The thieves did not steal these records for the thrill of breaking in or to enhance their reputations among other hackers. They did it to steal information to make fraudulent credit card purchases in the names of the customers whose information had been stolen. These fraudulent purchases based on the stolen information did, in fact, take place.

TJX did not inform customers about the data breach until nearly a month later. The company said that it needed time to beef up its security. The company also said that law enforcement officials had told TJX not to release information about the breach immediately to avoid tipping off the data thieves about the investigation. Of course, the delay also left the customers ignorant of the danger they faced.

How did the breaches occur? When the attackers were caught, it was determined that the data thieves broke into poorly protected wireless networks in some Florida stores to get into the central TJX credit and debit card processing system in Massachusetts.[1] These stores protected their wireless network, but they used the obsolete wired equivalent privacy (WEP) standard instead of newer and better security standards. In Massachusetts, poor firewall protection[2] allowed the data thieves to enter several systems and to install a sniffer that listened to the company's poorly encrypted traffic passing into and out of the processing center. Another problem was that TJX retained some sensitive credit card information that should not have been retained; it is this improperly retained information that the data thieves found valuable.[3]

A number of earlier (and smaller) data breaches had prompted the major credit card companies to create the **Payment Card Industry–Data Security Standard (PCI–DSS)**. Failure to implement PCI–DSS control objectives can result in fines and even the revocation of a company's ability to accept credit card payments.

At the time the data breach was discovered, TJX was far behind in its PCI–DSS compliance program. The company complied with only three of the twelve required control objectives. Internal memos[4] revealed that the company knew that it was in violation of the PCI–DSS requirements, particularly with respect to its weak encryption in retail store wireless networks. However, the company deliberately decided not to move rapidly to fix this problem. In November 2005, a staff member noted prophetically that "saving money and being PCI-compliant is important to us, but equally important is protecting ourselves against intruders. Even though we have some breathing room with PCI, we are still vulnerable with WEP as our security key. It must be a risk we are willing to take for the sake of saving money and hoping we do not get compromised."

When the staff member noted that "we have some breathing room with PCI," he probably was referring to the fact that TJX had been given an extension allowing it to be compliant beyond the standard's specified compliance date.[5] This additional time, ironically, was given after the data breaches had already begun. This extension was dependent upon evaluation of a TJX report on its compliance project by June 2006. It is unknown whether TJX complied with this requirement. The letter that authorized the

---

[1] Mark Jewel, "Encryption Faulted in TJX hacking," *MSNBC.com*, September 25, 2007.

[2] Ross Kerber, "Details Emerge on TJX Breach," *The Boston Globe*, October 25, 2007.

[3] Mark Jewel, op. cit. www.msnbc.msn.com/id/20979359/.

[4] Evan Schuman, "VISA Fined TJX Processor for Security Breach," *Eweek.com*, October 28, 2007. www.eweek.com/article2/0,1895,2208615,00.asp.

[5] Evan Schuman, "In 2005, Visa Agreed to Give TJX Until 2009 to Get PCI Compliant," *StorefrontBacktalk*, November 9, 2007. storefrontbacktalk.com/story/110907visaletter.

extension was sent by a fraud control vice president for Visa. It ended with, "I appreciate your continued support and commitment to safeguarding the payment industry."

The company quickly became embroiled in commercial lawsuits and government investigations. These lawsuits involved the filing of briefs that shed additional light on the break-ins. For instance, sealed evidence from Visa and MasterCard placed the number of account records stolen at 94 million—roughly double TJX's estimates.[6]

TJX was sued by seven individual banks and bank associations. In December 2007, TJX settled with all but one of these banks, agreeing to pay up to $40.9 million. This would reimburse the banks for the cost of reissuing credit cards and other expenses.

The company also received a large fine from Visa. Actually, Visa could not fine TJX directly but could only fine TJX's merchant bank, the Fifth Third Bank of Ohio. (Merchant banks are financial institutions that serve—and should control—retail organizations that accept credit card payments.) However, merchant banks typically pass on the fine to the retailer, in this case TJX. During the summer of 2007, Visa fined TJX's merchant bank $880,000 and announced that it would continue to impose fines at $100,000/month until TJX had fixed its security problem. However, in the TJX settlement with the seven banks and banking associations, this fine was to be reduced by an undisclosed amount.

In this battle of corporate giants, consumers were handled last. At the time of this writing, TJX has proposed a settlement that would only involve very limited measures such as help with ID theft through insurance and other measures for the roughly 455,000 victims who had given personally identifiable information when they returned goods without a receipt. Other victims would be given a modest voucher or the opportunity to buy TJX merchandise at sale prices.[7]

On August 25, 2008, the Department of Justice charged 11 individuals with conducting the TJX break-in and the subsequent use of the stolen information.[8] Three were Americans, and they were jailed rapidly. Two more were in China. The other six lived in Eastern Europe. Although the three Americans conducted the actual data theft, they fenced the stolen information overseas. Two of the American defendants rapidly entered plea deals to testify against the alleged ringleader, Albert Gonzalez of Miami, Florida. Gonzalez was sentenced in 2010 to 20 years in prison.

One surprising thing about the indictment is that this criminal gang had not only plundered TJX of customer information. Subsequent investigation found that the attackers had repeated the crime with at least a half dozen other major companies.[9] These break-ins also began with the exploitation of WEP security.

Test Your Understanding

1. a) What did the attackers do first to break into TJX and other companies? b) Why do you think TJX failed to upgrade to stronger security than WEP? (There may be more than one consideration.) c) How was the TJX break-in an international crime?

---

[6] Ross Kerber, "Court Filling in TJX Breach Doubles Toll," *The Boston Globe*, October 24, 2007.

[7] John Leyden, "TJX Consumer Settlement Sale Offer Draws Scorn," *TheRegister.com*, November 20, 2007. www.theregister.co.uk/2007/11/20/tjx_settlement_offer_kerfuffle/.

[8] U.S. Department of Justice, "Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers," August 5, 2008. www.usdoj.gov/criminal/cybercrime/gonzalez-Indict.pdf.

[9] Ibid.

802.11 WLAN SECURITY

WLAN Security Threats

For most companies, security is the biggest problem with 802.11 wireless LANs. There are several major security threats to 802.11 WLANs:

- Most seriously, **drive-by hackers** park just outside a company's premises and intercept the firm's data transmissions. They can also mount denial-of-service attacks, send malware into the network, and do other mischief. Drive-by hacking software is readily downloadable from the Internet.
- Less importantly, **war drivers** are people who drive around a city looking for working access points that are unprotected. War driving is not illegal. Only if war drivers try to break in do they become drive-by hackers.
- To guard against drive-by hackers, companies can secure their access points using techniques we will see a little later. However, departments or individual employees may set up unauthorized access points. These **rogue access points** often have no security, so they provide entry points for drive-by hackers who could not otherwise break into the network. Even if a company protects all of its official access points very well, a single rogue access point will make the security effort worthless.

Test Your Understanding

2. a) Distinguish between war drivers and drive-by hackers. b) What is a rogue access point?

Drive-by Hackers

Sit outside the corporate premises and read network traffic
Can send malicious traffic into the network
Easily done with readily available downloadable software

War Drivers

Merely discover unprotected access points—become drive-by hackers only if they break in
War driving per se is not illegal

Unprotected Access Points

Drive by hackers can associate with any unprotected access point
They gain access to the local area network without going through the site firewall

Rogue Access Points

Unauthorized access points that are set up by a department or an individual
Often have very poor security, making drive-by hacking easier
Often operate at high power, attracting many hosts to their low-security service

FIGURE 7-1 WLAN Security Threats (Study Figure)

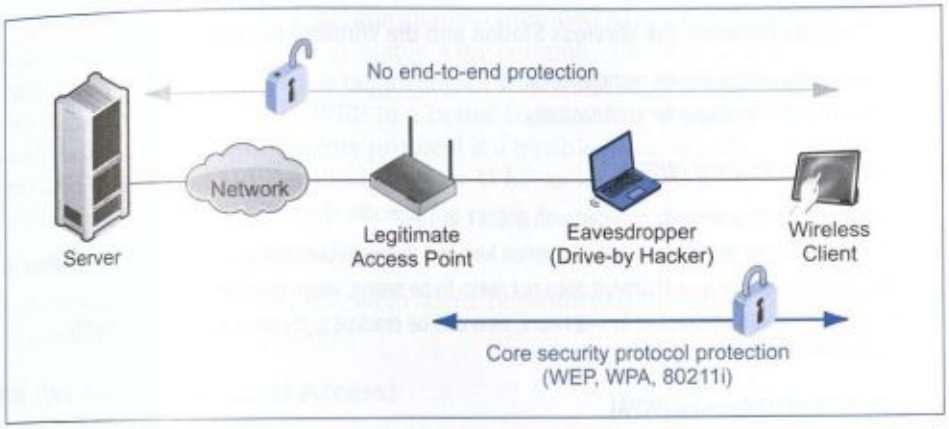


FIGURE 7-2 Core 802.11 Security Standards

802.11 Core Security Standards

Realizing the danger of drive-by hackers, the 802.11 Working Group decided to create a **core security standard** for wireless LANs. As Figure 7-2 shows, 802.11 core security standards provide protection between the wireless access point and the wireless host. This protection includes confidentiality, authentication, and message integrity. A drive-by hacker cannot intercept traffic to read it or send its own messages to the access point.

However, note in the figure that protection only extends between the wireless access point and the wireless host. It does not provide protection end-to-end between the wireless client host and the server host on the wired LAN (or the server host on the Internet). The core security standard has a very limited objective.

The protection provided by 802.11 core security standards only extends between the wireless access point and the wireless host.

Wired Equivalent Privacy (WEP) Security

When the 802.11 Working Group created its first standards in 1997, it only included a very rudimentary core security standard called **Wired Equivalent Privacy (WEP)**.[10] This is the weak security standard that was used by TJX, as we saw at the beginning of this chapter.

With WEP, everyone sharing an access point had to use the same key, and WEP had no automated mechanism for changing this key. In nearly all cases, a firm with many access points and users normally gave all access points the same WEP key. Everybody in the firm knew the WEP key, so many employees thought it was not really secret and often were willing to share the key with unauthorized users. In addition,

[10]The WEP specification was only 10 pages long. In contrast, the specification for 802.11i security (discussed later) is 200 pages long.

Provide Security between the Wireless Station and the Wireless Access Point

- Client (and perhaps server) authentication
- Encryption of messages for confidentiality

Wired Equivalent Privacy (WEP)

- Initial rudimentary security provided with 802.11 in 1997
- Everyone shared the same secret encryption key, and this key could not be changed automatically
- Because secret key was shared, it does not seem to be secret, users often give out freely
- Key initially could be cracked in 1–2 hours; now can be cracked in 3–10 minutes using readily available software

Wireless Protected Access (WPA)

- The Wi-Fi Alliance
  - Normally certifies interoperability of 802.11 equipment
  - Created WPA as a stop-gap security standard in 2002 until 802.11i was finished
- Designed for upgrading old equipment
  - WPA uses a subset of 802.11i that can run on older wireless NICs and access points
  - WPA added simpler security algorithms for functions that could not run on older machines
- Equipment that cannot be upgraded to WPA should be discarded

802.11i (WPA2)

- Uses AES-CCMP with 128-bit keys for confidentiality and key management
- Gold standard in 802.11 security
- But companies have large installed bases of WPA-configured equipment

FIGURE 7-3 802.11 Security Standards (Study Figure)

because there was no automated way to change all of the access point keys when an employee was fired, companies continued to use the same key even when there were clear security threats.

WEP had several other serious design problems. By 2001, software that would crack WEP keys quickly was readily available. Initially, cracking a WEP key with one of these programs took one or two hours. Today, it often takes only about 10 minutes. Many companies began putting the brakes on WLAN implementation, and many pulled out their existing access points.[11]

[11] Some companies began taking other steps, like hiding the SSID (Service Set Identifier) of the access point. Users need to know this SSID to use an access point even if WEP is not used. Another common step was to accept only computers whose wireless NICs had registered MAC addresses. (All 802 LANs have 48-bit MAC addresses.) Unfortunately, these measures take a great deal of work, and they are easily cracked by readily available hacking software. They make sense if you are concerned only about unsophisticated but nosy neighbors at home.

Despite problems with WEP, companies continued to use it long after better 802.11 core security standards became available. One company that did so was TJ-MAX in the United States. As we saw at the beginning of this chapter, TJ-MAX made a conscious decision not to upgrade from WEP to a better core security protocol. The result was a disaster. Using a weak core security protocol is a terrible security policy. Although access points and clients usually continue to offer WEP as well as newer security protocols, only the newer security protocols should be used.

Test Your Understanding

3. a) When 802.11 was created, what security protocol did it offer? b) How long does it take to crack WEP today?

WPA (Wireless Protected Access)

The **Wi-Fi Alliance** is an industry trade group that certifies 802.11 products for interoperability. Normally, the Wi-Fi Alliance leaves standards creation to the 802.11 Working Group. However, when WEP's fatal flaws were discovered in 2000 and 2001, the market for wireless products began to falter. Furthermore, the 802.11i security standard being developed by the 802.11 Working Group was going to take years to be ratified.

As a stop-gap measure until 802.11i could be developed, the Wi-Fi Alliance created an interim security standard, **Wireless Protected Access (WPA)**, based on an early draft of the 802.11i core security standard. So that WPA could be used on older wireless access points, the Wi-Fi Alliance watered down the 802.11i draft standard, using weaker security protocols. It announced this standard in 2002 and began certifying products for compliance in early 2003. Despite its weaknesses, WPA was much stronger than WEP. Companies flocked to it.

Test Your Understanding

4. a) Who created WPA? b) What is WPA's disadvantage compared with 802.11i?

802.11i (WPA2)

In 2004, the 802.11 Working Group finally ratified the **802.11i** standard. Most important, the 802.11i standard uses extremely strong **AES-CCMP** encryption. AES-CCMP has 128-bit keys and a key management method for automatically changing keys. In general, for every aspect of security, it uses the strongest security algorithms. Confusingly, the Wi-Fi Alliance refers to the 802.11i standard as **WPA2**.

However, before 802.11i appeared, most companies had already implemented WPA on their access points and wireless hosts. Reconfiguring all of these devices to work with 802.11i can be expensive, and until there were known cracks for WPA, companies were reluctant to make this investment. This changed in 2009, when a partial crack appeared for WPA. Companies that care strongly about WLAN security have transitioned to or are moving rapidly to 802.11i.

Test Your Understanding

5. a) What is the strongest security protocol for 802.11 today? b) What does the Wi-Fi Alliance call 802.11i? c) What encryption method does 802.11i use? d) What is deterring companies from converting from WPA to 802.11i? e) Why is WPA no longer viewed as a safe solution?

802.1X Mode Operation with Added Client–Access Point Security

WPA and 802.11i have two modes of operation. For large firms, the only mode that makes sense is **802.1X mode**. (The Wi-Fi Alliance calls it **enterprise mode**.) In Chapter 5, we saw that 802.1X was created for Ethernet wired networks. Its goal is to prevent attackers from simply walking into a building and plugging a computer into any wall jack or directly into a switch.

Figure 7-5 shows that each workgroup switch acts as an authenticator. The computer wishing access to the Ethernet network connects to the authenticator via UTP. Actual authentication is done by a central authentication server that normally uses the RADIUS protocol.

For Ethernet access, there is no need to have security between the computer seeking access and the workgroup switch that controls access. It is difficult for another person to tap the wired access line between the computer and the switch, and there are easier ways to break into a network. Consequently, as Figure 7-5 shows, there is no security between the wired hosts and the switch that is the 802.1X network access server.

With access points, however, transmissions between a wireless host and the access point are easy to intercept and mimic. The path between the host and the access point needs to be secure. To address this problem, the 802.11 Working Group extended the 802.1X standard by adding security between the access point and the wireless host before 802.1X mode authentication is done. The most common standard for adding this protection is the Protected Extensible Authentication Protocol (PEAP). Other standards for adding this security include EAP-TLS and EAP-TTLS. All of these standards create

802.1X Mode (See Figure 8-5)

- Uses a central authentication server for consistency
- Authentication server also provides key management
- Wi-Fi Alliance calls this *enterprise mode*
- 802.1X standard protects communication with an extensible authentication protocol
  - Several EAP versions exist with different security protections
  - Firm implementing 802.1X must choose one
  - Protected EAP (PEAP) is popular because Microsoft favors it

Pre-Shared Key (PSK) Mode: Stations Share a Key with the Access Point

- For networks with a single access point
- Access point does all authentication and key management
- All users must know an initial pre-shared key (PSK)
- Each, however, is later given a unique key
- If the pre-shared key is weak, it is easily cracked
- Pass phrases that generate key must be at least 20 characters long
- Wi-Fi Alliance calls this *personal mode*

FIGURE 7-4 802.11 Security in 802.1X and PSK Modes (Study Figure)

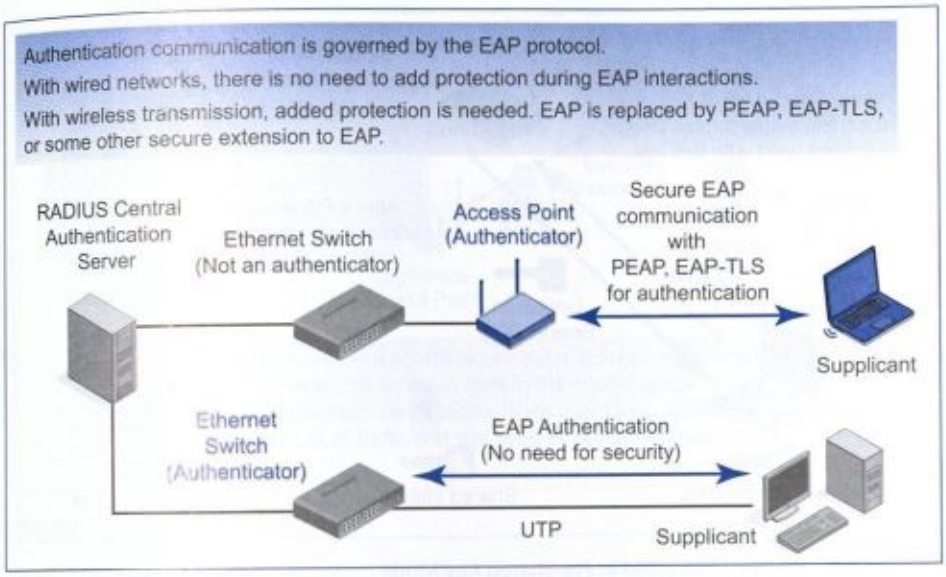


FIGURE 7-5 802.1X Mode for 802.11i (and WPA)

an SSL/TLS connection between the wireless access point and the wireless client before 802.1X is applied.

Test Your Understanding

6. a) In what mode of 802.11i and WPA operation is a central authentication server used? b) What does the Wi-Fi Alliance call 802.1X mode? c) Why does 802.1X not need security between the authenticator and the computer in Ethernet? d) Why does 802.1X need security between the authenticator and the computer in 802.11 wireless access? e) Why is extra EAP security necessary in 802.11 networks using 802.1X? f) What is the most popular standard for extended 802.1X security?

Pre-Shared Key (PSK) Mode

For homes and small businesses, adding a separate authentication server would be absurd. Consequently, the 802.11 Working Group created a simpler mode of operation beyond 802.1X mode. In this simpler mode, called **pre-shared key mode**, a single access point does all the work to provide a core security protocol. The Wi-Fi Alliance calls this personal mode.

PSK mode in 802.11i and WPA is for homes and small businesses with a single access point.

Figure 7-6 shows that the access points and wireless hosts begin with a shared 64-bit key. Everybody allowed to use the access point is told the shared key. This sounds like WEP, but this shared key is only used in initial authentication. After initial authentication, the wireless access point gives each authenticated user a new unique key to use

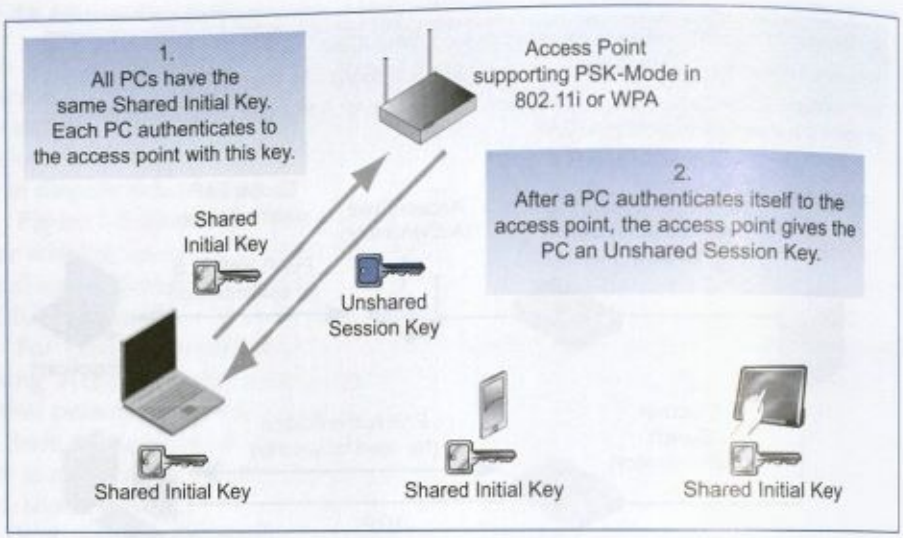


FIGURE 7-6 802.11i (and WPA) in Pre-Shared Key Mode

while on the Internet. It also changes this key frequently. With this approach, too little traffic is created with each key to allow a drive-by hacker to crack the key.

In a home or very small business, having a handful of people know the shared key is not too dangerous. The larger danger is that the household or small business will select a weak key. To create the pre-shared key, the household or company creates a long **pass phrase** (which is much longer than a password) that the access point and each host use to generate the key. This pass phrase must be at least 20 characters long to provide adequate security. If short pass phrases are used, 802.11i and WPA in PSK mode are almost as easy to crack as WEP.

Test Your Understanding

7. a) How does PSK mode differ from 802.1X mode? b) What is a potential weakness of PSK mode? c) How long should pass phrases be with PSK?

Evil Twin Access Points and Virtual Private Networks (VPNs)

Strong core security standards that protect communication between the wireless access point and wireless clients can greatly reduce risks. However, there is one type of attack that can break core security standards. This is the evil twin access point.

EVIL TWIN ACCESS POINTS Figure 7-7 illustrates an evil twin access point attack. Normally, the wireless client shown in the figure will associate with its legitimate access point. The two will establish a core security standard connection between them.

An **evil twin access point** is a notebook computer configured to act like a real access point. The evil twin operates at very high power. If the wireless host is configured to choose the highest-power access point, it will associate with the evil twin access point instead of the legitimate access point. The evil twin will establish a

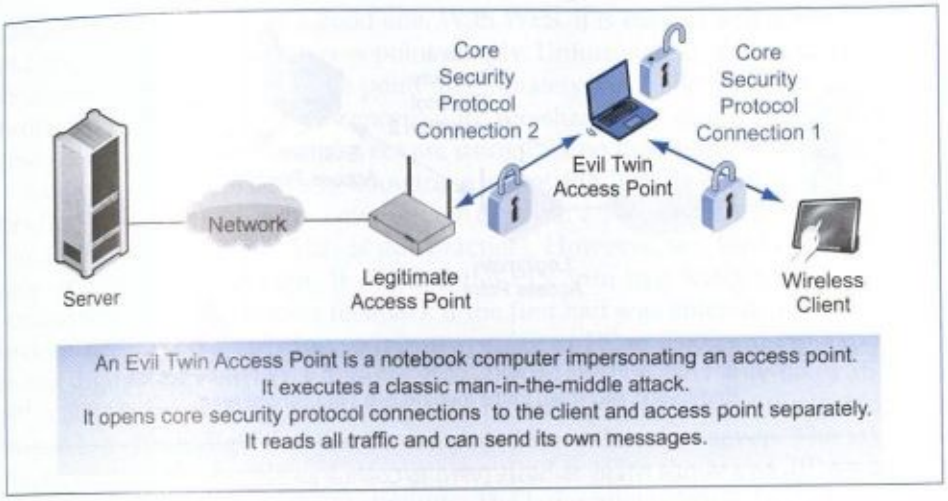


FIGURE 7-7 Evil Twin Access Point

secure connection with the wireless client. This is Core Security Connection 1. Next, the evil twin associates with the legitimate access point, creating Core Security Connection 2.

An evil twin access point is a notebook computer configured to act like a real access point.

The evil twin can now read all traffic flowing between the wireless client and the legitimate wireless access point. When the wireless client sends encrypted frames, the evil twin decrypts them and then re-encrypts them before sending them on to the wireless access point. It does the same with traffic going in the other direction. Neither the wireless client nor the wireless access point knows that this is happening. Both seem to experience a normal secure connection. The wireless client has no problem getting to servers on the main wired LAN or getting to Internet servers.

What damage can an evil twin access point do? Most obviously, it can eavesdrop on the communication between the wireless client and the servers it uses. This allows the evil twin to steal important keys, corporate trade secrets, or personal information transmitted by the client.

The evil twin can also launch attacks against the client or any server attached to the network. On the client, the evil twin may be able to read information on the user's hard drive or plant malware for ongoing exploitation. The evil twin can launch attacks directly against servers, bypassing the company's firewall.

VIRTUAL PRIVATE NETWORKS (VPNs) The evil twin attack is an example of a general class of attacks called man-in-the-middle attacks, in which an attacker intercepts messages and then passes them on. Man-in-the-middle attacks typically are very difficult to defeat. The main way to defeat them is to establish a virtual private

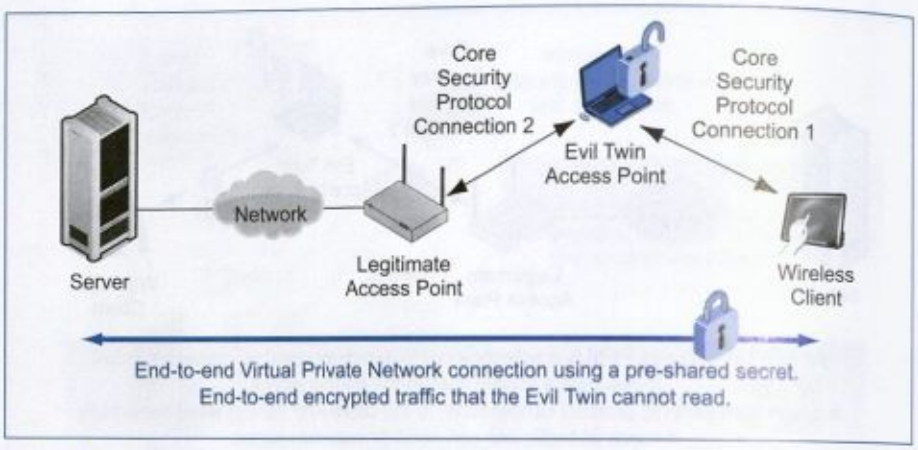


FIGURE 7-8 Using a Virtual Private Network (VPN) to Counter an Evil Twin Attack

network (VPN) connection between the wireless client and the server host it will use, as Figure 7-8 illustrates.

A **virtual private network (VPN)** is nothing more than a cryptographic system connection between a client and a server. A VPN gets its name from the fact that, as far as security is concerned, the client and server seem to have their own private network.

VPNs provide end-to-end protection between the client and the server, including end-to-end authentication. If VPN authentication is based on a pre-shared secret that the client and server know ahead of time, an evil twin will not be able to conduct a man-in-the-middle attack against the client and the server. Although the evil twin can read all wireless transmissions, it cannot intercept the pre-shared secret because this secret is never transmitted. So it will not be able to decrypt the messages passing between the client and the server, and it will not be able to send authenticated attack messages to either.

PERSPECTIVE Evil twin attacks are not theoretical concerns. They are commonplace, especially in wireless hot spots. Companies should use VPNs whenever clients and servers exchange sensitive communication.

Test Your Understanding

8. a) What is an evil twin access point? b) A company uses 802.11i for its core security protocol. How many 802.11i connections will the evil twin access point set up? c) What does the evil twin do when the client transmits to the legitimate access point? d) Distinguish between evil twin access points and rogue access points. e) How can VPNs defeat evil twin attacks? f) Why must the VPN secret be pre-shared to thwart a VPN attack?

Wi-Fi Protected Setup

One recent problem is a security weakness in **Wi-Fi Protected Setup (WPS)**. This standard is not a creation of the 802.11 Working Group. Rather, it was created by the Wi-Fi

Alliance. The basic idea was a good one. With WPS, it is easy to add a new client to a WPA2 pre-shared key mode access point simply. Unfortunately, if an attacker can use WPS to associate it with an access point illegitimately, he or she then has access to the network. Note that this is only a concern with pre-shared key mode. However, this is a business security concern if employees are using PSK on their home networks.

Part of the WPS process is knowing a secret PIN that is eight digits (the characters from 0 to 9) long. Exhaustive search on such a PIN should take about half of 10^8 or 50,000,000 attempts. This is not practical. However, the Wi-Fi Alliance made a poor decision in its design. It divided the PIN into two 4-digit halves. Then, it unfortunately gave an attacker feedback if the first half was entered correctly correct. Therefore, the attacker only has to try an average of 10^4 or 5,000 attempts to find the first four digits. Once these are known, cracking the second part only takes about half of 10^3 or 500 attempts. Why not half of 10^4? The answer is that one of the last four final numerals is a check digit that can be computed from the other seven. The take away is that by cutting the number of attempts required to learn the secret, PIN is reduced from 50,000,000 attempts to 5,500 attempts. The latter allows Wi-Fi Protected Setup to be broken in a few hours.

What can be done to protect against these weaknesses? For existing access points, the only possibility is to turn off Wi-Fi Protected Setup. Obviously, this means losing easy setup for clients at PSK wireless access points. In addition, it is not even possible to turn off WPS on many wireless routers.

Test Your Understanding

9. a) What does WPS do? b) For what 802.11i mode is it applicable? c) Why is it desirable? d) Why is it dangerous? e) What can be done to reduce the danger of the WPS security weakness?

Denial-of-Service Attacks

A final security concern for 802.11 wireless networks is the possibility of *denial-of-service (DoS)* attacks. In a typical wireless DoS attack, the attacker overloads an access point or causes a client to disassociate from an access point. One approach to DoS attacks is to flood an access point with traffic. This is best done with frames that request association or do something else that requires extensive processing on the access point. Another is to send disassociate frames to a client. This causes a client to disassociate with the access point, breaking the network connection. Wireless attacks are uncommon, and they are usually not effective, but companies must be concerned about that.

Test Your Understanding

10. a) What damage is done by a denial-of-service attack? b) What are the two types of wireless denial-of-service attacks?

802.11 WIRELESS LAN MANAGEMENT

Until recently, the term *WLAN management* was almost an oxymoron. Large WLANs were like major airports without control towers. Companies quickly realized that they needed tools for centralized WLAN management.

Access Point Placement

The first management issue is where to place access points. If placement is not done systematically, there will be many dead spots, interference between many access points, or both.

INITIAL PLANNING The first step is to determine how far signals should travel. In many firms, a good radius is about 30 meters. If the radius is too great, many hosts will be far from their access points. Hosts far from the access point must drop down to lower transmission speeds, and their frames will take longer to send. This will reduce the access point's effective capacity. If the radius is too small, however, the firm will need many more access points to cover the space to be served.

Once an appropriate radius is selected (say 30 meters), the company gets out its building architecture drawings and begins to lay out 30 meter circles with as little overlap as possible. Where there are thick walls or other obstructions, shorter propagation distances must be assumed. And, of course, in a multistory building, this planning must be done in three dimensions.

Access Points Placement in a Building

- Must be done carefully for good coverage and to minimize interference between access points
- Lay out 30-meter to 50-meter radius circles on blueprints
- Adjust for obvious potential problems such as brick walls
- In multistory buildings, must consider interference in three dimensions
- Install access points and do site surveys to determine signal quality
- Adjust placement and signal strength as needed

Remote Access Point Management

- The manual labor to manage many access points: can be very high
- Centralized management alternatives (See Figure 8-10)
  - Smart access points
  - Dumb access points, with intelligence in WLAN switches
- Desired functionality
  - Notify the WLAN administrators of failures immediately
  - Support remote access point adjustment
  - Should provide continuous transmission quality monitoring
  - Allow software updates to be pushed out to all access points or WLAN switches
  - Work automatically whenever possible
- Desired security functionality
  - Notify administrator of rogue access points
  - Notify administrator of evil twin access points
  - Notify the administrator of flooding denial-of-service attacks
  - Notify the administrator of disassociate message denial-of-service attacks
  - Instantly deny access to selected stations

FIGURE 7-9 Wireless LAN Management (Study Figure)

Finally, planners assign channels to access point positions. They attempt to minimize interference while doing so.

INSTALLATION AND INITIAL SITE SURVEYS Next, the access points are installed provisionally in the indicated places. However, the implementation work has just begun. When each access point is installed, an **initial site survey** must be done of the area around the access point to discover whether there are any dead spots or other problems. This requires signal analyzer software, which can run on a notebook computer or even a smartphone.

When areas with poor signal strength are found, surrounding access points must be moved appropriately, or their signal strengths must be adjusted until all areas have good signal strength.

ONGOING SITE SURVEYS Although the initial site survey should result in good service, conditions will change constantly. More people may be given desks in a given access point's range, signal obstructions may be put up for business purposes, and other changes must occur. Site surveys must be done periodically to ensure good service. They may also be done in response to specific reports of problems. To address problems, the network staff can adjust the power settings of nearby access points or take other actions.

Test Your Understanding

11. a) Describe the process by which access point locations are selected. b) After access points are installed provisionally, what must be done next?

Remote Management: Smart Access Points versus Wireless Switches

Large organizations have hundreds or even thousands of 802.11 wireless access points. Traveling to each one for manual configuration and troubleshooting would be extremely expensive. To keep management labor costs under control, organizations need to be able to manage access points remotely, from a central management console. Figure 7-10 illustrates two approaches to centralized wireless access point management.

SMART ACCESS POINTS The simplest approach architecturally is to add intelligence to every access point. The central management console can then communicate directly with each of these **smart access points**[12] via the firm's Ethernet wired LAN. However, adding management capacity raises the price of access points considerably. Using smart access points is an expensive strategy.

WIRELESS LAN SWITCHES A second approach illustrated in Figure 7-10 is to use **WLAN switches**. As the figure shows, multiple access points connect to each wireless LAN switch. The management intelligence is placed in the WLAN switch rather than in the

[12] Smart access points are also called fat access points.

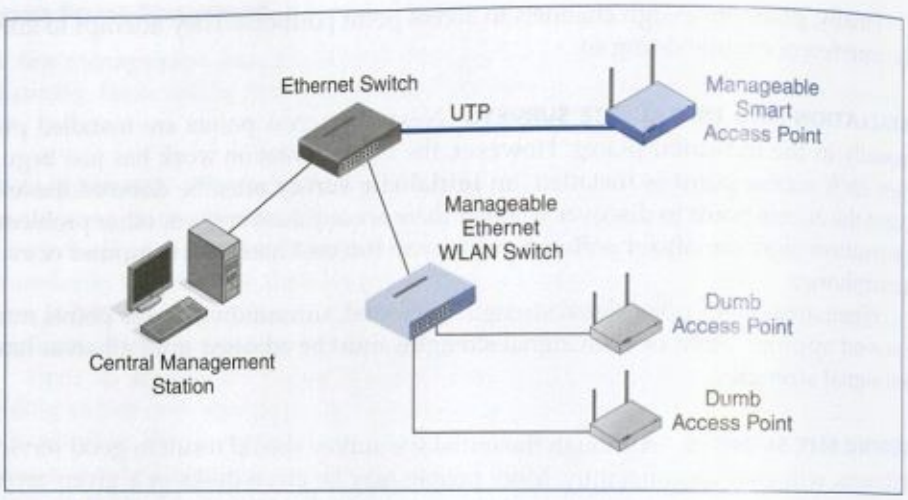


FIGURE 7-10 Wireless Access Point Management Alternatives

access points themselves. Vendors who sell WLAN switches claim that this approach reduces total cost because only inexpensive **dumb access points** are needed. Of course, smart access point vendors dispute these cost comparisons.

WIRELESS LAN MANAGEMENT FUNCTIONALITY Although technological approaches to centralized WLAN management vary, vendors generally agree on the types of functionality these systems should provide.

- These systems should notify the WLAN administrators of failures immediately so that malfunctioning access points can be fixed or replaced rapidly.
- They should provide continuous transmission-quality monitoring at all access points. In effect, they should provide continuous site surveys.
- They should help provide security by detecting rogue access points, evil twin access points, or legitimate access points that have improperly configured security.
- They should allow remote adjustment—for instance, telling nearby access points to increase their power to compensate for an access point failure. Such adjustments are also needed over time as furniture is moved (creating different shadow zones) or as the number of users in an area changes.
- They should allow software updates to be pushed out to all access points or WLAN switches, bypassing the need to install updates manually.
- The management software should be able to work automatically, taking as many actions as possible without human intervention.

WIRELESS MANAGEMENT SECURITY FUNCTIONALITY Centralized wireless LAN management also needs to provide support for detecting and correcting security problems.

- First, the WLAN management system should notify the administrator if a rogue access point appears.

- Second, it should notify the administrator if an evil twin access point appears.
- It should also notify the administrator of jamming denial-of-service attacks that flood an access point with traffic.
- It should notify the administrator of disassociate message that causes a wireless host to drop its connection with an access point.
- Acting on its own, it should instantly deny access to wireless hosts under specified conditions.

Test Your Understanding

12. a) Why is centralized access point management desirable? b) What are the two technologies for remote access point management? c) What functions should remote access point management systems provide?

Expressing Power Ratios in Decibels

In networking, you often need to express the ratio of two signal power levels. For example, you might wish to say that a larger antenna will quadruple the signal power. Or, you might say that signal power at one location is only half as strong as it is at a certain closer location. Or, you might wish to say that the connector between a radio and an antenna reduces power by 30 percent. In each case, percentages and ratios work fine.

Computing Ratios in Decibels

The problem is that radio power ratios often vary by several orders of magnitude, say between 50 Watts and 0.005 Watt. In such cases, ratios expressed as percentages become difficult to read. Instead, it is easier to read ratios expressed in a logarithmic scale. Consequently, relative signal strengths in radio transmission are almost always given in watts. Equation 7-1 shows how to express the ratio between two power levels, P_1 and P_2, in **decibels (dB)**. This looks a bit complicated, but it is easy to do in practice, with the help of a spreadsheet program.

Equation 7–1 Expressing Power Ratios in Decibels

$$L_{db} = 10 * Log_{10}\left(\frac{P_2}{P_1}\right)$$

Computing Ratios

We will discuss the equation backwards, from *right to left*. You first divide the second power level, P_2, in watts, by the first power level, P_1, again in watts. To give an example, if P_1 is 40 W and P_2 is 80 W, the resultant ratio is 80/40 or 2. If the second power level is larger than the first, the ratio will be greater than one. For example, this happens if an antenna boosts a radio's initial power P_1 before sending it out as transmitted power P_2.

If the second power level is larger than the first, the ratio will be greater than one.

In contrast, suppose that P_2 is 40 W and P_1 is 80 W. In that case, the resultant ratio is 40/80 or 0.5. If the second power level is less than the first, the ratio will be smaller than one.

(continued)

This happens if there is a decrease in power, say from attenuation of the signal as it propagates or in case of a power loss in the connector between the radio and the antenna.

If the second power level is larger than the first, the ratio will be less than one.

We have said that both power levels must be measured in watts. Actually, this was a slight lie. As long as both powers are expressed in the same units, for example, milliwatts, it will be fine. However, if one is given in watts and the other in milliwatts, the calculation will not work. You have to put them in the same units.

Expressing Ratios in Decibels

Next, you take the Base 10 logarithm of the ratio. Computing Base 10 logarithms is very difficult. Therefore, you should cheat. Use Excel or some other spreadsheet program. In Excel, the function for Base 10 logarithms is LOG10(). The second column in Equation 7-1 shows Base 10 logarithms for a number of ratios from 100 to −100. This gives the power ratios in Bels, named after Alexander Graham Bell. However, engineers multiply Bels by 10 to give decibels (dB). Decibels prove to be more useful numbers for radio signal measurement. The third column gives this decibel calculation. You now have ratios in decibels. You have mastered Equation 7-1.

Notice the general pattern in Figure 7-11 for decibels. If the ratio is greater than one—that is, if P_2 is larger than P_1, then the number of decibels is positive. In contrast, if the ratio is less than one, that is, if P_2 is smaller than P_1, then the number of decibels is negative. By

Ratio	Bels Log10	Decibels 10 * Log10	Approximately
100	2	20	20
50	1.699	16.990	NA
20	1.301	13.010	13
10	1	10	10
8	0.903	9.031	9
4	0.602	6.021	6
3	0.477	4.771	NA
2	0.301	3.010	3
1	0	0	0
0.5	−0.301	−3.010	−3
0.3333	−0.477	−4.772	NA
0.25	−0.602	−6.021	−6
0.125	−0.903	−9.031	−9
0.1	−1	−10	−10
0.05	−1.301	−13.010	−13
0.01	−2	−20	−20

FIGURE 7-11 Decibel (dB) Calculations for Various Ratios

looking at the sign of the decibel value, you can tell at a glance if the power increased from P_1 to P_2 or if it decreased.[13]

If ratio is greater than one—that is, if P_2 is larger than P_1, then the number of decibels is positive. In contrast, if the ratio is less than one, that is, if P_2 is smaller than P_1, then the number of decibels is negative.

Working with Approximations

The fourth column in Figure 7-11 shows that if the ratio is 1, 2, 4, or 8, there are approximations you can use to estimate decibel values without having to compute Equation 7-1. This is useful if you do not have a spreadsheet program readily available or if you just want to get a feel for a number you are given. In the case of powers of two, the estimation rule is that each doubling is an additional 3 decibels. So a ratio of 2 is 3 db, of 4 is 6 db, and of 8 is 9 dB. What would a ratio of 16 be?[14] These are only approximations, but they are very good ones. The true value for each doubling, 3.010, is extremely close to 3.

Each doubling in the power ratio corresponds approximately to 3 dB.

What about ratios less than one? One half is very nearly –3dB, one quarter is nearly -6 dB, and one eighth can be estimated to be –9 dB. What is one sixteenth?[15]

Each halving in the power ratio corresponds approximately to –3 dB.

Things are even easier if ratios are some power of 10. A ratio of 10 is 10 dB. A ratio of 100 is 20 dB. Each multiplication by 10 gives an additional 10 dB. So if the power ratio is 1,000, this is 30 dB. What if the power ratio is 10,000?[16] Going the other way, a ratio of 1/10 is –10 dB, and a ratio of 1/100 is –20 dB. What is a ratio of 1/1,000?[17] These are listed in the table as approximations, but they are really exact. Each increase by a factor of 10 adds exactly 10 dB, and each decrease by a factor of 10 reduces the decibels by a factor of exactly 10.

Each increase by a factor of 10 adds exactly 10 dB, and each decrease by a factor of 10 reduces the decibels by a factor of exactly 10.

These "tricks" for 2 and 10 can be used together. For example, what about a ratio of 20? In this case, you have an increase by a factor of 10 and another by a factor of 2. The order is not important. In power levels, you multiply by 10 and by 2. In logarithms, you *add* the two logarithms. Multiplying by 10 gives 10 db, and multiplying by 2 gives 3 db. Therefore, the decibel

(continued)

[13] Of course, if you know the ratio of P_2 to P_1, it is even easier to tell, but if you are just given decibel levels, you can't do this.

[14] Yep, 12 dB.

[15] –12 dB.

[16] Yep, 40 dB.

[17] It is –30 dB. Got it again.

value for a power ratio of 20 should be 10 plus 3 or 13 dB. You can see in Figure 7-11 that this is in fact the case. (The actual value is 13.010 dB.)

What about a ratio of 1/20? Again, you *add* the two approximations. One tenth is −10 dB, and one half is −3 dB. So you get an approximate decibel value of −13 dB.

What about other ratios, like 3:1, 50:1, 1:3, and 1:50? Sorry. There aren't approximations for these. Go to Excel and work it out. You will have to do this for precise calculations anyway, even if you are talking about factors of 2 or ½. Approximations just let you work things out in your head.

At the same time, working with factors of 2 and 10 can give you an approximate range of actual values. For example, what about a ratio of 25? A ratio of 20, which is a little *lower* than 25, would give 13 dB, as we have just seen, so the correct value will be a little *more* than 13 dB. In turn, 32, which is larger than 25, is five doublings or 15 dB. So the value in decibels must be between 13 dB and 15 dB. If you go to Excel and get a number smaller than 13 dB or larger than 15 db, check your work. By the way, the correct answer using Equation 7-1 is 13.98.

dBm

We have looked at expressing ratios in terms of decibels. However, when you look at the power of a radio, you often see it expressed in dBm. This means decibels expressed are relative to one **milliwatt (mW)**, which is one thousandth of a watt.

For example, suppose that your radio has a power of 0.1 Watt. This is 100 milliwatts. So the ratio for the power of the radio compared to one milliwatt is 100. This would give a decibel ratio of 20 dBm. In turn, if the radio had a power of eight milliwatts, this would be a ratio of 8 or 9 dBm. If a radio has a power of 1 Watt, then the ratio compared to one milliwatt is 1,000, and the radio has a power of 30 dBm. If a radio has a power of 10 Watts, then the ratio would be 10,000, and the dBm value would be 40 dBm. A 100 Watts, which would be the power of a light bulb, would have a value of 50 dBm.

One reason that radio engineers like to use dBm is that the ratio is almost always positive. A radio with a power of less than a milliwatt generally will not be able to transmit with any speed or distance.

Perspective: Multiplication versus Addition

One advantage of working with decibels is that while you must multiply with ratios, you can simply add logarithms. For example, suppose that you start with a radio strength of 33 dBm. Also, suppose that the signal strength at a particular location is 1/10 that of the signal strength near the radio. Therefore, you have an attenuation of −10 dB. Finally, suppose that the receiver has a high-gain antenna that will boost the signal by a factor of two (+3 dB). The final signal strength at the receiver will be 33 dBm −10 dB + 3 dB or 26 dBm.

Converting Decibels Back to Power Levels

Sometimes when you are given a decibel value, you wish to know what power ratio this represents. To do this calculation, simply solve Equation 7-1 for P_2/P_1. (Yeah, right.) OK, here is what you get:

Equation 7–2 Converting Decibel Values to Power Levels

$$\frac{P_2}{P_1} = 10^{(L_{dB}/10)}$$

Equation 7-2 looks forbidding, but it is simple. Divide the L_{dB} value by 10. Then raise 10 to that power. Here is how it looks in Excel:

$$(P_2/P_1) = 10\text{^}(L_{db}/10)$$

For example, try an L_{dB} value of 20. Obviously, 20 divided by 10 is 2. Ten squared is 100. So an L_{dB} value of 20 corresponds to a power ratio of 100. Of course, you already knew that.

Test Your Understanding

13. a) Using a spreadsheet program, compute the decibel value for a ratio of 17:1. b) For 1/33. c) Estimate, without using Excel, the decibels for a ratio of 8/1. d) For 1/20. e) For 1/8. f) For 16/1. g) Estimate, without using Excel, the decibels for a ratio of 80/1. h) For 1/40. i) For 1/800. j) For 16,000/1. k) Estimate, without using Excel, the dBm value for 2 mW. l) For a radio with 16 mW. m) For a radio with 2 W. n) For a radio with 0.2 W
14. a) Estimate the final dBm value for a radio if the radio has .1 Watt of power, if there is a 4:1 amplifier before transmission, and if there is attenuation to 1/8 the original signal strength between the sender and receiver. b) Estimate the final dBm value for a radio if the radio has .4 Watt of power, if there is a 10:1 amplifier before transmission, and if there is attenuation to 1/1,000 the original signal strength between the sender and the receiver, and if the receiver's antenna loses half of the signal strength before delivering the signal to the receiver.
15. a) What power ratio does –30 dB represent? b) What power ratio does –21 dB represent? c) What absolute power does 78 dBm represent?

OTHER LOCAL WIRELESS TECHNOLOGIES

The 802.11 Wi-Fi standards were designed to work with Ethernet. In fact, many have called 802.11 "wireless Ethernet." With service radiuses of 30 meters and larger, 802.11 access points can cover the substantial distances required for office-wide communication. In addition, 802.11 access points are designed to work together to cover much larger areas, such as corporate buildings. Their speeds allow them to serve quite a few wireless clients in an area, giving each client fast Internet access, file transfers, video, and other processes that require reasonably high throughput. To serve such long distances, of course, access points consume quite a bit of electrical power. They must be connected to the main electrical lines of the building or to Ethernet switches with power over Ethernet (which we saw in Chapter 5).

Not all local application needs require such large service distances and high speeds. For their more modest requirements, other local wireless technologies have been developed. These technologies offer shorter transmission distances and lower speeds. In compensation, they have much smaller energy requirements. This makes them suitable for even hand-held devices. In this section, we will look at two of these low-performance low-energy technologies, Bluetooth and near field communication (NFC).

Figure 7-12 shows the main characteristics of 802.11, Bluetooth, and NFC. It also gives the main characteristics of ultrawideband (UWB) transmission which has the short distance limitation of Bluetooth but offers far higher speeds (and power consumption).

Characteristic (Typical)	802.11	Bluetooth	Near Field Communication (NFC)	Ultrawideband (UWB)
Use	Typically, infrastructure WLANs linked to Ethernet switches Wi-Fi Direct gives direct communication between two wireless hosts	Personal area networks (PANs) around a desk or a person's body	Very-near communication between two wireless hosts	Extremely high-speed short-distance transmission
Typical Speed	20–300 Mbps	2 Mbps	106, 212, or 424 kbps	100 Mbps
Service Range	30–50 m	10 m	10 cm	10 m
Requires Wall Power	Yes	No	No	Yes
Service Band	2.4 and 5 GHz	2.4 GHz	13.56 kHz	UWB channels typically span multiple entire service bands

FIGURE 7-12 Local Wireless Technologies

In Chapter 6, we saw that newer 802.11 standards allow Wi-Fi Direct communication, in which two wireless hosts communicate peer-to-peer without using an access point. This reduces the difference in scope between 802.11 and Bluetooth.

Bluetooth

If you have a wireless headset for your mobile phone or pocket music player, if you have a wireless mouse and keyboard, or if you have a hands-free cellular system in your car, you may already be using Bluetooth. These are precisely the kinds of short-distance modest-speed applications Bluetooth was created to handle. **Bluetooth** is a short-range radio technology that is designed for **personal area networks (PANs)**—small groups of devices around a person's body or in the area around a desk.

THREE MODES OF OPERATION How fast is Bluetooth? The answer is that the latest version of the Bluetooth standard, Bluetooth 4.0, has three modes of operation with different transmission speeds and power requirements. Figure 7-13 illustrates these three modes.

Classic Bluetooth The 802.11 standards are created by the IEEE Standards Association's 802.11 Working Group. In contrast, Bluetooth is created by the **Bluetooth Special Interest Group**, an association of hardware manufacturers and other

	Classic Bluetooth	High-Speed Bluetooth	Low-Energy Bluetooth
Principal Benefit	Good performance at low power	High-speed transfers available when needed	Ultra-long battery life and ultra-fast setup times
Speed	Up to 3 Mbps	Up to about 24 Mbps	Up to 200 kbps
Expected Duty Cycle	Low to high	Low to high	Very low
Power Required	Low	High	Very low
Distance	~10 m	~30 m	~15 m
Setup Time	< 6 s	Not given	< 3 ms

FIGURE 7-13 Bluetooth Modes of Operation (Study Figure)

organizations. The original version of Bluetooth, created in 1994, has extremely low transmission rates—only 721 kbps in one direction and about one tenth that speed in the other direction. Bluetooth 2.0 through 2.2 introduced what most people think of as the "standard" Bluetooth speed of 2 to 3 Mbps. This is still very slow compared to current versions of 802.11, but it is fast enough for voice communication and even modest-quality video transmission. This is now called **classic Bluetooth**.

High-Speed Bluetooth In 2009, the Bluetooth SIG introduced Bluetooth 3.0. This introduced a new mode of Bluetooth transmission, **high-speed Bluetooth**. This new mode retains ordinary Bluetooth speeds for most operations. However, for operations that require higher speeds, such as webpage downloads, a Bluetooth device capable of high-speed Bluetooth can turn on a second radio that uses a version of 802.11 limited to peer-to-peer transmission between two devices. In other words, the Bluetooth SIG "borrowed" radio transmission technology from its rival, 802.11. Of course, this requires two radios in the phone—one to implement Layer 1 and Layer 2 of classic Bluetooth and one to implement the same layers in 802.11. High-speed Bluetooth consumes a good deal of power, like regular 802.11. However, high-speed Bluetooth conserves battery power by only using faster speeds when they are needed. In the future, high-speed Bluetooth may be used for other radio transmission standards as well, such as ultra-wideband transmission, which we will see a little later in this section.[18]

Low-Energy Bluetooth In 2010, the Bluetooth SIG introduced Bluetooth 4.0. In addition to other improvements, this standard introduced a third mode of operation, **low-energy Bluetooth**. Low-energy Bluetooth is for device pairs that have low duty cycles, that is, only communicate with each other a small percentage of the time, such as 0.25 percent. For devices that are used this way, low-energy Bluetooth allows devices with "coin" batteries to work for several years on a single battery. Low-energy Bluetooth also reduces power by restricting transmission speed to about 200 kbps.

[18] In general, non-Bluetooth radio transmission alternatives are called alternative mac/phy (AMP).

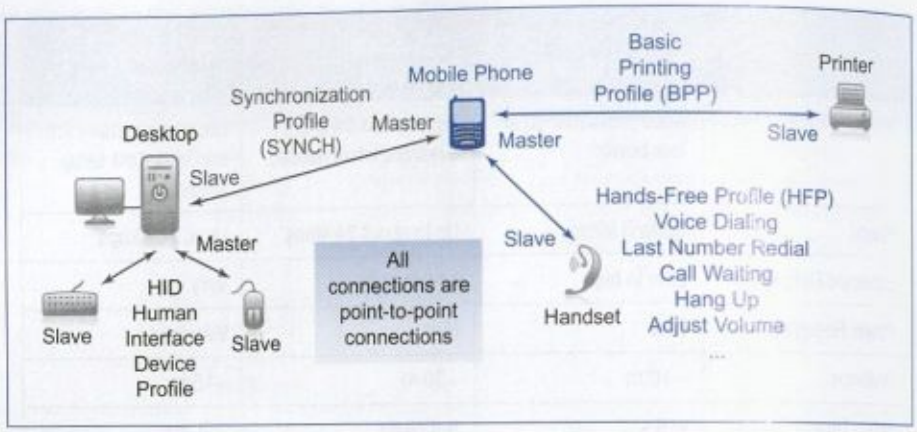


FIGURE 7-14 Bluetooth Operation

As a side benefit low-energy Bluetooth operation, there is an extremely short setup time—less than 3 milliseconds as compared to classic Bluetooth's less than 6 second setup time.

ONE-TO-ONE, MASTER–SLAVE OPERATION Figure 7-14 shows how several devices communicate through Bluetooth. The device in the top center is a mobile phone. To its right is a printer. The mobile phone user wishes to print a webpage on the mobile's screen. It selects print, chooses the target printer, and prints. In seconds, the user walks up to the printer and picks up the output.

Bluetooth always uses a **one-to-one** connection between a pair of devices. There is no many-to-many networking, as is possible with 802.11 and Ethernet. Reducing operation to one-to-one communication simplifies Bluetooth protocols.

Bluetooth always uses point-to-point communication between a pair of devices.

Bluetooth also uses **master–slave control**. One device is the master, and the other device is the slave. In the printing scenario, the mobile device is the master and the printer is the slave. The mobile phone drives the printing process.

In Bluetooth, one device is the master and the other device is the slave.

Although communication is always one-to-one communication, a master may have multiple slaves. In addition to controlling the printer, the mobile phone in Figure 7-14 also controls the user's hands-free handset. In this case, a single master controls two slaves. However, the operation is still one-to-one. The mobile phone's connections to the two devices are separate Bluetooth connections.

The desktop computer on the left side of the figure also controls two slaves—a keyboard and a mouse. In both of these cases, then, there was one master and two slaves. Can there be more than two slaves, and, if so, how many slaves can a master have? In Bluetooth, a master may have up to seven slaves. A master and its slaves are called, collectively, a **piconet**. A piconet may therefore have up to eight devices—one master and seven slaves. Most masters have only one or two.

A master and its slaves are called, collectively, a piconet. A piconet will have a master and up to seven slaves.

It is even possible for a Bluetooth device to be a master and slave simultaneously. Consider the relationship between the mobile phone and the desktop computer. The two are synchronizing information. The mobile phone is the master, and the desktop is the slave. However, we have just seen that the desktop is master to the keyboard and mouse.

A Bluetooth device may be a master of one device and a slave to another device simultaneously.

Although one device is always the master and the other the slave, they sometimes switch roles during an interaction. For example, when the wearer of a hands-free headpiece initiates a call, the headpiece is the master and the mobile phone is the slave. However, they switch roles afterward, allowing the more powerful mobile phone to control the call interactions.

BLUETOOTH PROFILES Like 802.11, Bluetooth specifies transmission at the physical and data link layers. The 802.11 Working Group did not have to worry about applications because devices on local area networks have traditionally had many applications.

However, the Bluetooth SIG faced a different situation. Not only were there no transmission standards for short-range one-to-one communication; there also were no application protocols in existence. Consequently, in addition to defining transmission standards, the SIG also defined application profiles, which are called Bluetooth profiles. Profiles govern how devices share information and control messages for various uses.

- In Figure 7-14, the mobile phone communicates with the hands-free handset using the **Hands-Free Profile (HFP)**. This profile governs device–device communication for voice dialing, adjusting volume, hanging up, number redial, call waiting, and other telephone use actions.
- For printing, the mobile phone uses the **Basic Printing Profile (BPP)**. For synchronizing information with the desktop computer, the mobile phone uses the **Synchronization Profile (SYNCH)**.
- The desktop, in turn, uses the **Human Interface Device (HID) profile**. This is probably the most widely used profile.

Peering

When two devices first encounter each other, they must go through a negotiation process
This negotiation process is called peering
It involves the exchange of device information
It may involve authentication
It may also involve one or both of the device owners explicitly deciding if the two devices should be allowed to communicate

Service Discovery Profile (SDP)

Peering uses the Service Discovery Profile (SDP)
Normally, a device is in discoverable mode
If it receives a Service Discovery Protocol request, it will send information about itself:
- Name
- Device class
- Bluetooth profiles supported
- Technical information such as manufacturer's name
- ...

Binding

After peering is complete, the two devices are bound
They can begin communicating
If they are brought together later, they are still bound
They will begin communication without the peering process
This allows fast setup
The owner of either device can end the binding

FIGURE 7-15 Peering and Binding (Study Figure)

Corporate buyers need to be astute about Bluetooth profiles. In many cases, there are multiple profiles that do roughly the same thing but vary in functionality. For example, the *Bluetooth Headset Profile (HSP)* allows hanging up and volume adjustment. However, it does not support other useful functions that users would like. For that, companies should purchase headsets that implement the *Hands-Free Profile (HFP)*. This profile defines advanced telephone control features such as call waiting and voice dialing.

PEERING AND BINDING For two Bluetooth devices to work together, they must first go through an initial handshaking stage called **peering**. This will require them to exchange information about themselves. It may also involve authentication and requiring each device owner to decide whether to allow the two devices to communicate or not.

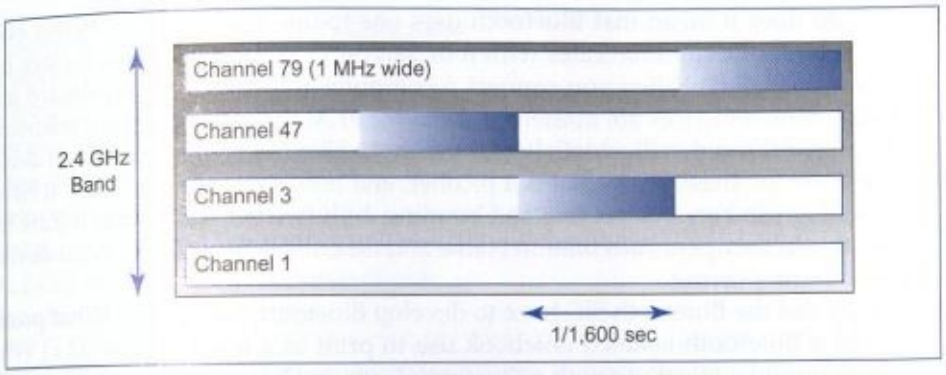


FIGURE 7-16 Frequency Hopping Spread Spectrum

Peering uses the Bluetooth **Service Discovery Profile (SDP)**. Bluetooth devices are normally in discoverable mode. In this mode, when they receive a Service Discovery Profile request, they will transmit information about themselves, including device name, device class, lists of Bluetooth profiles supported, and technical information such as the device's manufacturer and model.

Once two devices have peered, they are said to have been bound. **Binding** is semi-permanent. When the two devices again encounter each other, they do not have to go through peering again. They are bound, so they connect very quickly and without human intervention. Of course, the owner of either of the devices may end the binding at any time.

BLUETOOTH RADIO TRANSMISSION Bluetooth operates in the same 2.4 GHz band that 802.11 uses. However, 802.11 uses 20 MHz-wide channels, while Bluetooth divides the service band into seventy-nine 1 MHz channels. Up to every 1,600 microseconds, Bluetooth jumps to a different 1 MHz channel. This is called **frequency hopping spread spectrum**. (See Figure 7-16.)

All but the earliest Bluetooth devices avoid channels if they are already carrying traffic. This permits Bluetooth devices to only use free channels, increasing the probability that the Bluetooth communication will get through. This practice also minimizes interference between Bluetooth and 802.11 transmission in the 2.4 GHz unlicensed band.

Test Your Understanding

16. a) What is a PAN? (Do not just spell it out.) b) What organization creates Bluetooth standards? c) Compare the speeds, distances, and duty cycles of classic Bluetooth, high-speed Bluetooth, and low-energy Bluetooth. d) What do these characteristics mean for battery life? e) What is the other benefit of low-energy Bluetooth? f) Would two devices typically use high-speed Bluetooth during their total communication time? Explain.

17. a) What does it mean that Bluetooth uses one-to-one operation? b) Is this even true if a master communicates with four slaves? c) What does master–slave operation mean? d) When you connect a computer to a Bluetooth keyboard and mouse, which devices are masters and slaves? e) At the beginning of a telephone call placed through a Bluetooth headset with the Hands-Free Profile, which device is initially the master? f) What is a piconet, and how many devices may it have? g) Distinguish between peering and bonding. h) If two devices communicate frequently, do they peer each time? i) Name and describe the profile that two devices use to begin peering.
18. a) Why did the Bluetooth SIG have to develop Bluetooth profiles? b) What profile would a Bluetooth-enabled notebook use to print to a nearby printer? c) What profile would a tablet use with a Bluetooth keyboard? d) What *two* profiles might a mobile phone use to communicate with a headset? e) Which is a better profile to use and why? Be specific.
19. a) What service band does Bluetooth use? b) Describe the type of spread spectrum transmission classic Bluetooth uses. c) What other major local wireless technology uses this service band? d) What does Bluetooth do to minimize interference with other wireless technologies in this band?

Near Field Communication (NFC)

REDUCING DISTANCE AND POWER REQUIREMENTS TO THE EXTREME Reducing the service distance between devices reduces transmission power and therefore increases battery power. Taken to the logical extreme, the greatest reduction in transmission power would occur if two devices were physically "bumped" together. In fact, there is a technology that does precisely this. It is called **near field communication (NFC)**. It is governed by the NFC Forum. Figure 7-17 illustrates near field communication.

In NFC, the two devices actually do not have to touch physically. However, they must be within about 4 cm (roughly 2 in.). It is difficult to judge such small distances, so the normal practice is to bump the two devices to ensure communication.

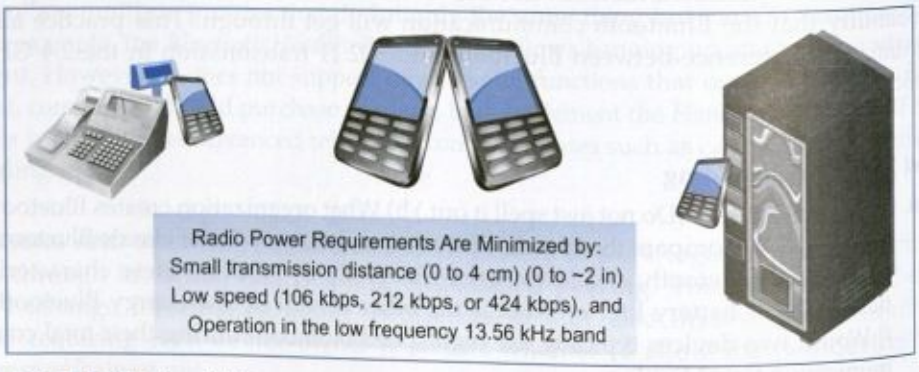


FIGURE 7-17 Near Field Communication (NFC)

Payment of bus fares (already popular in some countries)
Opening car doors
Turning on the ignition
Door entry control
Sharing business cards
Sharing webpages between mobile devices
Retail payments, including loyalty points and coupons (beginning to be popular)
NFC posters with tap points for more communication
Passive Radio Frequency ID (RFID) Tags

FIGURE 7-18 Possible Near Field Communication Applications (Study Figure)

With direct contact or nearly direct contact, transmission distances are small, so transmission power is very low. In addition, the transmission speed is only 106 kbps, 212 kbps, or 424 kbps. Slow transmission also minimizes transmission power. In addition, NFC operates at the 13.56 kHz band. This is a far lower frequency band than the 2.4 GHz and 5 GHz bands. At these lower frequencies, radios use less power than they are at gigahertz frequencies. Overall, NFC devices are very energy efficient. They often use inexpensive "coin" batteries, and these batteries may last for months or even years.

APPLICATIONS NFC has many possible applications. For example, consider Vishal, who is late to an office meeting. As Vishal leaves his house, he taps his mobile phone against the front door, activating the intruder alarm. He walks to his car and taps the handle with his mobile. This unlocks the car. It also moves the driver's seat to his preferred position. Bumping the ignition with the mobile turns on the car.

At work, Vishal taps his mobile against the building door to gain admittance. To share business cards, he and a visitor tap their phones together. To share a webpage, they do the same.

At the building's convenience store, Vishal bumps his mobile against the reader to pay for a purchase. This also records his loyalty points for the purchase and makes use of any coupons Vishal had loaded onto his mobile last night. On his way out, he sees a poster advertising a new ice cream flavor, chicken ripple. He bumps his phone against a small mark on the poster. This transfers information about the product to his mobile.

RFID TAGS Many items on the store shelf have small wire arrangements embedded in paper or plastic. These are **passive radio frequency ID (RFID) tags**.[19] When Vishal bumps his mobile against one of these tags, his phone receives the price and some other information about the product. The store uses these passive RFID tags to maintain

[19] Active RFID tags contain batteries and can be read from longer distances.

information about its inventory. Using RFID also speeds scanning at checkout. There is no need to line up the item's UPC tag with a laser reader.

The selection of 13.56 kbps as the operating frequency was no accident. This is the frequency that ISO/IEC had already assigned for communication with passive RFID tags. The NFC Forum has defined four tag types with different speed and distance capabilities.

For passive applications, a target device being bumped has no power source at all. When the two devices are brought together, the powered device sends a pulse of radio to the passive device. This provides just enough power for the passive device to generate a reply. This is the same basic process that allows wireless device recharging.

APPLICATIONS IN USE TODAY Although many of the applications we discussed are years away, NFC is already seeing some use. One popular application is to use a card specifically designed to allow someone to use a bus or subway. The user simply taps the card against a reader near the front of the bus. It may not even be necessary to take the card out of the wallet. This application is very popular in Europe and Japan.

Another application with growing popularity is the use of mobile phones as electronic wallets for making purchases. This requires special NFC readers in stores. Several European and Asian countries have experimented with NFC wallets for some time. In 2011, Google released its NFC Google Wallet specification in the United States, and a number of companies such as Starbucks quickly began to implement it.

SECURITY Security is a concern for NFC. For passive devices in particular, cryptographic protections usually are prohibitively power-demanding. It has been said that given the small distances at which passive devices can be read, eavesdroppers would have no chance to read transmissions. However, eavesdroppers may have extremely sensitive highly directional receivers capable of reading transactions at some distance away. NFC communication is also vulnerable to data modification attacks and to jamming denial of service attacks.

Test Your Understanding

20. a) What is the distance limit for near field communication? b) What three factors give NFC low transmission power requirements? c) In what transmission band does NFC operate? d) At what speeds does NFC operate? e) Passive RFID chips have no batteries. How can they transmit when queried? f) How can attackers eavesdrop on NFC transmissions?

Radio frequency ID tags contain information about an item
A passive RFID tag has no internal power source
When read by an NFC device, the power of the reader request gives power for the response
13.56 kHz was specified by ISO/IEC for passive RFID tags long before NFC standards were created
With sensitive antennas, NFC transmission can be eavesdropped upon from a distance

FIGURE 7-19 Passive Radio Frequency ID (RFID) Tags (Study Figure)

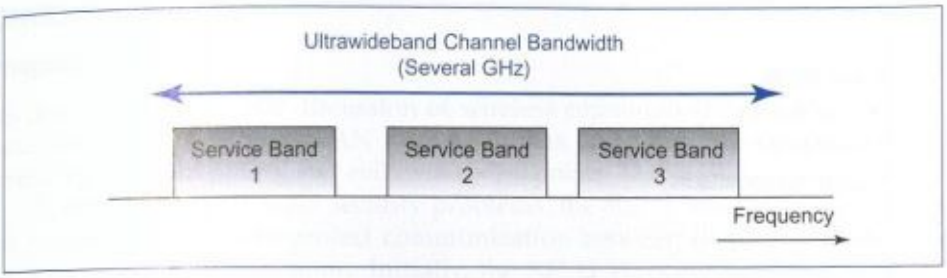


FIGURE 7-20 Ultrawideband (UWB) Transmission

Ultrawideband (UWB)

In 802.11, a channel is 20 MHz or 40 MHz wide. We saw in Chapter 6 that wider wireless transmission channels permit the faster transmission of information. **Ultrawideband (UWB)** transmission channels are far wider than 802.11 channels. Often, UWB channels are several gigahertz wide. They typically are so wide that they cut across multiple service bands (see Figure 7-20).

To avoid interfering with other devices, the power per hertz of bandwidth is very low—far lower than 802.11 power densities. This is necessary because it is important for UWB not to interfere with other transmissions taking place within its enormous bandwidth. In effect, a UWB transmission is like an enormously wide ocean wave arriving at a shore. The total energy is very large, but the wave usually has a gentle effect on each foot of shoreline.

UWB transmission typically produces very high transmission speeds, often 100 Mbps or more. However, it has very short range—about 10 meters, which is the typical distance limit for classic Bluetooth. UWB is likely to be used for local video transmission.

UWB standardization has lagged behind advances in other local wireless technologies. At the time of this writing, UWB is promising, but its standardization is so incomplete that manufacturers are not investing heavily in it. If the standards situation settles out, this could change rapidly.

Test Your Understanding

21. a) How does UWB achieve high data rates? b) How does UWB avoid interfering with other transmissions within its channel bandwidth? c) What is UWB's major limitation?

Security in Emerging Local Wireless Transmission Technologies

Security is a complex situation for emerging local wireless transmission technologies. These technologies face a number of serious threats, including eavesdropping, data modification, impersonation, and denial-of-service attacks.

Some of these technologies have no cryptographic security at all. The classic example is using NFC to read passive RFID tags. Bluetooth probably has the best security among emerging wireless technologies, but its security is still weaker than

Threats

Eavesdropping
Data modification
Impersonation
Denial-of-service attacks

Cryptological Security

Some have no cryptological security
Example: Near field communication for reading passive ID tags
They rely on short transmission distances to foil eavesdroppers
Directional antennas and amplifiers can defeat this

Strength of Security

Some have reasonably good security
Example: Bluetooth
However, still not as strong as 802.11i and WPA security

Device Loss or theft

In this age of bring your own device (BYOD) to work, this is a serious problem
Most devices are only protected by short PINs

Maturity

In general, new security technologies take some time to mature
During this period, they often have vulnerabilities that must be fixed quickly
User companies must master security for each new technology

FIGURE 7-21 Security in Emerging Wireless Technologies (Study Figure)

802.11i or WPA. In today's world of bring your own device (BYOD) at work, emerging local wireless technologies make a worrisome corporate security situation even more problematic. For example, if devices such as mobile phones are lost or stolen, they are often protected only by brief PINs. Any thief who discovers the PIN may be able to impersonate the owner in significant transactions.

In general, security for new local wireless technologies is simply new. As a general rule, new security technologies tend to have vulnerabilities that take time to discover and protect against. One must hope that technology vendors will be quicker to act than attackers. In any case, companies need to fully understand security for each technology.

Test Your Understanding

22. a) What threats do new wireless transmission technologies face? b) Describe the state of cryptographic security for new transmission standards. c) Why is device theft or loss a serious danger?

CONCLUSION

Synopsis

This chapter continues our discussion of wireless communication. We began with a discussion of 802.11 wireless LAN security threats, including drive-by hackers, war drivers, rogue access points, and evil twin access points.

To address most of these security problems, the 802.11 Working Group created core security standards to protect communication between the wireless client and its nearest wireless access point. Initially, the 802.11 Working Group created WEP as a core security protocol. WEP was badly designed and was soon easily exploited. Later, the 802.11 Working Group created the excellent 802.11i core security standard. Before they did, the Wi-Fi Alliance used an early draft of 802.11i to create a somewhat weaker core security protocol, WPA. They did this because they could develop WPA more quickly, and the industry badly needed something better than WEP. WPA has not been completely cracked, but parts of it have, so companies are advised to upgrade to 802.11i.

The 802.11 Working Group based 802.11i on the 802.1X security standard we saw in Chapter 5. The 802.1X standard uses a central authentication server. However, they needed to extend 802.1X by adding security between the access point and each wireless client during initial authentication, before full 802.1X security is set up. The 802.11i standard also has a pre-shared key mode, which is used for companies that only have a single access point. The wireless clients share a single pre-shared key, which must be kept secret from outsiders. After authentication, however, the wireless access point creates a unique session key for each wireless client.

Evil twin access points impersonate legitimate access points. To avoid being snared by evil twin access points, the clients need to have a virtual private network (VPN) connection to the servers they will use. This connection must use a pre-established secret that is not transmitted during interactions and so cannot be intercepted by the evil twin access point. We also looked at security problems with Wi-Fi Protected Setup (WPS) and looked briefly at the danger of denial-of-service (DoS) attacks.

We discussed wireless LAN management, including strategies for placing access points to give good coverage with a minimum of overlap and with a minimum of interference from nearby access points operating on the same channel. Good access point placement requires initial and ongoing site surveys of signal strength and interference. We also looked at the remote management of access points using smart access points or dumb access points controlled by wireless LAN switches. A central manager can detect rogue access points, allow the remote adjustment of access point power, push software updates out to the access points, and do all this and more automatically, with a minimum of intervention.

We looked at other local wireless technologies, including Bluetooth, which is for personal area networks (PANs) in which all devices are located nearby, often on the same desk or around the body of a person. We then looked at other emerging local wireless technologies, including high-speed, short-distance ultrawideband (UWB) transmission, ZigBee for wireless monitoring systems, and radio frequency ID (RFID) to allow items to be identified within a short distance of a scanner.

END-OF-CHAPTER QUESTION

Essay

1. A friend is interested in installing a wireless LAN in her small business. She has about a dozen employees. She is concerned about security. Write a two-page letter to explain what security threats she is facing and how she can reduce these threats. Remember that you are writing for a friend, not for a teacher. Do not hand in disorganized notes. Double spacing is good.

Perspective Questions

1. What was the most surprising thing you learned in this chapter?
2. What was the most difficult part of this chapter for you?

8 TCP/IP INTERNETWORKING I

LEARNING OBJECTIVES

By the end of this chapter, you should be able to:

- Explain basic TCP/IP, IP, TCP, and UDP concepts.
- Define hierarchical IP addresses, networks and subnets, border and internal routers, and masks.
- Describe router operation when a packet arrives, including ARP. Given a routing table and an arriving packet's destination IP address, be able to predict what the router will do.
- Explain the IPv6 packet header fields and IPv6's use of extension headers. Be able to convert a 128-bit IP address into compressed hexadecimal notation.
- Explain TCP fields and session closings.
- Explain other important TCP/IP standards, including dynamic routing protocols and ICMP.

INTRODUCTION

Switched networks and wireless networks are governed by standards at Layer 1 and Layer 2. We looked at switched wired single networks in Chapter 5. We looked at wireless single networks in Chapters 6 and 7. In this chapter and in Chapter 9, we will discuss internetworking, which is governed by Layer 3 and Layer 4 standards.

We will only look at TCP/IP internetworking because TCP/IP dominates the work of network professionals at the internet and transport layers. However, real-world routers cannot limit themselves to TCP/IP internetworking. They are multiprotocol routers, which can route not only IP packets but also IPX packets, SNA packets, AppleTalk packets, and other types of packets.

TCP/IP RECAP

The TCP/IP Architecture and the IETF

We first looked at TCP/IP in some depth in Chapter 2. Recall from that chapter that the *Internet Engineering Task Force (IETF)* sets TCP/IP standards. TCP/IP is an architecture for setting individual standards. Figure 8-1 shows a few of the standards the IETF has created within this architecture. Some of the standards are shaded in this figure. We will look at these standards in this chapter.

Layer	User Applications			Supervisory Applications		
5 Application	HTTP	SMTP	Many Others	DNS	Dynamic Routing Protocols	Many Others
4 Transport	TCP				UDP	
3 Internet	IP			ICMP		ARP
2 Data Link	None: Use OSI Standards					
1 Physical	None: Use OSI Standards					

FIGURE 8-1 Major TCP/IP Standards

Note: Shaded protocols are discussed in this chapter.

Simple IP at the Internet Layer

Recall also, from Chapter 1, that internetworking operates at two layers. The internet layer moves packets from the source host to the destination host across a series of routers. Figure 8-1 shows that the primary standard at the internet layer is the Internet Protocol (IP). Figure 8-2 shows that IP is a simple (connectionless and unreliable) standard. This simplicity minimizes the work that each router has to do along the way, thereby minimizing routing costs. The internet layer is Layer 3.

Reliable Heavyweight TCP at the Transport Layer

In turn, TCP at the transport layer corrects any errors at the internet layer and lower layers as well. As we saw in Chapter 2, when the transport process on a destination host receives a TCP supervisory or data segment, it sends back an acknowledgment. If the transport process on the source host does not receive an acknowledgment for a TCP segment, it resends the segment. TCP is both connection-oriented and reliable, making it a heavyweight protocol. However, the work of implementing TCP only occurs on the source and destination hosts, not on the many routers between them. This keeps the cost of reliability manageable. The transport layer is Layer 4.

Protocol	Layer	Connection-Oriented/ Connectionless	Reliable/ Unreliable	Lightweight/ Heavyweight
TCP	4 (Transport)	Connection-oriented	Reliable	Heavyweight
UDP	4 (Transport)	Connectionless	Unreliable	Lightweight
IP	3 (Internet)	Connectionless	Unreliable	Lightweight

FIGURE 8-2 IP, TCP, and UDP

Unreliable Lightweight UDP at the Transport Layer

In Chapters 1 and 2, we saw that TCP/IP offers an alternative to heavyweight TCP at the transport layer. This is the User Datagram Protocol (UDP). Like IP, UDP is simple (connectionless and unreliable) and lightweight protocol. This reduces processing requirements on the hosts and also reduces network traffic.

Test Your Understanding

1. a) Compare TCP and IP along the dimensions in Figure 8-2. b) Compare TCP and UDP along the dimensions in Figure 8-2.

IP ROUTING

In this section, we will look at how routers make decisions about forwarding packets—in other words, how a router decides which interface to use to send an arriving packet back out to get it closer to its destination. (In routers, ports are called **interfaces**.)

Router ports are called interfaces.

This forwarding process is called **routing**. Router forwarding decisions are much more complex than the Ethernet switching decisions we saw in Chapter 5. As a consequence of this complexity, routers do more work per arriving packet than switches do per arriving frame. Consequently, routers are more expensive than switches for a given level of traffic. A widely quoted network adage reflects this cost difference: "Switch where you can; route where you must."

When routers forward incoming packets closer to their destination hosts, this is routing.

Hierarchical IP Addressing

To understand the routing of IP packets, it is necessary to understand IP addresses. In Chapter 1, we saw that IP Version 4 (IPv4) addresses are 32 bits long. However, IP addresses are not simple 32-bit strings. They have internal structure, and this internal structure is important in routing.

HIERARCHICAL ADDRESSING As Figure 8-3 shows, IP addresses are **hierarchical**. They usually consist of three parts that locate a host in progressively smaller parts of the Internet. These are the network, subnet, and host parts. We will see later in this chapter that hierarchical IP addressing simplifies routing tables.

Network Part First, every IP address has a **network part** which identifies the host's network on the Internet. In this case, *network* is an organizational concept. It is a user organization such as a manufacturing corporation or an ISP. The organization effectively controls part of the Internet.

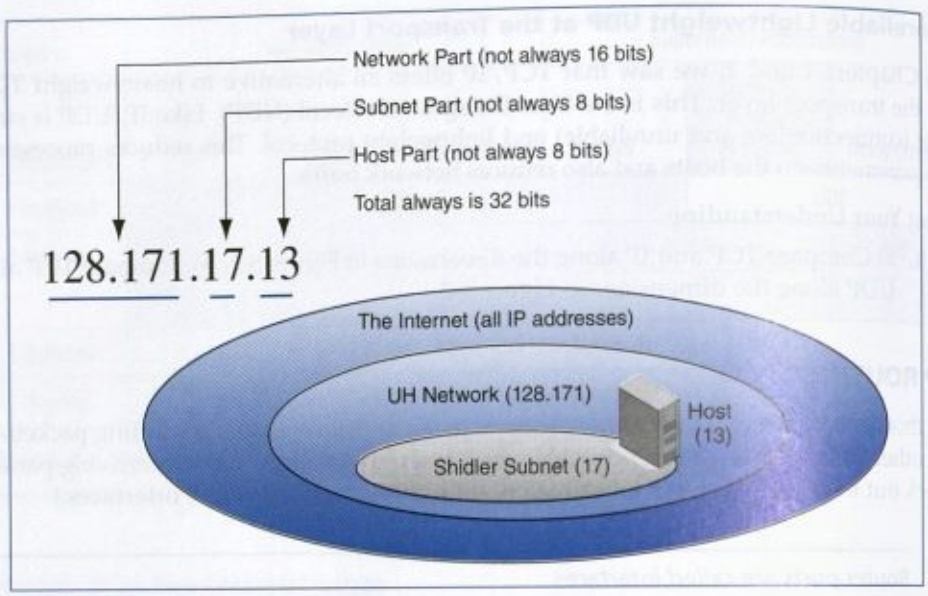


FIGURE 8-3 Hierarchical IPv4 Address

In IP addressing, network is an organizational concept. A network is an organization that controls part of the Internet. It may be a user organization such as a manufacturing corporation or an ISP.

In Figure 8-3, the network part is 128.171. This is two IP segments. Each segment is 89 bits long, so the network part for the University of Hawai`i is 16 bits long. This happens to be the network part for the University of Hawai`i Network on the Internet. All host IP addresses within this network begin with 128.171.

Do not get hung up on the network part being 16 bits. This is only an example. Different organizations have different network parts that range from 8 to 24 bits in length.

Subnet Part Most large organizations further divide their networks into smaller units called **subnets**. After the network part in an IP address come the bits of the **subnet part**. The subnet part bits specify a particular subnet within the network.

For instance, Figure 8-3 shows that in the IP address 128.171.17.13, the first 16 bits (128.171) correspond to the network part, and the next 8 bits (17) correspond to a subnet on this network. (Subnet 17 is the Shidler College of Business subnet within the University of Hawai`i Network.) All host IP addresses within this subnet begin with 128.171.17.

Again, do not get hung up on the subnet part being 8 bits long. In different organizations, subnet lengths vary widely. Keep clear in your head that the UH Network is only being used as an example.

Host Part The remaining bits in the 32-bit IP address constitute the **host part**, which identifies a particular host on the subnet. In Figure 8-3, the host part is eight

bits long with a value of 13. This corresponds to a particular host, 128.171.17.13, on the Shidler College of Business subnet of the University of Hawai`i Network. Again, host parts in different organizations differ in size.

VARIABLE PART LENGTHS The IPv4 IP address is 32 bits long. Can you tell just by looking at an IP address what bits correspond to the network, subnet, and host parts? The answer is no. For instance, if you see the IP address 60.47.7.23, you may have an 8-bit network part of 60, an 8-bit subnet part of 47, and a 16-bit host part of 7.23. In fact, parts may not even break conveniently at 8-bit boundaries. The only thing you can tell when looking at an IP address by itself is that it is 32 bits long.

Test Your Understanding

2. a) What is routing? b) What are the three parts of an IP address? c) How long is each part? d) What is the total length of an IP address? e) In the IP address, 10.11.13.13, what is the network part?

Routers, Networks, and Subnets

BORDER ROUTERS CONNECT DIFFERENT NETWORKS As Figure 8-4 illustrates, networks and subnets are very important in router operation. Here we see a simple site internet. The figure shows that a **border router**'s main job is to connect different networks. This border router connects the 192.168.x.x network within the firm to the 60.x.x.x network of the firm's Internet service provider. Here, the xs are the remaining bits of the IP address, so 192.168 and 60 are the network parts of the two networks.

A border router's main job is to connect different networks.

INTERNAL ROUTERS CONNECT DIFFERENT SUBNETS The site network also has an internal router. An **internal router**, Figure 8-4 demonstrates, connects different subnets within a firm—in this case, the 192.168.1.x, 192.168.2.x, and 192.168.3.x subnets. Many sites have multiple internal routers to link the site's subnets.

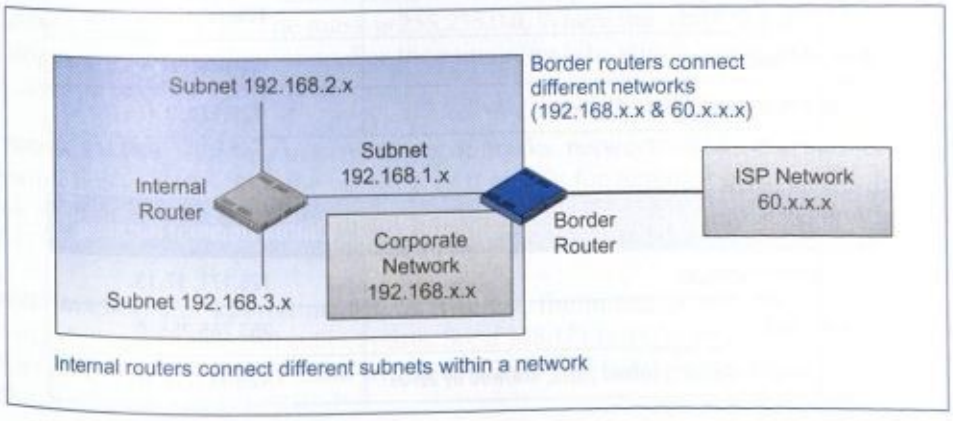


FIGURE 8-4 Border Router, Networks, and Subnets

An internal router only connects different subnets within a firm.

Test Your Understanding

3. Connecting different networks is the main job of what type of router? b) What type of router only connects different subnets?

Network and Subnet Masks

If you know how the University of Hawai'i organizes its IP addresses, you know that the first 16 bits are always the network part, the next 8 are the subnet part, and the final 8 are the host part. However, the sizes of the network, subnet, and host parts differ. Routers need a way to tell the sizes of key parts. The tool that allows them to do it is masks.

32-BIT STRINGS Figure 8-5 illustrates how masks work. A mask is a series of 32 bits like an IP address. However, a mask always begins with a series of 1s, followed by a series of 0s. In a network mask, the bits in the network part of the mask are 1s, while the

The Problem

There is no way to tell by looking at an IP address what sizes the network, subnet, and host parts are—only their total of 32 bits

The solution: masks

Series of initial ones followed by series of final zeros for a total of 32 bits

Example: 255.255.0.0 is 16 ones followed by 16 zeros

In prefix notation, /16

(Decimal 0 is 8 zeros and Decimal 255 is 8 ones)

Result: IP address where mask bits are ones and zeros where the mask bits are zero

Mask Operation

Network Mask	Dotted Decimal Notation
Destination IP address	128.171.17.13
Network mask	255.255. 0. 0
Bits in network part, followed by zeros	128.171. 0 .0

Subnet Mask	Dotted Decimal Notation
Destination IP address	128.171. 17.13
Subnet mask	255.255.255. 0
Bits in network part and subnet parts, followed by zeros	128.171. 17. 0

FIGURE 8-5 IP Network and Subnet Masks

remaining bits are 0s. In subnet masks, the bits of both the network and subnet parts are 1s, and the remaining bits are 0s.

A mask is a 32-bit string of 1s and 0s.
The mask always has a certain number of initial 1s. The remaining bits are always 0s.
In network masks, the initial 1s correspond to the network part.
In subnet masks, the initial 1s correspond to the network and subnet parts.

For example, suppose that the mask is 255.255.0.0. This means that the four 8-bit segments have the values 255, 255, 0, and 0. In dotted decimal notation eight 1s is 255 and eight 0s is 0. So the four segments have, in order, eight 1s, eight 1s, eight 0s, and eight 0s. Putting this together, the mask has sixteen 1s followed by sixteen 0s.

PREFIX NOTATION FOR MASKS Writing 255.255.255.0 is not very difficult, but networking professionals often use a shortcut called prefix notation. The mask 255.255.255.0 is twenty-four 1s followed by eight 0s. In prefix notation, this mask is represented by /24. Do you see the pattern? In **prefix notation**, a mask is represented by a slash followed by the number of initial 1s in the mask. What about 255.0.0.0? Yes, it is /8. Prefix notation is simpler to write than dotted decimal notation. By the way, we call this prefix notation because it focuses on the first part of the mask—the part that is all 1s.

In prefix notation, a mask is represented by a slash followed by the number of initial 1s in the mask.

Another advantage of prefix notation for a mask is that it is even simple if the number of leading ones is not a multiple of eight. For example, suppose that the mask is eighteen 1s followed by fourteen 0s, the mask in prefix notation is obviously /18. How would you write this in dotted decimal notation? Hmm. Let me get a binary to decimal calculator.

MASKING IP ADDRESSES Figure 8-5 shows what happens when a mask is applied to an IP address, 128.171.17.13. The mask is 255.255.0.0. Where the mask has one, the result is the original bits of the IP address. For the remaining bits, which are 0s, the result is 0. In this case, the result is 128.171.0.0.

NETWORK MASKS Routers use two types of masks: network masks and subnet masks. **Network masks** have 1s in the network part and 0s for remaining bits. If the network mask is 255.255.0.0 and the IP address is 128.171.17.13, then the result of masking is 128.171.0.0. This is the network part followed by 0s.

SUBNET MASKS For **subnet masks**, in contrast, the initial 1s indicate the number of bits in *both* the network and subnet parts. So, if 128.171 is the network part and 17 is the subnet part, then the subnet mask will be 255.255.255.0 (/24). If you mask 128.171.17.13 with /24, you get 128.171.17.0.

Why mark the 1s in both parts in a subnet mask? Think of a network as a state and a subnet as a city. In the United States, there are two major cities named Portland—one

in Maine and the other in Oregon. You cannot just say "Portland" to designate a city. You must give both the state and city—analogously, the network and subnet parts. Another way to look at it is that if you only had 1s in the subnet part of a subnet mask, you would break the rule that masks must have a number of leading 1s followed by a number of trailing 0s.

ROUTERS DO NOT CARE Although it is important to understand the difference between network and subnet masks in order to design masks properly, routers do not care about the distinction. To a router, a mask is simply a mask. It gets an IP address and a mask and applies the mask without asking what type of mask it is.

This lack of distinction in router operation is not an accident. Network masks were created first, and routers were designed to use them to mask IP addresses. Later, subnets were created, and the idea of masking was extended to subnet masks. However, routers do not have to know about the type of mask it is applying, so router operation remained unchanged when subnet masks were created. Again, people have to know the distinction to write masks, but routers do not.

Test Your Understanding

4. How many bits are there in a mask? b) What do the 1s in a network mask correspond to in IP addresses? c) What do the 1s in a subnet mask correspond to in IP addresses? d) When a network mask is applied to any IP address on the network, what is the result?
5. a) A mask has eight 1s, followed by 0s. Express this mask in dotted decimal notation. b) Express this mask in prefix notation. c) In prefix notation, a mask is /16. Express this mask in dotted decimal notation. d) Express the mask /18 in dotted decimal notation.
6. Do routers know the difference between network and subnet masks? Who does have to know the difference, and why do they need to know it?

HOW ROUTERS PROCESS PACKETS

Switching versus Routing

In Chapter 5, we saw that Ethernet switching is very simple. Ethernet switches must be organized in a hierarchy. This means that there is only a single possible path between any two hosts across the network. This means that when a packet arrives, there is only one possible port to use to send the frame back out. As Figure 8-6 shows, this means that each Ethernet address only appears in a single row. This row tells the switch which port to send the frame back out. This single row can be found quickly, so an Ethernet switch does little work per frame. This makes Ethernet switching fast and inexpensive.

In contrast, firms organize routers in meshes. This gives more reliability because it allows many possible alternative routes between endpoints. Figure 8-6 shows that in a routing table, each row represents an alternative route for a packet. Consequently, to **route** (forward) a packet, a router must first find all rows representing alternative routes that a particular incoming packet can take. It must then pick the best alternative route from this list. This requires quite a bit of work per packet, making routing more expensive than switching.

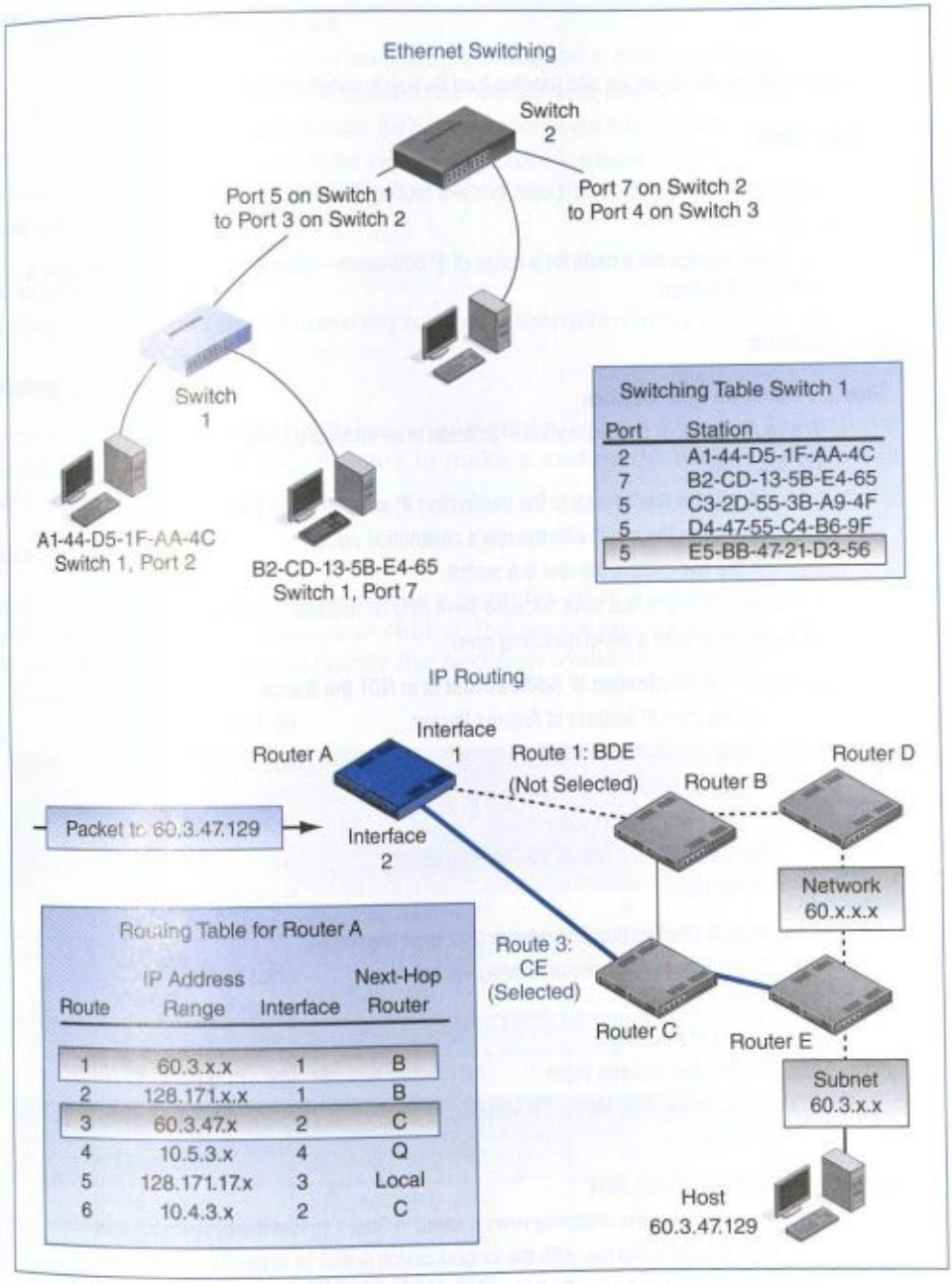


FIGURE 8-6 Ethernet Switching versus IP Routing

Routing

Processing an individual packet and passing it on its way is called routing

The Routing Table

Each router has a routing table that it uses to make routing decisions

Routing Table Rows

Each row represents a route for a range of IP addresses—often packets going to the same a network or subnet

A Routing Decision

Step 1: Finding All Row Matches

The router looks at the destination IP address in an arriving packet

For each row:

Apply the row's mask to the destination IP address in the packet

Compare the result with the row's destination value

If the two match, the row is a match

The router do this to ALL rows because there may be multiple matches

This step ends with a set of matching rows

Example 1: A Destination IP Address that is in NOT the Range

Destination IP Address of Arriving Packet	60.43.7.8
Apply the (Network) Mask	255.255.0.0
Result of Masking	60.43.0.0
Destination Column Value	128.171.0.0
Does Destination Match the Masking Result?	No
Conclusion	Not a match.

Example 2: A Destination IP Address that is in the Range

Destination IP Address of Arriving Packet	128.171.17.13
Apply the Mask	255.255.0.0
Result of Masking	128.171.0.0
Destination Column Value	128.171.0.0
Does Destination Match the Masking Result?	Yes
Conclusion	Row is a match.

Step 2: Find the Best-Match Row

The router examines the matching rows it found in Step 1 to find the best-match row

Basic Rule: It selects the row with the longest match (Initial 1s in the row mask)

Tie-Breaker Rule: If there is a tie on longest match, select among the tie rows based on metric

For cost metric, choose the row with the lowest metric value

For speed metric, choose the row with the highest metric value

FIGURE 8-7 The Routing Process (Study Figure)

Step 3: Send the Packet Back Out

Send the packet out the interface (router port) designated in the best-match row

Address the packet to the IP address in the next-hop router column

If the address says Local, the destination host is out that interface

Sends the packet to the destination IP address in a frame

FIGURE 8-7 Continued

Test Your Understanding

7. Why are routing tables more complex than Ethernet switching tables? Be articulate.

Routing Table

Figure 8-8 shows a routing table. It has a number of rows and columns. We will see how a router uses these rows and columns to make a routing decision—a decision about what to do with an arriving packet.

Rows Are Routes

In the routing table, each row represents a route for all IP addresses within a range of IP addresses—typically a network or subnet. It does not specify the full route, however, only the next step in the route (either the next-hop router to handle the packet next or the destination host).

Row	Destination Network or Subnet	Mask (/Prefix)	Metric (Cost)	Interface	Next-Hop Router
1	128.171.0.0	255.255.0.0 (/16)	47	2	G
2	172.30.33.0	255.255.255.0 (/24)	0	1	Local
3	60.168.6.0	255.255.255.0 (/24)	12	2	G
4	123.0.0.0	255.0.0.0 (/8)	33	2	G
5	172.29.8.0	255.255.255.0 (/24)	34	1	F
6	172.40.6.0	255.255.255.0 (/24)	47	3	H
7	128.171.17.0	255.255.255.0 (/24)	55	3	H
8	172.29.8.0	255.255.255.0 (/24)	20	3	H
9	172.12.6.0	255.255.255.0 (/24)	23	1	F
10	172.30.12.0	255.255.255.0 (/24)	9	2	G
11	172.30.12.0	255.255.255.0 (/24)	3	3	H
12	60.168.0.0	255.255.0.0 (/16)	16	2	G
13	0.0.0.0	0.0.0.0 (/0)	5	3	H

FIGURE 8-8 Routing Table

In the routing table, each row represents a route for all IP addresses within a range of IP addresses—typically a network or subnet.

This is important because the routing table does not need a row for *each IP address* as an Ethernet switching table does. It only needs a row for each *group of IP addresses*. This means that a router needs many fewer rows than an Ethernet switch would need for the same number of addresses.

However, there are many more IP addresses on the Internet than there are Ethernet addresses in an Ethernet network. Even with rows representing groups of IP addresses, core routers in the Internet backbone still have several hundred thousand rows. In addition, while an Ethernet switch only needs to find a single row for each arriving frame, we will see that routers need to look carefully at *all* rows.

ROW NUMBER COLUMN The first column in Figure 8-8 is a route (row) number. Routing tables actually do not have this column. We include it to allow us to refer to specific rows in our discussion. Again, each row specifies a route to a destination.

Test Your Understanding

8. In a routing table, what does a row represent? b) Do Ethernet switches have a row for each individual Ethernet address? c) Do routers have a row for each individual IP address? d) What is the advantage of the answer to the previous subpart of this question?

Step 1: Finding All Row Matches

We will now see how the router uses its routing table to make routing decisions. The first step is to find which of the rows in the routing table match the destination IP address in an arriving packet. Due to the existence of alternative routes in a router mesh, most packets will match more than one row.

ROW MATCHES How does the router know which IP addresses should be governed by a row? The answer is that it uses the *Destination Network or Subnet (destination)* column and the *Mask* column.

Suppose that all IP addresses in the University of Hawai`i (UH) network should be governed by a row. The mask would be the network mask 255.255.0.0, because the UH Network has a 16-bit network part. If this mask is applied to any UH address, the result will be 128.171.0.0. This is the value that will be in the destination column. In fact, this is Row 1 in Figure 8-8.

Let's see how routers use these two fields in Figure 8-8. Suppose that a packet arrives with the IP address 60.43.7.8. The router will look first at Row 1.

- In this row, the router applies the mask 255.255.0.0 to the arriving packet's destination IP address, 60.43.7.8. The result is 60.43.0.0.
- Next, the router compares the masking result, 60.43.0.0, to the destination value in the row, 128.171.0.0. The two are different, so the row is not a match.

However, suppose that a packet arrives with the IP address 128.171.17.13. Now, the situation is different.

- Again, router applies the mask 255.255.0.0 in Row 1 to the destination IP address, 128.171.17.13. The result is 128.171.0.0.
- Next, the router compares 128.171.0.0 to the destination value in the row, 128.171.0.0. The two are identical. Therefore, the row is a match.

MASK AND COMPARE This may seem like an odd way to see if a row matches. A human can simply look at 60.43.7.8 and see that it does not match 128.171.0.0. However, routers do not possess human pattern-matching abilities.

While routers cannot do sophisticated pattern recognition, routers (and all computers) have specialized circuitry for doing masking and comparing—the two operations that row matching requires. Thanks to this specialized circuitry, routers can blaze through hundreds of thousands of rows in a tiny fraction of a second.

THE DEFAULT ROW The last row in Figure 8-8 has the destination 0.0.0.0 and the mask 0.0.0.0. This row will match *every* IP address because masking any IP address with 0.0.0.0 will give 0.0.0.0, which is the value in the destination field of Row 13. This row ensures that at least one row will match the destination IP address of every arriving packet. It is called the **default row**. In general, a "default" is something you use if you do not have a more specific choice.

THE NEED TO LOOK AT ALL ROWS Thanks to their mesh topology, internets have many alternative routes. Consequently, a router cannot stop the first time it finds a row match for each arriving packet because there may be a better match further on. A router has to look at each and every row in the routing table to see which match. So far, we have seen what the router does in Row 1 of Figure 8-8. The router then goes on to Row 2 to see if it is a match by masking and comparing. After this, it goes on to Row 3, Row 4, Row 5, and so on, all the way to the final row (Row 13 in Figure 8-8).

Test Your Understanding

9. In Row 3 of Figure 8-8, how will a router test if the row matches the IP address 60.168.6.7? Show the calculations in the format given in the text. Is the row a match? b) Why is the last row called the default row? c) Why must a router look at all rows in a routing table? d) What rows match 172.30.17.6? e) Which rows match 60.168.7.32? Show your calculations for rows that match. f) Which rows in Figure 8-8 match 128.171.17.13? (Don't forget the default row.) Show your calculations for rows that match.

Step 2: Selecting the Best-Match Row

LIST OF MATCHING ROWS At the end of Step 1, the mask and compare process, the router has a list of matching rows. For a packet with the destination IP address 128.171.17.13, two rows in Figure 8-8 match. The first is Row 1, as we have already seen. The second is Row 7, with a destination of 128.171.17.0 and a mask of 255.255.255.0. From these, the router must select the **best-match row**, the row that represents the best route for an IP address.

BASIC RULE: LONGEST MATCH RULE How does the router decide whether to follow Row 1 or Row 7? The answer is that it follows the rule of selecting the **longest match**. Row 1 has a mask of 255.255.0.0, which means that it has a 16-bit match. Row 7, in turn, has the prefix /24, meaning that it has a 24-bit match. Row 7 has the longest match, so the router selects it.

Why the longest match rule? The answer is that the closer a route gets a packet to the destination IP address, the better. Row 1 only gets the packet to the UH network, 128.171.x.x, while Row 7 gets the packet all the way to the Shidler College of Business subnet of the University of Hawai`i, 128.171.17.x—the subnet that contains host 128.171.17.13.

TIE-BREAKER RULE: BEST METRIC VALUE The Metric Column for Match Length Ties. What if two rows have the same longest match? For instance, the destination IP address 172.29.8.112 matches both Row 5 and Row 8 in Figure 8-8. Both have a match length of 24 bits—a tie.

In case of a tie for longest match, the tie-breaker rule is to use the **metric** column which describes the "goodness" of a route. For instance, in Figure 8-8, the metric is cost. Row 5 has a cost of 34, while Row 8 has a cost of 20. *Lower cost is better than higher cost*, so the router selects Row 8.

In this case, the row with the *lowest* metric won. However, what would have happened if the metric had been *speed* instead of cost? *More speed is better*, so the router would choose Row 5, with the *higher* speed (34).

Test Your Understanding

10. a) Distinguish between Step 1 and Step 2 in the routing process. b) If any row other than the default row matches an IP address, why will the router never choose the default row? c) Which rows in Figure 8-8 match 128.171.17.13? (Don't forget the default row.) Show your calculations. d) Which of these is the best-match row? Justify your answer. e) What rows match 172.40.17.6? Show your work. f) Which of these is the best-match row? Justify your answer. g) Which rows match 172.30.12.47? Show your work. h) Which of these is the best-match row? Justify your answer. i) How would your previous answer change if the metric had been reliability?

Step 3: Sending the Packet Back Out

In Step 1, the router found all rows that matched the destination IP address of the arriving packet. In Step 2, it found the best-match row. Finally, in Step 3, the router sends the packet back out.

INTERFACE Router ports are called **interfaces**. The fifth column in Figure 8-8 is interface number. If a router selects a row as the best match, the router sends the packet out the interface designated in that row. If Row 1 is selected, the router will send the packet out Interface 2.

Router ports are called interfaces.

NEXT-HOP ROUTER In a switch, a port connects directly to another switch or to a computer. However, a router interface connects to an entire subnet or network. Therefore, it is not enough to select an interface to send the packet out. It is also necessary to specify *a particular device* on the subnet.

In most cases, the router will send the packet on to another router, called the **next-hop router**. The next-hop router column specifies the router that should receive the packet. It will then be up to that next-hop router to decide what to do next. In Figure 8-8, the next-hop router value is G.[1]

In some cases, however, the destination host will be on the subnet out a particular interface. In that case, the router should send the packet to the destination host instead of to another router. In this case, the next-hop router field will say *local*.

Test Your Understanding

11. a) Distinguish between Step 2 and Step 3 in routing. b) What are router ports called? c) If the router selects Row 13 as the best-match row, what interface will the router send the interface out? d) To what device? e) Why is this router called the default router? (The answer is not in the text.) f) If the router selects Row 2 as the best-match row for packet 172.30.33.6, what interface will the router send the interface out? g) To what device? (Don't say, "the local device.")

Cheating (Decision Caching)

We have discussed what happens when a packet arrives at a router. However, what will the router do if another packet for the same destination IP address arrives immediately afterward? The answer is that the router *should* go through the entire process again. Even if a thousand packets arrive that are going to the same destination IP address, the router should go through the entire three-step process for each of them.

As you might expect, a router might cheat, or as it is euphemistically named, cache (remember) the decision it made for a destination IP address. It will then use this decision for successive IP packets going to the same destination. Using a **decision cache** greatly reduces the work that a router will do for each successive packet.

However, caching is not prescribed in the Internet Protocol. In addition, it is dangerous. The Internet changes constantly as routers come and go and as links between routers change. Consequently, a cached decision that is used too long will result in non-optimal routing or even routes that will not work and that will effectively send packets into a black hole.

Test Your Understanding

12. a) What should a router do if it receives several packets going to the same destination IP address? b) How would decision caching speed the routing decision for packets after the first one? c) Why is decision caching dangerous?

---

[1] Actually, this column should have the IP address of Router G, rather than its name. However, we include the letter designation rather than the IP address for simplicity of understanding.

Masking When Masks Do Not Break at 8-Bit Boundaries

Masks That Break at 8-Bit Boundaries

All of the masks we have seen up to this point have had their parts broken at 8-bit segment boundaries. For example, at the University of Hawai`i, the network part is 16 bits long, which corresponds to two segments (128.171), the subnet part is 8 bits long (17), and the host part is 8 bits long. All of the masks in Figure 8-8 break also at 8-bit segment boundaries.

Masks that break at 8-bit boundaries are easy for humans to read. In general, you can look at a mask in the table and decide if it matches a particular IP address. For instance, if the mask is 255.255.0.0 (/16), and if the destination column value is 128.171.0.0, this definitely matches the IP address 128.171.45.230.

However, masks do not always break at 8-bit boundaries. For example, suppose that a mask is 11111111 11111000 00000000 00000000 (spaces added for reading). In dotted decimal notation, this is 255.248.0.0, and suppose that the destination address column value is 00000011 10001000 00000000 00000000 (3.264.0.0).

Now suppose that a destination IP address is 3.143.12.12. Does this IP address match the row? There is no way to tell just by looking at the dotted decimal notation versions of the destination, the mask, and the destination IP address. To solve the problem, you go to the raw 32-bit numbers. Figure 8-9 shows that the masked destination IP address matches the destination value in the row, so the row is a match.

IP address: (3.143.12.12)	00000011	10001111	00001100	00001100
Mask: (255.136.0.0)	11111111	11111000	00000000	00000000
Result: (3.136.0.0)	00000011	10001000	00000000	00000000
Destination: (3.264.0.0)	00000011	10001000	00000000	00000000
Match?	Yes	Yes	Yes	Yes

FIGURE 8-9 Using a Mask Whose 1s Do Not Break at an 8-Bit Boundary

Test Your Understanding

13. a) An arriving packet has the destination IP address 128.171.180.13. Row 86 has the destination value 128.171.160.0. The mask is 255.255.224.0. Does this row match the destination IP address? Show your work. You can use the Windows Calculator if you have a Windows PC. In Windows Vista and earlier versions of Windows, choose scientific when you open the calculator. In the Windows 7 calculator, choose programmer mode.

The Address Resolution Protocol

The final step in the routing process for each arriving packet is to send the packet back out another interface, to a next-hop router or the destination host. This seems easy enough, but there is one additional thing that routers must do.

To send a packet to a next-hop router or a destination host, the router's interface must place the packet into a frame and send this frame to the next-hop router or destination host.

To do this, the interface must know the data link layer address of the destination host. Otherwise, the router's interface will not know what to place in the destination address field of the frame.

The router's internet layer process may only know the IP address of the destination host. If the router's interface is to deliver the frame containing the packet, the internet layer process must discover the data link layer address of the destination host. This is called address resolution.

Address Resolution on an Ethernet LAN with ARP

Determining a data link layer address when you know only an IP address is called **address resolution**. Figure 8-10 shows the **Address Resolution Protocol (ARP)**, which provides address resolution on Ethernet LANs. There are other address resolution protocols for other subnet technologies.

ARP Request Message

Suppose that the router receives an IP packet with destination address 10.19.8.17. Suppose also that the router determines from its routing table that it can deliver the packet to a host on one of its Ethernet subnets.

- First, the router's internet layer process creates an ARP request message that essentially says, "Hey, device with IP address 10.19.8.17, what is your 48-bit MAC layer address?" The router then broadcasts this ARP packet to all hosts on the subnet.[2]

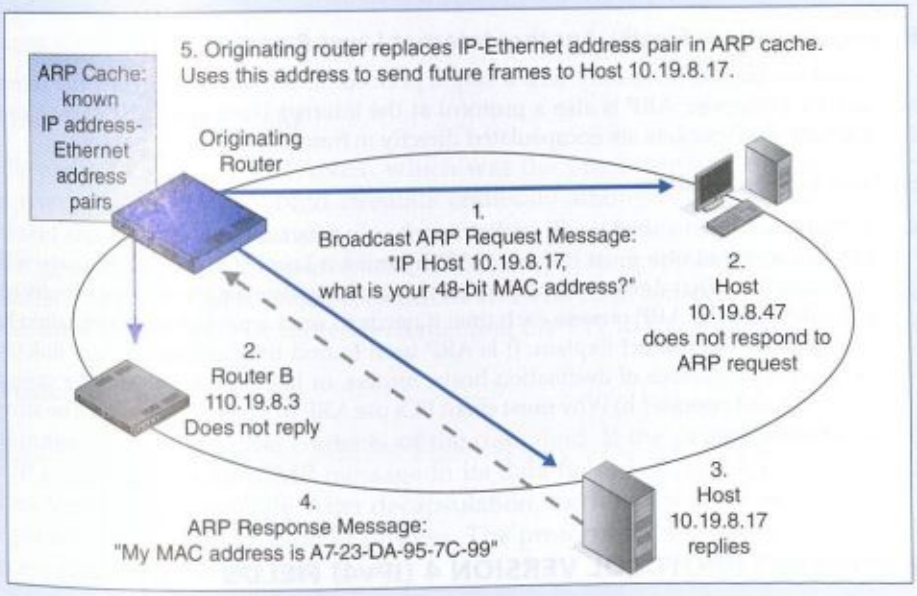


FIGURE 8-10 Address Resolution Protocol (ARP)

(continued)

[2] Actually, the router passes the packet down to the data link layer process on the subnet's interface. It tells the data link layer process to broadcast its ARP packet. If the subnet standard is Ethernet, the data link layer process places the packet into a frame with the destination Ethernet address FF-FF-FF-FF-FF-FF (forty-eight 1s). This is the Ethernet broadcast address. Switches will send frames with this broadcast address to all stations, and all stations will accept it as they would a frame addressed to their specific Ethernet address.

- Second, the internet layer process on every host examines the ARP request message. If the target IP address is not that of the host, the host's internet layer process ignores the ARP request message. However, host 10.19.8.17 composes an ARP response message that includes its 48-bit MAC layer address (A7-23-DA-95-7C-99). The target host sends this ARP response message back to the router.
- Third, the router's internet layer process now knows the subnet MAC address associated with the IP address. It will deliver the packet to that host in a frame addressed to A7-...

The ARP Cache

ARP is a time-consuming process, and the router does not want to do it for each arriving packet. Consequently, the internet layer process on the router saves the IP address–data link layer address information in its **ARP cache** (section of memory). Afterward, whenever an IP packet comes for this IP destination address, the router will send the IP packet down to its NIC, together with the required MAC address. The NIC's MAC process will deliver the IP packet within a frame containing that MAC destination address.

Using ARP for Next-Hop Routers

We have looked at how routers use ARP when they deliver packets to destination hosts. A router also needs to know the data link layer destination addresses of next-hop routers. Routers use ARP to find the data link layer destination addresses of both destination hosts and other routers.

ARP Encapsulation: Finally, Another Internet Layer Protocol!

In this book so far, we have only seen a single protocol at the internet layer—the Internet Protocol (IP). However, ARP is also a protocol at the internet layer, and ARP messages are called packets. ARP packets are encapsulated directly in frames, just like IP packets.

Test Your Understanding

14. A router wishes to send an IP packet to a host on its subnet. It knows the host's IP address. a) What else must it know? b) Why must it know it? c) What message will it broadcast? d) What device will respond to this broadcast message? e) Does a router have to go through the ARP process each time it needs to send a packet to a destination host or to a next-hop router? Explain. f) Is ARP used to find the destination data link layer destination addresses of destination hosts, routers, or both? g) At what layer does the ARP protocol operate? h) Why must client PCs use ARP to transmit packets? The answer is not in the text.

THE INTERNET PROTOCOL VERSION 4 (IPv4) FIELDS

We have focused on IP routing. However, the Internet Protocol has other properties that networking professionals need to understand.

As noted in Chapter 1, most routers today on the Internet and private internets are governed by the **IP version 4 (IPv4)** standard. (There were no versions 0 through 3.) Figure 8-11 shows the IPv4 packet. Its first four bits contain the value 0100 (binary for 4) to indicate that the packet is formatted according to IPv4. Although we have looked already at some of the fields in IPv4, here we will look at fields that we have not yet seen.

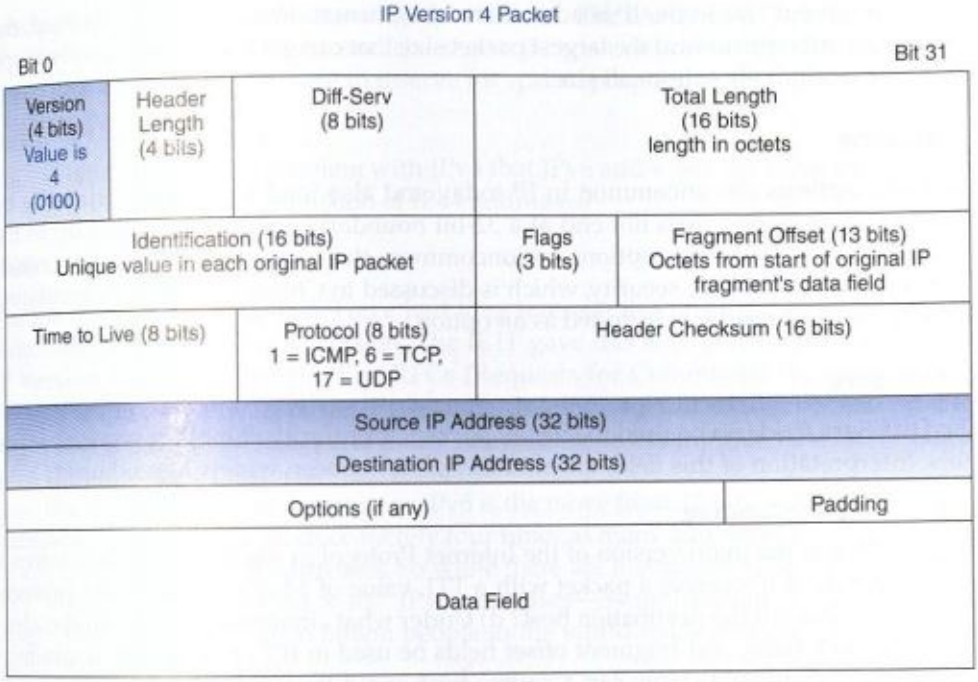


FIGURE 8-11 IP Version 4 (IPv4) Packet

IP Time to Live (TTL) Field

In the early days of the ARPANET, which was the precursor to the Internet, packets that were misaddressed would circulate endlessly among packet switches in search of their nonexistent destinations. To prevent this, IP added a **time to live (TTL)** field that is given a value by the source host. Different operating systems have different TTL defaults. Most insert TTL values between 64 and 128. Each router along the way decrements the TTL field by 1. A router decrementing the TTL to 0 will discard the packet.

IP Protocol Field

The **protocol field** tells the contents of the data field. If the protocol field value is 1, the IP packet carries an ICMP message in its data field. TCP and UDP have protocol values 6 and 17, respectively. After decapsulation, the internet layer process must pass the packet's data field to another process. The protocol field value designates which process should receive the data field.

IP Identification, Flags, and Fragment Offset Fields

If a router wishes to forward a packet to a particular network and the network's maximum packet size is too small for the packet, the router can fragment the packet into two or more smaller packets. Fragmentation can even happen at multiple routers along the way. The destination host's internet layer process must put the fragments back together.

In practice, fragmentation is rare. In fact, it often indicates an attempt to get around security protections. In any case, most modern operating systems set the

"do not fragment" bit in the IP header so that fragmentation cannot occur. Instead, the source host attempts to find the largest packet size that can get through or simply keeps packets to a relatively safe small size.

IP Options

Similarly, **options** are uncommon in IP today and also tend to be used primarily by attackers. If an option does not end at a 32-bit boundary, **padding** is added up to the 32-bit boundary. Although options are uncommon, they cannot be completely avoided. For example, in IPsec security, which is discussed in Chapter 10, the Encapsulating Security Payload header is included as an option.

IP Diff-Serv

The **Diff-Serv** field can be used to label IP packets for priority and other service parameters. Interpretation of this field, unfortunately, has not been widely agreed upon.

Test Your Understanding

15. a) What is the main version of the Internet Protocol in use today? b) What does a router do if it receives a packet with a TTL value of 1? c) What does the protocol field value tell the destination host? d) Under what circumstances would the identification, flags, and fragment offset fields be used in IP? e) Why is IP fragmentation suspicious? f) How can a source host avoid fragmentation? g) Why are IP options suspicious? h) What security standard uses IPv4 options? i) What is the purpose of the Diff-Serv field?

IP VERSION 6 (IPv6)

Outgrowing IPv4

Although IPv4 continues to dominate the Internet's traffic, it has passed its prime. Most seriously, the 32-bit IPv4 address space has proven to be too small. In theory, the 32-bit IPv4 address space permits over four billion IP addresses. Unfortunately, these addresses were given out inefficiently. First, the United States, which originated the architecture, assigned about a third of all IPv4 addresses to itself. Second, and more seriously, IP addresses were only given out in chunks of approximately 256 addresses, 65,536, or 16.8 million addresses.[3] If a firm needed 300 IP addresses, it was bumped up to the next step, 65,536 addresses. In such firms, nearly all of the IP addresses went unused. Although the Internet Assigned Number Authority (IANA) fairly quickly switched to the classless inter-domain routing (CIDR) system, which gave number assignments in smaller increments, assignments were almost always generous to allow room for growth. Overall, only about 14 percent of all IPv4 numbers are actively used.

This limited supply of IPv4 addresses, the rapid Internet growth of economies in Asia, and the explosive growth of mobile devices needing their own IP addresses were

[3] A handful of the addresses within each of these three block sizes could not be used for reasons we will see in Chapter 9.

a recipe for disaster. In 2011, the disaster occurred. The IANA gave out the last of its IP addresses to regional registrars. The registrars soon ran out of this last allocation, apart from a few addresses kept in reserve for special purposes.

Test Your Understanding

16. a) What is the main problem with IPv4 that IPv6 addresses? b) What factors combined to cause the exhaustion of IPv4 addresses?

IPv6

The Internet Engineering Task Force had long foreseen this crisis. In its 1994 meeting, it decided to create a new IP version. The IETF gave this new version the designation **IP Version 6 (IPv6)** when the first RFCs (Requests for Comments) were released in 1995. Over the next few years, the IPv6 standards family continued to grow and mature. It was soon ready to be used, and many networking and computer vendors began to build IPv6 into their products.

The most fundamental change in IPv6 is the move from 32-bit addresses to 128-bit addresses. This does not produce merely four times as many addresses. Each additional bit *doubles* the number of addresses. So while there are just under 4.3 billion (4.3×10^9) IPv4 addresses, there are 3.4×10^{38} IPv6 addresses—34 undecillion. To see what this means, there are about seven billion people in the world today. For each person, there are 5×10^{28} IPv6 addresses.

Organizations soon found that using these new equipment capabilities, however, was a great deal more work than simply turning them on. For many years, few organizations saw the need to make the expensive upgrade to IPv6 because they had enough addresses. In addition, Network Address Translation (NAT) greatly extended the use of existing IP addresses in the firm, at the cost of some complexity, but at the gain of some security. IPv6 would have the mandatory inclusion of IPsec security functionality, but IPsec was quickly modified to work with IPv4 as well. Seeing no hard business case for upgrading, few companies did. Now, however, nearly all companies are beginning to at least plan for the implementation of IPv6, and many have already done so. As we will see in Chapter 9, companies have found that IPv6 implementation is a long and complex process. They need employees who understand this new protocol and other "v6" protocols such as ICMPv6 and DHCPv6.

In this chapter, we have focused on IPv4. We will look at IPv6 and its implementation in Chapters 8 and 9.

Test Your Understanding

17. a) What is the designation of the newest version of the Internet Protocol? b) What is its biggest improvement over IPv4? c) Is the conversion from IPv4 to IPv6 relatively inexpensive?

Writing 128-Bit IPv6 Addresses

For IPv4, strings of 32 ones and zeros are difficult for people to write and remember. Therefore, for human use, we write IPv4 addresses in dotted decimal notation—four decimal numbers between 0 and 255 separated by dots. This gives addresses like 128.171.17.13. People can actually remember these addresses.

For the 128-bit addresses of IPv6, we would still like simpler ways to write them, but anything we do will still overload human memory. Consequently, when we write IPv6 addresses for human consumption, we do so only to make the writing easier.

A 128-bit IPv6 address is shown in the following example. This is obviously difficult to write without making a mistake, and it is impossible to read.

1011010001010111101101000101011110110100010101101011010001010111101101000
1010111101101000101011110110100010111111011010001010111

To simplify this number, IPv6 does not use dotted decimal notation as IPv4 does. Rather, IPv6 uses hexadecimal notation, which we saw in Chapter 5, in the context of Ethernet MAC addresses. Each "nibble" of four bits is converted into a hex symbol from 0 through F. A 128-bit IPv6 address, then, would be translated into 32 hex symbols.

In Ethernet, we write hex symbols in pairs, separating each pair with a dash. This gives addresses like A1-B2-C3-D4-E5-F6. In IPv6, in contrast, we group hex symbols in tetrads (groups of four). Each tetrad is called a **field**. An example of a field is *fe56*. Note that we write the hex symbols in *lowercase* when writing IPv6 addresses. Each symbol is still four bits, so fe56 represents 16 bits. A full IPv6 address will have eight groups of these tetrads, which are separated by *colons* instead of dashes. The following is an IPv6 address written in hexadecimal notation.

2001:0027:fe56:0000:0000:0000:cd3f:0fca

This is still very long. Fortunately, there several rules to help us shorten the writing of addresses a little. The first is that in each field, *any leading zeros are dropped*. This is easy to understand. If the reader sees :27:, this must be :0027:. Note that only *leading* zeros are dropped. If trailing zeros or zeros anywhere were dropped, the reader could not know if :27: was :0027:, :2700:, or 0270:. Dropping leading zeros is also natural because we do that when writing decimal numbers. Here is what the IPv6 address looks like after leading zeros are dropped. This is much shorter.

2001:27:fe56::::cd3f:fca

Note that if a field has four zeros, it will become :: by the first rule. In other words, all four "leading" zeros are dropped, and only the colons remain. A second rule is that if several consecutive fields of zero occur, *one* sequence of *all-zero fields* can be reduced to a simple ::. So if an IPv6 address has a sequence :0000:0000:0000:, this can be replaced by ::. This further simplifies our IPv6 address to the following:

2001:27:fe56::cd3f:fca

These two rules reduce length, but applying them has some subrules that appliers must follow.

- First, address simplification should be done whenever possible. If the two rules can be combined, they should be combined.
- Second, only a *single* group of consecutive zeros may be shortened this way in an IP address. If only one group of zero segments is shortened, then counting the number of fields in a shortened address will tell the reader how many zeros need to be added back in. In the example above, there are five fields, not counting the ::. Therefore, three fields of zeros must be added to bring the total to eight fields.
- Third, the *longest* group of consecutive zero fields should be shortened. This just makes sense. One might as well shorten things as much as possible.
- Fourth, if there are two groups of consecutive zeros of the same length, the *first* group must be shortened. This is not an important rule, but reducing ambiguity is a good thing.

All of these rules can be a little daunting, but it is important to know how to write IPv6 addresses properly. Following these rules means that everyone will write IP addresses the same way. If some people drop some initial zeros while others do not, and if some writers violate the three rules while others do not, the same IP address will be written in different ways by different people. This will make it more difficult to determine if two written addresses are the same or different. It will also make automatic searching in databases and configuration fields far more difficult and error prone.

Test Your Understanding

18. a) Are IPv6 addresses written in uppercase or lowercase letters? b) Are IPv6 addresses written in decimal or hexadecimal symbols? c) How many symbols are there in a field, and how are fields delimited?
19. a) List the rules for simplifying IPv6 addresses. b) Simplify the following IP address: 2001:0ed2:056b:00d3.000c:abcd:0bcd:0fe. c) Simplify the following IP address: 2001:0002:0000:0000:0000:abcd:0bcd:0fe. d) Simplify the following IP address: 2001:0000:0000:00fe:0000:0000:0000:cdef. e) What is the advantage of simplifying IPv6 addresses according to strict rules?

The IPv6 Header

The increase from 32 bits to 128 bits is the most important improvement from IPv4 to IPv6, so we have focused heavily on IPv6 addresses. We will now turn to improvements in the IPv6 header compared to the IPv4 header. Figure 8-12 illustrates both. The most obvious difference is that IPv4 headers are 20 octets long while IPv6 headers are 40 octets long.

The second difference is that the IPv6 header, although longer, is less cluttered, with fewer fields for routers and hosts to consider. This relative simplicity means that routers can actually process longer IPv6 headers faster than they can process IPv4 headers.

VERSION NUMBER FIELD Both headers begin with a 4-bit **version number** field. For IPv4, the field value is 0100 (four). For IPv6, it is 0110 (six).

TRAFFIC CLASS AND FLOW LABEL FIELDS In the first row of the IPv6 header, there are an 8-bit type of service field and a 20-bit flow label.[4] The **traffic class field** in IPv6 allows

[4] In the original definition of IPv6, these fields were 4 bits and 24 bits, respectively. The change to 8 bits and 20 bits was made in 1998.

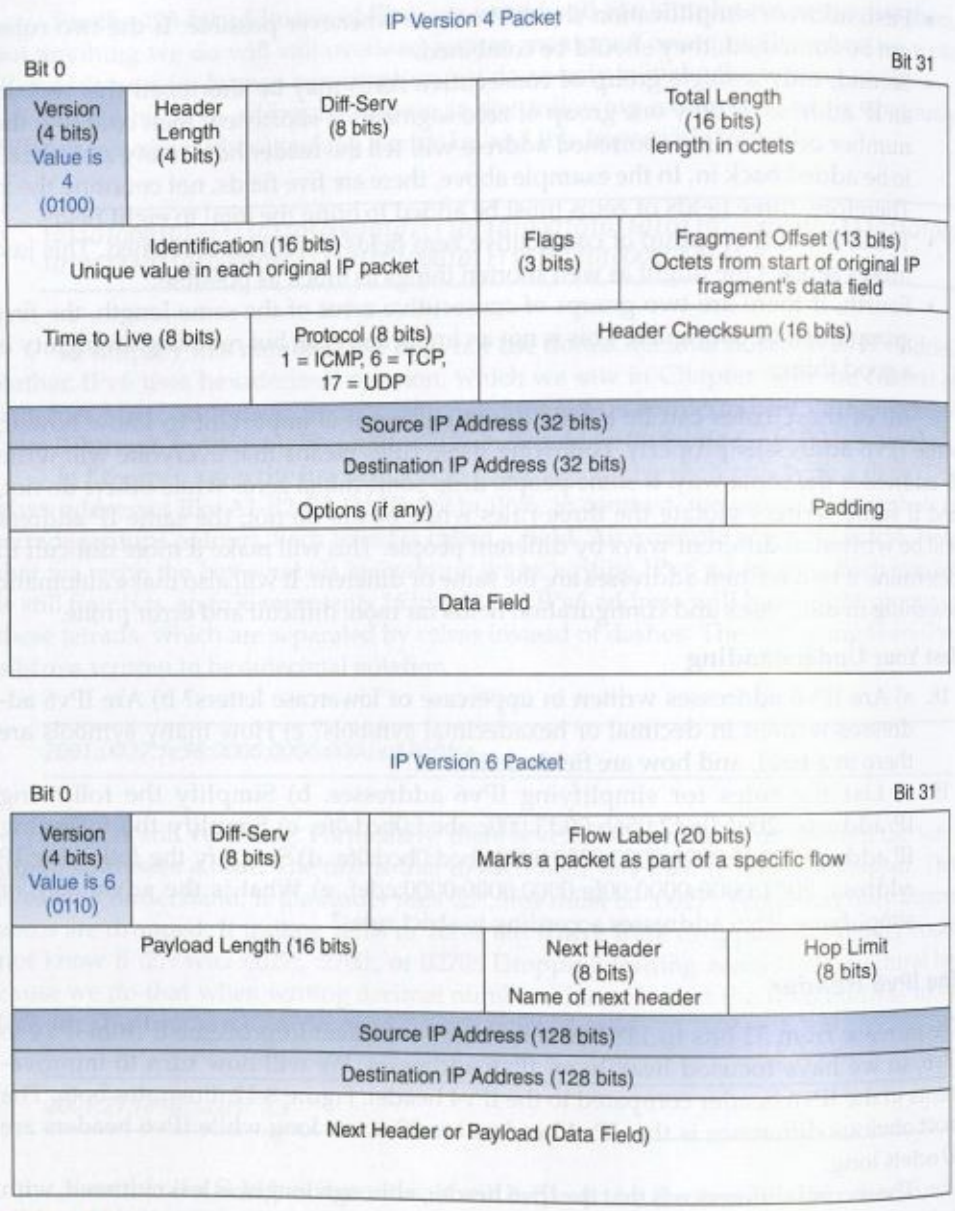


FIGURE 8-12 IPv4 and IPv6 Packet Header

up to 256 special handling conditions to be specified. It is almost completely equivalent to the 8-bit type of service field in IPv4.

The **flow label field** allows a stream of packets to be identified as part of a single stream. After the first packet is processed by a router, the router can apply certain processing rules to following packets in the stream, including those in the traffic class field. This further reduces processing time per packet.

Unfortunately, the definitions of these fields are still embryonic, and they are seeing little use currently.

LENGTHS For IPv4, two fields are used to compute the length of the data field in the IP packet. The header length field gives the length of the header in 32-bit units, while the total length field gives the total length of the packet in octets.

In IPv6, the main packet header is always 40 octets long, so the **payload length field** only needs to give the length of the payload in octets. A router can quickly determine how long the packet is.

The payload length field is 16 bits long, so payloads can be up to 65,536 octets long. IPv6 also has an option for far larger **jumbo headers**. Greater packet length means that routers can handle fewer packets to deliver an application message. This also speeds up router operation.

However, the sending host must limit its packet length so that all of the links between routers along the way can support that packet length. The maximum packet size that can be transmitted without segmentation across a packet's route is called the **maximum transmission unit (MTU)** length. For IPv4, a method for finding the MTU is described in RFC 1191, which was published in 1990. For IPv6, a similar method was published in RFC 1981 (1996). A more robust method for IPv6 MTU discovery was published in RFC 4821 (2007). Without MTU discovery, the maximum packet size must be set to 1,280 octets. All data links are required to support packets of this size.

It should be noted that payload length is not the same as the length of the data field. We will see that an IPv6 packet can have one or more extension headers before the data field. These are included in the payload length.

FRAGMENTATION In IPv4, routers along a packet's path may be required to fragment a packet so that it can travel through a network with a small MTU. The second row in the IPv4 header allows the destination host to reassemble the fragmented packet. As discussed earlier in the chapter, router fragmentation has become a largely obsolete capability.

IPv6 does not permit routers along the route to fragment packets at all. Therefore, it does not need to have the reassembly information in the IPv4 header. This shortens the IPv6 header by 32 bits.

However, IPv6 does allow a host to fragment a packet *before sending it*. We will see later that there is an extension header to govern packet reassembly on the destination host. This extension header is only added when fragmentation occurs, and routers along the way do not have to consider it.

HOP LIMIT FIELD IPv4 has a time to live field. As we noted earlier in this chapter, each router along the way decrements this field's value by one. If a router decrements it to zero, the router discards the packet. Internet old timers know that when IPv4 was created, the time to live value was supposed to be an actual clock time. However, this was quickly discovered to be unworkable in practice. The value was then interpreted as the maximum number of hops permitted by the packet.

In IPv6, the corresponding field was the same length as it was in the IPv4 packet header. However, it was renamed the **hop limit field** to more properly identify it. For people not old enough to remember the early definition of time to live, however, it is simply a matter of confusion.

CHECKSUM FIELD. WHAT CHECKSUM FIELD? IPv4 has a checksum field. When IPv4 was created, there was a concern that if packet headers contained errors, they could cause serious problems for the Internet. Experience showed that this concern was overblown. Consequently, IPv6 has no checksum field. The computations needed to check for errors in IPv4 were heavy, even for a 20-octet header. Dropping the checksum field significantly reduces packet handling time on routers.

SOURCE AND DESTINATION IPV6 ADDRESSES Although the IPv6 header has fewer fields than the IPv4 header, the IPv6 source and destination addresses are four times as long as they are in IPv4. Consequently, the IPv6 header is 40 octets long, as opposed to IPv4 header's 20 octets length—assuming no options in the IPv4 header.

Test Your Understanding

20. a) How do the version number fields in IPv4 and IPv6 differ? b) In IPv6, how can the receiver tell the length of packet? c) Does the payload length field include the lengths of any extension headers in the packet? d) What is the maximum possible lengths for ordinary IPv6 payloads? e) What are jumbo packets, and why are they desirable? f) What is the maximum MTU size? g) How is it determined in IPv6? h) If a source host does not do MTU discovery, what is the longest packet it can safely send?
21. a) Compare fragmentation in IPv4 and IPv6. b) How is the hop limit field used? c) Does IPv6 have a header checksum field? d) What are the implications of this? e) What is the general purpose of the traffic class field? f) Of the flow label field?

Extension Headers

The IPv4 packet has an *options* field that allows the sender to add options. Few IPv4 packets have options, but each router must check each packet for options, and this can cost significant time. IPv6 took another approach. In the IPv6 header, there is no options field. Instead, there is a **next-header field**. Instead of having an open-ended options field, the IETF has organized optional information into a series of optional **extension headers**. These extension headers only have to be processed if they are present.

Each extension header has its own next-header field identifying the following extension header. As Figure 8-13 shows, this allows the main header and one or more extension headers to be daisy-chained together.

Figure 8-14 shows that next header values have been defined for particular extension headers. In addition, values have been designed for types of final data fields (upper layer messages) if there are no more extension headers. If these upper layer message values seem familiar, it is because these are the values that are used in the protocol field of the IPv4 header. In essence, the next-header field is an extension of the protocol field in IPv4.

Two of the six currently defined extension headers are the **authentication header** and the **encapsulating security payload (ESP) field**. Both are designed for security. The authentication header allows the packet to validate the sender, but there is no encryption for confidentiality. This has proven to be of little value.

The ESP option, in contrast, gives all of the traditional protections of cryptographic systems, including encryption for confidentiality, authentication, message integrity, and replay protection.

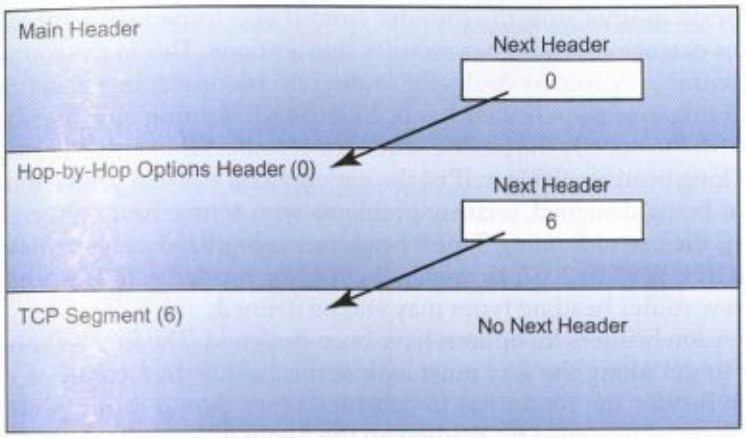


FIGURE 8-13 Next Headers in IPv6 Packet Headers

Header Type	Next Header Code
Extension Headers	
Hop-by-Hop Options	0
Routing Header	43
Fragment Header	44
Authentication Header	51
Encapsulating Security Payload Header	50
Destination Options	60
Mobility Header	135
No Next Header	59
Upper Layer Messages	
TCP	6
UDP	17
ICMPv6	58

FIGURE 8-14 IPv6 Next Header Values

Initially, security was a defining characteristic of IPv6, distinguishing it from IPv4. However, the IETF quickly made the encapsulating security payload (and authentication header) available in IPv4 by allowing their values (50 and 51) to appear in the IPv4 protocol field. In addition, while it is often said that the use of security is

mandatory in IPv6, the truth is that providing the *capability* for ESP and authentication header security is mandatory. Their *use* is not mandatory. Consequently, making security an option in IPv4 stole the thunder from IPv6's touted security advantage.

One other extension header has security implications. This is the routing header. This should control how routers deal with routing decisions for the packet. So far, only one type of routing extension header has been released, Routing Heading Type 0. This permits the header to specify the precise sequence of routers that should process it. This capability has long been available in IPv4 through options as loose source routing. Even when IPv6 was being designed, security problems with source routing were being discovered. Today, the use of Routing Type 0 headers is recognized as being risky and was deprecated by RFC 5095 in 2007. However, the routing header as a whole has not been deprecated. New router heading types may still be defined.

Two extension headers for options have been designed. The first is for hop-by-hop options. Each router along the way must look at this header. In fact, this is usually the only extension header the router has to consider, other than a routing header. Other extension headers are designed for reading by the destination host.

The second is for destination host options. These can be safely ignored by routers. In both cases, having specific extension headers for hop by hop and destination host addresses allows options to be handled elegantly if they exist. If there are no hop-by-hop options, hosts do not have to waste any time looking for options.

Test Your Understanding

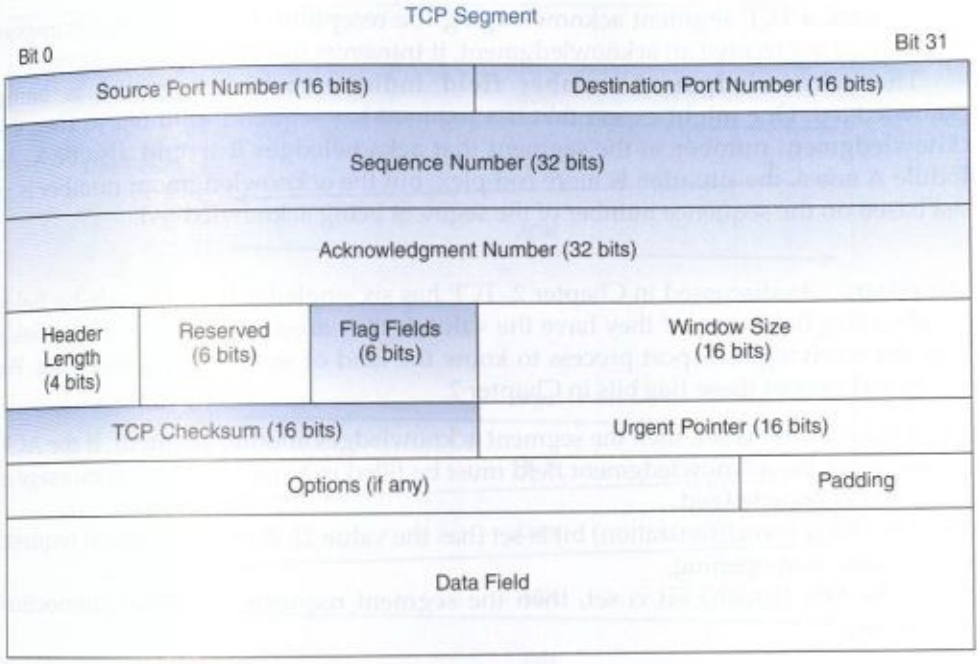
22. a) Why is handling options the way that IPv4 does undesirable? b) Why is the approach of using optional extension headers desirable? c) Distinguish between protections provided by the authentication header and the encapsulating security payload. d) Are these two security extension headers available in IPv6, IPv4, or both? e) What does it mean that the Routing Header Type 0 has been deprecated? f) What is usually the only extension header that routers normally have to consider? g) What is another they might have to consider? h) How does the last extension header before a UDP datagram indicate that the UDP datagram comes next? (You must infer the answer from the text.) i) If you see 51 in the next header field of a header, what will follow this header? j) If you see 59 in the next header field of a header, what will follow this header?

THE TRANSMISSION CONTROL PROTOCOL (TCP)

Fields in TCP/IP Segments

In Chapter 2, we looked briefly at the syntax of messages (segments) for the **Transmission Control Protocol (TCP)**. In this section, we will look at the syntax of this complex protocol in more depth. When IP was designed, it was made a very simple "best effort" protocol (although its routing tables are complex). The IETF left more complex internetwork transmission control tasks to TCP. Consequently, network professionals need to understand TCP very well. Figure 8-15 shows the organization of TCP messages, which are called TCP segments.

SEQUENCE NUMBERS TCP can handle messages of almost any length. In Chapter 2, we saw that it does so by fragmenting application messages into many TCP segments and sending each segment in a packet. So that the receiver can put the segments back



Flag fields are 1-bit fields. They include SYN, ACK, FIN, and RST.

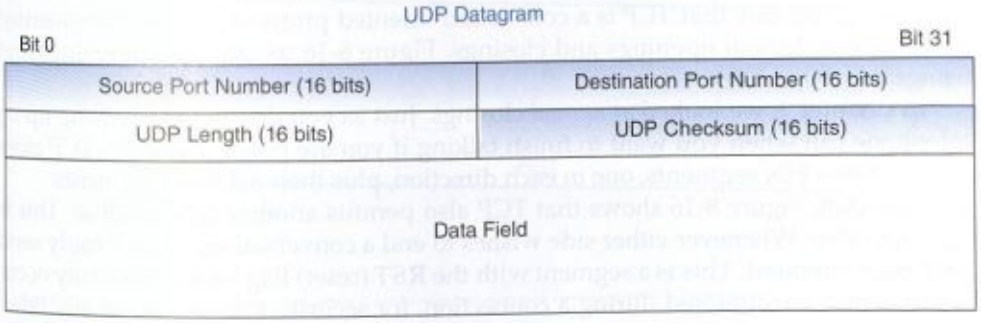


FIGURE 8-15 TCP Segment and UDP Datagram

in order, each segment has a **sequence number** that gives its position in the stream of segments. The receiving TCP process puts the segments in order of increasing sequence number, creating the full application message. The TCP process then passes the application message up to the correct application process indicated in the port number.[5]

ACKNOWLEDGMENT NUMBERS In Chapter 2, we saw that TCP uses **acknowledgments (ACKs)** to achieve reliability. If a transport process receives a TCP segment correctly,

[5] Module A has a detailed discussion of TCP sequence and acknowledgment numbers.

it sends back a TCP segment acknowledging the reception. If the sending transport process does not receive an acknowledgment, it transmits the TCP segment again.

The **acknowledgment number field** indicates which segment is being acknowledged. One might expect that if a segment has sequence number X, then the acknowledgment number in the segment that acknowledges it would also be X. As Module A notes, the situation is more complex, but the acknowledgment number is at least based on the sequence number of the segment being acknowledged.

FLAG FIELDS As discussed in Chapter 2, TCP has six single-bit fields. Single-bit fields are called flag fields, and if they have the value 1, they are said to be set. These fields allow the receiving transport process to know the kind of segment it is receiving. We saw several uses of these flag bits in Chapter 2.

- If the ACK bit is set, then the segment acknowledges another segment. If the ACK bit is set, the acknowledgment field must be filled in to indicate which message is being acknowledged.
- If the SYN (synchronization) bit is set (has the value 1), then the segment requests a connection opening.
- If the FIN (finish) bit is set, then the segment requests a normal connection closing.

Openings and Abrupt TCP Closes

In Chapter 2, we saw that TCP is a connection-oriented protocol. Connection-oriented protocols have formal openings and closings. Figure 8-16 recaps these openings and closings.

In Chapter 2, we looked at *normal* closings. Just as you do not simply hang up on a telephone call when you want to finish talking if you are polite, a normal TCP close consists of two FIN segments, one in each direction, plus their acknowledgments.

However, Figure 8-16 shows that TCP also permits another type of close. This is an abrupt close. Whenever either side wishes to end a conversation, it can simply send a **TCP reset segment**. This is a segment with the **RST** (reset) flag bit set. This may occur if a problem is encountered during a connection, for security reasons, or for any other reason.

Note in Figure 8-16 that an RST segment is not acknowledged. The side that sent the RST segment is not listening any longer, so acknowledging a reset would be as pointless as saying goodbye after someone has hung up on you. The RST segment is one of two segment types that are not acknowledged. As noted in Chapter 2, a pure acknowledgment is not acknowledged because doing so would create an endless loop of acknowledgments.

Test Your Understanding

23. Why is TCP complex? b) Why is it important for networking professionals to understand TCP? c) What are TCP messages called?
24. Why are sequence numbers good? b) What are 1-bit fields called? c) If someone says that a flag field is set, what does this mean? d) If the ACK bit is set, what other field must have a value? e) What is a FIN segment? f) Distinguish between four-way closes and abrupt resets. g) Why is a reset segment not acknowledged?

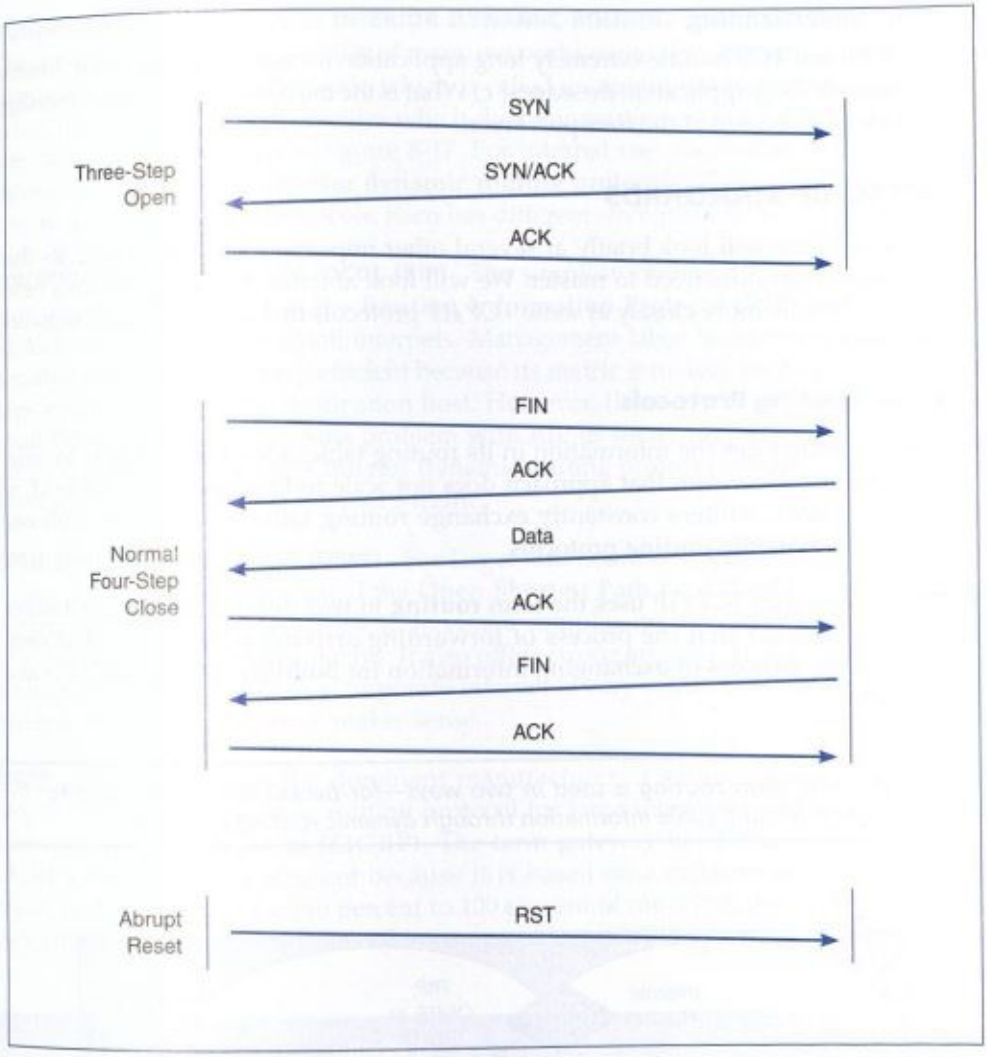


FIGURE 8-16 TCP Session Openings and Closings

THE USER DATAGRAM PROTOCOL (UDP)

We saw UDP in Chapter 2. This is a very simple protocol, so the discussion in that chapter is sufficient except for one point. In the section on TCP, we noted that segmentation and reassembly allows very long application messages—messages far too long to fit into a single packet.

In contrast, UDP cannot do segmentation. It has nothing like sequence numbers or acknowledgment numbers. This means that an application message must fit into a single UDP datagram. The length field in the UDP header is 16 bits long, so the maximum length of the UDP data field, and therefore the maximum length of an application message, is 65,536 octets.

Test Your Understanding

25. a) Why can TCP handle extremely long application messages? b) Can UDP handle extremely long application messages? c) What is the maximum application message size if UDP is used at the transport layer.

OTHER TCP/IP STANDARDS

In this section, we will look briefly at several other important TCP/IP standards that network administrators need to master. We will look at some of these protocols here. Chapter 9 will look more closely at some TCP/IP protocols that are focused on network management.

Dynamic Routing Protocols

How does a router get the information in its routing table? One possibility is to enter routes manually. However, that approach does not scale to large internets. Instead, as Figure 8-17 shows, routers constantly exchange routing table information with one another using **dynamic routing protocols**.

ROUTING Note that TCP/IP uses the term **routing** in two different but related ways. First, we saw earlier that the process of forwarding arriving packets is called routing. Second, the process of exchanging information for building routing tables is also called routing.

*In TCP/IP, the term **routing** is used in two ways—for packet forwarding and for the exchange of routing table information through dynamic routing protocols.*

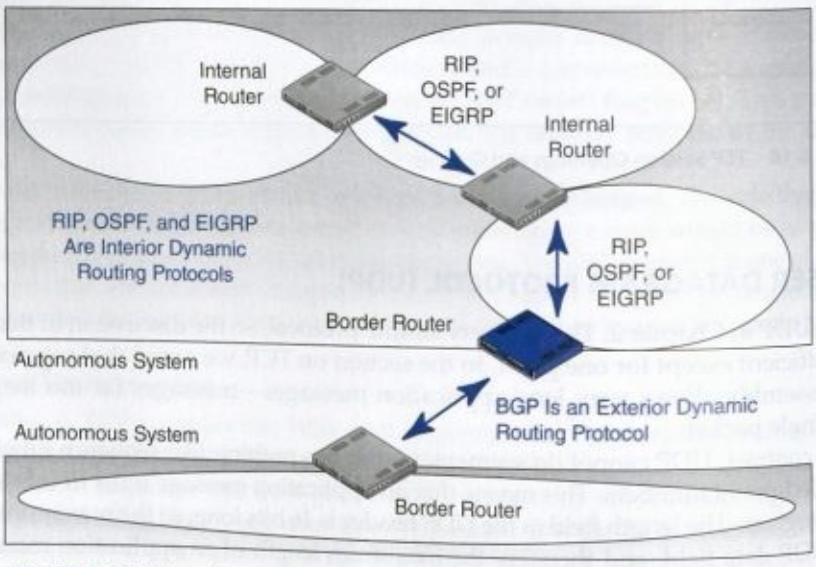


FIGURE 8-17 Internal and External Dynamic Routing Protocols

AUTONOMOUS SYSTEMS AND INTERIOR DYNAMIC ROUTING PROTOCOLS Recall from Chapter 1 that the Internet consists of many networks owned by different organizations. Within an organization's network, which is called an **autonomous system**, the organization owning the network decides which dynamic routing protocol to use among its internal routers, as shown in Figure 8-17. For internal use, the organization is free to choose among available **interior dynamic routing protocols**. There are three popular interior dynamic routing protocols. Each has different strengths and weaknesses.

ROUTING INFORMATION PROTOCOL (RIP) The simplest interior dynamic routing protocol created by the IETF is the **Routing Information Protocol (RIP)**. RIP's simplicity makes it attractive for small internets. Management labor is relatively low. On the negative side, RIP is not very efficient because its metric is merely the number of router hops needed to get to the destination host. However, this is not a serious problem for small internets. The one serious problem with RIP in small internets is poor security. If attackers take over a firm's interior dynamic routing protocol communications, they can maliciously reroute the internet's traffic.

OPEN SHORTEST PATH FIRST (OSPF) For larger autonomous systems, or if security is a serious concern, the IETF created the **Open Shortest Path First (OSPF)** dynamic routing protocol. OSPF is very efficient, having a complex metric based on a mixture of cost, throughput, and traffic delays. It also offers strong security. It costs much more to manage than RIP, but unless a corporate internet is very small, OSPF is the only IETF dynamic routing protocol that makes sense.

EIGRP Cisco Systems is the dominant manufacturer of routers. Cisco has its own proprietary interior dynamic routing protocol for large internets—**Enhanced Interior Gateway Routing Protocol (EIGRP)**. The term **gateway** is another term for *router*. EIGRP's metric is very efficient because it is based on a mixture of interface bandwidth, load on the interface (0 percent to 100 percent of capacity), delay, and reliability (percentage of packets lost). EIGRP is comparable to OSPF, but many companies use

Dynamic Routing Protocol	Interior or Exterior Routing Protocol?	Remarks
RIP (Routing Information Protocol)	Interior	Only for small autonomous systems with low needs for security
OSPF (Open Shortest Path First)	Interior	For large autonomous systems that only use TCP/IP
EIGRP (Enhanced Interior Gateway Routing Protocol)	Interior	Proprietary Cisco Systems protocol. Not limited to TCP/IP routing. Also handles IPX/SPX, SNA, and so forth
BGP (Border Gateway Protocol)	Exterior	Organization cannot choose what exterior routing protocol it will use

FIGURE 8-18 Dynamic Routing Protocols (Study Figure)

it instead of OSPF because it can route SNA and IPX/SPX traffic as well as IP traffic. On the negative side, EIGRP is a proprietary protocol, and using it forces the company to buy only Cisco routers.

EXTERIOR DYNAMIC ROUTING PROTOCOLS For communication outside the organization's network, the organization is no longer in control. It must use whatever **exterior dynamic routing protocol** the external network to which it is connected requires. The almost universal exterior dynamic routing protocol is the **Border Gateway Protocol (BGP)**. BGP is designed specifically for the exchange of routing information between autonomous systems.

Test Your Understanding

26. a) What is the purpose of dynamic routing protocols? b) In what two ways does TCP/IP use the term *routing*? c) What is an autonomous system? d) Within an autonomous system, can the organization choose its interior dynamic routing protocol? e) What are the two TCP/IP interior dynamic routing protocols? f) Which IETF dynamic routing protocol is good for small internets that do not have high security requirements? g) Which IETF dynamic routing protocol is good for large internal internets that have high security requirements? h) What is the main benefit of EIGRP compared to OSPF as an internal dynamic routing protocol? i) When might you use EIGRP as your interior dynamic routing protocol? j) May a company select the routing protocol its border router uses to communicate with the outside world? k) What is the almost universal exterior dynamic routing protocol?

Internet Control Message Protocol (ICMP) for Supervisory Messages at the Internet Layer

SUPERVISORY MESSAGES AT THE INTERNET LAYER IP is only concerned with packet delivery. For supervisory messages at the internet layer, the IETF created the **Internet Control Message Protocol (ICMP)**. IP and ICMP work closely together. As Figure 8-19

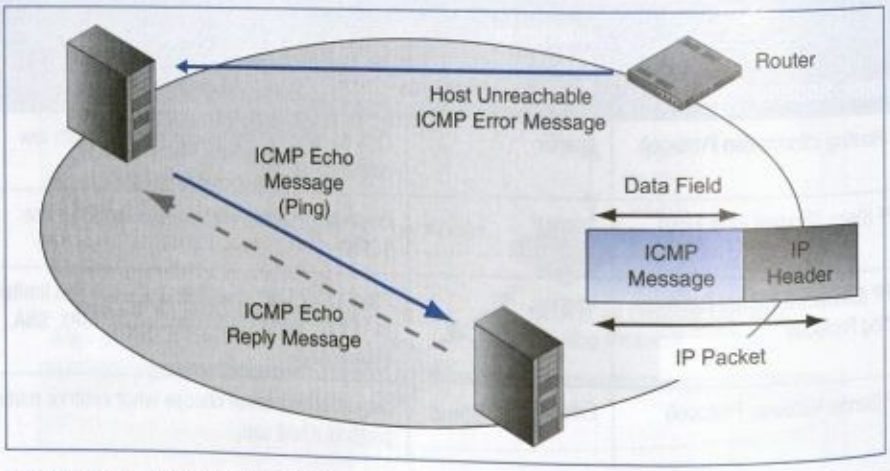


FIGURE 8-19 Internet Control Message Protocol (ICMP) for Supervisory Messages

shows, IP encapsulates ICMP messages in the IP data field, delivering them to their target host or router. There are no higher-layer headers or messages.

ERROR ADVISEMENT IP is an unreliable protocol. It offers no error correction. If the router or the destination host finds an error, it discards the packet. Although there is no retransmission, the router or host that finds the error may send an **ICMP error message** to the source device to inform it that an error has occurred, as in Figure 8-19. This is **error advisement** (notification) rather than *error correction*. There is no mechanism within IP or ICMP for the retransmission of lost or damaged packets. ICMP error messages are only sent to help the sending process or its human user diagnose problems.

One important subtlety is that sending error advisement messages is not mandatory. For security reasons, many firms do not allow error advisement messages to leave their internal internets because hackers can exploit the information contained in them.

ECHO (PING) Perhaps the most famous ICMP error message type is the **ICMP echo** message. One host or router can send an echo request message to another. If the target device's internet process is able to do so, it will send back an **ICMP echo reply** message.

Sending an echo request is often called **pinging** the target host, because it is similar to a submarine pinging a ship with sonar to see if it is there. In fact, the most common program for pinging hosts is called **ping**.[6] Echo is a good diagnostic tool because if there are network difficulties, a logical early step in diagnosis is to ping many hosts and routers to see if they can be reached.

Test Your Understanding

27. a) For what general class of messages is ICMP used? b) Explain error advisement in ICMP. c) Explain the purpose of ICMP echo messages. d) Sending an ICMP echo message is called the target host.

CONCLUSION

Synopsis

TCP/IP is a family of standards created by the Internet Engineering Task Force (IETF). IP is TCP/IP's main standard at the internet layer. IP is a lightweight (unreliable and connectionless) protocol. At the transport layer, TCP/IP offers two standards: TCP, which is a heavyweight protocol (reliable and connection-oriented), and UDP, which is a lightweight protocol like IP.

IPv4 addresses are hierarchical. Their 32 bits usually are divided into a network part, a subnet part, and a host part. All three parts vary in length. A network mask tells what bits are in the network part, while a subnet mask tells what bits are in the total of the network or subnet parts. Masks always begin with a certain number of 1s followed

[6]The echo reply message also gives the latency for the reply—the number of milliseconds between echo messages and echo reply messages. This is useful in diagnosing problems.

by enough 0s to fill the mask out to 32 bits. For human reading, masks are expressed in dotted decimal notation or prefix notation.

Routers forward packets through an internet. Border routers move packets between the outside world and an internal site network. Internal routers work within sites, moving packets between subnets. Ports in routers are called interfaces. Different interfaces may connect to different types of networks—for instance, Ethernet or Frame Relay networks. Most routers are multiprotocol routers, which can handle not only TCP/IP internetworking protocols, but also internetworking protocols from IPX/SPX, SNA, and other architectures. Routers are designed to work in a mesh topology. This creates alternative routes through the internet. Alternative routes are good for reliability. However, the router has to consider the best route for each arriving packet, and this is time consuming and therefore expensive.

To make a routing decision (deciding which interface to use to send an incoming packet back out), a router uses a routing table. Each row in the routing table represents a route to a particular network or subnet. All packets to that network or subnet are governed by the one row. Each row (route) has destination, mask, metric, interface, and next-hop router fields.

If the destination IP address in an arriving packet is in a row's range, that row is a match. After finding all matches in the routing table, the router finds the best-match row on the basis of match length and, in the case of tied match lengths, on metric values. Once a best-match route (row) is selected, the router sends the packet out a particular interface to the next-hop router specified in that row or to the destination IP address if the destination host is out the interface.

In the examples in the main text, masks broke at 8-bit boundaries, making it easy to specify them with dotted decimal notation. If you read the box "Masking When Masks Do Not Break at 8-Bit Boundaries," you can deal more realistically with the world of masking because masks often do not break at 8-bit boundaries.

If you read the box, "The Address Resolution Protocol (ARP)," you saw that the router must encapsulate the packet in a frame in order to send it out. ARP is a protocol to learn the data link layer destination of the device to which a router or host will send a frame if the router or host only knows the destination host's IP address.

IP version 4 has a number of important fields besides the source and destination address fields. The time to live (TTL) field ensures that packets that are misaddressed do not circulate endlessly around the Internet. The protocol field describes the contents of the data field—ICMP message, TCP segment, UDP datagram, and so forth.

IP version 6 will require networking and security professionals to understand a new approach to expressing addresses. IPv6 addresses are 128 bits long. For human comprehension, they are expressed in hexadecimal notation. In addition, there are certain rules that compress the hex version of the address to reduce its complexity.

The IPv6 header is simpler than the IPv4 header, but because the two address fields are far larger in IPv6 than in IPv4, the IPv6 header is 40 octets long instead of the 20 octet length of IPv4 headers if there are no options. The IPv6 header saves time on each router by not checking for errors and not allowing fragmentation. The IPv6 header has a mechanism for specifying quality-of-service parameters for the packet and for marking the packet as a member of a flow of packets with predefined quality-of-service parameters.

IPv6 does not have options. Instead, it specifies a number of optional extension header for hop-by-hop options, security, and other matters. The next-header field in the main header and each extension header specifies the type of header (or upper layer protocol) that follows this header.

The Transmission Control Protocol (TCP) has sequence numbers that allow the receiving transport process to place arriving TCP segments in order. The TCP header has several flag fields that indicate whether the segment is a SYN, FIN, ACK, or RST segment. Connection openings use a three-step handshake that uses SYN segments. Normal closes involve a four-step message exchange that use FIN segments. Resets close a connection with a single segment (RST) instead of the normal four.

Routers build their routing tables by listening to other routers. Routers frequently exchange messages, giving information stored in their routing tables. These messages are governed by one of several available dynamic routing protocols.

IP itself does not have supervisory messages. For internet layer supervisory messages, hosts and ro uters use the Internet Control Message Protocol (ICMP). We looked at two types of ICMP messages—error advisement messages and echo messages (ping). ICMP messages are carried in the data fields of IP packets.

END-OF-CHAPTER QUESTIONS

Thought Questions

1. How do the postal services use hierarchical sorting? How does this simplify delivery decisions?
2. Give a non-network example of hierarchical addressing, and discuss how it reduces the amount of work needed in physical delivery. Do not use any example in the book, a postal service, or the telephone network.
3. A client PC has two simultaneous connections to the same webserver application program on a webserver. (Yes, this is possible, and in fact, it is rather common.) What will be different between the TCP segments that the client sends on the two connections?
4. A router that has the routing table in Figure 8-8 receives an incoming IPv4 packet. The source IP address is 10.55.72.234. The destination host is 10.4.6.7. The TTL value is 1. The Protocol field value is 6. What will the router do with this packet?

Harder Thought Question

1. For security reasons, many organizations do not allow error reply messages to leave their internal internets. How, specifically, could hackers use information in echo reply messages to learn about the firm's internal hosts? (Hint: Notice that ICMP message are carried in the data fields of IP packets.)

Troubleshooting Question

1. You suspect that the failure of a router or of a transmission line connecting routers has left some of your important servers unavailable to clients at your site. How could you narrow down the location of the problem using what you learned in this chapter?

Perspective Questions

1. What was the most surprising thing you learned in this chapter?
2. What was the most difficult material for you in this chapter?

9 TCP/IP INTERNETWORKING II

LEARNING OBJECTIVES

By the end of this chapter, you should be able to:

- Explain TCP/IP management: IP subnet planning, Network Address Translation (NAT), Multiprotocol Labor Switching (MPLS), the Domain Name System (DNS), DHCP servers, the Simple Network Management Protocol (SNMP), and IPv6 management.

INTRODUCTION

In Chapter 8, we looked at important TCP concepts. In this chapter, we will focus on the security and management of TCP/IP networks.

CORE TCP/IP MANAGEMENT TASKS

If a firm uses TCP/IP as its internetworking protocol, it must do a considerable amount of work to build and maintain the necessary infrastructure of TCP/IP. While switched networks are (generally) capable of operating for long periods of time without intervention by network managers, TCP/IP internets require constant tuning and support. This results in a need for considerable TCP/IP expertise and management effort. As we saw in Chapter 1, network managers say, "Switch where you can, route where you must."

IP Subnet Planning

As Chapter 8 discussed, IP addresses are 32 bits long. Each organization is assigned a network part. We saw that the University of Hawai`i's network part (128.171) is 16 bits long. There is nothing a firm can do to alter its network part. However, it was up to the university to decide what to do with the remaining 16 bits.

SUBNETTING AT THE UNIVERSITY OF HAWAI`I The University, like most organizations, chose to subnet its IP address space. It divided the 16 bits over which it has discretion into an 8-bit subnet part and an 8-bit host part.

THE $2^N - 2$ RULE With N bits, you can represent 2^N possibilities. Therefore, with 8 bits, one can represent 2^8 (256) possibilities. This would suggest that the university can have

Step	Description				
1	Total size of IP address (bits)	32			
2	Size of network part assigned to firm (bits)	16		8	
3	Remaining bits for firm to assign	16		24	
4	Selected subnet/host part sizes (bits)	8/8	6/10	12/12	8/16
5	Possible number of subnets ($2^N - 2$)	254 ($2^8 - 2$)	62 ($2^6 - 2$)	4,094 ($2^{12} - 2$)	254 ($2^8 - 2$)
6	Possible number of hosts per subnet ($2^N - 2$)	254 ($2^8 - 2$)	1,022 ($2^{10} - 2$)	4,094 ($2^{12} - 2$)	65,534 ($2^{16} - 2$)

FIGURE 9-1 IP Subnetting

256 subnets, each with 256 hosts. However, a network, subnet, or host part cannot be all 0s or all 1s.[1] Therefore, the university can have only 254 (256 – 2) subnets, each with only 254 hosts. Figure 9-1 illustrates these calculations.

In general, if a part is N bits long, it can represent $2^N - 2$ networks, subnets, or hosts. For example, if a subnet part is 9 bits long, there can be $2^9 - 2$, or 510, subnets. Or if a host part is 5 bits long, there can be $2^5 - 2$, or 30, hosts.

In general, if a part is N bits long, it can represent $2^N - 2$ networks, subnets, or hosts.

BALANCING SUBNET AND HOST PART SIZES The larger the subnet part, the more subnets there will be. However, the larger the subnet part is made, the smaller the host part will be. This will mean fewer hosts per subnet. There is always a trade-off. More subnets mean fewer hosts, and more hosts mean fewer subnets.

The University of Hawai`i's choice of 8-bit network and subnet parts was acceptable for many years because no college needed more than 254 hosts. Its advantage is that its subnet mask (255.255.255.0) was very simple, breaking at 8-bit boundaries. This made it easy to see which hosts were on which subnets. The host at 128.171.17.5, for instance, was the fifth host on the *17th* subnet. If the subnet mask did not break at an 8-bit boundary, you cannot see which subnet a host is on by looking at the address in dotted decimal notation.

However, many colleges in the university now have more than 254 computers, and the limit of 254 hosts required by its subnetting decision has become a serious problem. Several colleges now have two subnets connected by routers. This is expensive and awkward.

The university would have been better served had it selected a smaller subnet part, say 6 bits. As Figure 9-1 shows, this would have allowed 62 college subnets, which probably would have been sufficient. A 6-bit subnet part would give a 10-bit host part, allowing 1,022 hosts per subnet. This would be ample for several years to come.

[1] If you have all 1s in an address part, this indicates that broadcasting should be used. All 0s parts are used by computers when they do not know their addresses. As we will see later in this chapter, most client PCs get their IP addresses from DHCP servers. All-zero addresses can only be used in the source addresses of DHCP messages sent from a host to a DHCP server.

A CRITICAL CHOICE In general, it is critical for corporations to plan their IP subnetting carefully, in order to get the right balance between the sizes of their network and subnet parts.

Test Your Understanding

1. a) Why is IP subnet planning important? b) If you have a subnet part of 9 bits, how many subnets can you have? c) Your firm has an 8-bit network part. If you need at least 250 subnets, what must your subnet size be? d) How many hosts can you have per subnet? e) Your firm has a 20-bit network part. What subnet part would you select to give at least 10 subnets? f) How many hosts can you have per subnet?

Network Address Translation (NAT)

One issue that firms face is whether to allow people outside the corporation to learn their internal addresses. This is a security risk. If attackers know internal IP addresses, this allows them to send attack packets from the outside world. To prevent this, companies

NAT

Sends false external IP addresses that are different from internal IP addresses

NAT Operation (Figure 10-13)

NAT Is Transparent to Internal and External Hosts

Security Reason for Using NAT

External attackers can put sniffers outside the corporation
Sniffers can learn IP addresses
Attackers can send attacks to these addresses
With NAT, attackers only learn false external IP addresses

Expanding the Number of Available IP Addresses

Companies may receive a limited number of IP addresses from their ISPs
There are roughly 4,000 possible ephemeral port numbers for each IP address
So for each IP address, there can be 4,000 external connections
If a firm is given 248 IP addresses, there can be roughly one million external connections
Even if each internal device averages several simultaneously external connections, there should not be a problem providing as many external IP connections as a firm desires

Private IP Addresses

Can only be used inside firms
10.x.x.x
192.168.x.x (most popular)
172.16.x.x through 172.31.x.s

Protocol Problems with NAT

IPsec, VoIP, etc.
Work-arounds must be considered very carefully in product selection

FIGURE 9-2 Network Address Translation (NAT) (Study Figure)

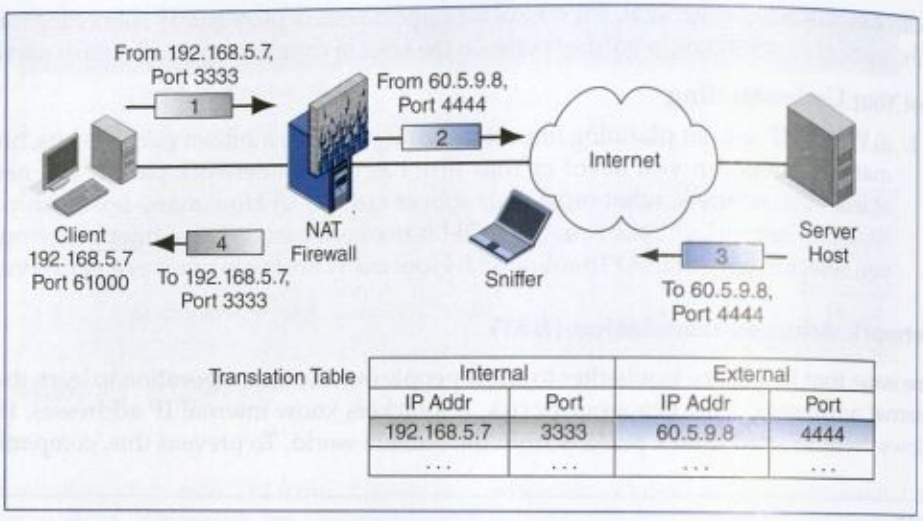


FIGURE 9-3 Network Address Translation (NAT) Operation

can use **network address translation (NAT)**, which presents external IP addresses that are different from internal IP addresses used within the firm.

NAT OPERATION Figure 9-3 shows how NAT works. An internal client host, 192.168.5.7, sends a packet to an external server host. The source address in this packet is 192.168.5.7, of course. The source port number is 3333, which is an ephemeral port number that the source host made up for this connection.

When the NAT firewall at the border receives the packet, it makes up a new row in its translation table. It places the internal IP address and port number in the table. It then generates a new external source IP address and external source port number. These are 60.5.9.8 and 4444, respectively.

When packets arrive from the external host, they have 60.5.9.8 in their destination IP address fields and 4444 in their destination port number fields. The NAT firewall looks these values up in its translation table, replaces the external values with the internal values, and sends them on to the client PC.

TRANSPARENCY NAT is transparent to both internal and external hosts. Hosts do not even know that NAT is happening. Consequently, there is no need to change the ways in which they operate.

SECURITY Figure 9-3 shows how NAT brings security. An attacker may be able to install a **sniffer program** beyond the corporation's NAT firewall. This sniffer will be able to read all packets coming out of the firm. With NAT, an eavesdropper only learns false (external) IP addresses and port numbers. In theory, if an attacker can attack immediately, it can send packets to the external IP addresses and port numbers, and the NAT firewall will pass them on to the internal host. However, this is rarely possible. NAT provides a surprising amount of security despite its simple operation.

EXPANDING THE EFFECTIVE NUMBER OF AVAILABLE IP ADDRESSES An equally important potential reason for using NAT is to permit a firm to have many more internal IP addresses than it is given by its ISP. Suppose that an ISP only gives the firm 254 IP addresses by giving it a host part with 24 bits. Without NAT, a firm can only have 254 PCs simultaneously using the Internet.

However, NAT is really network address translation/port address translation (NAT/*PAT*). With Microsoft Windows, there are almost 4,000 ephemeral port numbers. Even if internal hosts maintained four simultaneous connections to the outside world on average, each IP address could be used by 1,000 client PCs to make outside connections by giving each client PC a different set of port numbers for its connections. If a firm has 254 IP addresses, it can multiply this already large number of connections by 4,000. This could support almost a quarter million PCs using the Internet simultaneously, with each PC having four external connections. While no firm would push the number of connections this far, having 10 to 100 internal hosts for each external IP address is very common.

USING PRIVATE IP ADDRESSES To support NAT, the Internet Assigned Numbers Authority (IANA) has created three sets of **private IP address ranges** that can only be used *within* firms. These are the three ranges:

- 10.x.x.x
- 192.168.x.x
- 172.16.x.x through 172.31.x.x

The 192.168.x.x private IP address range is the most popular because it allows companies to use 255.255.0.0 and 255.255.255.0 network and subnet masks, respectively. These break at convenient 8-bit boundaries. However, the other two private IP address ranges are also widely used.

PROTOCOL PROBLEMS WITH NAT In terms of security and expanding IP effective address ranges, NAT is a simple and effective tool. However, some protocols cannot work across a NAT firewall or can work only with considerable difficulty. These include the popular IPsec cryptographic system in transport mode and several voice over IP (VoIP) protocols. The decision to use NAT must be made only after a careful assessment of protocols.

Test Your Understanding

2. a) What is NAT? (Do not just spell it out.) b) Describe NAT operation. c) What are the two benefits of NAT? d) How does NAT enhance security? e) How does NAT allow a firm to deal with a shortage of IP addresses given to it by its ISP? f) How are private IP address ranges used? g) What are the three ranges of private IP addresses? h) What problems may firms encounter when using NAT?

The Domain Name System (DNS)

As we saw in Chapter 1, if a user types in a target host's host name, the user's PC will contact its local Domain Name System (DNS) server. The DNS server will return the IP address for the target host or will contact other DNS servers to get this information. The user's PC can then send IP packets to the target host. In this chapter, we will look at DNS and its management in more detail.

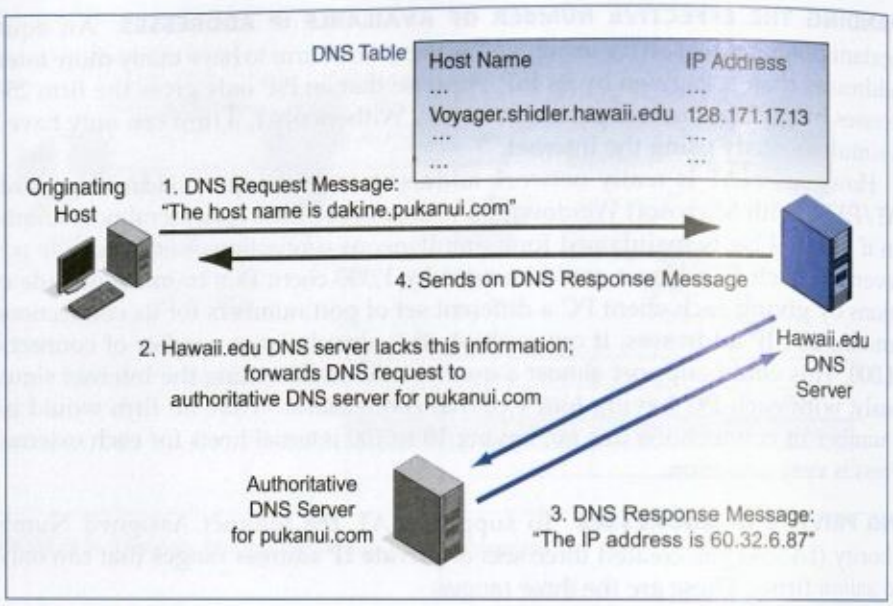


FIGURE 9-4 Domain Name System (DNS) Lookup

Figure 9-4 looks at how a DNS provides IP addresses when a host sends a request message containing a host name. In many cases, as we saw in Chapter 1, the local DNS server will know the IP address and send it back. In other cases, the local DNS host will not know the host's IP address. It must then find the **authoritative DNS server** for the domain in the host name. In the figure, dakine.pukanui.com's authoritative DNS server is authoritative for the pukanui.com domain. This DNS server will send the IP address to the local DNS server, which will pass the address on to the host that sent the DNS request.

WHAT IS A DOMAIN? Figure 9-5 shows that the **Domain Name System (DNS)** and its servers are not limited to providing IP addresses for host names. More generally, DNS is a general system for naming domains. A **domain** is any group of resources (routers, single networks, and hosts) under the control of an organization. The figure shows that domains are hierarchical, with host names being at the bottom of the hierarchy.

A domain is any group of resources (routers, single networks, and hosts) under the control of an organization.

ROOT The domain name system is organized in a hierarchy. At the top of the DNS hierarchy is the root, which consists of all domain names. The overall control of the root, and therefore of the entire directory tree, is the Internet Corporation for Assigned Names and Numbers (ICAAN). There are 13 **root DNS servers** that keep overview information for the system.

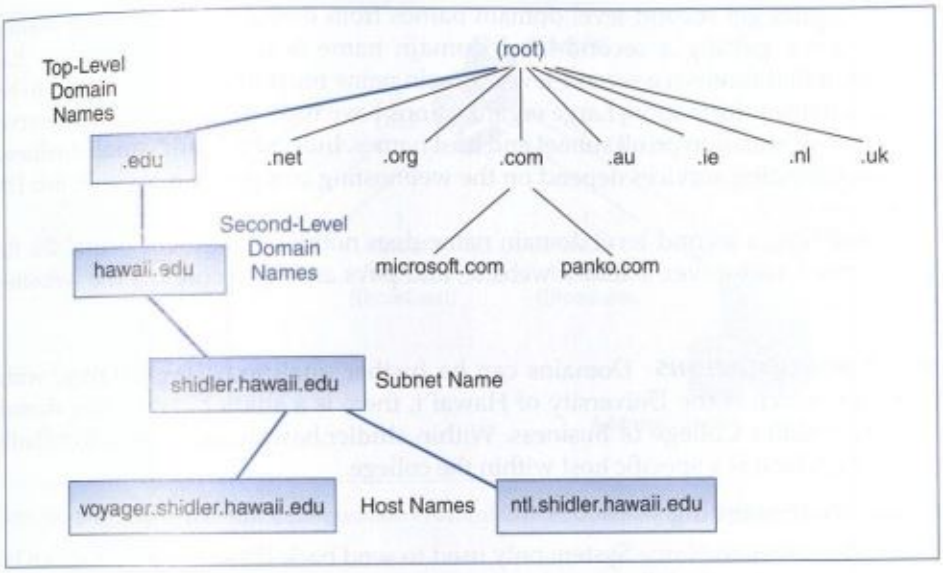


FIGURE 9-5 Domain Name System (DNS) Hierarchy

TOP-LEVEL DOMAINS Under the root are **top-level domains** that categorize the domain in one of two ways.

- **Country top-level domains** specify the country of the domain owner. Examples are .uk, .ca, .ie, .au, .jp, .nl, .tv, .md, and .ch.
- **Generic top-level domains (gTLDs)** specify that the domain is of a particular type. The first gTLDs included .com, .edu, .net, .info, .gov, and .org. Later, several more gTLDs were added, such as .name. In 2012, ICANN opened the naming system, permitting any organization to come forth with new generic top-level domains.

Note the distinction between the root and top-level domains. The root consists of all domains. It is not named as a level, however. If you are familiar with the UNIX operating system, the root directory concept is similar.

Also note that it is common for a domain to have two first-level designations, for instance, AAAA.com.ie. Most organizations, however, tend to use either a country TLD or a generic TLD.

SECOND-LEVEL DOMAINS Under first-level domains are **second-level domains**, which usually specify a particular organization (microsoft.com, hawaii.edu, cnn.com, etc.). Sometimes, however, specific products, such as movies, get their own second-level domain names. Competition for good second-level domain names is fierce. Organizations and individuals compete fiercely to get second-level domains because this is how the public will reach them.

Organizations and individuals compete fiercely to get second-level domains because this is how the public will reach them.

Companies get second-level domain names from domain registrars for nominal fees. However, getting a second-level domain name is only the beginning. Each organization that receives a second-level domain name must have a DNS server to host its domain name information. Large organizations have their own internal DNS servers that contain information on all subnet and host names. Individuals and small businesses that use webhosting services depend on the webhosting company to provide this DNS service.

In addition, a second-level domain name does nothing for the firm until the firm buys or rents a webserver, builds a website, and pays an ISP to connect the website to the Internet.

FURTHER QUALIFICATIONS Domains can be further qualified. For instance, within hawaii.edu, which is the University of Hawai`i, there is a shidler.hawaii.edu domain. This is the Shidler College of Business. Within shidler.hawaii.edu is voyager.shidler.hawaii.edu, which is a specific host within the college.

Test Your Understanding

3. a) Is the Domain Name System only used to send back IP addresses for given host names? Explain. b) What is a domain? c) Distinguish between the DNS root and first-level domains. d) What are the two types of top-level domains? e) Which level of domain name do corporations most wish to have? f) What are DNS root servers? g) How many DNS root servers are there? h) How does a company or individual obtain a second-level domain name? i) Why is getting a second-level domain name only the beginning?

DHCP Servers

In Chapter 1, we saw that client PCs usually get their IP addresses and other configuration information from DHCP servers. This means that they have current configuration information each time they boot up. It also means that they usually get a different IP address each time they boot up. In contrast, servers get static (permanent) IP addresses so that they have the same IP address all the time. This allows clients to find them.

In Chapter 1, we also saw that when a client PC wakes up, it realizes that it has no IP address. It broadcasts a Dynamic Host Configuration Protocol (DHCP) message to all nearby hosts. Only the DHCP server responds.

Figure 9-6 shows that the situation actually is a bit more complex. As the figure shows, there may be multiple DHCP servers, and each will send a response back to the client PC. These initial responses do not carry configuration information. Rather, they are offers of what configuration a DHCP server will provide, including the length of time a PC may use its IP address before surrendering it and starting another DHCP search to get a new IP address.

The user selects among the offers and sends back an acceptance message to the "winning" DHCP server. That server responds with the configuration information. If there is only a single DHCP server, the client PC still goes through the seek–offer–accept–receive cycle. So the DHCP discussion in Chapter 1 was a simplification.

Which of a firm's DHCP servers will respond to an initial DHCP request? The answer is that each DHCP server has a DHCP scope parameter that lists the subnets to which it will respond with an offer.

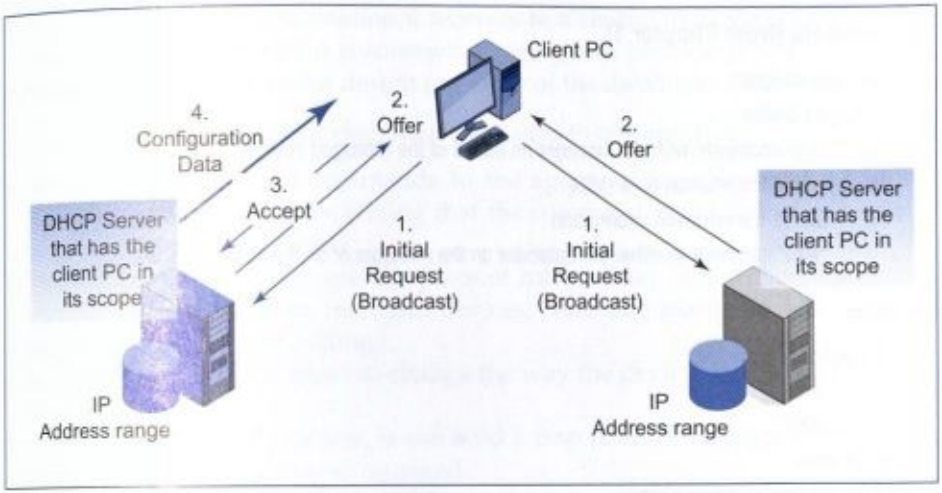


FIGURE 9-6 Dynamic Host Configuration Protocol (DHCP) Operation

The fact that several DHCP servers may respond can provide redundancy and therefore reliability. However, companies must manage each DHCP server's scope and list of available IP addresses carefully.

In addition, when a firm changes its DNS servers to another IP address, changes its subnet masks, or makes any other changes that will affect client PC configuration, it must push these changes out to all DHCP servers.

Test Your Understanding

4. a) What hosts are given static IP addresses? b) Why do these hosts need static IP addresses? c) What are dynamic IP addresses? d) How do clients get dynamic IP addresses? e) Can the client send a DHCP request information to multiple DHCP servers? f) Do DHCP servers update the configuration information they store automatically? g) What are DHCP scopes?

Simple Network Management Protocol (SNMP)

We saw the *Simple Network Management Protocol (SNMP)* in the first chapter and in several chapters since. We will now look at it in a little more detail.

CORE SNMP ELEMENTS In Chapter 1, we saw that SNMP has several components.

- The network administrator works at a central computer that runs a program called the network management program, or, more simply, the manager.
- The SNMP manager is responsible for many managed devices—devices that need to be administered, such as printers, switches, routers, and other devices.
- Managed devices have pieces of software (and sometimes hardware) called network management agents, or, more simply, agents. SNMP agents communicate with the SNMP manager on behalf of their managed devices. In other words, the manager does not communicate with the managed device directly, but rather with the device's agent.

Core Elements (from Chapter 1)

- Manager program
- Managed device
- Agents (communicate with the manager on behalf of the managed device)
- Management information base (MIB)
  - Stores the retrieved information
  - "MIB" can refer to either the database on the manager or on the database schema

Messages

- Commands
  - Get
  - Set
- Responses
- Traps (alarms sent by agents)
- SNMP use UDP at the transport layer to minimize the burden on the network

RMON Probes

- Remote monitoring probes
- A special type of agent
- Collects data for a part of the network
- Supplies this information to the manager

Objects (see Figure 10-19)

- Information about which information is stored
- Number of rows in the routing table
- Number of discards caused by lack of resources (indicates a need for an upgrade)

Set Commands

- Dangerous if used by attackers
- Many firms disable set to thwart such attacks
- However, they give up the ability to manage remote resources without travel
- SNMPv1: community string shared by the manager and all devices
- SNMPv3: each manager–agent pair has a different password

User Functionality

- Reports, diagnostics tools, etc. are very important
- They are not built into the standard
- They are added by SNMP manager vendors
- Critical in selection

FIGURE 9-7 Simple Network Management Protocol (SNMP) (Study Figure)

- The manager stores information it receives in a central management information base (MIB). The term *MIB* is somewhat ambiguous because it can refer either to the database itself or to the design (schema) of the database.

To work together, these devices send messages to one another.

- The manager can send commands to the agent, telling the agent what to do. Agents send responses confirming that the command was fulfilled or explaining why it could not be fulfilled.
- *Get* commands ask for a specific piece of information. In practice, the manager constantly polls all of its managed devices, collecting many pieces of data from each in every round of polling.
- *Set* commands tell the agent to change the way the device operates, say by going into self-test mode.
- If an agent detects a problem, it can send a trap (alarm) message to the manager without waiting passively to be asked.
- These commands are sent via UDP to reduce the traffic burden on the network. This leads to occasional errors, but single errors only mean that a few pieces of information are a few seconds or minutes out of date.
- In addition, there is a specialized type of agent called an **RMON probe** (remote monitoring probe). This may be a stand-alone device or software running on a switch or router. An RMON probe collects data on network traffic passing through its location instead of information about the RMON probe itself. The manager can poll the RMON probe to get summarized information about the distribution of packet sizes, the number of various types of errors, the number of packets processed, the 10 most active hosts, and other statistical summaries that may help pinpoint problems. This generates far less network management traffic than polling many devices individually.

The SNMP MIB schema is organized as a hierarchy of **objects** (properties of managed devices). Figure 9-8 shows the basic model for organizing SNMP objects. First, there is the system. This might be a computer, switch, router, or another device. In addition, there are TCP, UDP, IP, and ICMP objects and objects for individual interfaces. Each of these objects has sub-objects under it, and those sub-objects may have further sub-sub-objects.

For example, if a router does not appear to be working properly, the manager can issue **Get** commands to collect appropriate router objects. A first step might be to check if the router is in forwarding mode. If not, it will not route packets. If this does not clarify the problem, the manager can collect more information, including error statistics and general traffic statistics of various types.

The **Set** command is even more powerful. The manager can use a Set command to tell an agent to change the configuration of a managed device. If a router interface seems to be malfunctioning, the manager can have the interface put into testing mode or even turned off. Set commands can also turn off interfaces to avoid using expensive transmission lines when existing less expensive lines can be used. The Set command can send even more detailed commands, for instance, changing how long an interface waits before sending a retransmission because no acknowledgment has been received. By allowing administrators to manage devices remotely, the Set command can save companies a great deal of money by avoiding travel to fix problems.

System Objects

System name
System description
System contact person
System uptime (since last reboot)

IP Objects

Forwarding (for routers). Yes if forwarding (routing), No if not
Subnet mask
Default time to live
Traffic statistics
Number of discards because of resource limitations
Number of discards because could not find route
Number of rows in routing table
Rows discarded because of lack of space
Individual row data

TCP Objects

Maximum/minimum retransmission time
Maximum number of TCP connections allowed
Opens/failed connections/resets
Segments sent
Segments retransmitted
Errors in incoming segments
No open port errors
Data on individual connections (sockets, states)

UDP Objects

Error: no application on requested port
Traffic statistics

ICMP Objects

Number of errors of various types

Interface Objects (One per Interface)

Type (e.g., 69 is 100Base-FX; 71 is 802.11)
Status: up/down/testing
Speed
MTU (maximum transmission unit—the maximum packet size)
Traffic statistics: octets, unicast/broadcast/multicast packets
Errors: discards, unknown protocols, etc.

FIGURE 9-8 SNMP Hierarchical Object Model

SET COMMANDS AND SNMP SECURITY Unfortunately, most firms are very reluctant to use Set commands because of security dangers. If setting is permitted and attackers learn how to send Set commands to managed devices, the results could be catastrophic. Fortunately, SNMP security has improved over time.

- The original version of SNMP, SNMPv1, had almost no authentication at all, making this danger a distinct possibility. The manager and all managed devices merely had to be configured with the same secret **community name**. With hundreds or thousands of devices sharing the same community name, if attackers can learn the community name, they can implement massive attacks. Of course, "everybody" knows the community name, so there is usually little effort to keep it secret.
- SNMPv3 has added passwords for each manager–agent pair, and these pairwise passwords are used to authenticate and encrypt transmissions. This requires a great deal of work to set up, but it is the only way to secure SNMP.

Most products today permit two SNMPv3 passwords for each manager–device pair. One is for *Get* commands and the other is for the more dangerous *Set* commands.

Of course, poor implementation can defeat SNMPv3 security. If a lazy administrator uses the same password for all manager–agent pairs, then this is no better security than community strings.

USER INTERFACE FUNCTIONALITY Collecting data in the MIB is worthless if there is no good way to get it out. All SNMP manager products have the ability to produce reports, diagnose problems, and do many other things that network administrators need to manage networks.

This functionality is not built into the standard. The standard just handles the mechanics of collecting and storing object data from managed devices. User interface functionality is a critical factor in selecting SNMP products.

Test Your Understanding

5. a) List the main elements in a network management system. b) Does the manager communicate directly with the managed device? Explain. c) Explain the difference between managed devices and objects. d) Is the MIB a schema or the actual database? (This is a trick question.) e) Why must user interface functionality for the SNMP manager be considered carefully in selecting SNMP manager products?
6. List one object in each of the following areas: the system, IP, TCP, UDP, ICMP, and an interface.
7. a) In SNMP, which device creates commands? b) Responses? c) Traps? d) Explain the two types of commands. e) What is a trap? f) Why are firms often reluctant to use *Set* commands? g) Describe SNMPv1's poor authentication method. h) Describe SNMPv3's good authentication method.

MULTIPROTOCOL LABEL SWITCHING

Making Routing More Efficient

In Chapter 8, we looked at how routers handle IP packets. They look at an incoming packet's destination IP address. They then compare that IP address to every row in the routing table, select the best match, and send the packet back out a certain port to a

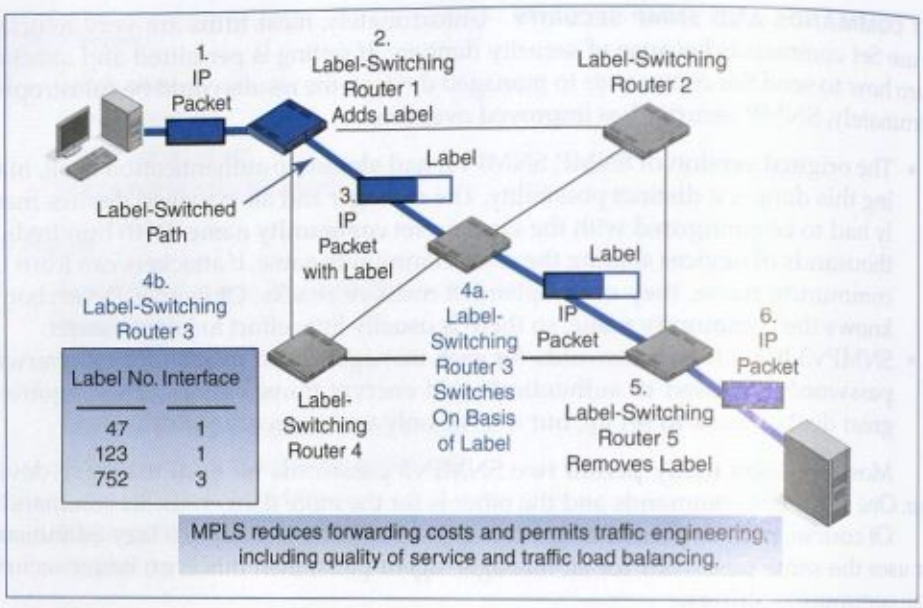


FIGURE 9-9 Multiprotocol Label Switching (MPLS)

certain IP address. The next packet to arrive gets the same treatment—*even if it is going to the same IP address*.

We also noted that many router vendors do decision caching, in which they remember their decisions for certain IP address ranges. We noted that this is somewhat dangerous. Fortunately, there is a more systematic way to avoid having to look at all rows for all packets. This is the **Multiprotocol Label Switching (MPLS)** standard, which Figure 9-9 illustrates.

MPLS Operation

When two hosts begin to communicate, an MPLS network does not immediately send packets. Instead, it determines the best path for the packets. This best path is called the **label-switched path**. This is what gives MPLS its advantages. It may be slow to select a label-switched path at the beginning of a conversation, but we will see that MPLS handles each subsequent packet very quickly.

As Figure 9-9 shows, the source host sends an ordinary IP packet during the rest of the conversation. The router to which the source host connects is a label-switching router. This router places a **label header** in front of the IP header (and after the frame header). Note that this means that there is no need to change either the IP packet syntax or the frame syntax. The label header is simply pushed into place between the frame header and the IP header.

The label header has a **label number** that identifies the label-switched path previously selected for packets in this conversation. The first label-switched router and all others along the label-switching path have a simple MPLS look-up table. This table allows the label-switched router to look up the label number, read the corresponding interface, and send the packet out the indicated interface. For example, if the label number is 47, the router in Figure 9-9 will send it out Interface 1. There is no need to

look at many regular routing table rows to select the best interface to send a packet back out. That work was already done when the label-switched path was selected.

Each label-switched router along the way repeats this simple look-up process and forwards the packet on its way. The last label-switched router removes the label, because the destination host does not need it. Note that neither the source host nor the destination host knows that label switching was done.

All packets between two host IP addresses might be assigned the same label number. More likely, all traffic between two *sites* might be assigned a single label number because it would all be going to and from the same site.

Benefits of Label Switching

MPLS offers three major benefits: cost reduction, quality of service, and traffic engineering.

LABEL SWITCHING FOR COST REDUCTION MPLS is much faster than traditional routing calculations because there is only a single row for each label number. This simplicity dramatically lowers the cost of routing.

QUALITY OF SERVICE Lowering routing costs is the main attraction of MPLS, but there are other advantages as well. One is quality of service. Traffic flowing between two sites might be assigned different label numbers. One label number might be for VoIP, which is latency-intolerant, and the other might be for latency-tolerant traffic between the sites. For latency-intolerant traffic, it is even possible to reserve capacity at routers along the selected path. This gives full quality of service.

TRAFFIC ENGINEERING MPLS can also be used for **traffic engineering**, that is, to manage how traffic will travel through the network. One capability is **load balancing**, that is, to move some traffic from a heavily congested link between two routers to an alternative route that uses different and less-congested links. MPLS does this by setting up multiple label-switched routes ahead of time and by sending traffic based on the congestion along different label-switched routes.

MPLS Boundaries

Corporations can use MPLS internally, and most ISPs now use MPLS for their internal traffic, but it is currently impossible to implement MPLS across the entire Internet because of coordination difficulties among the ISPs.

Test Your Understanding

8. a) In MPLS, is selecting the best interface for each packet done when the packet enters the network or before? b) What is the name of the path selected for a particular conversation? c) When a source host first transmits to a destination host, what will happen? d) Do label-switching routers along the MPLS path look at the packet's IP address? Explain your reasoning. e) Why is MPLS decision making fast compared to traditional routing? f) On what does each label-switched router base routing decisions? g) Why is MPLS transparent to the source and destination hosts? h) What is MPLS's main attraction? i) What are its other attractions? j) What is traffic engineering? k) Can MPLS provide traffic load balancing? l) Is it possible to implement MPLS on the entire Internet?

SECURING INTERNET TRANSMISSION

When the Internet was first created, little thought was given to security. As Jon Postel, who edited the main Internet RFCs, explained to the first author, "It just wasn't a problem then, and we were stretched thin." Today, however, Internet security is very much a pressing issue. Companies are beginning to address the security of transmissions across the Internet (and within site networks as well) by using IPsec virtual private networks.

Virtual Private Networks

Figure 9-10 shows that corporations can cryptographically protect traffic flowing between two sites or between a site and a remote user. They can do this by using a **virtual private network (VPN)**, which is a cryptographically secured transmission path through an untrusted environment. Although the firm is using a shared network, it appears to be alone, as far as security is concerned. The Internet is not the only untrusted network, but it is by far the largest.

A virtual private network (VPN) is a cryptographically secured transmission path through an untrusted environment.

Figure 9-10 shows a **remote access VPN** connecting a remote user to a site and a **site-to-site VPN** that connects two corporate sites.

A remote access VPN connects a remote user to a site.

A site-to-site VPN connects two corporate sites.

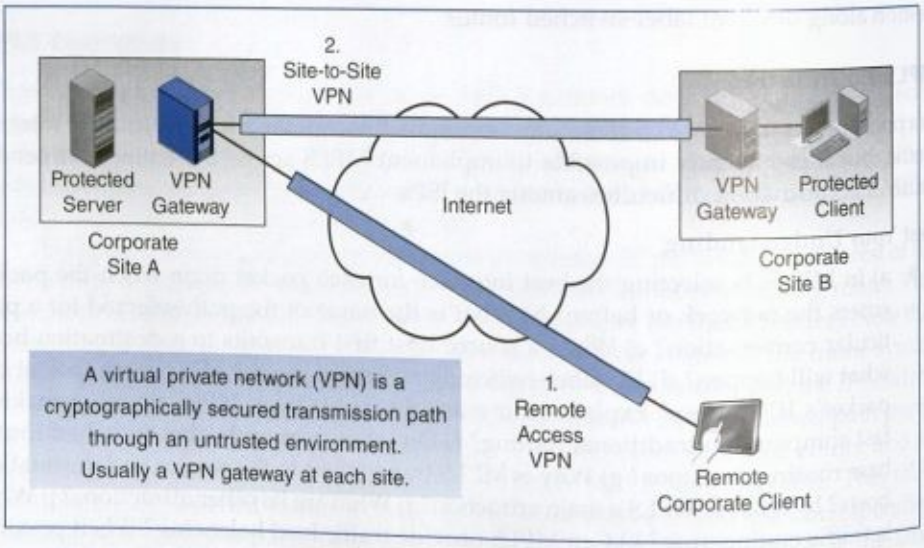


FIGURE 9-10 Virtual Private Networks (VPNs)

- Remote access VPNs are attractive because single hosts trying to connect to a corporate site via the Internet are extremely vulnerable. They are even more vulnerable if they connect to their network wirelessly.
- Site-to-site VPNs protect all traffic flowing between a pair of sites. Typically, sites have heavy traffic between themselves, so site-to-site VPNs tend to carry much more traffic than remote access VPNs.

Both remote-access VPNs and site-to-site VPNs usually terminate in a **VPN gateway** at a site. This VPN gateway handles cryptographic protections when dealing with remote users or a VPN gateway at another site.

IPsec VPNS

For security over the Internet, the Internet Engineering Task force created a family of standards collectively called **IP security (IPsec)**.[2] As its name suggests, IPsec operates at the internet layer. It provides security to all content at the internet, transport, and application layers.[3] This protection is **transparent**, meaning that nothing additional has to be done to protect upper-layer content and that all upper-layer content is protected. By securing packets and their contents, the IETF provided a single mechanism to protect TCP/IP traffic.

IPsec operates at the internet layer. It provides security to all content at the internet, transport, and application layers.

IPsec offers the strongest security and should eventually dominate remote access VPN transmission, site-to-site VPN transmission, and internal site IP transmission. However, IPsec networks are fairly complex to manage and therefore relatively expensive.

IPsec Transport Mode

Figure 9-11 shows IPsec's two modes of operation. In **transport mode**, the two computers that are communicating implement IPsec. This mode gives strong end-to-end security, but it requires IPsec configuration *and* a digital certificate on all machines. Although the cost per machine for configuration and for the digital certificate is small, the large number of computers in a company makes the aggregate cost of transport mode setup high.

IPsec Tunnel Mode

In contrast, in **tunnel mode**, the IPsec connection extends only between *IPsec gateways* at the two sites. This provides no protection within sites, but the use of tunnel mode IPsec gateways offers simple security. The two hosts do not have to implement IPsec

[2] IPsec is pronounced "eye-pea-sek," with emphasis on the *sek*.
[3] Actuall y, the term *all* is a bit too strong. In transport mode, which is discussed later, attackers can read the IP addresses because the packet is addressed to the destination host instead of to the IPsec gateway server. However, on exams, call it *all*.

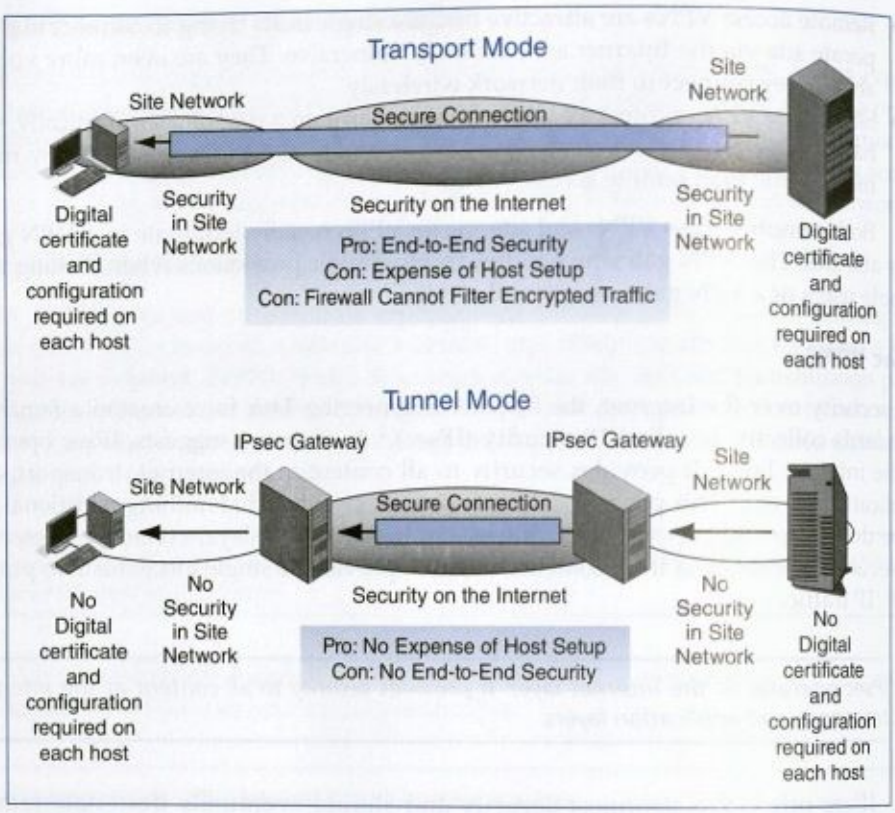


FIGURE 9-11 IPsec in Transport Mode and Tunnel Mode

security and, in fact, do not even have to know that IPsec is being used between the IPsec gateways. Most importantly, there is no need to install digital certificates on individual hosts. Only the two IPsec gateways need to have IPsec configuration and digital certificates. Tunnel mode minimizes costs but provides no protection for the traffic within the sites.

Remote-Access and Site-to-Site VPNs

IPsec is a versatile protocol that can be used simultaneously for both remote-access VPNs and site-to-site VPNs. Coupled with its ability to protect all upper-layer content transparently, IPsec is a general solution for a firm's cryptographic protection needs.

IPsec Security Associations and Policy Servers

One advantage of IPsec as a VPN technology is that it can be centrally managed. Figure 9-12 shows that before two IPsec gateways begin to communicate, they negotiate how they will perform security. The **security associations (SAs)** they negotiate specify what security options they will use.

The figure shows that the gateways implement an association in each direction. If security conditions require it, these SAs can use different security options. For example,

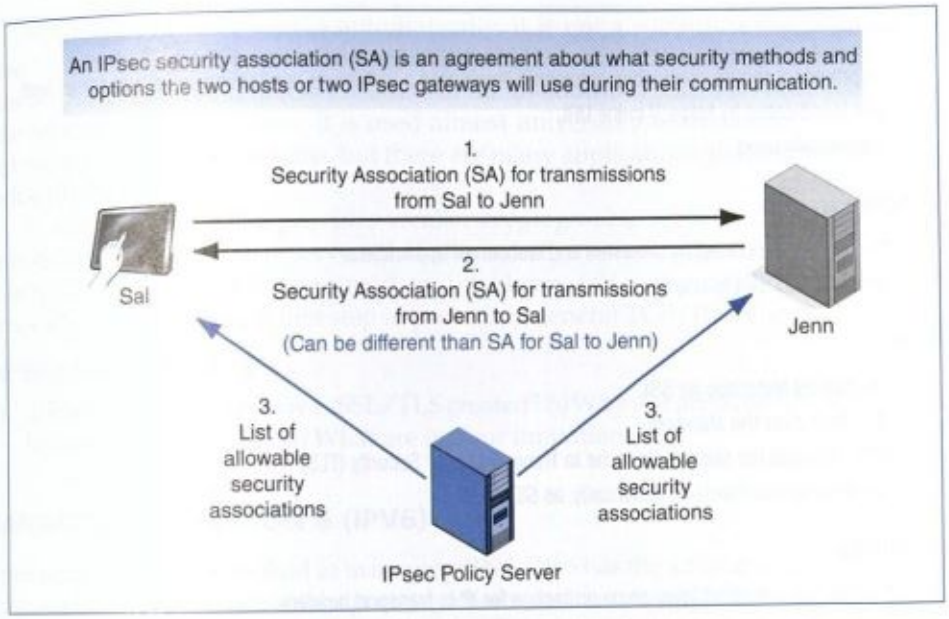


FIGURE 9-12 IPsec Security Associations (SAs) and IPsec Policy Servers

for a remote user, a remote access might have a stronger security association from the IPsec gateway to the user than from the user to the IPsec gateway

As we saw in Chapter 3, some security options are very strong. Others may not be. With IPsec, companies can use central **IPsec policy servers**. These servers specify what SA options are allowable for various gateway pairs and what options must not be used. Policy servers are especially important if a firm has many IPsec gateways.

Test Your Understanding

9. a) At what layer does IPsec operate? b) What layers does IPsec protect? c) Does IPsec protect these layers transparently? d) Describe IPsec tunnel mode. e) What is the main advantage of tunnel mode? f) What is the main disadvantage of tunnel mode? g) Describe IPsec transport mode. h) What is the main advantage of transport mode? i) What is the main disadvantage of transport mode? j) In which IPsec mode are clients and servers required to have digital certificates? k) Which IPsec mode does not require clients and servers to have digital certificates? l) Is IPsec used for remote-access VPNs, site-to-site VPNs, or both?
10. a) In IPsec, what are security associations (SAs)? b) Must security associations be the same in the two directions? c) Describe how IPsec gateways can be managed centrally to ensure that weak SAs are not permitted.

SSL/TLS VPNs

Although IPsec is an enormously powerful tool for creating highly secure VPNs, IPsec is expensive to implement. For many networked applications, companies build remote-access VPNs using the SSL/TLS security protocols. These protocols are far less expensive to implement.

Purpose

To provide a secure connection between a browser to a webserver applications on a webserver host
Use is indicated by https:// in the URL
Very widely used

Attraction

Universally supported by browsers and webserver applications
So no added cost to use it!

Origin

Created by Netscape as SSL
IETF took over the standard
IETF changed the standard's name to Transport Layer Security (TLS)
We refer to the standard, generically, as SSL/TLS

Limitations

Operates at transport layer so no protection for IP or transport headers
Limited to applications written to work with SSL/TLS: HTTP and e-mail, primarily
Cryptographically weaker than IPsec
No policy servers for centralized management

Overall

Good quality, cheap, and easy security
Only a first step in providing TCP/IP security

FIGURE 9-13 SSL/TLS VPNs (Study Figure)

You have personally used these protocols. In fact, you probably used them today. If you have ever purchased something online, your URL at some point began with https://. The *s* signified that the transaction was secure. It meant that your traffic was secured with the SSL/TLS protocols. In addition, if you use a webmail e-mail service, it is likely that all communication between you and the webserver from which you get your mail is secured by SSL/TLS.

The SSL protocol was developed by Netscape, which produced the first popular browser. Right from the start, the Netscape browser was capable of using SSL. Webservers capable of using SSL merely had to turn on their SSL functionality to be able to work securely with browsers. Soon, all browsers and webserver programs were capable of SSL security. With SSL on all browsers around the world, creating security for a webserver administrator is a simple task that requires brief configuration of the server and no configuration whatsoever on the browser itself. This automaticity makes SSL very inexpensive and simple to use. Many corporations routinely protect all webserver traffic with SSL.

Eventually, Netscape turned over the standardization of SSL to the IETF. The Task Force improved the standard and called its versions Transport Layer Security (TLS). We refer to the standards family generically as SSL/TLS.

Although SSL/TLS works automatically, it is not a substitute for IPsec. As the name Transport Layer Security suggests, SSL/TLS works at the transport layer. It provides no protection for IP packet headers at all. In addition, SSL/TLS only works with some networked applications. It is used almost universally with webservers, and it is used widely by e-mail programs, but there are many applications that are not written to work with SSL/TLS.

In addition, SSL/TLS provides weaker cryptographic security than IPsec. It also has nothing like IPsec policy servers that allows a firm to centrally manage its SSL/TLS security. Overall, SSL/TLS offers good quality, cheap, and easy security. However, most firms view it primarily as a first step in providing general TCP/IP security.

Test Your Understanding

11. a) For what application was SSL/TLS created? b) Why is it attractive? c) Distinguish between SSL and TLS. d) What are its four limitations?

MANAGING IP VERSION 6 (IPV6)

In this chapter, we have looked at managing IPv4. IPv6 has the same management needs. In this section, we will focus on important differences in managing IPv4 and IPv6.

Internet Layer Protocol Stacks

The internet layer sits between the transport layer and the data link layer. As Figure 9-14 illustrates, there has traditionally been a single internet layer process sitting between a host's transport layer process and its data link layer process. The internet layer process is called an **internet layer protocol stack** because it handles more than the internet protocol (IP). For example, it also handles the internet control message protocol (ICMP) and, in the case of IPv4, the address resolution protocol (ARP). It is usually called, simply, the *IP stack*.

Figure 9-14 shows that there was only a single IP stack on hosts originally—the **IPv4 stack**. The coming of IPv6 created two more alternatives.

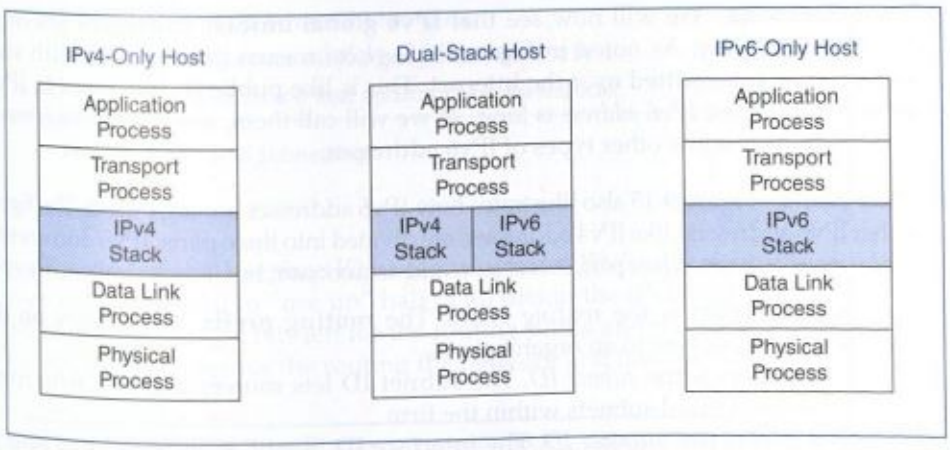


FIGURE 9-14 Internet Layer Protocol Stacks

- One is for hosts to have a single **IPv6 stack** instead of a single IPv4 stack.
- The other is to have a **dual-stack** host with both IPv4 and IPv6 stacks. This allows the host to transmit either IPv4 or IPv6 packets and to execute IPv4 or IPv6 internet layer protocols as needed.

The Internet Engineering Task Force expected that dual-stack implementation would become the norm. This would allow the gradual replacement of IPv4 by IPv6. However, the exhaustion of IPv4 addresses has created a growing number of hosts that have a single IPv6 stack and no IPv4 stack. In addition, although IPv6 was defined in the 1990s, many vendors still sell operating systems that have the IPv46 stack turned off and not trivially turned on, weak IPv6 stacks that cause problems if turned on, and sometimes, as in the case of Apple's Version 6 airport product released in January 2012, no IPv6 stack at all. As we will see in this section, these unexpected developments have caused problems for companies that wish to offer IPv6 service internally and externally.

Test Your Understanding

12. a) What does it mean for a host to have a dual stack for IP? b) Why is it desirable to have a dual stack? c) Why is having only an IPv6 stack problematic?

IPv6 Subnetting

Earlier in this chapter, we looked at IPv4 subnetting. Subnetting in IPv6 is similar, but 128-bit addresses change the situation considerably. Figure 9-15 summarizes some of the key changes.

IPV6 GLOBAL UNICAST ADDRESSES Earlier in this chapter, we looked at IPv4 addresses. These were really unicast addresses—addresses for packets going from one host to another. We saw that IPv4 unicast addresses have three parts—a host part, a subnet part, and a network part. Although the total length is always 32 bits, the lengths of the three parts are all variable.

These IPv4 addresses are normally public, meaning that they can be used on the Internet. In contrast, private IPv4 addresses can be used only within a corporate site or home network.

GLOBAL ADDRESSES We will now see that **IPv6 global unicast addresses** are organized in the same way. As noted in Figure 9-15, *global* means that packets with such addresses can be transmitted over the Internet. This is like public IP addresses in IPv4. The term *global unicast IPv6 address* is long, so we will call them, simply, *IPv6 addresses*. Module A discusses some other types of IPv6 addresses.

THE THREE PARTS Figure 9-15 also illustrates how IPv6 addresses are organized. The figure shows that IPv6 addresses, like IPv4 addresses, are divided into three parts. IPv6 documentation does not use the terms *host part*, *subnet part*, and *network part*, but it uses similar concepts.

- The network part is the *routing prefix*. The **routing prefix** lets routers on the Internet route packets to an organization.
- The subnet part is the *subnet ID*. The **subnet ID** lets routers within a firm route packets to individual subnets within the firm.
- The host part is the *Interface ID*. The **interface ID** identifies an individual host in the firm.

IPv6 Global Unicast Addresses

Like IPv4 public addresses

Terminology

IPv6 Address Part	Corresponding IPv4 Address Part	Length
Routing Prefix	Network Part	Variable
Subnet ID	Subnet Part	Variable
Interface ID	Host Part	64 bits
Total	32 bits	128 bits

Routing Prefix and Subnet ID

Total length is 64 bits

If the routing prefix is 20 bits, the subnet ID must be 44 bits long

A longer routing prefix means a smaller subnet ID and therefore fewer subnets

A shorter routing prefix means a larger subnet ID and therefore more subnets

Creating the 64-Bit Interface ID

MAC addresses are only 48 bits long

Too short for 64-bit interface IDs

The IEEE has defined a way of creating 64-bit extended unique identifiers (EUI-64s) from 48-bit MAC addresses

These can be used as interface IDs

Creating EUI-64s

1. Begin with the MAC in hexadecimal notation
2. Divide the 48 bits into two halves (24 bits each)
3. Insert ***fffe*** between the two halves
4. Write all three into four-hex groups separated by :s
5. Flip the second-least significant bit in the first octet

FIGURE 9-15 IPv6 Subnetting

The size of the Interface ID in global unicast IPv6 addresses is fixed at 64 bits. It may seem wasteful to "use up" half of all bits in the IPv6 addresses to designate a host. However, with 64 bits left for the routing prefix and the subnet ID, there are still 1.8×10^{19} possibilities for the routing the network and host parts.

The size of the Interface ID in global unicast IPv6 addresses is fixed at 64 bits.

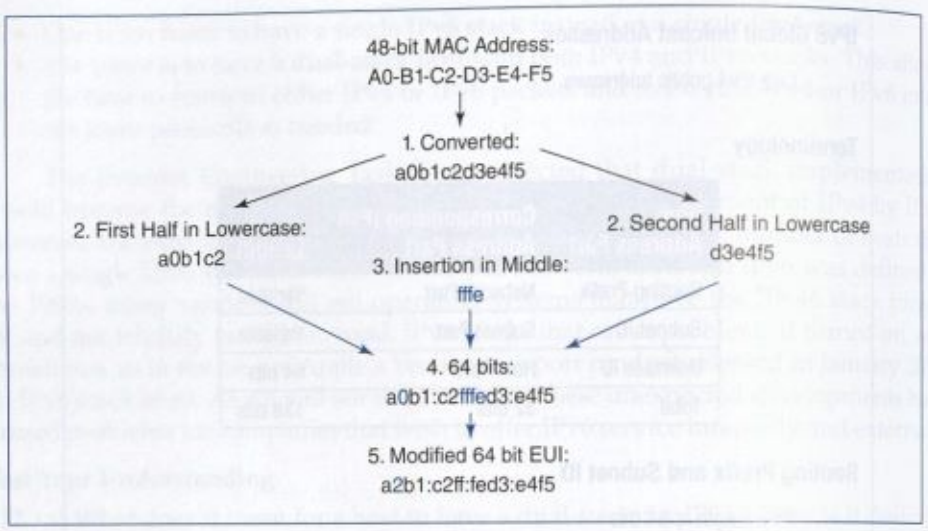


FIGURE 9-16 Converting a MAC address into an EUI-64

ROUTING PREFIX AND SUBNET ID Figure 9-15 indicates that the routing prefix and subnet ID are variable in length, although their total must be 64 bits because the interface ID has already consumed 64 of the 128 bits. To give an example, if the routing prefix is 20 bits, the subnet ID must be 44 bits. If an address registrar gives a firm a small routing prefix, then the company can have a large subnet ID and can therefore have many subnets. Smaller firms, needing fewer subnets, are given a larger routing prefix.

CREATING THE 64-BIT INTERFACE ID It would be nice to be able to use a host's link layer address as the interface ID. However, the most common type of link layer address is the MAC address, which is only 48 bits long. Fortunately, the IEEE 802 Committee has defined a way to create a 64-bit **Extended Unique Identifier (EUI-64)** from a 48-bit MAC address.[4] This EUI-64 can go into the interface ID field.

Creating an EUI-64 from a MAC address requires five steps, which are illustrated in Figure 9-16. These steps are straightforward, and there are good technical reasons for each step. However, without a lot of in-depth knowledge, which frankly is not worth learning for information systems professionals, these five steps can appear to be illogical and weird. Just think of them as a mystical protocol for joining an obscure secret society.

- First, if the MAC address is displayed in hexadecimal notation, the dashes are removed from the MAC address, and the letters are changed to lowercase. So A0-B1-C2-D3-E4-F5 becomes a0b1c2d3e4f5.
- Second, the 48 bits are divided into two half. Each half has 24 bits. In this case, the first half is a0b1c2 and the second half is d3e4f5.

[4]The IEEE has actually deprecated the term *MAC address* for the term *extended unique identifier (UI)*. More specifically, the traditional MAC address is called an EUI-48. The 64-bit version is called the EUI-64.

- Third, the hex symbol *fffe* is inserted between the two halves.[5] This gives a0b1c2fffed3e4f5. (The fffe is blue for easier reading in this example).
- Fourth, the first half, the new group, and the second half are written together and regrouped into four fields with four hex symbols apiece. These fields are separated by colons. This gives the result: a0b1:c2ff:fed3:e4f5. Notice that a colon separates the ff and the fe. Use this as a cross-check to make sure you have done things right.
- Fifth, the *second least-significant bit* (the second bit from the right end) in the first octet is inverted. For example, the MAC address in our example begins with A0. These two hex symbols constitute the first octet. In binary, they are 10100000. This must be changed to 10100010 by inverting the *second* least-significant bit.[6] This gives A2 instead of A0. So the final EUI-64 is a2b1:c2ff:fed3:e4f5.

There may be some fields that begin with one or more zeroes. It may be tempting to reduce them now. However, this should not be done until the rest of the IPv6 address is created, including the routing prefix and the interface ID.

Test Your Understanding

13. a) What field in an IPv6 global unicast address corresponds to the network part of a public IPv4 unicast address? b) What field in an IPv6 global unicast address corresponds to the subnet part of a public IPv4 unicast address? c) If the subnet ID is 16 bits long (as it often is), how long is the routing prefix? d) If you are a large company, do you want a large routing prefix or a small routing prefix?
14. a) What field in a global unicast IP address corresponds to the host part of a public unicast IPv4 address? b) How long is this field? c) What are these addresses called? d) Convert the following MAC address to an EUI-64 address: AA-00-00-FF-FF-00. e) Repeat for this MAC address: 9B-E5-33-21-FF-0D.

IPv6 Configuration

When a client host boots up, it needs an IP address to use as its own address. It also needs other configuration information, such as the IP address of its default router. A client with a dual IP stack needs configuration information for each stack.

DHCPv6 AUTOCONFIGURATION An IPv4 client uses a DHCP server to get an IPv4 address and other configuration information. IPv6 clients, in turn, can use DHCPv6 servers to obtain similar configuration information for the IPv6 stack.

STATELESS AUTOCONFIGURATION However, unlike IPv4 clients, IPv6 clients also have a second way to obtain an IPv6 address for themselves. This is **stateless autoconfiguration**. In stateless autoconfiguration, the client host creates an IP address by itself. No DHCP server is needed—only a router configured to support stateless autoconfiguration.

There are two phases in stateless autoconfiguration:

[5] It just is.
[6] See previous footnote.

Configuration

When a client boots up, it needs an IP address and other configuration information

A client with a dual IP stack needs configuration information for both

DHCPv6 Configuration

IPv4 clients request configuration parameters from DHCP servers

IPv6 clients can do this with DHCPv6 servers

Stateless Autoconfiguration

IPv6 defines another way to do client configuration for the IPv6 stack

The client configures itself, without using a DHCPv6 server

First, the client creases a link-local IPv6 address

Second, the client creates a global unicast IPv6 address

Creating the Link-Local IPv6 Addresses

Link-local IPv6 addresses can be used only within a single network (wireless or switched wired)

If the client does not need a global IP address, the autoconfiguration process can stop here

Creating the link-local address

- First create a 64-bit interface ID using the MAC address of the client
- Add a routing prefix 111 1110 10 followed by 56 bits of zeroes
- This is the link-local IP address: *fe80::x*, where *x* is the octets of the EUI-64

Testing the link-local address

- Another host may be using this address
- So the client uses the ICMPv6 neighbor discovery protocol to ask if any other host in the single network is using this address
- If none reply, the client may use this address within its single network

Creating the Global Unicast IPv6 Address

Needed for communication over the Internet

Begin with the link-local address

Keep the interface ID but get a new routing prefix and subnet ID

Client sends an ICMPv6 *router solicitation* message to the address FFF02::1

Routers respond with IPv6 *router advertisement* messages

The router advisor message may state that autoconfiguration is not allowed

If this is not the case, the message gives the routing prefix and subnet ID

The client now has a global unicast IPv6 address

Limits and Uses

More limited than traditional DHCP autoconfiguration

- At a minimum, router advertisement messages give only a routing prefix and subnet ID
- Of course, the packet gives the IPv6 address of the router, which becomes the default router

(continued)

FIGURE 9-17 IPv6 Configuration (Study Figure)

Uses

How can a client get other IPv6 configuration information?

If a client is dual-stack client, the IPv4 stack can obtain full configuration information, which the IPv6 stack can use

If the client is not a dual-stack client, it needs at least one more piece of configuration information—the IPv6 addresses of DNS servers

The IETF has extended router advertisement messages to provide the IPv6 addresses of DNS servers

However, this is only an option

Known security weaknesses

An attacker might create an address that does not use its proper EUI-64

An attacker may create an address that uses the EUI-64 of another host to impersonate it

Several operations can be used to create flooding denial-of-service attacks

IPv6 Address Renumbering

Stateless autoconfiguration may be used to renumber all IP addresses in a firm automatically, changing subnet IDs and even routing prefixes

FIGURE 9-17 Continued

- The first is to create a **link-local** IPv6 address, which can be used only within the client's single network (switched wired or wireless). If the client does not have to communicate with hosts outside this single network, the autoconfiguration process can stop here.
- The second is to create a global unicast IPv6 address. This second step requires information from a router. This step is necessary if the client wishes to communicate beyond its single network, even with hosts on different single networks within a firm.

CREATING A LINK-LOCAL UNICAST IPv6 ADDRESS To create a **link-local** IPv6 address, the client does not have to look outside itself. It creates an EUI-64 from its link address, as discussed earlier in this section. This becomes the final 64 bits of its link-local IPv6 address. For the first 64 bits, the client uses a string created specifically for link-local unicast addresses. The first 10 bits are *1111 1110 10*. The next 54 are *0*s. Therefore, the link local address is *fe80::EUI-64* after the 0s in the middle are taken out.

There is the danger, albeit slight, that another host on the network is already using this address. Therefore, the client should use the ICMPv6 **neighbor discovery protocol** to ask if any other host is using the link-local unicast IPv6 address it has created. If no host replies that it is using this address, the client may use this link-local unicast IP address to communicate with other hosts on its single network.

CREATING A GLOBAL UNICAST IPv6 ADDRESS If the client wishes to communicate outside its single network, it needs help from a router configured to provide this kind of help.

- The client transmits an ICMPv6 **router solicitation** message to the *FF02::1* multicast address. All routers should read this message.
- One or more routers will respond with an ICMPv6 **router advertisement** message.
- The client reads the router advertisement message to determine if it may use stateless autoconfiguration. (The advertisement message may prohbit this.)
- If stateless autoconfiguration is permitted, the router advertisement gives the client the routing prefix and subnet ID for the client's subnet. The client replaces the fe80:: link-local prefix with the routing prefix and subnet ID it has just received. The client now has an IPv6 global unicast address.

Now that the client has a global unicast IPv6 address, it may communicate with all hosts available on the Internet.

LIMIT AND USES Although stateless autoconfiguration reduces costs compared to traditional DHCP configuration, it is limited. Most importantly, it offers only very limited configuration information. At a minimum, it provides only two pieces of information. The first is a routing prefix plus subnet ID. The second is the IPv6 address of the router that sent it the router advertisement message. This becomes the IPv6 address of the client's default router.

Stateless autoconfiguration, without options, only provides the client with an IPv6 address and gives the client the IPv6 address of a default router.

How is the client to find DNS servers, network time protocol servers, and other servers it may need? In some cases, the client will *not need additional configuration parameters*. If the client is a dual-stack client, it can begin by doing DHCP configuration for its IPv4 stack. The IPv6 stack has access to this configuration information. In this case, stateless autoconfiguration of the IPv6 stack is fine.

Stateless autoconfiguration is especially attractive for nomadic environments that have many clients coming and going frequently. An example of this is a Wi-Fi hot spot. For some clients, basic IPv6 router advertisement messages will contain all the information they need.

Most, however, will also need another critical piece of configuration information—the IP addresses of DNS servers. Without this, clients cannot browse the Internet and do other things by host name. To address this concern, the IETF has created an option for including DNS server addresses in router advertisement messages. However, this is only an option. Many routers and clients do not implement it yet, and many never will.

In addition, it has known security issues. For instance, a host may decide not to create an EUI-64 based on its link layer address, in order to be anonymous. It may even use an EUI-64 that would allow it to impersonate another client. In addition, several of the interactions in stateless autoconfiguration are susceptible to flooding denial-of-service attacks. Stateless autoconfiguration will have to mature to address these security issues.

IPv6 ADDRESS RENUMBERING One other use of stateless autoconfiguration is bulk **IPv6 address renumbering**. With traditional IPv6, it is difficult to change the network part or subnet part of all IPv4 clients in a company. However, stateless autoconfiguration supports the changing of all IPv6 addresses in company in a (relatively) simple and rapid

way. Each router gives all clients it serves leases (agreements that include a deadline for using its IPv6 routing prefix and subnet ID). In address renumbering, all leases are created to expire at the same time. The IPv6 routers then change all leases, providing new routing information and subnet IDs in the process. There is also a mechanism for telling all routers to change routing prefixes and subnet IDs at the same time. This mechanism includes distributing different subnet IDs to each router.

Test Your Understanding

15. a) Can a client computer use DHCP to get IPv6 configuration information? Explain. b) What other option is available for IPv6 client configuration? c) What are the two phases in IPv6 stateless autoconfiguration? d) What is a link-local IP address? e) For a link-local address, what are the contents of the routing prefix, subnet ID, and interface ID? f) Why must a client use the neighbor discovery protocol after creating a link-local IPv6 address? g) For a global IP address, what are the contents of the routing prefix, subnet ID, and interface ID? h) In what ICMPv6 message are the routing prefix and subnet ID delivered? i) May the router advertisement message forbid the use of stateless autoconfiguration for creating a global IPv6 address?
16. a) At a minimum, what configuration information does a router advertisement message give a client? b) Why is this sufficient for dual-stack clients? c) For single-stack IPv6 clients, what additional piece of configuration information is almost certainly needed? d) How may this information be obtained? e) Is the mechanism for giving the IPv6 addresses of DNS servers mandatory or optional? f) What are the known security weaknesses of IPv6? g) Can stateless autoconfiguration be used to change all routing prefixes and subnet IDs in a firm?

Other IPv6 Standards

In order to make IPv6 work effectively, the Internet Engineering Task Force also had to upgrade a number of support standards. For example, it had to extend ICMP to ICMPv6 with new capabilities. To give an example of this, stateless autoconfiguration needs to use the router solicitation and the router advertisement messages, both of which are ICMPv6 message types.

Another major standard to require changing is DNS, although here the main change is minor. For each host name, a DNS server actually contains multiple records giving information about the particular host using that name.

- **DNS A Record**. The A record contains the IPv4 address for a target host. When your computer sends a DNS message to request the IPv4 address for a particular host name, the DNS server replies with information in the target host's A record.
- **DNS AAAA Record**. For IPv6 addresses, a new address field had to be added. IPv6 addresses are four times as long as IPv4 addresses, so the added record is called the AAAA record.

THE ADDRESS RESOLUTION PROTOCOL (ARP) In IPv4, the address resolution protocol (ARP) did not use IP packets. It had its own packet type. For IPv6, the functionality of ARP was subsumed into ICMPv6, into the **neighbor discovery protocol**, which defines two types of messages. Instead of sending an ARP request message, the sending

ICMPv6

Many new types were created for neighbor discovery, stateless autoconfiguration

Domain Name System (DNS)

The DNS information for a host is contained in several records

DNS A Record. The A record contains the IPv4 address for the target host

DNS AAAA Record. For IPv6 addresses, a new address record had to be added. IPv6 addresses are four times as long as IPv4 addresses, so the added record is called the AAAA record.

Address Resolution Protocol (ARP) Messages

In IPv6, handled by the ICMP neighbor discovery protocol, which has two message types

Neighbor solicitation messages ask host to respond

Neighbor advertisement messages give the host's data link address

There is no ARPv6

FIGURE 9-18 Other IPv6 Standards (Study Figure)

host transmits an ICMPv6 **neighbor solicitation** message. The host with the requested IPv6 address sends back an ICMPv6 **neighbor advertisement** message containing the requested data link layer address.

Test Your Understanding

17. a) Does ICMPv6 contain new ICMP message types? b) In the Domain Name System, distinguish between the information contained in the A and AAAA records for a host name. c) What standard replaces the Address Resolution Protocol in IPv6? d) What are the two types of messages in the neighbor discovery protocol? e) What does each contain?
18. a) I type in the host name of an IPv6 host. What does my computer do? I know the IPv6 address of a particular host. b) How can I find its data link layer address so that I can send it frames?

CONCLUSION

Synopsis

Chapter 8 dealt with TCP/IP concepts. This chapter focuses on TCP/IP management. The TCP/IP standards that dominate internetworking require a great deal of management attenuation, both initially and on an ongoing basis. The first step is to develop an IP subnet schema for the firm. This creates a basic trade-off between the number of subnets and the number of hosts per subnet. The firm also has to decide whether or not to use network address translation (NAT). NAT has several benefits, including added security and increasing the effective number of public IP addresses a firm has; but NAT causes problems for certain protocols.

In this chapter, we looked more closely at the Domain Name System (DNS). We saw that the system is a hierarchical system of named domains (collections of resources under the control of an organization). Corporations want second-level domain names, such as pearsonhighered.com. After they get one, they must maintain two or more DNS servers for their second-level domain. We also saw that if a local DNS server does not know the IP address for a host name, it contacts the authoritative DNS server for the domain in the IP address.

We looked in more depth at the Dynamic Host Configuration Protocol, focusing on the need to define scopes for each DHCP servers and to assign IP address groups in a way consistent with the DHCP server's scope.

We have seen the Simple Network Management Protocol (SNMP) repeatedly since we first saw it in Chapter 1. This chapter looked at SNMP operation in a bit more detail, focusing on the concept of objects and the types of objects specified in MIB schemas. We also saw RMON probes.

The Internet is attractive for WAN transmission because it has a very low cost per bit transmitted. However, companies are concerned about security on the Internet. To obtain better security, they use remote-access and site-to-site VPNs.

There are two main VPN protocols. IPsec offers the strongest security. It also offers the important choice between two modes of operation—transport mode and tunnel mode. Most importantly, IPsec offers central manageability.

SSL/TLS can be used for remote-access VPNs. SSL/TLS is attractive because all browsers know how to create a secure SSL/TLS connection with host computers. This means that there is no need to add anything to the client computer. However, there are limitations on the services that SSL/TLS can provide easily.

We ended the chapter with a long discussion on the management of IPv6. Managing IPv6 is similar to managing IPv4, but it is not the same. We began with a discussion of single-stack IPv4-only hosts, single-stack IPv6-only hosts, and dual-stack IPv4/IPv6 hosts. Originally, the IETF believed that dual-stack machines would make the introduction of IPv6 painless. However, implementing IPv6 on dual-stack machines and managing IPv6 traffic proved to be expensive. Now that we have run out of IPv4 addresses, however, single-stack IPv6 hosts are finally driving the introduction of IPv6.

In IPv4, addresses have three parts: network, subnet, and host. In IPv6 global unicast addresses, the comparable parts are called the routing prefix, the subnet ID, and the interface ID. The interface ID is always 64 bits long. It is created from the host's MAC address by a somewhat complex process that we reviewed. This process results in a 64-bit extended unique identifier (EUI-64) that is used as the interface ID. The company is assigned a routing prefix. This sets the size of its subnet ID and determines how many subnets it can have.

For client configuration, DHCPv6 exists. However, IPv6 permits another type of configuration, stateless autoconfiguration, in which the host does its own configuration, without using a DHCPv6 server. First, the host creates a link-local IPv6 address that can be used only within a single network. Second, with the help of an ICMPv6 router advertisement message, it creates a global unicast IPv6 address that can be used on the Internet. For dual-stack devices, the IPv4 stack can obtain configuration information from the DHCP server, so stateless autoconfiguration on the IPv6 stack, which provides only an address for the client host and the IPv6 address of a default router, is sufficient. For single-stack IPv6 computers, the router advertisement message has

an optional ability to give the IPv6 addresses of DNS servers. An important feature of stateless autoconfiguration is that it can be used to renumber all hosts in a corporate network.

IPv6 required the extension of existing helper standards. ICMPv6 introduces many new message types, and DHCPv6 can be used for IPv6 configuration. The major change to DNS is the introduction of an AAAA record for host names. This record contains the IPv6 address of the named host. (IPv4 addresses are contained in traditional A records.)

END-OF-CHAPTER QUESTIONS

Thought Questions

1. Both DNS servers and DHCP servers send your client PC an IP address. Distinguish between these two addresses.
2. Assume that an average SNMP response message is 100 bytes long. Assume that a manager sends 40 SNMP *Get* commands each second. a) What percentage of a 100 Mbps LAN link's capacity would the resulting response traffic represent? b) What percentage of a 128 kbps WAN link would the response messages represent? c) What can you conclude from your answers to these questions?
3. A firm is assigned the network part 128.171. It selects an 8-bit subnet part. a) Draw the bits for the four octets of the IP address of the first host on the first subnet. (Hint: Use Windows Calculator.) b) Convert this answer into dotted decimal notation. c) Draw the bits for the second host on the third subnet. (In binary, 2 is 10, while 3 is 11.) d) Convert this into dotted decimal notation. e) Draw the bits for the last host on the third subnet. f) Convert this answer into dotted decimal notation.
4. A firm is assigned the network part 128.171. It selects a 10-bit subnet part. a) Draw the bits for the four octets of the IP address of the first host on the first subnet. (Hint: Use Windows Calculator.) b) Convert this answer into dotted decimal notation. c) Draw the bits for the second host on the third subnet. (In binary, 2 is 10, while 3 is 11.) d) Convert this into dotted decimal notation. e) Draw the bits for the last host on the third subnet. f) Convert this answer into dotted decimal notation.

Troubleshooting Question

1. In your browser, you enter the URL of a website you use daily. After some delay, you receive a DNS error message that the host does not exist. a) What may have happened? Explain your *reasoning. Again, do NOT just come up with one or two possible explanations.* b) How would you logically disconfirm or test each possibility?

Perspective Questions

1. What was the most surprising thing to you about the material in this chapter?
2. What was the most difficult thing for you in the chapter?

10 WIDE AREA NETWORKS

LEARNING OBJECTIVES

By the end of this chapter you should be able to:

- Contrast LANs and WANs in terms of technology diversity, economics, speed, and need for optimization.
- Contrast the technologies of the business and residential local loops of telephone companies. Contrast these technologies with UTP wiring within buildings.
- Distinguish between access lines and leased lines. Discuss the main lower-speed leased lines and bonding. Describe the standards used in leased lines above 50 Mbps.
- Explain the technology used in DSL lines. Explain the differences between residential and business DSL lines.
- Explain the technology used in cable modem service.
- Describe the technologies of leased line networks and public switched data networks. Discuss metropolitan area Ethernet and its attractions. If you read the box, "Virtual Circuits," explain the problem they address and how they address it.
- Explain why it is attractive for companies to use the Internet for WAN service and what issues concern them in using the Internet. Describe how companies can mitigate security concerns. Describe how companies can mitigate performance issues.
- Explain why cellular systems use cells, distinguish between handoffs and roaming in 802.11 and cellular systems. Explain the generations of cellular technology to date. Explain the standards situation today and the direction in which it is moving. Explain why individual throughput is usually far lower than rated speeds. Describe how Wi-Fi and cellular technology are converging.

LANs AND WANs (AND MANs)

One of the most fundamental distinctions in networking is the one between local area networks (LANs) and wide area networks (WANs). Figure 10-1 shows how these two types of networks differ. We will also see how they compare to intermediate-distance networks called metropolitan area networks (MANs).

LANs versus MANs and WANs

ON AND OFF THE CUSTOMER PREMISES Some authors base the difference between LANs and WANs on physical distance. For instance, some say that the dividing line between LANs and WANs is one mile or one kilometer. However, the real distinction appears to be that **local area networks (LANs)** exist within a company's site, while **wide area networks (WANs)** connect different sites within an organization or between organizations.

Category	Local Area Network	Metropolitan Area Network	Wide Area Network
Abbreviation	LAN	MAN	WAN
Service Area	*On customer premises* (home, apartment, office, building, campus, etc.)	*Between sites* in a metropolitan area (city and its suburbs) A Type of WAN	*Between sites* in a region, a country, or around the world.
Implementation	Self	Carrier	Carrier
Ability to Choose Technology	High	Low	Low
Who manages the network?	Self	Carrier	Carrier
Price	Highly related to cost	Based on strategy. Highly unpredictable.	Based on strategy. Highly unpredictable.
Cost per Bit Transmitted	Low	Medium	High
Therefore Typical Transmission Speed	100 Mbps to 1 Gbps or more	10 to 100 Mbps	1 to 50 Mbps
Can Use Switched Technology?	Yes	Yes	Yes
Can Use Routed Technology?	Yes	Yes	Yes

FIGURE 10-1 LANs, MANs, and WANs

Local area networks (LANs) exist within a company's site, while wide area networks (WANs) connect different sites within an organization or between organizations.

For LANs, then, the company owns the property and can do anything it wants. It can choose any LAN technology it wishes, and it can implement it any way it wishes.

There is no such freedom for WANs. A company cannot legally lay wires between two of its sites. (Consider how your neighbors would feel if you started laying wires across their yards.) The government gives certain companies called **carriers**[1] permission (**rights of way**) to lay wires in public areas and offer service to customers. In return, carriers are subject to government regulation.

When you deal with carriers, you can only get the services they offer, and you must pay their prices. Although there may be multiple carriers in an area, the total number of service choices is likely to be quite limited.

On the positive side, you do not need to hire and maintain a large staff to deal with WANs because carriers handle nearly all of the details. In contrast, if you install a LAN, you also have to maintain it. As the old saying goes, anything you own ends up owning you.

[1]Carriers were originally called *common carriers*. The name reflected the fact that these carriers were required by law to provide service to anyone or any organization requesting services. Regulation was originally instituted in the railroad industry because many companies that owned railroads also owned other companies and refused to provide services to competitors of these other companies.

ECONOMICS Another fundamental difference between LANs and WANs stems from economics. You know that if you place a long-distance call, this will cost more than a local call. An international call will cost even more. As distance increases, the price of transmission increases. The cost per bit transmitted therefore is higher in WANs than in LANs.

You know from basic economics that as unit price increases, fewer units are demanded. Or, in normal English, when the price for an item increases, you usually buy less of it. Consequently, companies tend to purchase lower-speed WAN links than LAN links. Typically, LANs bring 100 Mbps to 1 Gbps to each desktop. WAN speeds more typically vary from 256 kbps to about 50 Mbps.

In addition, companies spend more time optimizing their expensive WAN traffic than their relatively inexpensive LAN traffic. For example, companies may be somewhat tolerant of looking at YouTube videos on LANs, but they usually clamp down on this type of information on their WAN links. They also tend to compress data before sending across a WAN so that it can be handled with a lower-capacity WAN link.

Another aspect of economics is pricing. For LANs, you have a good idea of what installing and using a wired or wireless LAN will cost you. In carrier WANs, however, the price of services is only somewhat related to costs. Carriers change their prices strategically, for example, to encourage users to switch from one service to another. Consequently, price changes for WANs are less predictable that they are for customer-owned LAN technology.

TECHNOLOGIES Another difference between LANs and WANs is that LAN technology has largely settled on two related families of standards—Ethernet (802.3) for wired LANs and Wi-Fi (802.11) for wireless LANs. As we saw in Chapter 6, 802.11 WLANs are primarily used today to extend corporate Ethernet wired LANs to mobile devices.

The technological situation is more complex in wide area networking. Multiple technologies are used, including leased line data networks, public switched data networks, and wireless networks. Within these categories are multiple options. Furthermore, WAN technologies are at different stages in their life cycles, with some increasing rapidly in use and others declining.

Test Your Understanding

1. a) Distinguish between LANs and WANs. b) What are rights of way? c) What are carriers? d) Why do you have more flexibility with LAN service than with WAN service? Why?
2. a) Why are typical WAN speeds slower than typical LAN speeds? Give a clear and complete argument. b) Why are future WAN prices difficult to predict? c) Compare the diversity of technologies in LANs and WANs.

Other Aspects of WANs

METROPOLITAN AREA NETWORKS (MANs) All WANs connect sites between customer premises and cost more per bit transmitted than LANs. However, WANs differ considerably in the distances they span. Some are international and others span single nations. At the small end, some WANs are **metropolitan area networks (MANs)**, which connect sites in a city and its suburbs.

Technology	LAN	WAN
Can be a single switched or wireless network?	Yes	Yes
Can be an internet?	Yes	Yes

FIGURE 10-2 Single Networks versus Internets

Although MANs are WANs, their relatively short distance span means that the cost per bit transmitted is lower than it is in national and international WANs. Consequently, typical transmission speeds are faster. If you have a smartphone or tablet with 3G or 4G cellular access, then you already use a MAN. Cellular networks almost always span a single MAN or even a single city. However, we will see that wired MANs are important for corporations because site-to-site traffic is large and is more efficiently transmitted over wires.

SINGLE NETWORKS VERSUS INTERNETS Some people think that LANs are single networks, while WANs are internets. However, as Figure 10-2 shows, that is not the case. Small LANs usually will be single networks, but a larger LAN, such as one on a university campus, is likely to be a local internet.

For WANs, there can also be single networks or internets. Of course, the global Internet is a WAN, and we will see that many companies use it extensively for data transmission among their premises. We will also see that companies also use wide area single switched networks. These are large networks, but they are still switched single networks.

Test Your Understanding

3. a) Why do MANs have higher typical speeds than broader-scope WANs? b) Are LANs single networks or internets? c) Are WANs single networks or internets? d) Is the Internet a WAN?

The Three Basic WAN Components

Figure 10-3 shows that there are three basic components to wide area networks:

- First comes the customer premises with the **customer premises equipment (CPE)** needed to connect to the WAN. With mobile devices, your customer premises is wherever you are, and your mobile device is your customer premises equipment. For connecting corporate sites to wired access lines, the customer premises equipment is likely to be a border router.
- **Access links** connect the customer premises to the network core of the WAN. We will focus on wired access links because they are so prevalent. Later in the chapter, we will look at wireless access links.
- The **network core** connects access links to other access links. Again, we show it as a cloud because customers do not have to understand how it works in detail. The carrier takes care of the network core. Of course, as an IT professional, you have to understand what happens inside the cloud, and we will spend time looking at network core technologies.

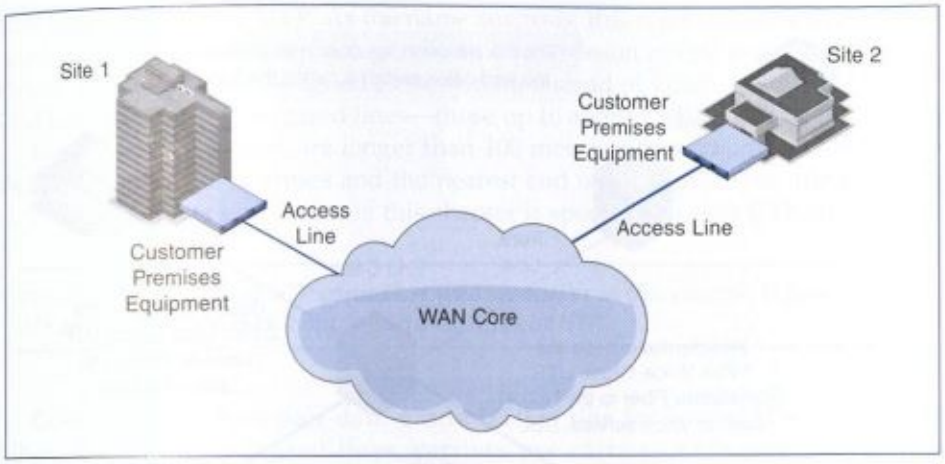


FIGURE 10-3 Components of a Wide Area Network (WAN)

Test Your Understanding

4. a) List the three basic components of wide area networks. b) Are access links wired or wireless? c) What is CPE?

WIRED ACCESS LINKS

We will begin looking at the technology of WANs with wired access links. Although wireless access is common for consumer products, wired access still dominates for corporate and residential access. There are two dominant technologies for access links: public switched telephone network access links and cable modem service. The latter is primarily available within the United States. Later in this chapter, we will look at wireless access links in mobile telephone systems.

Public Switched Telephone Network (PSTN) Access Lines

The traditional wired telephone system is officially the **public switched telephone network (PSTN)**. Although the PSTN was created for voice communication, its lines can carry data as well, and both corporations and private homes use these lines for WANs access.

THE BUSINESS LOCAL LOOP The access link between the customer premises and the nearest telephone company switch (called the end office switch) is called the **local loop**. Figure 10-4 shows the four main technologies that dominate the PSTN local loop.

Figure 10-5 looks at these technologies in more depth. For perspective, it also compares local loop twisted pair wiring to internal 4-pair UTP, which we saw in Chapter 5.

Two-Pair Data-Grade UTP Two of these technologies are used to provide leased lines to business. One of these is a type of UTP wiring we have not discussed before.