Corporate Computer Security, 4th Edition

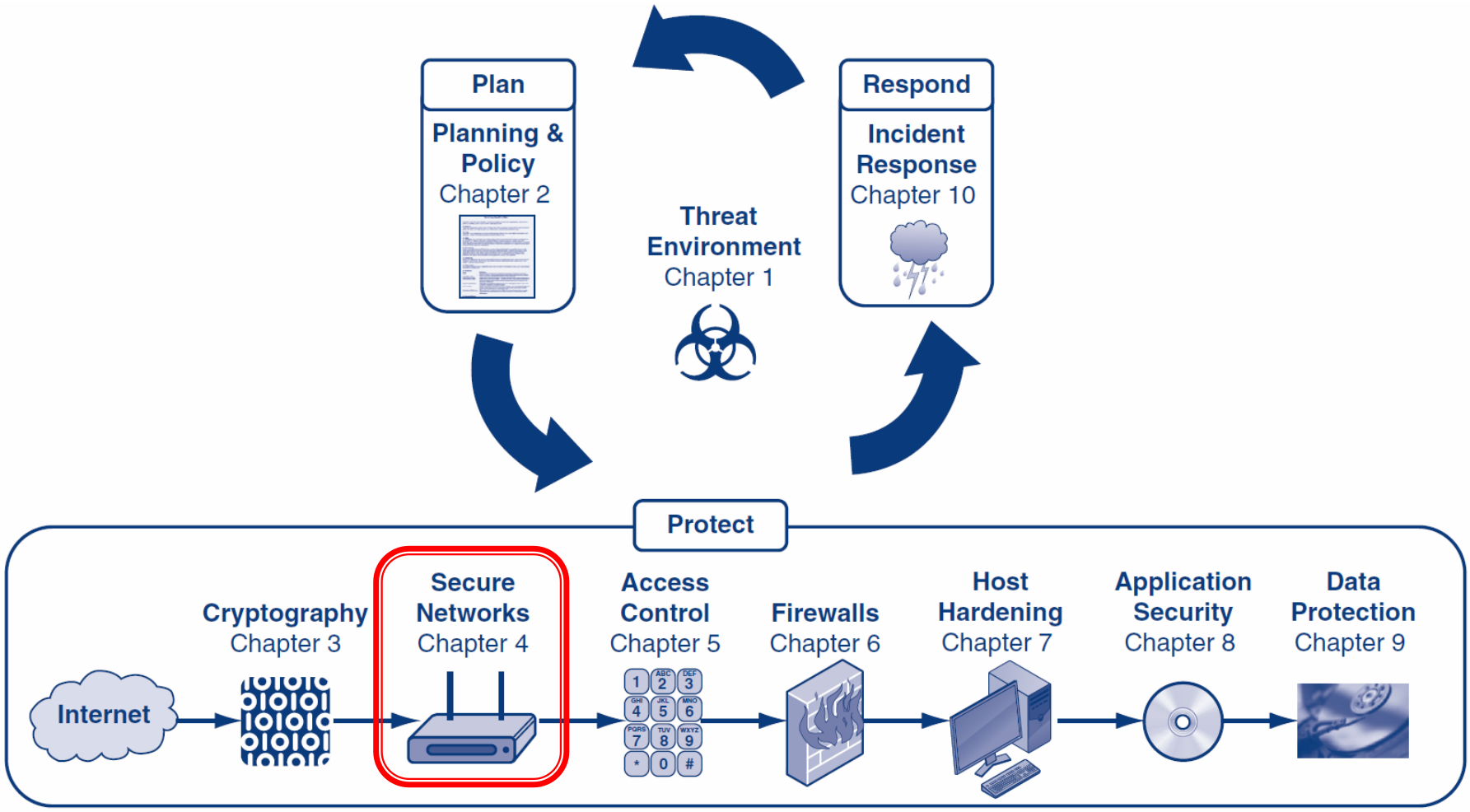
Randall J. Boyle & Raymond R. Panko

Security Networks

Chapter 4

Learning Objectives

- Describe the goals of creating secure networks.
- Explain how denial-of-service (DoS) attacks work.
- Explain how ARP poisoning works.
- Know why access controls are important for networks.
- Explain how to secure Ethernet networks.
- Describe wireless (WLAN) security standards.
- Describe potential attacks against wireless networks.



Orientation

- Chapter 3 looked at how cryptography can protect data being sent across networks
- Chapter 4 looks at how networks themselves are attacked
- We will look at how attackers can gain unauthorized access to networks
- We will also look at how attackers can alter the normal operation of a network
- We will look at both wired (LAN) and wireless (WLAN) networks

What's Next?

- 4.1 Introduction
- 4.2 Denial-of-Service (DoS) Attacks
- 4.3 ARP Poisoning
- 4.4 Access Control for Networks
- 4.5 Ethernet Security
- 4.6 Wireless Security

4.1: Threats to Secure Networks

- Cryptography provides confidentiality, authenticity, and message integrity
- Modern Networks have additional vulnerabilities
  - The *means* of delivering the messages could be stopped, slowed, or altered
  - The *route* the messages took could be altered
  - Messages could be *redirected* to false recipients
  - Attackers could gain *access* to communication channels that were previously considered closed and confidential

4.1: Creating Secure Networks

Goals of Creating Secure Networks

1. Availability—users have access to information services and network resources
2. Confidentiality—prevent unauthorized users from gaining information about the network
3. Functionality—preventing attackers from altering the capabilities or normal operation of the network
4. Access control—keep attackers or unauthorized employees from accessing internal resources

4.1: Death of the Perimeter

- The “castle” model
  - Good guys on the inside, attackers on the outside, and a well-guarded point of entry
- Death of the Perimeter
  - It is impractical, if not impossible, to force all information in an organization through a single point in the network
  - New means of attacking networks (e.g., smart phones) are constantly emerging
  - Line between “good guys” and “bad guys” has become blurred

4.1: Death of the Perimeter

- The “city” model
  - No distinct perimeter, and there are multiple ways of entering the network
  - Like a real city, who you are will determine which buildings you will be able to access
  - Greater need for:
    - Internal intrusion detection
    - Virtual LANs
    - Central authentication servers
    - Encrypted internal traffic

What's Next?

- 4.1 Introduction
- 4.2 Denial-of-Service (DoS) Attacks
- 4.3 ARP Poisoning
- 4.4 Access Control for Networks
- 4.5 Ethernet Security
- 4.6 Wireless Security

4.2: Denial of Service (DoS) Attacks

- What is a DoS attack?
  - An attempt to make a server or network unavailable to legitimate users by flooding it with attack packets
- What is NOT a DoS attack?
  - Faulty coding that causes a system to fail
  - Referrals from large websites that overwhelm smaller websites

4.2: Goals of DoS Attacks

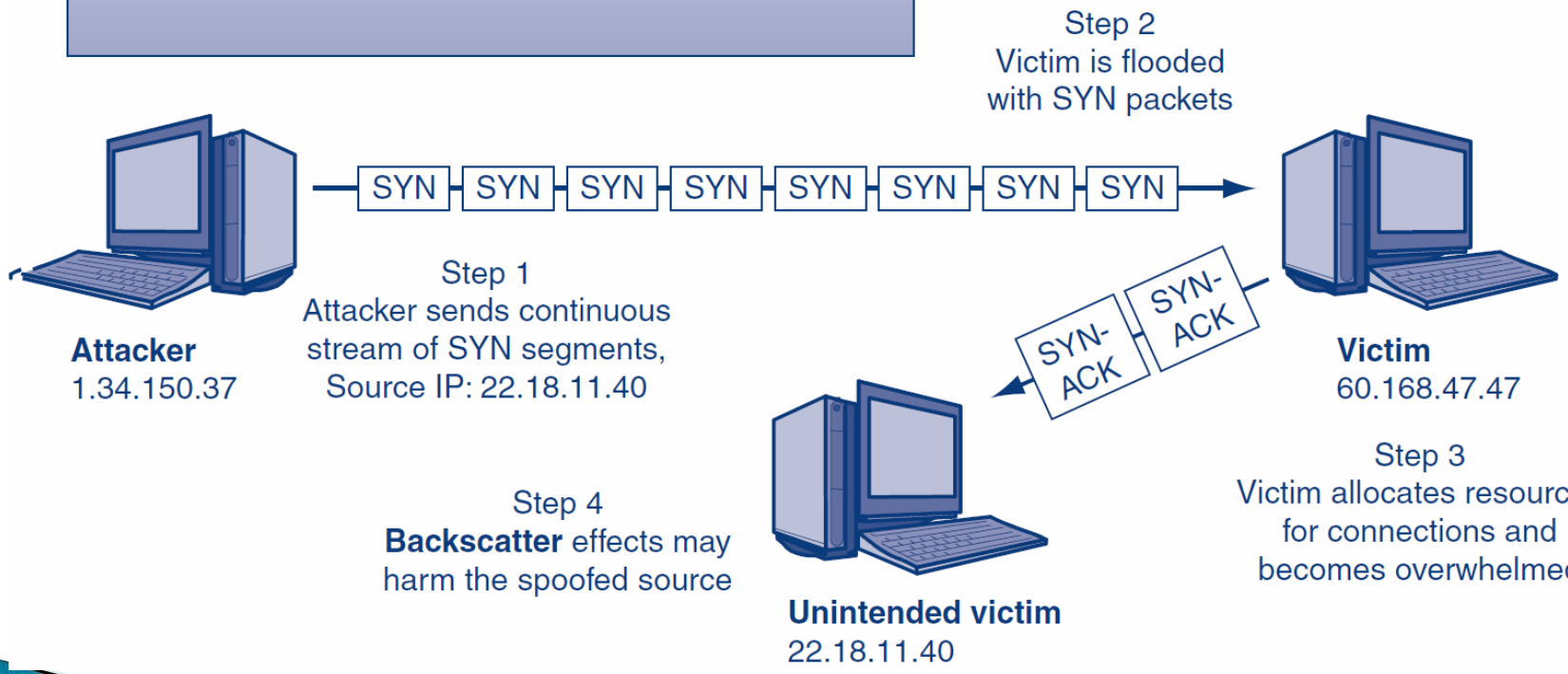
- Ultimate goal of DoS attacks is to cause harm
  - Harm includes: losses related to online sales, industry reputation, employee productivity, customer loyalty, etc.
- The two primary means of causing harm via DoS attacks include:
  1. Stopping critical services
  2. Slowly degrading services

4.2: Methods of DoS Attacks

- Direct DoS Attack
  - An attacker tries to flood a victim with a stream of packets directly from the attacker's computer
- Indirect DoS Attack
  - The attacker's IP address is **spoofed** (i.e., faked) and the attack appears to come from another computer

4.2: SYN Flood DoS Attack

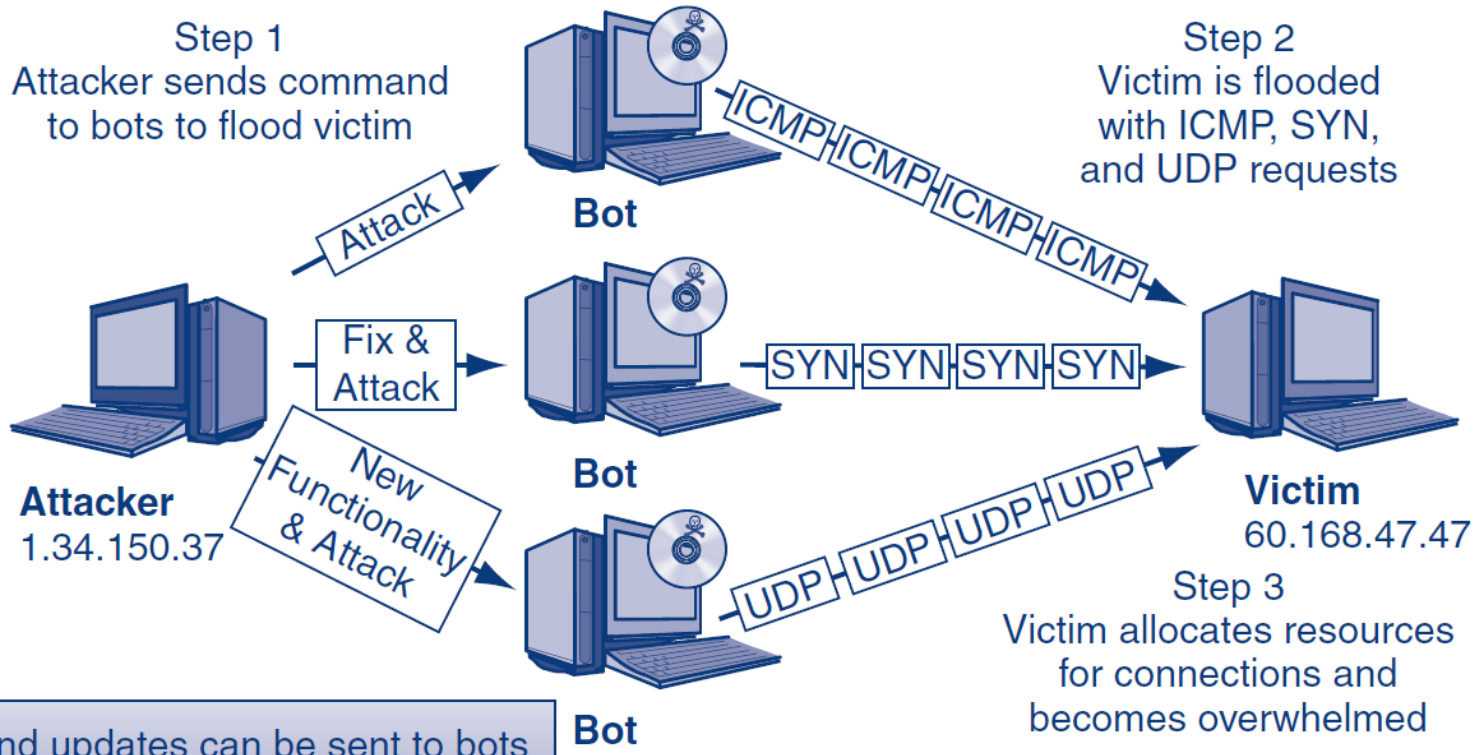
Attacker's IP address may be known or spoofed
Attacker cannot see SYN-ACK responses if the source IP address is spoofed
Attacker must have *more resources* than victim
Victim's *network* is also clogged with SYN traffic
Backscatter effects from victim can crash bots too



4.2: Intermediaries (Bots)

- **Bots**
  - Updatable attack programs
  - Botmaster can update the software to change the type of attack the bot can perform
    - May sell or lease the botnet to other criminals
  - Botmaster can update the bot to fix bugs
- Botmaster can control bots via a handler
  - Handlers are an additional layer of compromised hosts who are used to manage large groups of bots

4.2: Fixing and Updating Bots



Fixes and updates can be sent to bots
New **functionality** can be implemented

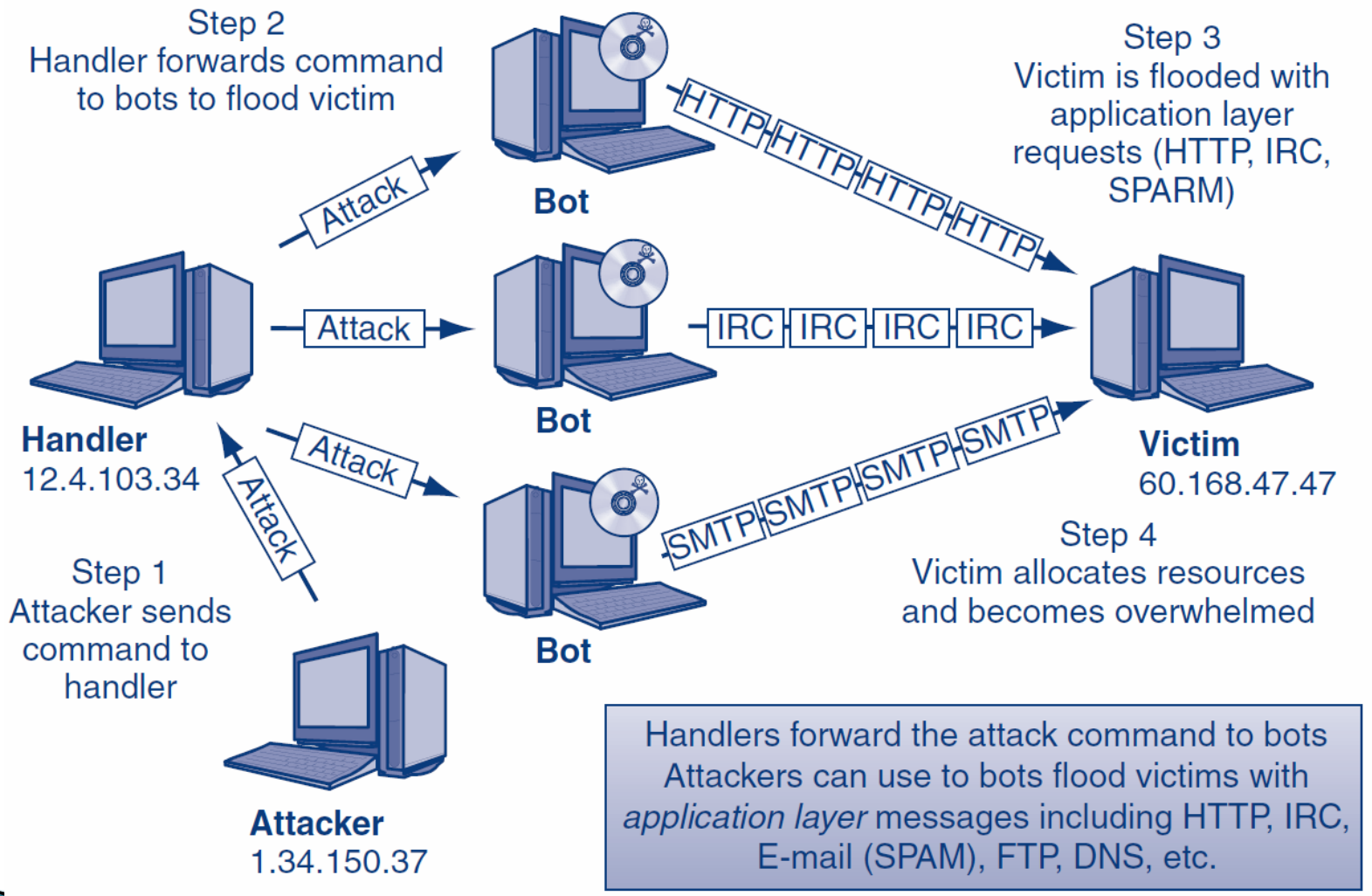
Attacker doesn't directly attack the victim
Attackers can use many bots to flood victims with different requests including ICMP (echo), SYN, UDP, etc.

4.2: Types of DoS Packets Sent

- Types of packets sent:

	Name	Description
TCP	Transmission Control Protocol	Guarantees delivery of packets over the Internet
SYN	Synchronize	First part of a three-way TCP handshake to make a network connection
SYN-ACK	Synchronize-Acknowledge	Second part of a three-way TCP handshake sent in response to a SYN
ICMP	Internet Control Message Protocol	Supervisory protocol used to send error messages between computers
HTTP	Hypertext Transfer Protocol	Protocol for sending data over the Web

4.2: DDoS Attack

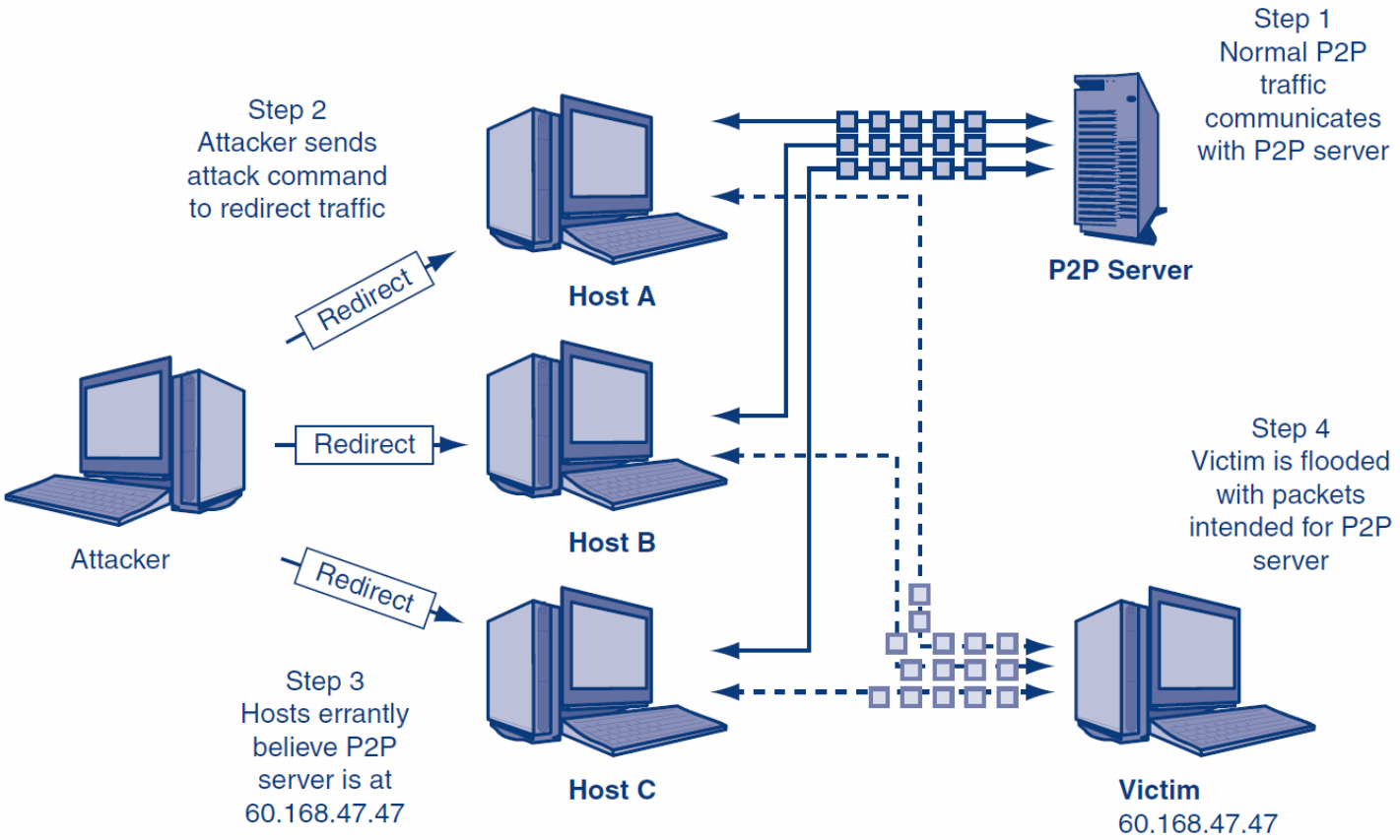


Handlers forward the attack command to bots Attackers can use to bots flood victims with *application layer* messages including HTTP, IRC, E-mail (SPAM), FTP, DNS, etc.

4.2: P2P DoS Attacks

- **Peer-to-peer (P2P) redirect DoS attack**
  - Uses many hosts to overwhelm a victim using normal P2P traffic
  - Attacker doesn't have to control the hosts, just redirect their *legitimate* P2P traffic

4.2: Peer-to-Peer Redirect Attack

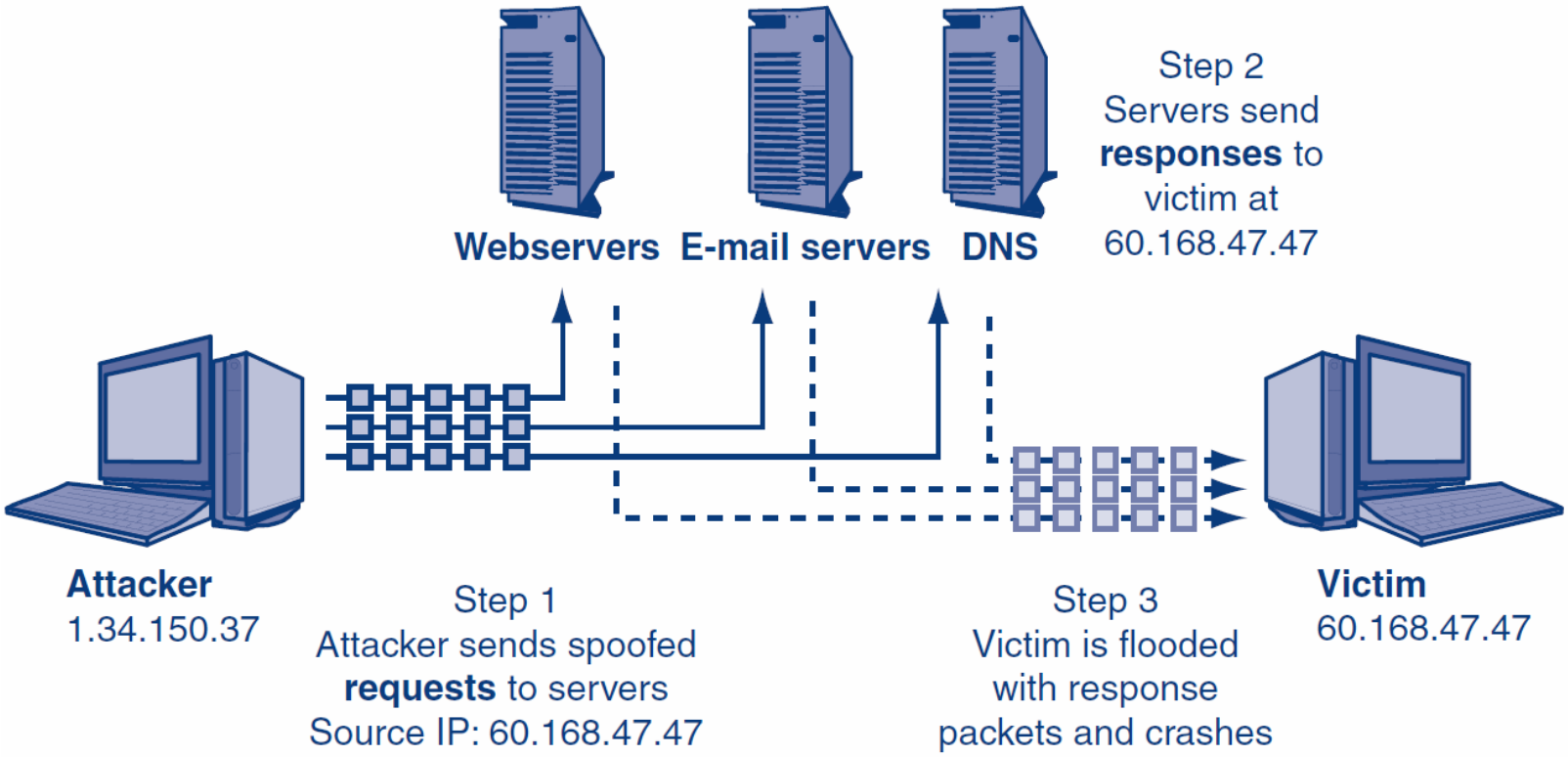


P2P networks have *many* hosts
Attacker doesn't control the hosts
Attacker redirects legitimate traffic to the victim
Victim can't block all traffic from hosts

4.2: Reflected DoS Attacks

- **Reflected DoS attack**
  - Responses from legitimate services flood a victim
  - The attacker sends *spoofed* requests to existing legitimate servers (Step 1)
  - Servers then send all responses to the victim (Step 2)
  - There is no redirection of traffic

4.2: Reflected DRDoS Attack

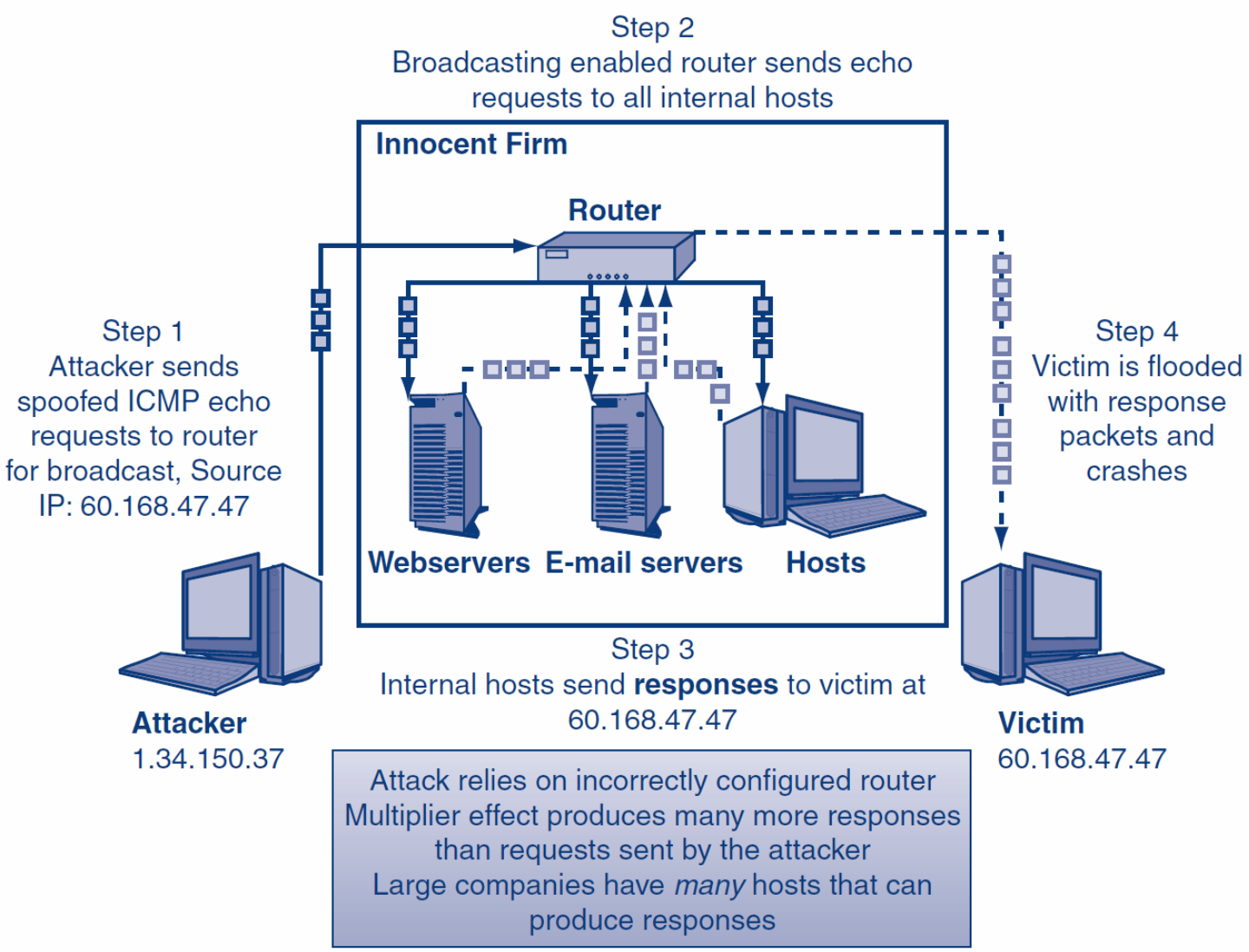


Attack appears to come from legitimate servers
Blocking legitimate servers also harms victim
Servers have the capacity to handle the attack

4.2: Reflected DoS Attacks

- Smurf Flood
  - The attacker sends a *spoofed* ICMP echo request to an *incorrectly* configured network device (router)
  - Broadcasting enabled to all internal hosts
  - The network device forwards the echo request to *all* internal hosts (multiplier effect)

4.2: Smurf Flood



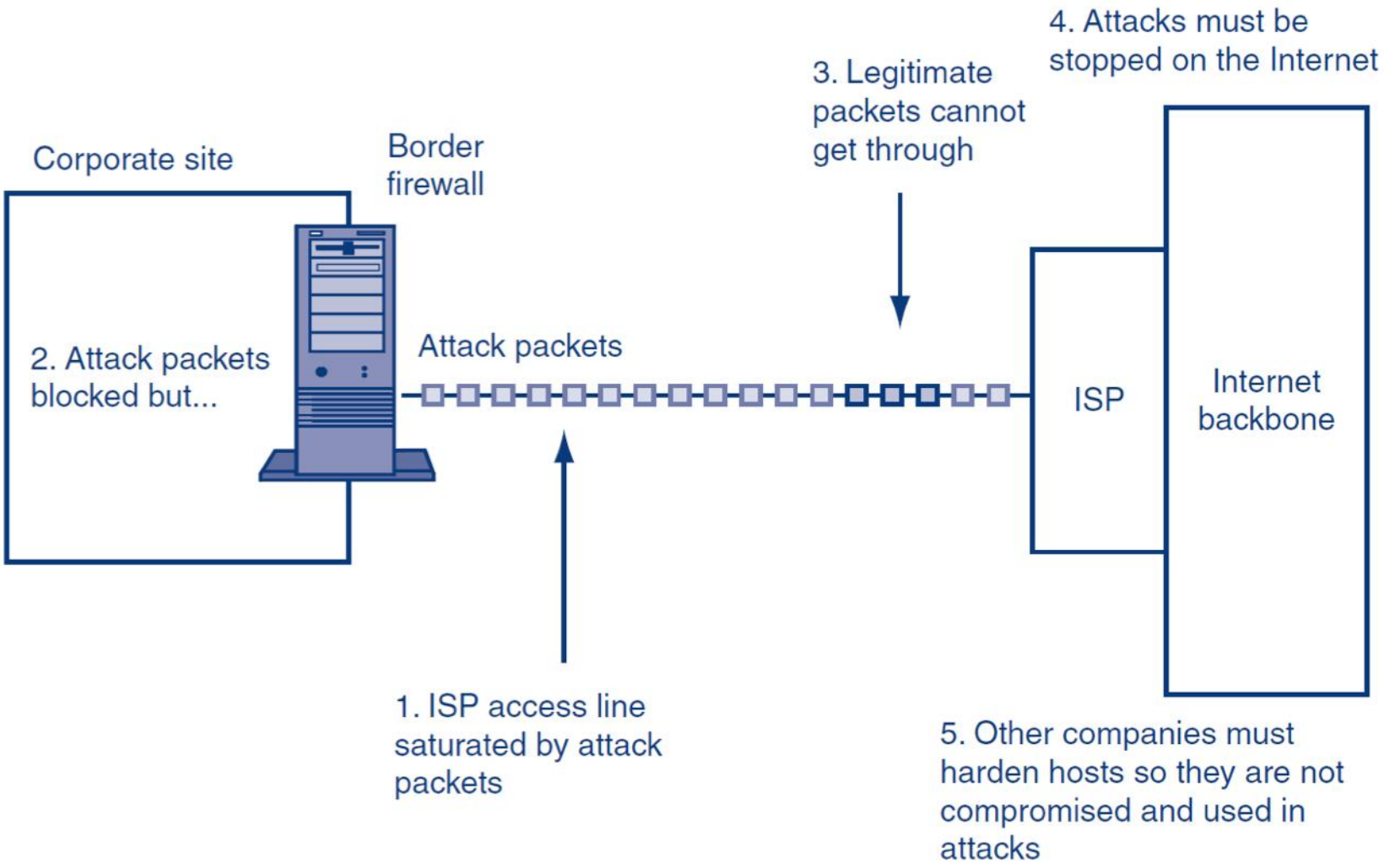
4.2: Defending Against DoS Attacks

- Black holing
  - Drop all IP packets from an attacker
  - Not a good long-term strategy because attackers can quickly change source IP addresses
  - An attacker may knowingly try to get a trusted corporate partner black holed

4.2: Defending Against DoS Attacks

- Validating the handshake
  - Whenever a SYN segment arrives, the firewall itself sends back a SYN/ACK segment, without passing the SYN segment on to the target server (false opening)
  - When the firewall gets a legitimate ACK back, the firewall sends the original SYN segment on to the intended server
- Rate limiting
  - Used to reduce a certain type of traffic to a reasonable amount
  - Can frustrate attackers and legitimate users

4.2: Stopping DoS Attacks



What's Next?

- 4.1 Introduction
- 4.2 Denial-of-Service (DoS) Attacks
- 4.3 ARP Poisoning
- 4.4 Access Control for Networks
- 4.5 Ethernet Security
- 4.6 Wireless Security

4.3: ARP Poisoning

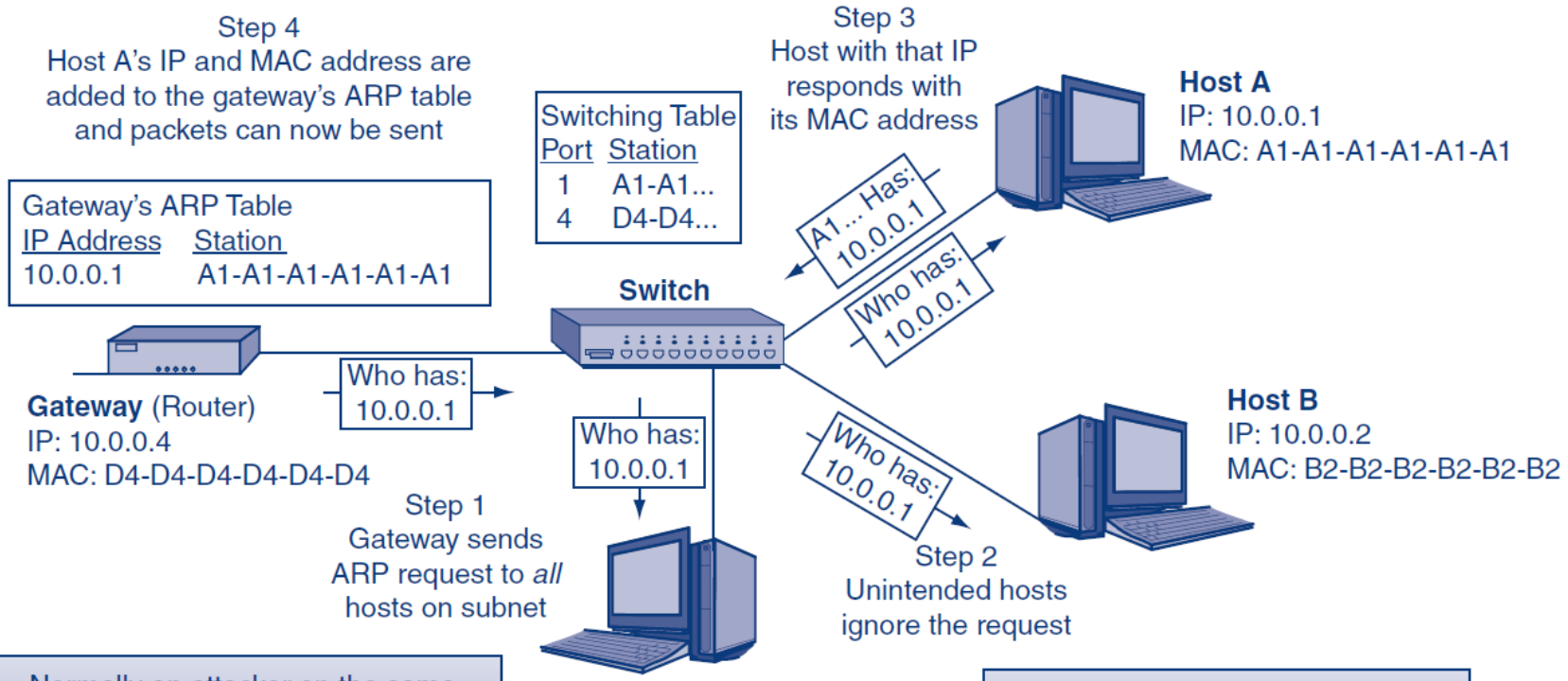
- ARP Poisoning
  - Network attack that manipulates host ARP tables to reroute local-area network (LAN) traffic
  - Possible man-in-the-middle attack
  - Requires an attacker to have a computer on the local network
  - An attack on both the *functionality* and *confidentiality* of a network

4.3: ARP Poisoning

- **Address Resolution Protocol (ARP)**
  - Used to resolve 32-bit IP addresses (e.g., 55.91.56.21) into 48-bit local MAC addresses (e.g., 01-1C-23-0E-1D-41)
  - ARP tables store resolved addresses (below)

Internet Address	Physical Address	Type
55.91.74.11	f8-66-f2-75-58-7f	dynamic
55.91.74.12	00-24-e8-c4-df-b1	dynamic
55.91.74.13	00-22-19-03-1a-ff	dynamic
55.91.74.14	00-15-c5-41-d9-04	dynamic
55.91.74.15	5c-26-0a-0f-7d-c9	dynamic

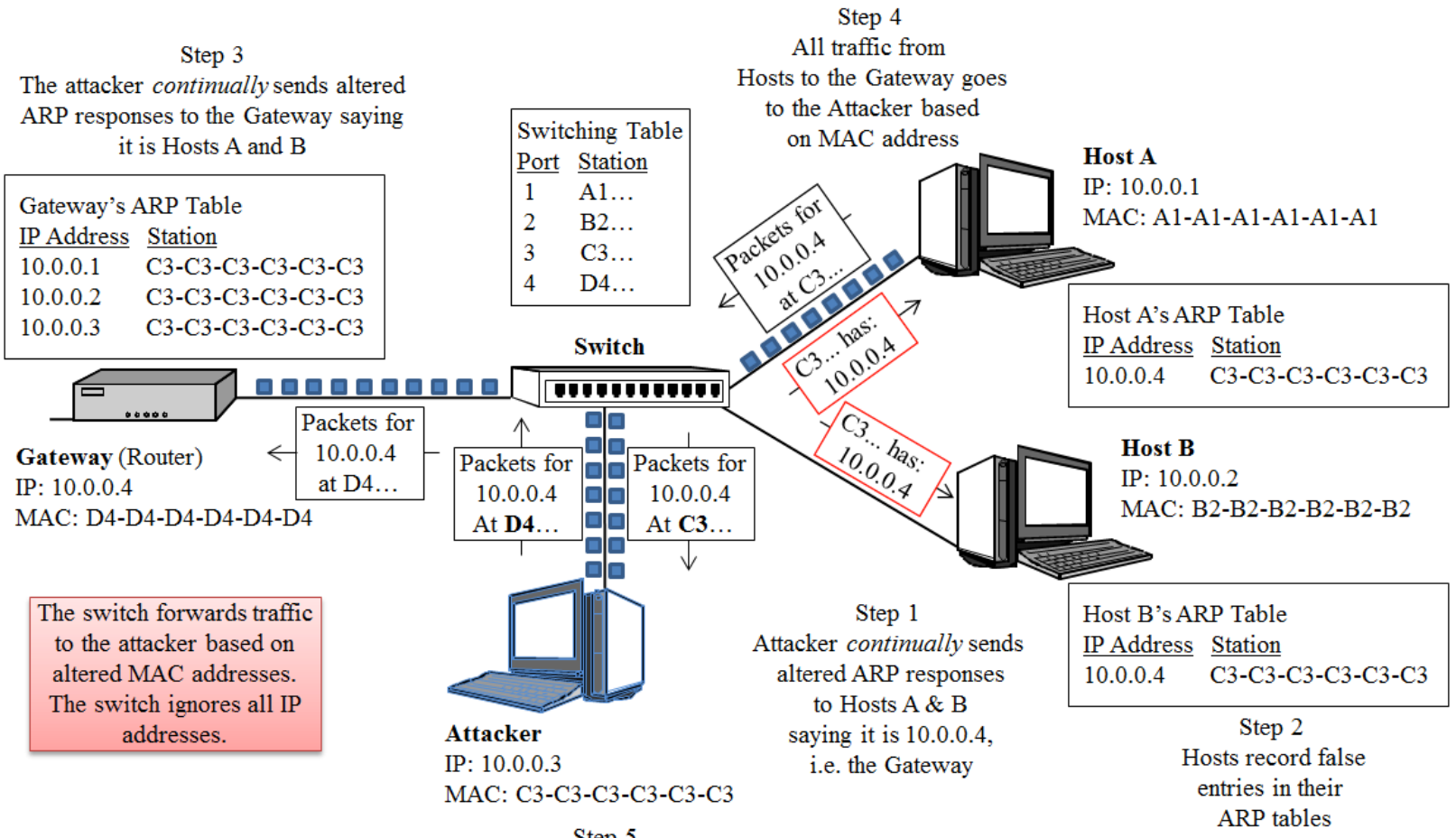
4.3: Normal ARP Operation



4.3: ARP Poisoning

- The problem: ARP requests and replies do NOT require authentication or verification
  - All hosts trust all ARP replies
  - ARP spoofing uses false ARP replies to map any IP address to any MAC address
  - An attacker can manipulate ARP tables on all LAN hosts
  - The attacker must send a continuous stream of unsolicited ARP replies

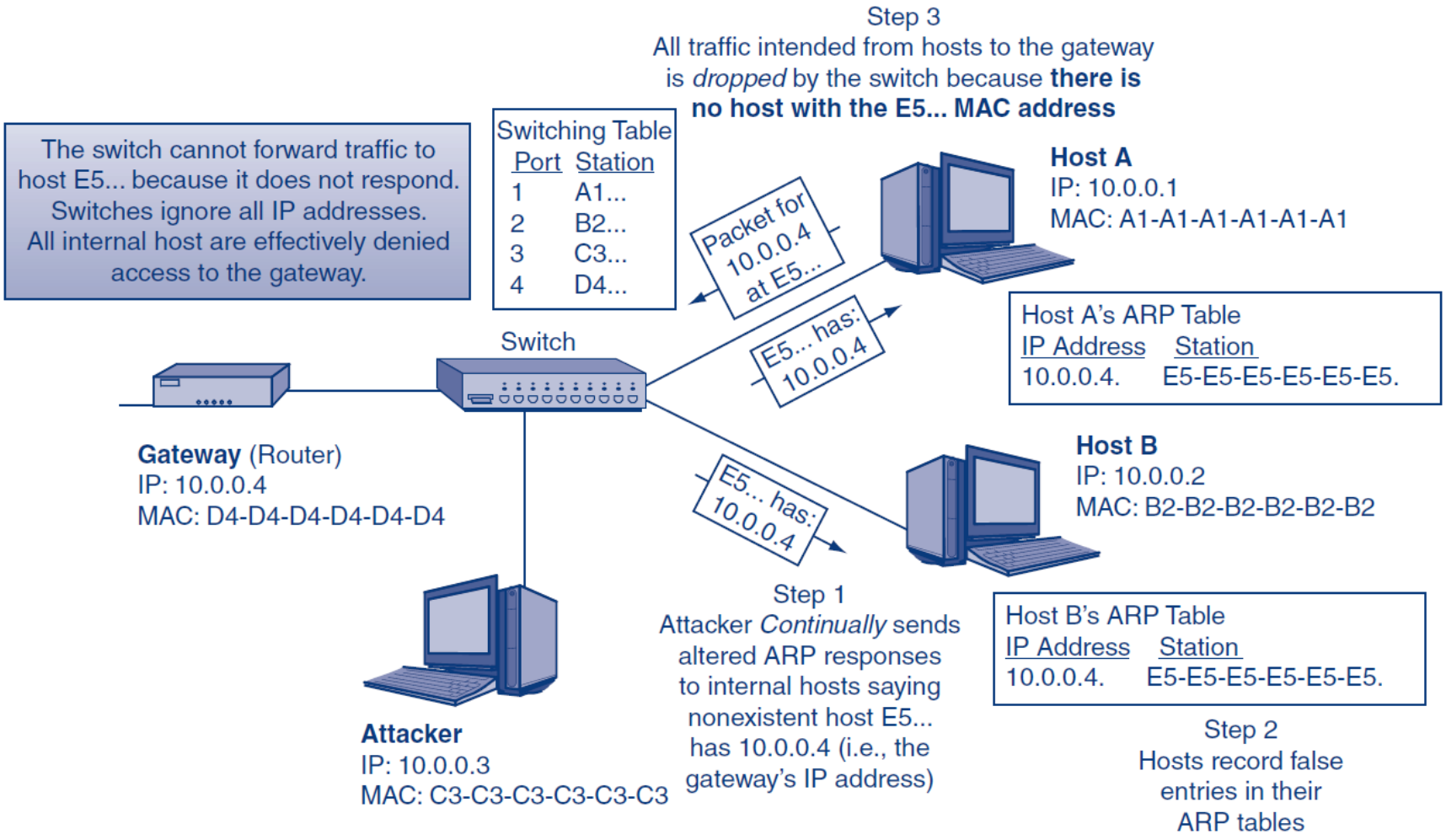
4.3: ARP Poisoning



4.3: ARP Poisoning

- ARP DoS Attack
  - Attacker sends all internal hosts a continuous stream of unsolicited spoofed ARP replies saying the gateway (10.0.0.4) is at E5-E5-E5-E5-E5-E5 (Step 1)
  - Hosts record the gateway's IP address and nonexistent MAC address (Step 2)
  - The switch receives packets from internal hosts addressed to E5-E5-E5-E5-E5-E5 but cannot deliver them because the host does not exist
  - Packets addressed to E5-E5-E5-E5-E5-E5 are dropped

4.3: ARP DoS Attack



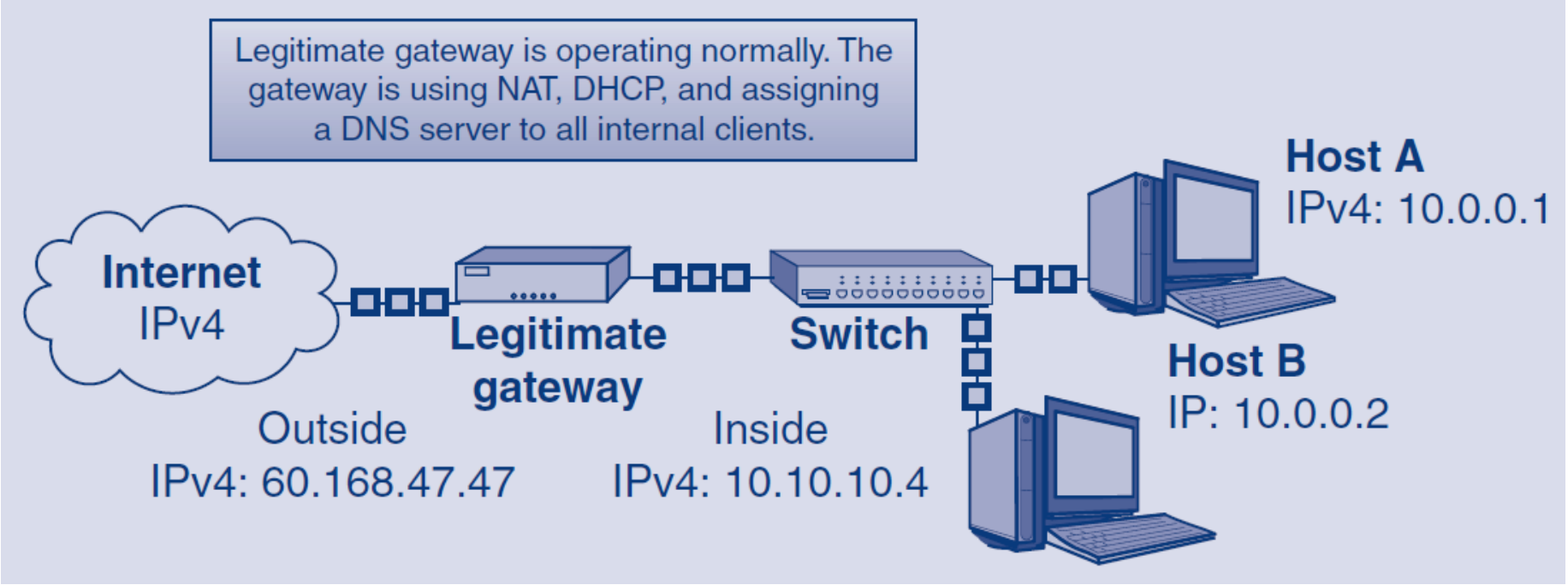
4.3: ARP Poisoning

- Preventing ARP Poisoning
  - Static ARP tables are manually set
    - Most organizations are too large, change too quickly, and lack the experience to effectively manage static IP and ARP tables
  - Limit Local Access
    - Foreign hosts must be kept off the LAN

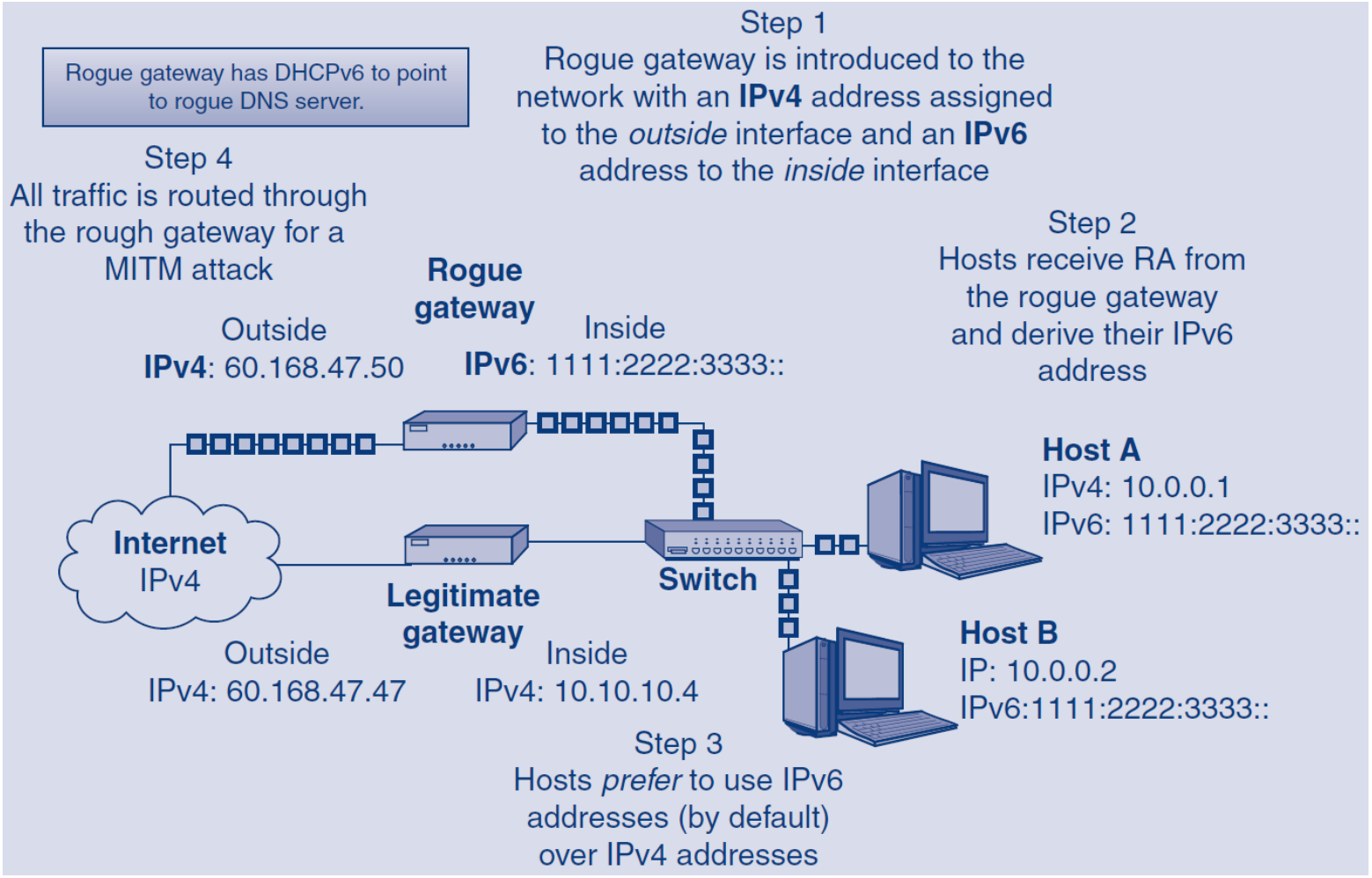
4.3: SLAAC Attack

- **Stateless Address Auto Configuration (SLAAC) attack**
  - An attack on the *functionality* and *confidentiality of a network*
  - This attack occurs when a rogue IPv6 router is introduced to an IPv4 network
  - All traffic is automatically rerouted through the IPv6 router, creating the potential for a MITM attack

4.3: Normal IPv4 LAN



4.3: SLAAC Attack

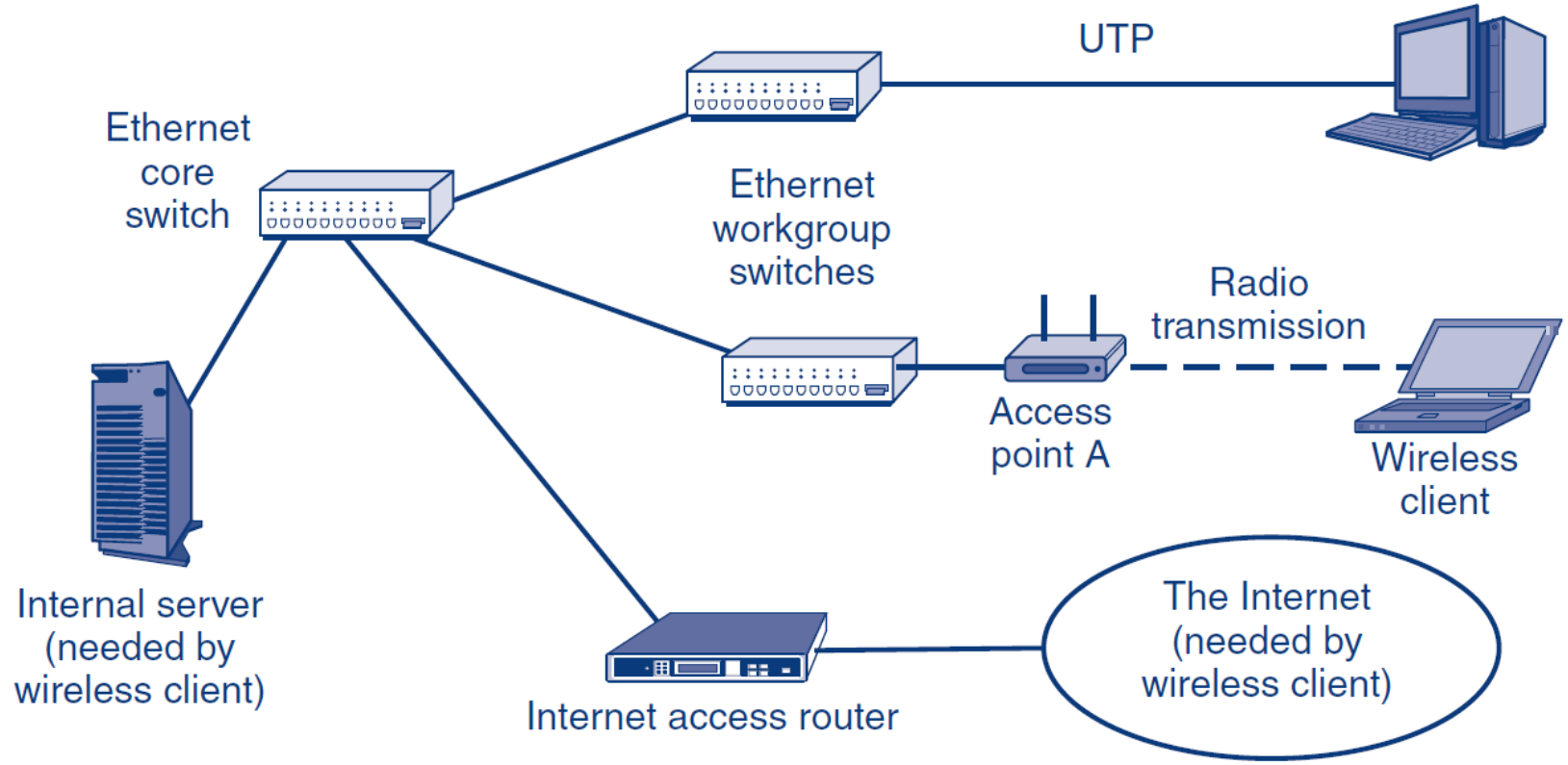


What's Next?

- 4.1 Introduction
- 4.2 Denial-of-Service (DoS) Attacks
- 4.3 ARP Poisoning
- 4.4 Access Control for Networks
- 4.5 Ethernet Security
- 4.6 Wireless Security

4.4: Corporate LAN

Threats:
Attacker can connect to Ethernet switch or access point, bypassing the site firewall.
Can intercept and read wireless transmissions.

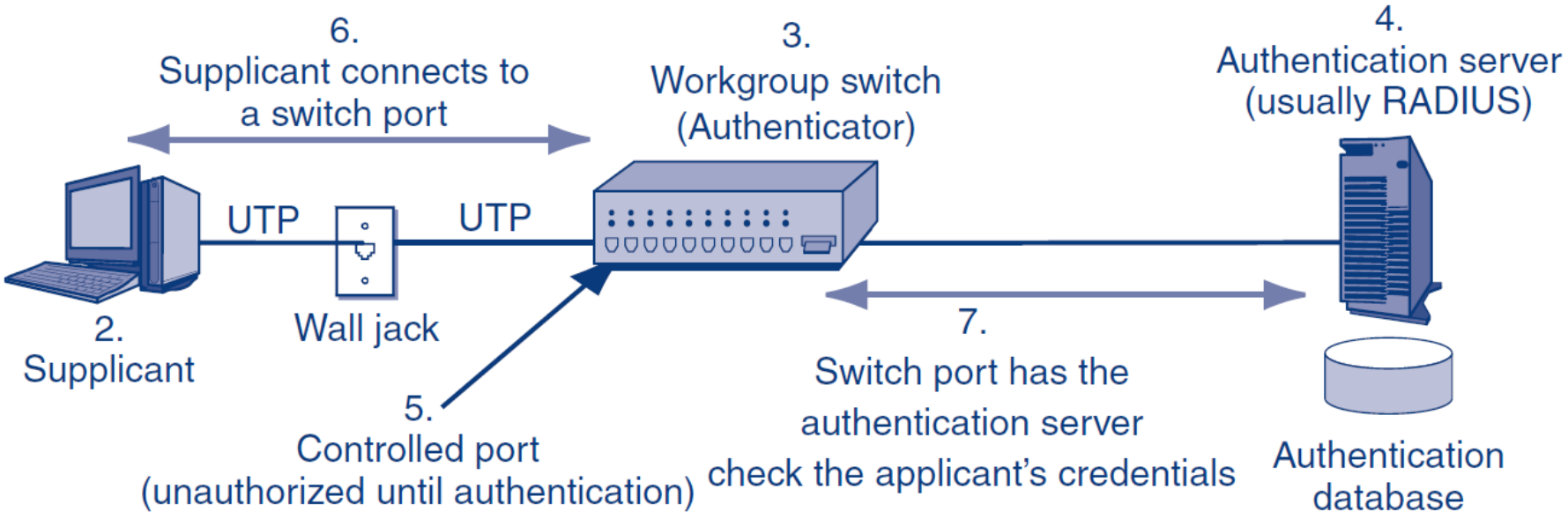


What's Next?

- 4.1 Introduction
- 4.2 Denial-of-Service (DoS) Attacks
- 4.3 ARP Poisoning
- 4.4 Access Control for Networks
- 4.5 Ethernet Security
- 4.6 Wireless Security

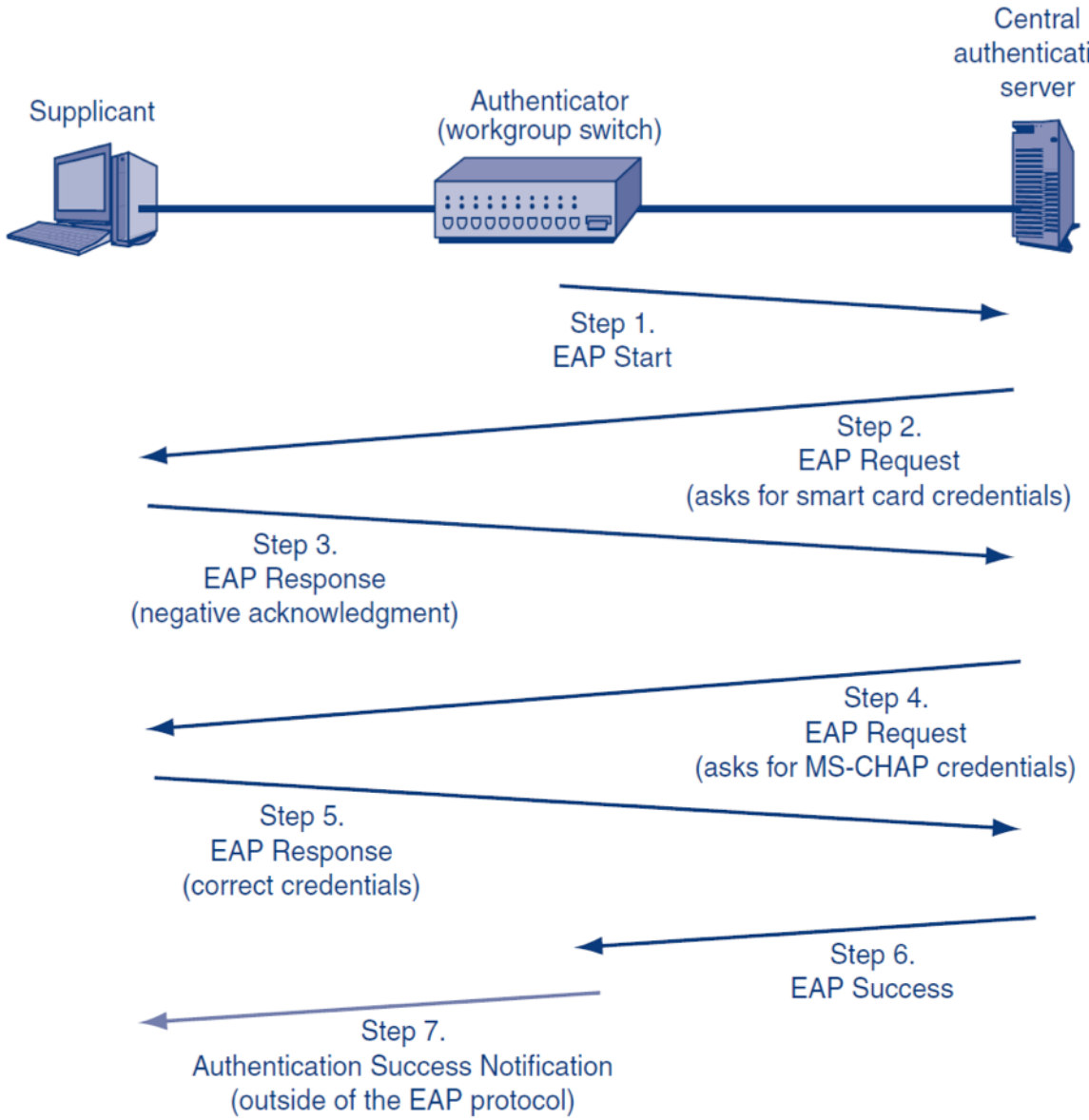
4.5: Ethernet and 802.1X

1.
Attacker can walk up to any wall jack and connect to the network, bypassing the border firewall. 802.1X requires the supplicant to authenticate itself before giving entry to the network.

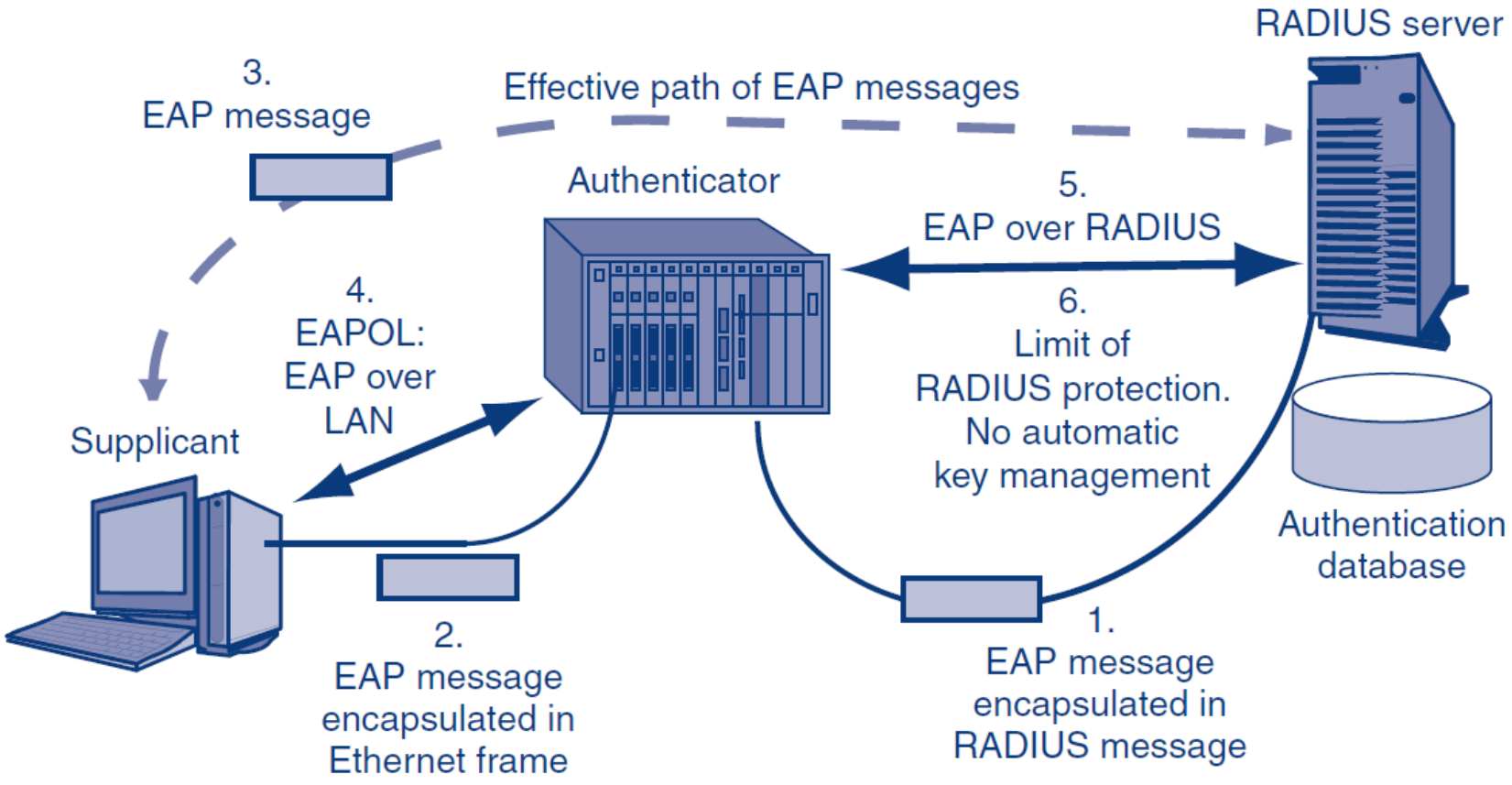


8.
Use of a central authentication server reduces the cost per switch, brings consistency of authentication, and allows immediate changes to authentication data.

4.5: Extensible Authentication Protocol (EAP)



4.5: EAPOL and EAP over RADIUS



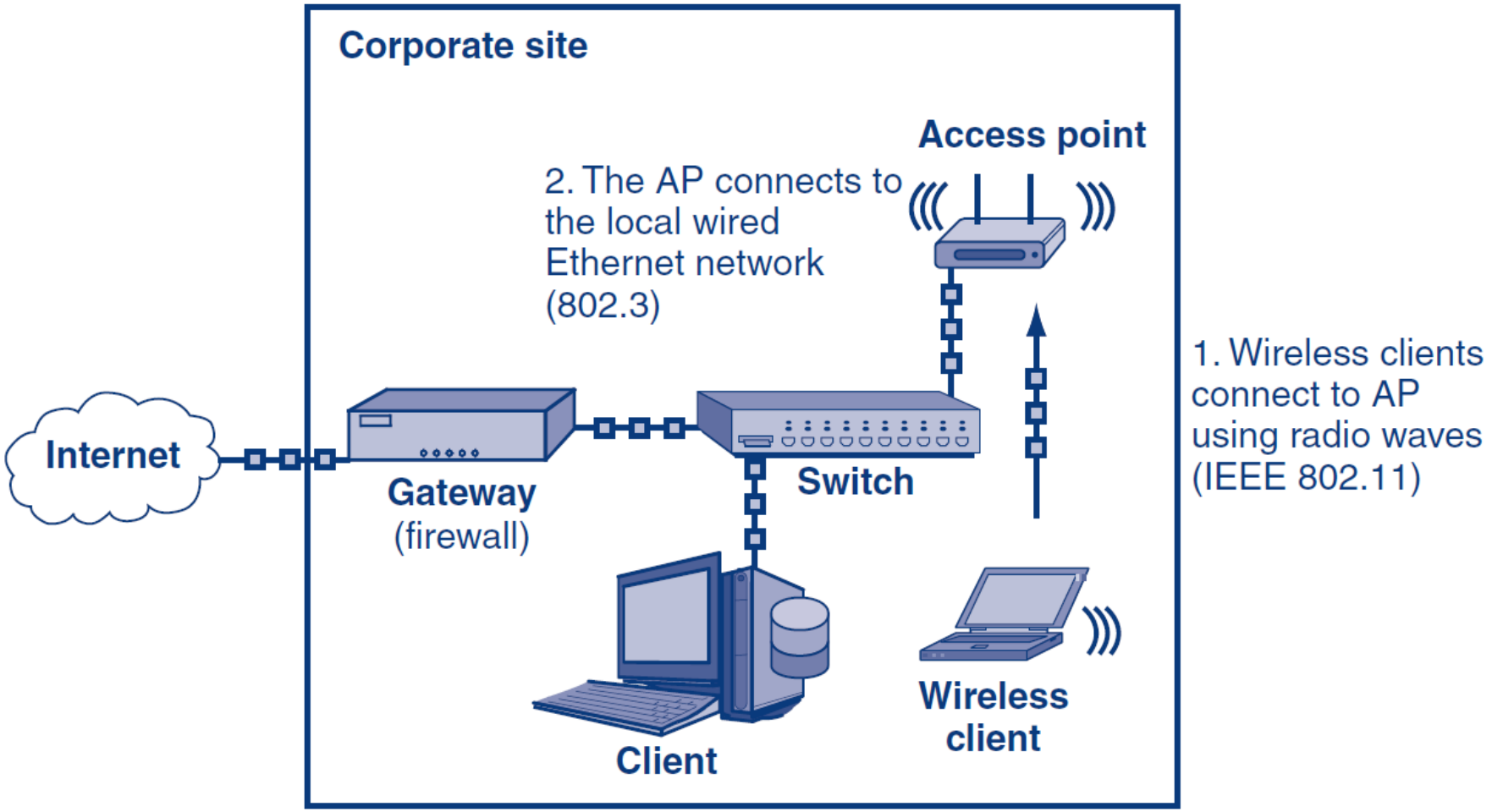
4.5: RADIUS and EAP

RADIUS Functionality		
Authentication	Authorizations	Auditing
Uses EAP	Uses RADIUS authorization functionality	Uses RADIUS auditing functionality

What's Next?

- 4.1 Introduction
- 4.2 Denial-of-Service (DoS) Attacks
- 4.3 ARP Poisoning
- 4.4 Access Control for Networks
- 4.5 Ethernet Security
- 4.6 Wireless Security

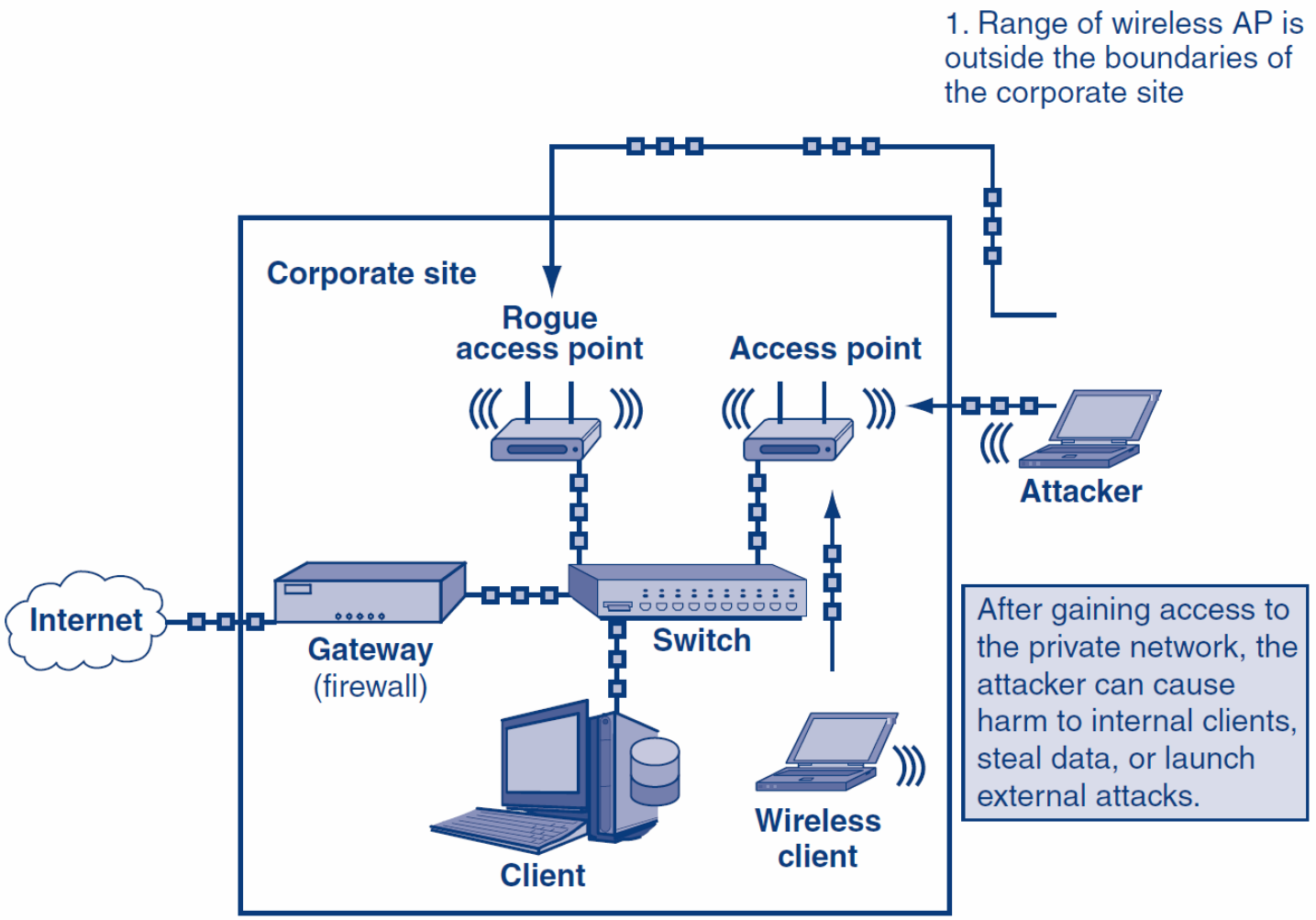
4.6: Wireless Network Access



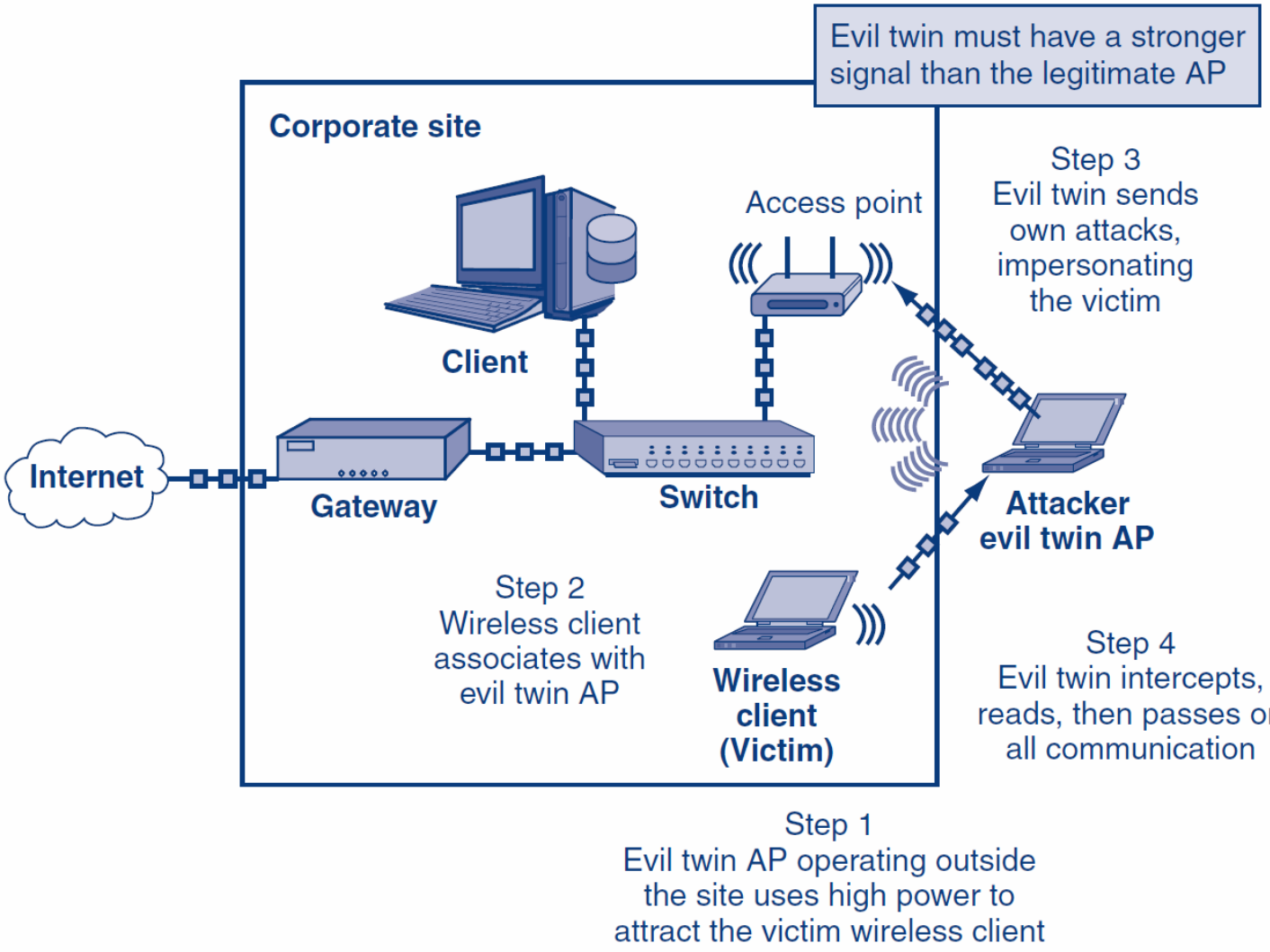
4.6: Unauthorized Network Access

- *Open networks* can be legally accessed by anyone
  - Found in public places like cafés, coffee shops, universities, etc.
- *Private networks* that do not allow access unless specifically authorized
- *Secured networks* have security protocols enabled
  - Users are authenticated and wireless traffic is encrypted

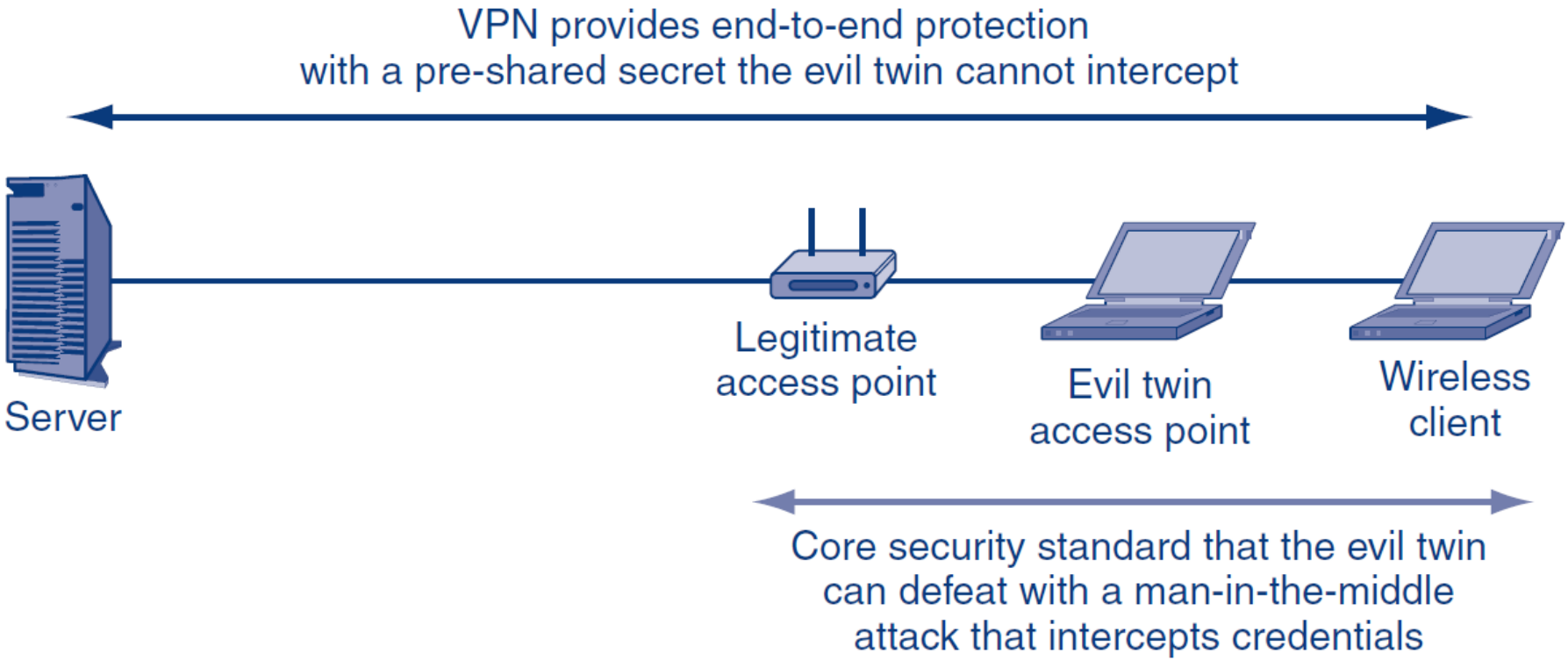
4.6: Unauthorized Wireless Access



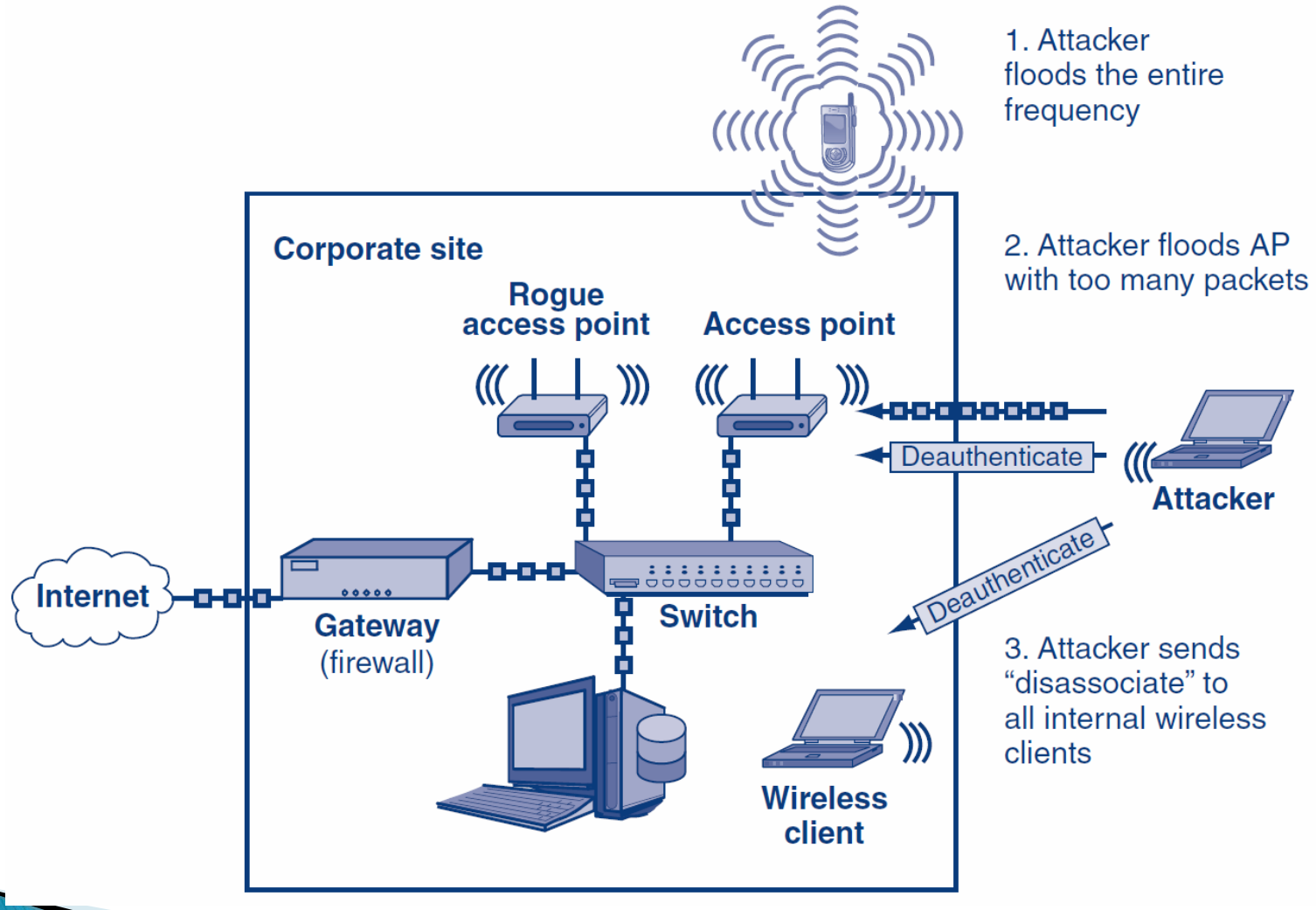
4.6: Evil Twin Access Point



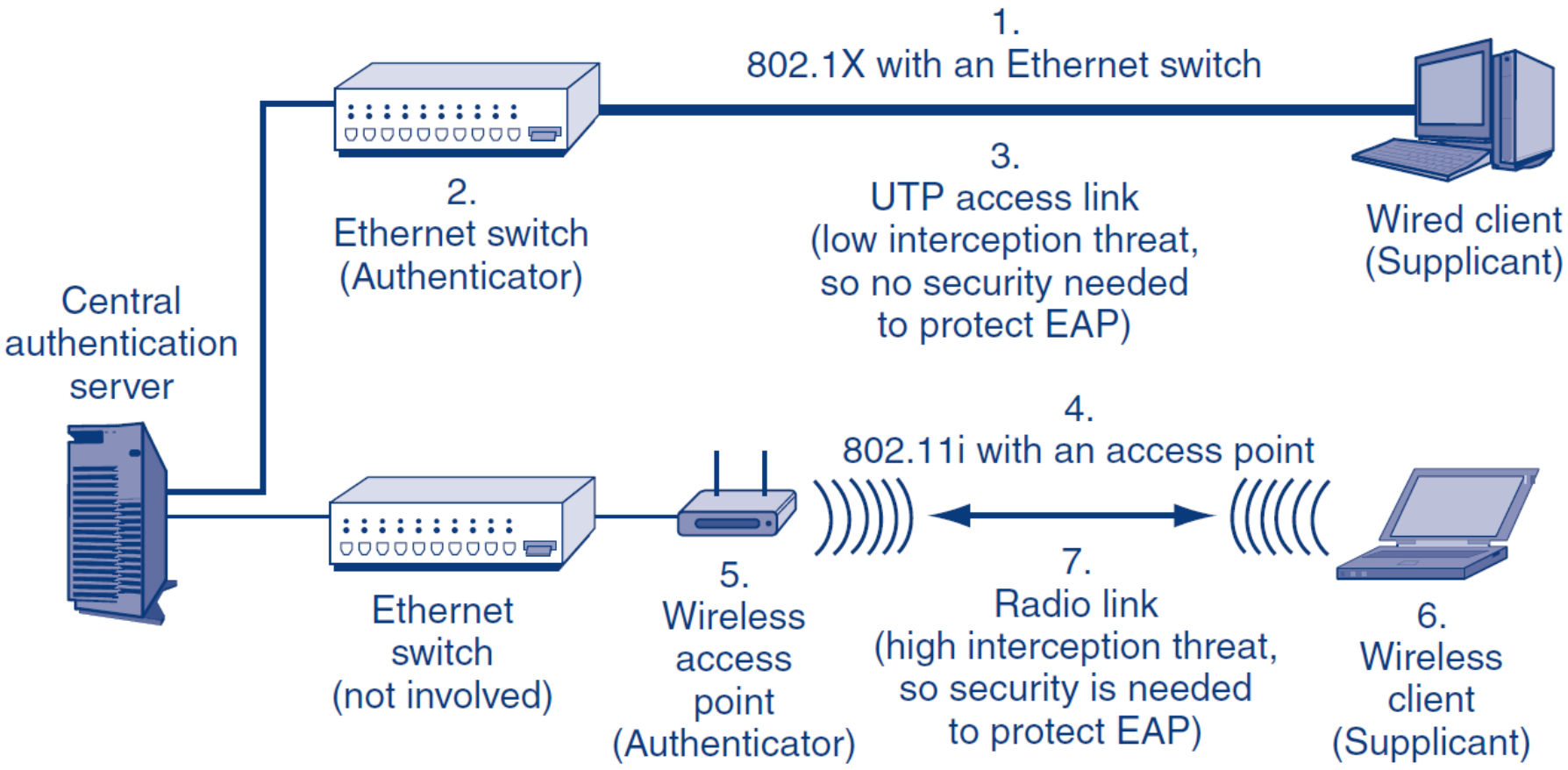
4.6: VPN Protection Against Evil Twin APs



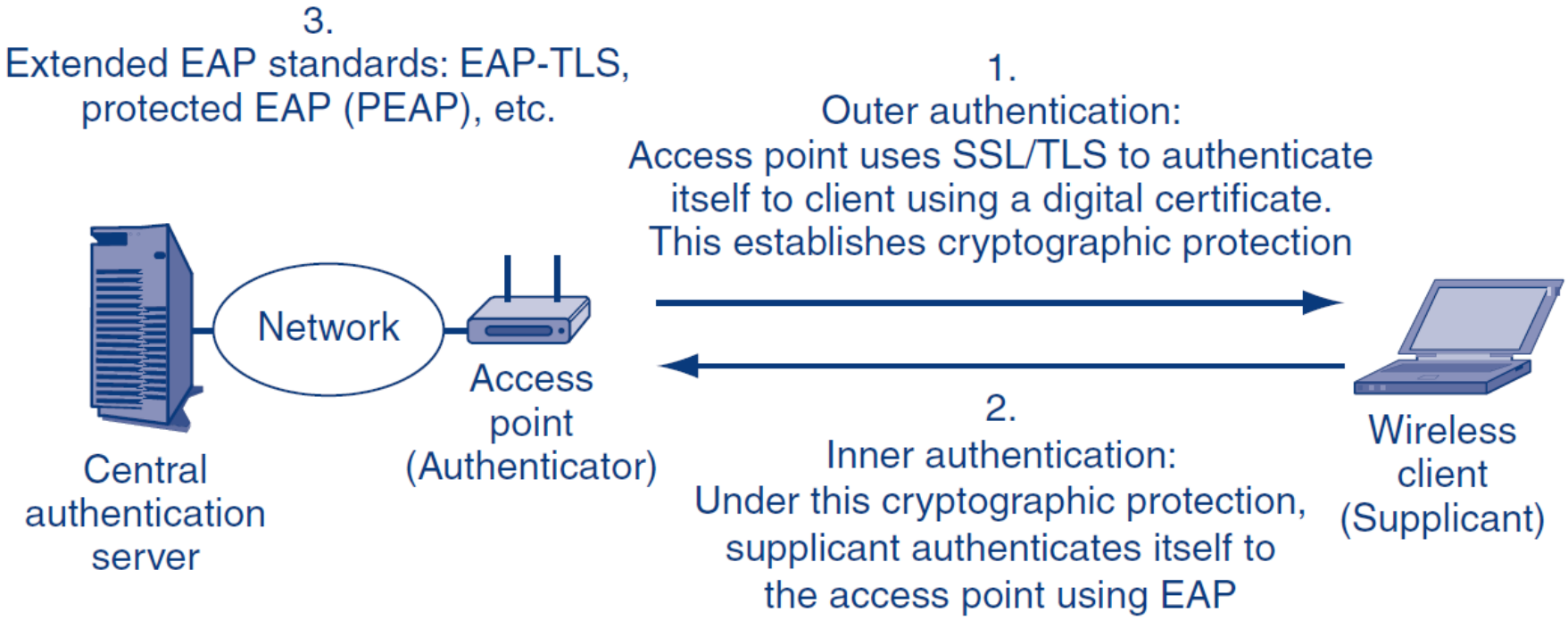
4.6: Wireless DoS – Disassociation & Jamming



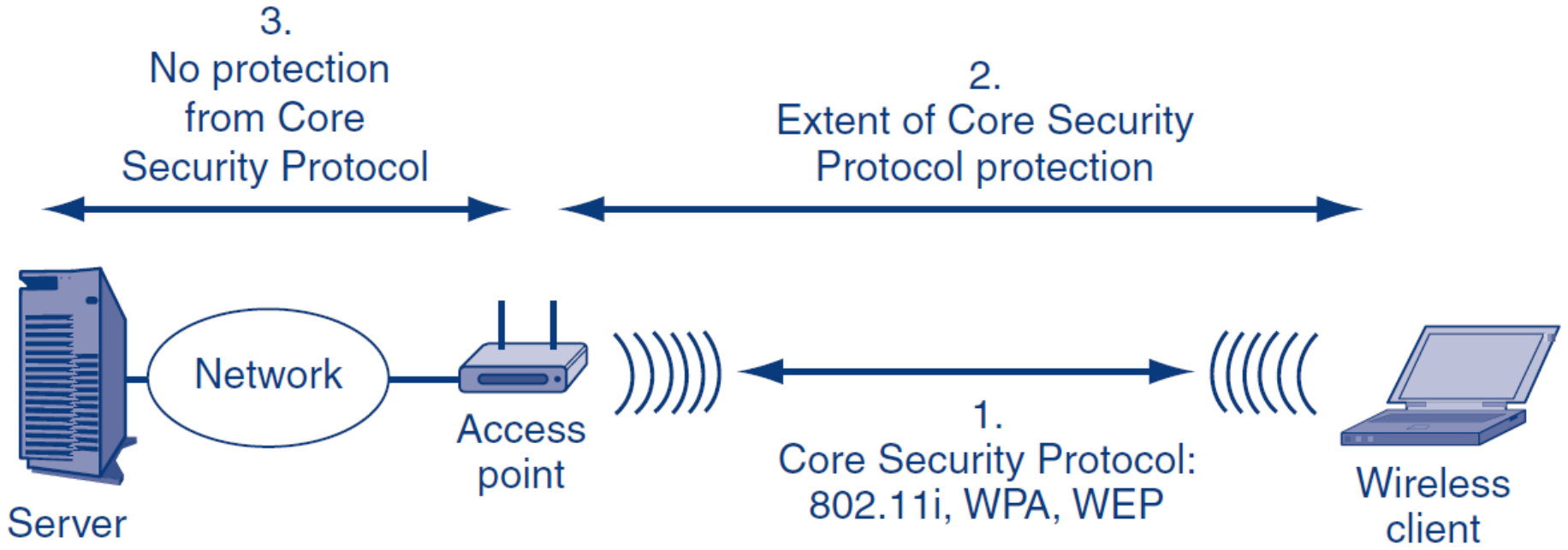
4.6: 802.11i or WPA Wireless LAN Access Control in 802.1X Mode



4.6: Extended EAP Protocols



4.6: 802.11 Core Security Protocol



4.6: Wired Equivalent Privacy (WEP)

- **Origin of WEP**
  - Original core security standard 802.11, created in 1997
- **Uses a Shared Key**
  - Each station using the access point uses the same (shared) key
  - The key is supposed to be secret, so knowing it "authenticates" the user
  - All encryption uses this key

4.6: Wired Equivalent Privacy (WEP)

- **Problem with Shared Keys**
  - If the shared key is learned, an attacker near an access point can read *all* traffic
  - Shared keys should be changed frequently
    - WEP had no way to do automatic rekeying
    - Manual rekeying is expensive if there are many users
    - Manual rekeying is operationally next to impossible if many or all stations use the same shared key, because of the work involved in rekeying many or all corporate clients

4.6: Wired Equivalent Privacy (WEP)

- **Problem with Shared Keys**
  - Because “everybody knows” the key, employees often give it out to strangers
  - If a dangerous employee is fired, the necessary rekeying may be impossible or close to it

4.6: Wired Equivalent Privacy (WEP)

- **RC4 Initialization Vectors (IV)**
  - WEP uses RC4 for fast and therefore cheap encryption
  - If two frames encrypted with the same RC4 key are compared, the attacker can learn the key
  - To solve this, WEP encrypts with a *per-frame key,* which is the shared WEP key *plus* an initialization vector (IV)
  - However, many frames "leak" a few bits of the key
  - With high traffic, an attacker using readily available software can crack a shared key in two or three minutes
  - (WPA uses RC4 but with a 48-bit IV that makes key bit leakage negligible)

4.6: Wired Equivalent Privacy (WEP)

- **Conclusion**
  - Corporations should never use WEP for security

4.6: Wi-Fi Protected Access (WPA)

- WPA
  - WPA extends the security of RC4 primarily by increasing the IV from 24 bits to 48 bits
  - This extension vastly reduces leakage and so makes RC4 much harder to crack
- WPA2 (802.11i)
  - 802.11 Working Group completed the 802.11i standard (WPA2) in 2002
  - Uses stronger security methods

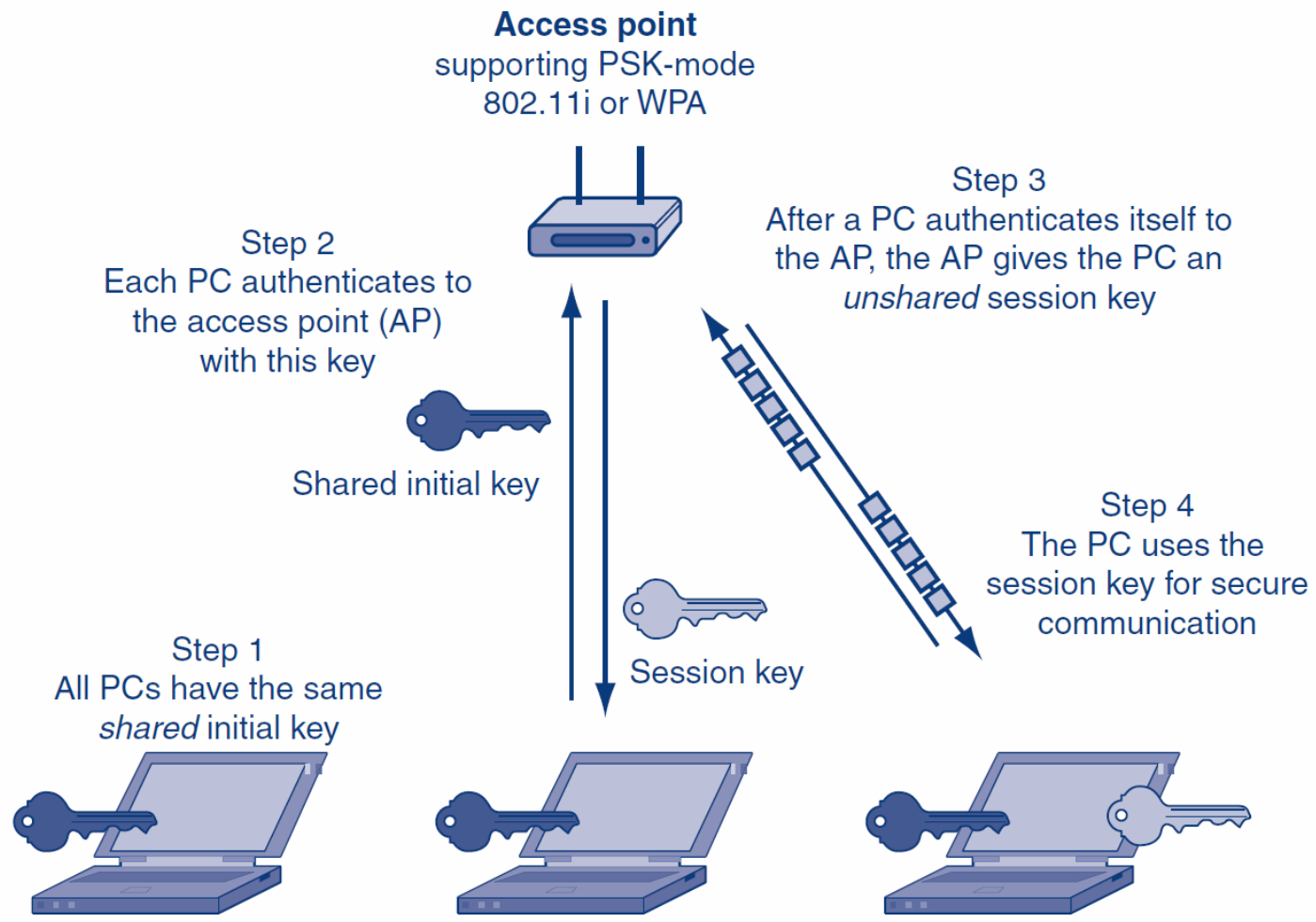
4.6: 802.11

Cryptographic Characteristic	WEP	WPA	802.11i (WPA2)
Cipher for Confidentiality	RC4 with a flawed implementation	RC4 with 48-bit initialization vector (IV)	AES with 128-bit keys
Automatic Rekeying	None	Temporal Key Integrity Protocol (TKIP), which has been partially cracked	AES-CCMP Mode
Overall Cryptographic Strength	Negligible	Weaker, but no complete crack to date	Extremely strong

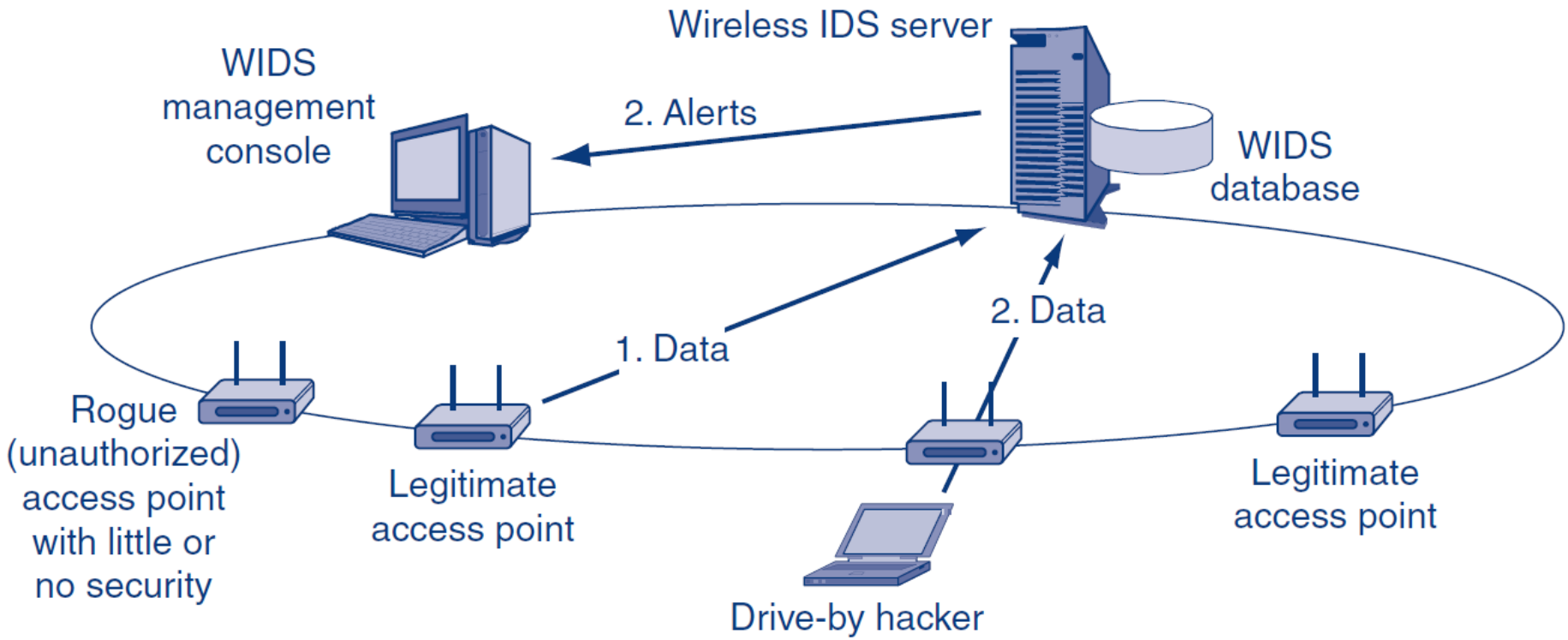
4.6: 802.11

Cryptographic Characteristic	WEP	WPA	802.11i (WPA2)
Operates in 802.1X (Enterprise) Mode?	No	Yes	Yes
Operates in Pre-Shared Key (Personal) Mode?	No	Yes	Yes

4.6: Pre-Shared Key (PSK)/Personal Mode for 802.11i and EPA



4.6: Centralized Wireless Intrusion Detection System



4.6: False 802.11 Security

- **Spread Spectrum Operation and Security**
  - Signal is spread over a wide range of frequencies
  - NOT done for security, as in military spread spectrum transmission

4.6: False 802.11 Security

- **Turning Off SSID Broadcasting**
  - Service set identifier (SSID) is an identifier for an access point
  - Users must know the SSID to use the access point
  - Drive-by hacker needs to know the SSID to break in
  - Access points frequently broadcast their SSIDs

4.6: False 802.11 Security

- **Turning off SSID Broadcasting**
  - Some writers favor turning off of this broadcasting
  - Turning off SSID broadcasting can make access more difficult for ordinary users
  - Will not deter the attacker because he or she can read the SSID.
    - Transmitted in the clear in each transmitted frame

4.6: False 802.11 Security

- **MAC Access Control Lists**
  - Access points can be configured with MAC access control lists
  - Only permit access by stations with NICs having MAC addresses on the list
  - However, MAC addresses are sent in the clear in frames, so attackers can learn them
  - Attacker can then spoof one of these addresses

4.6: False 802.11 Security

- **Perspective**
  - These “false” methods, however, may be sufficient to keep out nosy neighbors
  - Drive-by hackers hit even residential users
  - Simply applying WPA or 802.11i provides much stronger security and is easier to do

The End