changing it. So at this point, I’ll show you the different ways to configure the core of the network and the advantages and disadvantages of each. In the past, the core of the network was always a Layer 2 structured design. I will show you some of the ways a Layer 3 setup can provide a more deterministic flow of traffic and increase reliability when there is a failure. You will see how STP handles a link that has gone down, and then compare that to the way a routing protocol handles the same link failure.

**Enterprise Edge**  

Moving out of FutureTech’s primary internal infrastructure into the service provider’s network requires an understanding of how and where to make external connections. Those external connections fall into the Internet, WAN, and remote access/VPN categories. Many companies today use connectivity that differs from the traditional WANs of years past. One of the most common types of new connections is the VPN. VPNs can be used to connect branch offices and home offices to the primary enterprise. VPN client software loaded on almost any personal computer or laptop can give a single user the ability to connect to the enterprise from almost anywhere they have an Internet connection.

**Internet Connectivity**  

Internet connectivity might require you to route between your network and the ISP. In this case, I’ll show you the uses and complexities of border gateway protocol (BGP). You’re probably already aware that BGP is a routing protocol that falls into the exterior gateway protocols (EGP) category. With the decision to use BGP comes a much larger responsibility and the need for a working knowledge of its operation. Being that FutureTech has redundant Internet connections and multiple ISPs, the use of BGP will allow the network a much more consistent presence on the Internet, as well as higher availability.
Wide Area Network (WAN)  Of course, while considering ISP connections, I will talk about ways to connect parts of the FutureTech network. Traditionally, these connections are made using WAN protocols such as frame relay or dedicated circuits like T1 and T3. I'll help you explore a newer and nontraditional connection type; that newer type of WAN offering is MPLS. MPLS isn't available in all geographic areas or through all service providers, but it can be obtained from more and more ISPs all the time. MPLS has many of the same characteristics of older protocols but with a bunch of new benefits. Some of the benefits are not immediately apparent to the customer or even in your network, but they allow the ISP to make service offerings that were either not possible before or were much more costly and complex to implement. These services allow users to make connections and move data between sites and other companies in ways that were not possible with other protocols.

Virtual Private Network (VPN)  Many of you, I am sure, have at least heard of VPNs, but maybe you haven’t used them. You will see how they connect people and networks like never before. VPNs provide a way to connect remote users and offices with much greater bandwidth and service than they ever had with dial-up. You’ll also get a look at how a VPN can provide a different way to make a WAN connection. These VPN connections can serve as a primary connection or a backup connection to an already existing WAN circuit of a different type. How and where to use them depends on load constraints and the importance of dedicated bandwidth.

---

Concept: VPNs

I want to make a quick distinction between the two different types of VPNs. Most people are at least vaguely familiar with a security VPN, a VPN that is secured with the use of a protocol such as internet protocol security (IPSec). There is another type of VPN, primarily used by service providers, that is a multiprotocol label switching (MPLS) VPN. Service providers use MPLS VPNs to separate and manage traffic as it travels across their network to different customers.

Security, Convergence, and Upper Layer Applications

At this point in the design, you will learn to add features to the framework that you have built up to now. The complexity and high use of networks today requires that you efficiently manage and keep secure every piece of the network. The different kinds of traffic that you could experience on a network will have their own challenges and requirements. I will explain the many different security, management, and convergence features that are available.

Network Management and Security  Because there are so many types of traffic to be handled and many new regulations to be adhered to, the topic of security is more important than ever. So, to make the task of securing your network easier and less error prone, new features are built right into the routers and switches that you use every day. These new features include
one-step lockdown wizards, fully configurable stateful firewalls, and intrusion prevention systems. All of these run on our good ol’ routers and switches.

In addition to the configurable security features, routers and switches now have the ability to generate alerts and warnings when less than desirable conditions exist. All of those messages can be sent to management stations for proper action and documentation. To get these messages sent, you have to add a few other configurations, so I will show you how to set up logging, authentication, authorization, and accounting. The authentication, authorization, and accounting functions are also known as AAA for short. Additional protocols facilitate their actions. I will cover remote dial-in user service (RADIUS) and terminal access control access control service plus (TACACS+).

Converged Data and Traffic Management I have already mentioned a couple of the other exciting things that are going to be added into the FutureTech network. Voice traffic will require some extra configurations on the switches and routers. It will most likely require the use of quality of service (QoS). There will also be some discussion about where all the backend voice equipment will be placed and the requirements for those devices.

Looking to the Future

FutureTech as a whole will have to consider and plan for other types of traffic, as well as changes that are coming in the information technology (IT) industry. The requirement to provide more data and different kinds of data is becoming more important and more of a challenge every day. Like your fictional counterparts, you have to be on top of all things that are changing and new. A huge change that is not far on the horizon is Internet Protocol version 6 (IPv6). We work in a great field that is always giving way to better things and new ways to do them. It can be exciting if you like a challenge or get bored doing the same thing all of the time like I do!

Multicast and Video With a global company, you know there are going to be a bunch of meetings (pointless or otherwise). It will be up to you to make sure everyone can attend. That could mean some new cool video equipment to play with! Along with video and some other cool applications, like online training and webcasts, comes the need to transmit data a little differently. It requires sending a large amount of data out onto the network so many people can access and use it. A ton of bandwidth will be needed unless we use something called multicast. Multicast provides just what is needed; it sends a large volume of data to a group of end users or devices in a single stream of data.

Internet Protocol version 6 (IPv6) Internet Protocol version 6 (IPv6) is the next generation of network layer protocols. It provides many benefits over the current Internet Protocol version 4 (IPv4) that is in use today. The most prevalent of the improvements is the size and number of available addresses in the address space. IPv4 uses 32-bit addresses that provide a maximum of 4.29 billion addresses and, out of those addresses, fewer than half are actually usable. With IPv6 you have a 128-bit address, which provides a maximum number of $3.4 \times 10^{38}$ addresses. Yes, that is a ton of addresses. In fact, it is thousands of addresses for every person. You will be able to have your computers, phones, cars, televisions, refrigerators, and toasters
on the Internet. Well, maybe we don’t need the toaster, but if I could remotely make toast that could be cool!

I show you how to implement IPv6 into enterprise networks. It is going to take more than a one-night maintenance window to get this done. For that reason, I show you a few migration techniques that you can use to help make the transition less painful and more deliberate. Three of them will be covered in a little more detail:

- Dual stacking
- Tunneling (manual and automatic called 6to4 tunneling)
- Network Address Translation - Protocol Translation (NAT-PT)

### Concept: NAT-PT

This type of NAT is not like the NAT in IPv4, where one IPv4 address is translated to another. This is protocol translation that allows translation between IPv4 addresses and IPv6 addresses.

---

**Wireless Local Area Network (WLAN)** Another fast-growing area in enterprise networking is the use of wireless local area networks (WLANs). Wireless networks have more presence and available devices than ever before. I will help you explore the entire new line of devices that make configuration and management of WLAN environments much simpler and consistent to implement. As with anything, but especially for WLAN, security is a huge concern. The transmission of data on a wireless network is unbounded. There is less control over where the transmission is being sent. You don’t have to worry about an attacker sitting in the parking lot and just listening to data that is passing over a wire like you do with wireless data. I’ll help you look closely at the security considerations of deploying wireless devices.

### Test Network

Now, you can’t just start turning on all of these things in a production network. A test environment suitable for practicing and testing is needed. For the purpose of a test network for FutureTech, I have set up a network topology. The test network, as I will refer to it from here on out, is primarily a group of routers and switches that are connected, basically in a full mesh setup. This configuration allows all the different configurations and technologies to be tested without messing up any real production networks. Figure 1.5 shows you a network diagram of the primary test network.

The information in Table 1.1 will help you keep track of all of the connections between the devices.
**FIGURE 1.5** FutureTech Test Network Diagram

**TABLE 1.1** Connections between Devices for Test Network

<table>
<thead>
<tr>
<th>Source Device and Interface</th>
<th>Destination Device and Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch1 - Fa0/1</td>
<td>Router1 - Fa0/0</td>
</tr>
<tr>
<td>Switch1 - Fa0/2</td>
<td>Router2 - Fa0/0</td>
</tr>
<tr>
<td>Switch1 - Fa0/3</td>
<td>Router3 - Fa0/0</td>
</tr>
<tr>
<td>Switch1 - Fa0/4</td>
<td>Router4 - Fa0/0</td>
</tr>
<tr>
<td>Switch1 - Fa0/5</td>
<td>Router5 - Fa0/0</td>
</tr>
</tbody>
</table>
**Table 1.1 Connections between Devices for Test Network (continued)**

<table>
<thead>
<tr>
<th>Source Device and Interface</th>
<th>Destination Device and Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch1 - Fa0/6</td>
<td>Router6 - Fa0/0</td>
</tr>
<tr>
<td>Switch1 - Fa0/9</td>
<td>Router7 - Fa0/0</td>
</tr>
<tr>
<td>Switch1 - Fa0/10</td>
<td>Router8 - Fa0/0</td>
</tr>
<tr>
<td>Switch1 - Fa0/11</td>
<td>Router9 - Fa0/0</td>
</tr>
<tr>
<td>Switch2 - Fa0/1</td>
<td>Router1 - Fa0/1</td>
</tr>
<tr>
<td>Switch2 - Fa0/2</td>
<td>Router2 - Fa0/1</td>
</tr>
<tr>
<td>Switch2 - Fa0/3</td>
<td>Router3 - Fa0/1</td>
</tr>
<tr>
<td>Switch2 - Fa0/4</td>
<td>Router4 - Fa0/1</td>
</tr>
<tr>
<td>Switch2 - Fa0/5</td>
<td>Router5 - Fa0/1</td>
</tr>
<tr>
<td>Switch2 - Fa0/6</td>
<td>Router6 - Fa0/1</td>
</tr>
<tr>
<td>Switch2 - Fa0/9</td>
<td>Router7 - Fa0/1</td>
</tr>
<tr>
<td>Switch2 - Fa0/10</td>
<td>Router8 - Fa0/1</td>
</tr>
<tr>
<td>Switch2 - Fa0/11</td>
<td>Router9 - Fa0/1</td>
</tr>
<tr>
<td>Switch1 - Fa0/19</td>
<td>Switch2 - Fa0/19</td>
</tr>
<tr>
<td>Switch1 - Fa0/20</td>
<td>Switch2 - Fa0/20</td>
</tr>
<tr>
<td>Switch1 - Fa0/21</td>
<td>Switch3 - Fa0/21</td>
</tr>
<tr>
<td>Switch1 - Fa0/22</td>
<td>Switch3 - Fa0/22</td>
</tr>
<tr>
<td>Switch2 - Fa0/7</td>
<td>Switch3 - Fa0/7</td>
</tr>
<tr>
<td>Switch2 - Fa0/8</td>
<td>Switch3 - Fa0/8</td>
</tr>
</tbody>
</table>
### Table 1.1 Connections between Devices for Test Network (continued)

<table>
<thead>
<tr>
<th>Source Device and Interface</th>
<th>Destination Device and Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAN Router - S1</td>
<td>Router1 - S0/0/0</td>
</tr>
<tr>
<td>WAN Router - S2</td>
<td>Router2 - S0/0/0</td>
</tr>
<tr>
<td>WAN Router - S3</td>
<td>Router3 - S0/0/0</td>
</tr>
<tr>
<td>WAN Router - S4</td>
<td>Router4 - S0/0/0</td>
</tr>
<tr>
<td>WAN Router - S5</td>
<td>Router5 - S0/0/0</td>
</tr>
<tr>
<td>WAN Router - S6</td>
<td>Router6 - S0/0/0</td>
</tr>
<tr>
<td>WAN Router - S9</td>
<td>Router7 - S0/0/0</td>
</tr>
<tr>
<td>Router1 - S0/0/1</td>
<td>Router3 - S0/0/1</td>
</tr>
<tr>
<td>Router7 - S0/0/1</td>
<td>Router8 - S0/0/0</td>
</tr>
</tbody>
</table>

In Table 1.2, you can see a list of the actual device models that I use in the test network.

### Table 1.2 My Equipment List

<table>
<thead>
<tr>
<th>Test Network Device Name</th>
<th>Device Model or Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routers 1 through 9</td>
<td>Cisco 2811 ISR with WIC-2T interfaces</td>
</tr>
<tr>
<td>Switches 1 through 3</td>
<td>Cisco Catalyst 3560 24 port</td>
</tr>
<tr>
<td>WAN router</td>
<td>Cisco 2522 router with 8 serial ports</td>
</tr>
</tbody>
</table>

A caveat about the devices that I used in the test network: if you don’t have access to exactly the models of routers that I have used, that is okay. I am going to give you some pointers about other devices that you can use as replacements. I have chosen this topology and these devices for flexibility and the gear’s ability to be used for most any test configuration you might need. By that, I mean this network allows you to test all the configurations in this book, and is perfect for future studies all the way to Cisco Certified Internetwork Expert (CCIE) Routing and Switching and CCIE Service Provider.

**Switches** I used the 3560 switches because they will support all the functions you might need, even for CCIE. You could use a 3550 switch, but it won’t support all of the QoS and
IPv6 functions needed for the CCIE. The switches in your test setup must be multilayer switches with the proper code to support all the routing protocols.

Here is one thing that might save you just a little cash. Cisco has made a great 3560 switch that only has eight ports. It has all the same functionality, but costs less because it is smaller. However, you only have eight ports and an uplink, so with the number of routers I use in the examples and trunk links to the other switches, you won’t have enough ports. You could scale down the size of the test network, though, to make this switch a cost-effective solution.

**Routers** The routers are a little more difficult. By more difficult, I mean it is harder to explain why I chose these particular models and present all of the options to consider when choosing your router models. There are quite a few router models that are okay for use. This is good as, hopefully, it means having more of them available to you.

The biggest differentiator to look for is whether the router runs a 12.4 version of code. Version 12.4 is the newest version of code and supports all of the functions you need to study. The other big thing, both for the exercises in this book and for studying for your Cisco Certified Network Professional (CCNP) certification, your router will have to support the Secure Device Manager (SDM).

### Concept: The Secure Device Manager

The SDM is a router flash memory resident graphical user interface (GUI). SDM supports a wide range of Cisco IOS software releases and is available free of charge on Cisco router models from Cisco 830 series to Cisco 7301. The SDM can be accessed by making a hypertext transport protocol (HTTP) or hypertext transport protocol secure (HTTPS) connection to the router. A Java-based applet will then open in your browser and allow you to configure and modify the router. Some CCNP objectives must be accomplished through this interface. I include explanations of this interface and how to use it where applicable.

Other routers that can meet your needs Table 1.3 is a list of alternate routers that support both the SDM and version 12.4 code requirements.

**Table 1.3** Alternative Routers

<table>
<thead>
<tr>
<th>Router Model</th>
<th>SDM</th>
<th>Version 12.4 code</th>
</tr>
</thead>
<tbody>
<tr>
<td>830 Series</td>
<td>Can be run</td>
<td>At least one version can run</td>
</tr>
<tr>
<td>850 series</td>
<td>Preinstalled</td>
<td>Preinstalled</td>
</tr>
<tr>
<td>870 series</td>
<td>Preinstalled</td>
<td>Preinstalled</td>
</tr>
<tr>
<td>1700 series</td>
<td>Can be run</td>
<td>At least one version can run</td>
</tr>
</tbody>
</table>
TABLE 1.3 Alternative Routers (continued)

<table>
<thead>
<tr>
<th>Router Model</th>
<th>SDM</th>
<th>Version 12.4 code</th>
</tr>
</thead>
<tbody>
<tr>
<td>1800 series</td>
<td>Preinstalled</td>
<td>Preinstalled</td>
</tr>
<tr>
<td>2800 series</td>
<td>Preinstalled</td>
<td>Preinstalled</td>
</tr>
<tr>
<td>2600 XM series</td>
<td>Can be run</td>
<td>At least one version can run</td>
</tr>
<tr>
<td>3600 series</td>
<td>Can be run</td>
<td>At least one version can run</td>
</tr>
<tr>
<td>3700 series</td>
<td>Can be run</td>
<td>At least one version can run</td>
</tr>
<tr>
<td>3800 series</td>
<td>Preinstalled</td>
<td>Preinstalled</td>
</tr>
<tr>
<td>7200 VXR series</td>
<td>Can be run</td>
<td>At least one version can run</td>
</tr>
<tr>
<td>7301 series</td>
<td>Can be run</td>
<td>At least one version can run</td>
</tr>
</tbody>
</table>

**Buyer Beware**

I have a couple of things you should look out for when choosing different models of routers. First, the 800 series models of routers don’t always include a full version of the SDM. There is a “lite” version of the software called Express SDM. It does not provide all of the functionality that the full version does.

The second caution that I offer to you, and I know this is hard because you might have to buy the equipment yourself: Don’t just buy the cheapest model that you can get. For instance, the 800 series again are pretty much a fixed interface router. They don’t have any module bays so you can’t add other interfaces or functionality. Even the 1700 and 1800 series routers don’t have all the necessary module bays. Depending on the model, they have between one and four WAN interface card (WIC) slots that allow the installation of high-performance WAN interface cards (HWIC) and voice WAN interface cards (VWIC). They don’t, however, have network module (NM) bays. Depending on your needs and what you plan to configure, this may or may not be a big deal. It is something you should look at though.

**Wireless Equipment**

I add a few more things to this network before all of the testing is done. For example, when I get to the wireless sections, I include much of the new equipment for practice. You
will get look at the new Wireless LAN controller devices, as well as the new lightweight access points.

You’ll even get a glimpse of a few really cool new devices and management suites that make a WLAN run smoother and much easier to manage. The management suite for Cisco WLANs is the Wireless Control System (WCS). This is a great GUI that provides central management of all your lightweight wireless equipment. If you are not familiar with the lightweight solution, fasten your seatbelt. I cover all the new protocols and setup for this exciting new offering.

The other new device I mentioned is the 2710 Location Appliance. The location appliance allows you to track clients and active radio frequency identification (RFID) tags. The great thing about this device is that it allows you to track, in real time, all of the devices on your network.

I show you how all of these things work and what they look like under the hood. Table 1.4 provides a list of devices that I will use for examples in this book.

<table>
<thead>
<tr>
<th>Type</th>
<th>Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless LAN controllers (WLC)</td>
<td>4402 series controller</td>
</tr>
<tr>
<td></td>
<td>2006 series controller</td>
</tr>
<tr>
<td></td>
<td>NM-WLC embedded controller</td>
</tr>
<tr>
<td>Lightweight access points (LAP)</td>
<td>1242 series</td>
</tr>
<tr>
<td></td>
<td>1000 series</td>
</tr>
<tr>
<td>Mesh access points</td>
<td>1510 series</td>
</tr>
<tr>
<td></td>
<td>1522 series</td>
</tr>
<tr>
<td>Location appliance</td>
<td>2710 series</td>
</tr>
<tr>
<td>Wireless Control System (WCS)</td>
<td>WCS Location version for Windows Server 2003</td>
</tr>
</tbody>
</table>

That sums up my discussion on devices for now. Remember, this is just a brief introduction to get you started. Now, hopefully, you can start to gather some gear to begin testing the topics I am going to cover in this book. It is imperative that you have some real equipment to practice and test configurations on—not only for testing and certification purposes but to test that you are able to properly implement new technology into your network.
Alternative Wireless Hardware

If you don’t have any of the APs I’m using in the test network, you might be able use ones that you already have. Some of the access points (APs) that have been out on the market from Cisco for a while can be upgraded to act as a lightweight AP. These APs can be controlled by a WLC. I am going to show you some of them. Both the 1100 and 1200 series access points are upgradeable.

There is also a new series of APs and WLCs that you can get. They are called the express versions. These controllers and APs are for smaller deployments, in small- and medium-sized businesses (SMB). They typically support a smaller number of APs and don’t offer all of the functions that would be used in a large enterprise implementation. The express devices can be a good place to start in learning about lightweight WLANs. They are included in the objectives for the CCNA Wireless concentration certification.

Here is a list of those devices:

- Cisco 526 Wireless Express Mobility Controller
- Cisco 521 Wireless Express Access Point

Summary

Wow, the first chapter is down! You have covered quite a few things here already. Remember, the chapter started off looking at how networks used to be designed with the three-layer hierarchical design model. You’ll want to remember the three layers (access, distribution, and core) and their basic functions in a network.

From the basic three-layer model, you moved on to the Enterprise Composite Network Model. The enterprise model provides a much more detailed explanation of which devices should be used and how they should be connected. The easiest way to remember the enterprise model is to start out with the three major areas—Enterprise Campus, Enterprise Edge, and Service Provider Edge. You learned about the pieces that make up the Enterprise Campus because that is where network administrators spend most of their time and money. The Enterprise Campus is made up of the Campus Infrastructure Module, Server Farm Block, and the Network Management Module. Now, with that better understanding of both the design models, you can see that the original three-layer model is still used but it’s called the Campus Infrastructure piece of the larger enterprise model.

Don’t forget about the Enterprise Edge. Without that piece, your network would not be connected to any one outside of your company. The edge has subsections as well. If you remember, there is the Internet module, WAN module, and the remote access/VPN module.
Each module provides a separate and distinct connection in and out of the enterprise, each with its own services.

Next, I briefly introduced you to the SONA and IIN strategies, both of which are used to help bring about change and future implementation ideas for the networks of tomorrow. With an idea for future paths and where to go, we can provide smarter networks and more compatible technologies for later.

Finally, I gave you a broad overview of the FutureTech case study that will be built on for the duration of this book. At this point, you should have a basic understanding of the areas of the network that I’ll help you work through. The test network provides a great way to ensure that everything placed in the network works together and a good understanding of effects they have on other devices, protocols, and applications.

Get ready for a ride through some of the newest, most exciting, and essential topics for network engineers today.
Review Questions

1. What is the fundamental building block of a network design?
   A. Switch block
   B. Core
   C. Campus infrastructure
   D. Edge

2. What was Cisco’s original design model called?
   A. IIN
   B. SONA
   C. Three-layer hierarchical model
   D. Enterprise composite

3. What part of the Enterprise Campus design model does most of the network fall into?
   A. Enterprise Campus
   B. Data Center
   C. Network Management
   D. Edge

4. What is the bottom component in a switch block?
   A. Edge
   B. Core
   C. Access layer
   D. Data center

5. What piece of the network has always been characterized as just needing to move data as fast as possible without data manipulation?
   A. Edge
   B. Core
   C. Access layer
   D. Data center

6. The Enterprise Edge typically contains firewalls.
   A. True
   B. False
7. SONA is the implementation strategy for what process?
   A. SWAN
   B. IIN
   C. WDS
   D. ITIL

8. What area of the enterprise composite model has very little configuration for enterprise administrators?
   A. Core
   B. Network Management
   C. Customer Edge
   D. Service Provider Edge

9. VPNs are not implemented in the Enterprise Edge?
   A. True
   B. False

10. The name of my made up company is FutureTech Inc.?
    A. True
    B. False
Answers to Review Questions

1. A. A switch block is the fundamental building piece to the network; it is where all of the users connected and data is brought into the network.

2. C. The three-layer hierarchical model is the original name..

3. A. The Enterprise Campus contains all of the primary switch blocks and the data center and management block.

4. C. The access layer is the bottom layer in a switch block; it is where users connect to the network.

5. B. The core of the network has always had the goal of not changing the data and to move it across the network as fast as possible.

6. A. True. The Enterprise Edge contains firewalls to protect the network from external connections.

7. B. SONA is the true implementation for the IIN process.

8. D. The service provider edge has devices controlled and configured by the ISP, not the enterprise administrators.

9. B. False. VPNs are typically implemented in the edge of the network to protect data over unsecured networks.

10. A. True. This was supposed to be funny!