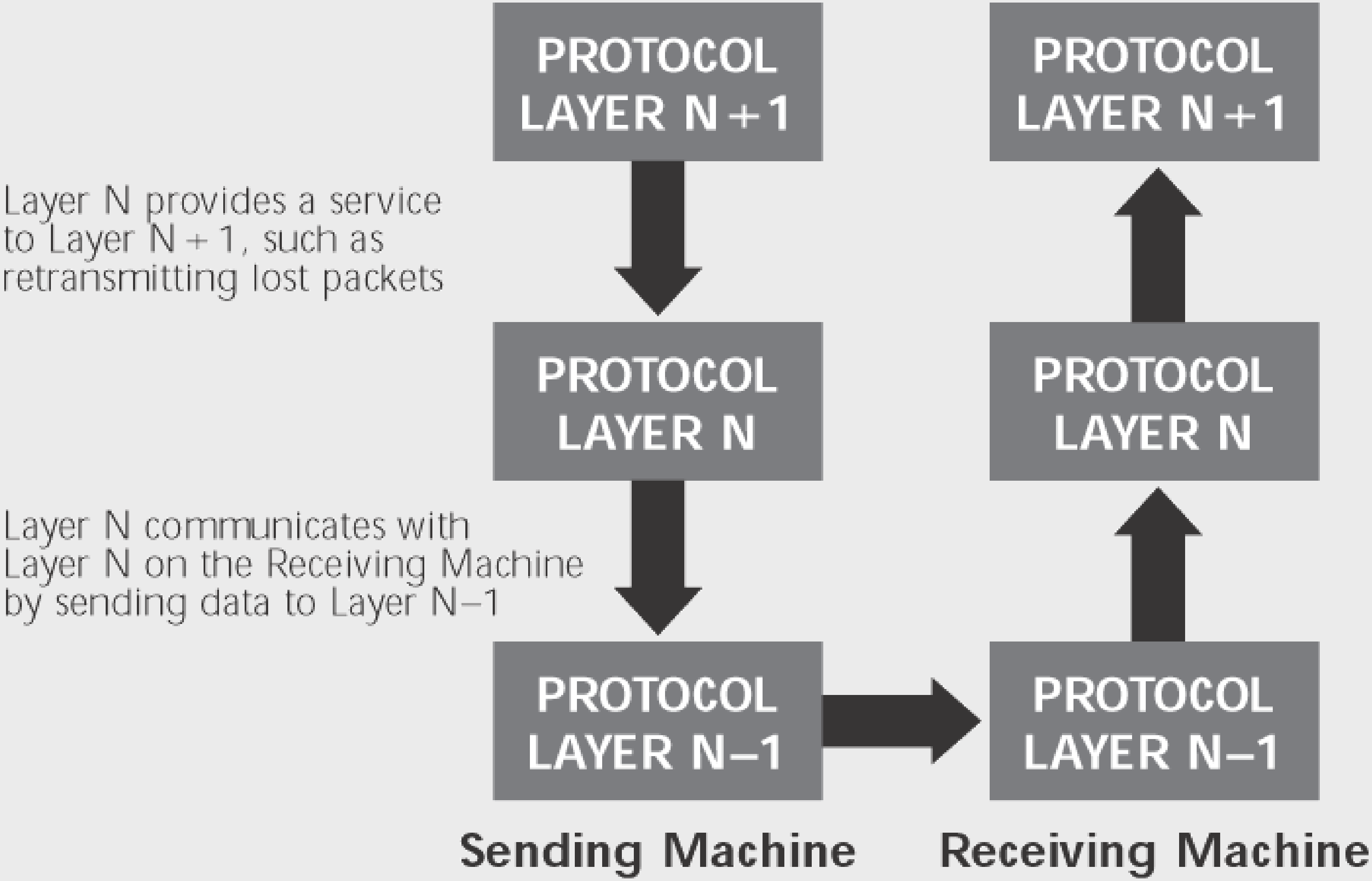
Chapter 2 Networking Overview



Layer N provides a service to Layer N + 1, such as retransmitting lost packets

Layer N communicates with Layer N on the Receiving Machine by sending data to Layer N–1

Figure 2.1 Generic protocol layers move data between systems

OSI Reference Model

- Layer 7 Application Layer
- Layer 6 Presentation Layer
- Layer 5 Session Layer
- Layer 4 Transport Layer
- Layer 3 Network Layer
- Layer 2 Datalink Layer
- Layer 1 Physical Layer

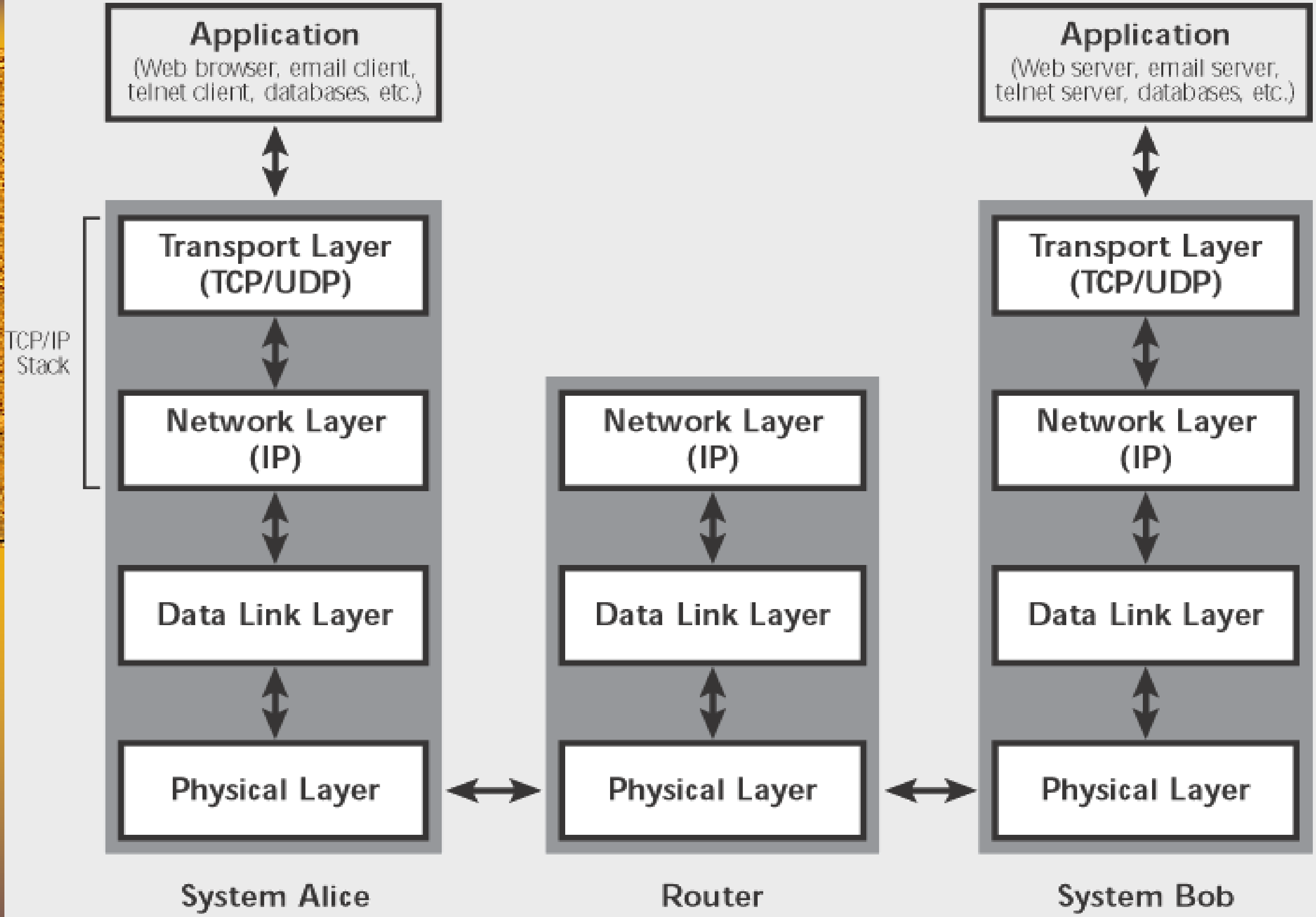
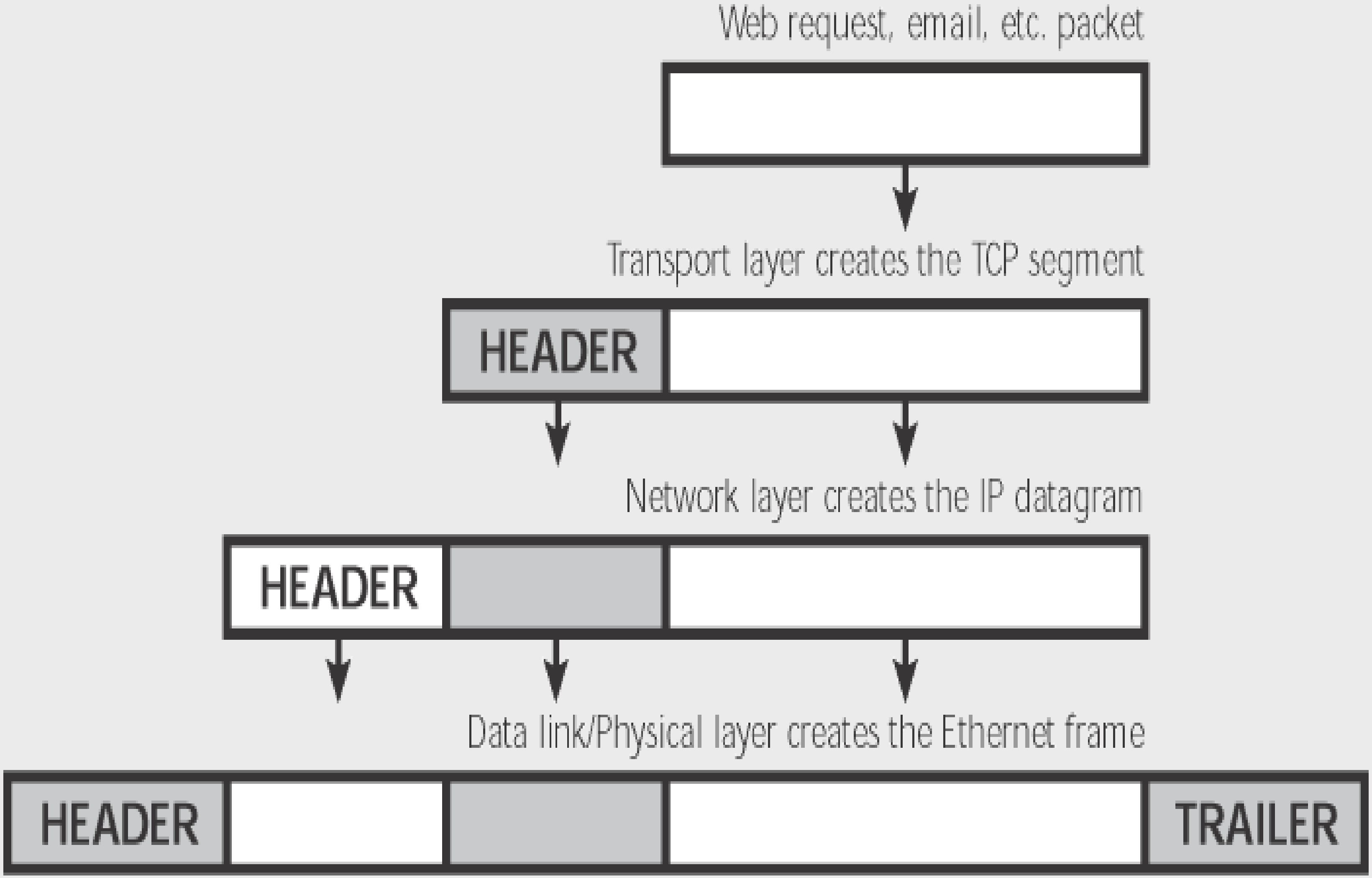


Figure 2.2 Protocol Layering in TCP/IP

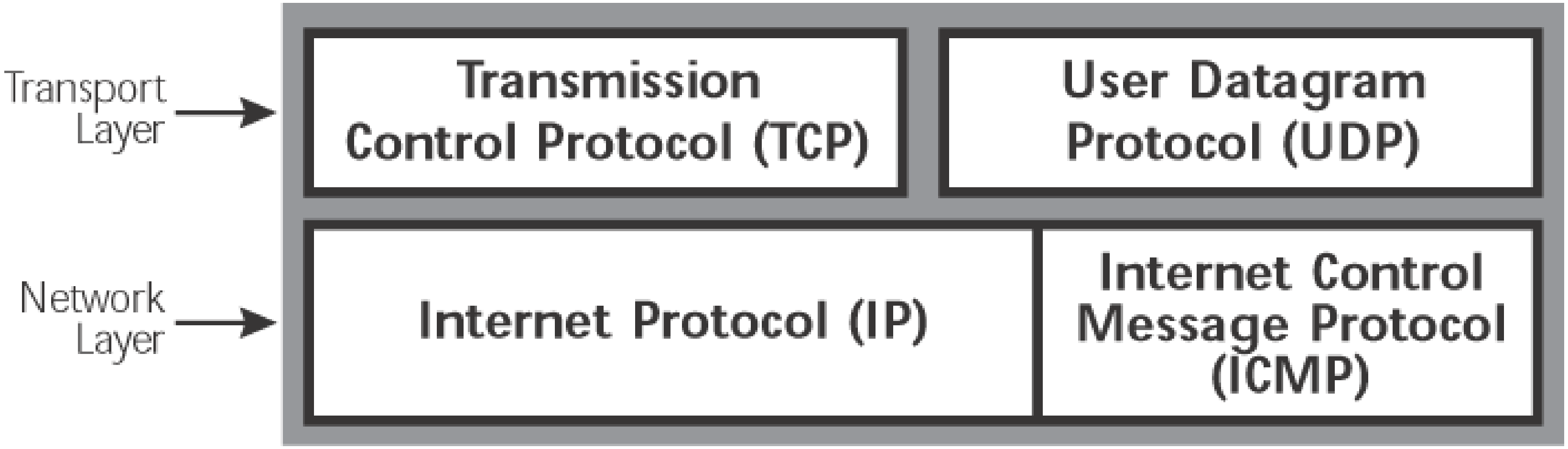


Web request, email, etc. packet
Transport layer creates the TCP segment
HEADER
Network layer creates the IP datagram
HEADER
Data link/Physical layer creates the Ethernet frame
HEADER
TRAILER

Figure 2.3 Adding headers (and a trailer) to move data through the communications stack and across the network

Understanding TCP/IP

Requests for Comment documents
http://www.ietf.org/rfc.html



Transport Layer

Transmission Control Protocol (TCP)

User Datagram Protocol (UDP)

Network Layer

Internet Protocol (IP)

Internet Control Message Protocol (ICMP)

Figure 2.4 Members of the TCP/IP family

Transmission Control Protocol (TCP)

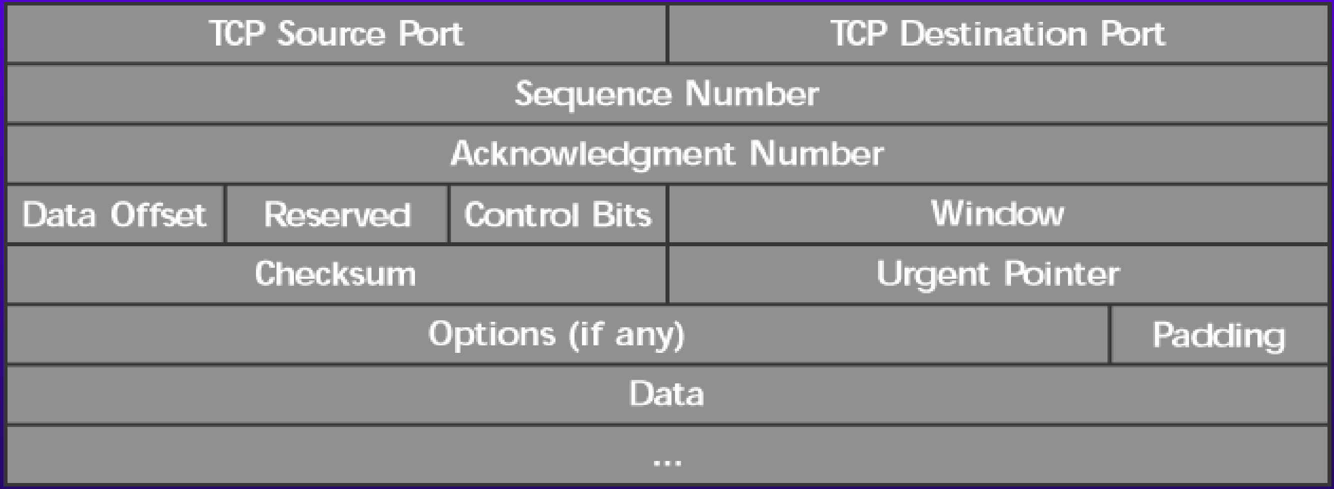
-Source/Destination ports

-Sequence number: increases for each byte of data transmitted

-Data Offset: length of TCP header in 32-bit words

-Checksum: data integrity of TCP header and data

-Urgent pointer: indicates location of urgent data in data stream

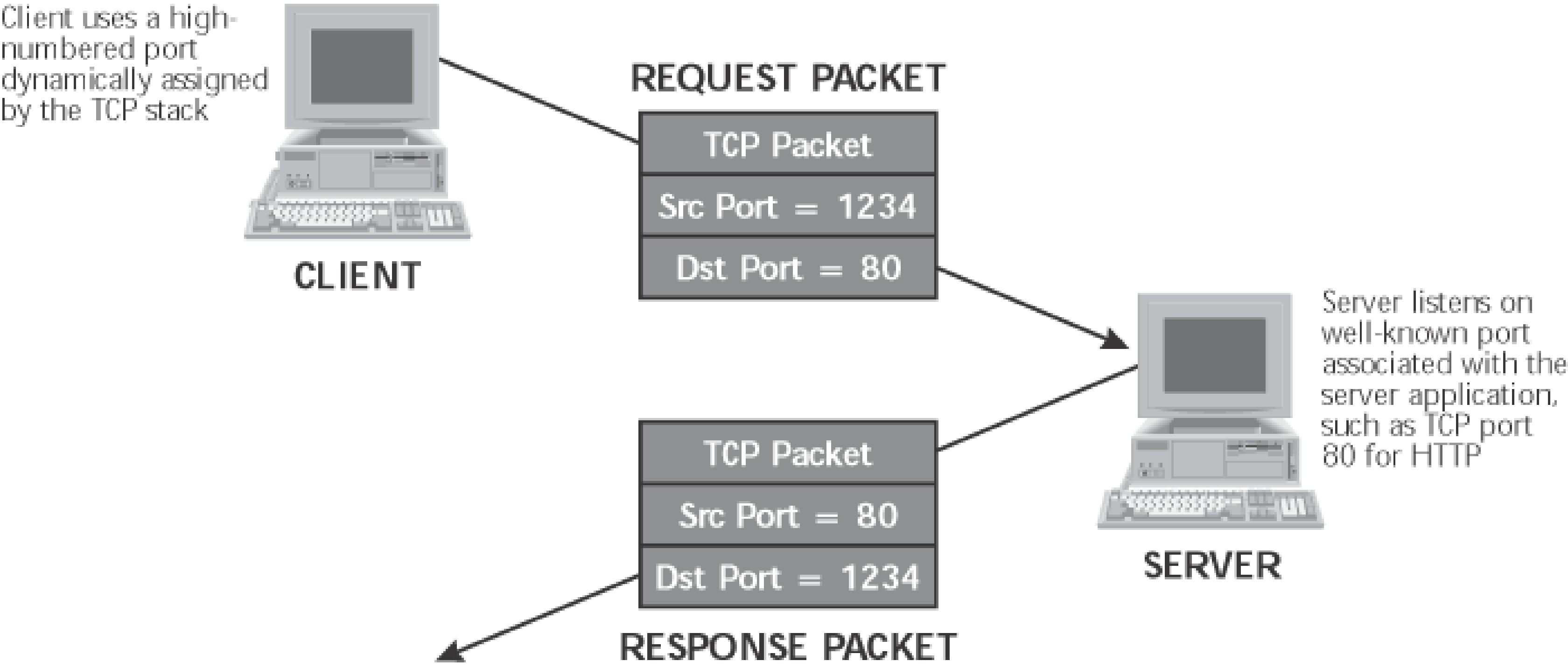


<table>
<tr><td colspan="2">TCP Source Port</td><td colspan="2">TCP Destination Port</td></tr>
<tr><td colspan="4">Sequence Number</td></tr>
<tr><td colspan="4">Acknowledgment Number</td></tr>
<tr><td>Data Offset</td><td>Reserved</td><td>Control Bits</td><td>Window</td></tr>
<tr><td colspan="2">Checksum</td><td colspan="2">Urgent Pointer</td></tr>
<tr><td colspan="3">Options (if any)</td><td>Padding</td></tr>
<tr><td colspan="4">Data</td></tr>
<tr><td colspan="4">...</td></tr>
</table>

Figure 2.5 TCP Header

TCP Port Numbers

- closed ports
- open ports
- RFC 1700 (well-known ports)

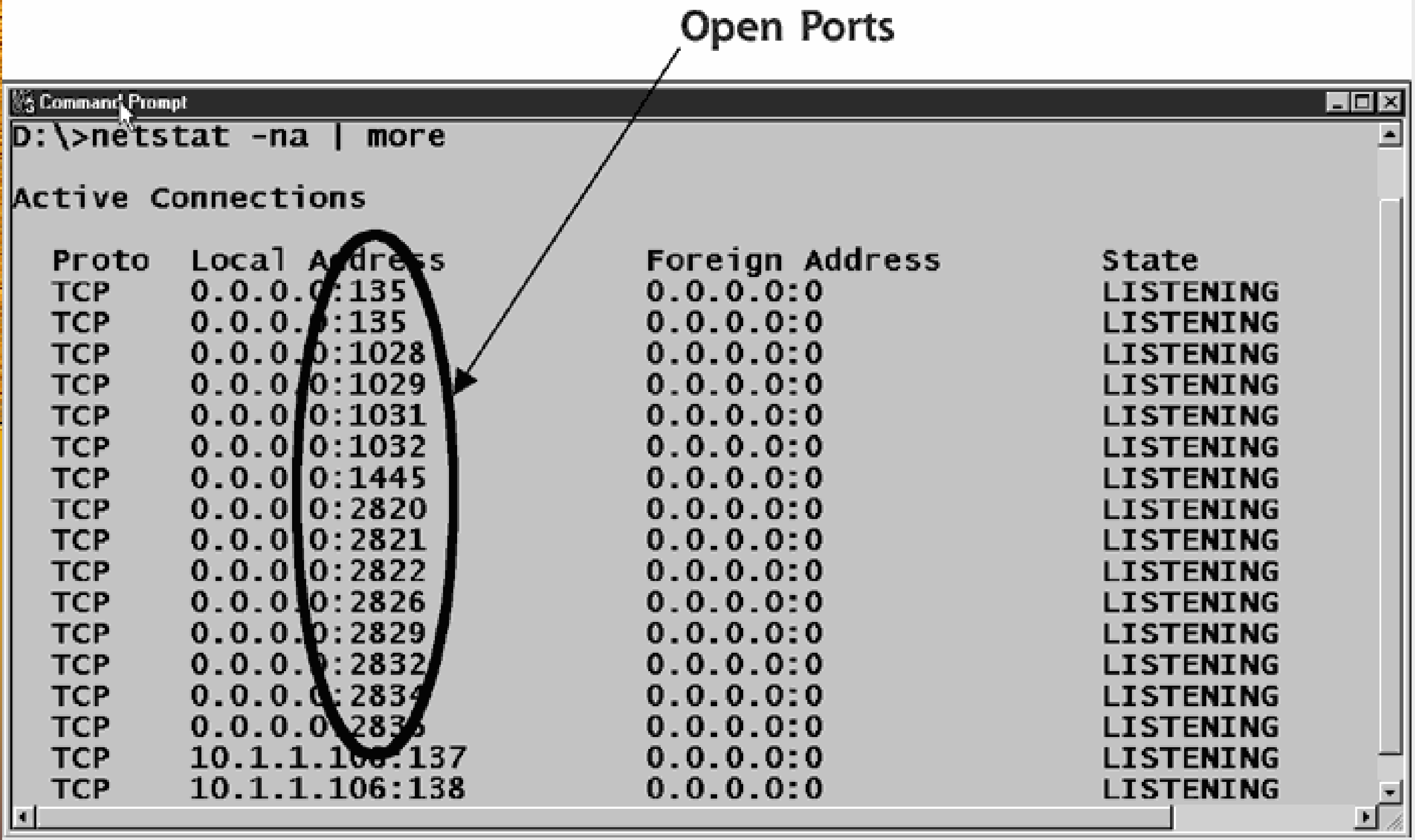


Client uses a high-numbered port dynamically assigned by the TCP stack

Server listens on well-known port associated with the server application, such as TCP port 80 for HTTP

Figure 2.6 TCP source & destination ports

Monitoring Ports in Use



```
D:\>netstat -na | more

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1028           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1029           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1031           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1032           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1445           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2820           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2821           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2822           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2826           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2829           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2832           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2834           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2835           0.0.0.0:0              LISTENING
  TCP    10.1.1.106:137         0.0.0.0:0              LISTENING
  TCP    10.1.1.106:138         0.0.0.0:0              LISTENING
```

Figure 2.7

TCP Control Bits

URG: Urgent pointer field is significant

ACK: Acknowledgment field is significant

PSH: Push data through TCP layer

RST: Reset connection (used also in response to unexpected data)

SYN: Synchronize sequence numbers

FIN: no more data from sender; tear down session

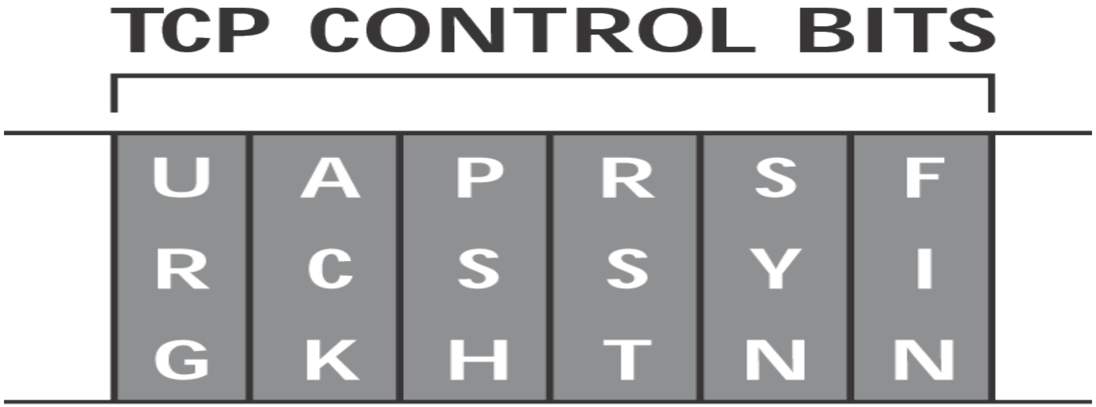


Figure 2.8

TCP 3-Way Handshake

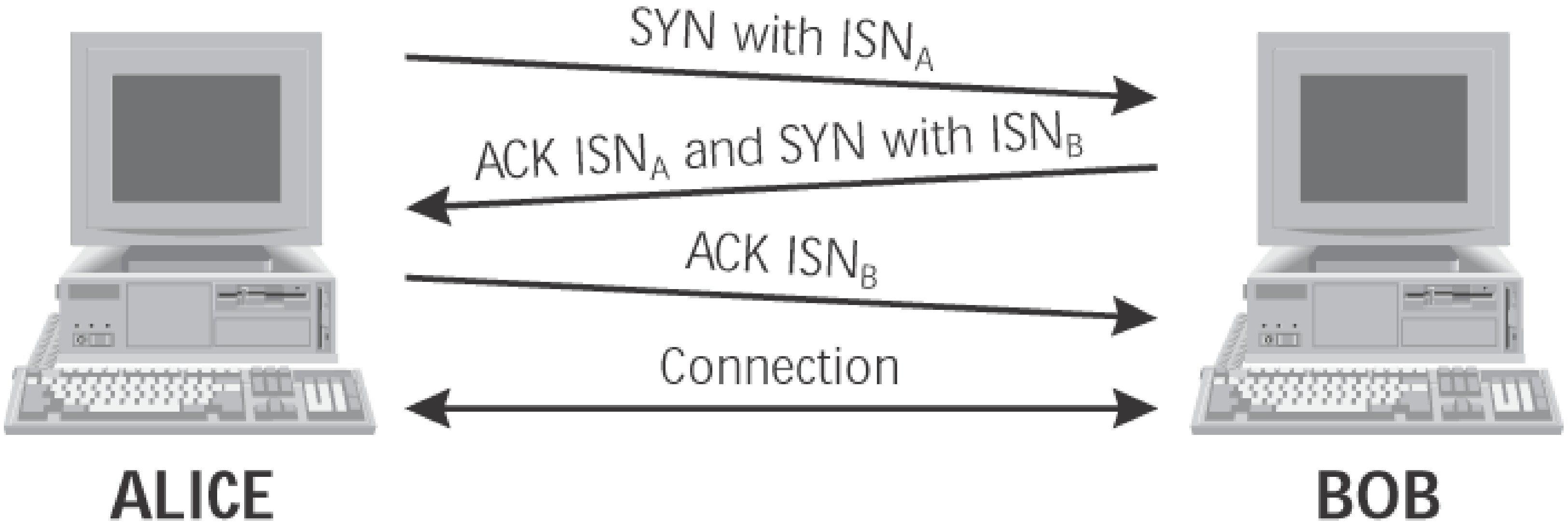
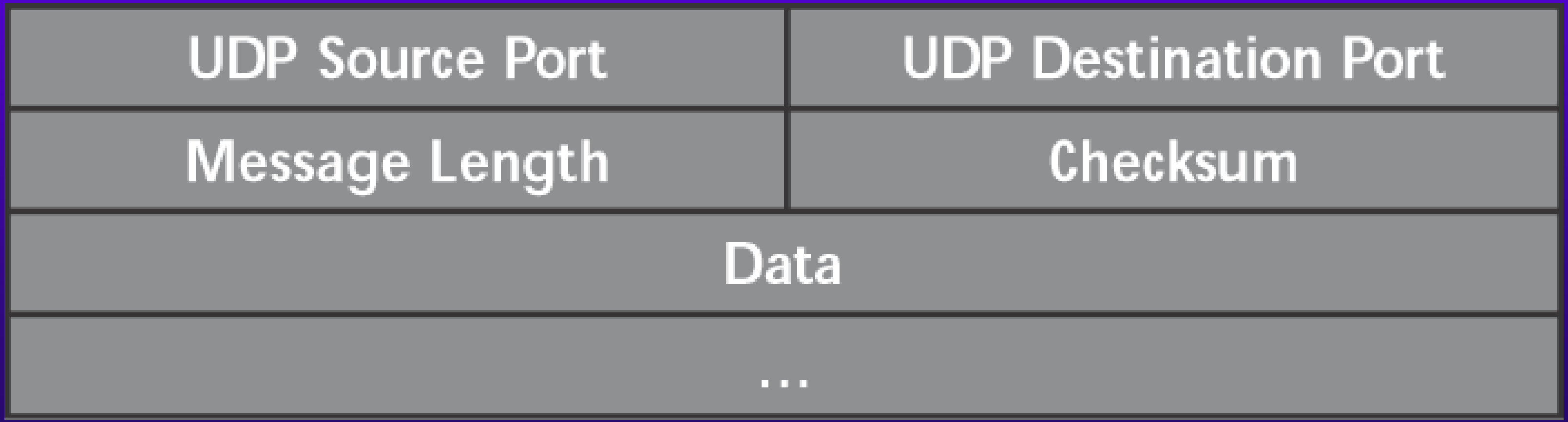

SYN with ISN_A
ACK ISN_A and SYN with ISN_B
ACK ISN_B
Connection
ALICE
BOB

Figure 2.9

User Datagram Protocol (UDP)

- Connectionless and unreliable
- packets not retransmitted
- Used by streaming audio/video, DNS queries/responses, TFTP, SNMP

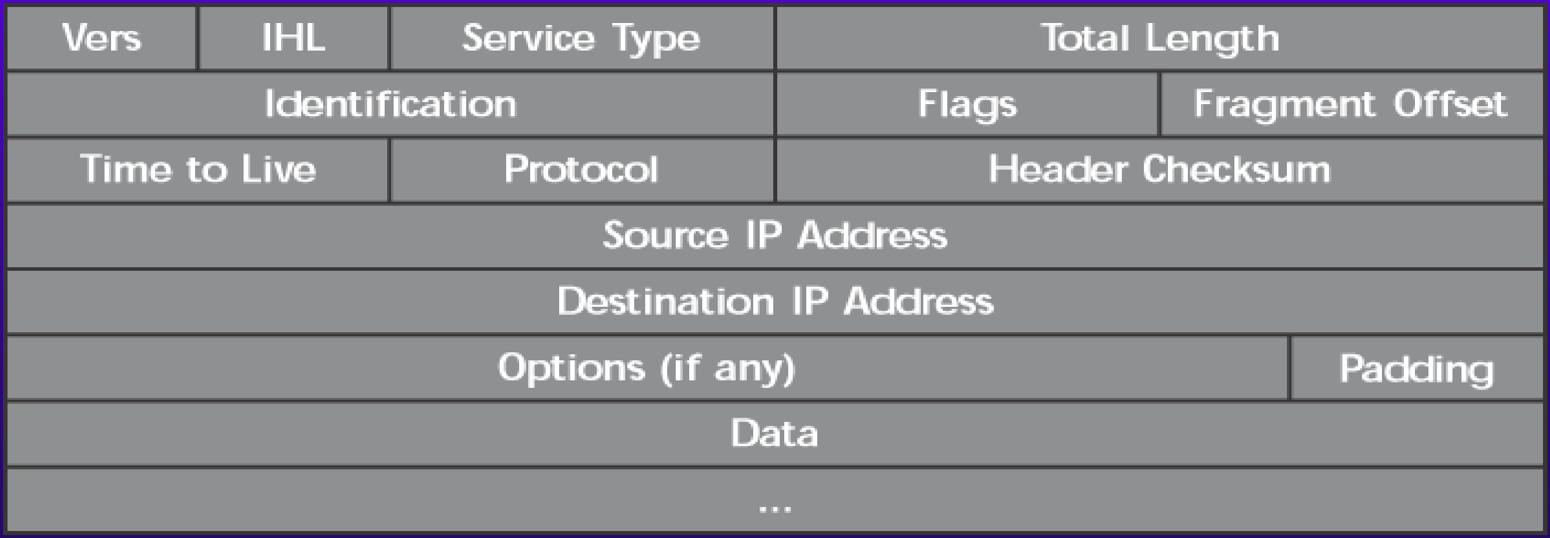


UDP Source Port	UDP Destination Port
Message Length	Checksum
Data	
...	

Figure 2.10

Internet Protocol (IP)

IHL: Internet Header Length
Service Type: QOS
Total Length: header and data
ID: support fragment reassembly
Flags: includes don’t fragment and more fragments
Protocol: used to indicate TCP, UDP, and ICMP



<table>
<tr><td>Vers</td><td>IHL</td><td colspan="2">Service Type</td><td colspan="4">Total Length</td></tr>
<tr><td colspan="4">Identification</td><td colspan="2">Flags</td><td colspan="2">Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td colspan="2">Protocol</td><td colspan="4">Header Checksum</td></tr>
<tr><td colspan="8">Source IP Address</td></tr>
<tr><td colspan="8">Destination IP Address</td></tr>
<tr><td colspan="7">Options (if any)</td><td>Padding</td></tr>
<tr><td colspan="8">Data</td></tr>
<tr><td colspan="8">...</td></tr>
</table>

Figure 2.10

Local Area Networks and Routers

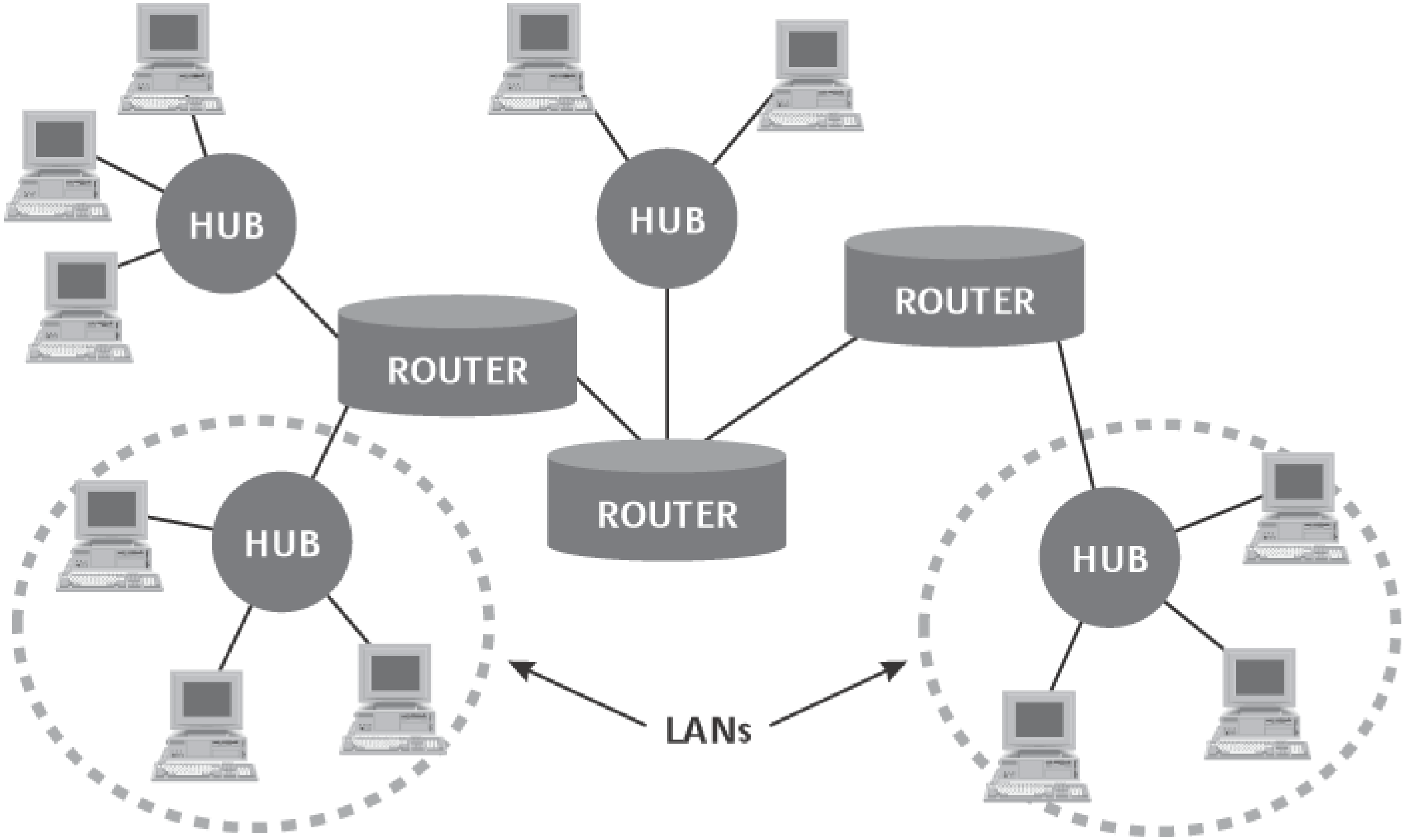
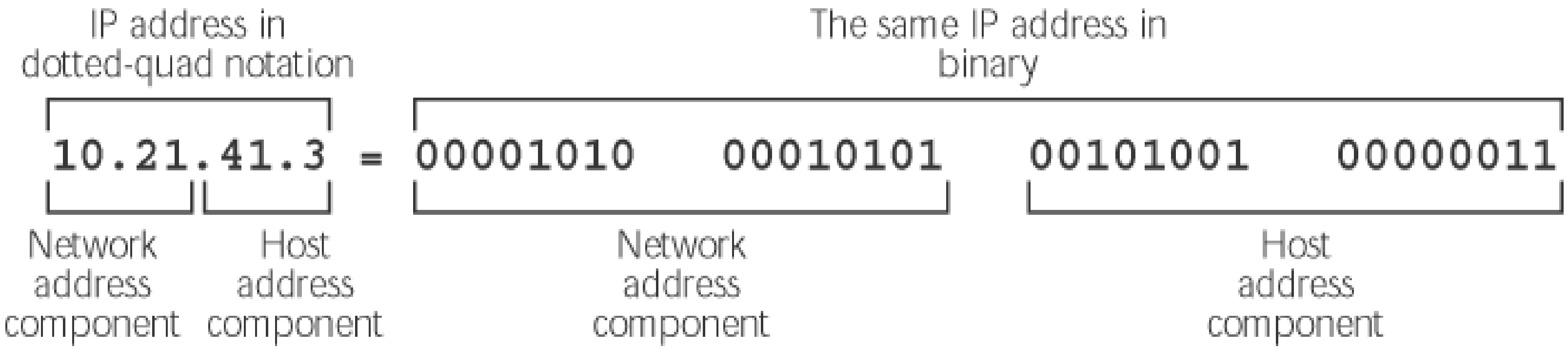


Figure 2.12

IP Addresses

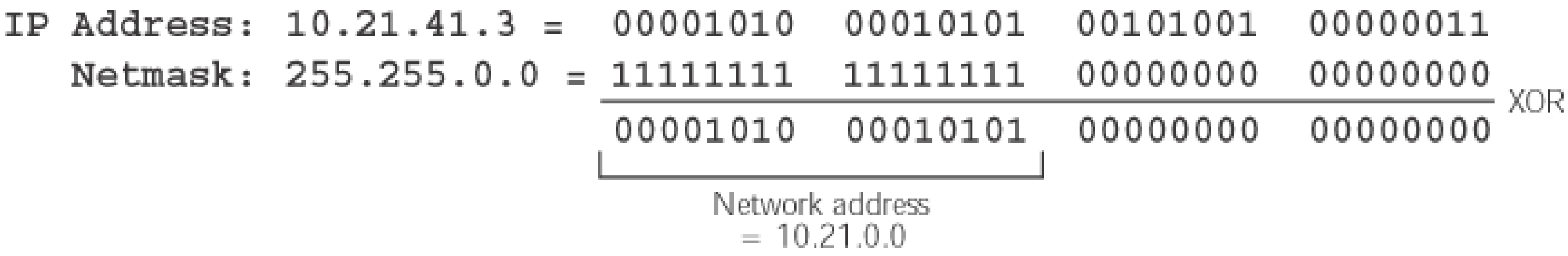


IP address in dotted-quad notation

The same IP address in binary

10.21.41.3 = 00001010 00010101 00101001 00000011

Figure 2.13



```
IP Address: 10.21.41.3 =  00001010  00010101  00101001  00000011
   Netmask: 255.255.0.0 = 11111111  11111111  00000000  00000000   XOR
                          00001010  00010101  00000000  00000000
```

Figure 2.14

Network Address Translation (NAT)

- Mapping IP addresses from private IP networks (10.x.y.z, 172.16.y.z, 192.168.y.z) to a single external routable IP address
- Helps hide internal network's address usage

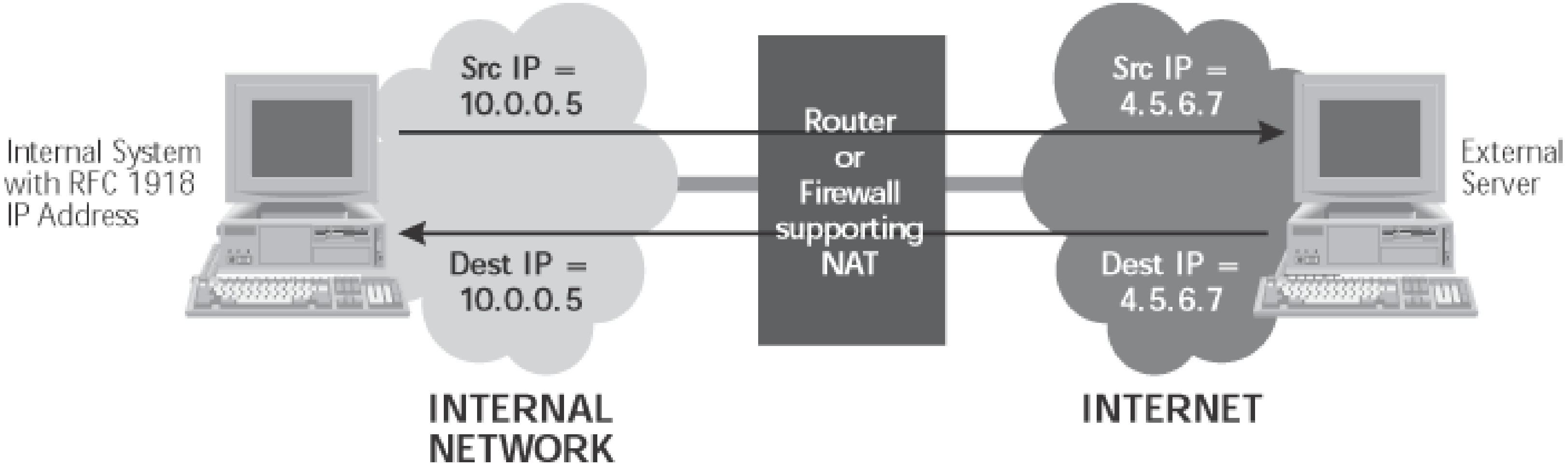


Figure 2.15

Firewalls

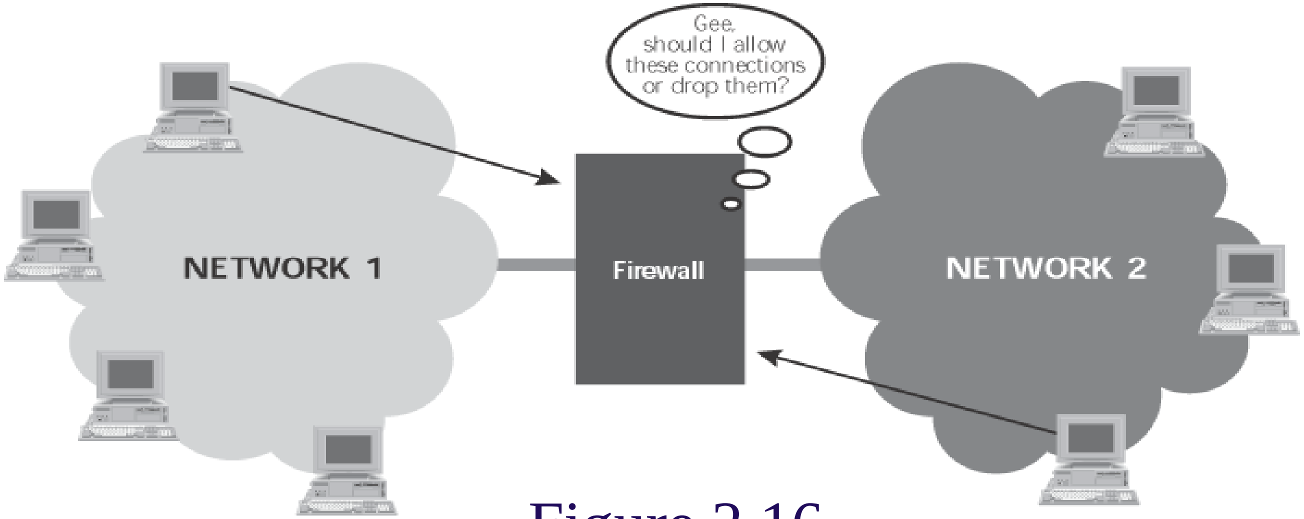


Figure 2.16

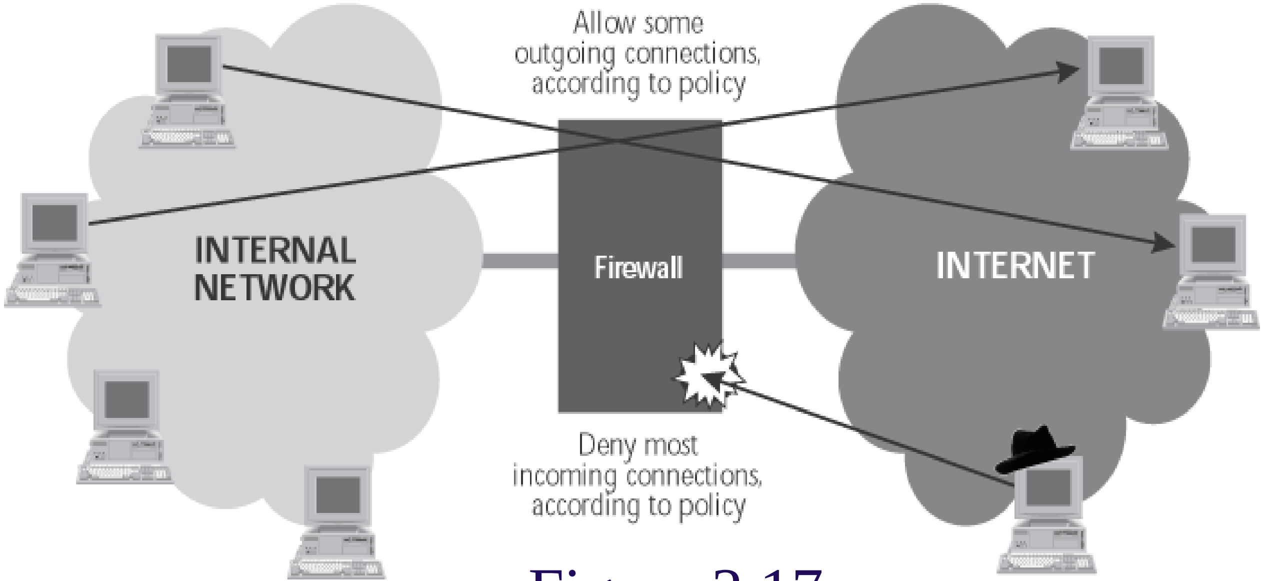

Allow some outgoing connections, according to policy
INTERNAL NETWORK
Firewall
INTERNET
Deny most incoming connections, according to policy

Figure 2.17

Firewall Technologies

- Traditional packet filters
- Stateful packet filters
- Proxy-based firewalls

Traditional Packet Filters

- Implemented on routers or firewalls
- Packet forwarding criteria
  - Source IP address
  - Destination IP address
  - Source TCP/UDP port
  - Destination TCP/UDP port
  - TCP code bits eg. SYN, ACK
  - Protocol eg. UDP, TCP
  - Direction eg. Inbound, outbound
  - Network interface

Stateful Packet Filters

- Keep tracks of each active connection via a state table
  - Monitoring of SYN code bits
  - Content of state table (source & destination IP address and port# , timeout)
- Basis of packet forwarding decision
  - State table
  - rule set
- ACK packets may be dropped if there was no associated SYN packet in state table
- May remember outgoing UDP packets to restrict incoming UDP packets to replies
- More intelligent but slower than traditional packet filters

Proxy-based Firewall

- Client interacts with proxy
- Proxy interacts with server on behalf of client
- Proxy can authenticate users via userid/password
- Web, telnet, ftp proxies
- Can allow or deny application-level functions eg. ftp put/get
- Caching capability in web proxies
- Slower than packet-filter firewalls

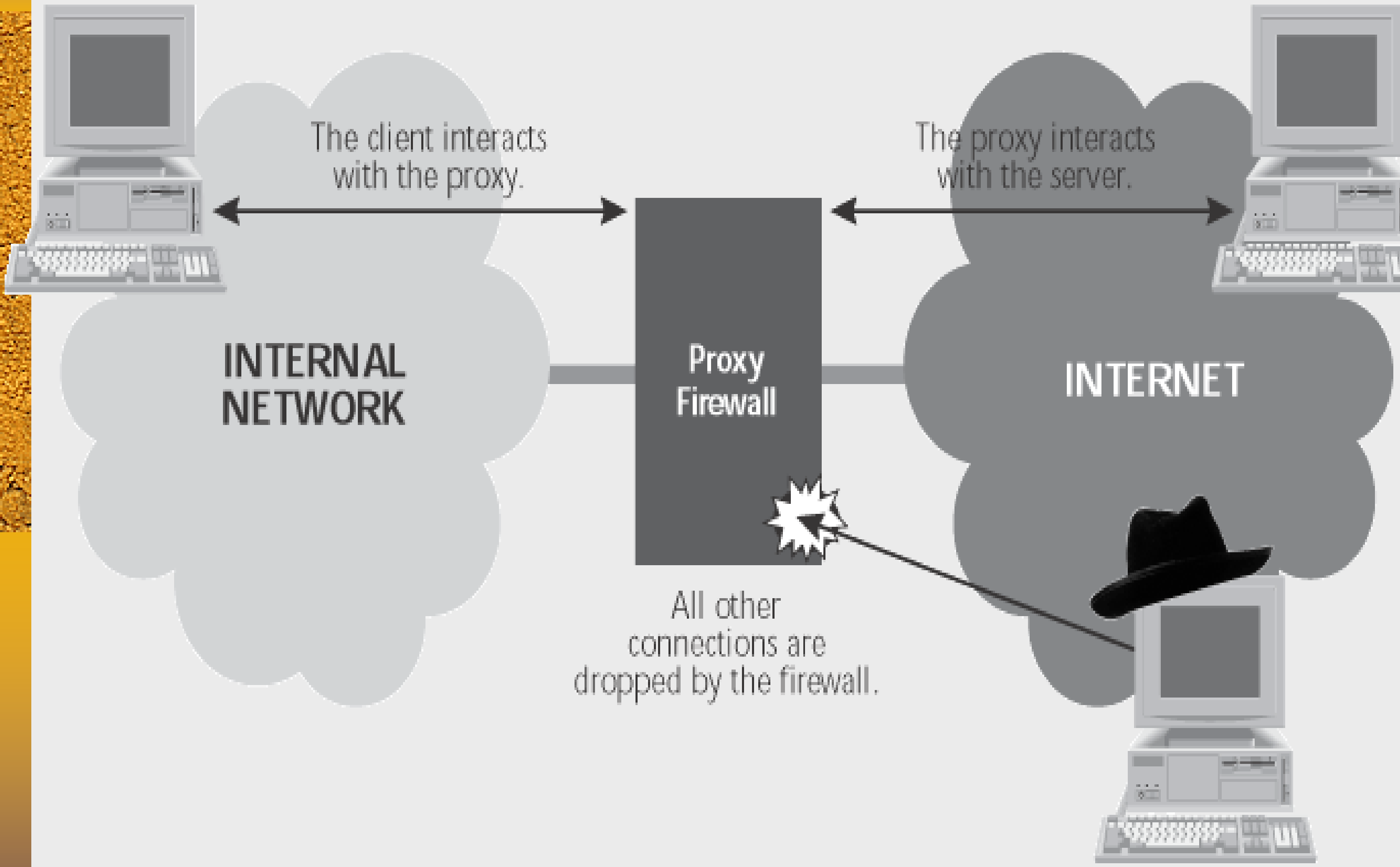

The client interacts with the proxy.
The proxy interacts with the server.
INTERNAL NETWORK
Proxy Firewall
INTERNET
All other connections are dropped by the firewall.

Figure 2.18 Proxy-based firewall with application-level controls

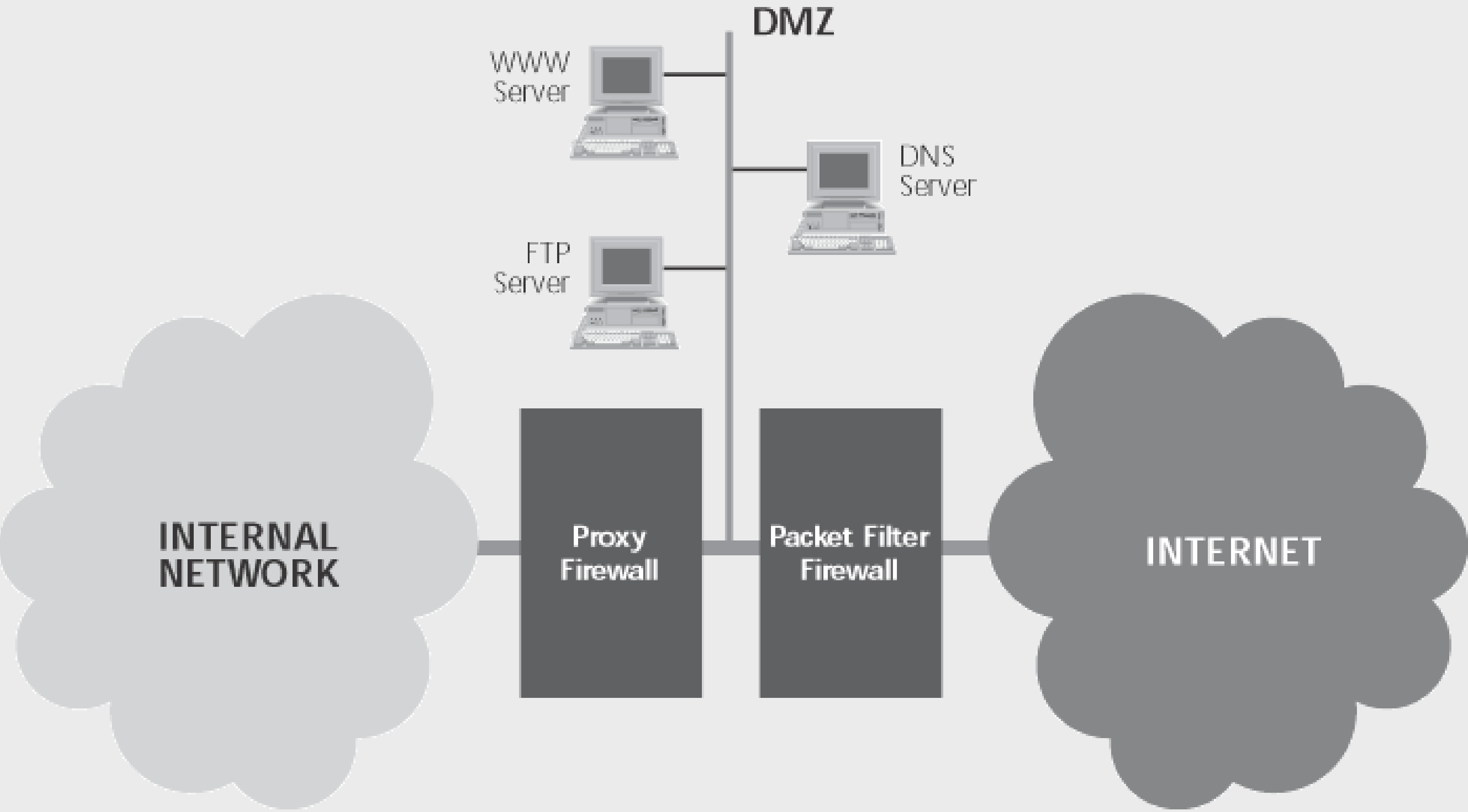


Figure 2.19 Using proxy and stateful packet filter firewalls

Personal Firewalls

- Installed on personal computers
- Eg. Zone Alarm, Black Ice
- Filter traffic going in and out of a machine
- Usually cannot detect viruses or malicious programs

Address Resolution Protocol (ARP) and Vulnerability to Spoofing

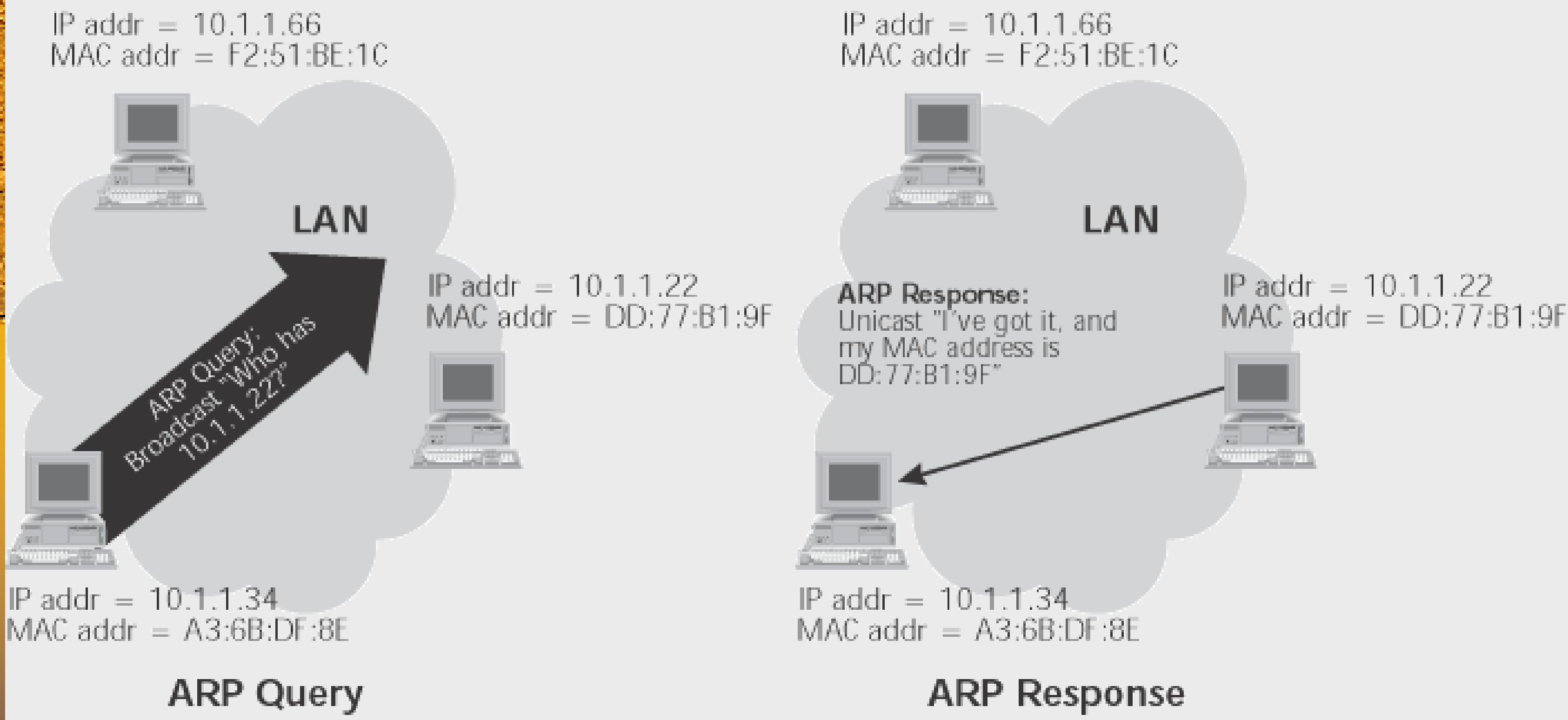
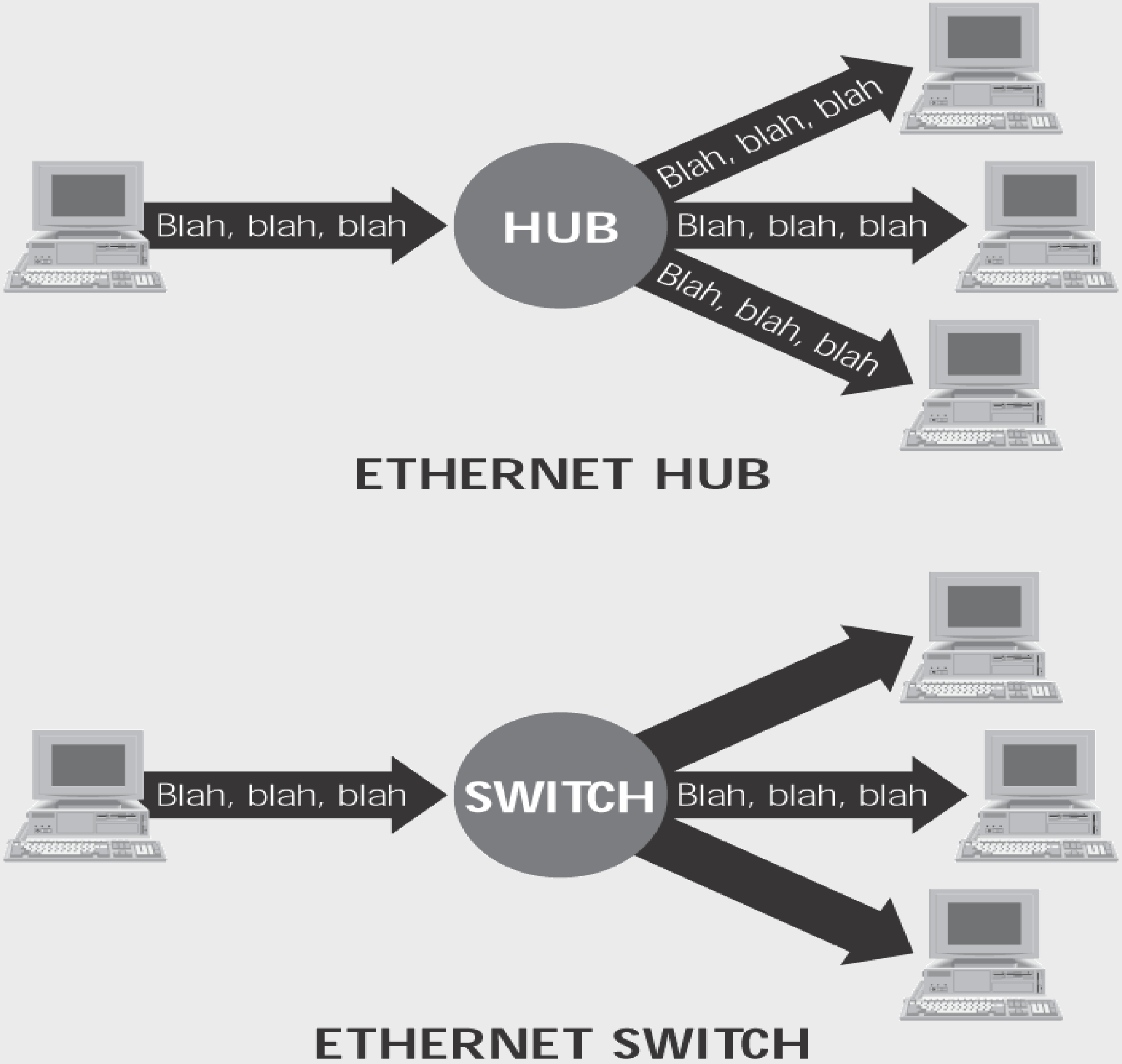


Figure 2.20 ARP

Hubs vs. Switches



Security Solutions for Networks

- Application-Layer Security
- Secure Sockets Layer (SSL)
- Internet Protocol Security (IPSec)

Application-Layer Security Tools

- Pretty Good Privacy (PGP) , Gnu Privacy Guard (GnuPG)
  - used to encrypt and digitally sign files for file transfer and email
- Secure/Multipurpose Internet Mail Extension (S/MIME)
  - Used to secure email at the application level
  - Supported by email clients such as MS Outlook and Netscape Messenger
- Secure Shell (SSH)
  - Provides remote access to a command prompt across a secure, encrypted session

Secure Socket Layer (SSL)

- Specification for providing security to TCP/IP applications at the socket layer.
- Allows an application to have authenticated, encrypted communications across a network
- Uses digital certificates to authenticate systems and distribute encryption keys
- Supports one-way authentication of server to client and two-way authentication
- Used by web browsers and web servers running HTTPS
- Layer 7 applications such as ftp and telnet can be modified to support SSL

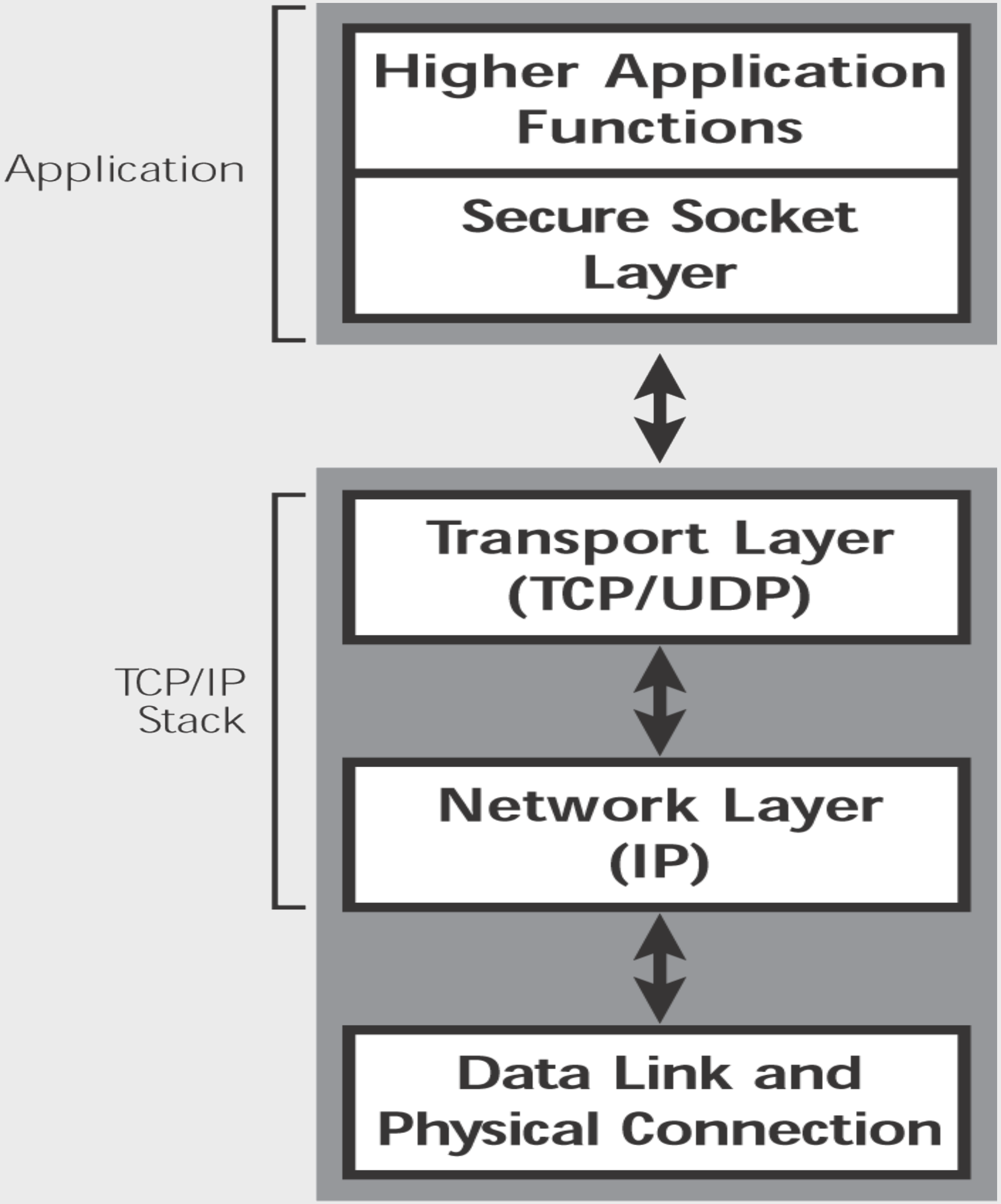

Application
Higher Application Functions
Secure Socket Layer
TCP/IP Stack
Transport Layer (TCP/UDP)
Network Layer (IP)
Data Link and Physical Connection

Figure 2.23 client/server applications modified to support SSL

IP Security (IPSec)

- Defined in RFCs 2401 to 2412
- Runs at IP layer software version 4 & 6
- Offers authentication of data source, confidentiality, data integrity, and protection against replays.
- Comprised of Authentication Header (AH) and Encapsulating Security Payload(ESP), which can be used together or separately
- Client/server must run compatible versions of IPSec