ETSF10 Part 3
Lect 2

DHCP, DNS, Security

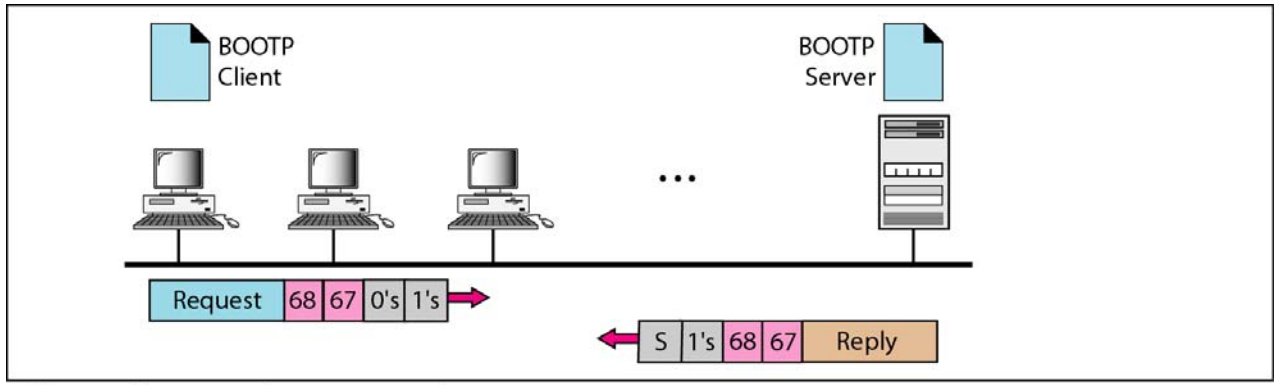
Jens A Andersson

Electrical and Information Technology

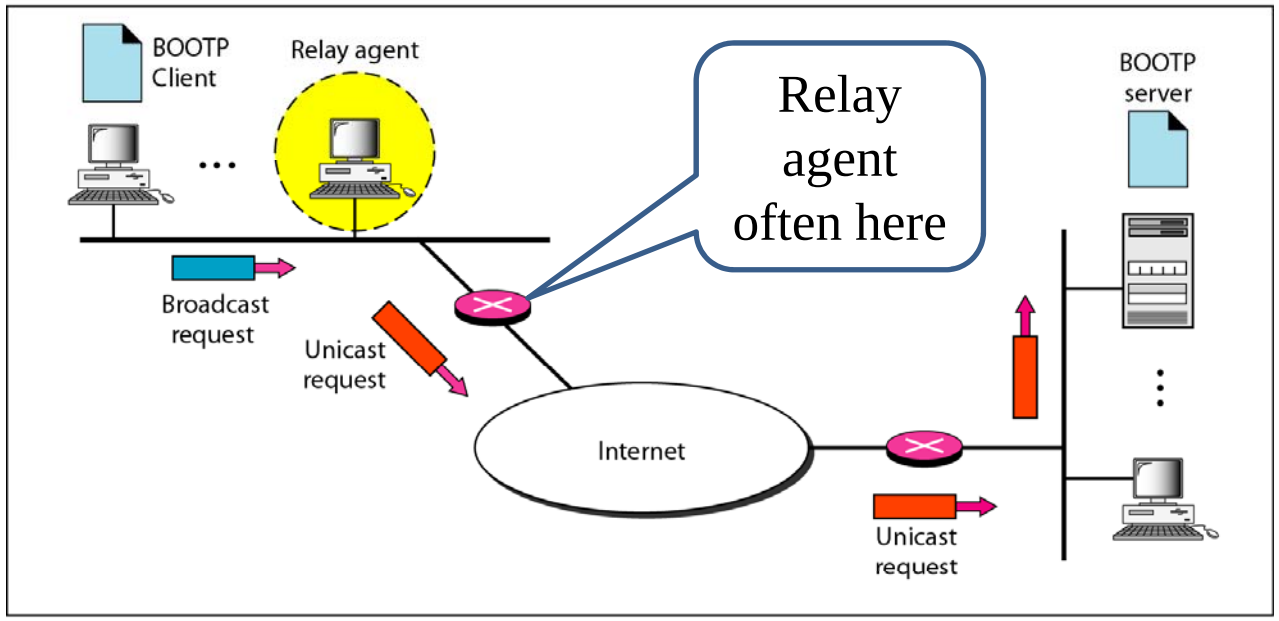
DHCP

- Dynamic Host Configuration Protocol
  - bootp is predecessor
- Alternative: manual configuration
  - IP address
  - Net mask
  - Default gateway
  - DNS server(s)

Figure 21.7 *BOOTP client and server on the same and different networks*



a. Client and server on the same network



b. Client and server on different networks

Figure 18.3 *Use of UDP ports*

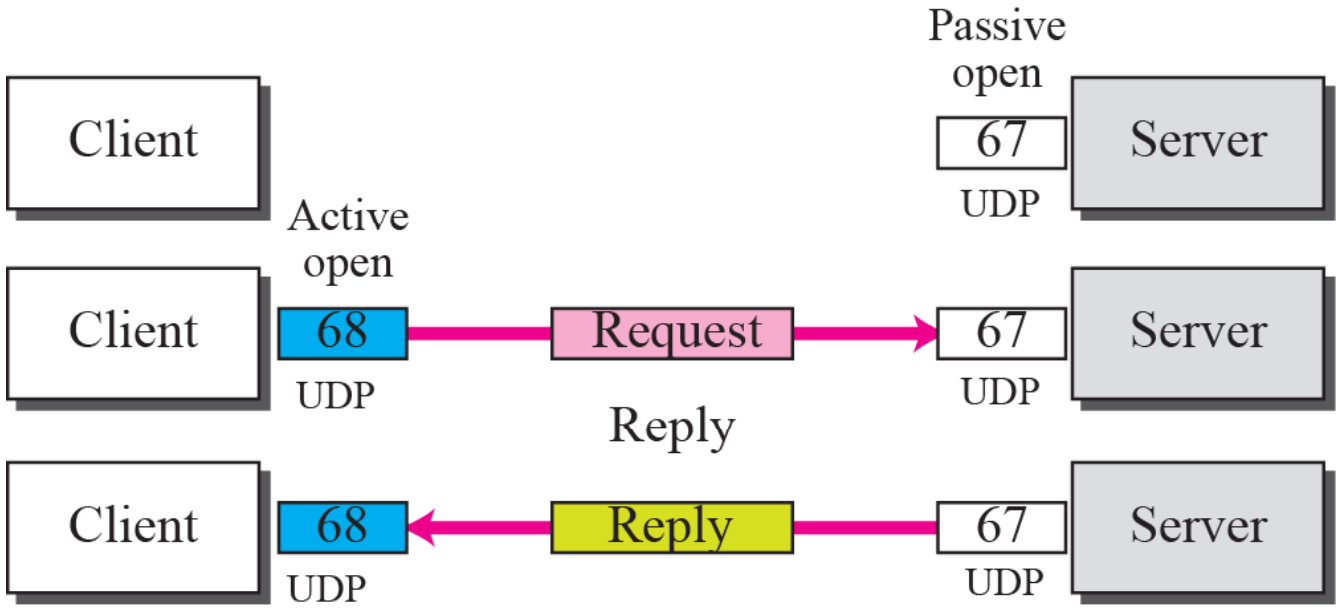
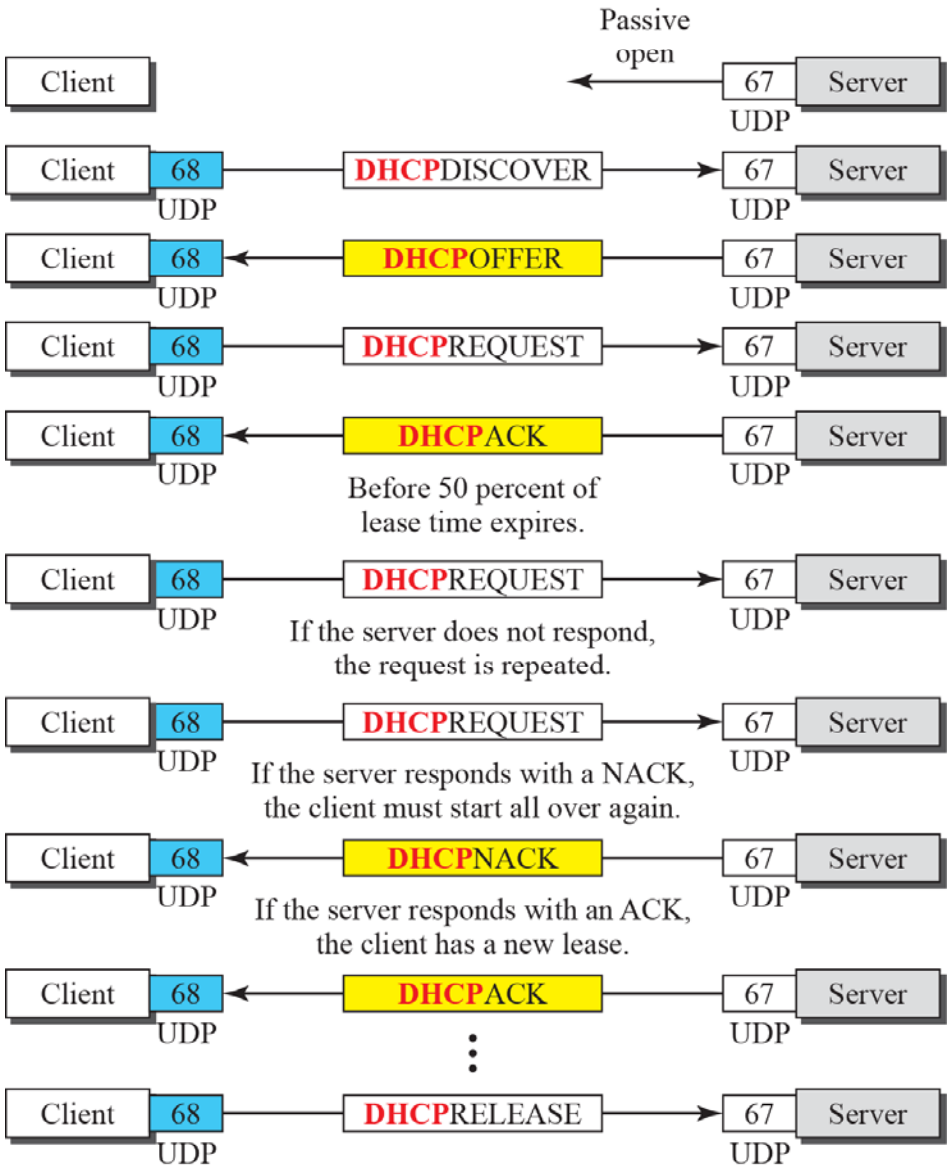


Figure 18.9 *Exchanging messages*



DHCP address allocation

- Static
  - Static mapping MAC – IP address
  - Client always get the same IP address
  - Used in clients home network
- Dynamic
  - Client gets IP address from pool
  - Used in open networks

DNS

- Domain Name System/Service
- Internets telephone book?
- ”Name to Number”
- ”Number to Name”
- Mail to which server
- Who’s responsible
- More …

Figure 25.1 *Example of using the DNS service*

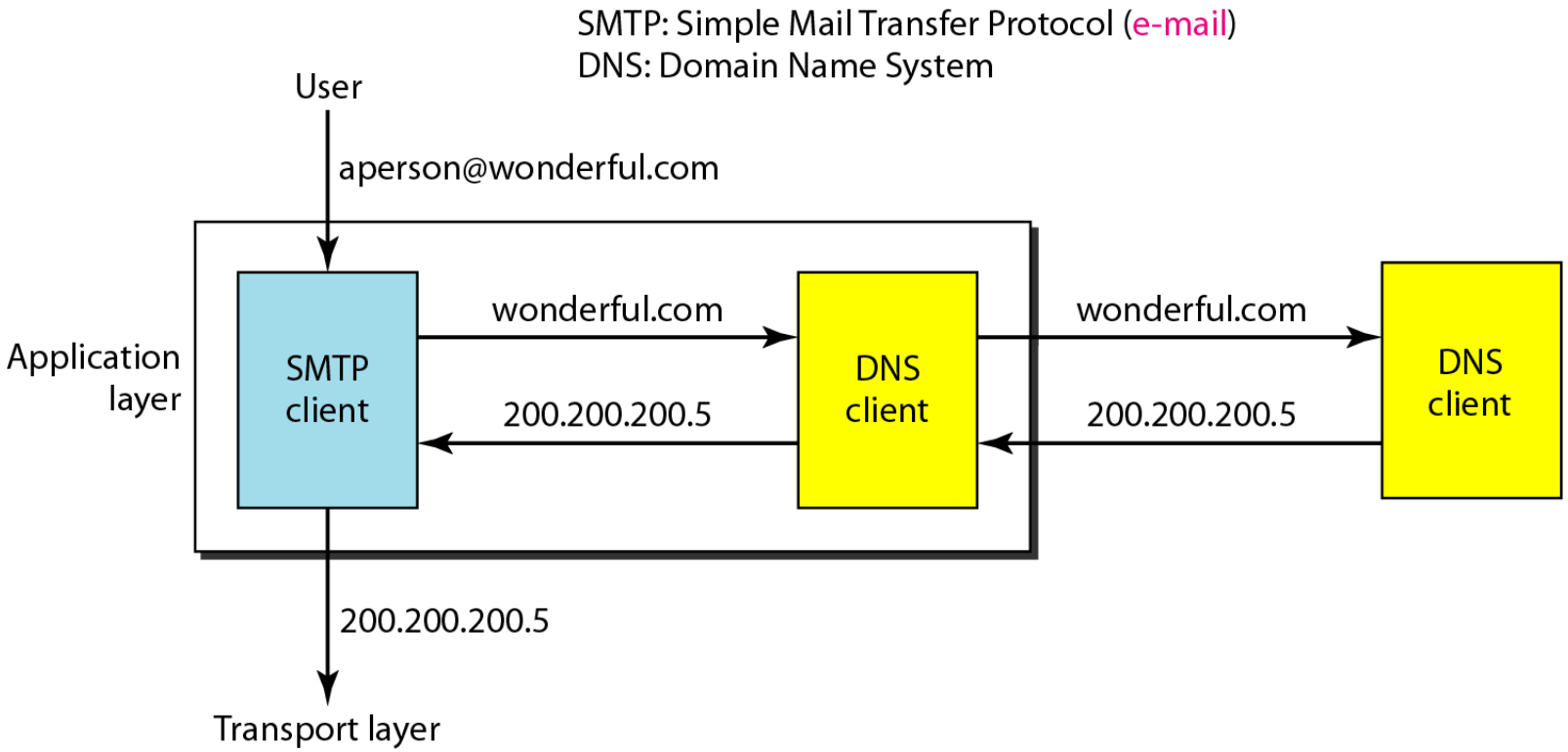


Figure 25.2 *Domain name space*

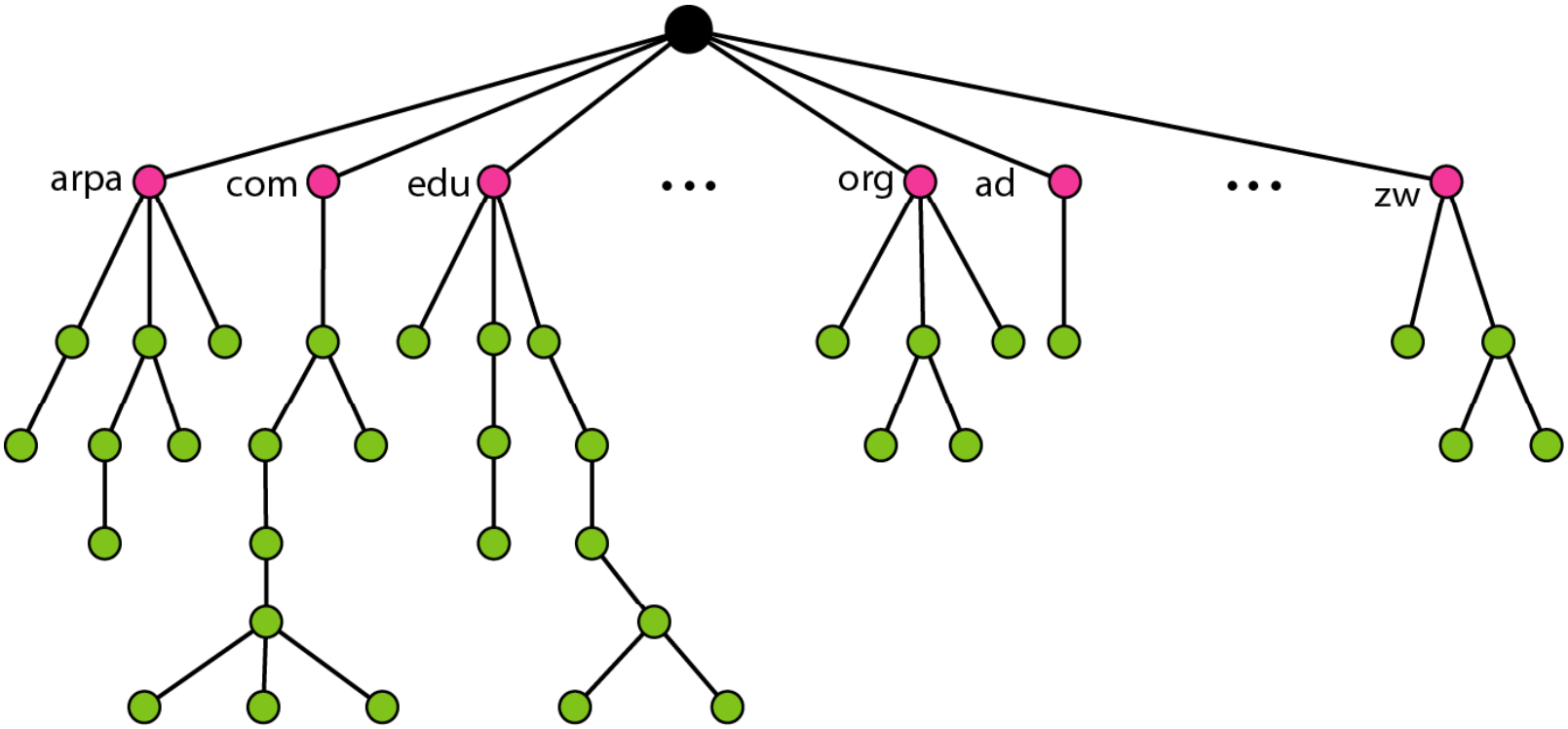


Figure 25.8 *DNS IN THE INTERNET*

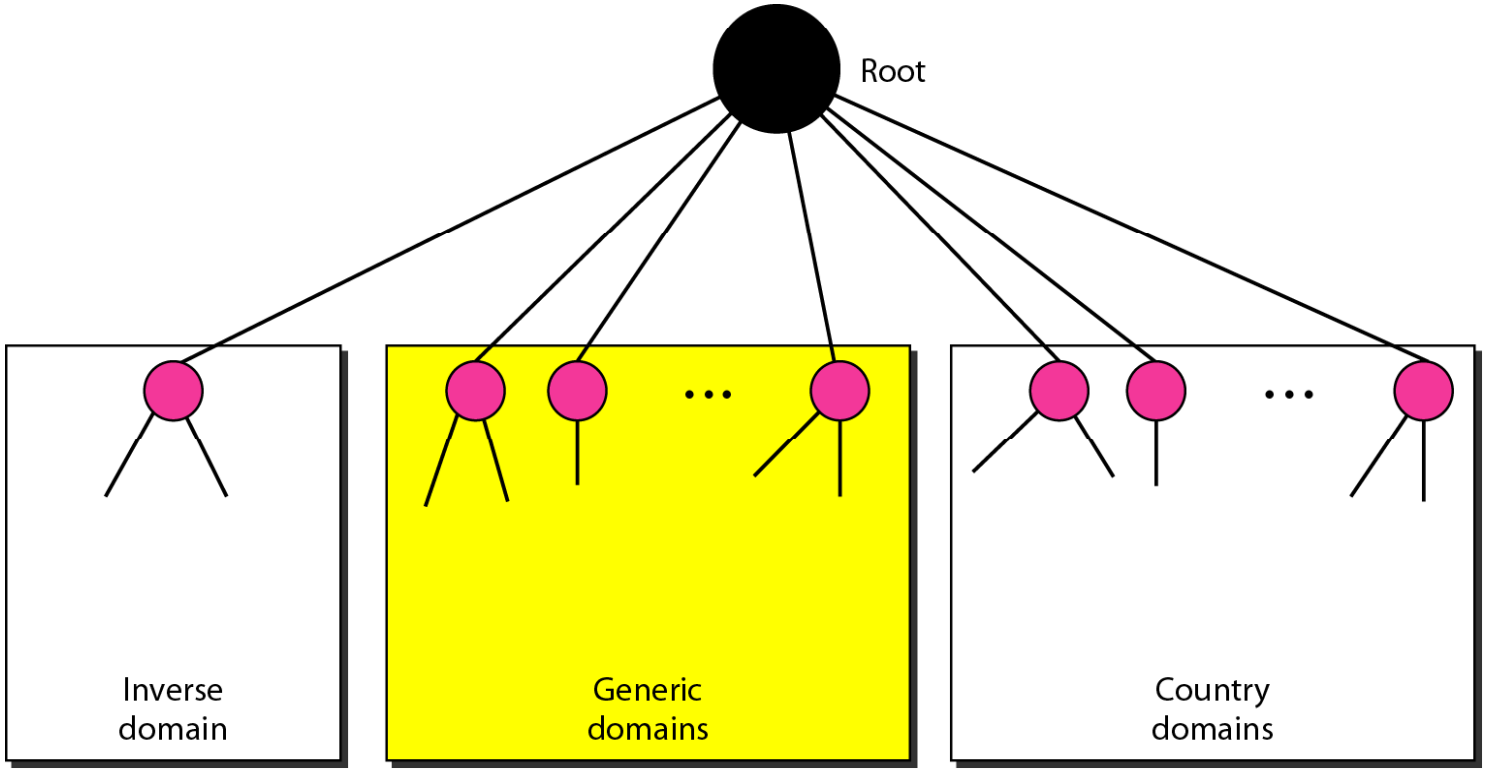


Figure 25.9 *Generic domains*

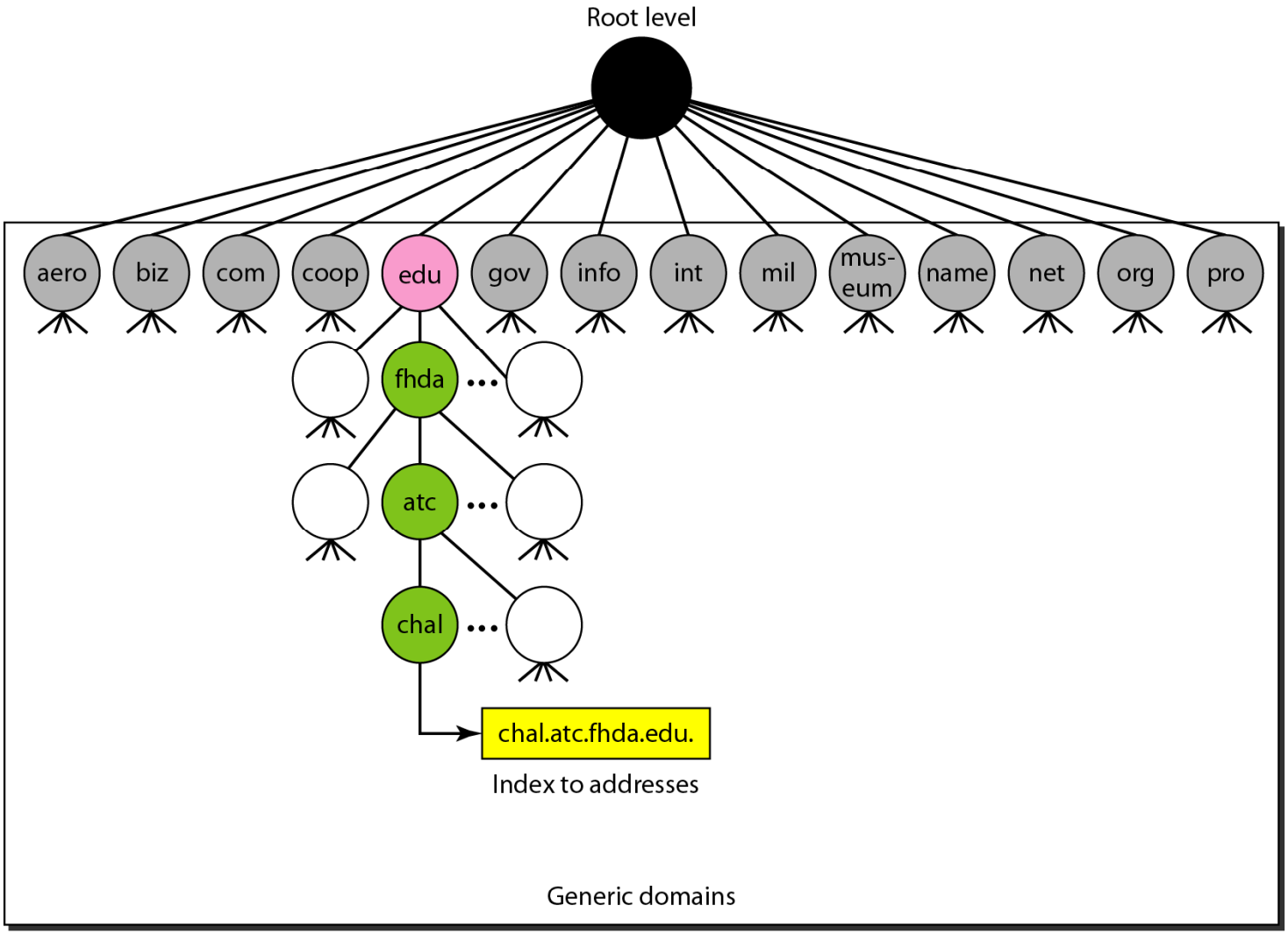
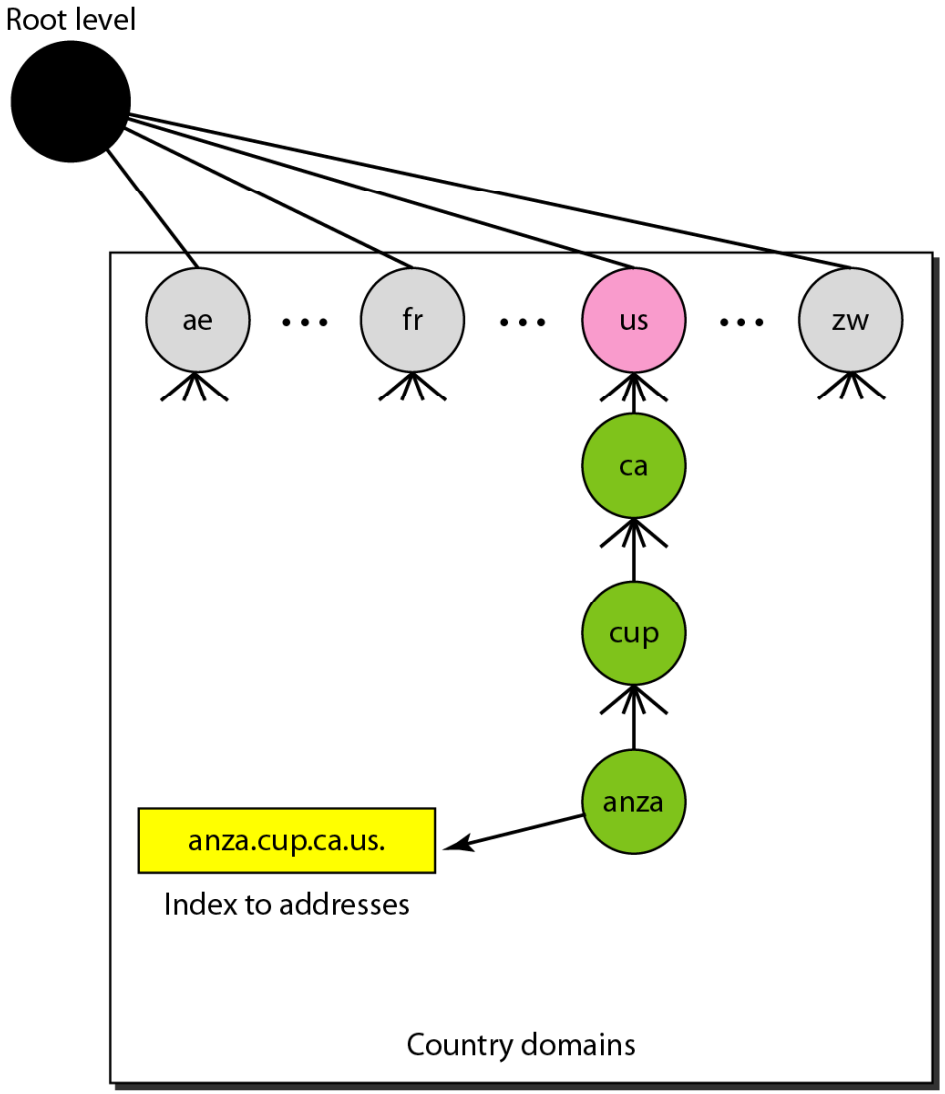


Table 25.1 *Generic domain labels*

Label	*Description*
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other nonprofit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

Figure 25.10 *Country domains*



Country domain

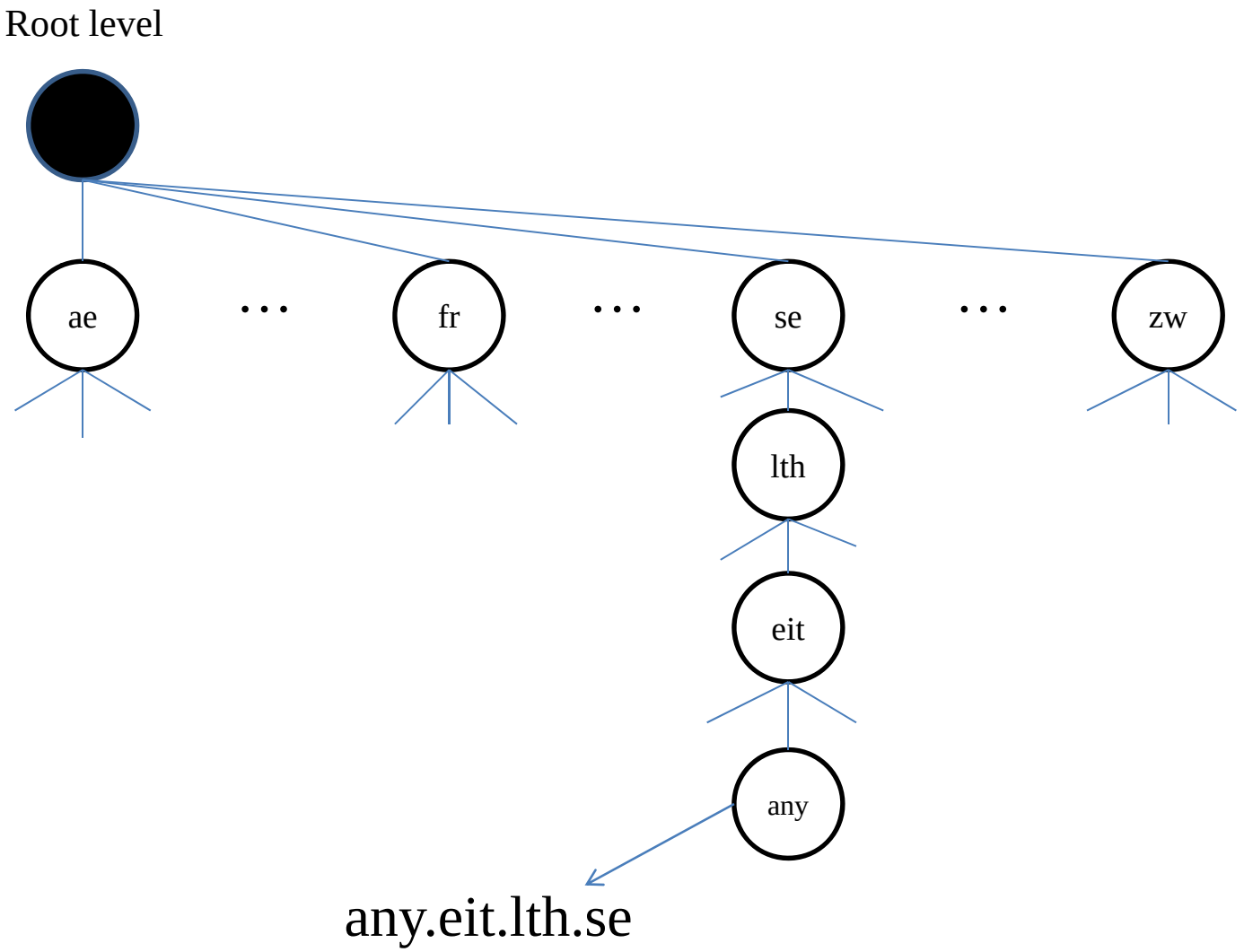


Figure 25.11 *Inverse domain*

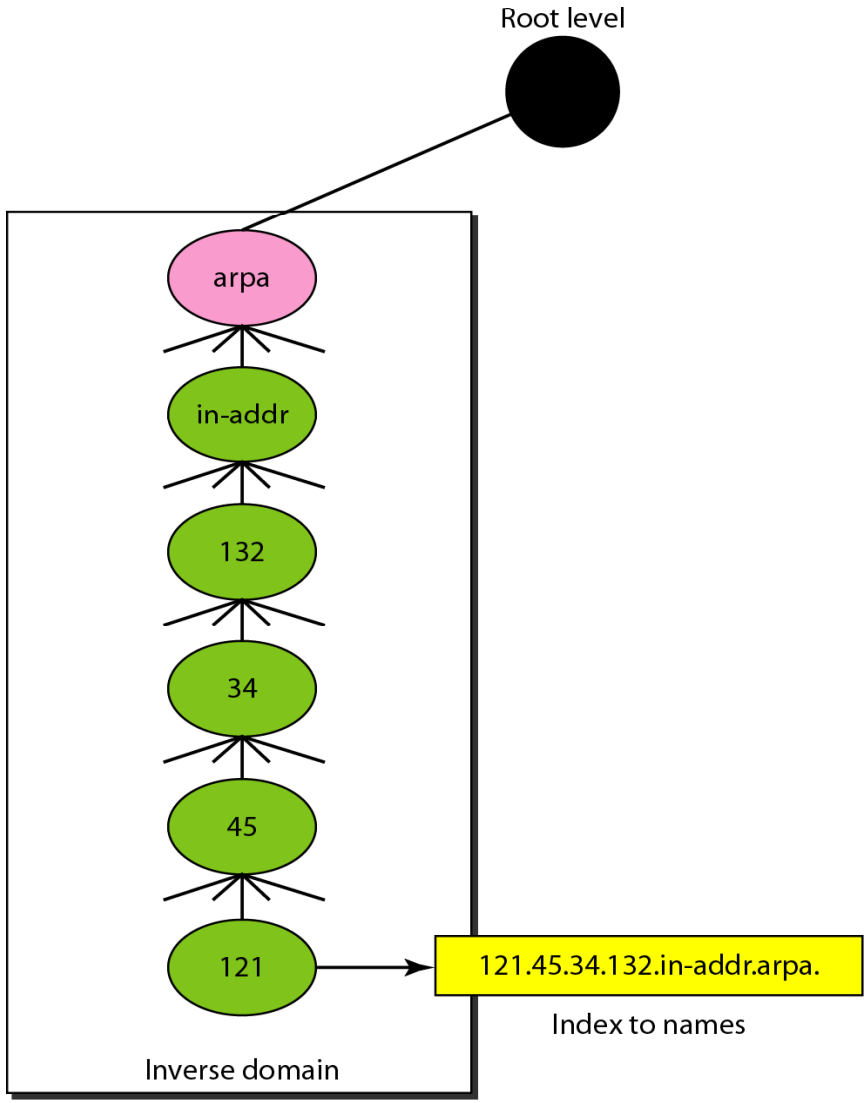


Figure 25.3 *Domain names and labels*

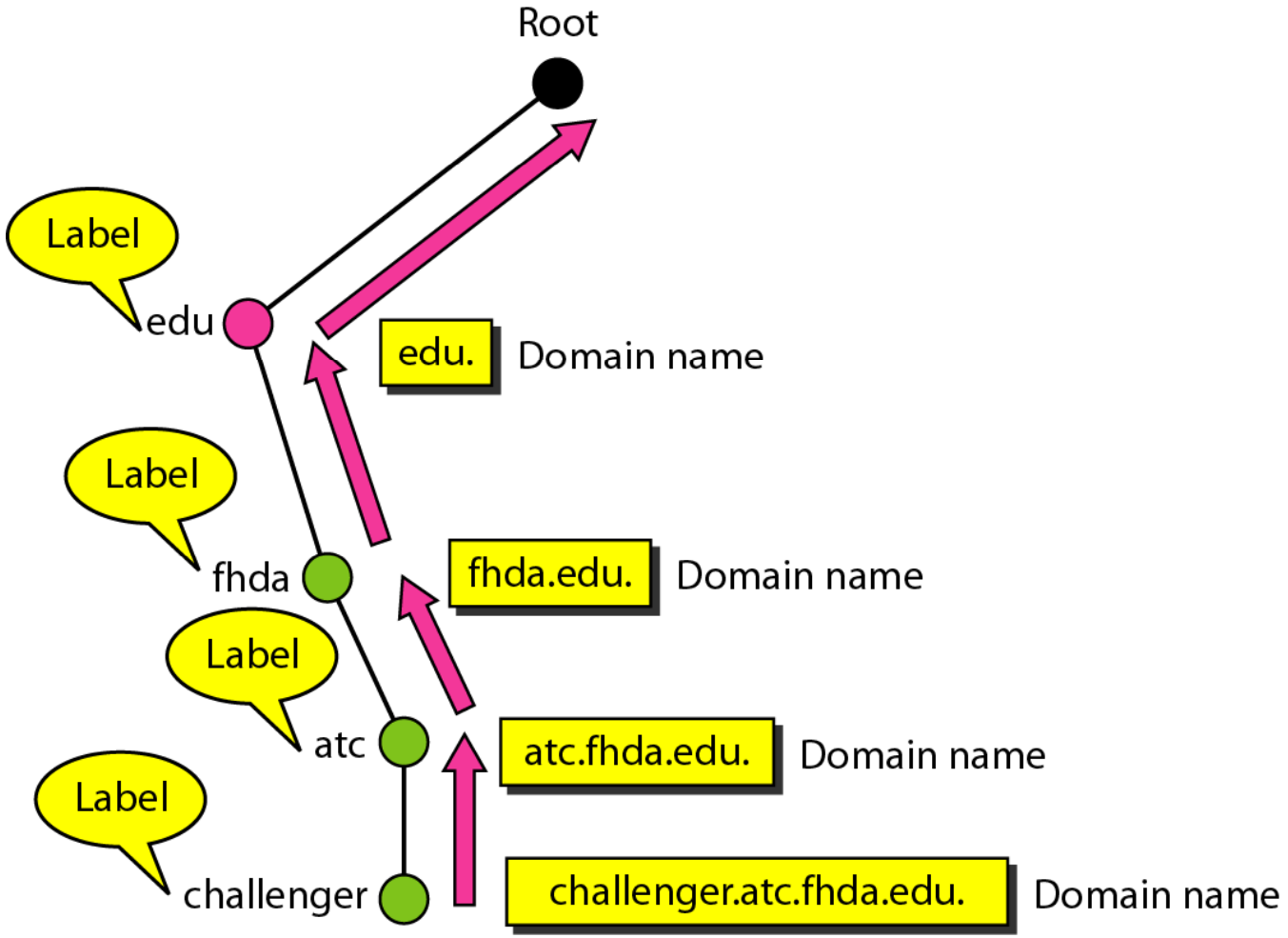
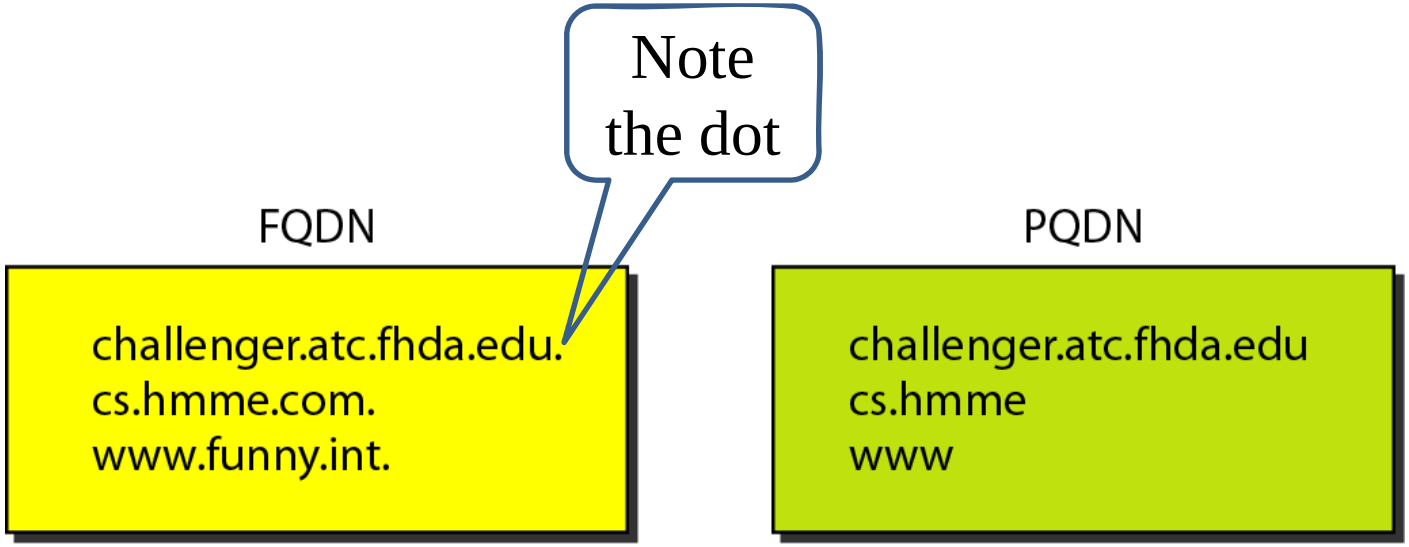


Figure 25.4 *FQDN and PQDN*



- FQDN = Fully Qualified Domain Name
- PQDN = Partially Qualified Domain Name

Figure 25.5 *Domains*

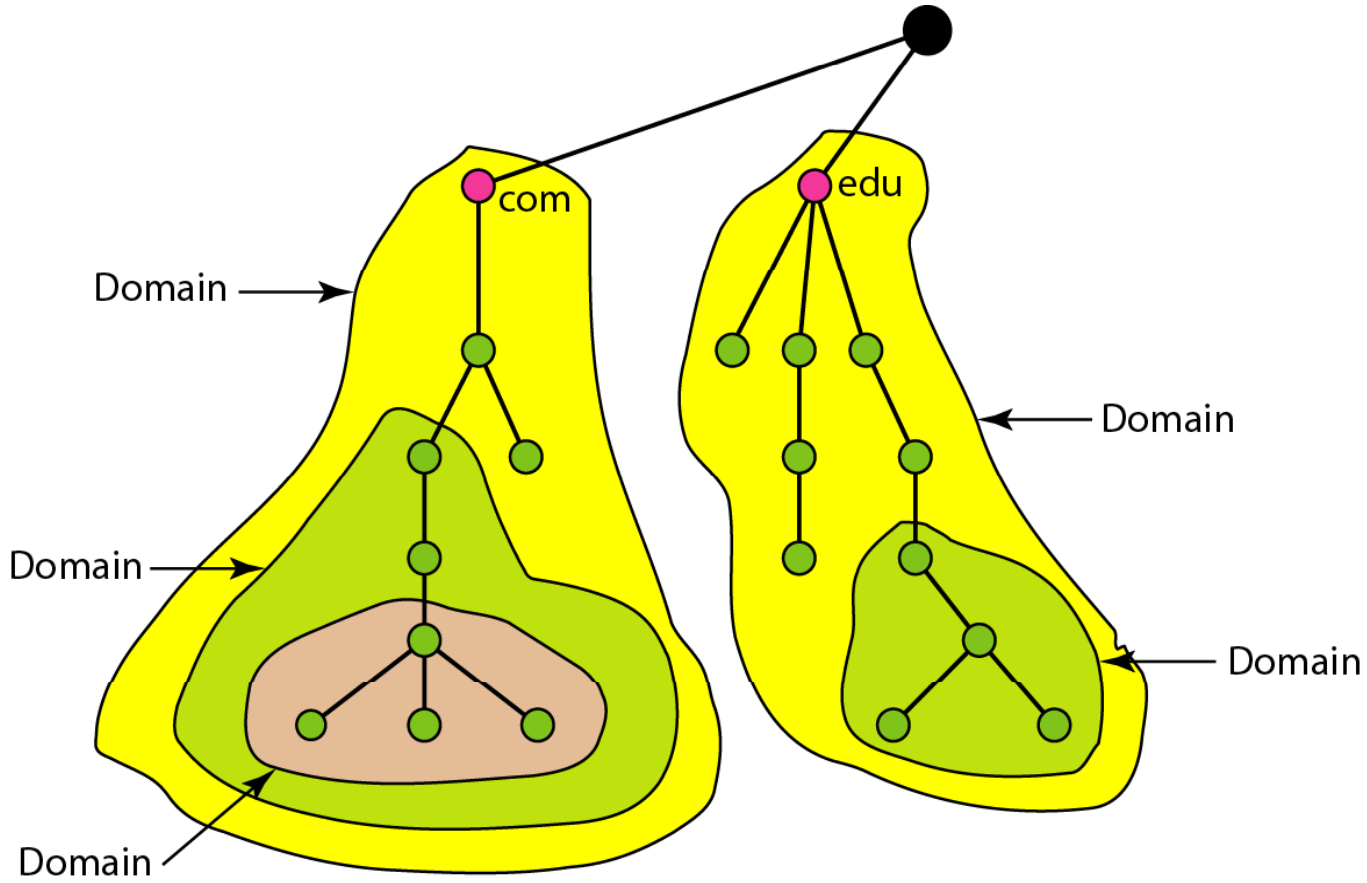


Figure 25.7 *Zones and domains*

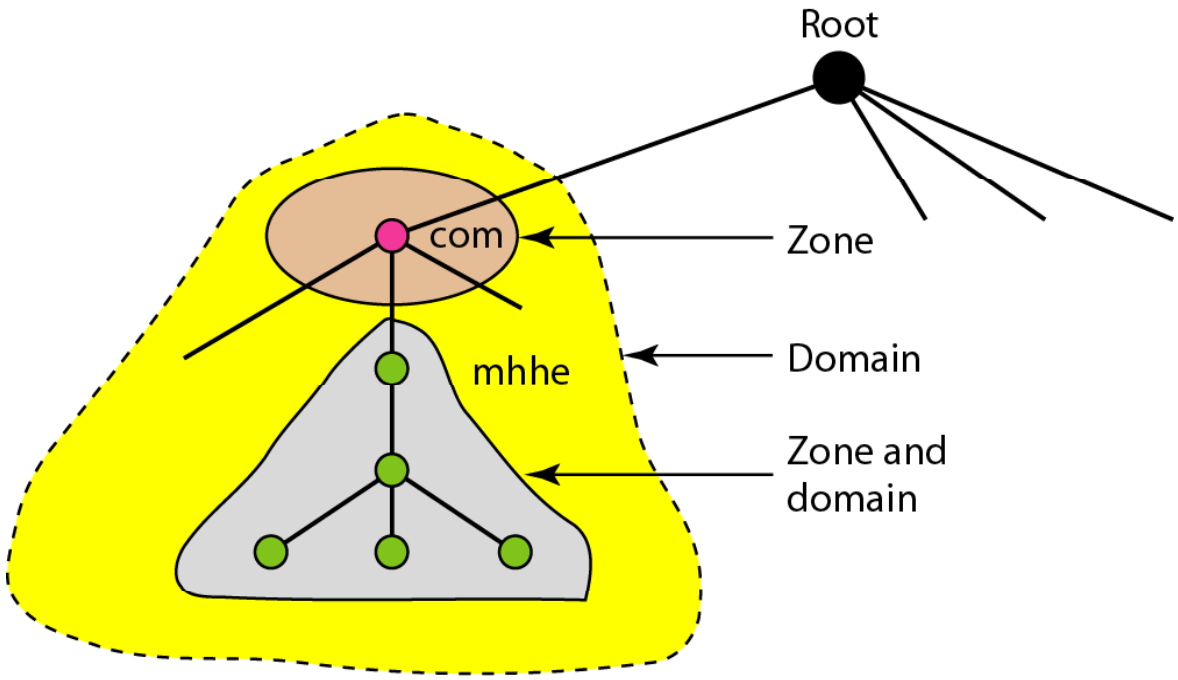


Figure 25.6 *Hierarchy of name servers*

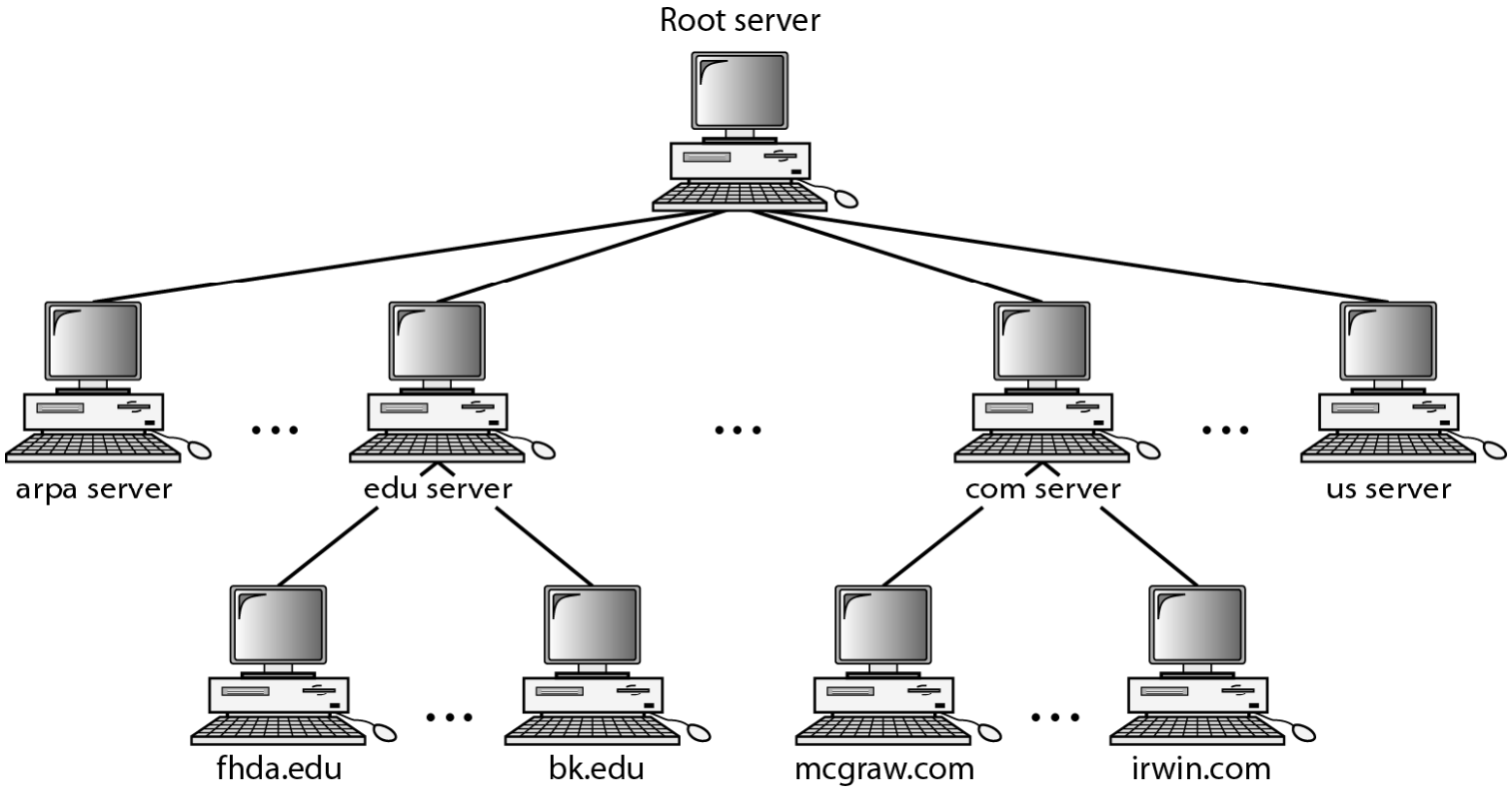


Figure 25.12 *Recursive resolution*

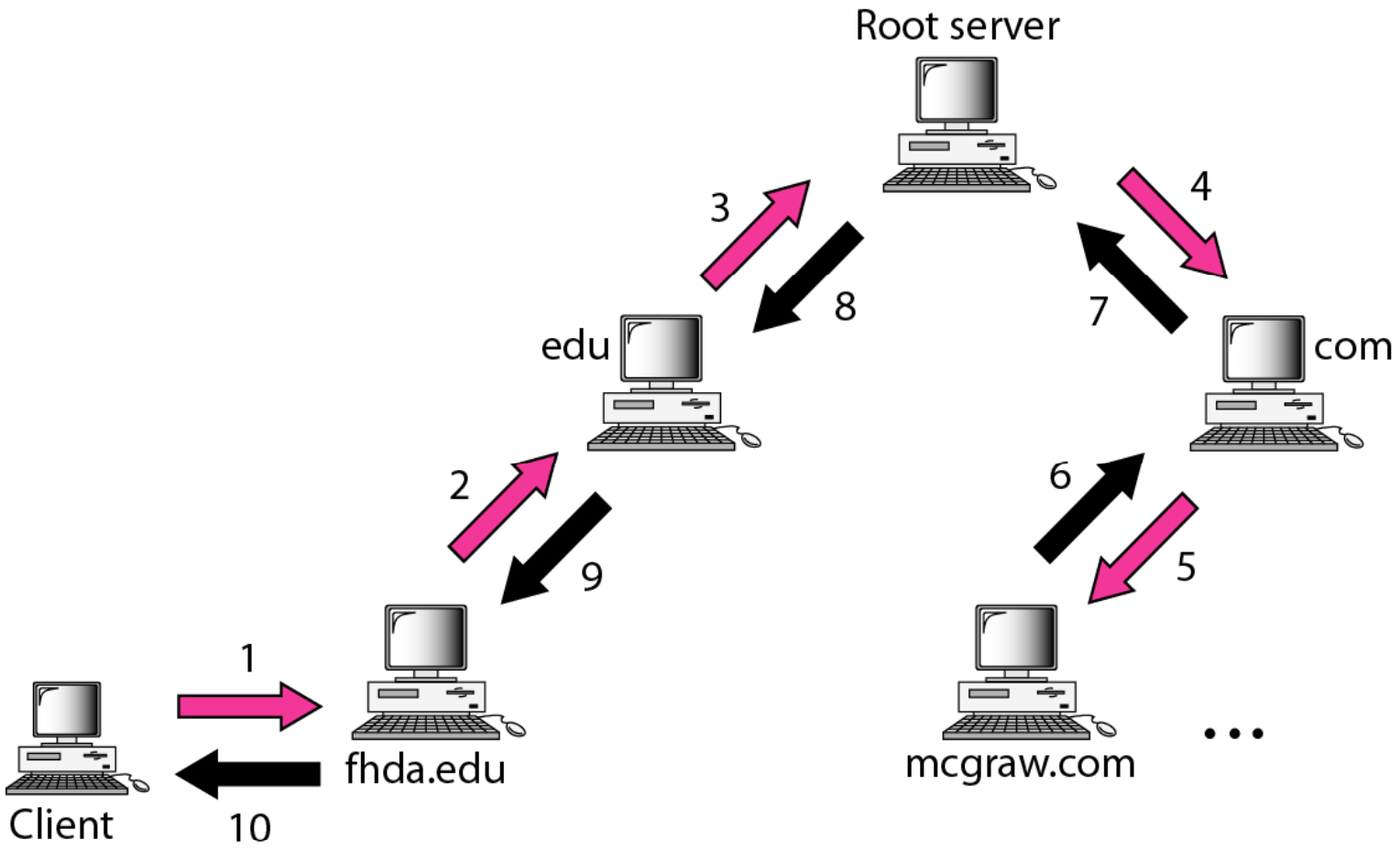
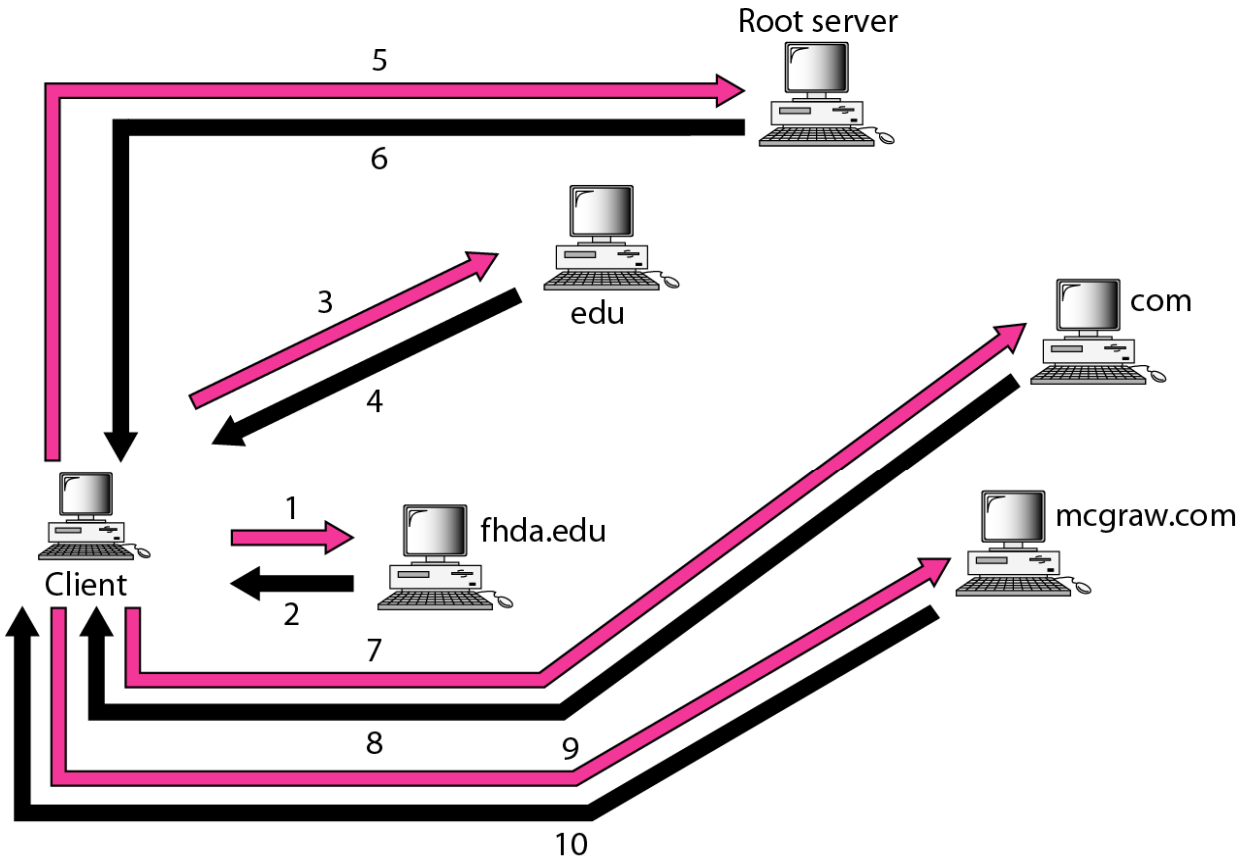


Figure 25.13 *Iterative resolution*

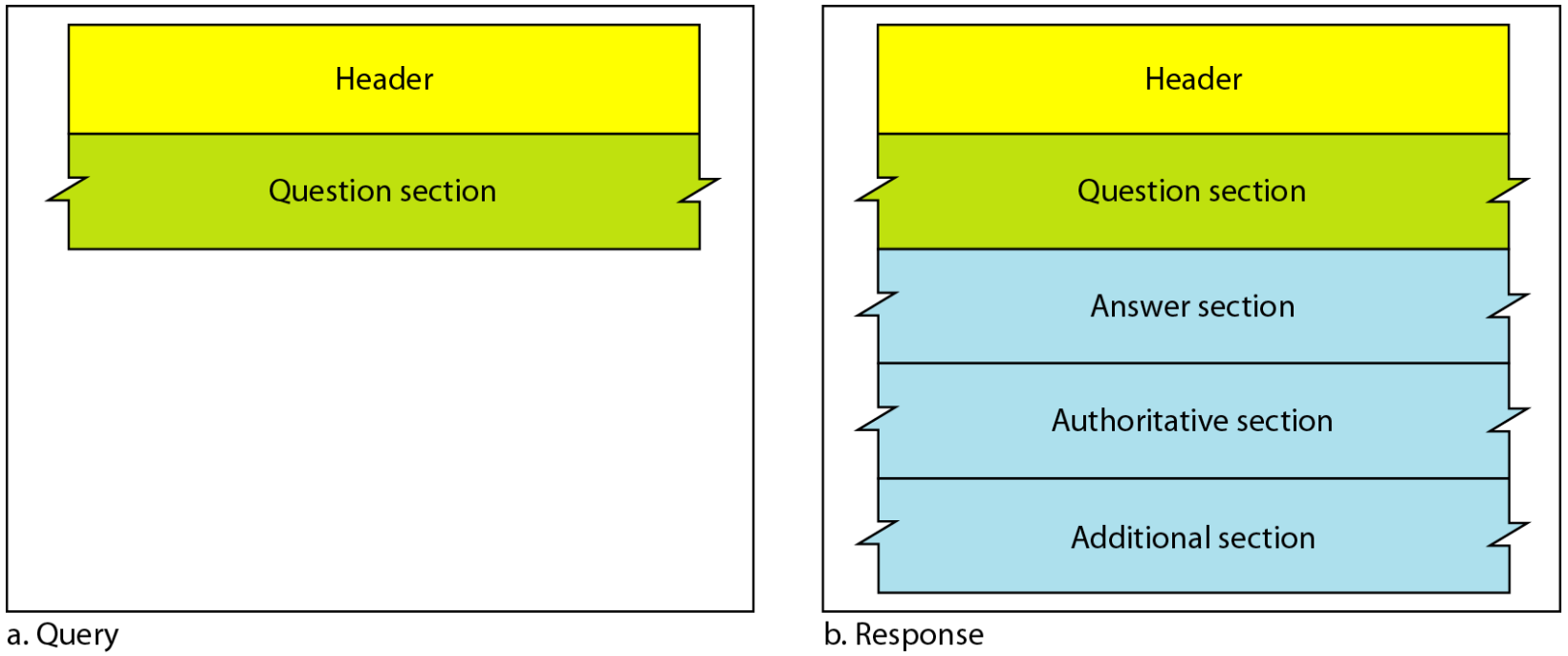


Caching

- Boost efficieny
  - Remember what you've learned
- Local host / client
- DNS servers

- (Zone transfer)
  - Request data of a zone
  - From primary to secondary DNS server

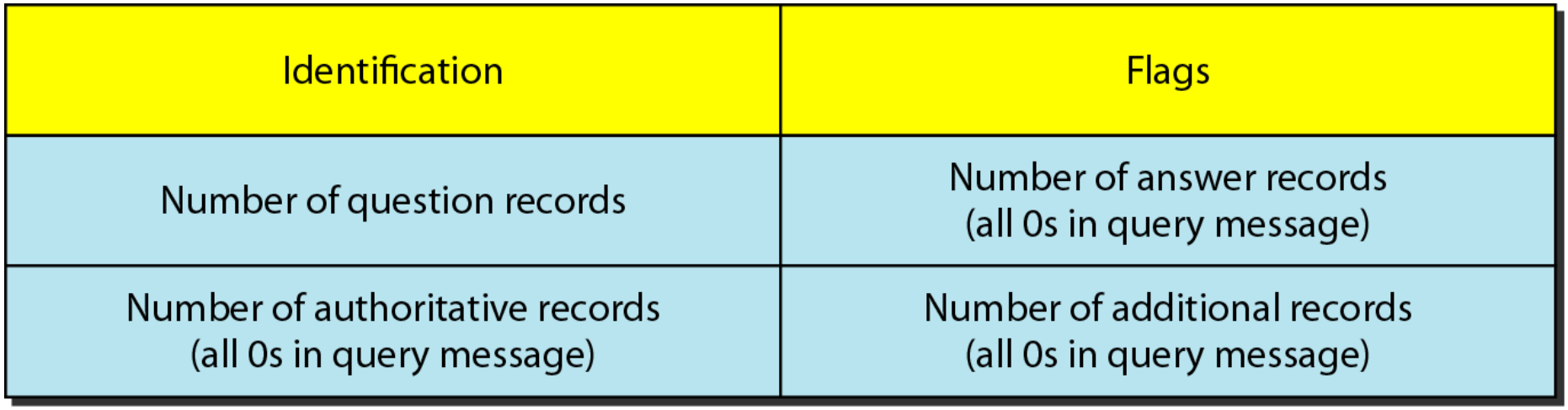
Figure 25.14 *Query and response messages*



a. Query

b. Response

Figure 25.15 *Header format*



Adding new domains

- Apply / Register by Regstrar
- Registrar:
  - Commercial entity (many)
  - Accredited by ICANN

DDNS

- Host may change IP address
- DHCP updates primary name server with new binding (IP address – Name)
- Authentication to update

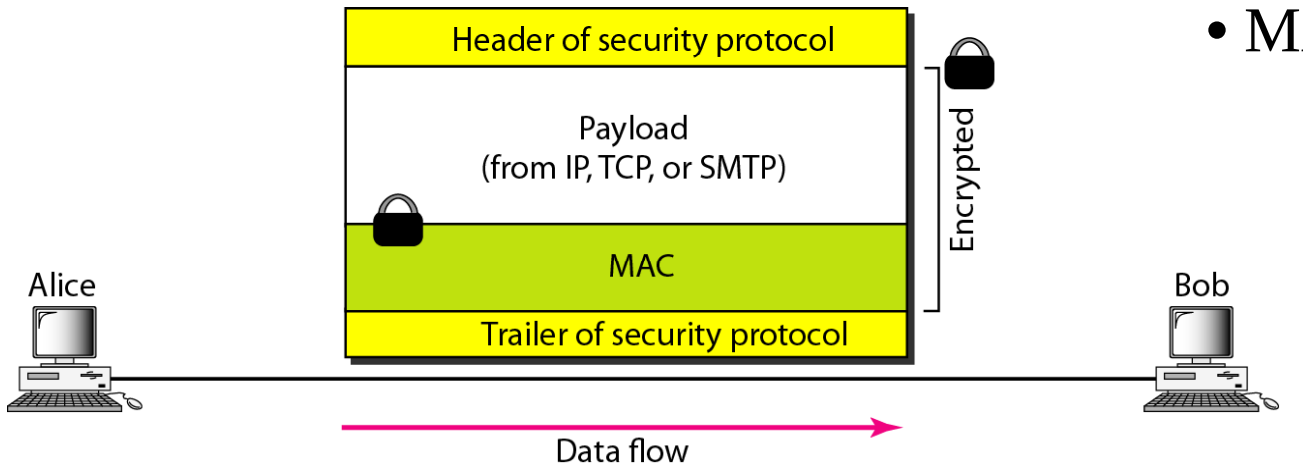
Encapsulation

- UDP
  - Message less than 512 bytes
- TCP
  - Message more than 512 bytes
  - Example: Zone transfer

IP Sec

- IP Security
- Collection of protocols
- Security for packets on network layer
  - Alternative: Security at
    - application layer
    - transport layer

Figure 32.1 *Common structure of three security protocols*



Normally two keys
- Payload
- MAC

MAC = Message Authentication Code

Figure 32.2 *TCP/IP protocol suite and IPSec*

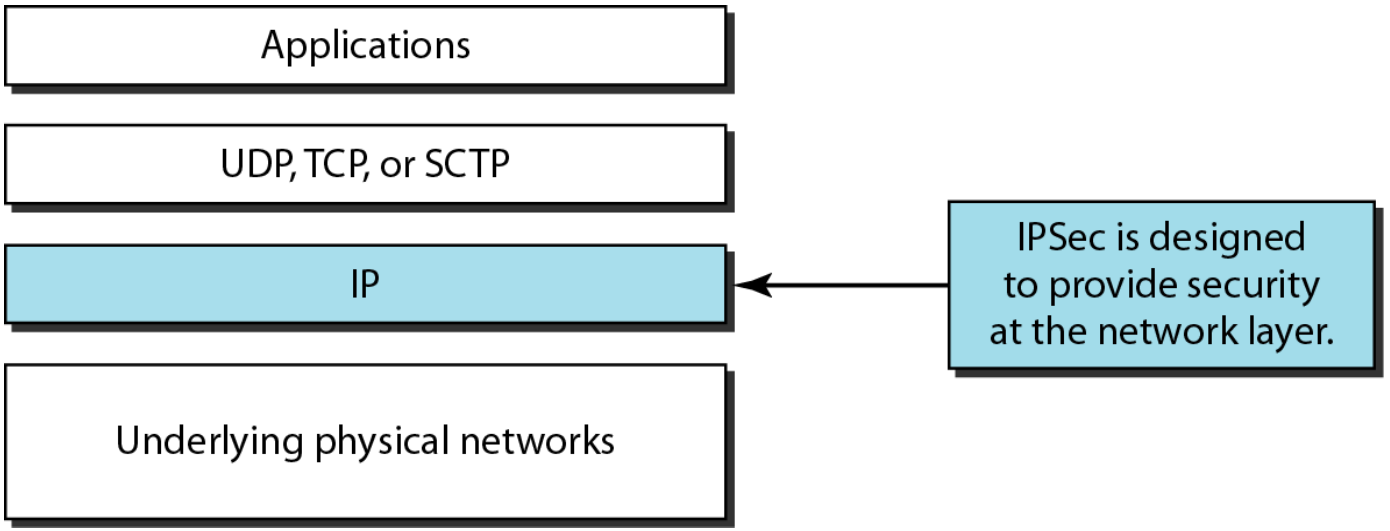


Figure 32.3 *Transport mode and tunnel modes of IPSec protocol*

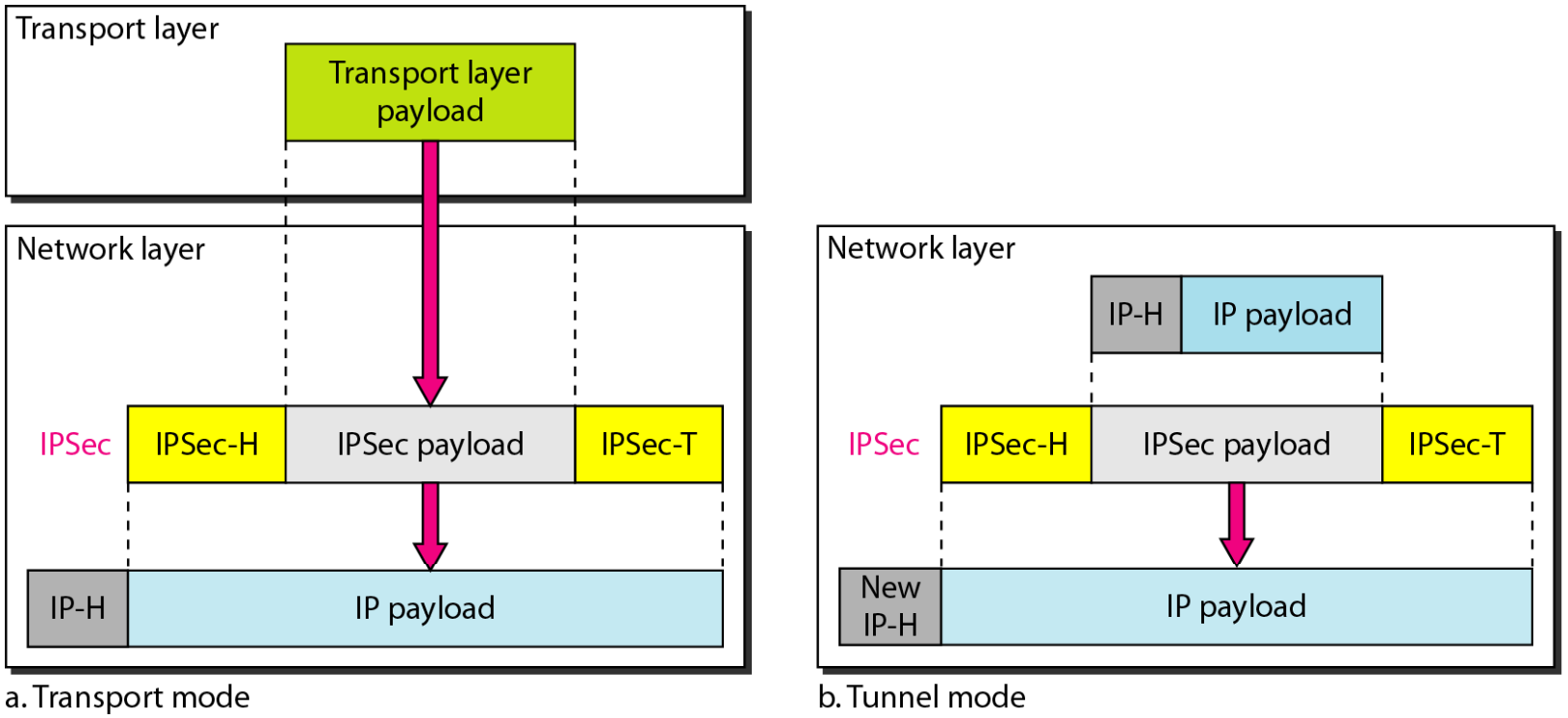


Figure 32.4 *Transport mode in action*

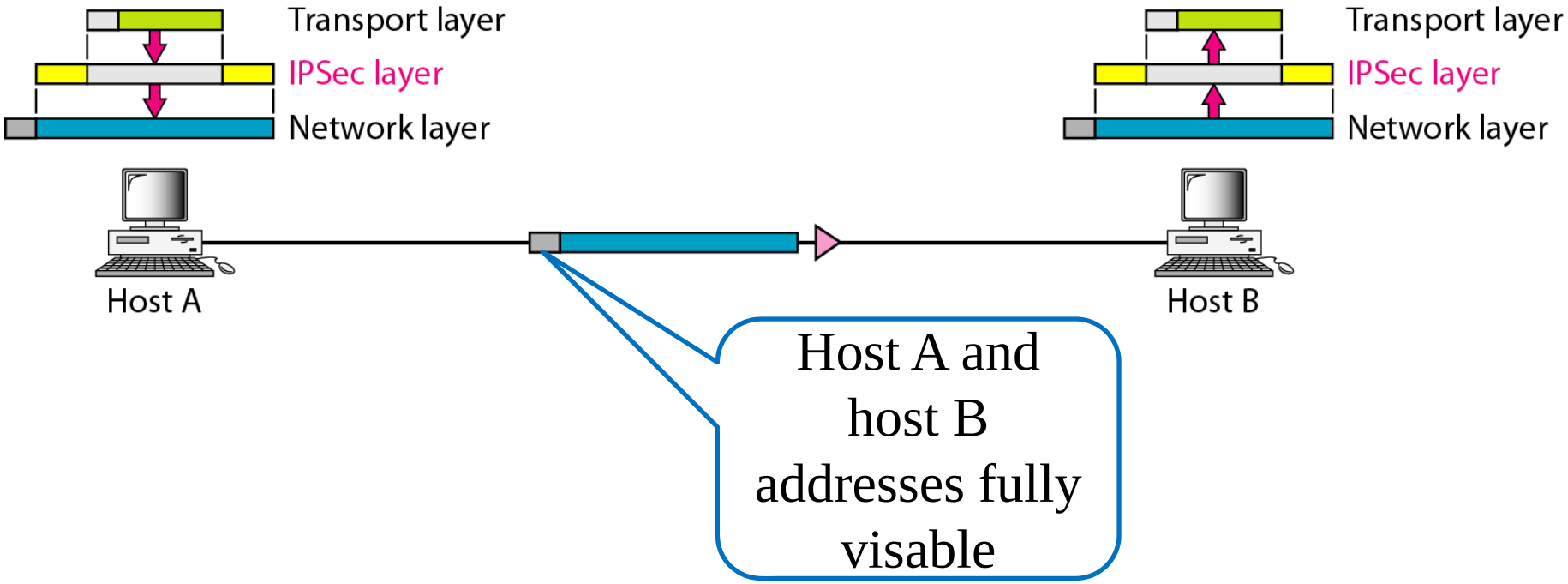
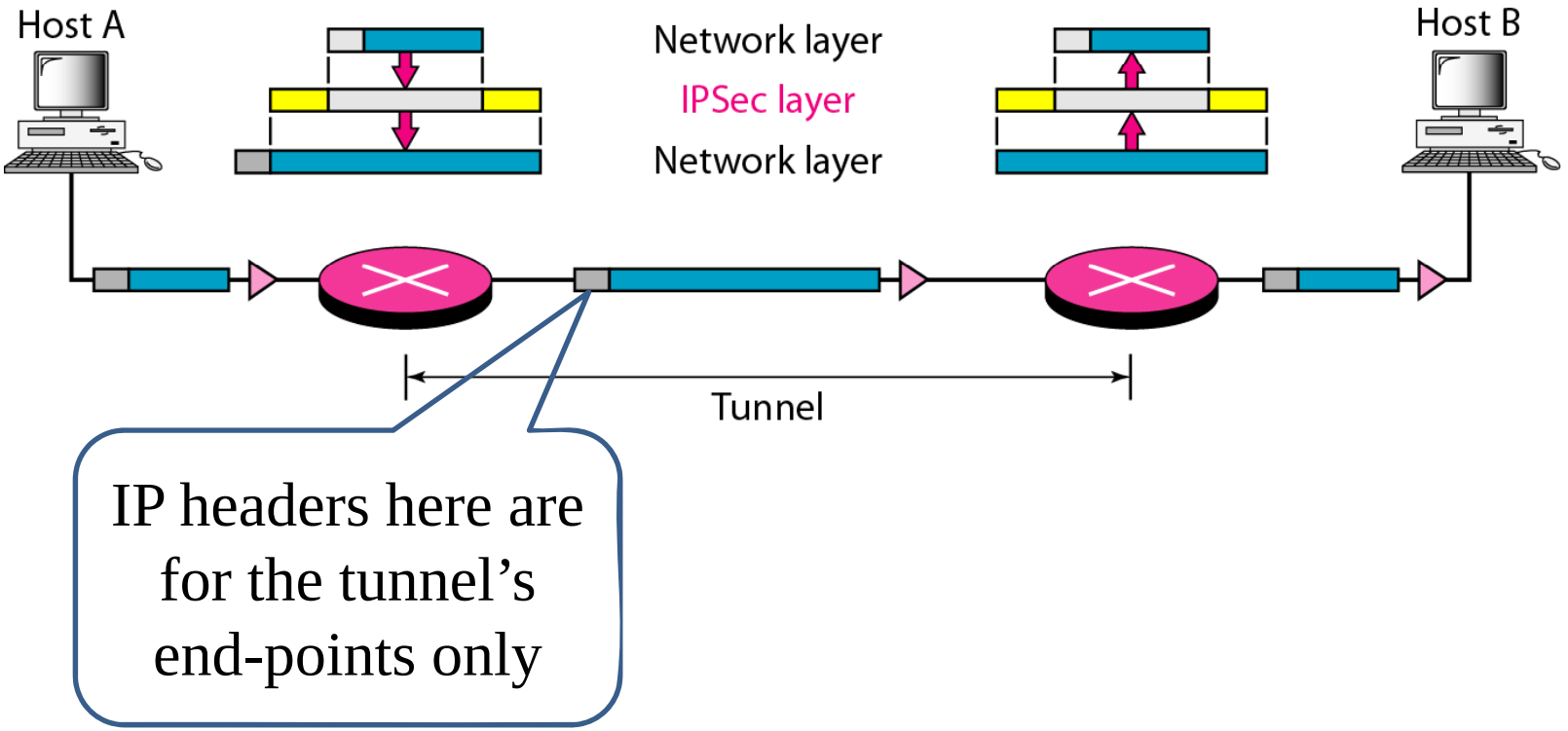


Figure 32.5 *Tunnel mode in action*



Two Protocols

- Authentication Header (AH)
  - Provides **source authentication and data integrity**
  - **No privacy**
- Encapsulating Security Payload (ESP)
  - Provides **source authentication and data integrity**
  - **Privacy**

Figure 32.6 *Authentication Header (AH) Protocol in transport mode*

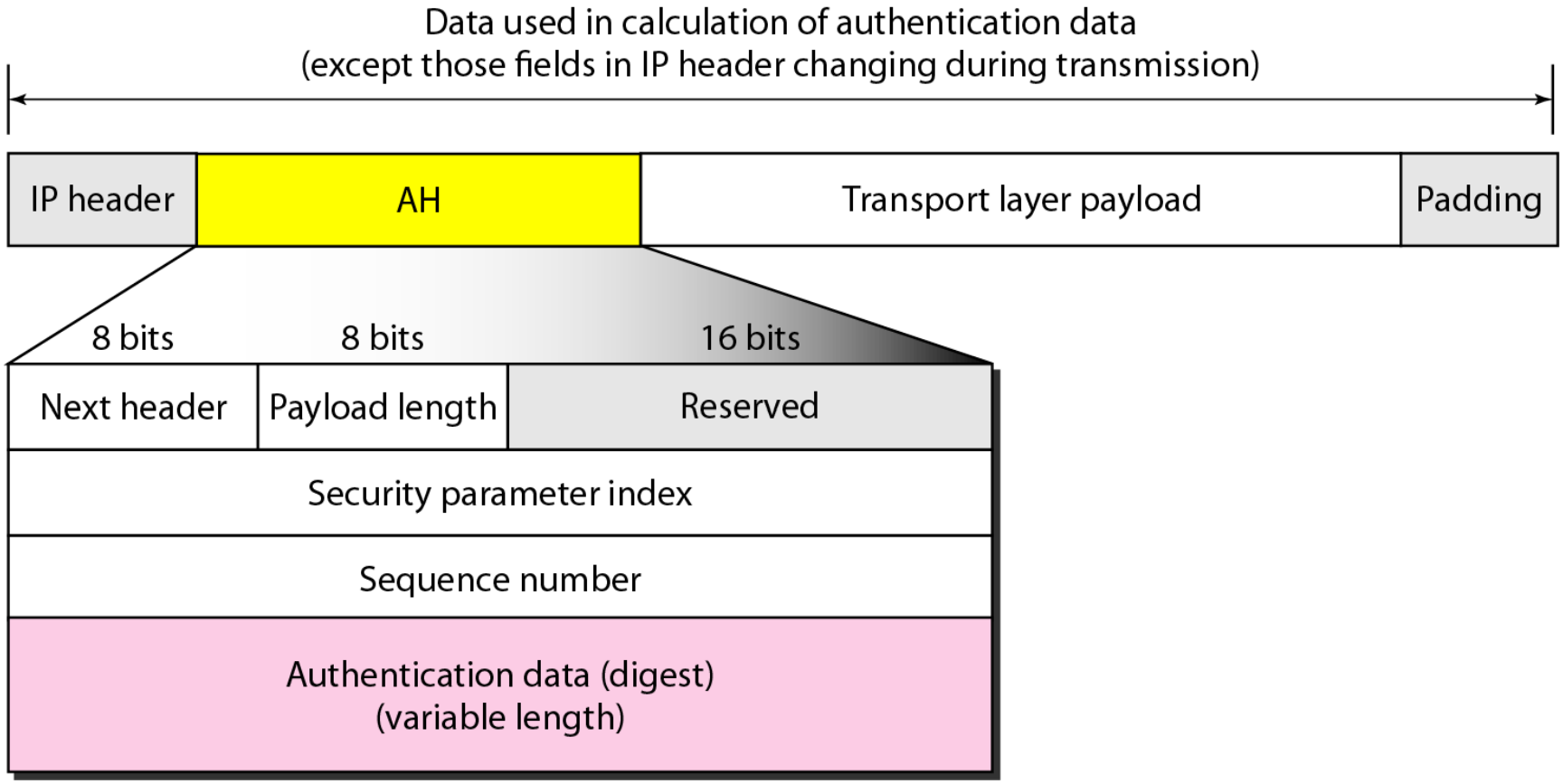


Figure 32.7 *Encapsulating Security Payload (ESP) Protocol in transport mode*

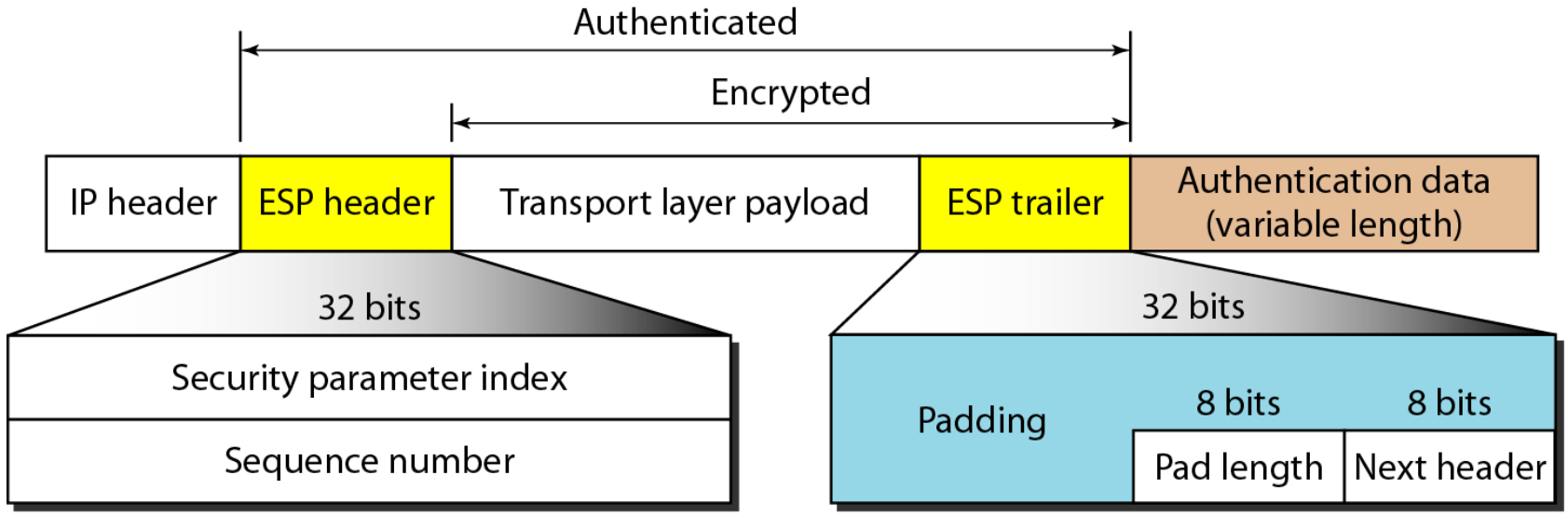


Table 32.1 *IPSec services*

Services	*AH*	*ESP*
Access control	Yes	Yes
Message authentication (message integrity)	Yes	Yes
Entity authentication (data source authentication)	Yes	Yes
Confidentiality	No	Yes
Replay attack protection	Yes	Yes

Exchange secrets

- Bob and Alice must exchange secrets
- For that they need a secured channel
- For the secured channel they nedd to exchange secrets
- For that they need a secured channel
- …

Asymetric encryption

- Pair of keys
  - Public, known by all
  - Private, secure, kept by owner
- Encrypt messages with receivers public key
  - Can only be decrypted with private key
- Sign/Authenticate messages with private key
  - Test with sender’s public key

IPSec

- Security Associations
- Logical secured channel between two parties
- Internet Key Exchange (IKE)
  - Creates SAs (inbound and outbound) in a database

Figure 32.8 *Simple inbound and outbound security associations*

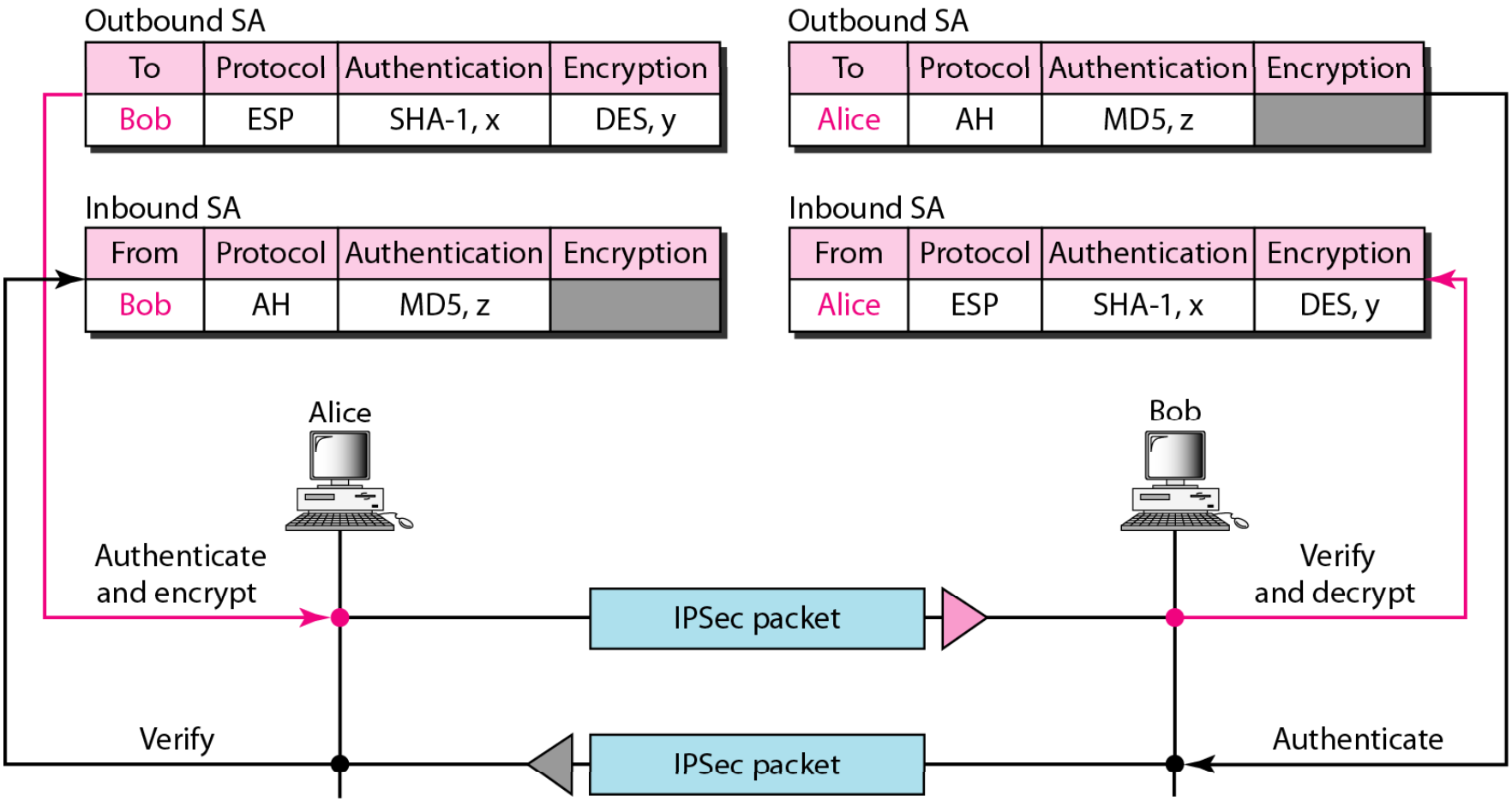
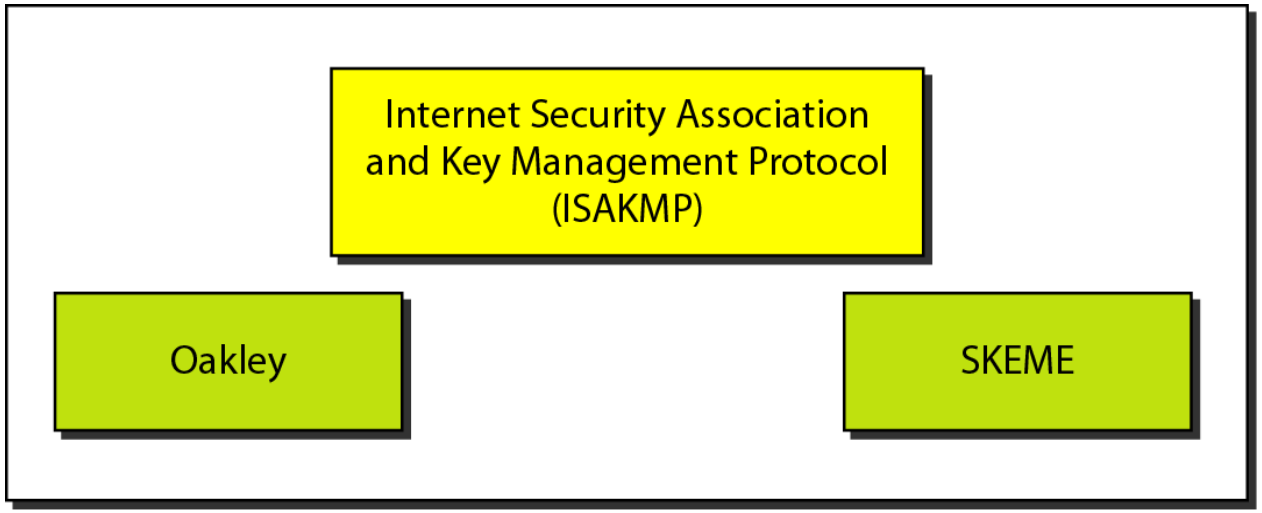


Figure 32.9 *IKE components*



(Virtual) Private Network

- VPN
- Overlay network
- Alternative to a really private network

Table 32.2 *Addresses for private networks*

Prefix	*Range*	*Total*
10/8	10.0.0.0 to 10.255.255.255	2^{24}
172.16/12	172.16.0.0 to 172.31.255.255	2^{20}
192.168/16	192.168.0.0 to 192.168.255.255	2^{16}

Figure 32.10 *Private network*

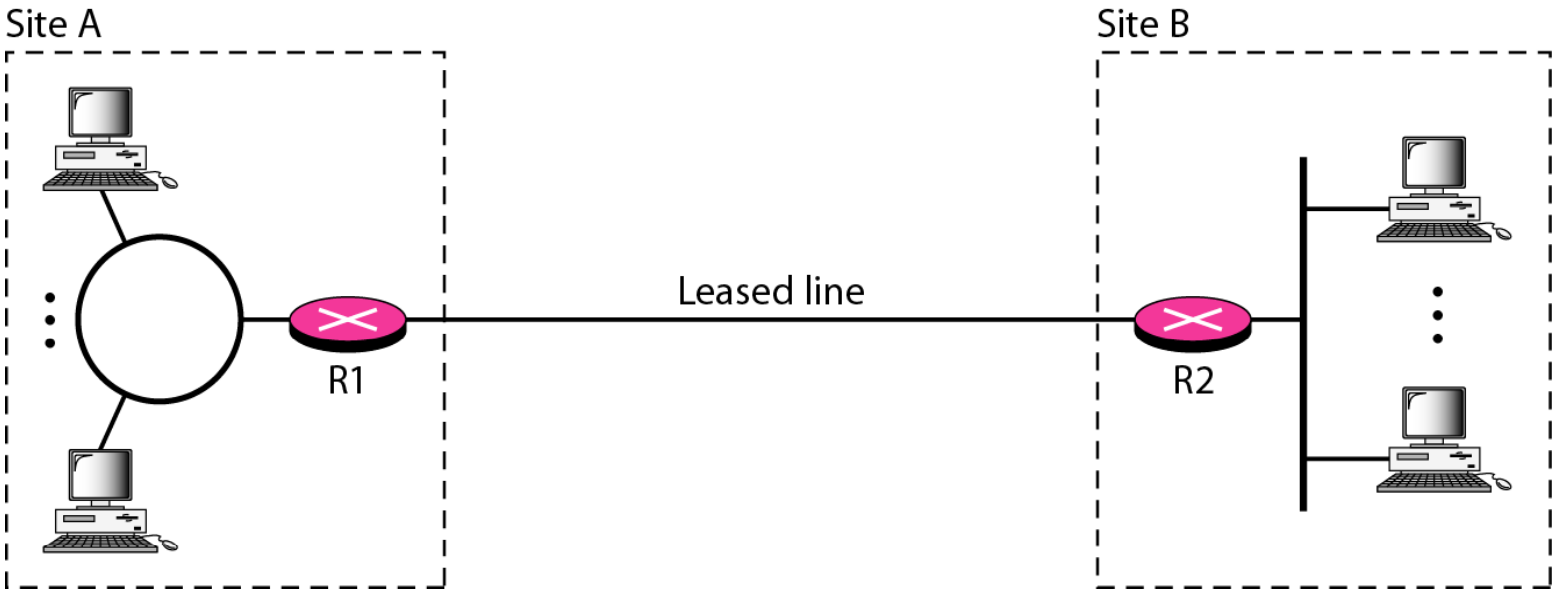


Figure 32.11 *Hybrid network*

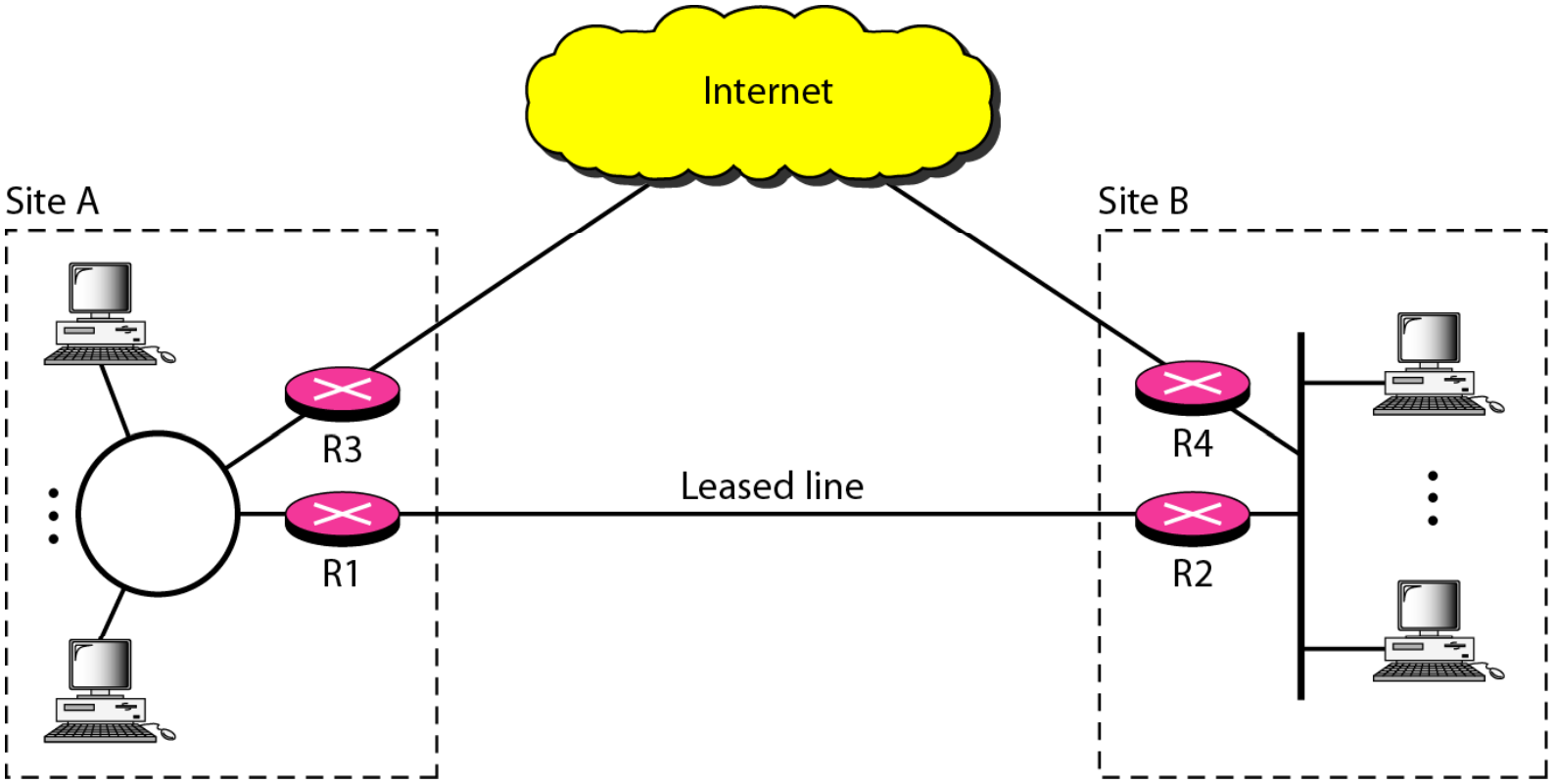
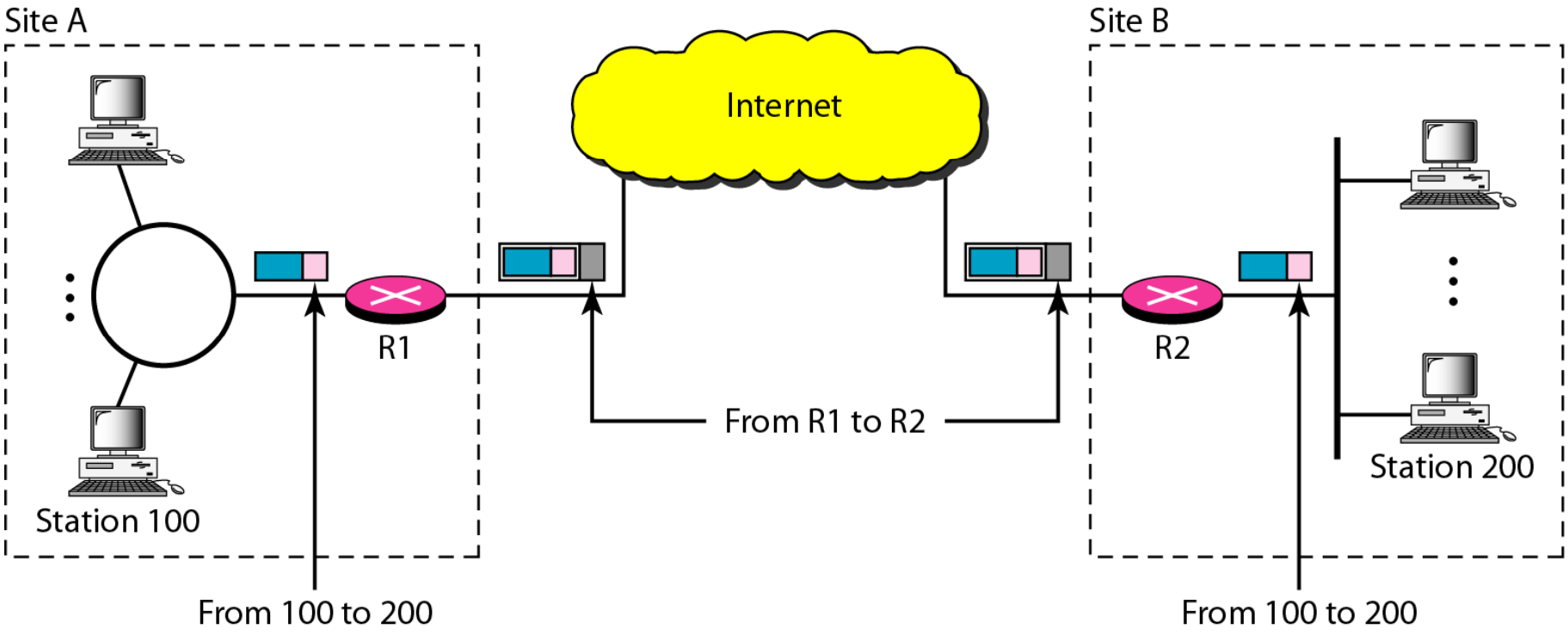


Figure 32.13 *A VPN*



SSL/TLS

- Secure Sockets Layer Protocol
- Transport Layer Security
- TLS is IETF version of SSL

Figure 32.14 *Location of SSL and TLS in the Internet model*

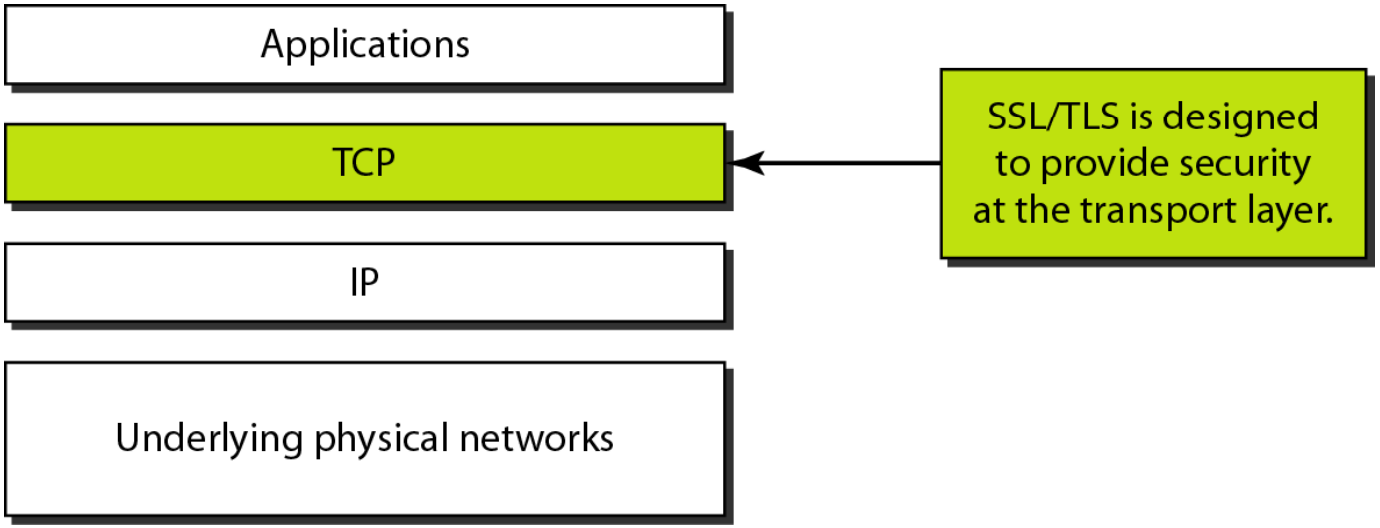


Table 32.3 *SSL cipher suite list*

Cipher Suite	*Key Exchange Algorithm*	*Encryption Algorithm*	*Hash Algorithm*
SSL_NULL_***WITH***_**NULL**_NULL	NULL	NULL	NULL
SSL_RSA_***WITH***_**NULL**_MD5	RSA	NULL	MD5
SSL_RSA_***WITH***_**NULL**_SHA	RSA	NULL	SHA
SSL_RSA_***WITH***_**RC4_128**_MD5	RSA	RC4_128	MD5
SSL_RSA_***WITH***_**RC4_128**_SHA	RSA	RC4_128	SHA
SSL_RSA_***WITH***_**IDEA_CBC**_SHA	RSA	IDEA_CBC	SHA
SSL_RSA_***WITH***_**DES_CBC**_SHA	RSA	DES_CBC	SHA
SSL_RSA_***WITH***_**3DES_EDE_CBC**_SHA	RSA	3DES_EDE_CBC	SHA
SSL_DH_anon_***WITH***_**RC4_128**_MD5	DH_anon	RC4_128	MD5
SSL_DH_anon_***WITH***_**DES_CBC**_SHA	DH_anon	DES_CBC	SHA
SSL_DH_anon_***WITH***_**3DES_EDE**_CBC_SHA	DH_anon	3DES_EDE_CBC	SHA

Table 32.3 *SSL cipher suite list (continued)*

Cipher Suite	*Key Exchange Algorithm*	*Encryption Algorithm*	*Hash Algorithm*
SSL_DHE_RSA_*WITH*_DES_CBC_SHA	DHE_RSA	DES_CBC	SHA
SSL_DHE_RSA_*WITH*_3DES_EDE_CBC_SHA	DHE_RSA	3DES_EDE_CBC	SHA
SSL_DHE_DSS_*WITH*_DES_CBC_SHA	DHE_DSS	DES_CBC	SHA
SSL_DHE_DSS_*WITH*_3DES_EDE_CBC_SHA	DHE_DSS	3DES_EDE_CBC	SHA
SSL_DH_RSA_*WITH*_DES_CBC_SHA	DH_RSA	DES_CBC	SHA
SSL_DH_RSA_*WITH*_3DES_EDE_CBC_SHA	DH_RSA	3DES_EDE_CBC	SHA
SSL_DH_DSS_*WITH*_DES_CBC_SHA	DH_DSS	DES_CBC	SHA
SSL_DH_DSS_*WITH*_3DES_EDE_CBC_SHA	DH_DSS	3DES_EDE_CBC	SHA
SSL_FORTEZZA_DMS_*WITH*_NULL_SHA	FORTEZZA_DMS	NULL	SHA
SSL_FORTEZZA_DMS_*WITH*_FORTEZZA_CBC_SHA	FORTEZZA_DMS	FORTEZZA_CBC	SHA
SSL_FORTEZZA_DMS_*WITH*_RC4_128_SHA	FORTEZZA_DMS	RC4_128	SHA

SSL

- Created by Netscape
- Authentictation
- Message integrity
- Confidentiallity

SSL Services

- Fragmentation
  - Create blocks of 2^{14} bytes or less
- Compression
- Message Integrity
- Confidentiality
- Framing

Figure 32.18 *Processing done by the Record Protocol*

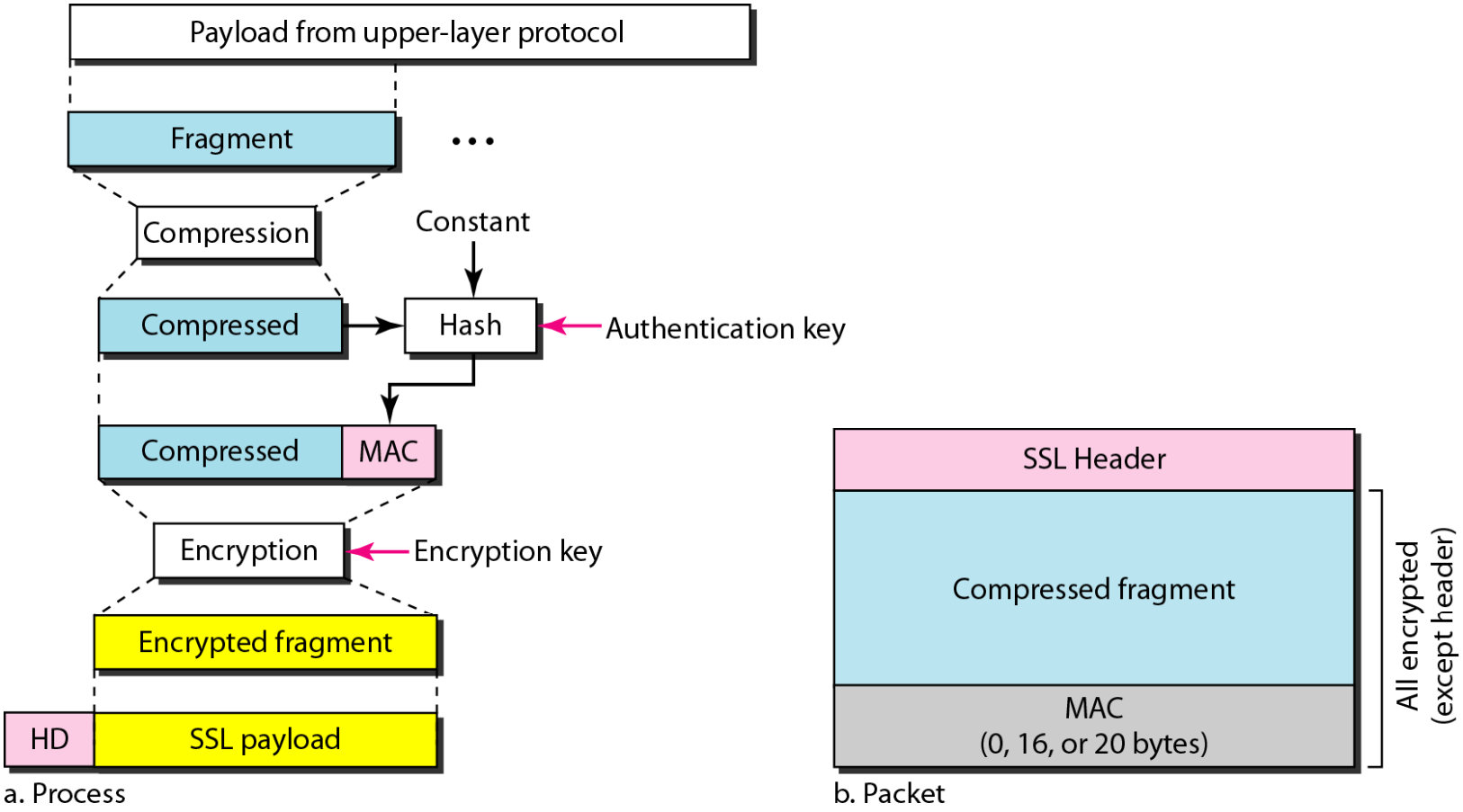


Figure 32.15 *Creation of cryptographic secrets in SSL*

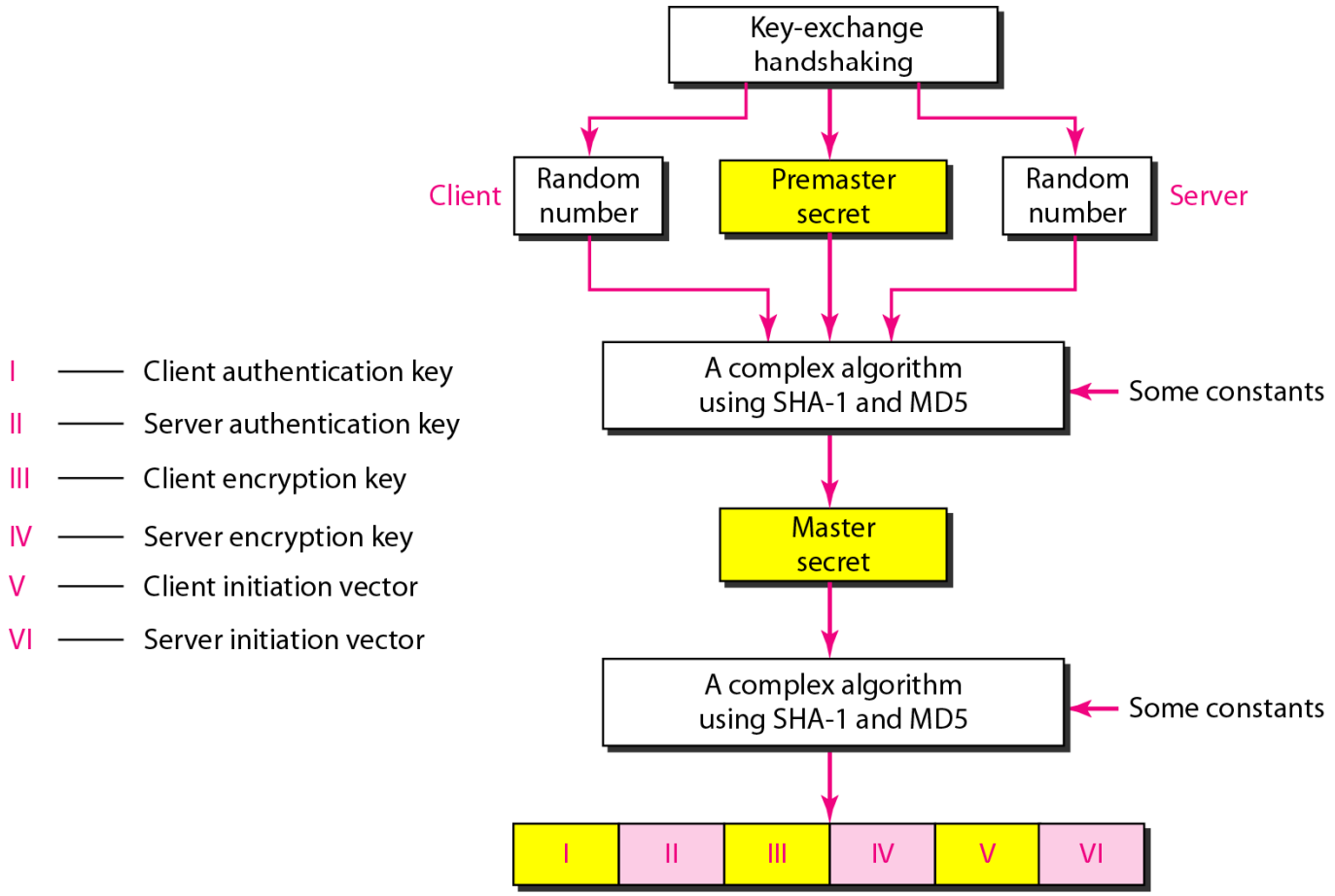
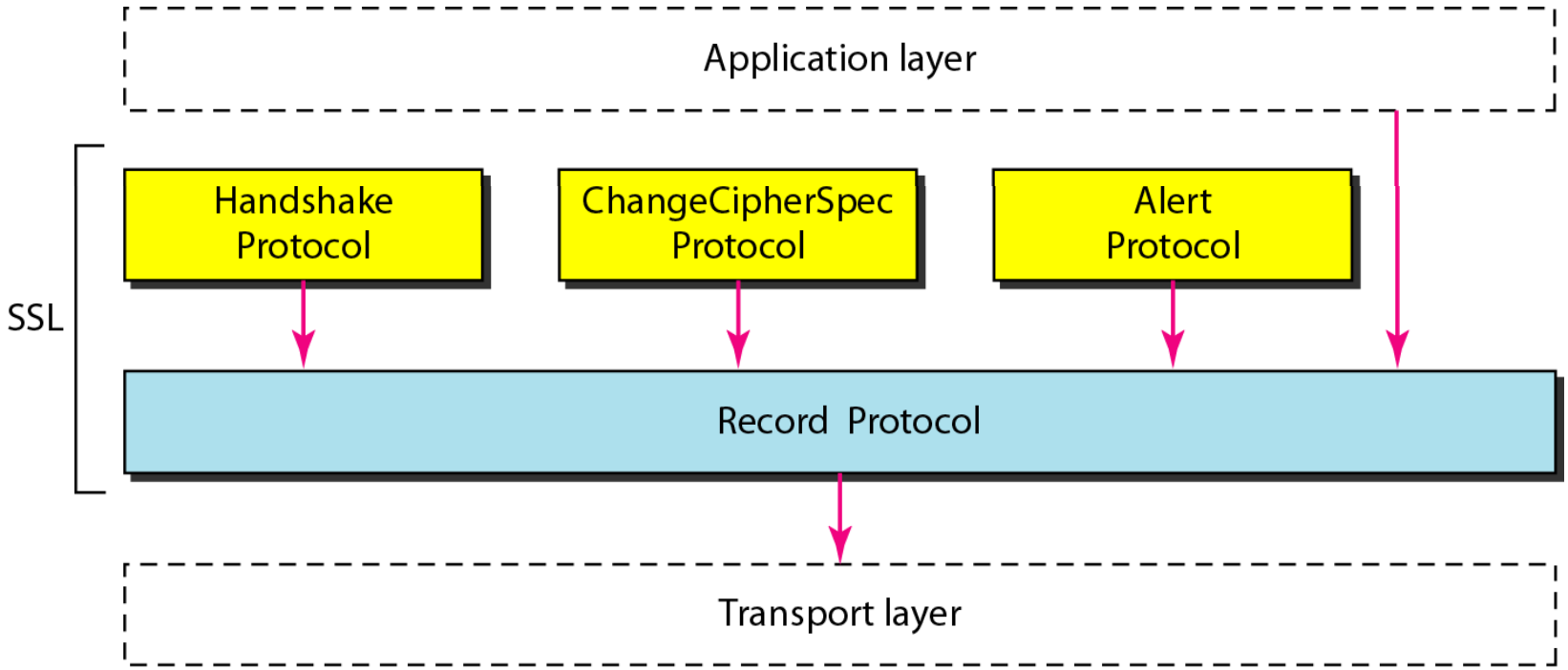


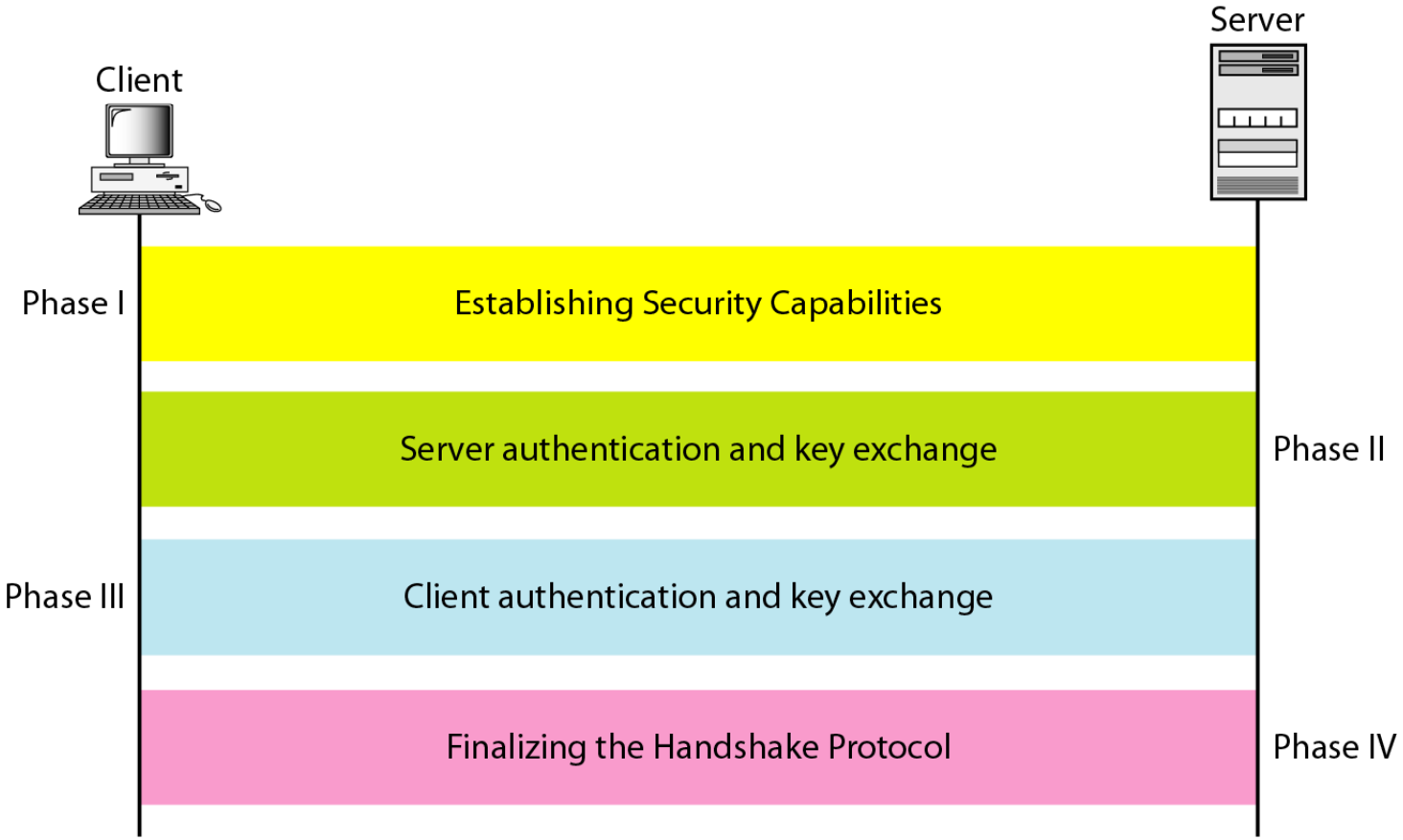
Figure 32.16 *Four SSL protocols*



Four protocols

- Record Protocol
  - The carrier
- Handshake Protocol
  - Authentication
  - Establishe cipher sets
  - Provides keys and security parameters
- ChangeCipherSPec Protocol
  - Crypotgraphic Secrets ready
- Alert Protocol
  - Signaling of abnormalities

Figure 32.17 *Handshake Protocol*



Firewalls

- Control system access
- Check/Drop packets
  - Network layer, Transport layer
  - Application layer

Figure 32.22 *Firewall*

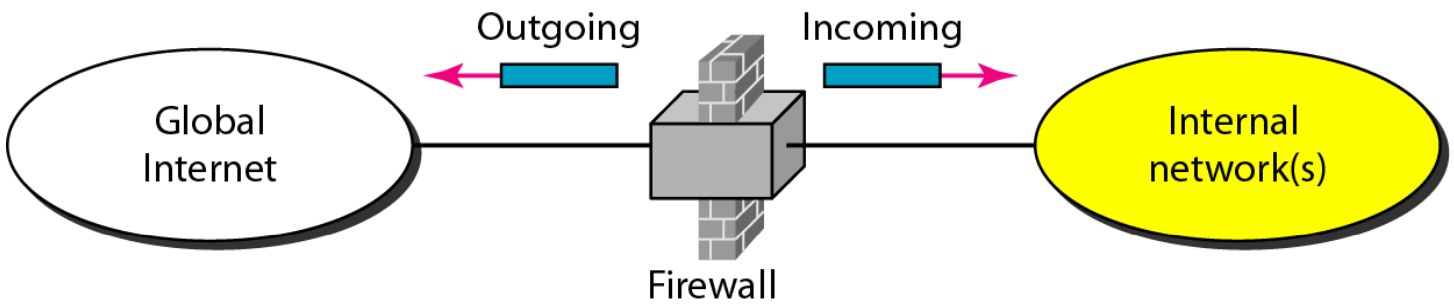
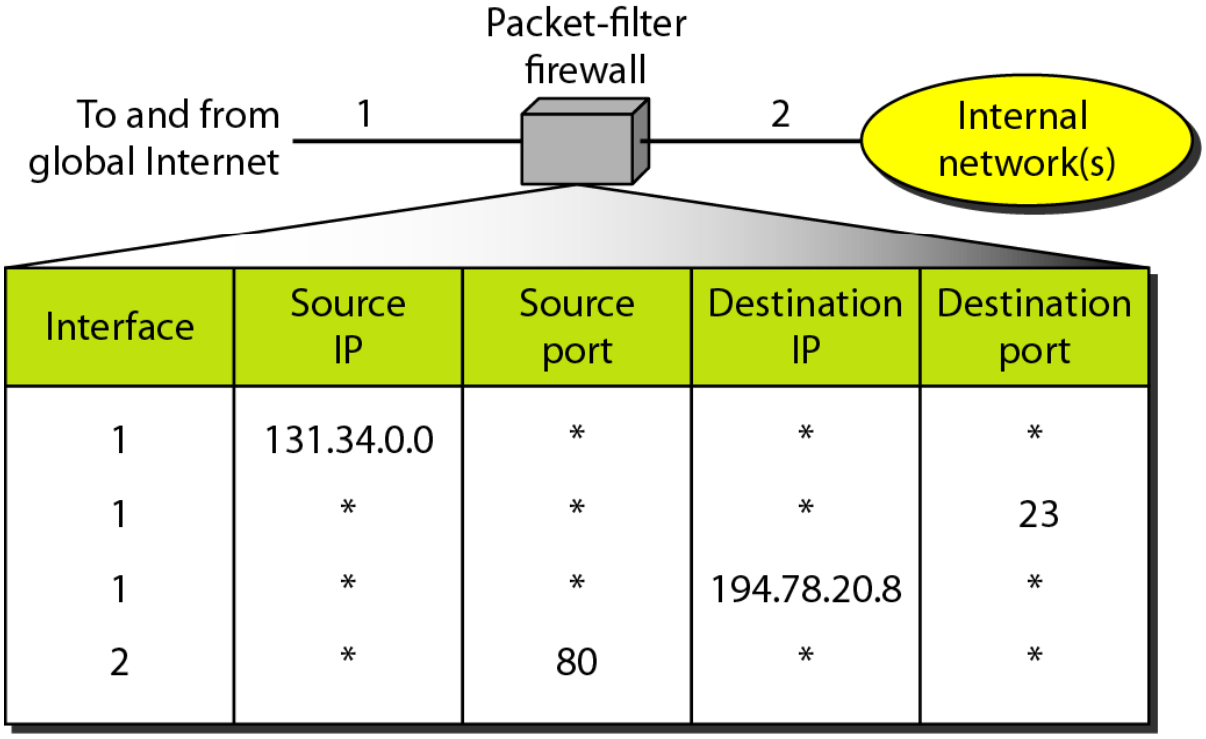


Figure 32.23 *Packet-filter firewall*



Interface	Source IP	Source port	Destination IP	Destination port
1	131.34.0.0	*	*	*
1	*	*	*	23
1	*	*	194.78.20.8	*
2	*	80	*	*

Application Gateway

- Firewall on Application Layer
- Acts as
  - server against client
  - client against requested service
- Checks
  - if user’s request is legitimate
  - application data integrity

Figure 32.24 *Example of proxy firewall for http*