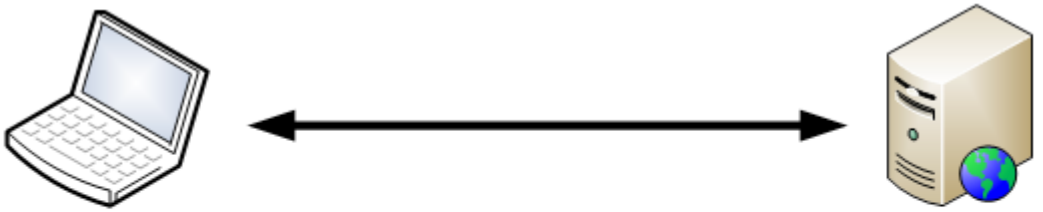
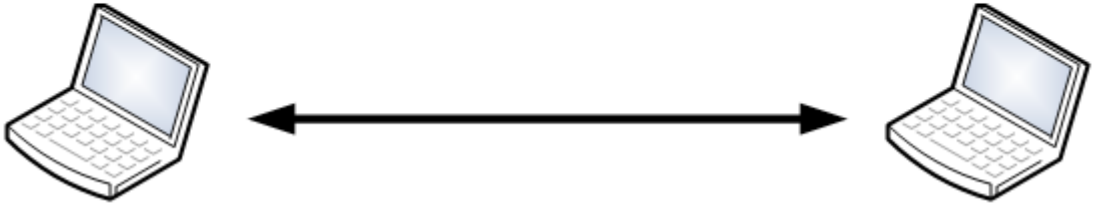


client

server
(e.g. webserver)



peer-to-peer network (P2P)

Metric prefixes

kilo	k	10^3
mega	M	10^6
giga	G	10^9
tera	T	10^{12}
peta	P	10^{15}

Note the discrepancy:
1000 (SI)
vs.
1024=2^{10} (used for memory and storage)

Bases

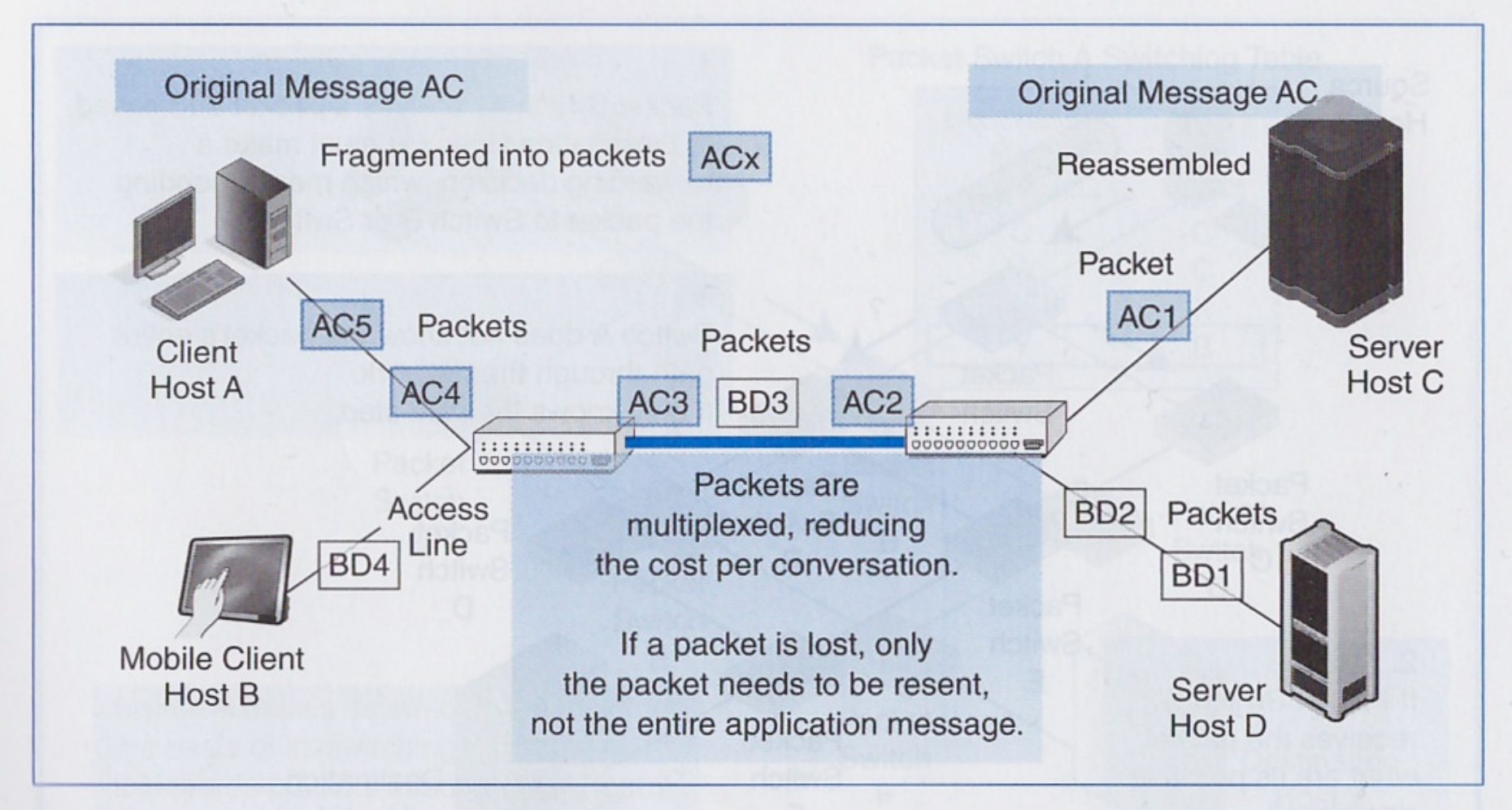
base 2	**binary**	[0-1]
base 10	**decimal**	[0-9]
base 16	**hexadecimal**	[0x0-0xF]

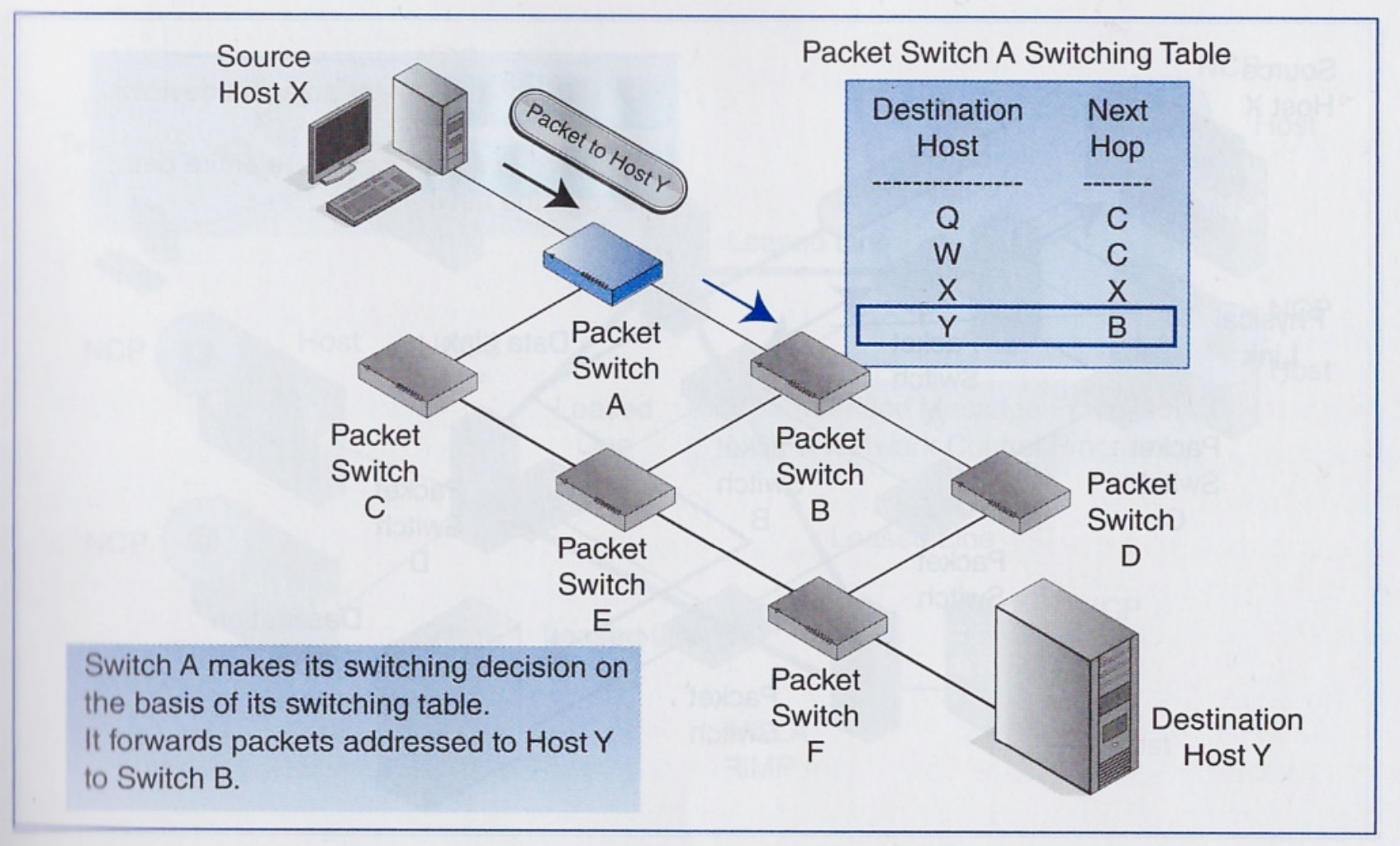
1	**bit**	values 0 to 1
1101	4 bits = 1 **nibble**	values 0 to 15
11010001	8 bits = 1 **byte**	values 0 to 255

Hexadecimal notation

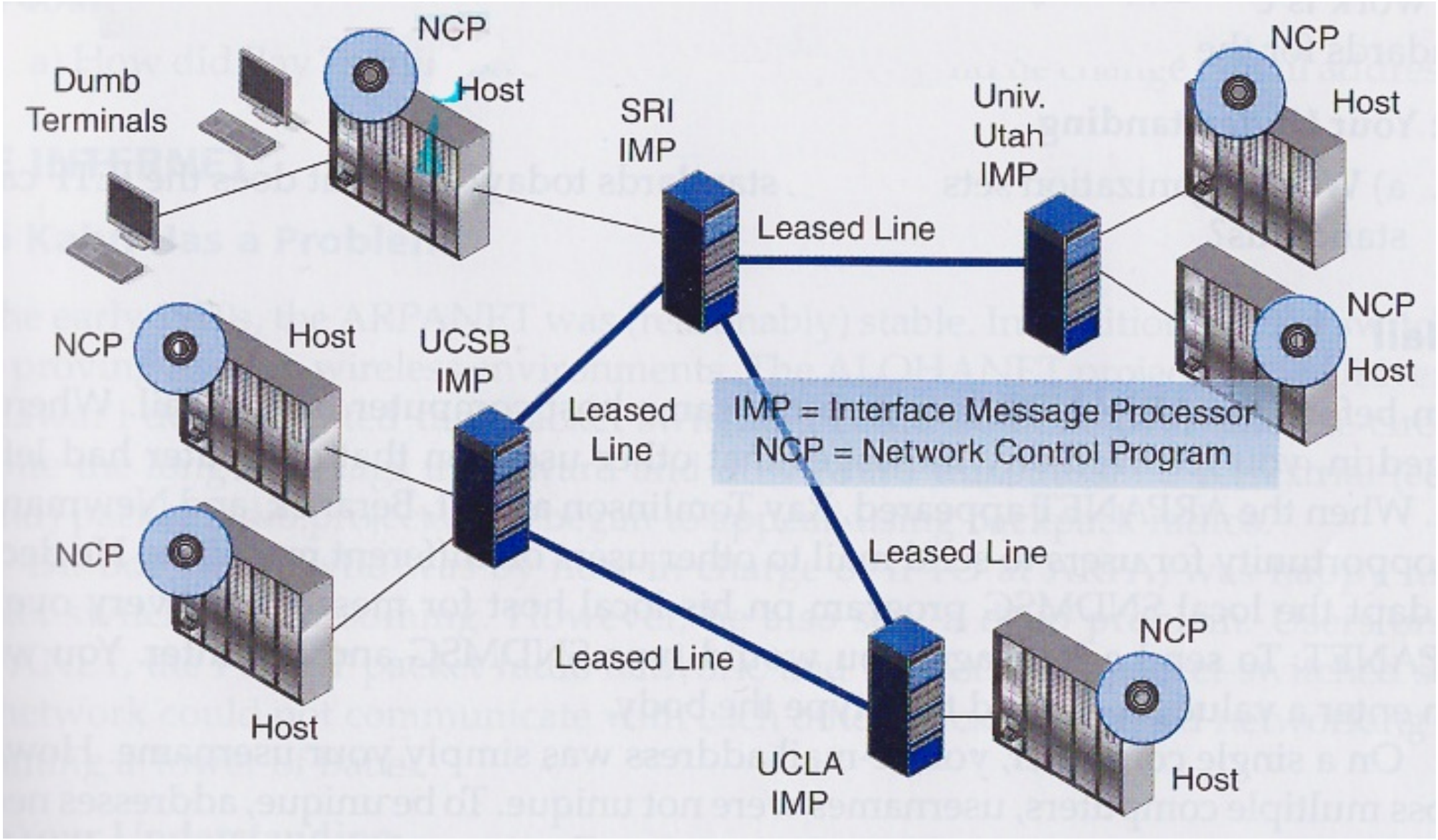
binary	*decimal*	*hex*
0000	0	0
0001	1	1
0010	2	2
0011	3	3
0100	4	4
0101	5	5
0110	6	6
0111	7	7
1000	8	8
1001	9	9
1010	10	A
1011	11	B
1100	12	C
1101	13	D
1110	14	E
1111	15	F

Packet switching is more efficient than reserved circuits

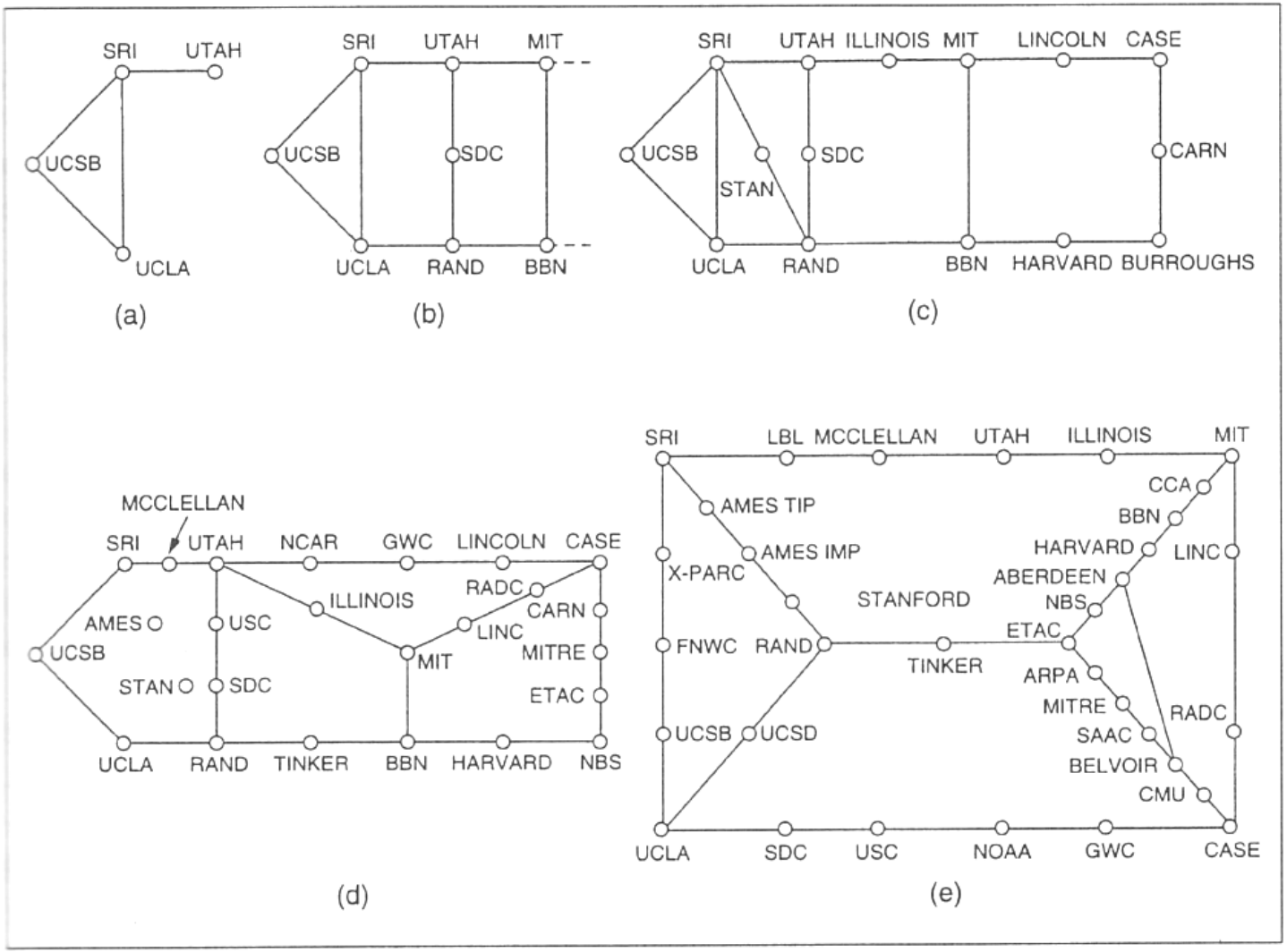




Each switch forwards the packet to the next hop based on its switching table; it does not know which full route the packet will take throughout the network



Structure of the ARPAnet (1969-1983)

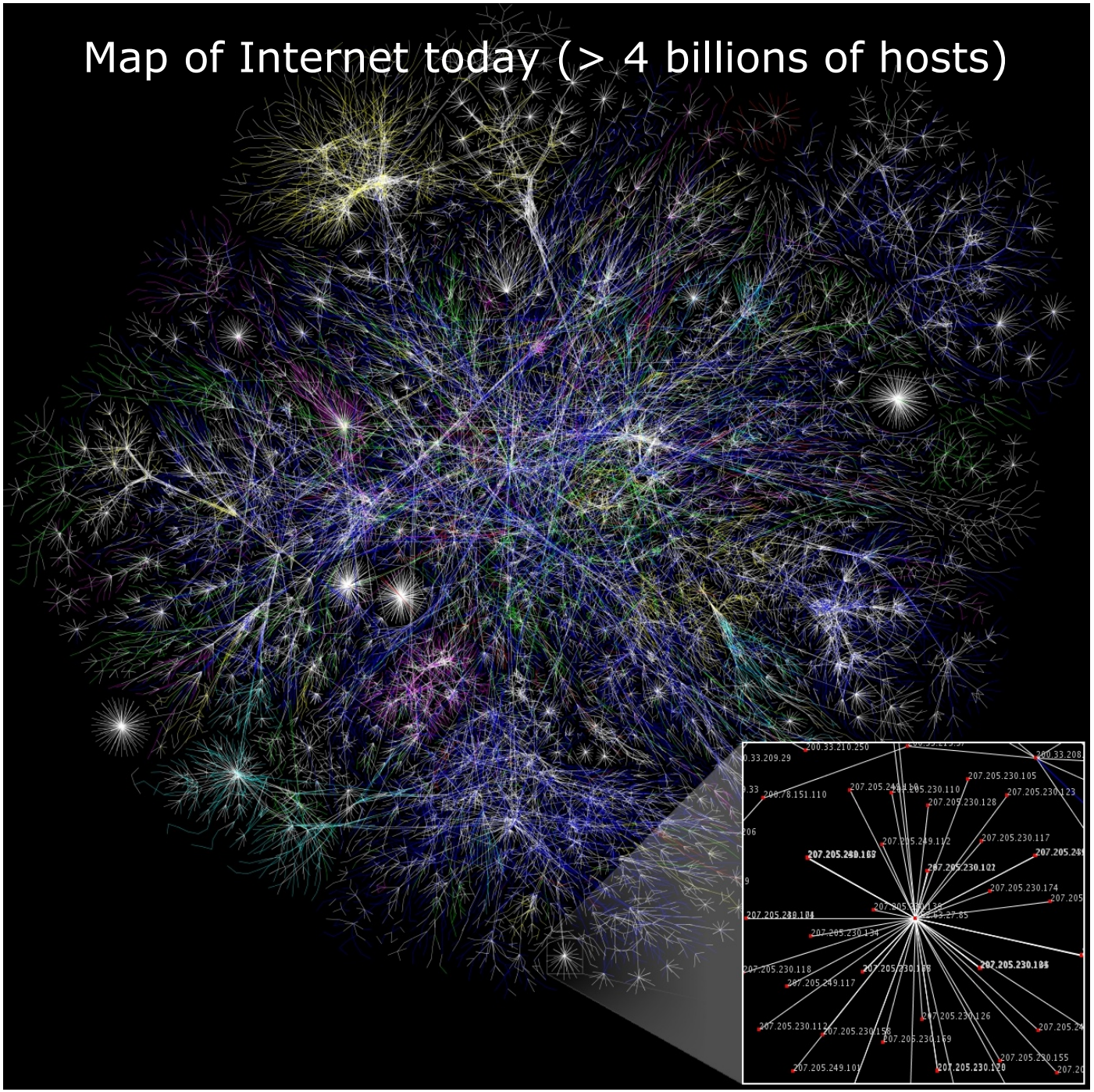


Map of the ARPAnet

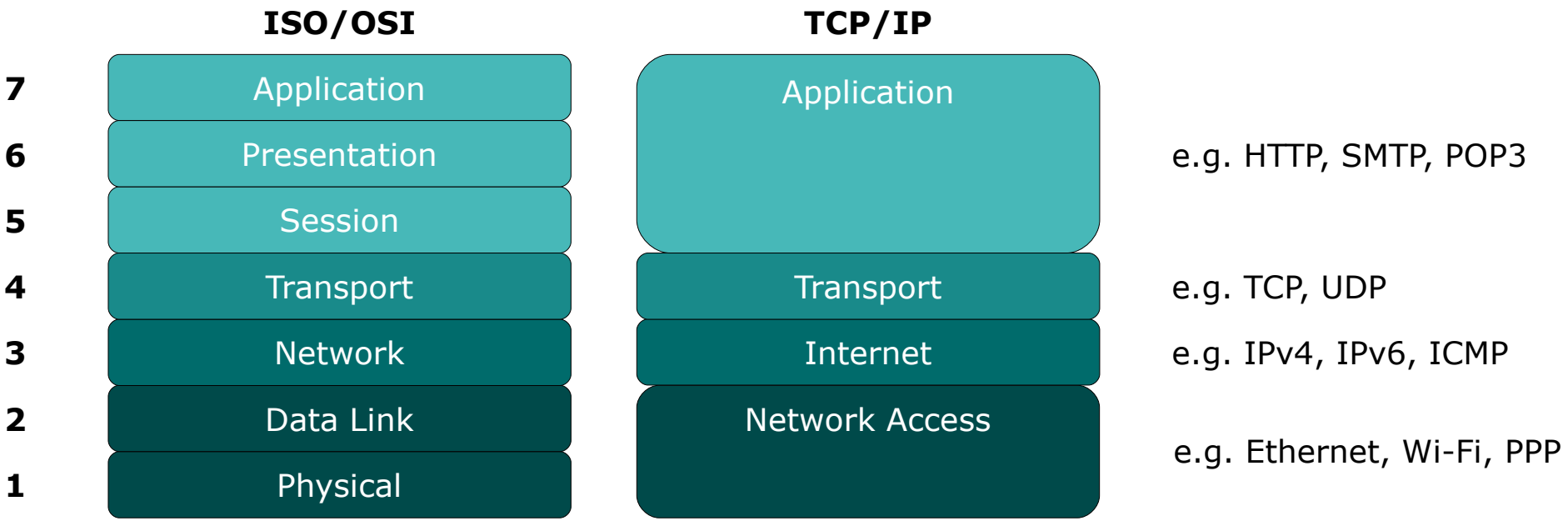
(a) December 1969 (b) July 1970 (c) March 1971

(d) April 1972 (e) September 1972

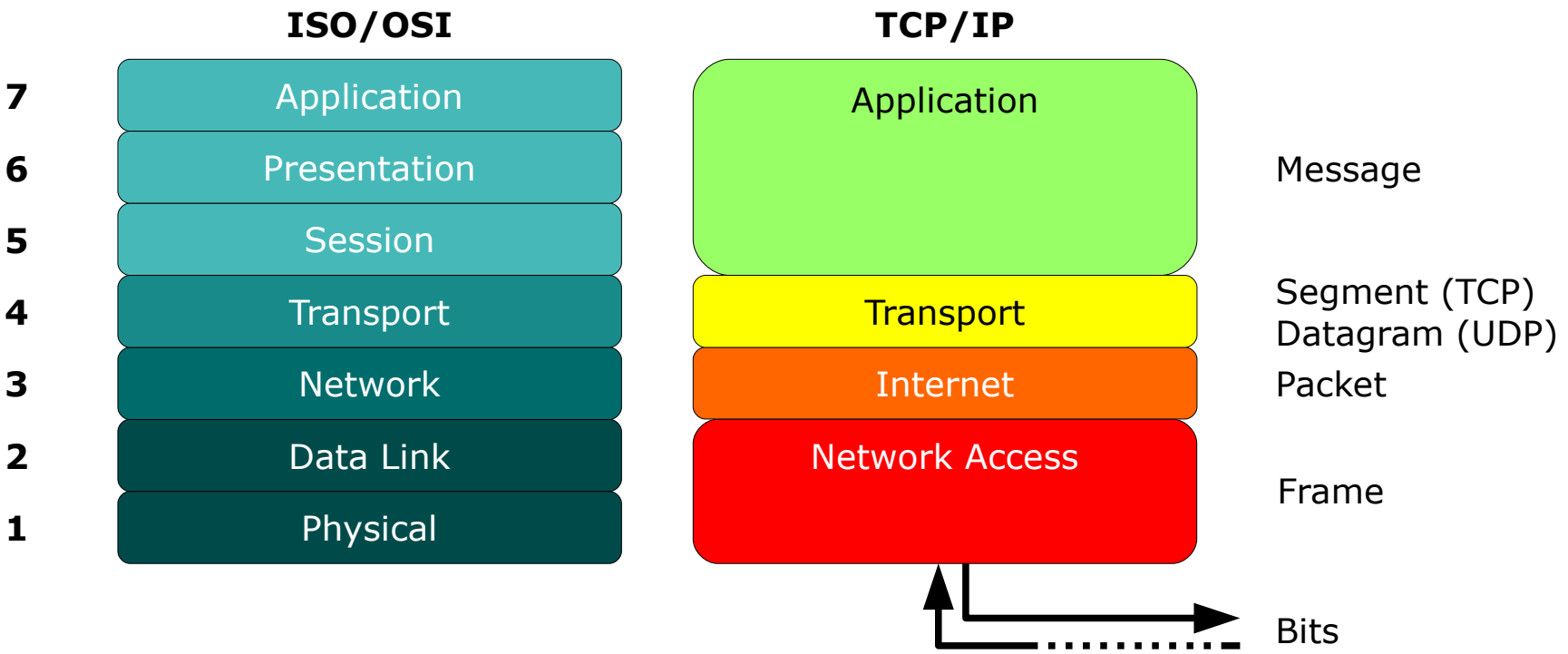
Map of Internet today (> 4 billions of hosts)



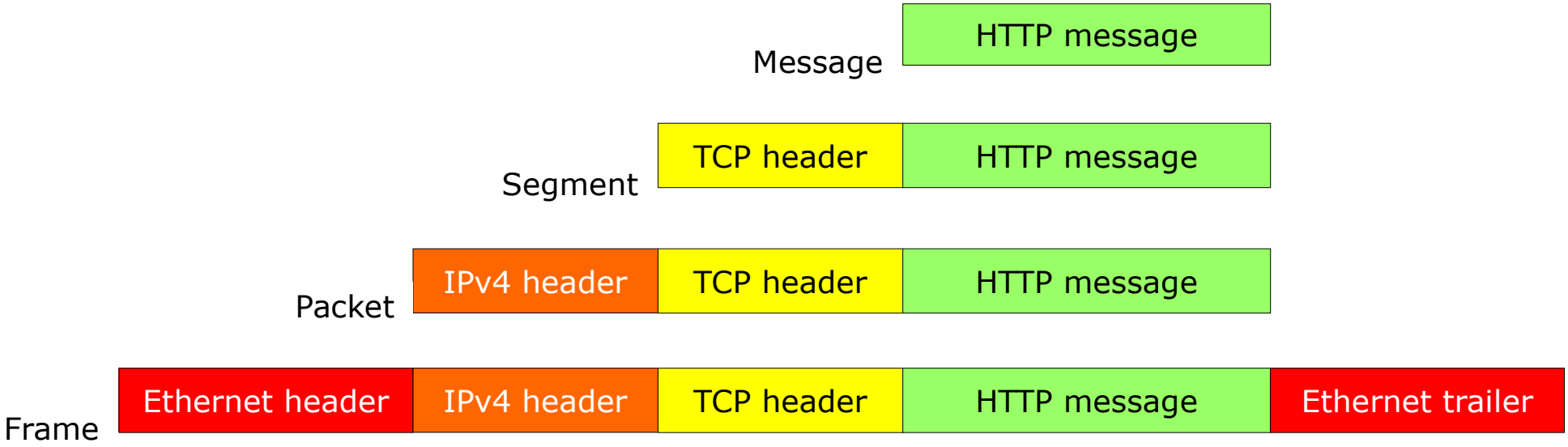
Networking layers: the hybrid ISO/OSI TCP/IP stack



Networking layers: the hybrid ISO/OSI TCP/IP stack

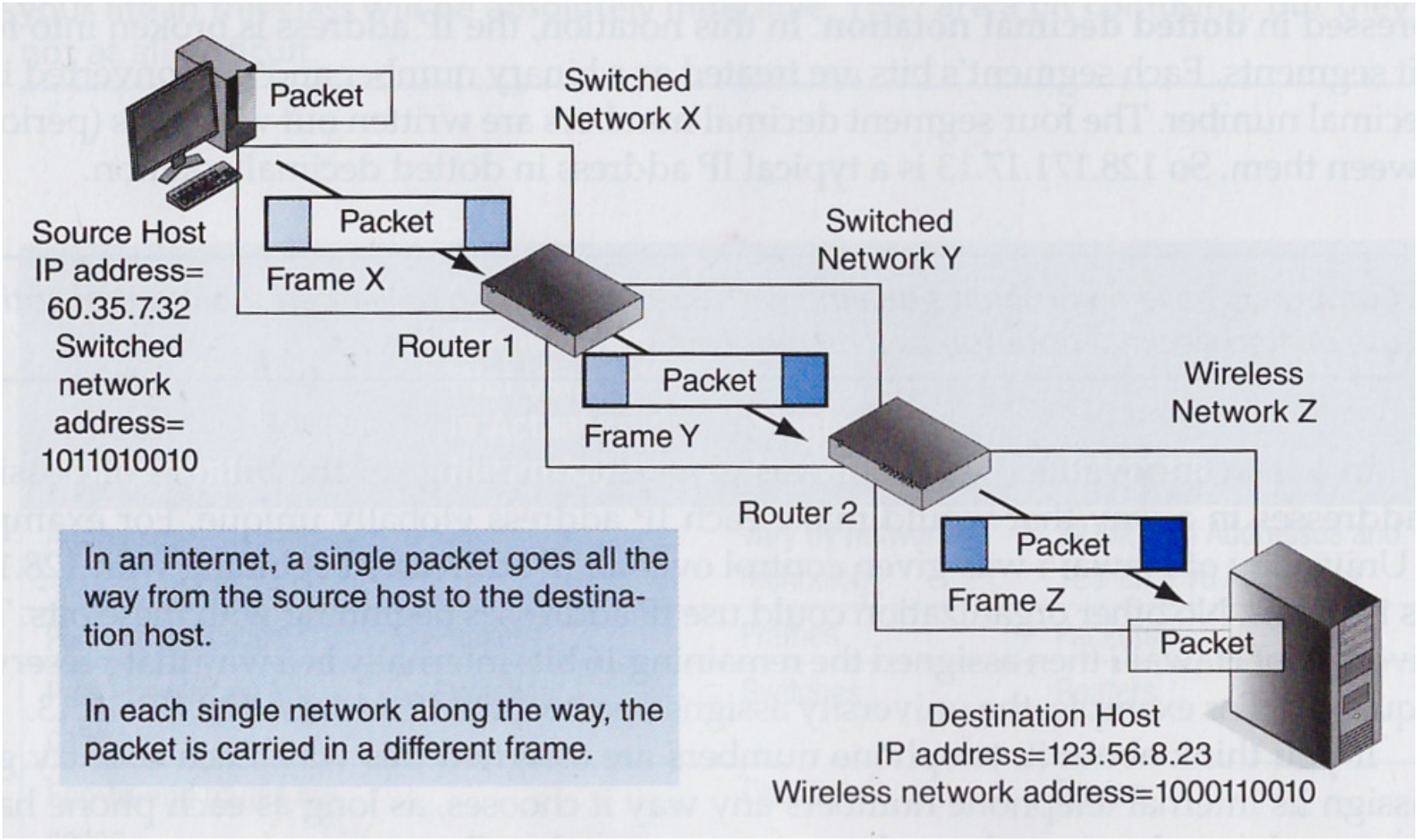


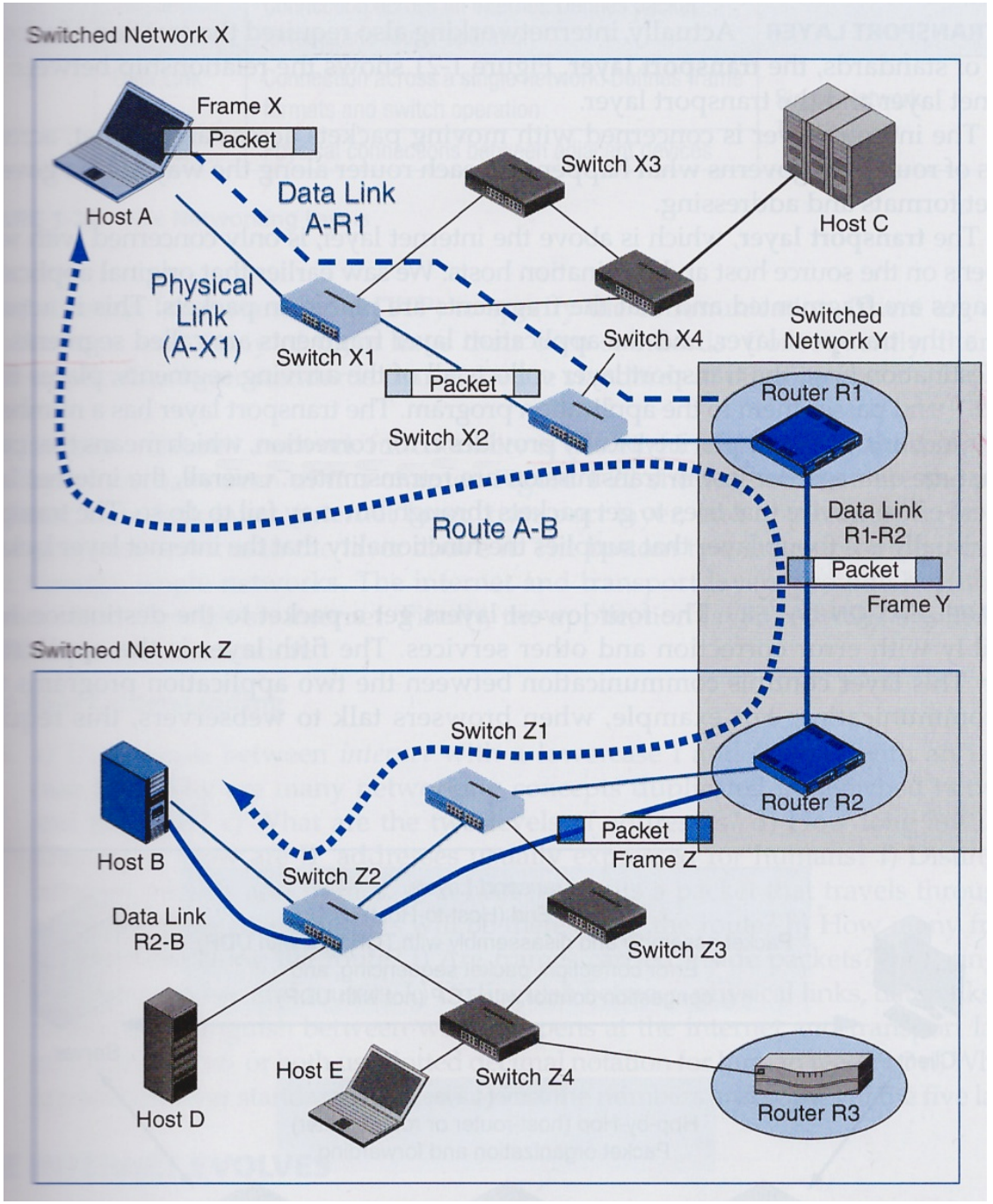
The application message is encapsulated, for each layer, by the sender host...



...and then decapsulated at the receiver's host end.

Note:
- the Network Access frame is decapsulated and encapsulated at each data-link hop
- the IP source and destination address in the IP packet can be modified in transit if NAT is in use


Packet
Switched
Network X
Source Host
IP address=
60.35.7.32
Switched
network
address=
1011010010
Packet
Frame X
Router 1
Switched
Network Y
Packet
Frame Y
Router 2
Wireless
Network Z
Packet
Frame Z
Packet
In an internet, a single packet goes all the way from the source host to the destination host.
In each single network along the way, the packet is carried in a different frame.
Destination Host
IP address=123.56.8.23
Wireless network address=1000110010


Switched Network X
Frame X
Packet
Host A
Data Link
A-R1
Switch X3
Host C
Physical
Link
(A-X1)
Switch X1
Switch X4
Switched
Network Y
Packet
Router R1
Switch X2
Route A-B
Data Link
R1-R2
Packet
Frame Y
Switched Network Z
Switch Z1
Router R2
Host B
Packet
Frame Z
Switch Z2
Data Link
R2-B
Switch Z3
Host D
Host E
Switch Z4
Router R3

Application layer: standards

HTTP (World Wide Web)

SMTP, POP3, IMAP (mail services)

NNTP (newsgroups)

FTP (file transfer)

DHCP

DNS

SSH

...

Transport layer: standards

TCP (Transmission Control Protocol)
- connection-oriented
- acknowledgements of segments (receiver) and re-sending if needed
- sequence numbers and reordering
- provides fragmentation (sender) and reassembling (receiver)
- provides congestion control
- provides error correction

UDP (User Datagram Protocol)
- lightweight and simple
- best-effort
- no fragmentation: application message fits inside a single datagram

Internet layer: standards

IPv4 (Internet Protocol version 4)
32-bit addresses, in quad dotted-decimal format.
e.g. 77.75.22.202

IPv6 (Internet Protocol version 6)
128-bit addresses, in hex.
e.g. 2001:0DB8:AC13:FE01:0000:0000:0000:0000
or 2001:0DB8:AC13:FE01::

To show own's IP addresses: `ipconfig /all`
To resolve a domain (DNS query): `nslookup www.google.com`
To traceroute to a remote host: `tracert 74.125.206.147`
(RTT for 3 packets are shown)

Network Access layer: standards

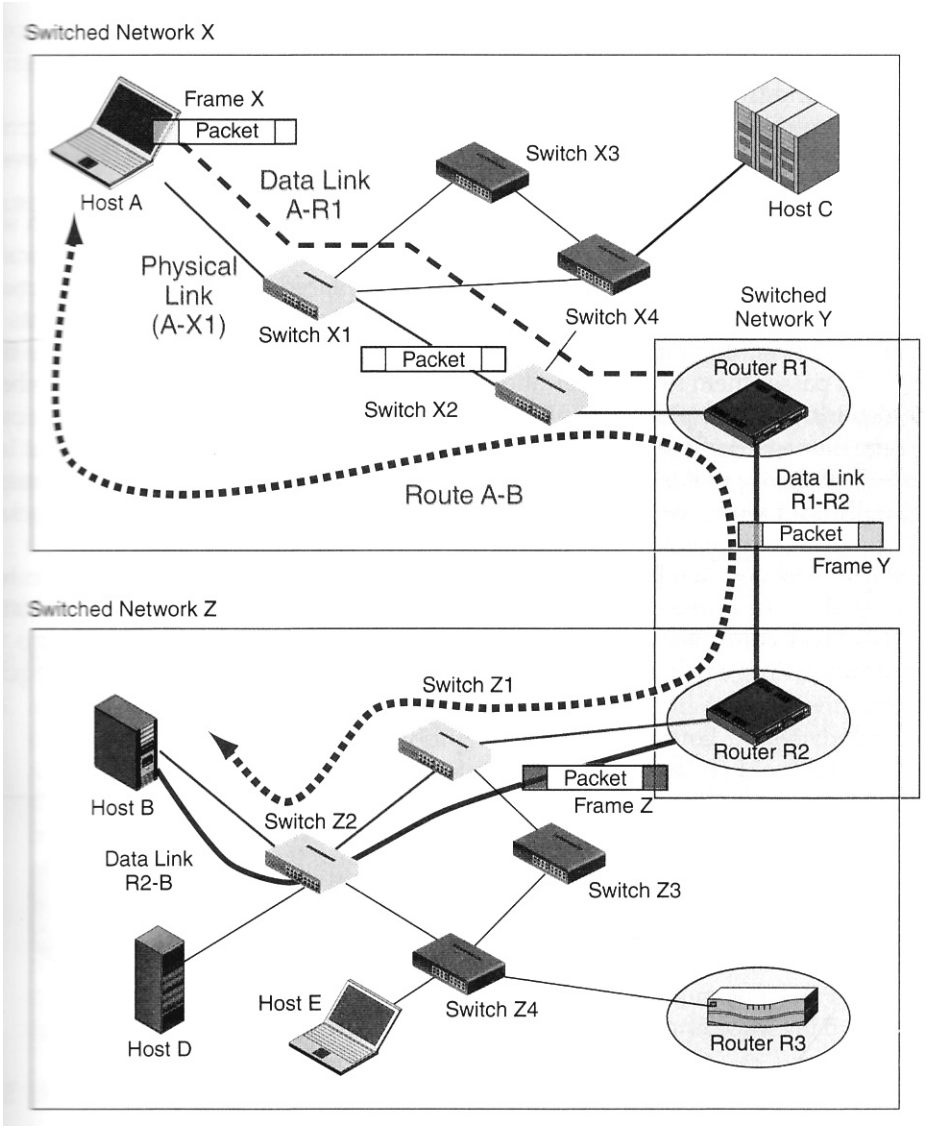
Ethernet (IEEE 802.3)
48-bit MAC addresses (aka physical address or hardware address), in hex. First 6 hex digits identify the vendor.
e.g. 00-16-CB-01-BC-E4, embedded in firmware
To show own's MAC addresses: `getmac /V`

Frame Relay
WAN technology originally designed for ISDN.
10-bit Data Link Connection Identifiers (=addresses to virtual circuits)

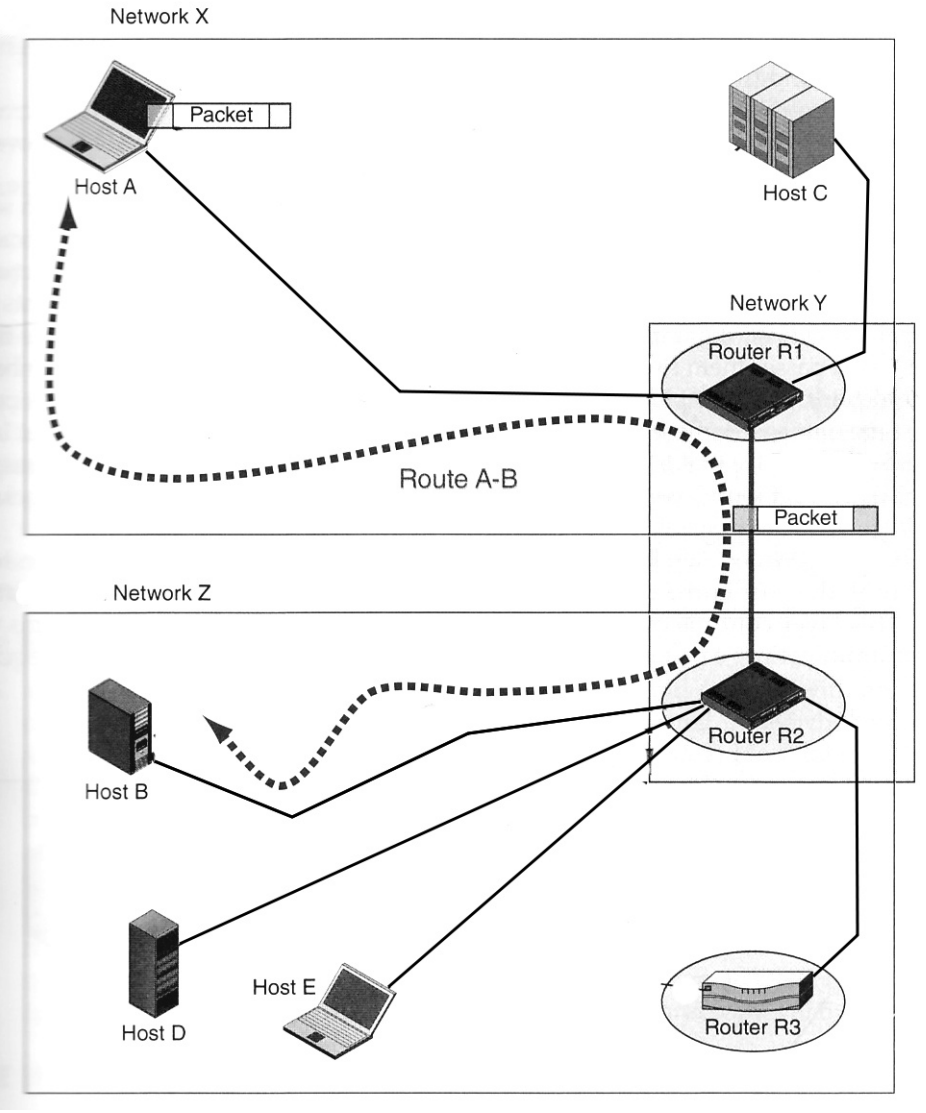
Wi-Fi (IEEE 802.11)

PPP (Point-to-Point Protocol)

Layer 2 network diagram



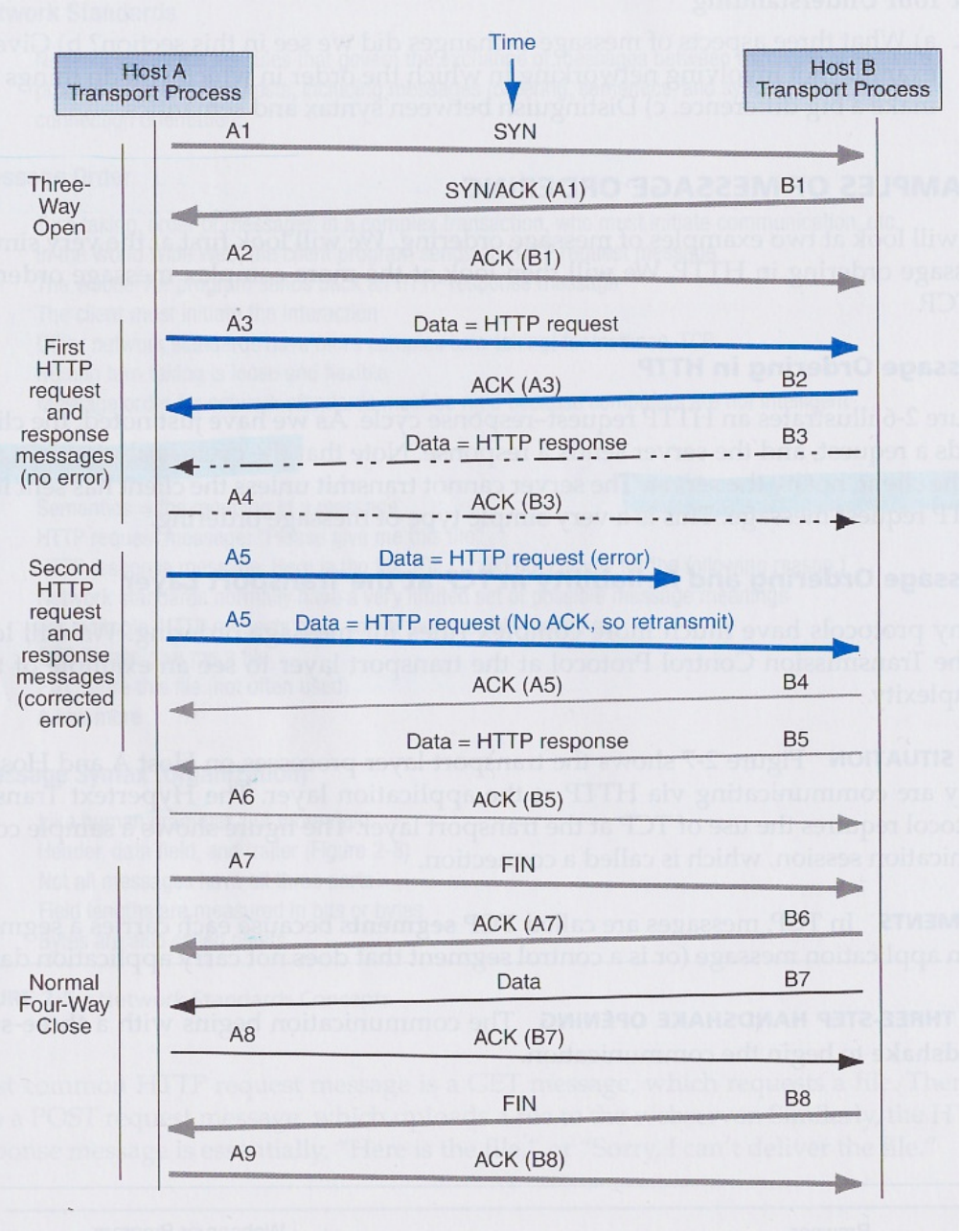
Layer 3 network diagram



SMTP session

```
220 smtp.webster.edu ESMTP Postfix                    server
HELO host1.webster.edu                                client
250 Hello host1.webster.edu, glad to meet you
MAIL FROM: alice@webster.edu
250 Ok
RCPT TO bob@example.com
250 Ok
RCPT TO eve@example.com
250 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
From: Alice <alice@webster.edu>
To: Bob <bob@example.com>
Cc: Eve <eve@example.com>
Date: Wed, 13 August 2014 18:02:43 -0500
Subject: Test message

This is a test message.
.
250 OK id=1OjReS-0005kT-Jj
QUIT
221 Bye
```

TCP session

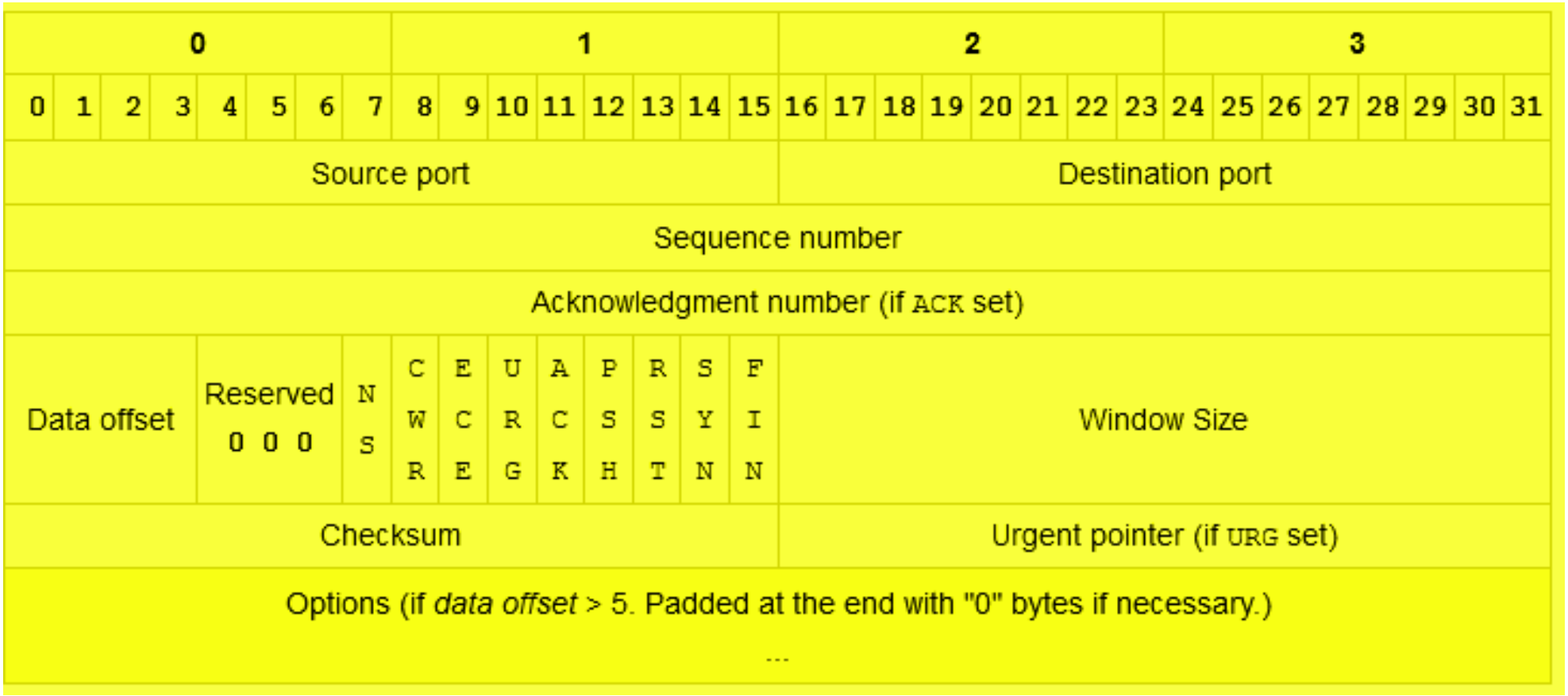


A **three-way handshake**
SYN →
← SYN/ACK
ACK →
begins the session.

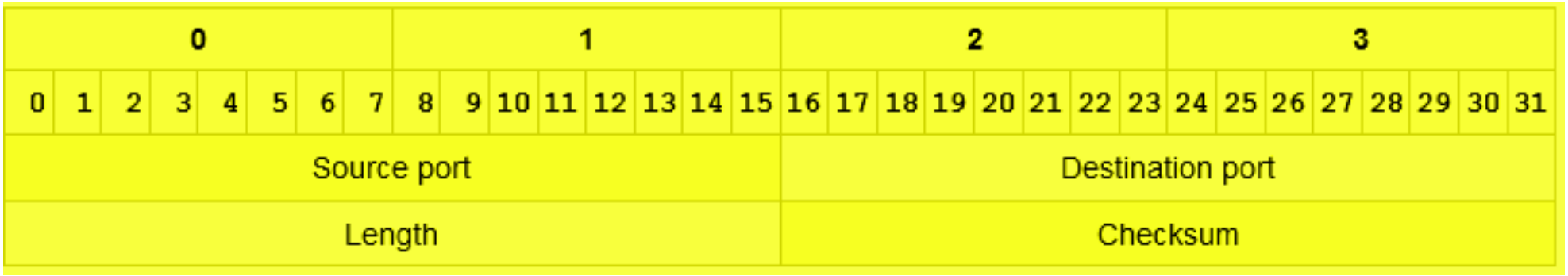
A **four-way handshake**
FIN →
← ACK
← FIN
ACK →
ends the session.

The session can also be abruptly terminated by either side:
RST →

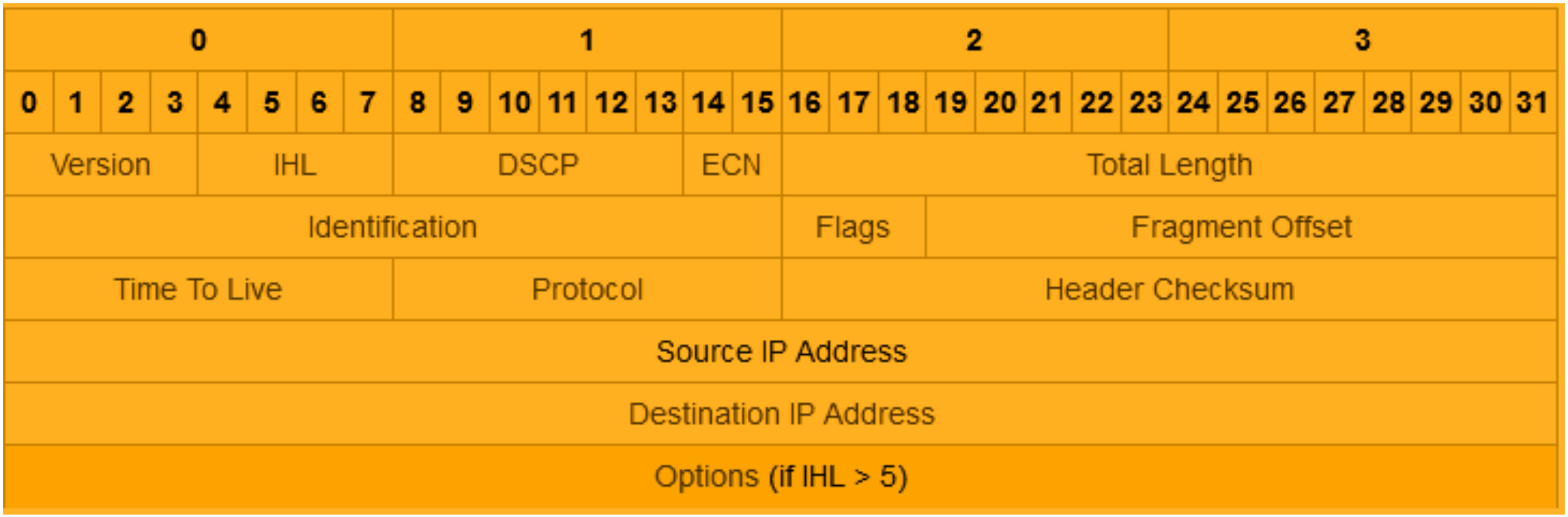
TCP header


0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Source port
Destination port
Sequence number
Acknowledgment number (if ACK set)
Data offset
Reserved
0 0 0
NS
CWR
ECE
URG
ACK
PSH
RST
SYN
FIN
Window Size
Checksum
Urgent pointer (if URG set)
Options (if data offset > 5. Padded at the end with "0" bytes if necessary.)
...

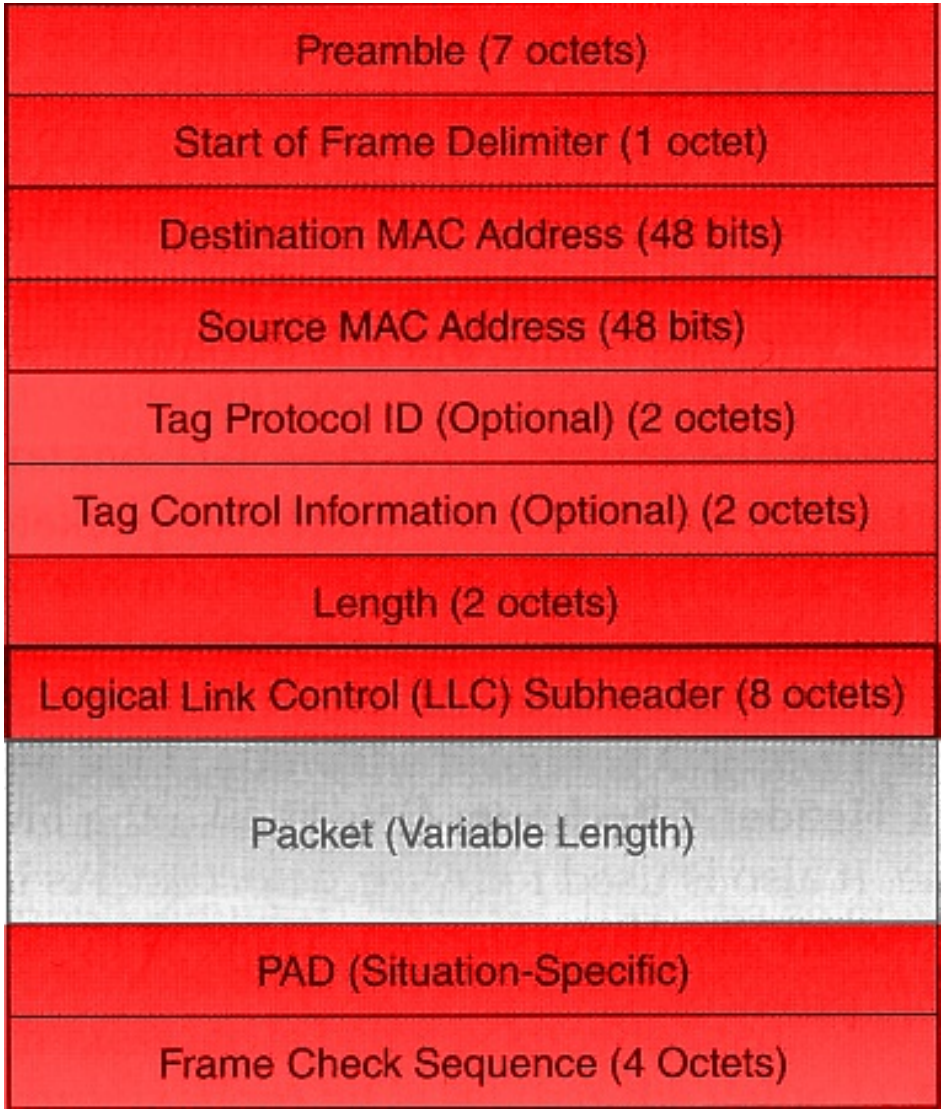
UDP header


0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Source port
Destination port
Length
Checksum

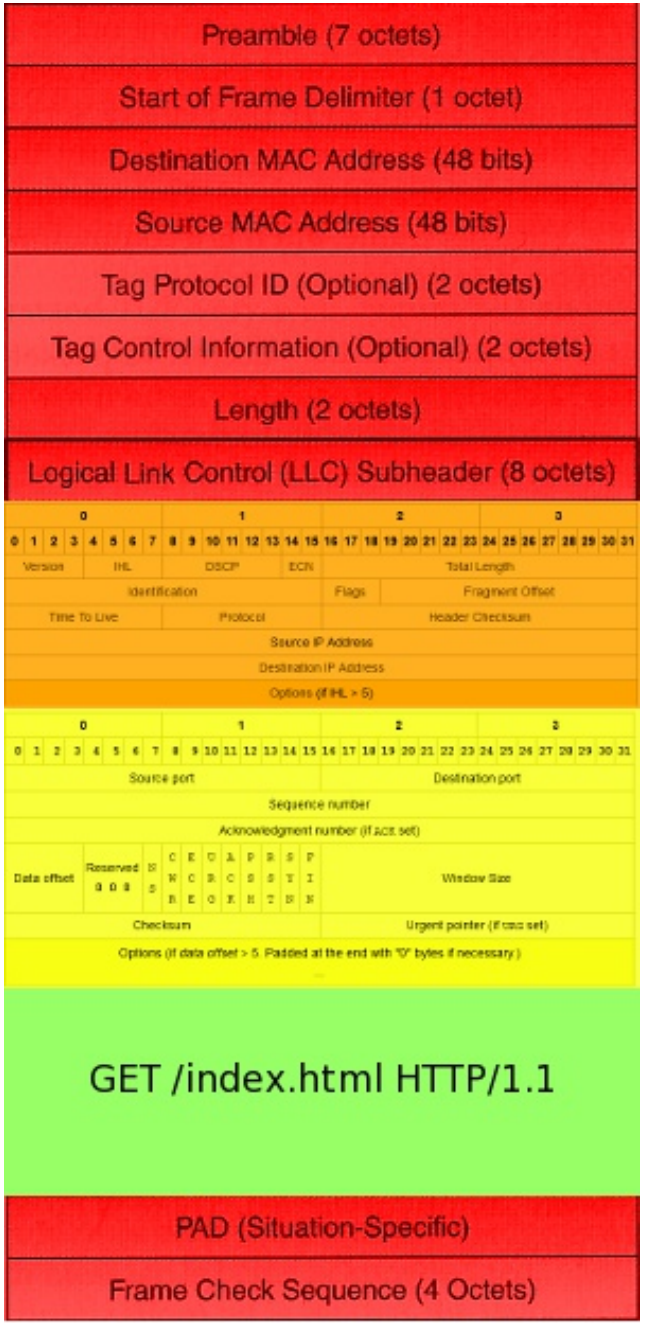
IPv4 header


0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
Version
IHL
DSCP
ECN
Total Length
Identification
Flags
Fragment Offset
Time To Live
Protocol
Header Checksum
Source IP Address
Destination IP Address
Options (if IHL > 5)

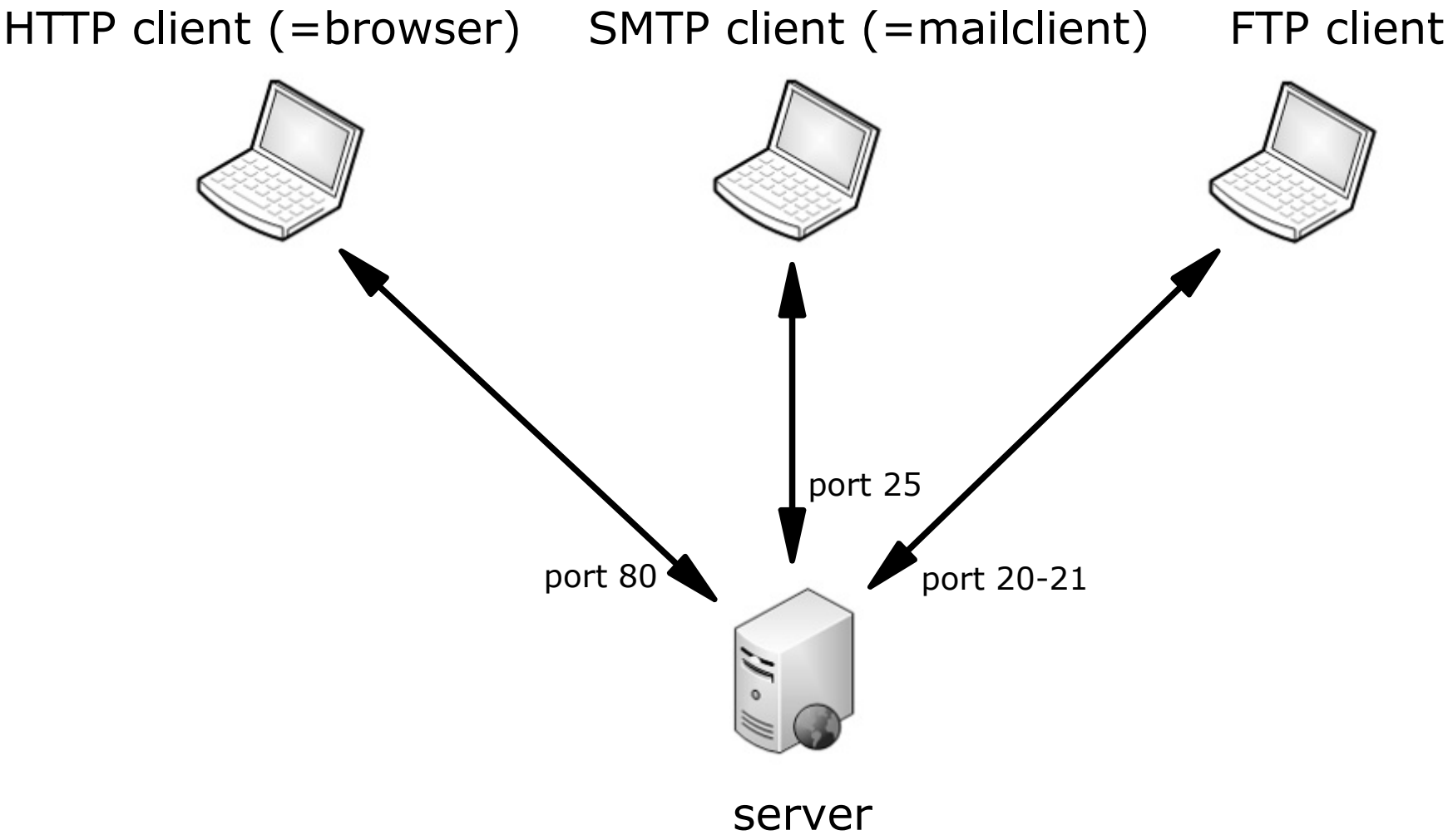
Ethernet header and trailer



The complete frame:

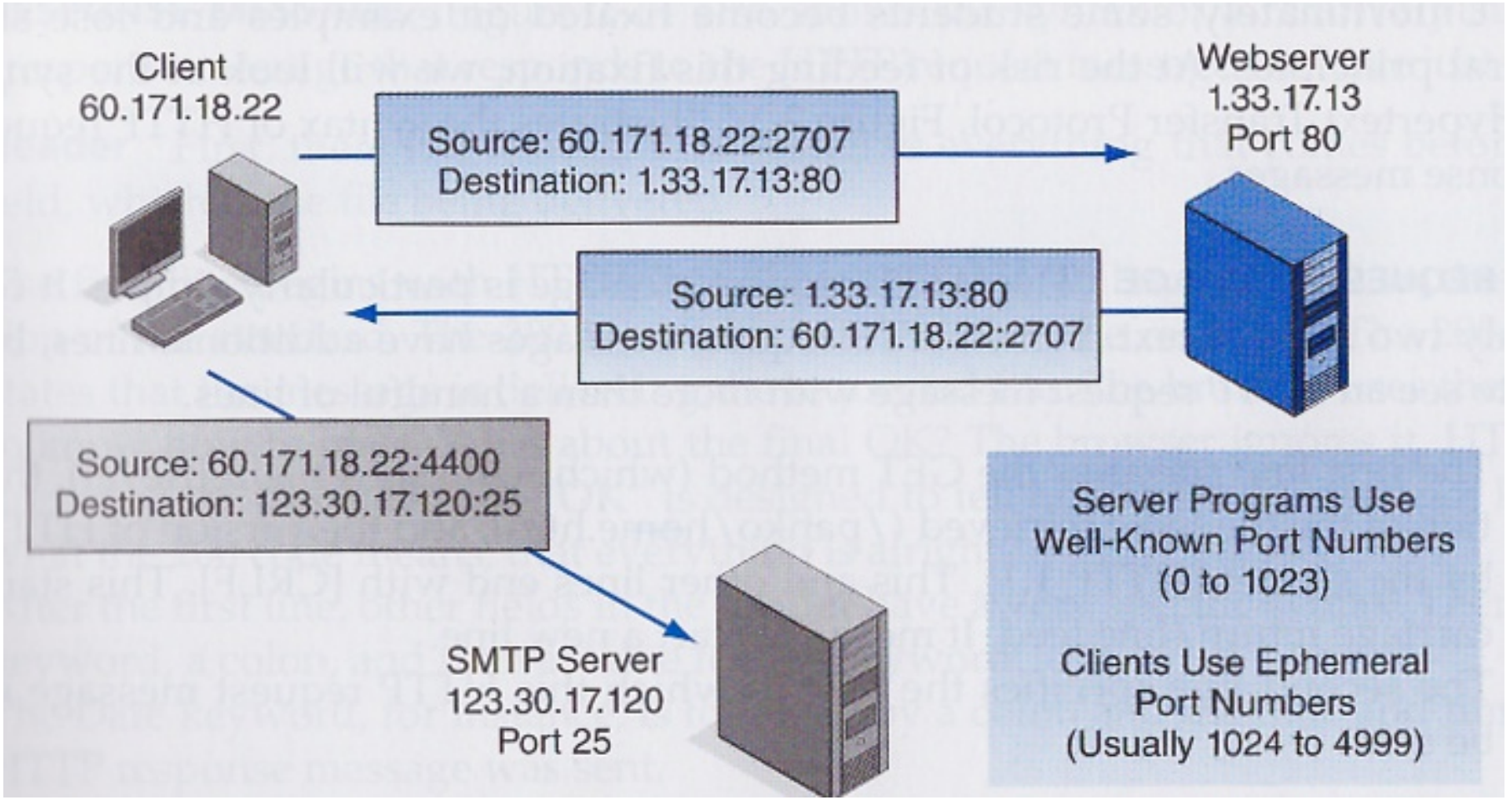


Network services and port numbers



Most frequently used well-known ports		
Port number		**Service**
20	TCP	FTP (data)
21	TCP	FTP (control)
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	TCP/UDP	DNS
67	UDP	BOOTP/DHCP (server)
68	UDP	BOOTP/DHCP (client)
80	TCP	HTTP
110	TCP	POP3
119	TCP	NNTP
139	TCP/UDP	Microsoft NetBIOS
143	TCP	IMAP
161	UDP	SNMP
443	TCP	HTTPS (HTTP over SSL/TLS)
465	TCP	SMTP over SSL
993	TCP	IMAPS (IMAP over SSL)
995	TCP	POP3S (POP3 over SSL)

1-1023: privileged ports, used server-side
1024-65535: unprivileged ports, used client-side



Connections are identified by their **socket** (*address:port*)

To display current network connections: `netstat -f`

7-bit ASCII encoding table

ASCII value	Character	Control character	ASCII value	Character	ASCII value	Character	ASCII value	Character
000	(null)	NUL	032	(space)	064	@	096	
001	☺	SOH	033	!	065	A	097	a
002	☻	STX	034	"	066	B	098	b
003	♥	ETX	035	#	067	C	099	c
004	♦	EOT	036	$	068	D	100	d
005	♣	ENQ	037	%	069	E	101	e
006	♠	ACK	038	&	070	F	102	f
007	(beep)	BEL	039	'	071	G	103	g
008	◘	BS	040	(	072	H	104	h
009	(tab)	HT	041	)	073	I	105	i
010	(line feed)	LF	042	*	074	J	106	j
011	(home)	VT	043	+	075	K	107	k
012	(form feed)	FF	044	,	076	L	108	l
013	(carriage return)	CR	045	-	077	M	109	m
014	♫	SO	046	.	078	N	110	n
015	☼	SI	047	/	079	O	111	o
016	►	DLE	048	0	080	P	112	p
017	◄	DC1	049	1	081	Q	113	q
018	↕	DC2	050	2	082	R	114	r
019	!!	DC3	051	3	083	S	115	s
020	π	DC4	052	4	084	T	116	t
021	§	NAK	053	5	085	U	117	u
022	▬	SYN	054	6	086	V	118	v
023	↨	ETB	055	7	087	W	119	w
024	↑	CAN	056	8	088	X	120	x
025	↓	EM	057	9	089	Y	121	y
026	→	SUB	058	:	090	Z	122	z
027	←	ESC	059	;	091	[	123	{
028	(cursor right)	FS	060	<	092	\	124	¦
029	(cursor left)	GS	061	=	093	]	125	}
030	(cursor up)	RS	062	>	094	^	126	~
031	(cursor down)	US	063	?	095	_	127	⌂

PAN (Personal Area Network)

LAN (Local Area Network)

MAN (Metropolitan Area Network)

WAN (Wide Area Network)

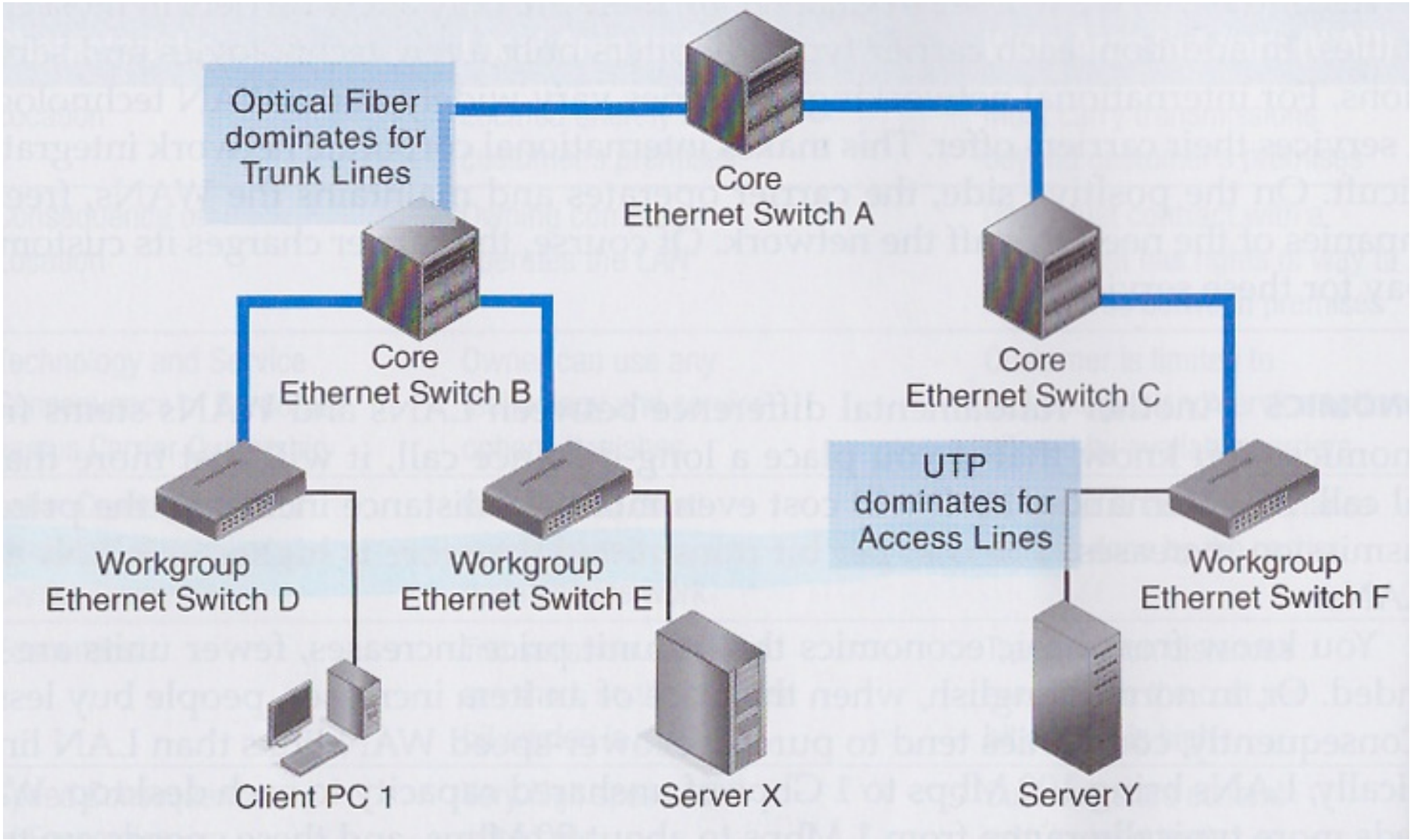


Diagram of an Ethernet LAN

The IEEE 802 LAN/MAN Standards Committee defines the IEEE 802 standards for variable-size packets.
It is composed of **Working Groups**:

802.1 Bridging, Network Management

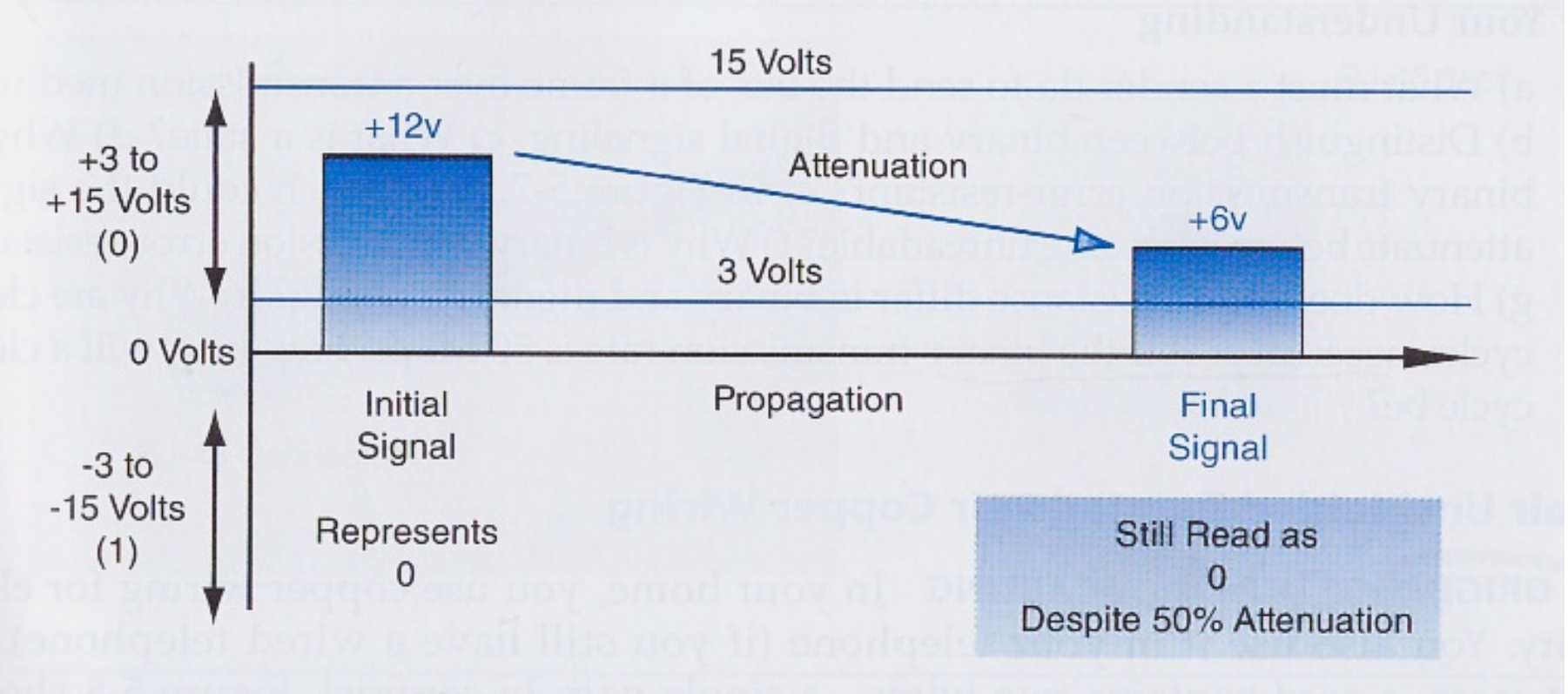
802.3 Ethernet

802.11 Wireless LANs (Wi-Fi)
- **802.11b** and **802.11g** use the 2.4 GHz band
- **802.11a** use the 5 GHz band
- **802.11i** defines the WPA/WPA2 (Wi-Fi Protected Access) standards

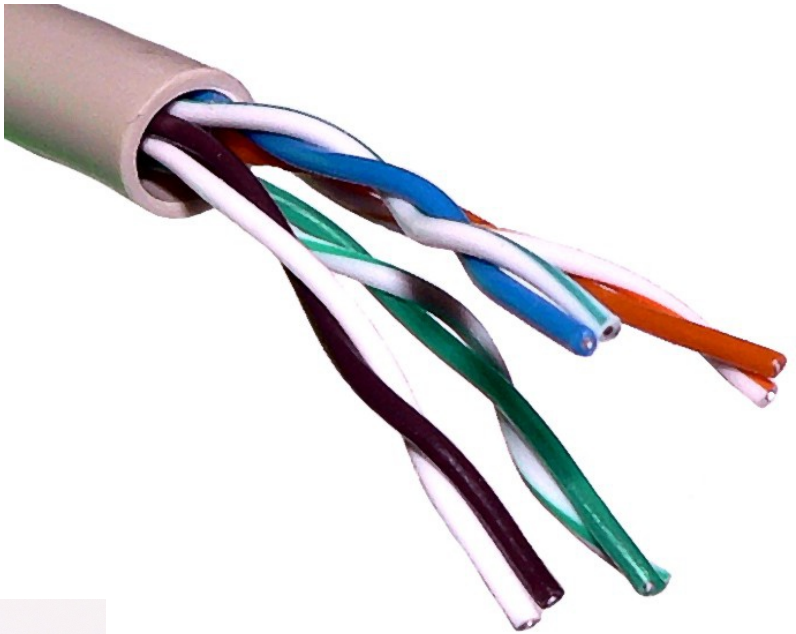
802.15 Wireless PANs
- **802.15.1** Bluetooth

Approval process: WGs $\rightarrow$ IEEE $\rightarrow$ ANSI $\rightarrow$ ISO

Binary (digital) signaling



Ethernet 4-pair UTP (Unshielded Twisted Pair) copper cable

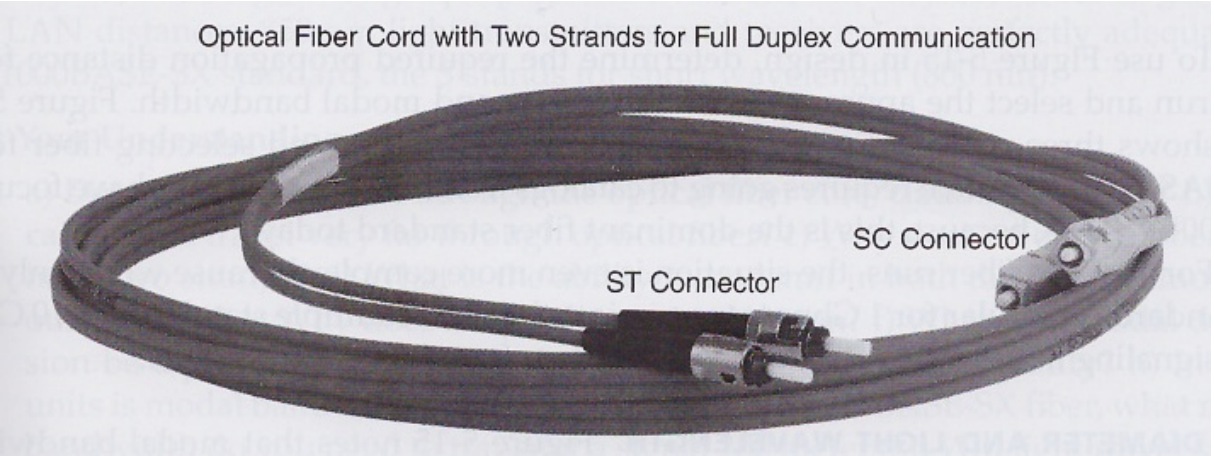


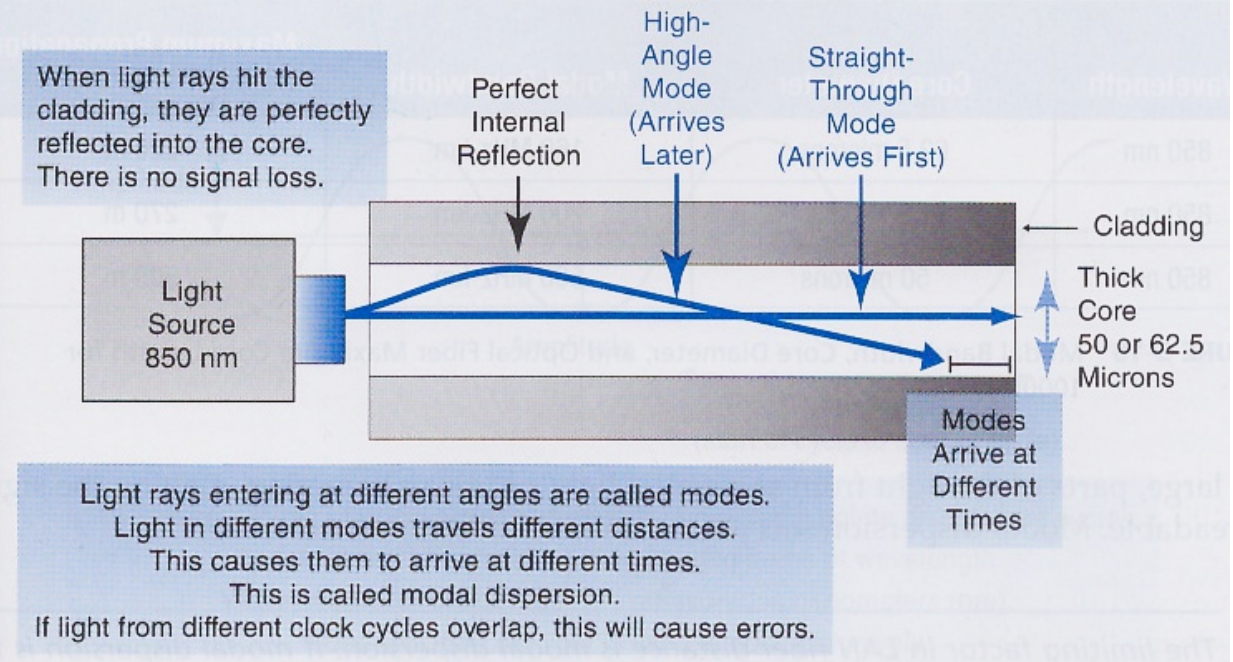
The cable ends with a RJ-45 connector that fits into a RJ-45 jack

Ethernet standard	*medium*
10BASE-T	copper
100BASE-TX	copper
100BASE-FX	fiber optics
1000BASE-T	copper
1000BASE-X	fiber optics
10GBASE-T	copper
10GBASE-LX4	fiber optics

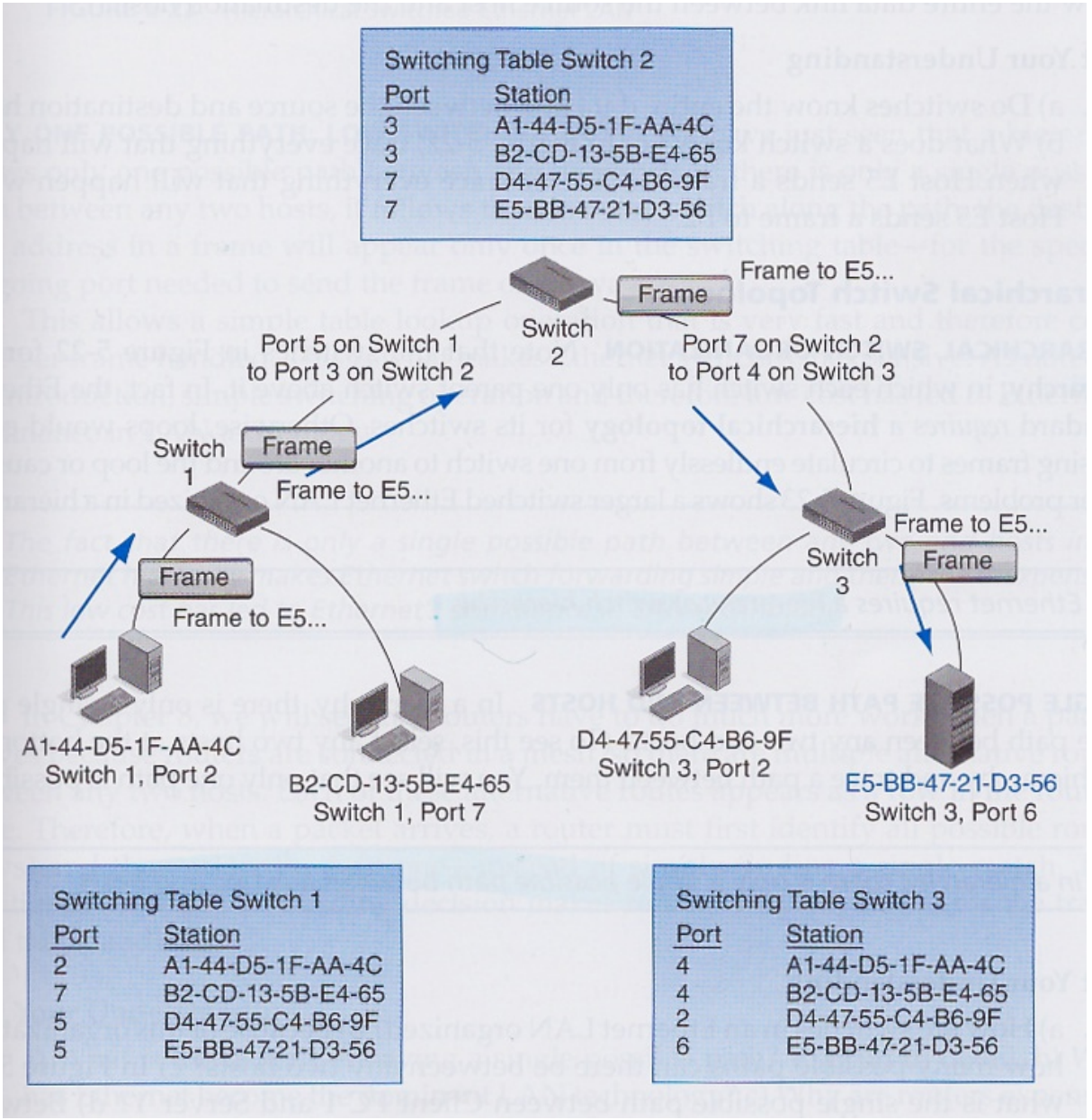
10 Mbps: original **Ethernet** standard (obsolete)
100 Mbps: **Fast Ethernet**
1 Gbps: **Gigabit Ethernet**
10 Gbps: **10-gigabit Ethernet**

Optical Fiber

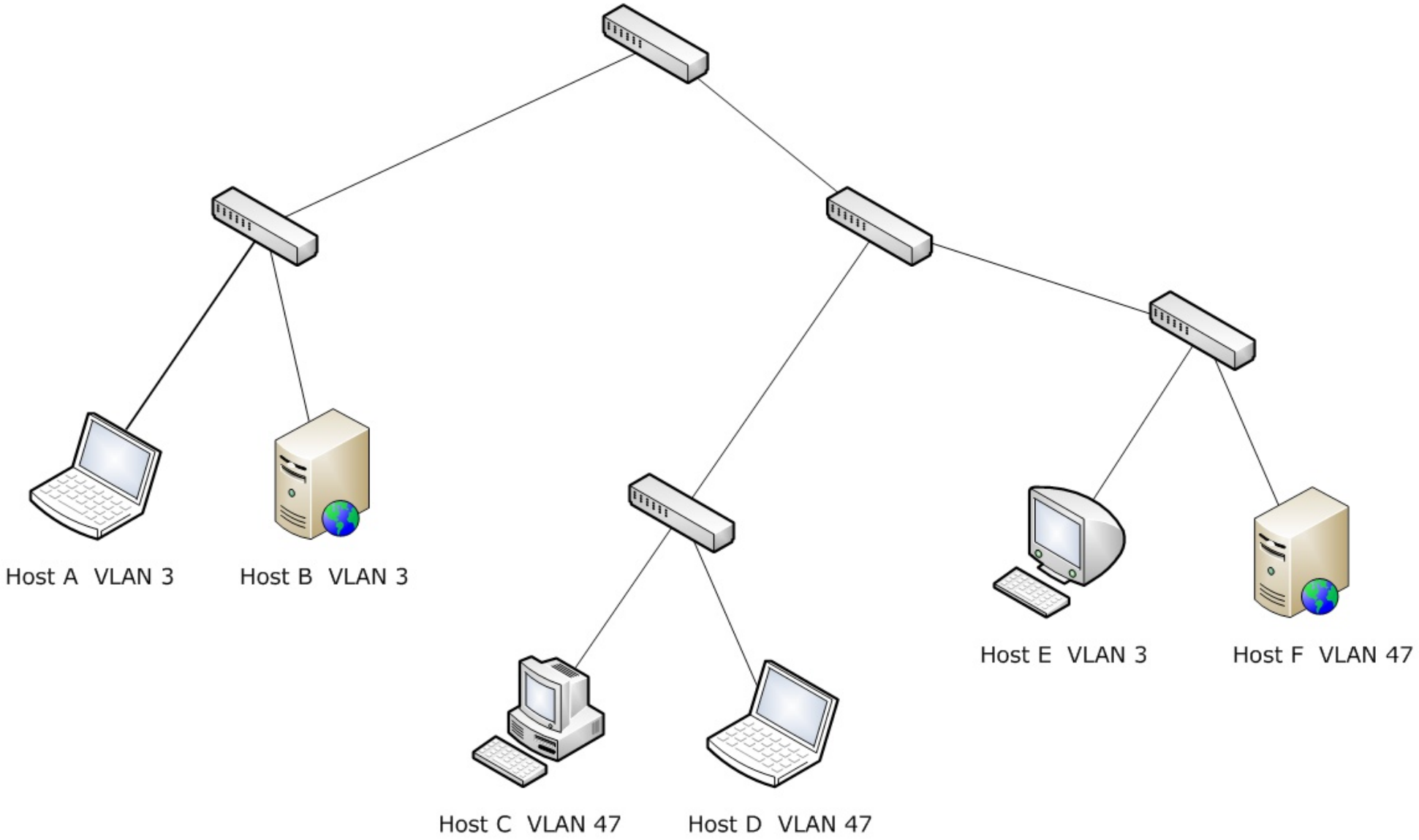




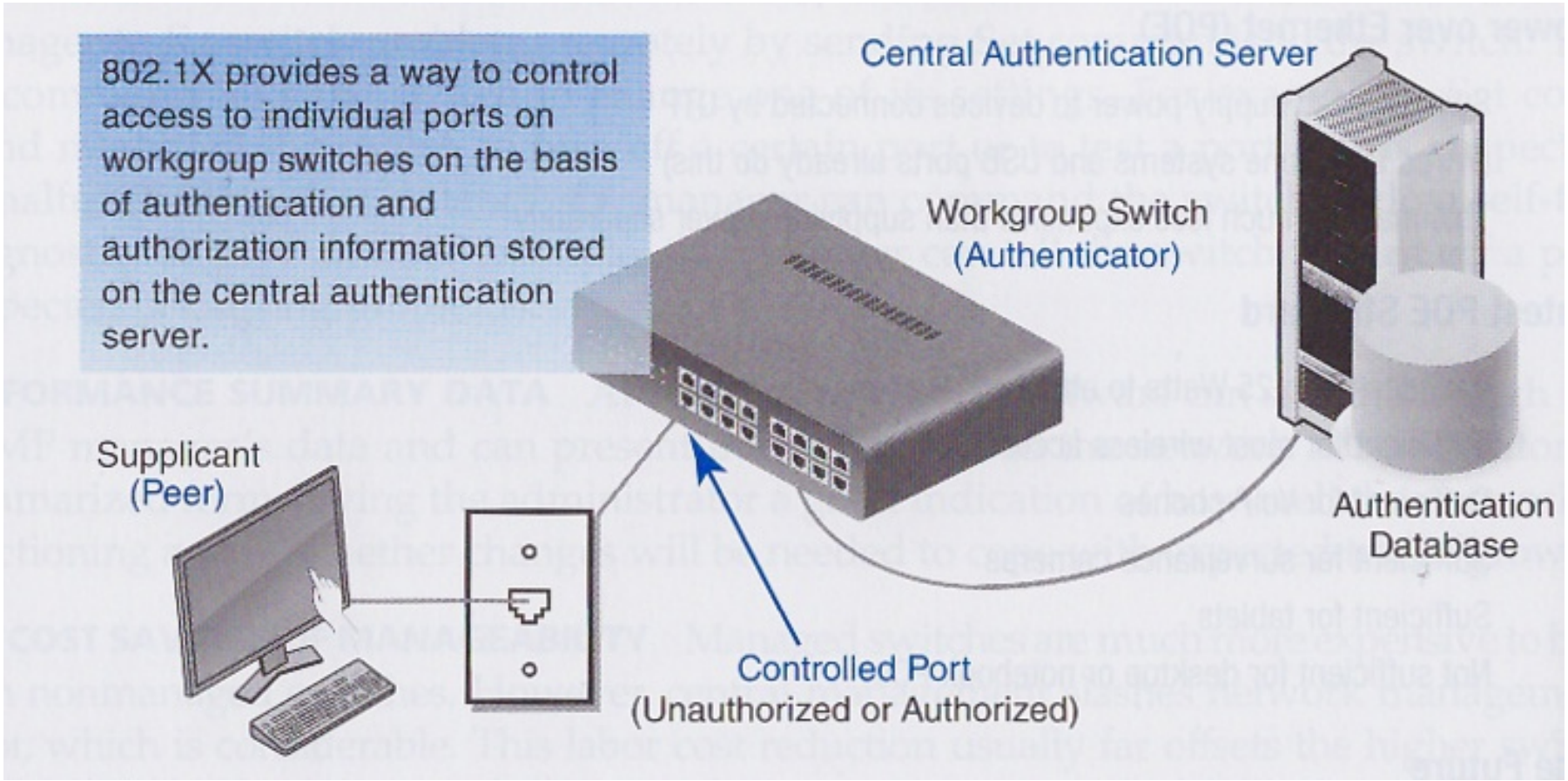
Frame forwarding



VLANs (802.1Q)


Host A VLAN 3
Host B VLAN 3
Host C VLAN 47
Host D VLAN 47
Host E VLAN 3
Host F VLAN 47

Port-Based Access Control (802.1X)



IP addressing

address of a host: 128.171.8.13/16

Address	10000000.10101011.00001000.00001101
Network mask	11111111.11111111.00000000.00000000

network part host part

We AND the address with the netmask to find the network address:

Network address	10000000.10101011.00000000.00000000
or, in decimal:	128.171.0.0/16

Addresses belonging to that network:

10000000.10101011.00000000.00000001
10000000.10101011.00000000.00000010
10000000.10101011.00000000.00000011
...
10000000.10101011.11111111.11111111

IP addressing

host address 128.171.8.13/16
=
host address 128.171.8.13, netmask 255.255.0.0

We can also do a **subnetting** of the network address:

Network address 10000000.10101011.00000000.00000000
Network mask 11111111.11111111.11111111.00000000

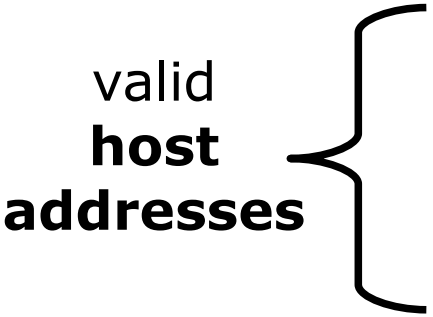
128.171.0.0/24 will provide us with 256 subnets of 254 hosts each:

Network address 10000000.10101011.00000000.00000000
network subnet host

IP addressing

Addresses belonging to the subnet 128.171.17.0/24:

Network address 10000000.10101011.00010001.00000000



10000000.10101011.00010001.00000001
10000000.10101011.00010001.00000010
10000000.10101011.00010001.00000011
...
10000000.10101011.00010001.11111110

Broadcast address 10000000.10101011.00010001.11111111

IP addressing

And if we needed subnets able to accommodate just fifty hosts?
128.171.0.0/26 will provide us with 1024 subnets of 62 hosts each:

Network address 10000000.10101011.00000000.00000000
network subnet host

Amongst all these 1024 subnets, let's consider this one:

Network address 10000000.10101011.00000110.01000000
10000000.10101011.00000110.01000001
10000000.10101011.00000110.01000010
...
10000000.10101011.00000110.01111110
Broadcast address 10000000.10101011.00000110.01111111

Subnet 128.171.6.64/26 (netmask is 255.255.255.192)
has broadcast address 128.171.6.127
and valid hosts in the range 128.171.6.65 - 128.171.6.126

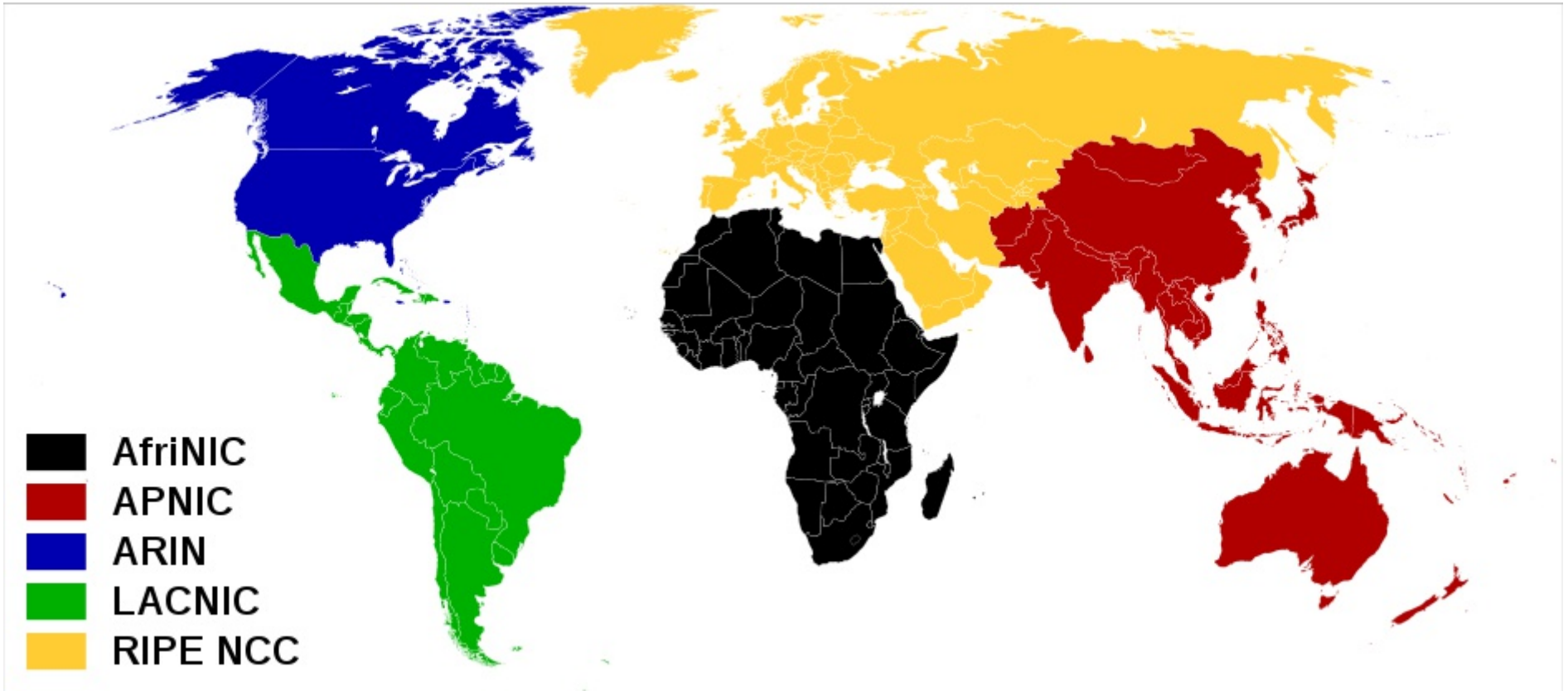
Prefix	**Netmask** *(bin)*	**Netmask** *(dec)*
...		
/8	11111111.00000000.00000000.00000000	255.0.0.0
/9	11111111.10000000.00000000.00000000	255.128.0.0
/10	11111111.11000000.00000000.00000000	255.192.0.0
/11	11111111.11100000.00000000.00000000	255.224.0.0
/12	11111111.11110000.00000000.00000000	255.240.0.0
/13	11111111.11111000.00000000.00000000	255.248.0.0
/14	11111111.11111100.00000000.00000000	255.252.0.0
/15	11111111.11111110.00000000.00000000	255.254.0.0
/16	11111111.11111111.00000000.00000000	255.255.0.0
/17	11111111.11111111.10000000.00000000	255.255.128.0
/18	11111111.11111111.11000000.00000000	255.255.192.0
/19	11111111.11111111.11100000.00000000	255.255.224.0
/20	11111111.11111111.11110000.00000000	255.255.240.0
/21	11111111.11111111.11111000.00000000	255.255.248.0
/22	11111111.11111111.11111100.00000000	255.255.252.0
/23	11111111.11111111.11111110.00000000	255.255.254.0
/24	11111111.11111111.11111111.00000000	255.255.255.0
/25	11111111.11111111.11111111.10000000	255.255.255.128
		...

IPv4 classful addressing

	Address range	Prefix	Number of addresses
Class A (Unicast)	0.0.0.0 – 127.255.255.255 first octet: 0XXX XXXX	/8	128 networks × 16,777,216 addresses
Class B (Unicast)	128.0.0.0 – 191.255.255.255 first octet: 10XX XXXX	/16	16,384 networks × 65,536 addresses
Class C (Unicast)	192.0.0.0 – 223.255.255.255 first octet: 110X XXXX	/24	2,097,152 networks × 256 addresses
Class D (Multicast)	224.0.0.0 – 239.255.255.255 first octet: 1110 XXXX	/4	268,435,456
Class E (Experimental)	240.0.0.0 – 255.255.255.255 first octet: 1111 XXXX	/4	268,435,456
Private Class A	10.0.0.0 – 10.255.255.255	10.0.0.0/8	16,777,216
Private Class B	172.16.0.0 – 172.31.255.255	172.16.0.0/12	1,048,576
Private Class C	192.168.0.0 – 192.168.255.255	192.168.0.0/16	65,536

The inefficiency of classful addressing caused address exhaustion. Solutions: CIDR, private addresses + NATing, name-based virtual hosting, and eventually IPv6

IP addresses are assigned by IANA (Internet Assigned Numbers Authority) which delegates to RIRs (Regional Internet Registries).



IPv6

IPv6 addresses are 128-bit long (32 hex digits), therefore providing for 3.4 x 10^{38} total addresses.

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

↓ *address shortening*

2001:27:fe56::cd3f:fca

Routing prefix	(= network part)	variable	} 64 bits
Subnet ID	(= subnet part)	variable	
Interface ID	(= host part)	64 bits	

IPv6

How to convert a MAC address into a **EUI-64 Interface ID**:

A0-B1-C2-D3-E4-F5

↓ *insert 0xfffe in the middle*

a0b1:c2ff:fed3:e4f5

↓ *flip the 2nd least-significant bit of the 1st octet*

a2b1:c2ff:fed3:e4f5

IPv6 stateless autoconfiguration

A host can create its own **link-local** address to communicate within its own network only:

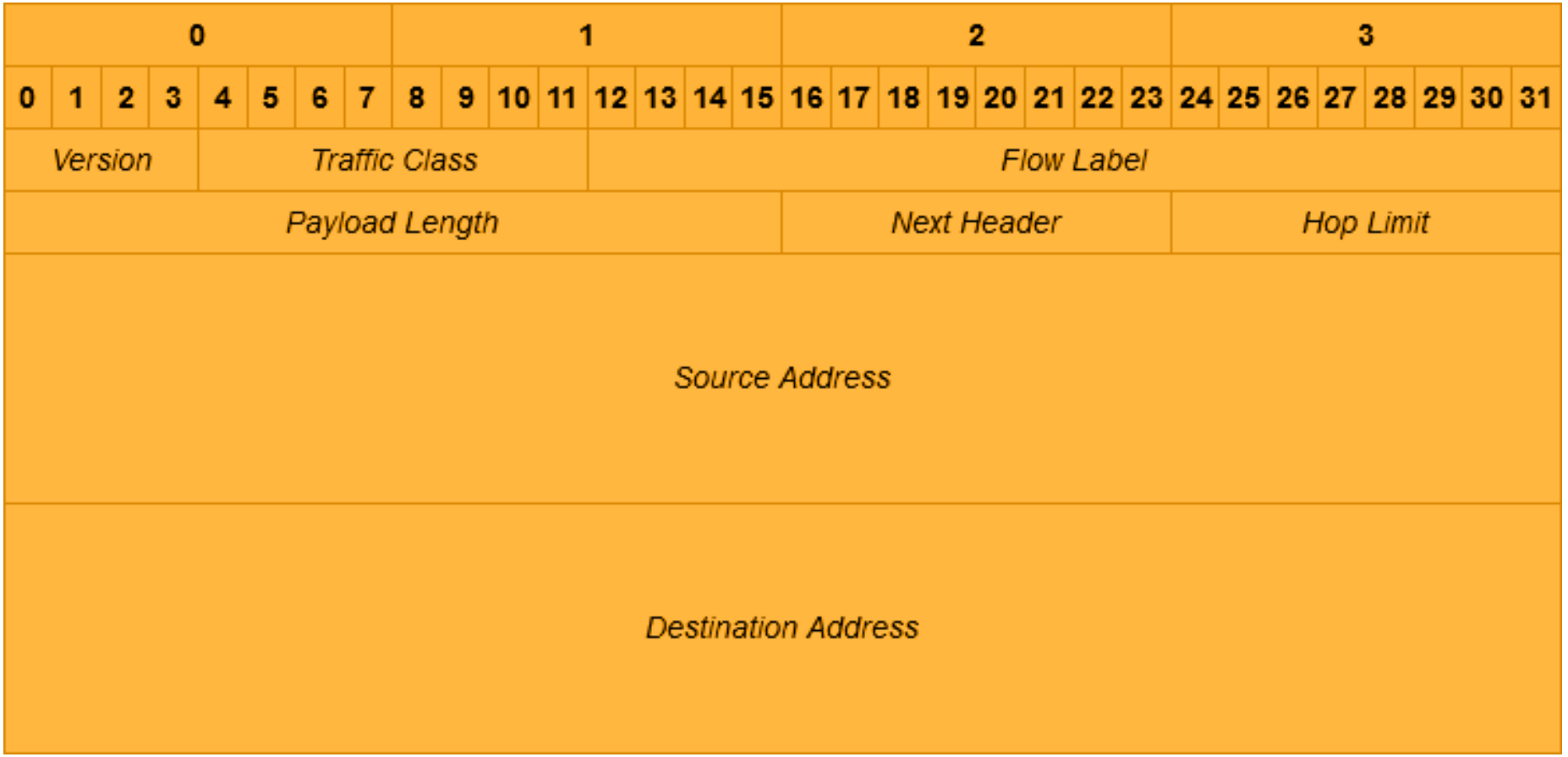
fe80:0000:0000:0000 + computed EUI-64

Before using it, the host checks (via the ICMPv6 **neighbor discovery protocol**) that this link-local address is not in use yet.

To communicate outside its network, a host needs to send a ICMPv6 **router solicitation** to multicast address ff02::1

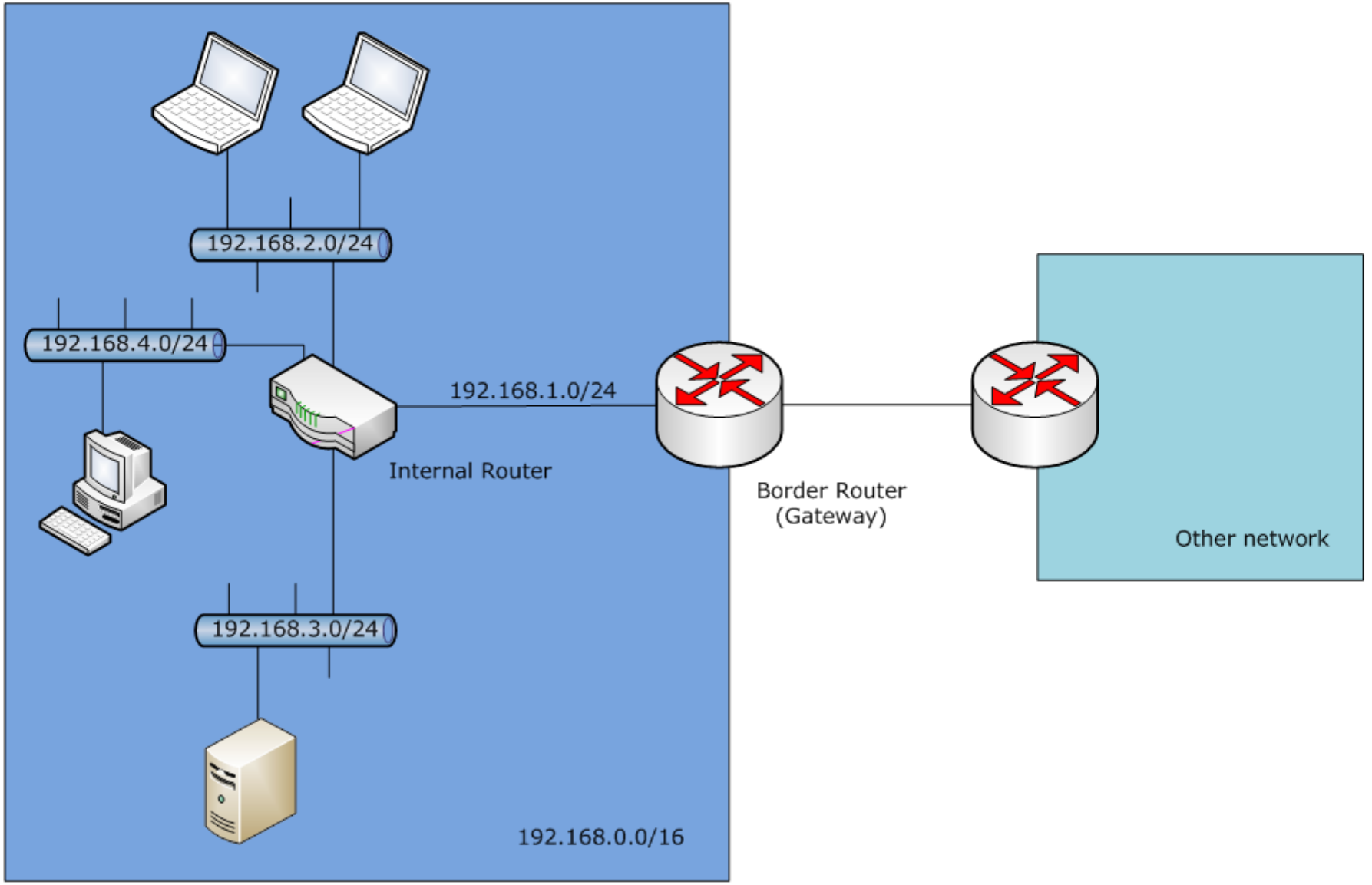
One (or more) routers reply with a ICMPv6 **router advertisement** assigning the router prefix and subnet ID to the host

IPv6 header

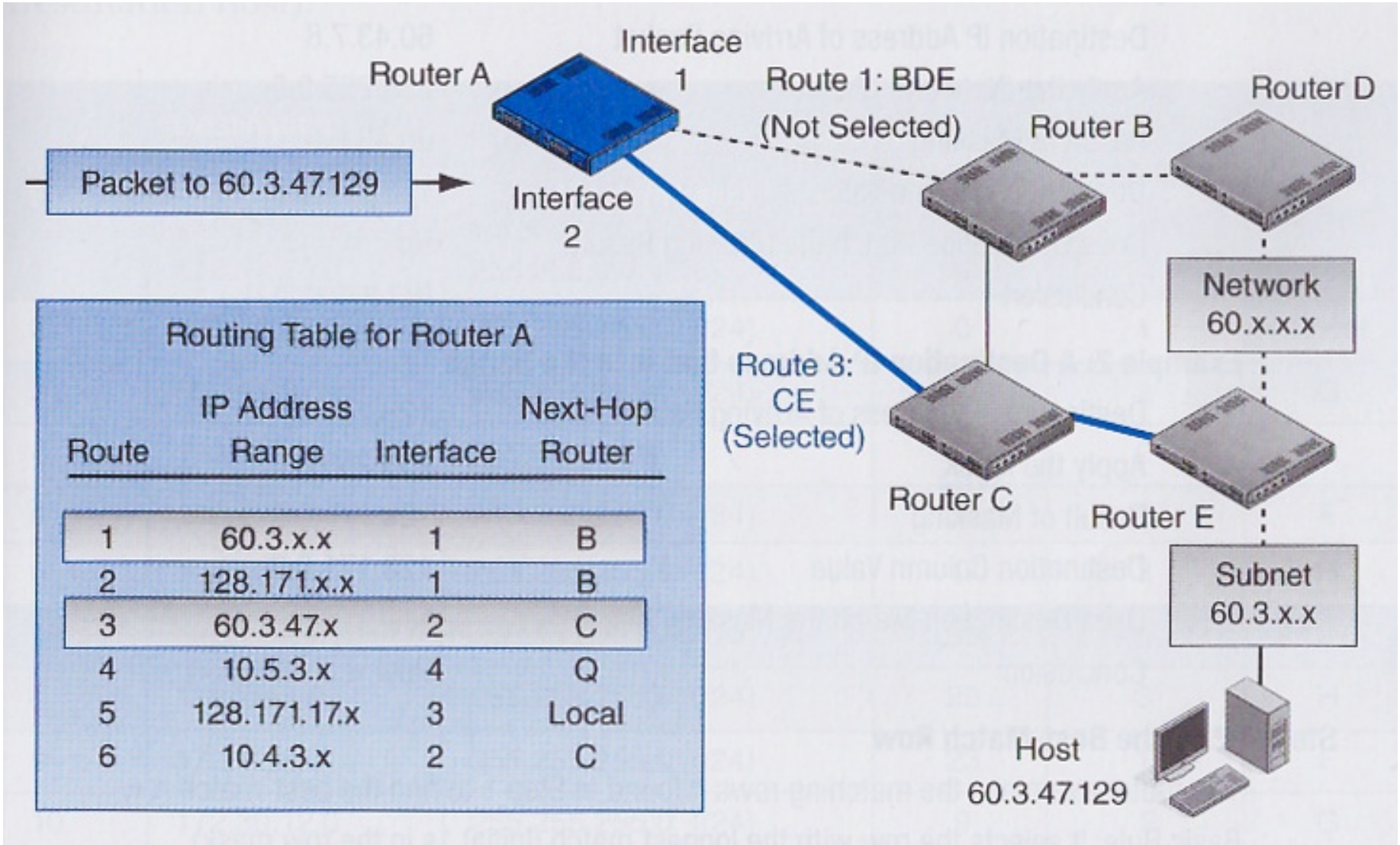


+ daisy chain of extension headers
(the Next Header field contains code# of next header)

Routing


192.168.2.0/24
192.168.4.0/24
192.168.1.0/24
Internal Router
Border Router
(Gateway)
Other network
192.168.3.0/24
192.168.0.0/16

Routing



Routing Table for Router A

Route	IP Address Range	Interface	Next-Hop Router
1	60.3.x.x	1	B
2	128.171.x.x	1	B
3	60.3.47.x	2	C
4	10.5.3.x	4	Q
5	128.171.17.x	3	Local
6	10.4.3.x	2	C

Routing table

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

Routing protocols

Interior (inside an Autonomous System):

RIP (Routing Information Protocol)

OSPF (Open Shortest Path First)

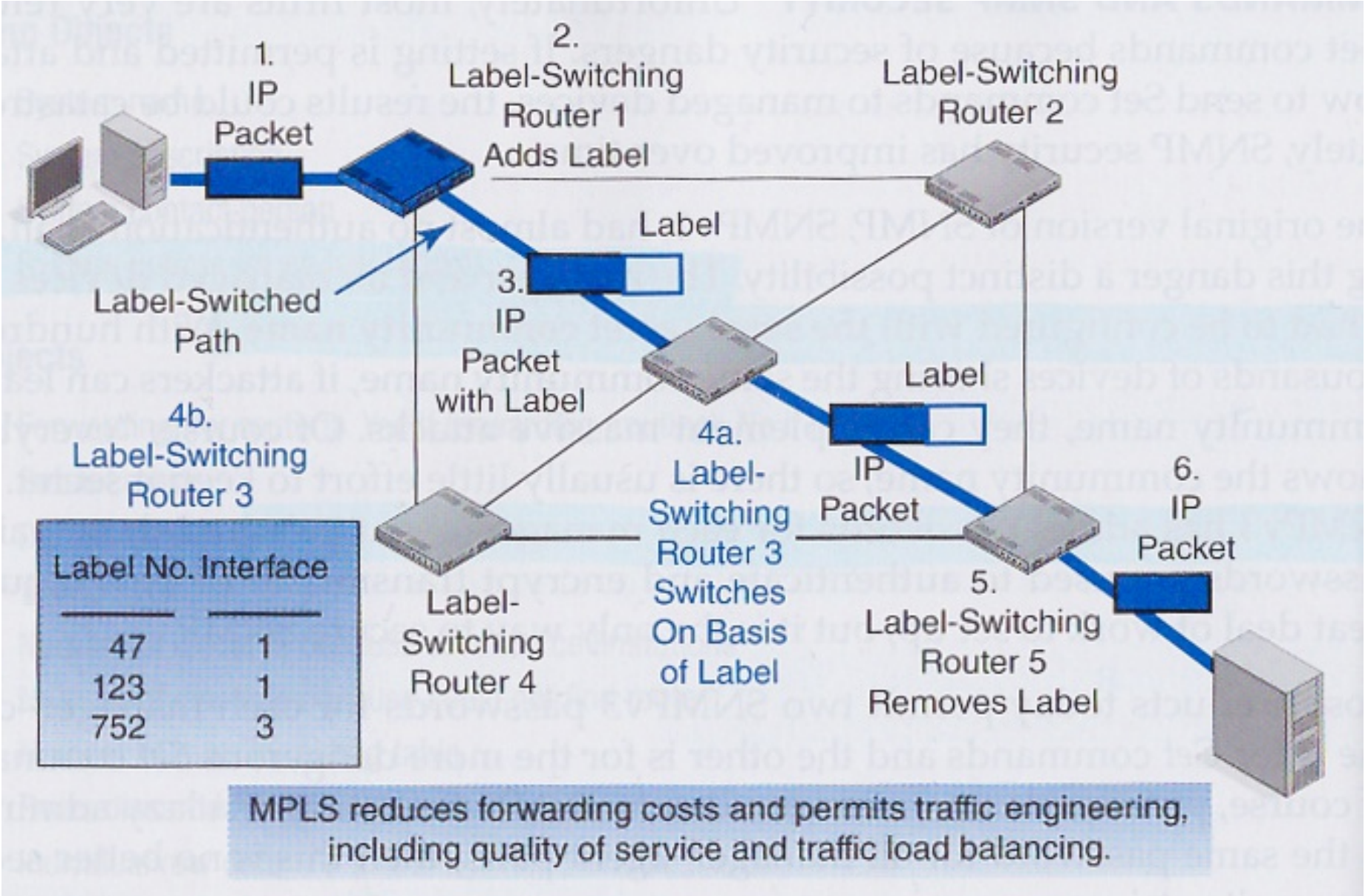
EIGRP (Enhanced Interior Gateway Routing Protocol)

Exterior:

BGP (Border Gateway Protocol)

For simple networks, we can use **static routes** instead of dynamic routes established by the routing protocol .

MPLS (MultiProtocol Label Switching)



ARP (Address Resolution Protocol)

ARP translates IP addresses (layer 3) into MAC addresses (layer 2).

When a router has to forward a packet to next hop 10.19.8.17:
- If the router has a entry in its ARP cache, it uses it, otherwise:
- The router sends out a ARP request for IP address 10.19.8.17 with destination **Ethernet broadcast address** FF-FF-FF-FF-FF-FF
- Host 10.19.8.17 replies with its MAC address A7-23-DA-95-7C-99

ARP information is encapsulated by layer 2, so ARP is a layer 3 protocol. However, ARP data is never routed across internetworks

To display the ARP table (cache) of your machine: `arp -a`

ICMP (Internet Control Message Protocol)

ICMP messages are encapsulated in the IP data field.
They provide error detection and test reachability of remote hosts.

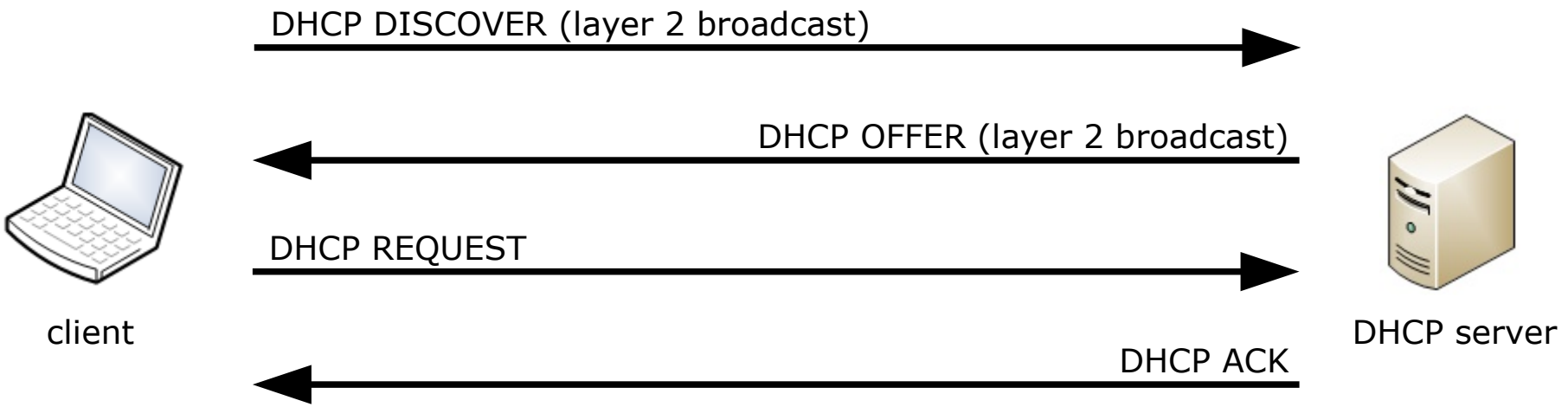
To ping a remote host and measure its RTT (=latency):
`ping 74.125.206.147`
To traceroute to a remote host: `tracert 74.125.206.147`

Examples of ICMP messages:
ICMP ECHO_REQUEST (ping request)
ICMP ECHO_RESPONSE (ping response)
ICMP TIME_EXCEEDED (TTL expired; traceroute uses increasing TTLs times)
ICMP DESTINATION_UNREACHABLE

Firewalls may block ICMP messages for security.
ICMP can be used for DoS attacks (Smurf, ping floods, Ping of Death).

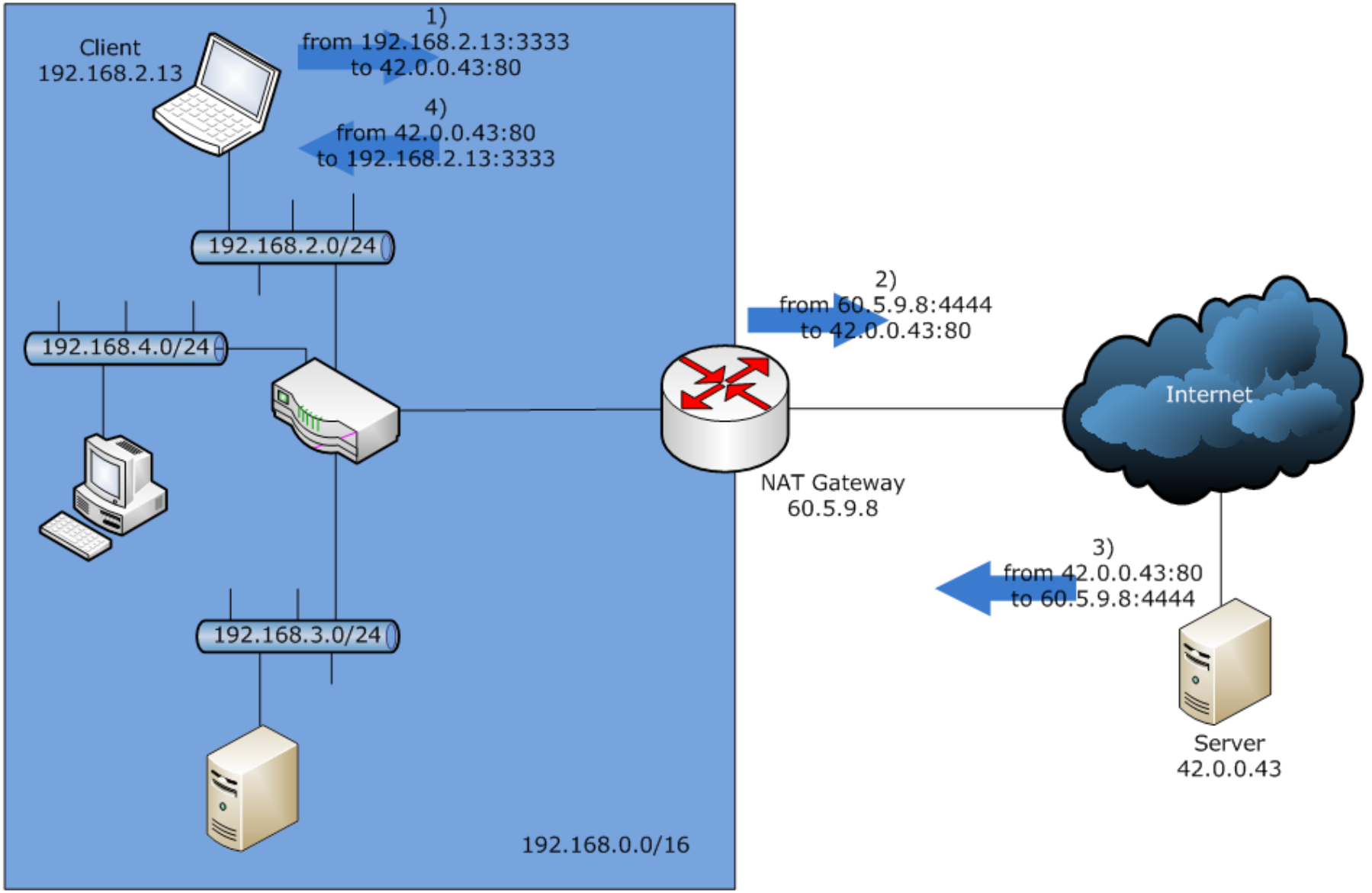
DHCP (Dynamic Host Configuration Protocol)

DHCP provides hosts with a **dynamic** IP address, subnet mask, and IP addresses of default gateway and DNS servers.



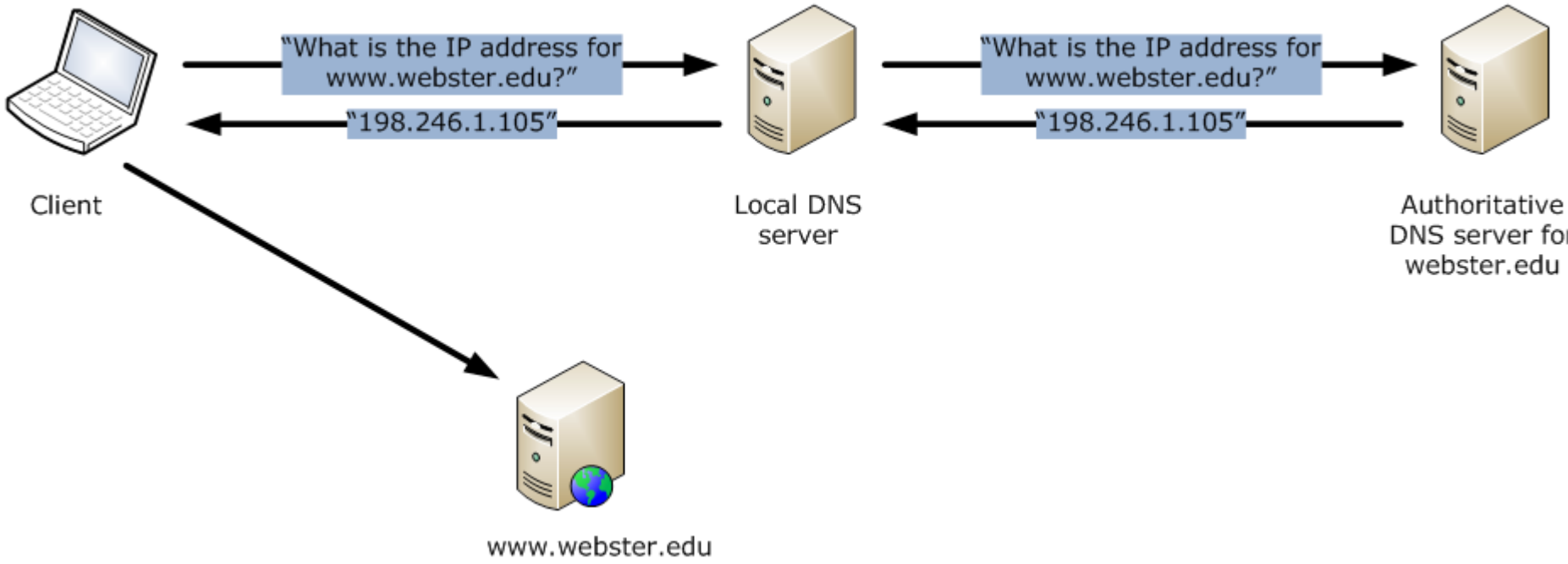
DHCP uses UDP port 68 (client) and 67 (server).
To see DHCP current lease: `ipconfig /all`
To renew the lease: `ipconfig /release` , then `ipconfig /renew`

NAT (Network Address Translation)



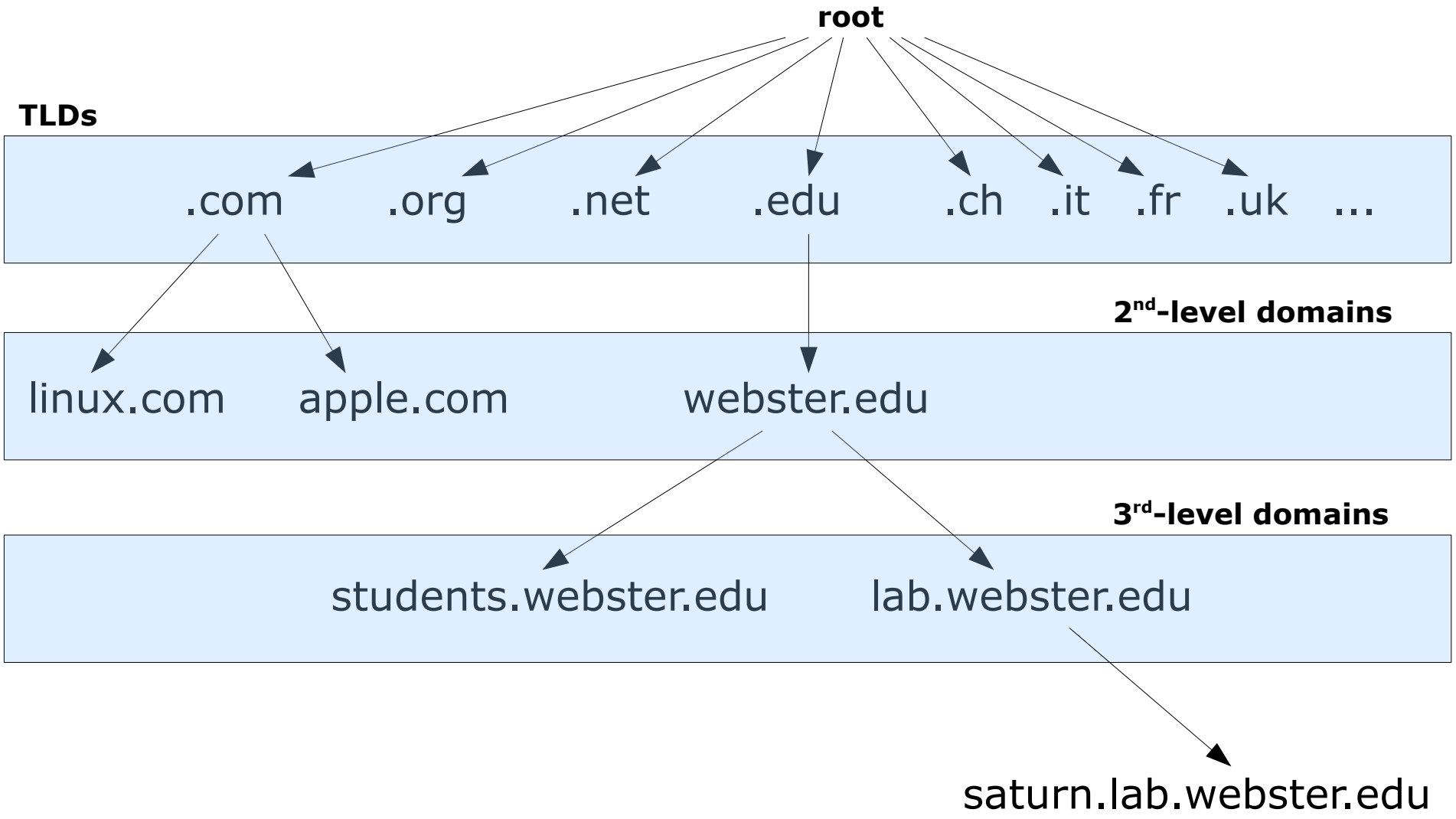
DNS (Domain Name System)

DNS provides name resolution (=conversion from domain name to IP).



In the early days of ARPAnet and Internet, name resolution was provided by a `HOSTS.TXT` file in each host.

DNS hierarchy



DNS

The ICANN (Internet Corporation for Assigned Names and Numbers) controls DNS root and TLDs.
2nd-level domains are obtained from domain name registrars.

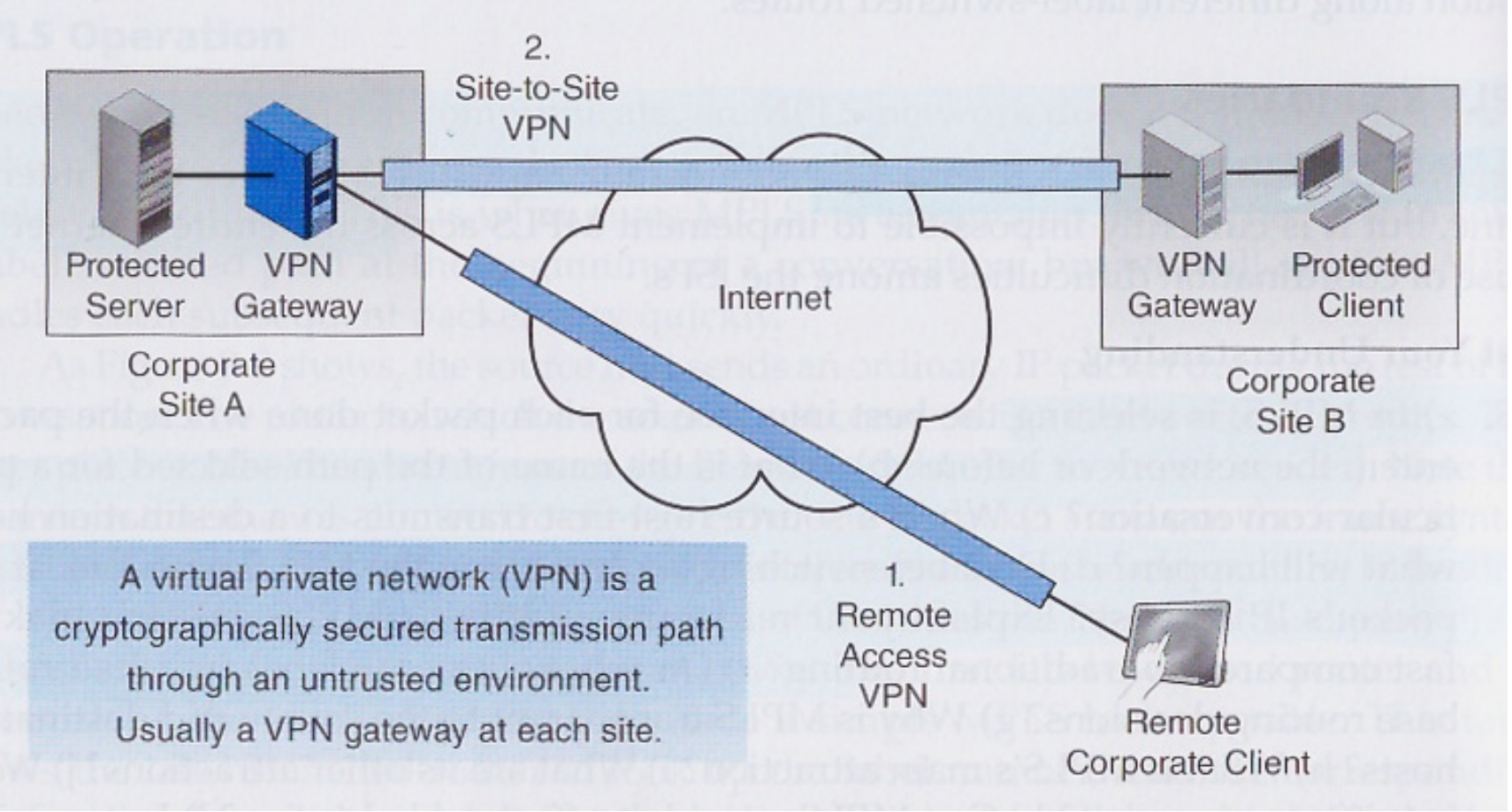
To manually resolve a FQDN: `nslookup www.webster.edu`
or use an online DNS lookup tool e.g.
`http://mxtoolbox.com/DNSLookup.aspx`

DNS zone file

```
$TTL 86400      ; TTL (1 day)
$ORIGIN webster.edu.
webster.edu IN SOA dns1.webster.edu. help.webster.edu. (
   2014052300   ; serial
   28800        ; refresh (8 hours)
   7200         ; retry (2 hours)
   604800       ; expire (1 week)
   600 )        ; negative TTL (10 mins)

        IN NS     dns1.webster.edu.
        IN NS     dns2.webster.edu.
        IN MX     10 mail1.webster.edu.
        IN MX     20 mail2.webster.edu.

dns1    IN A      224.123.240.3
dns2    IN A      224.123.240.4
mail1   IN A      224.123.240.73
mail2   IN A      224.123.240.77
foo     IN A      224.123.240.12
bar     IN A      224.123.240.13
www     IN A      224.123.240.19
baz     IN CNAME  bar

lab     IN NS     ns1.lab.webster.edu.   ; Glue records
        IN NS     ns2.lab.webster.edu.
ns1.lab.webster.edu.   IN A   224.123.240.201
ns2.lab.webster.edu.   IN A   224.123.240.202
```

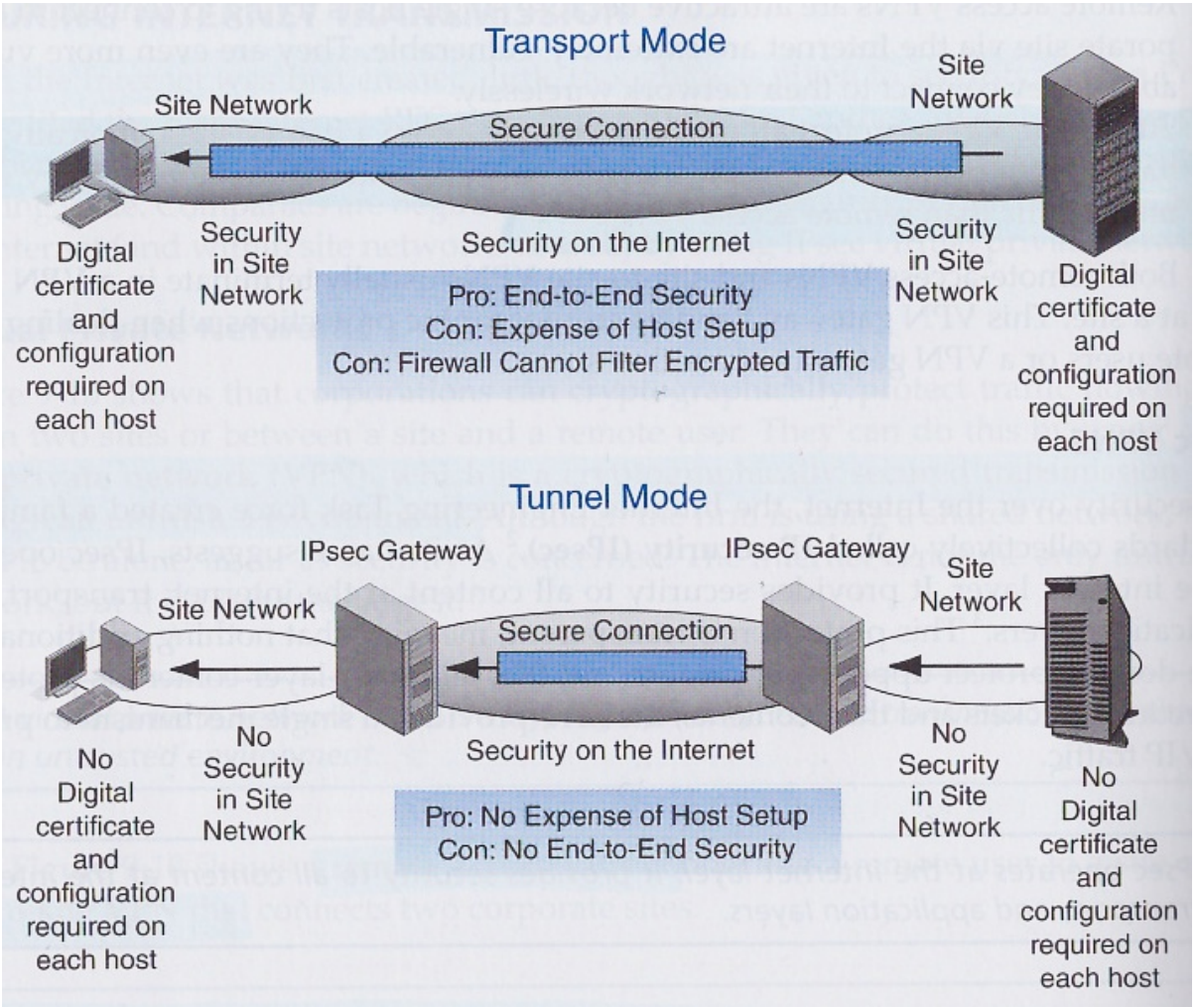
VPN (Virtual Private Network)

Network traffic can be captured by packet sniffers. This can be avoided by using a VPN, which is an encrypted tunnel that protects communications as they flow through the Internet.



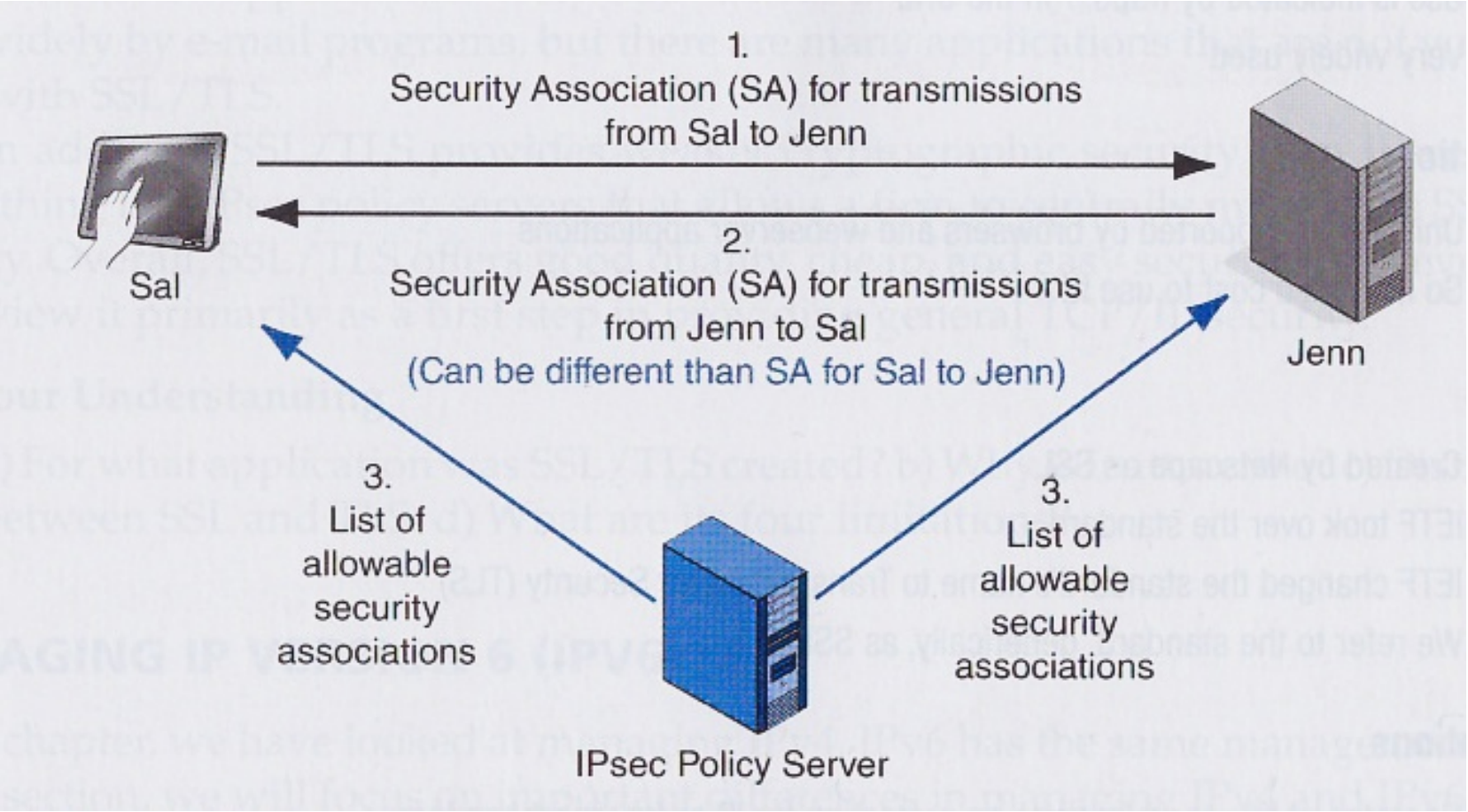
IPsec

IPsec (IP security) is a family of standards by the IETF. It operates at the layer 3 and provides protection to layers 3 to 7.



IPsec

An IPsec **SA (Security Association)** is an agreement about which security methods, cryptographic algorithms, options, and parameters will be used by the two ends of an IPsec communication.



SSL/TLS

SSL (Secure Socket Layer) by Netscape
TLS (Transport Layer Security) by IETF

SSL/TLS provides a cryptographic layer to secure different protocols. In origin, it was created to secure HTTP ($\rightarrow$ **HTTPS**).

SSL/TLS functions at layer 4 and above.

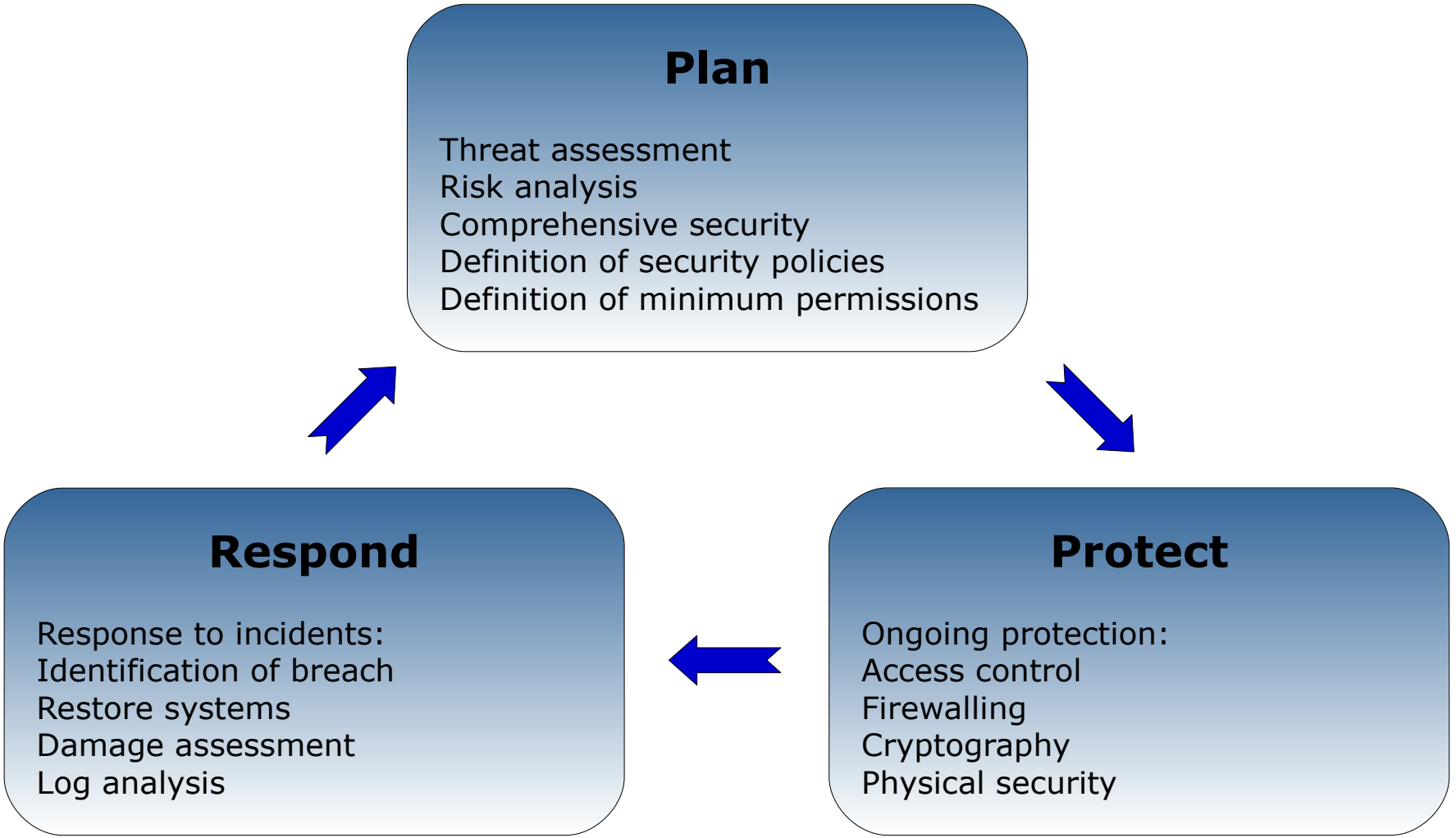
Many VPNs are implemented via SSL/TLS rather than IPsec, as it has a lower cost and is easier to manage.

Security

Important concepts about security:

- *"Security is a process, not a product"* -- Bruce Schneier
- A chain is as strong as its weakest link → **defense in depth**
- Security is inversely related to usability
- It is impossible to eliminate risk; the aim is to mitigate risk to an acceptable security/cost ratio
- *"The enemy knows the system"* -- Claude Shannon → **Security by obscurity** doesn't work when it is used as the only protection

The security cycle



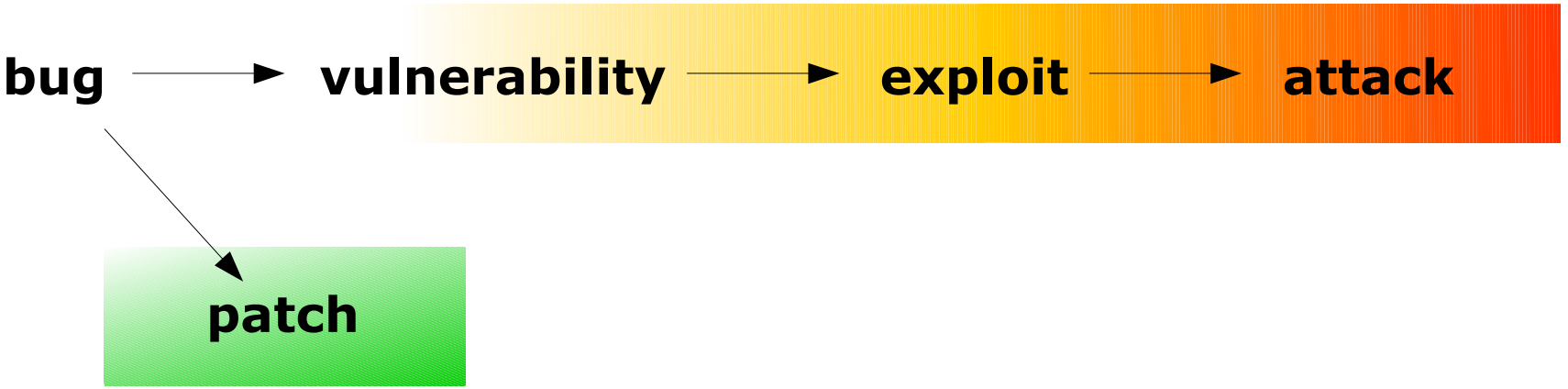
The security cycle

Response

Computer Security Incident Response Team (CSIRT)

- Detect the attack
- Stop the attack
  - Restore security perimeter
  - Remove **backdoors**
- Repair the damage
  - Procedures of **disaster recovery**
  - Reinstall systems
  - Restore data from **backups** (on-site or off-site)
  - Log analysis
- Pursue the attacker
  - **Forensic** procedures

Attacks



0-day attack: an attack that exploits a previously unknown vulnerability in a software (before a patch is available).

Malware

By type:

- **Viruses**
- **Trojan horses**
- **Worms**

By activity:

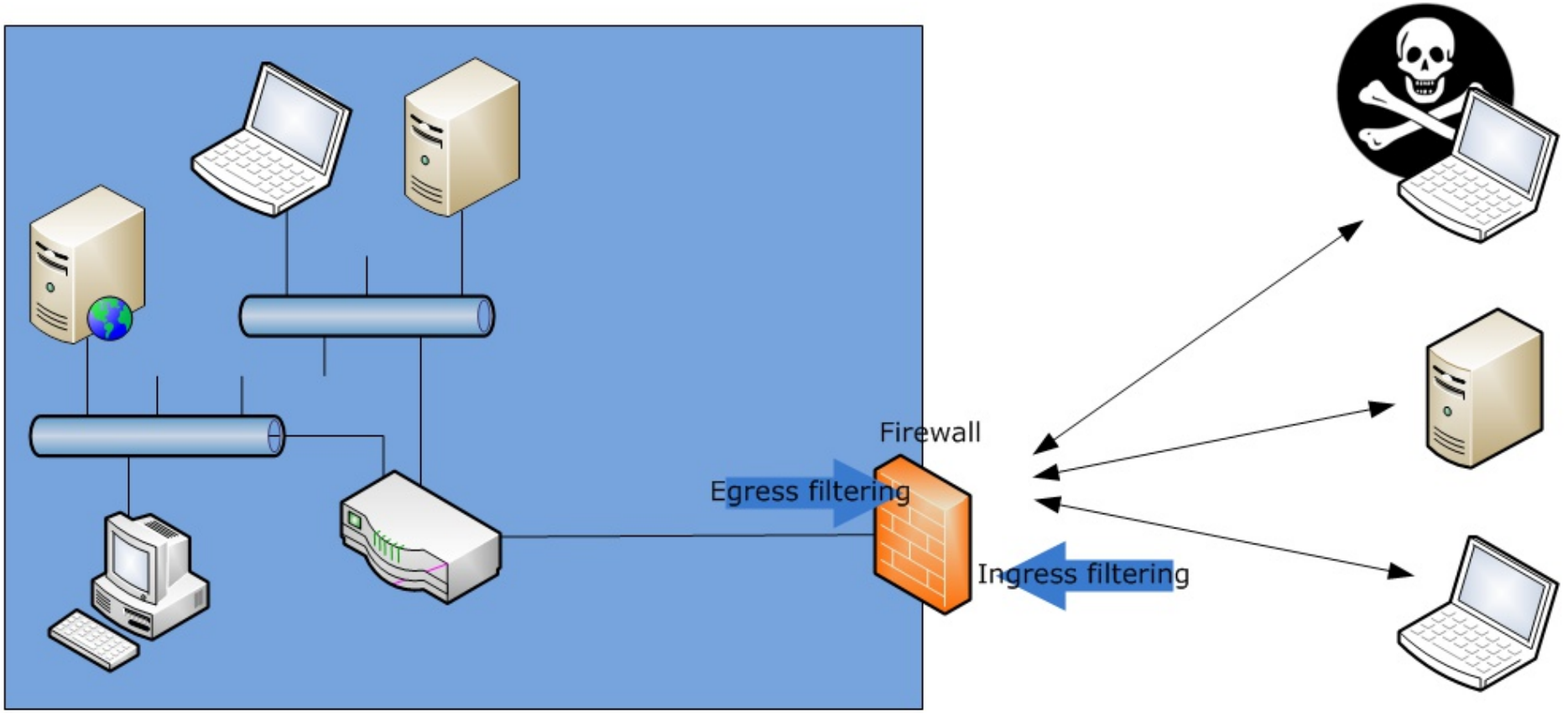
- **Adware** → advertisement, URL hijacking
- **Spyware** → credit card theft, identity theft
  - **Keyloggers**
- **Ransomware**
- Remote control software → **zombie** computer in a **botnet**
- **Dialers** (1990s) → connection hijacking
- **DoS** programs → DoS / DDoS (Denial of Service)

Attacks and defense channels

- Malware: viruses and trojans ← **Antivirus**
- Malware: worms ← **Firewalls**, system updates
- Direct hacking via network ← Firewalls, system updates
- **Social engineering** ← User training, security policies
- Physical attack ← Physical security

Firewalls

A **firewall** is a defensive network appliance that filters incoming or outgoing packets depending on specific criteria.



Firewalls

Static firewall rules:

N	SRC IP	SRC PORT	DEST IP	DEST PORT	DIRECTION	ACTION
1	192.168.3.66	ALL	ALL	80	OUT	DENY
2	192.168.3.0/24	ALL	ALL	80	OUT	ALLOW
3	192.168.0.0/16	ALL	60.13.13.13	25	OUT	ALLOW
4	192.168.0.0/16	ALL	ALL	25	OUT	DENY
5	77.77.77.77	ALL	ALL	ALL	IN	DENY

...

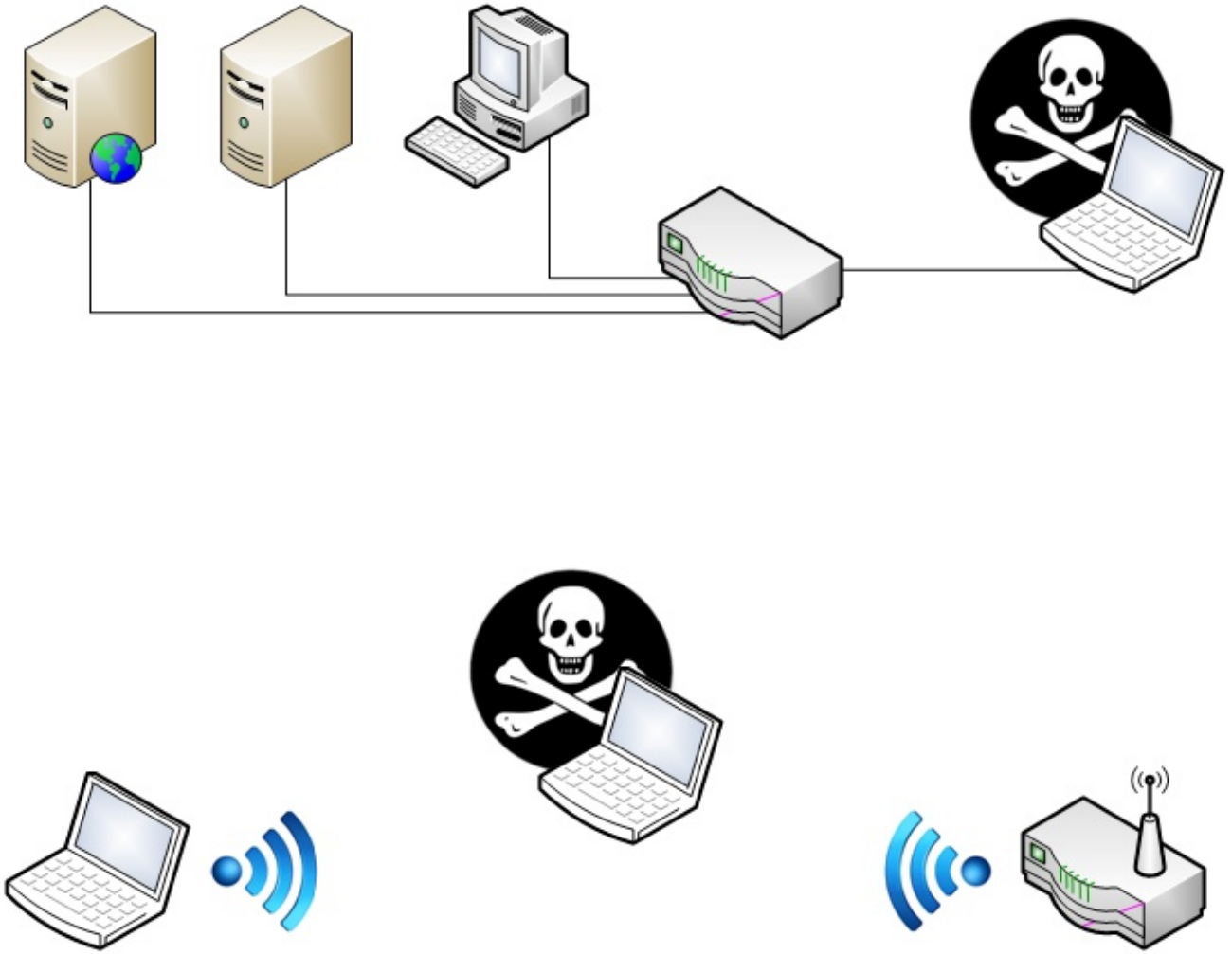
Static packet inspection examines packets one at a time.

Stateful packet inspection examines packets at different stages of a network communication. In this case, an **Access Control List (ACL)** is first looked up in order to accept or deny a connection attempt.

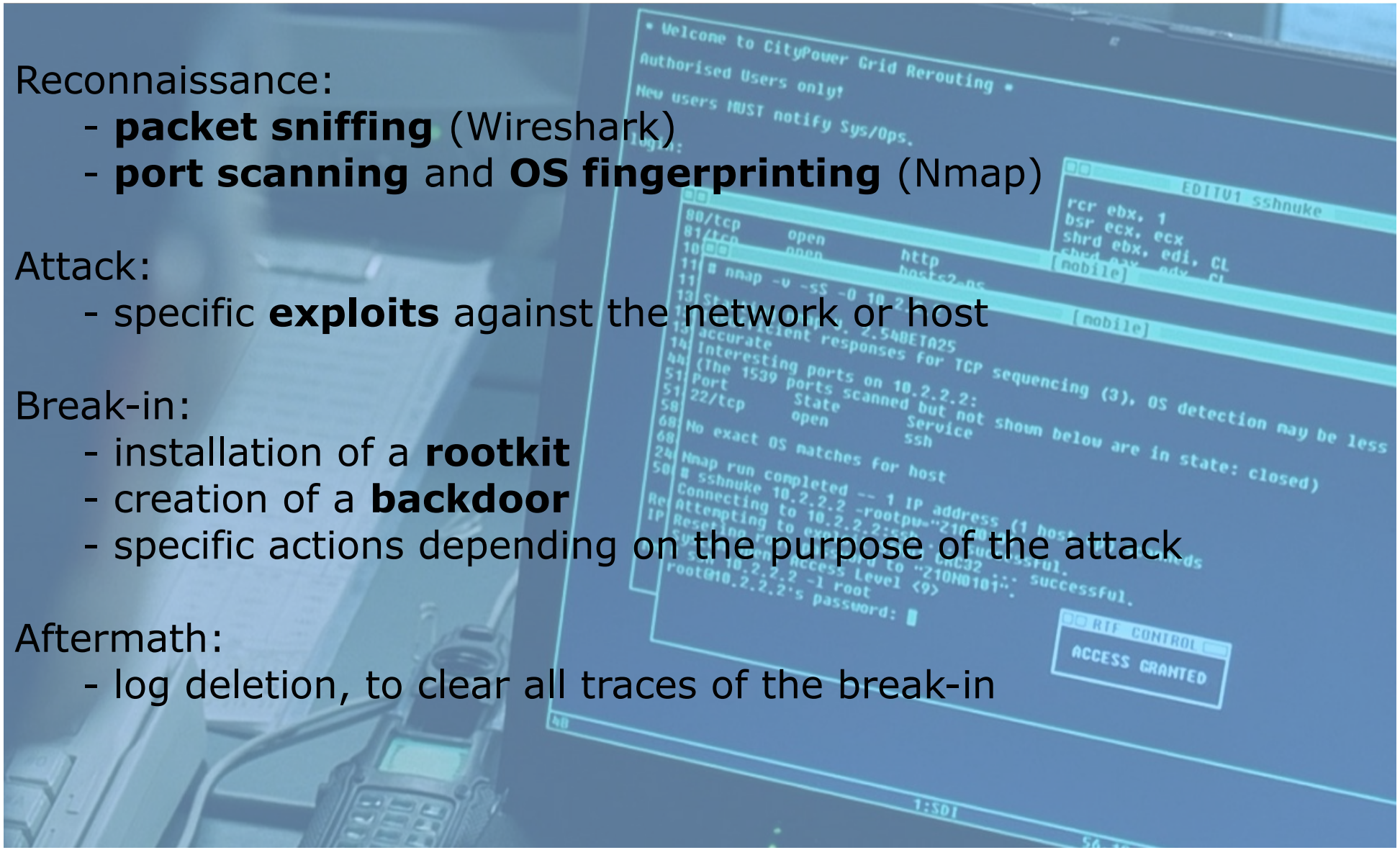
Intrusion Detection Systems (IDS) performs deep inspection on the packets, examining them as part of a stream.

Packet sniffers

A **packet sniffer** is a software that intercepts and logs traffic passing over a part of a network.



Break-in phases and tools



Reconnaissance:

- **packet sniffing** (Wireshark)
- **port scanning** and **OS fingerprinting** (Nmap)

Attack:

- specific **exploits** against the network or host

Break-in:

- installation of a **rootkit**
- creation of a **backdoor**
- specific actions depending on the purpose of the attack

Aftermath:

- log deletion, to clear all traces of the break-in

Motivations for attacks

- Curiosity (from **black hat hackers** / **crackers** and **script kiddies**)
- Fraud (from cybercriminals)
- Revenge (from disgruntled employees and ex-employees)
- Espionage (from competing firms and foreign governments)
- Terrorism and war (from political groups and foreign countries)

Security planning

✯ **Risk analysis**: type of attacker, probability of attack, evaluation of damage to assets, protection cost (including insurance)

✯ **Comprehensive security**: identify and close all vectors of attack

✯ **Defense in depth**: multiple lines of defense

✯ **Access control** with **minimal permissions**

✯ **Accountability**: log files, access records, CCTVs

✯ **Security audits** and **vulnerability tests**: hire a **white hat hacker** to "attack" your own network and identify weaknesses

Spam e-mail

- Advertisement
- Frauds (fake products, 419 scams, multilevel schemes)
- **Phishing**
- Propagation of viruses via attachments

Spam represents today around 70% of all e-mail traffic in the world. The majority of spam is sent by botnets.

Authentication

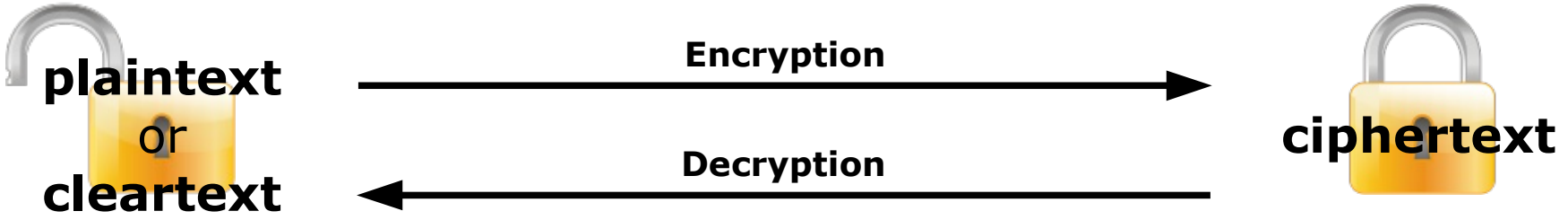
The **supplicant** tries to authenticate upon the **verifier** providing the appropriate credentials.

Authentication can be accomplished either
- by something you ***know*** (password, PIN, secret word)
- by something you ***have*** (key, bank card, badge, RSA SecurID)
- by something you ***are*** (biometrics: fingerprint / iris / face scanning)

or, better, by two of these (**two-factor authentication**).

Passwords are the easiest authentication factor to use in IT.
A strong password defies **password guessing**, **dictionary attacks** and **brute-force cracking**.

Cryptography



Encryption and decryption are done via a **cipher** (a cryptographic algorithm) and a **key**.

Encryption provides message **confidentiality**.

A **digital signature** provides message **authentication** and **integrity**, but not confidentiality.

Cryptography

Symmetric cryptography (2000 years old):

The same **shared secret key** is used both to encrypt and to decrypt.

Example of ciphers:
Caesar's cipher, substitution cipher, Vigenere (ancient)
3DES, AES, Blowfish (modern)

Cryptography

Asymmetric or **public-key cryptography** (40 years old):

Each person generates a **key pair** composed of a **private key** and its **public key**.
You encrypt a message with the recipient's public key and send it; the recipient will decrypt it with his private key.
You can also **digitally sign** a message with your private key; others will be able to check your signature using your public key.

Example of public-key cryptosystems: RSA, DSA, ElGamal

Used in HTTPS, SSL/TLS, PGP

Cryptography

The big problem in PKC is the attribution of a public key to the correct owner.
Solutions:

- ✯ decentralized approach → PGP's **Web Of Trust**
- ✯ centralized approach → **Trusted Third Party (TTP)**

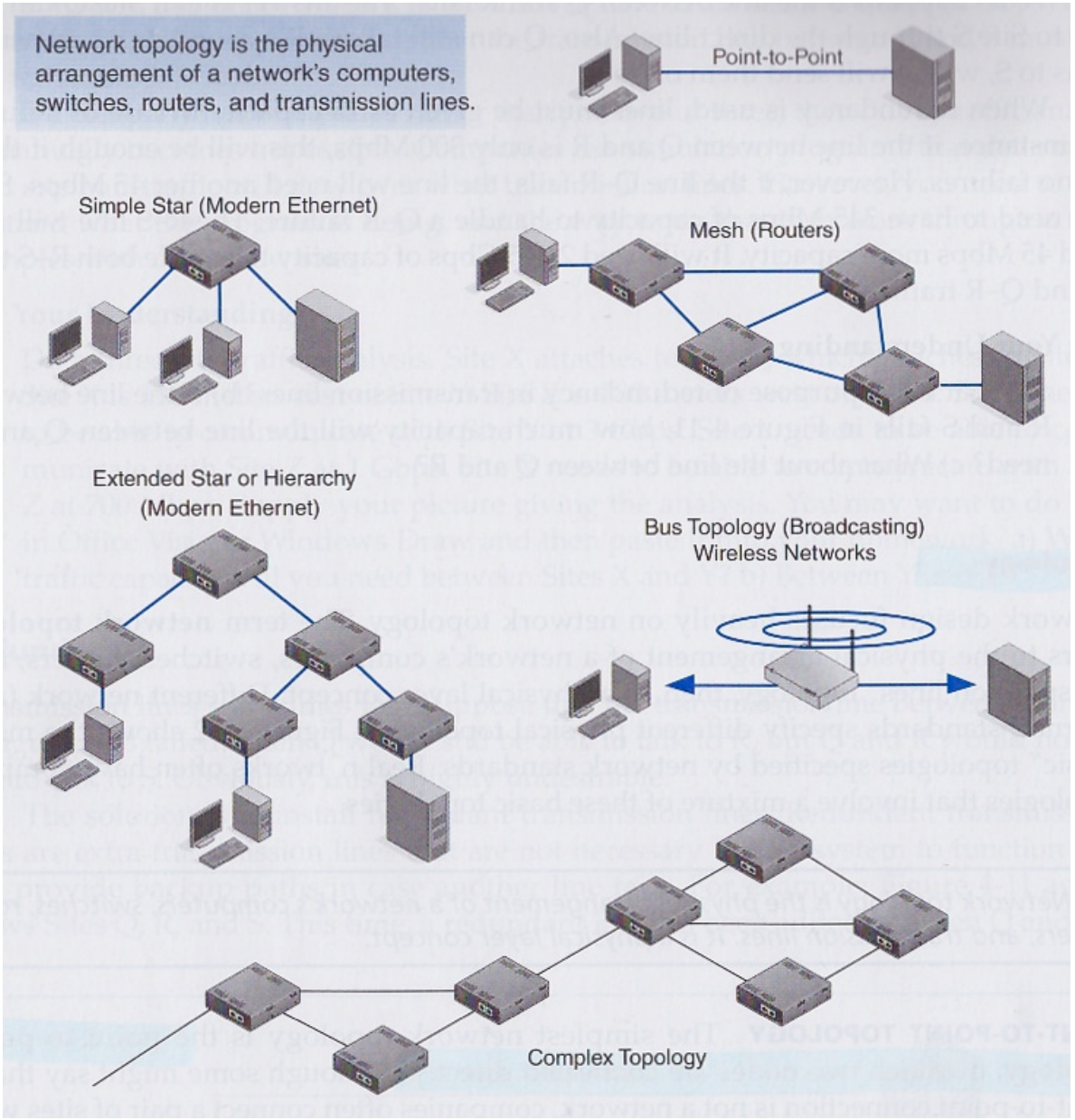
The TTP is implemented by a **Certificate Authority** that distributes the person's public key inside a **digital certificate**, signed with the CA's key.

QoS metrics

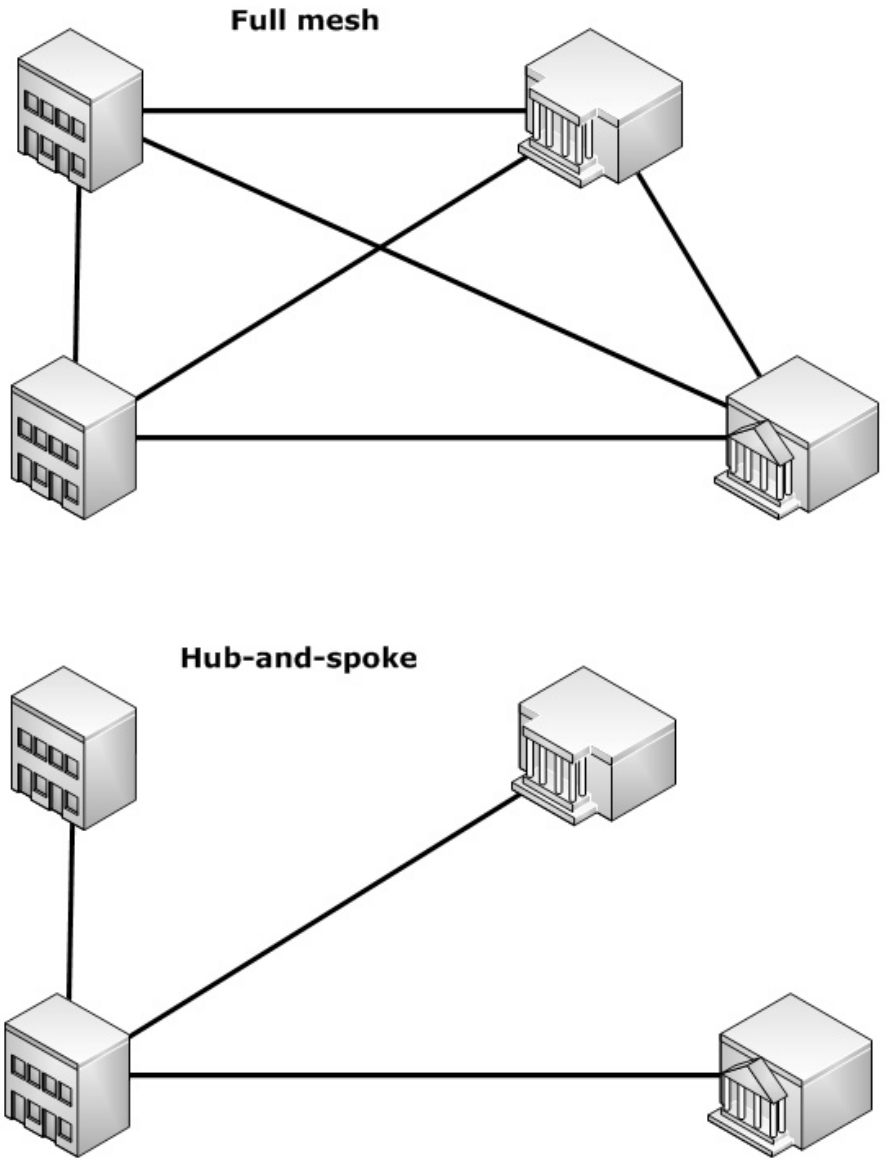
- Transmission **speed** (measured in bps)
  Rated speed vs **throughput** (individual or aggregate)
- **Availability** ↔ **Downtime**
  Target is "five nines" availability = 99.999%
- Packet or bit **error rate**
- **Latency** = packet RTT or network delay
- **Jitter** = variance in the latency of successive packets
- Application response time

SLAs are expressed as worst cases and often have %-time elements.

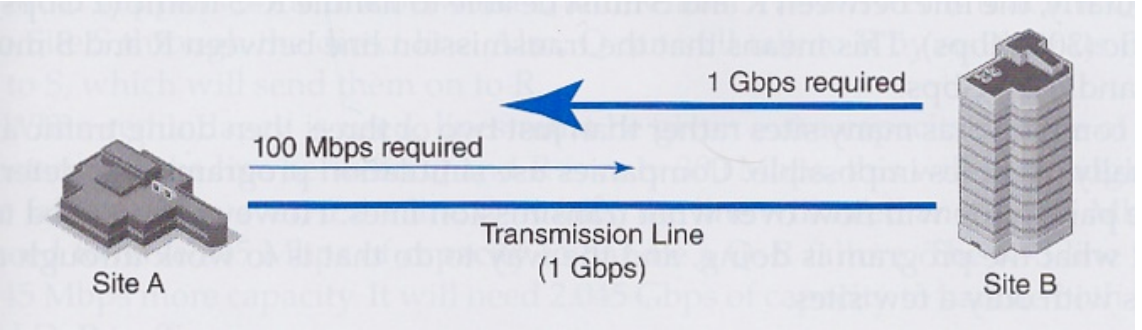
Network topology



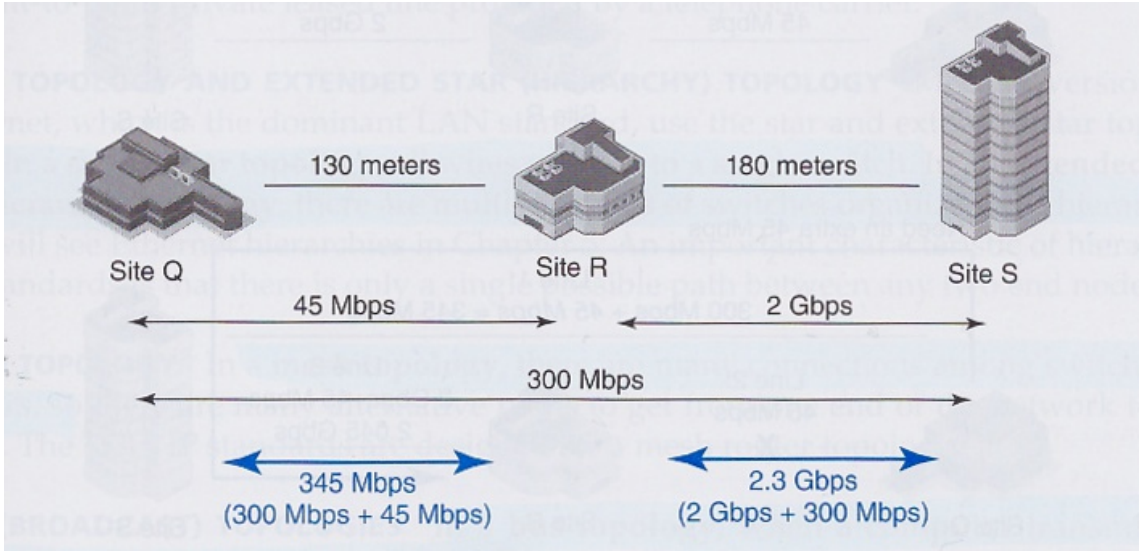
Leased line topology

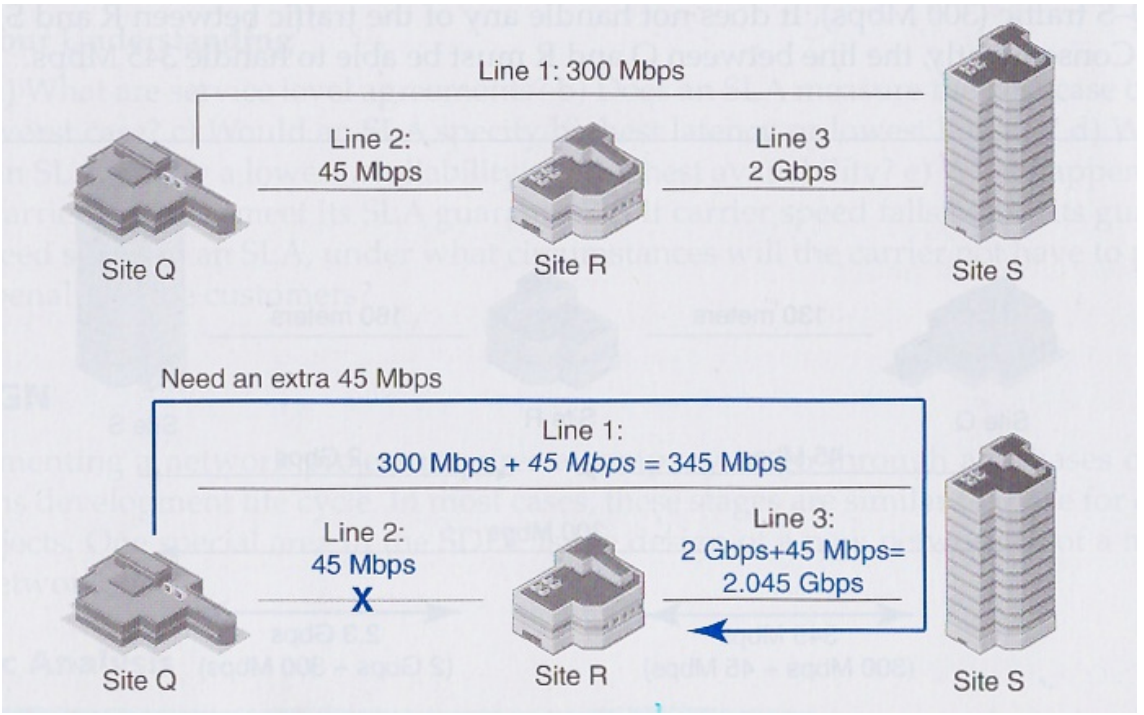


Traffic analysis



Traffic analysis





Network congestion management

How to handle momentary traffic peaks:

- **Overprovisioning**
- Assign higher **priority** to latency-intolerant applications
- **Traffic shaping**
  -  Filter out unwanted traffic
  - 

 Assign % of capacity to applications
- Network data **compression**

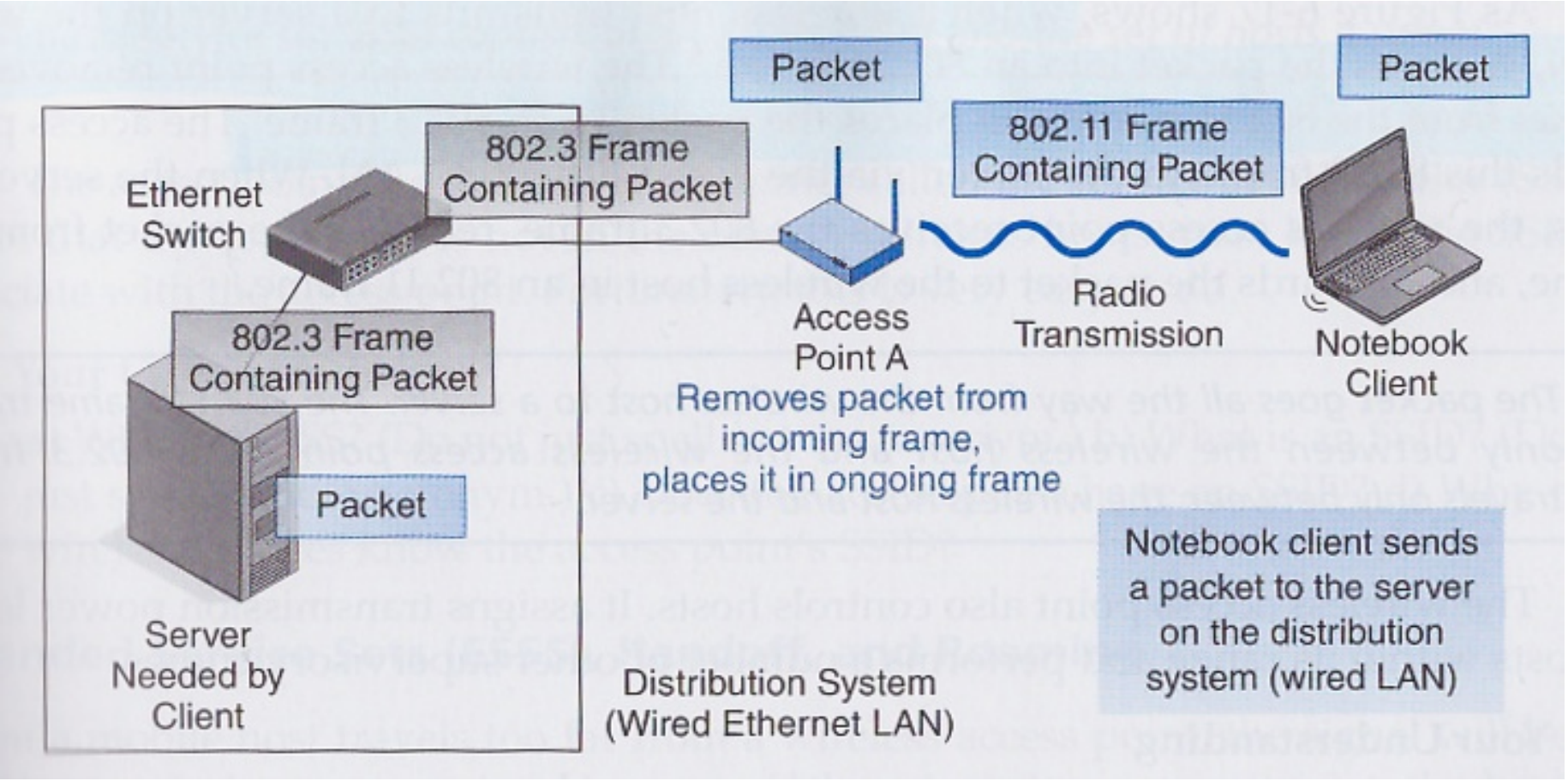
Network project management

- Evaluate **minimum requirements**
- Evaluate **scalability**
- Evaluate the **Total Cost of Ownership (TCO)**:
  + Hardware
  + Software
  + Labor (planning, installation, configuration, testing)
  + Operating and management

Operational management

- **Operations** (NOC): manage and monitor the network
- **Maintenance**: fix and prevent equipment failures
- **Provisioning**: set up the service, physically and logically
- **Administration**: prepare network projects and budgets, pay bills

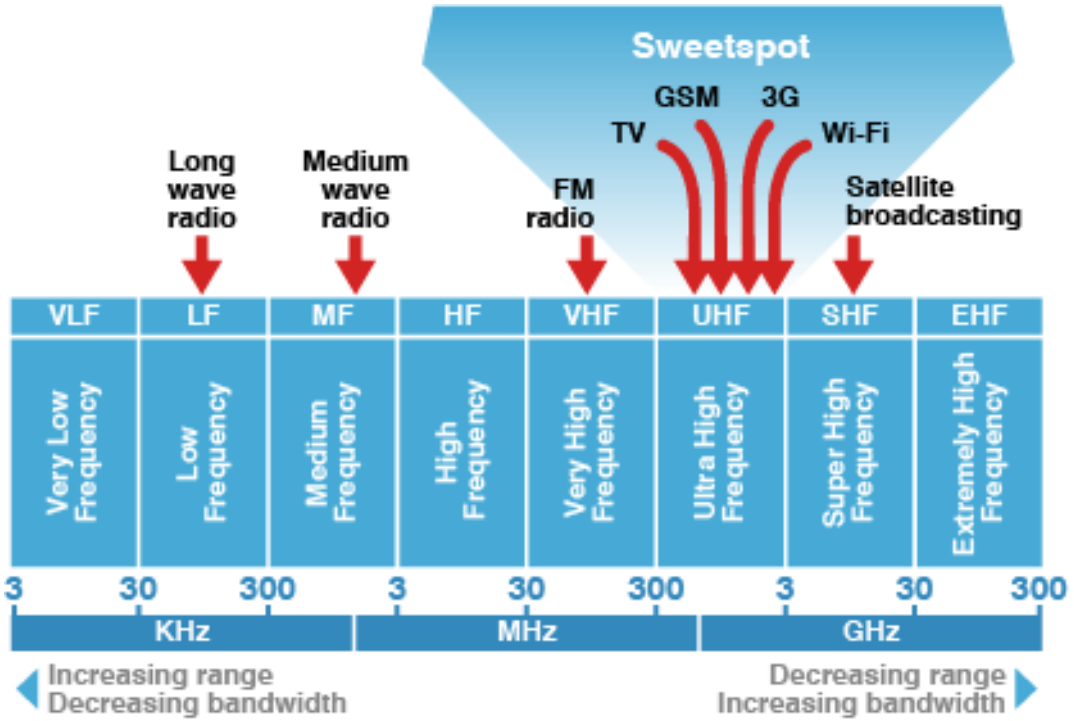
WLANs (Wireless LANs)



WLANs (Wireless LANs)

Radio waves are described in terms of **frequency**, measured in **Hertz** (1 Hz = 1 cycle/second)

Wi-Fi 802.11b/g uses the 2.4 GHz band
Wi-Fi 802.11a uses the 5 GHz band



Attenuation

A radio signal emitted from an omni antenna spreads over the area of a sphere → attenuation is proportional to the square of the emission radius (**inverse square law**)

Absorptive attenuation by air, plants, and trees

Electromagnetic interference (EMI) from electronic appliances (cordless phones and microwave ovens) operating at the same frequencies as Wi-Fi

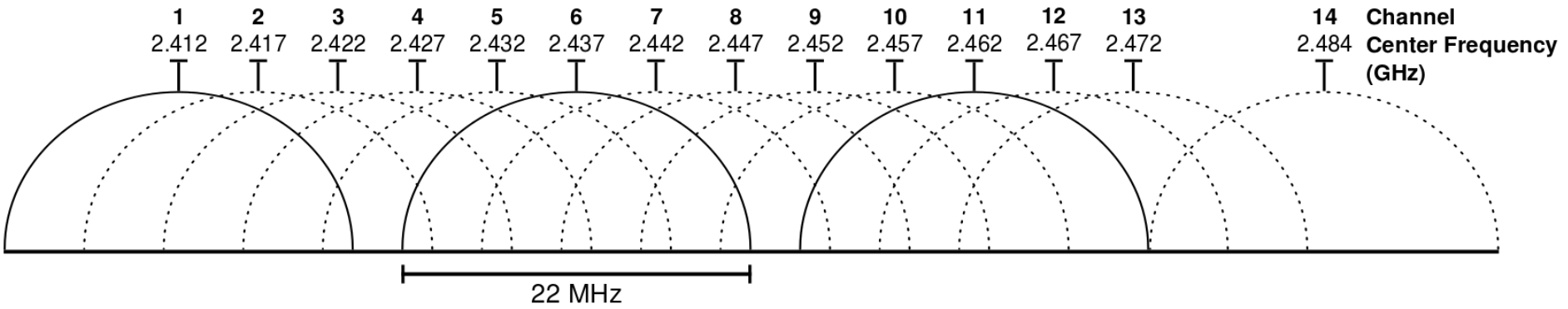
Multipath interference caused by signal bouncing off walls and metal objects and being reflected with a different phase

Hi-frequency radio waves suffer more from signal attenuation and have more difficulty penetrating objects, causing **shadow zones** and **dead spots**; hence it is better to have a **clear line of sight**

Frequencies

The **frequency spectrum** is divided into **service bands**, each of which is itself divided into **channels**.
Service bands and channels have a **bandwidth** (= max f - min f).

Wi-Fi 802.11b/g:
- uses the 2.4000-2.4835 GHz service band → bandwidth of 83.5 MHz
- it is divided into 14 overlapping channels of 22 MHz each



Frequencies

Shannon's Law: The maximum possible transmission speed is proportional to the channel's bandwidth

Broadband channels are channels with a large bandwidth $\rightarrow$ high transmission speed

Unlicensed radio bands, such as Wi-Fi, don't need a license to operate

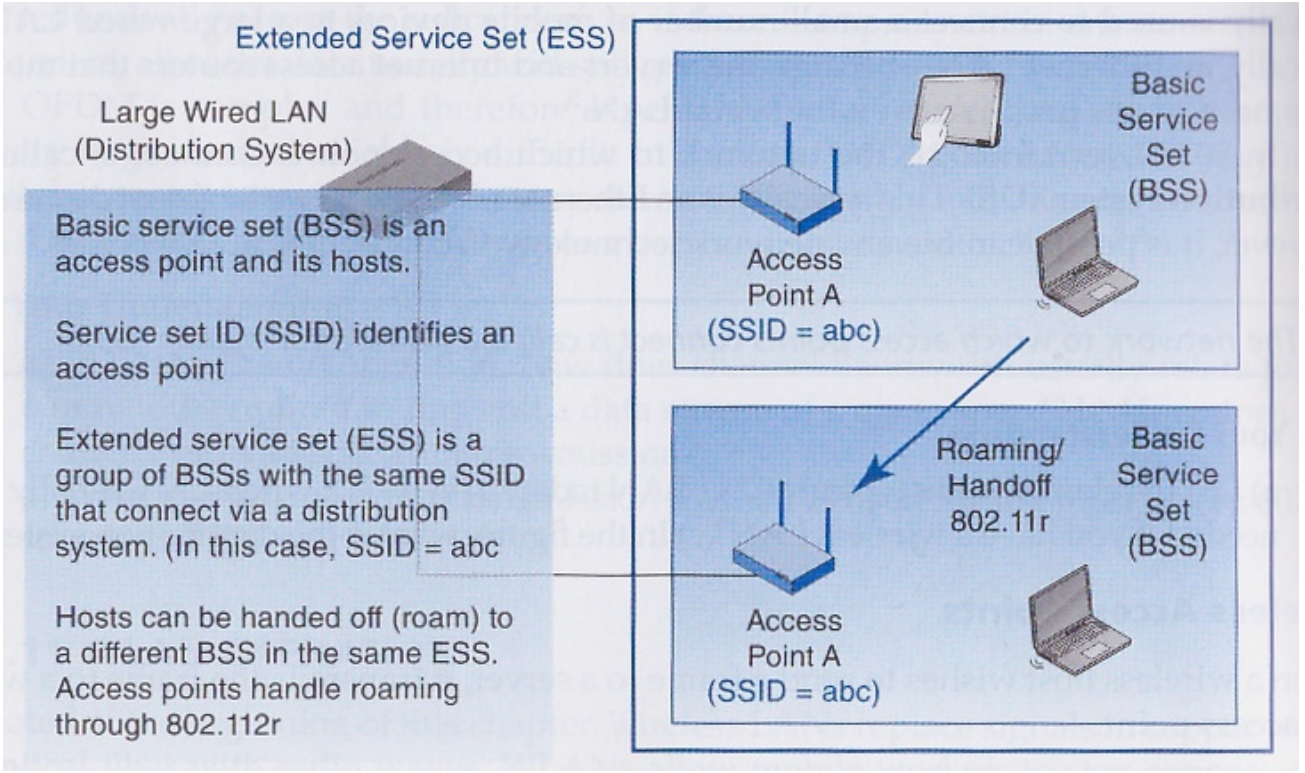
Spread Spectrum

Spread Spectrum transmission:
Spreads the energy of the original signal (**baseband signal**) over a channel bandwidth wider than required for the signal's speed.
Reduces propagation problems, especially multipath interference.

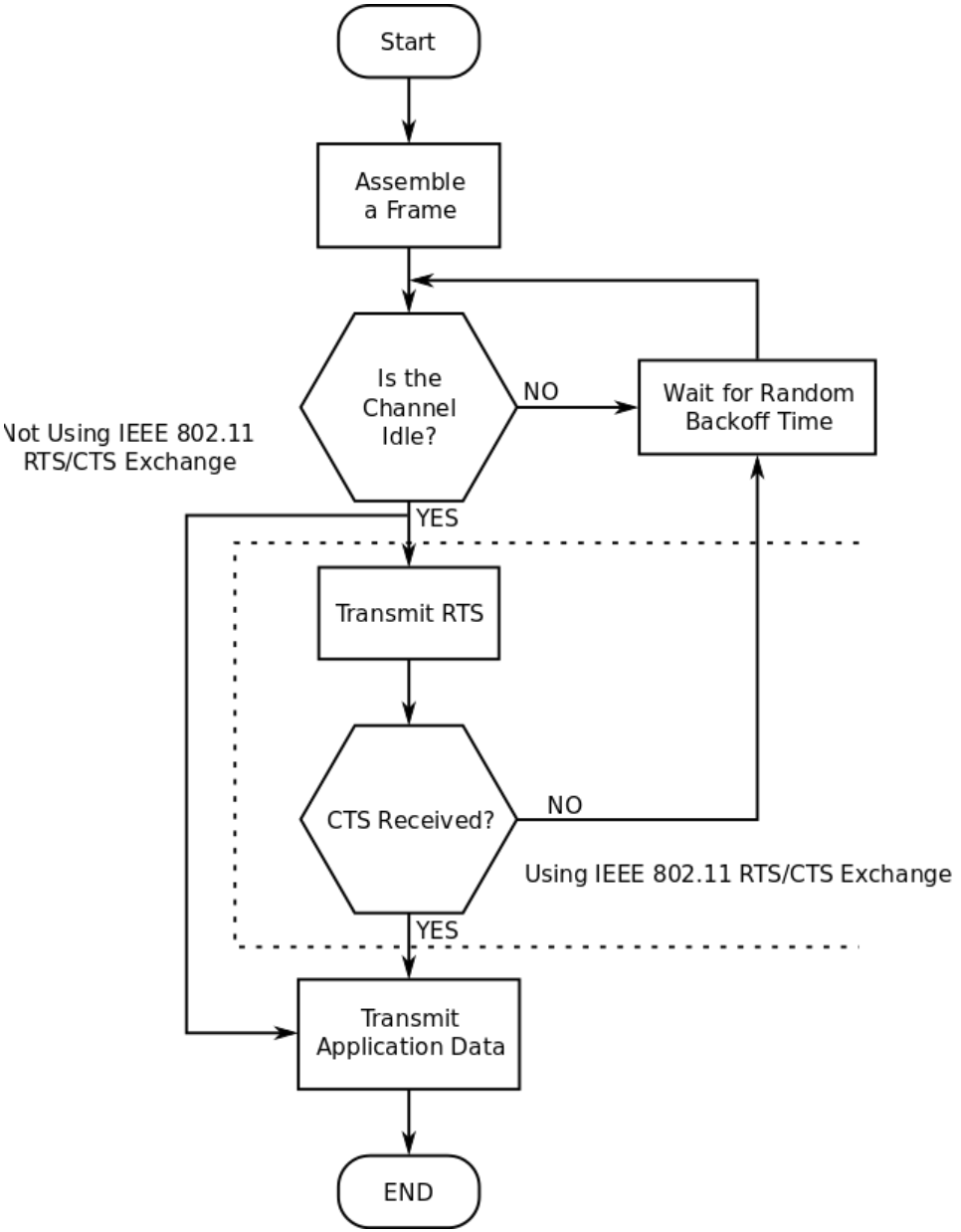
Orthogonal Frequency Division Multiplexing (OFDM):
Divides a broadband channel into smaller subchannels (**subcarriers**), each of which carries a part of a frame.
Increases reliability.

Basic Service Set / Extended Service Set

A **BSS** consists of an Access Point and all the hosts it serves.
The name of the network provided by the AP is the **SSID**.
Multiple BSSs connected to the same Distribution System and having the same SSID form a **ESS**.
Mobile hosts are able to keep connection with the same DS by **roaming** (aka **handoff**) between APs within the same ESS.



Medium Access Control: CSMA/CA



802.11 standards

802.11b Old. Rated speed: 11 Mbps, band: 2.4 GHz

802.11g Widely used. 54 Mbps up to 30 m, 2.4 GHz
Channel bandwidth: 20 MHz

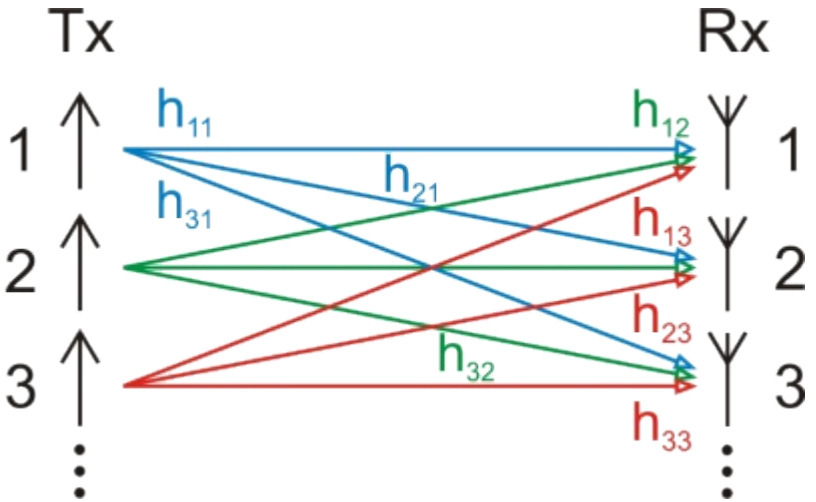
802.11n Dual band 2.4 and 5 GHz. 150 to 600 Mbps
Up to 70 m at 2.4 GHz, up to 50 m at 5 GHz
Channel bw: 40 MHz (drop to 20 MHz if interference)

802.11ac Emerging standard. 433 to 7000 Mbps, 5 GHz
Channel bw: 80 or 160 MHz

802.11ad Emerging standard for e.g. HDTV streaming
7 Gbps up to 10 m, 60 GHz
Channel bw: 2.1 GHz

MIMO

Multiple Input / Multiple Output (MIMO): the AP sends *n* signals (**spatial streams**, *n* = 2 to 4) on the same channel from *n* antennas, received by *n* antennas. The receiver can distinguish between the *n* signals because of the different arrival times.



Performances

- Throughput is often 50-70% of rated speed
- Aggregate throughput must be split amongst individual users
- Throughput decreases with distance
- Slower clients (802.11b) will slow down connection for everybody

WLAN security threats

- Wireless networks are much more vulnerable to intrusions
- Possible unauthorized access to Wi-Fi hotspots by **wardriving**
- Corporate wireless networks are at risk of **drive-by hacking**
- This risk may be greatly increased by **rogue APs**

WLAN security measures

- **WEP (Wired Equivalent Privacy)** (1999)
  40-bit or 104-bit key represented as hex digits
  Weak, easily crackable in minutes

- **WPA (Wi-Fi Protected Access)** (2003)
  Created by the Wi-Fi Alliance based on 802.11i draft

- **WPA2 (Wi-Fi Protected Access II)** aka **802.11i** (2004)
  In use today
  Can operate in two different modes:
  Pre-Shared Key or **802.1X (Enterprise)**

Additional simple security measures to protect a hotspot:

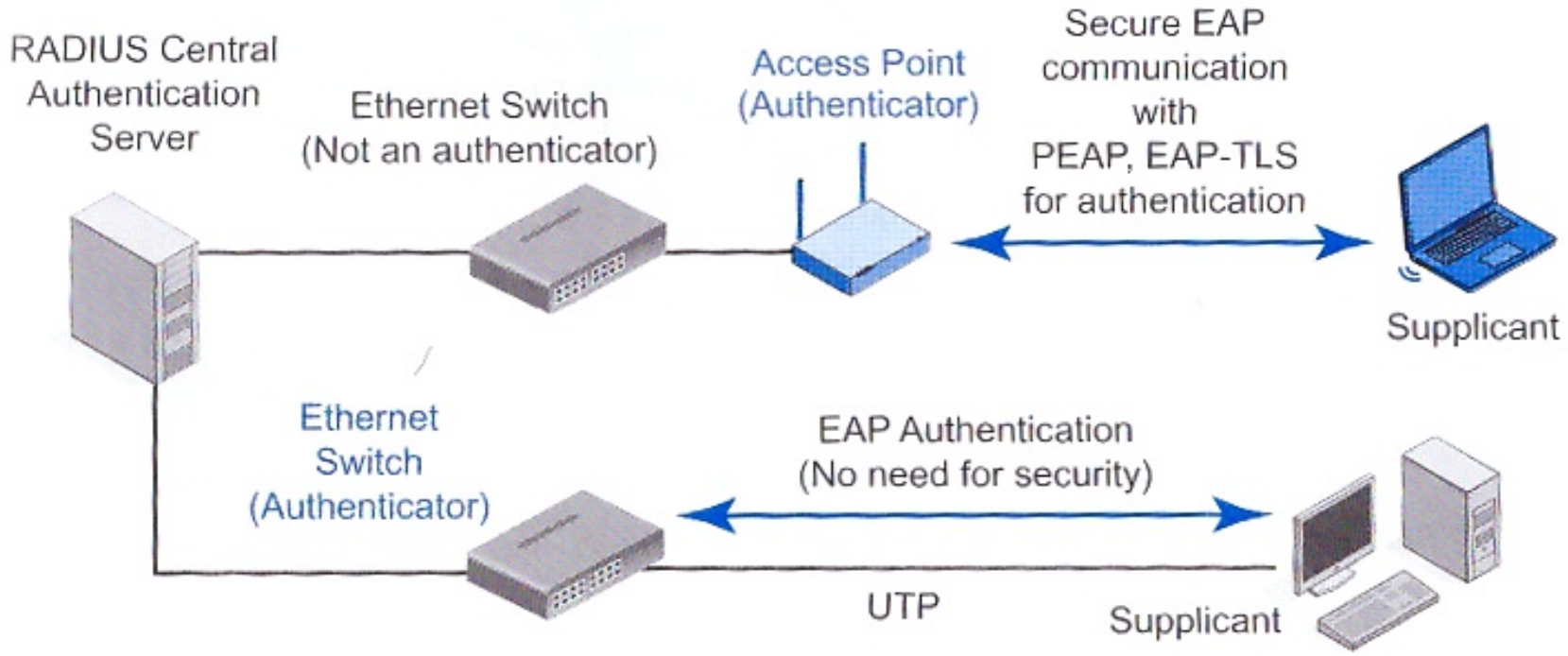
- **SSID cloaking**
- **MAC whitelisting**

WPA2: PSK mode

Used for home networks and small businesses.
A 64-bit pre-shared key is generated from a passphrase and is used for initial authentication of clients to the AP.
Then, the AP gives each client an unique key, renewed often.

WPA2: 802.1X mode

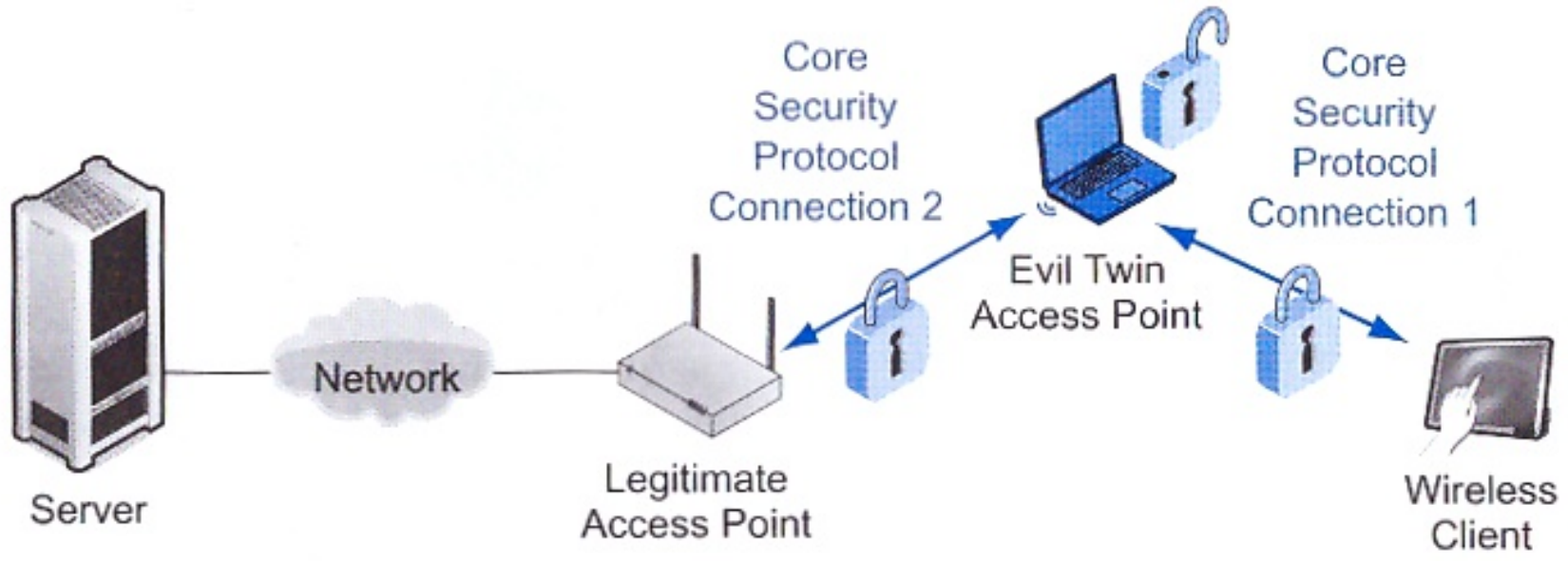
Used for enterprise networks.
Each workgroup switch acts as an authenticator. Actual authentication is done by a central server, usually via RADIUS.
Wireless clients connects to the authenticator via **PEAP (Protected Extensible Authentication Protocol)** or EAP-TTLS.



Man-in-the-middle attack

An attacker can set up a **evil twin AP** (with higher signal strength) and execute a **man-in-the-middle (MITM) attack**.
The attacker then tunnels and eavesdrops the private communication.

The use of a VPN between server and client can defeat this attack.



The WPS flaw

WPA2 in PSK mode is vulnerable to a flaw in the **Wi-Fi Protected Setup (WPS)** protocol.

Wi-Fi Protected Setup allows new clients to associate to an AP by entering a 8-digit PIN. The protocol is flawed and can be brute-forced in 5500 attempts in average.

DoS attacks against WiFi

Wireless networks are very vulnerable to DoS.

- ☠ Flooding fake authentication frames
- ☠ Flooding deauthentication frames for other clients
- ☠ Radio Frequency Interference **(jamming)**

Signal power ratios in dB (logarithmic scale)

$$L_{db} = 10 * \text{Log}_{10}(P_2/P_1)$$

If P_1 = 40 W and P_2 = 80 W $\Rightarrow$ ratio P_2/P_1 = 2 **bels**.
Log_{10} 2 = 0.301 $\Rightarrow$ L_{db} = 3.01 **decibels (dB)**.

If power increased from P_1 to P_2:
$P_2 > P_1 \Leftrightarrow$ ratio $P_2/P_1 > 1 \Leftrightarrow$ dB > 0

If power decreased from P_1 to P_2:
$P_2 < P_1 \Leftrightarrow$ ratio $P_2/P_1 < 1 \Leftrightarrow$ dB < 0

Each doubling in the power ratio = approx +3 dB
Each x10 in the power ratio = +10 dB

Ratio	*dB*
10000	40
100	20
50	16.990
10	10
8	9.031
4	6.021
3	4.771
2	3.010
1	0
0.5	-3.010
0.25	-6.021
0.1	-10
0.01	-20
0.0001	-40

Signal power ratios in dB (logarithmic scale)

Radio power is often expressed in **dBm** = dB relative to 1 mW

If a radio signal has a power of 100 mW:
ratio = 100/1 $\Rightarrow$ power = (Log_{10} 100/1) * 10 dBm $\Rightarrow$ power = 20 dBm

Other wireless technologies

802.11 (Wi-Fi):
11 to 600 Mbps, 2.4 and 5 GHz, 50 m avg range

Bluetooth:
Designed for PANs (mouse, keyboards, headsets, music players, ...)
2 Mbps, 2.4 GHz, 10 m max range

Near Field Communication (NFC):
Designed for very-near communication
106 to 424 kbps, 13.56 KHz, 5 cm max range

Ultra-Wide Band (UWB):
Not a standard yet. Designed for local video transmission
Over 100 Mbps, 10 m max range, 1 GHz channel bw

Bluetooth

1994: first version of Bluetooth
only 721 kbps in download, 72 in upload

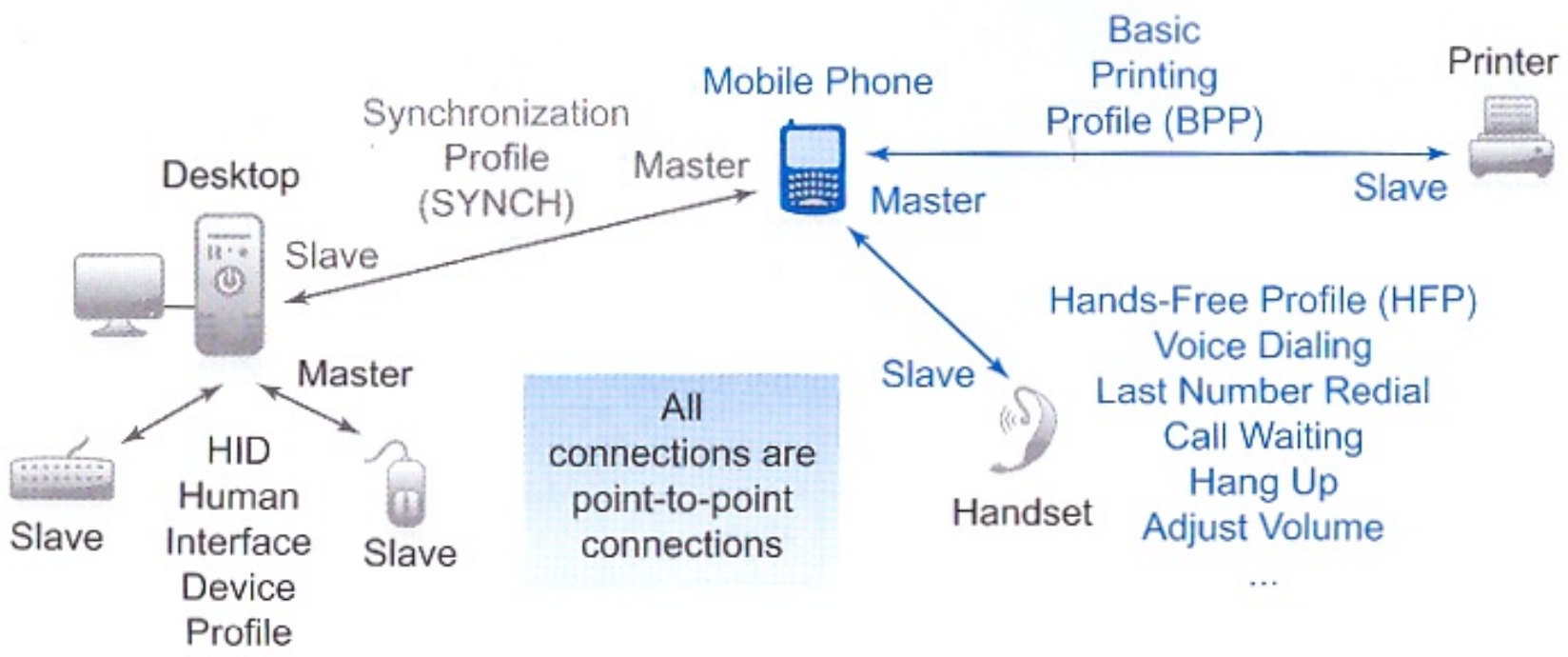
Classic Bluetooth (2.0): 2 to 3 Mbps

High-Speed Bluetooth (3.0):
uses a 802.11 radio for additional speed when needed

Low-Energy Bluetooth (4.0):
for devices with low-duty cycle (communicating 0.25% of the time)

Bluetooth

Bluetooth always uses point-to-point, one-to-one communication.
One device is the **master**, the other is the **slave** (although they can switch roles during an interaction).
A master can have up to 7 slaves.
A master and its slaves is called a **piconet**



Bluetooth

Bluetooth profiles govern how devices share data and messages:

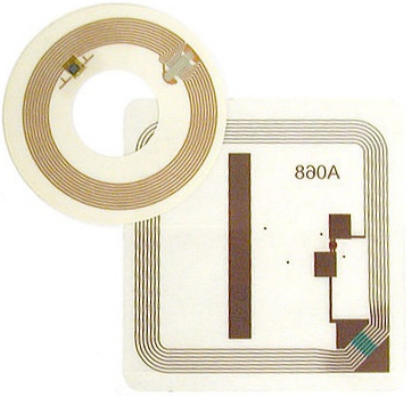
- Service Discovery Profile (SDP), used for **pairing**
- Hands-Free Profile (HFP)
- Headset Profile (HSP)
- Basic Printing Profile (BPP)
- Synchronization Profile (SYNCH)
- Human-Interface Device Profile (HID)

Bluetooth uses the 2.4 GHz band, divided into 79 1-MHz channels. It implements **Frequency Hopping Spread Spectrum (FHSS)**, changing channel every 1.6 millisec (avoiding busy channels)

Near Field Communication

Possible uses:

- public transports fares card / highway tolls
- micropayments
- operating doors / ignition of cars
- data exchange between phones
- interactive posters
- **RFID (Radio Frequency ID)** tags
  - anti-shoplifting tags
  - item tracking: goods, libraries' books, airports' luggages
  - implanted chips for pet (and human!) identification
  - biometric passports



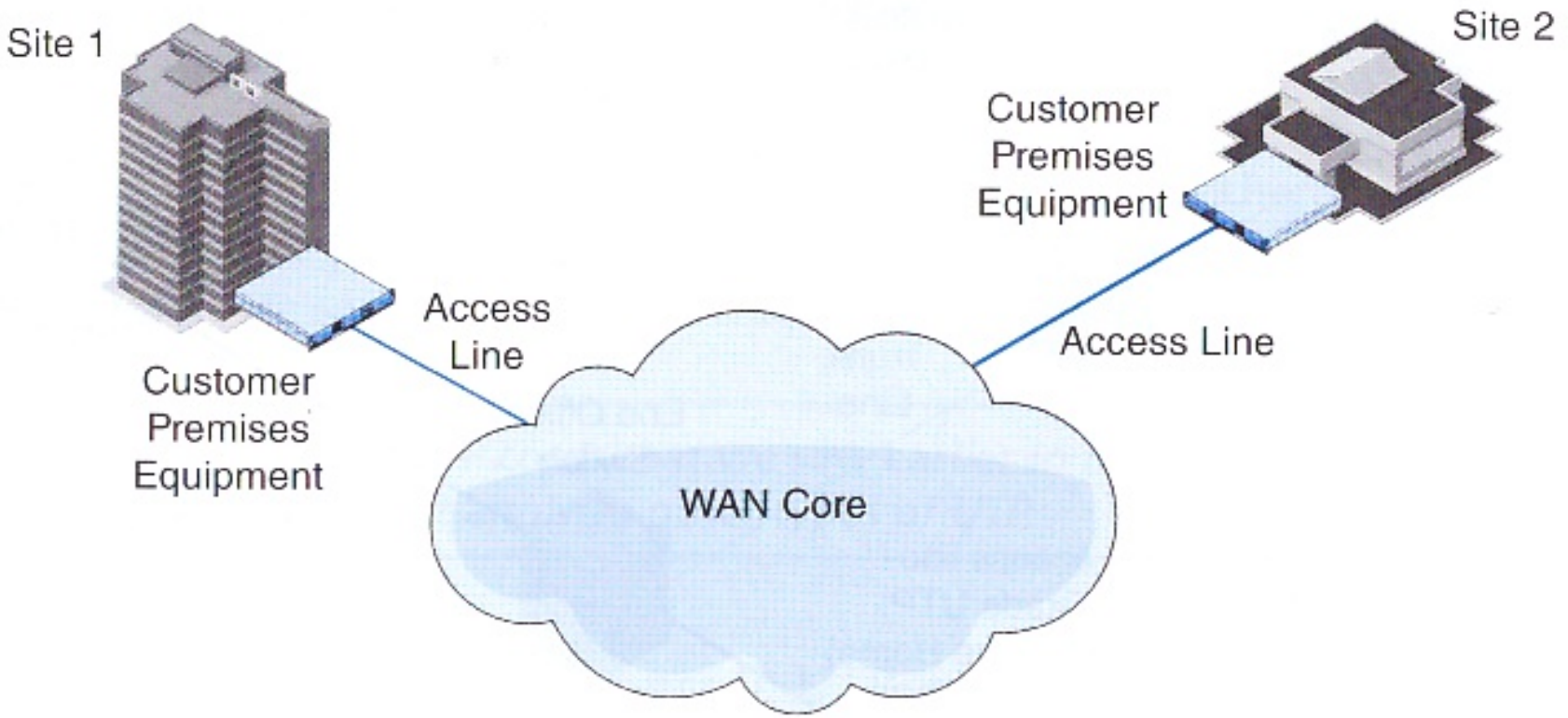
Devices require very low energy (button-sized batteries) or none at all (in the case of passive RFID)

Subject to eavesdropping; bank cards using RFID can be protected by using RFID-blocking wallets (**Faraday's cage**)

WANs

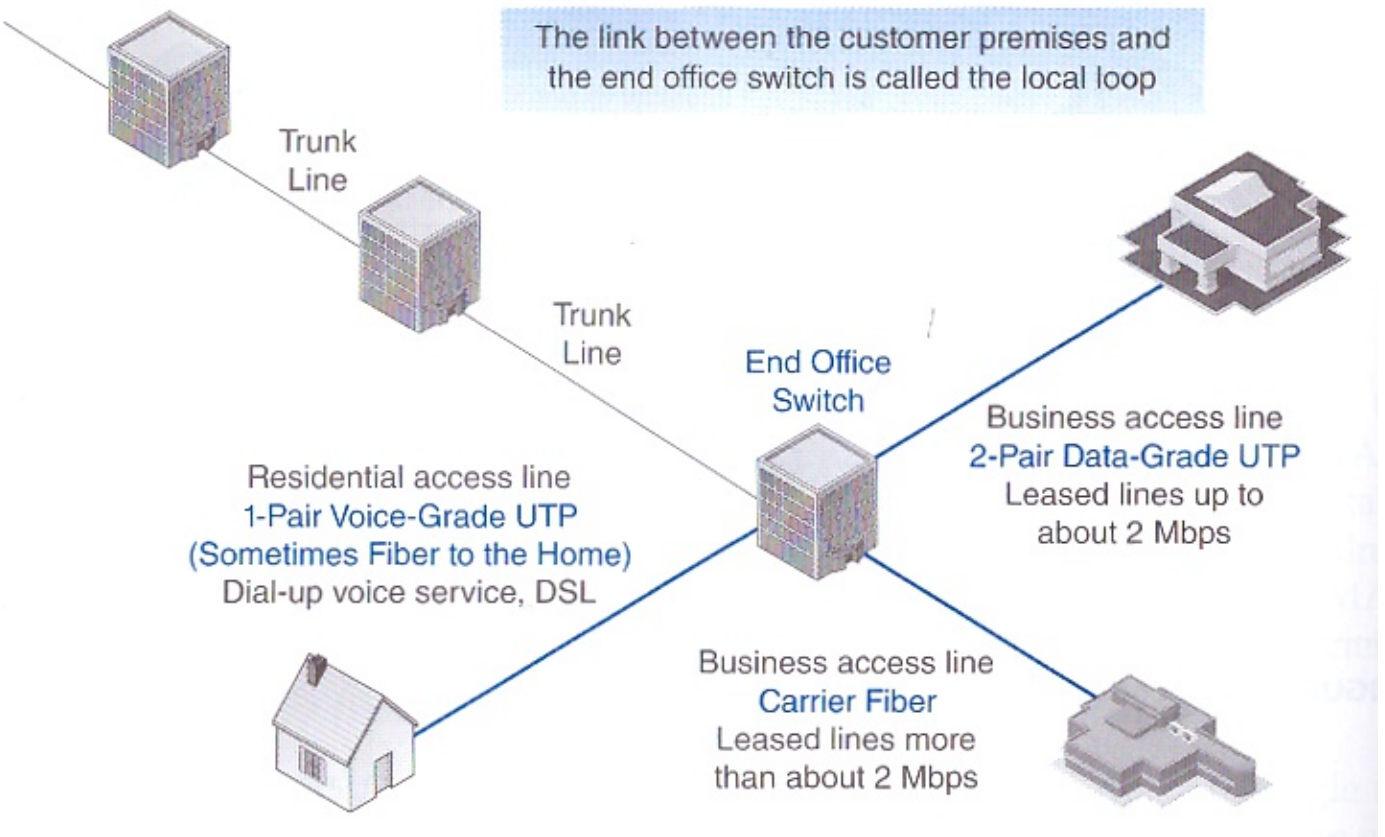
Category	Local Area Network	Metropolitan Area Network	Wide Area Network
Abbreviation	LAN	MAN	WAN
Service Area	*On customer premises* (home, apartment, office, building, campus, etc.)	*Between sites* in a metropolitan area (city and its suburbs) A Type of WAN	*Between sites* in a region, a country, or 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

WANs



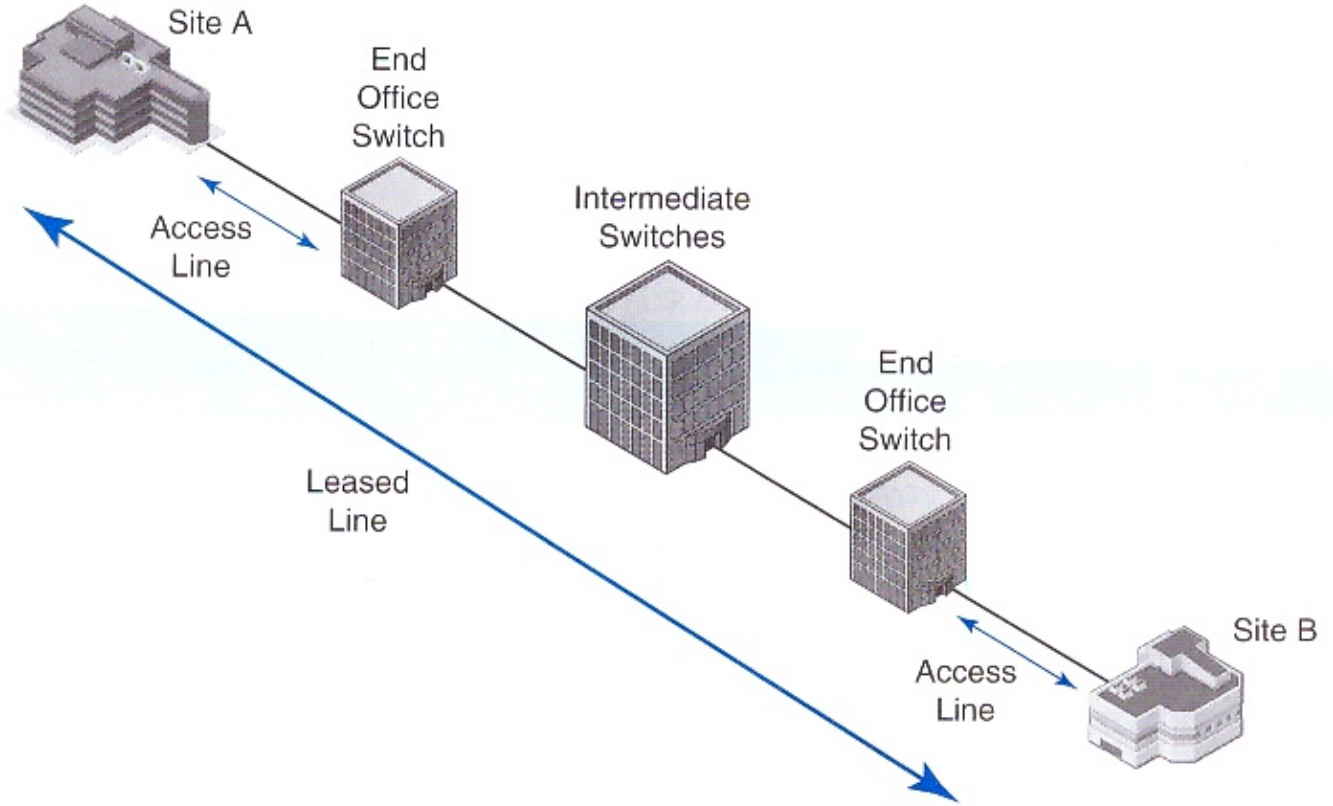
The customer's gateway (a border router or a firewall) connects the **Customer Premises Equipment** with the WAN core.
The dominant technologies for access lines are **PSTN** links and **cable modem** service.

PSTN



Public Switched Telephone Network (PSTN) lines were designed for voice but can carry data as well.
Several technologies for the **local loop** (aka **last mile**) are available.

Leased line



Leased lines run from one customer premises to another.

Dial-up vs leased lines

Dial-up telephone line

- ☎ Any number can be dialed
- ☎ Only exists during the call
- ☎ Pay by the minute
- ☎ Requires modems for data

Leased line connection

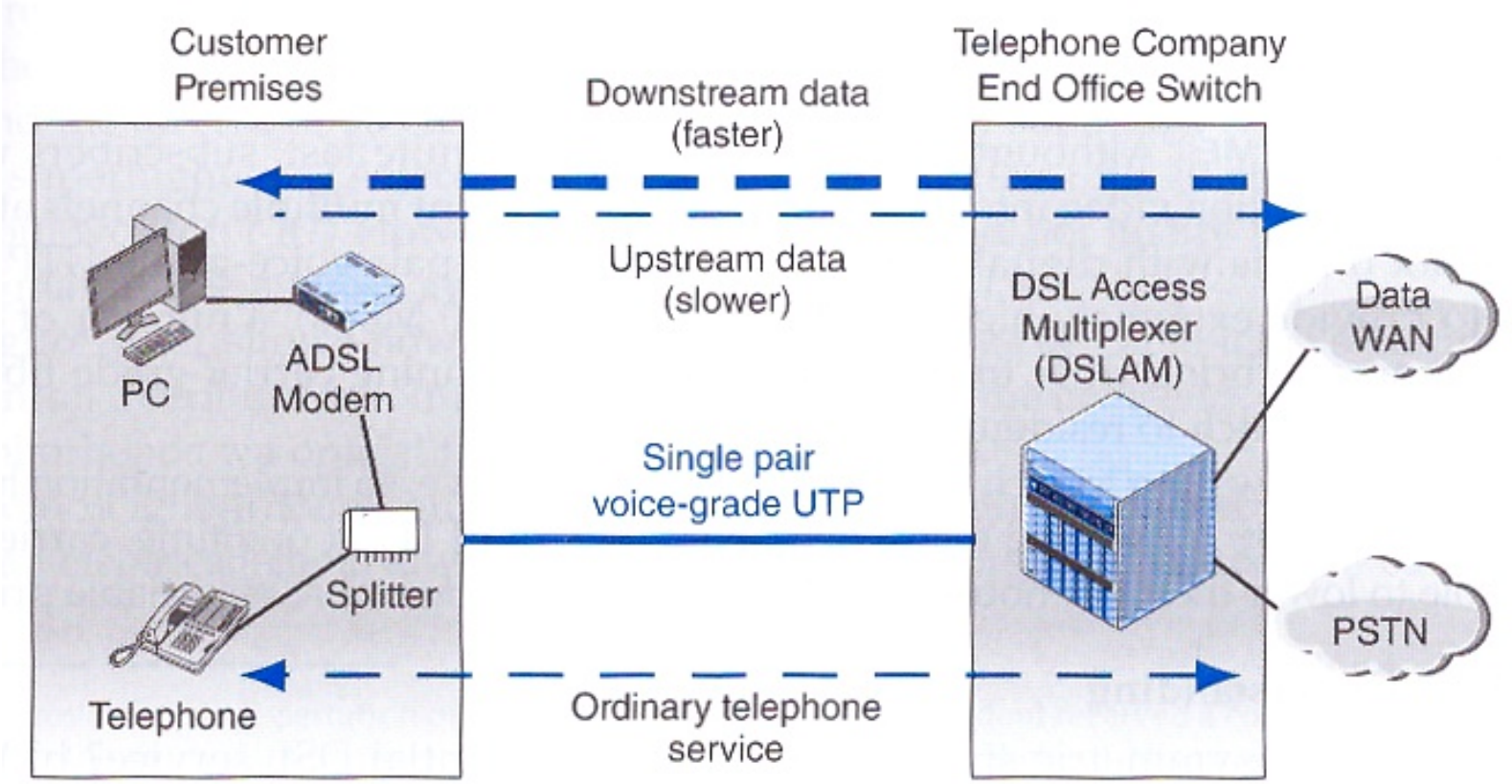
- ↕ Possible only point-to-point
- ↕ Always on
- ↕ Fixed cost + lease fees
- ↕ Can carry data much faster

Leased line speeds (US and EU)

North American Digital Hierarchy		
Line	Speed	Typical Transmission Medium
T1	1.544 Mbps	2-Pair Data-Grade UTP
Fractional T1	128 kbps, 256 kbps, 384 kbps, 512 kbps, 768 kbps	2-Pair Data-Grade UTP
Bonded T1s (multiple T1s acting as a single line)	Small multiples of 1.544 Mbps	2-Pair Data-Grade UTP
T3	44.736 Mbps	Carrier Optical Fiber
CEPT Hierarchy		
Line	Speed	Typical Transmission Medium
Fractional E1		2-Pair Data-Grade UTP
E1	2.048 Mbps	2-Pair Data-Grade UTP
Bonded E1	Small multiples of 2.048 Mbps	
E3	34.368 Mbps	Carrier Optical Fiber
SONET/SDH Speeds		
Line	Speed (Mbps)	Typical Transmission Medium
OC3/STM1	155.52	Carrier Optical Fiber
OC12/STM4	622.08	Carrier Optical Fiber
OC48/STM16	2,488.32	Carrier Optical Fiber
OC192/STM64	9,953.28	Carrier Optical Fiber
OC768/STM256	39,813.12	Carrier Optical Fiber

DSL

Digital Subscriber Lines (DSL) can carry data signals on traditional 1-pair UTP telephone voice lines; much faster than dial-up access via telephone modem (56 kbps downstream, 33 kbps upstream). Residential DSL service is **ADSL (Asymmetric DSL)**.

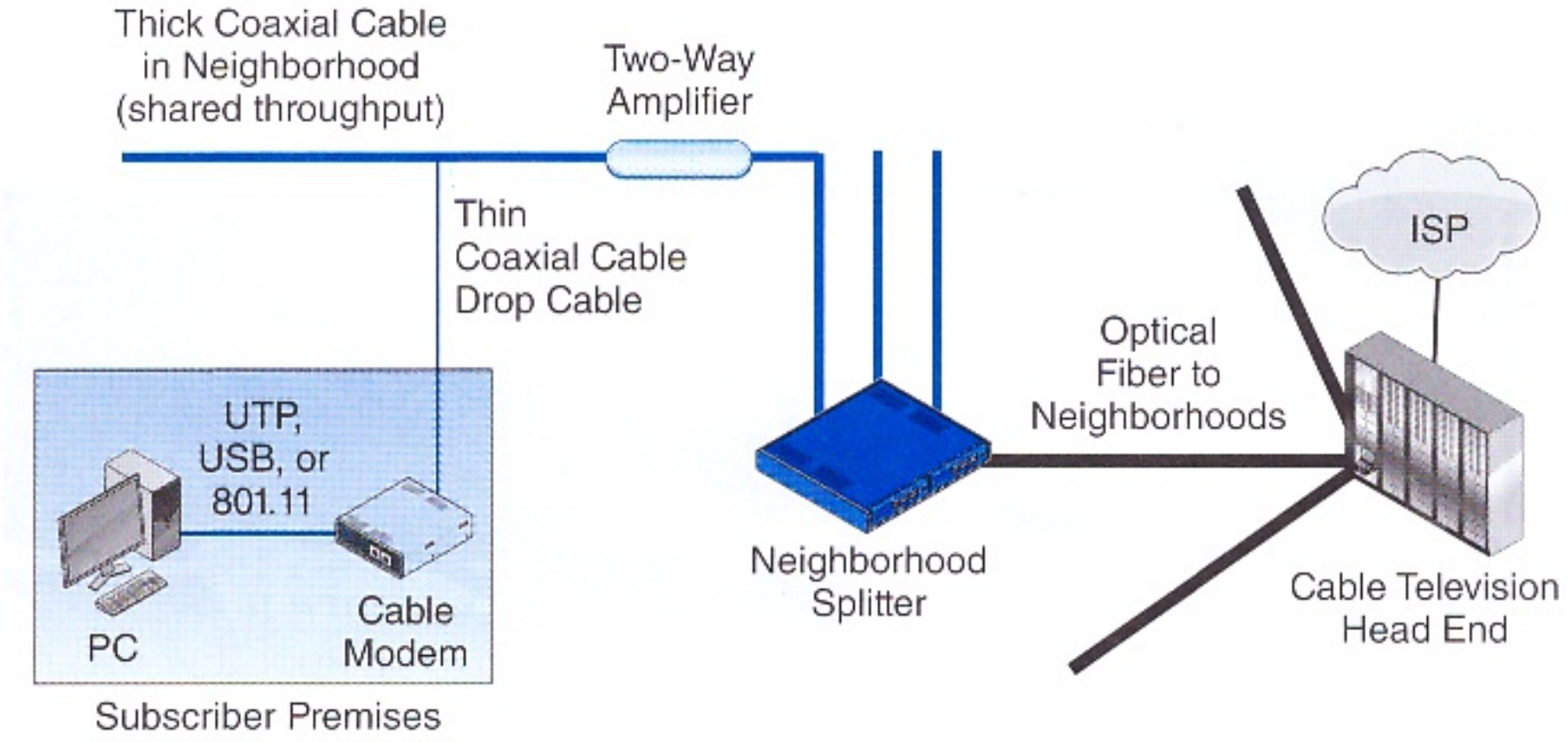


DSL speeds

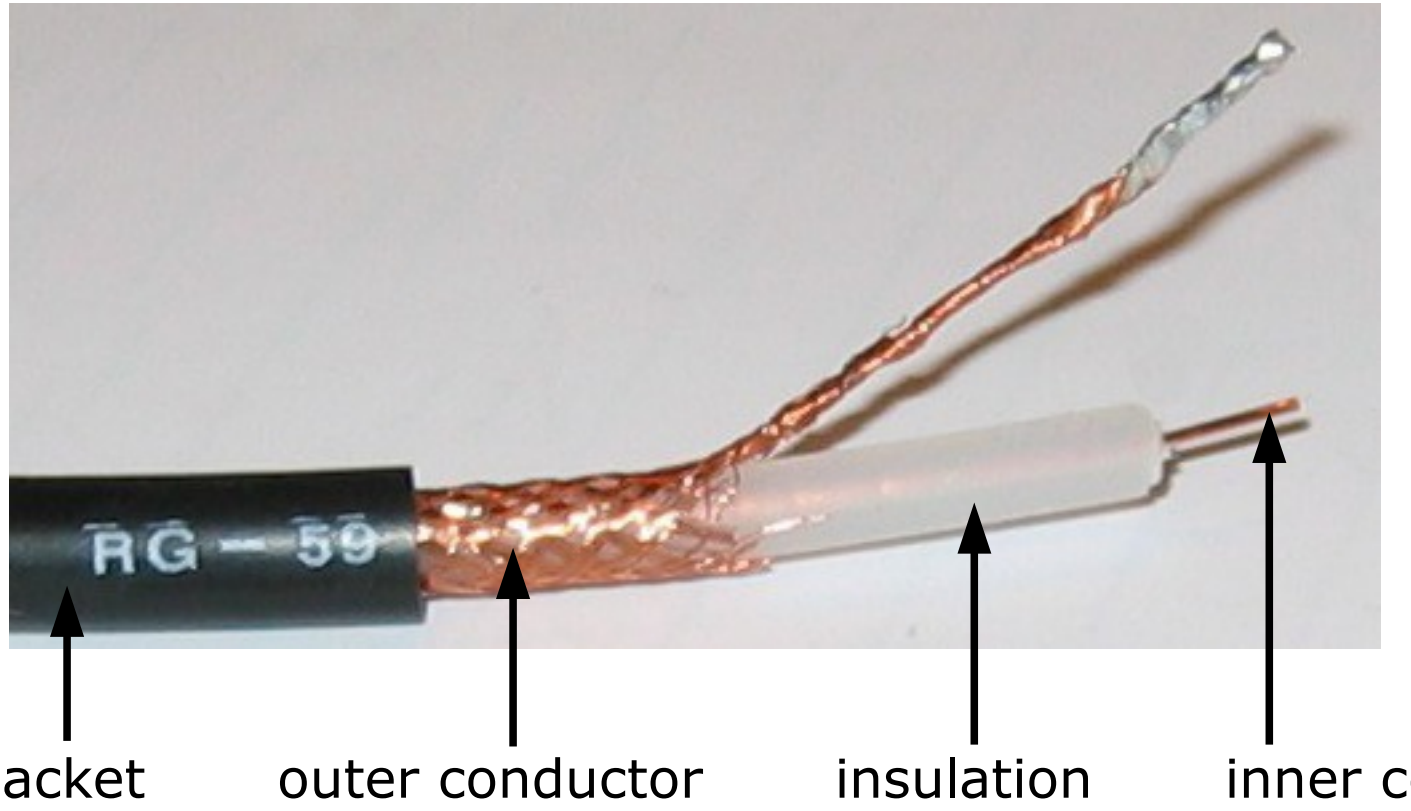
Feature	ADSL	VDSL	HDSL	HDSL2	SHDSL
Name	Asymmetric DSL	Very-High-Bit-Rate DSL	High-Rate Symmetric DSL	High-Rate Symmetric DSL Version 2	Super-High Rate Symmetric DSL
Uses Existing 1-Pair Voice-Grade UTP?	Yes*	Yes	Yes*	Yes*	Yes*
Target Market	Residences	Residences, multi-tenant units	Business	Business	Business
Downstream Rated Speed	Initially, 1.5 Mbps; now up to 12 Mbps	52 to 100 Mbps	768 kbps	1.544 Mbps	192 kbps to 2.3 Mbps
Upstream Rated Speed	Initially, up to 0.5 Mbps; now up to 3.3 Mbps	16 to 100 Mbps	768 kbps	1.544 Mbps	192 kbps to 2.3 Mbps
Speed Symmetry	Asymmetrical	Asymmetric or Symmetric	Symmetrical	Symmetrical	Symmetrical
Quality-of-Service Guarantees?	No	No	Yes	Yes	Yes

Cable modem

Cable modem service, successor to cable TV, provides customers' access to the WAN.



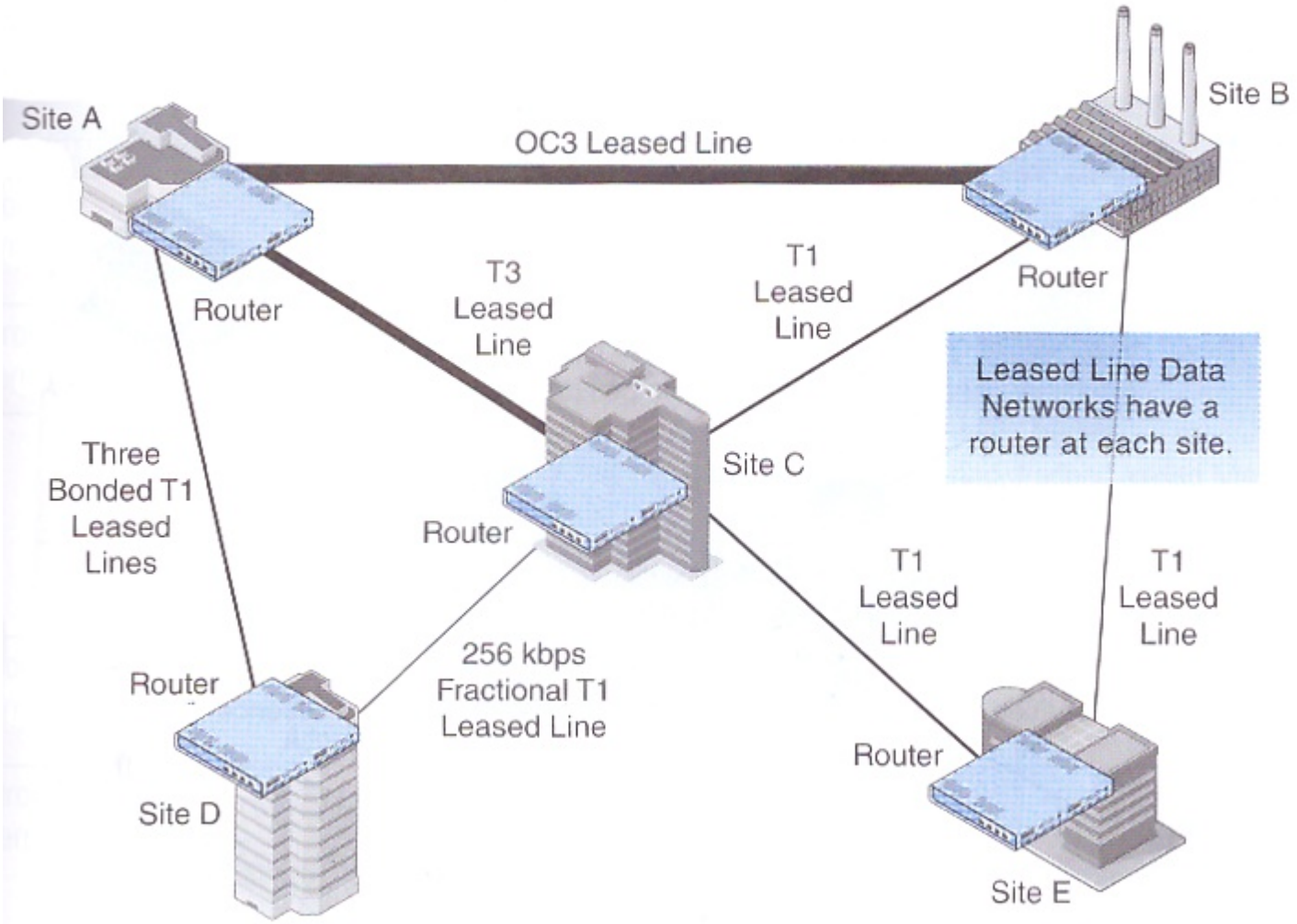
Coaxial cable



The transmission of an electric signal always requires two conductors.

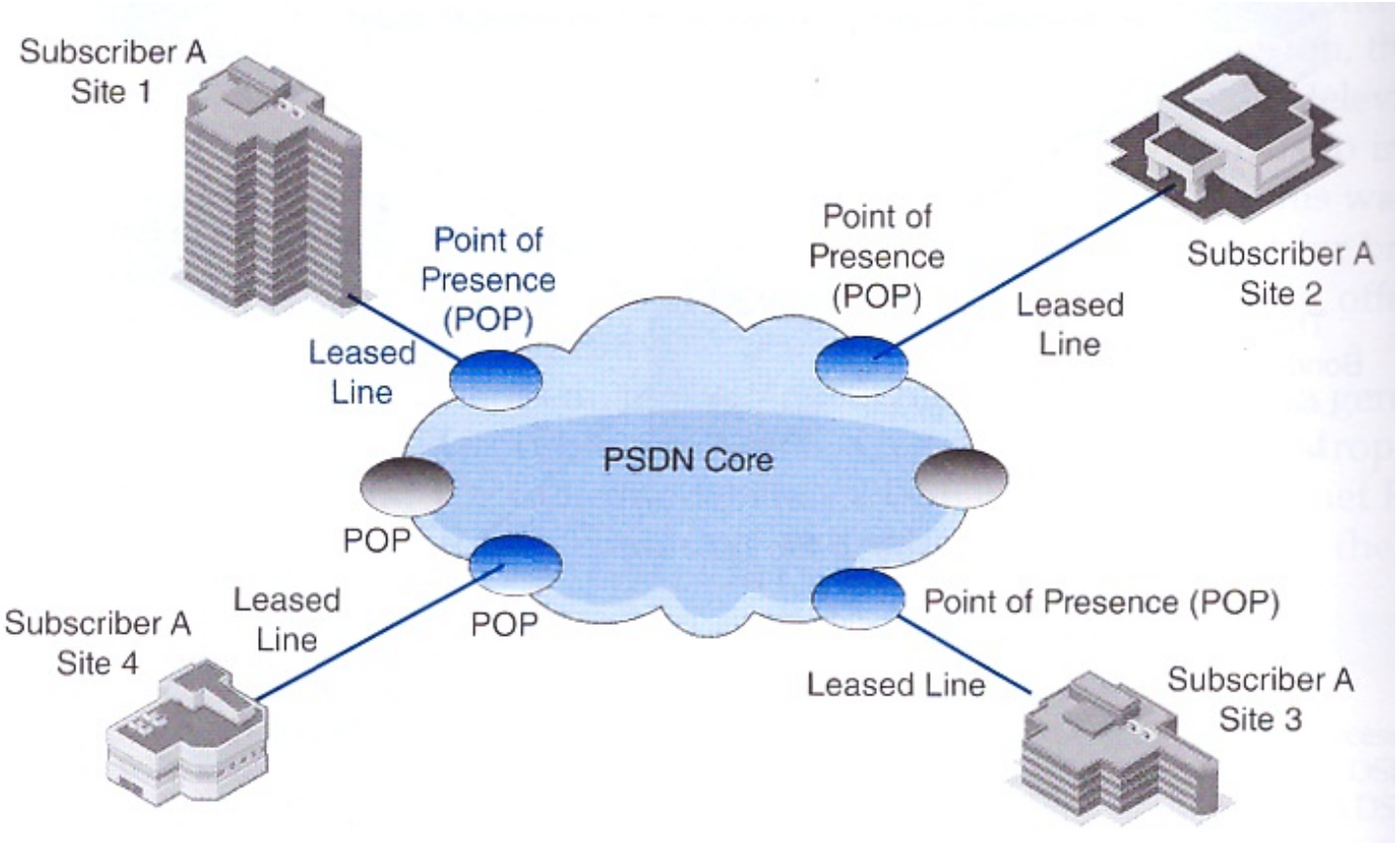
Network core

WAN core can be provided either by leased lines...



Network core

... or by **Public Switched Data Network (PSDN)**.
The corporation needs only one leased line per site, from the site to the nearest **Point Of Presence** (PSDN's access point).

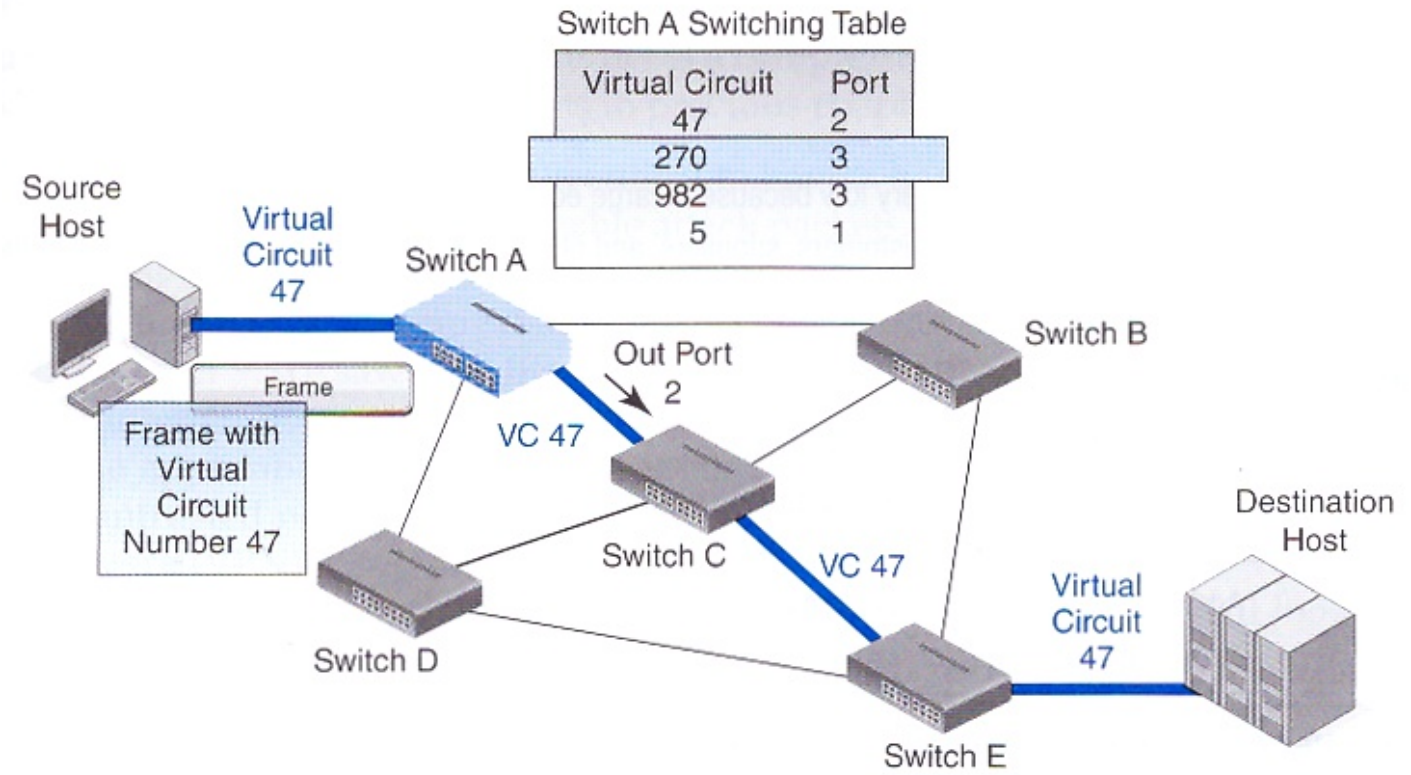


PSDN standards

X.25	Original PSDN standard in the 1970s, now obsolete. Slow and expensive.
Frame Relay	Cheaper than X.25. Rated speed from 256 kbps to 40 Mbps.
ATM	Asynchronous Transport Mode. Expensive. Rated speed from 1 Mbps to 300 Gbps.
Metro Ethernet	Good price/quality ratio. Rated speed from 1 to 100 Mbps.

PSDN core operations

PSDN switches inside the cloud are connected in a mesh topology. The best path between two sites (from source POP to destination POP) is calculated before transmission as a **virtual circuit**. Therefore, PSDN frame headers carry a 10-bit **Data Link Control Identifier (DLCI)** i.e. the VC number, instead of the destination's IP address.



Internet as a WAN

Advantages:

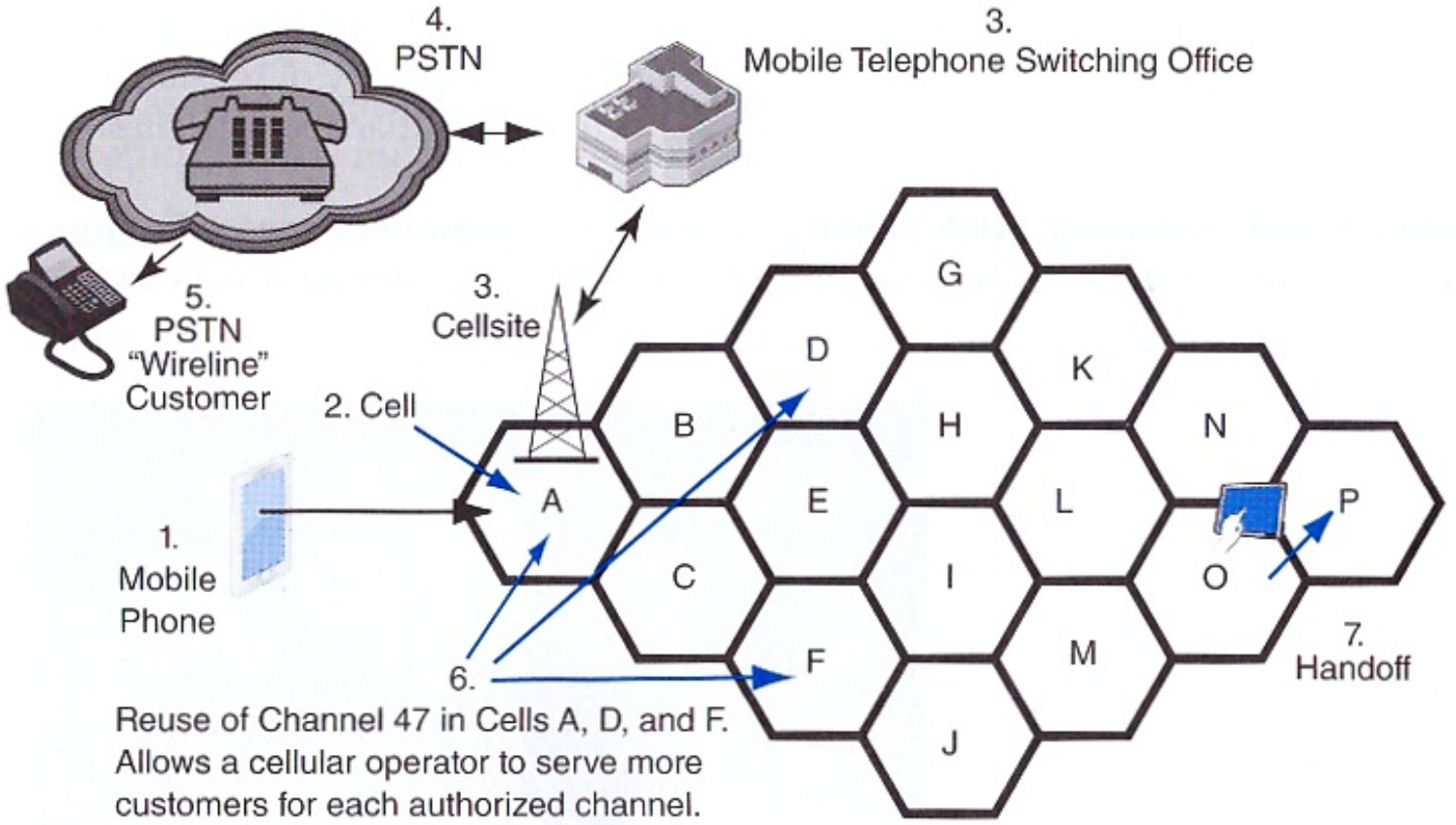
- ✓ Low cost per bit
- ✓ Easy connectivity, as the Internet is widespread

Issues:

- ☠ Security ← solvable by firewalls, IDSs, VPN, and malware filtering
- ☠ Non-guaranteed QoS ← solvable by using a single ISP (with MPLS)

Cellular telephony

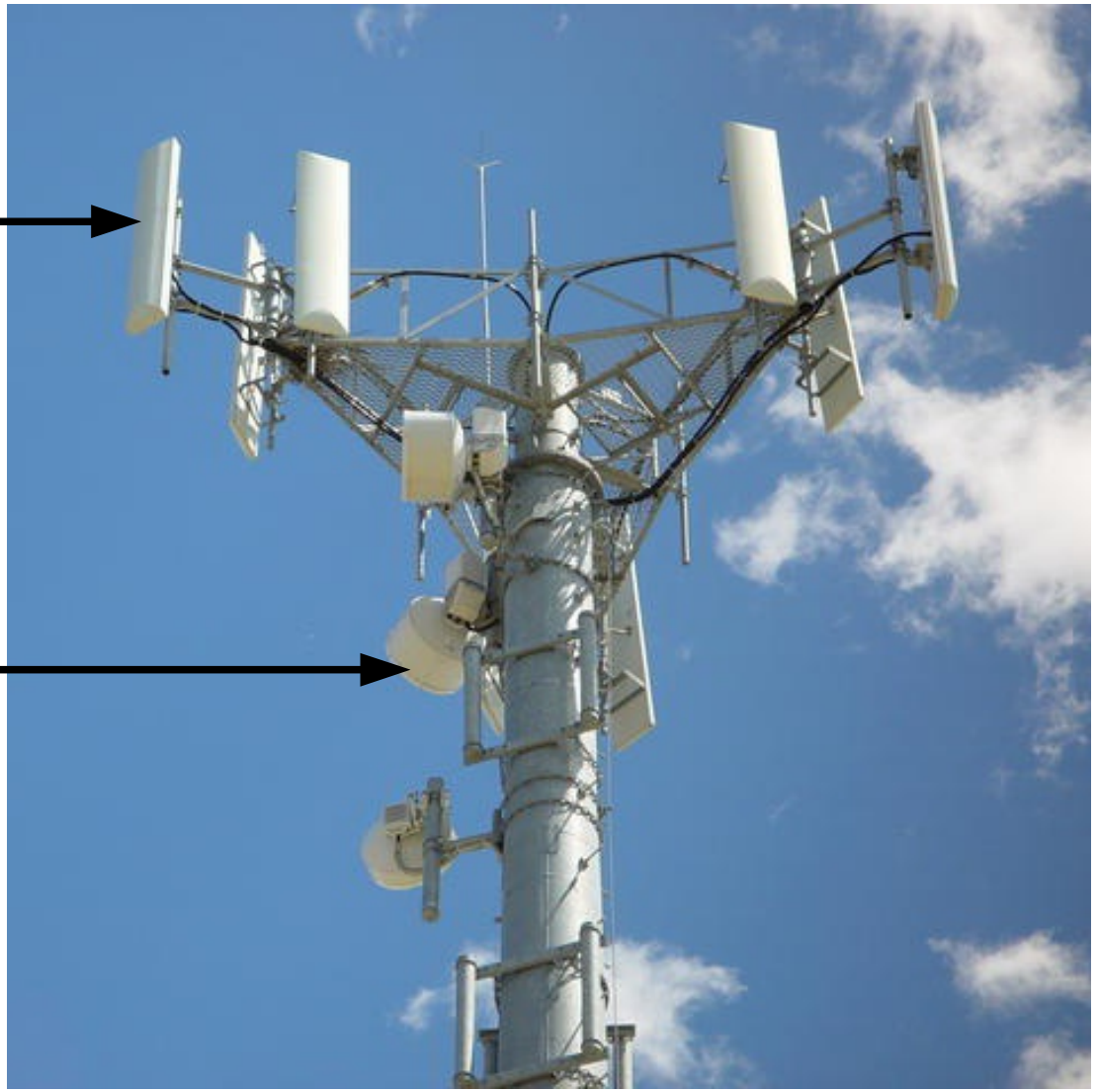
A phone operator's service area is divided into **cells**. In the middle of each cell, a **cell site** (aka **cell tower**) contains a **transceiver** antenna to relay signals from/to mobile phones and to the **MTSO**. Non-adjacent cells reuse the same channel frequency.



Cell tower

cellular antennas for phone to phone communication

microwave antennas for point-to-point transmission with the MTSO



Handoff and roaming

A mobile phone can travel from a cell's connection to another cell...

... of the same operator = **handoff**
... of another operator, in another cellular system = **roaming**

The two terms are not interchangeables as in 802.11 WLANs.

Cellular generations

1G (1980s) Analog radio transmission, < 10 kbps

2G (1990s) Digital radio transmission, 10 to 20 kbps

3G (2000s) 384 kbps (moving clients) to 2 Mbps (stationary)
Used for web surfing, video streaming, data sync
Smartphones, but also laptops and tablets
Enhanced by **HSPA+ (High Speed Access Packet plus)** and **LTE (Long Term Evolution)** providing up to 10 Mbps

4G (2010s) 200 Mbps (moving clients) to 1 Gbps (stationary)
Based on two technologies: **LTE Advanced** and **IEEE 802.16 (WiMAX)**

Networked applications

Networked applications are applications that require a network to operate.

The growth of networking in the 1990s has created a new type of application architecture: client/server processing.

Since the 2010s a huge number of services have been outsourced from the local PC to the **cloud** (e.g. document editing, ticketing, e-mail antivirus scanning).

VoIP

Voice over IP (VoIP) is the transmission of voice telephone signals over IP packet-switched internetworks.

The client can be a PC with multimedia hardware as well as a **VoIP phone**. They use **codecs** to convert analog voice signals into digital voice data.

A **media gateway** connects a VoIP system with the ordinary PSTN.

VoIP

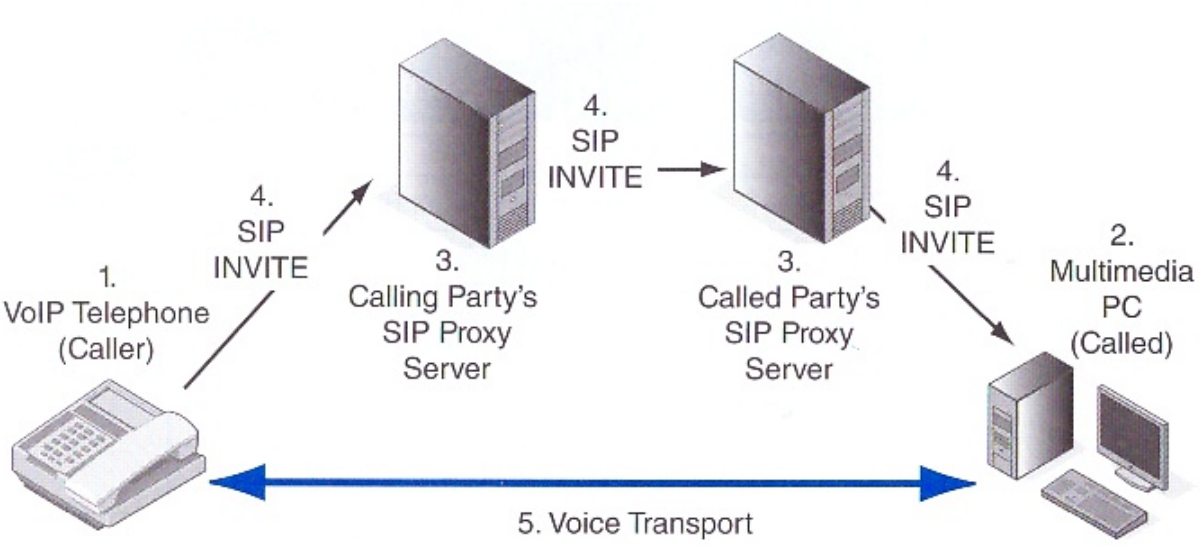
VoIP signaling: circuits set-up and disconnection, billing, and call supervision.

Standards:
- **H.323** by ISO
- **Session Initiation Protocol (SIP)** by IETF

VoIP transport: actual transfer of voice.

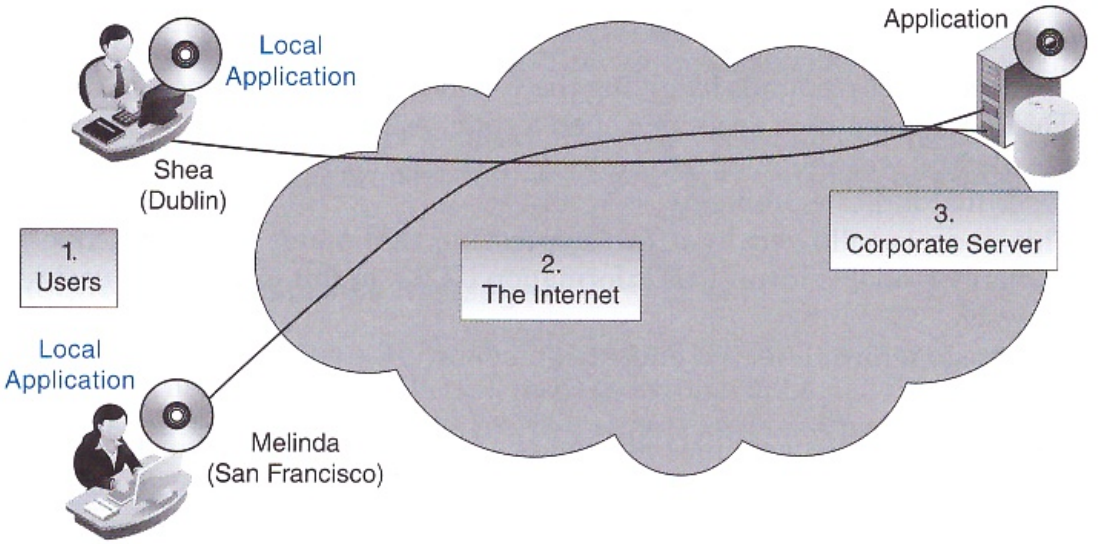
VoIP uses UDP and **Real Time Protocol (RTP)**.

The RTP header contains a sequence number to ensure that datagrams are delivered in order, and a timestamp to avoid jitter.

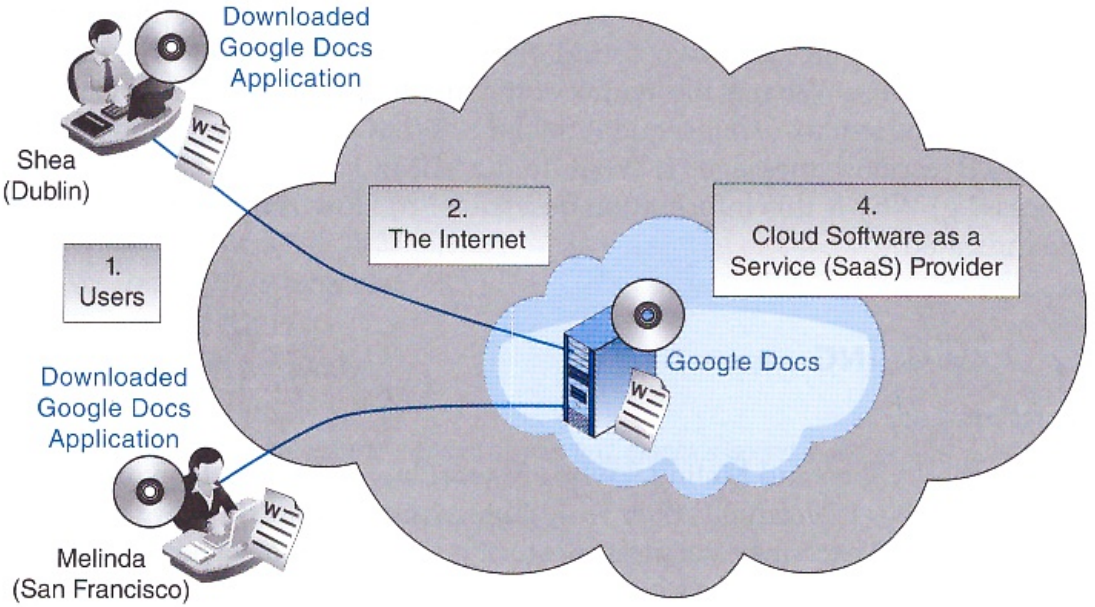


Cloud SaaS

Traditional sharing:
users keep their versions of the documents on a corporate server, accessible via the Internet.

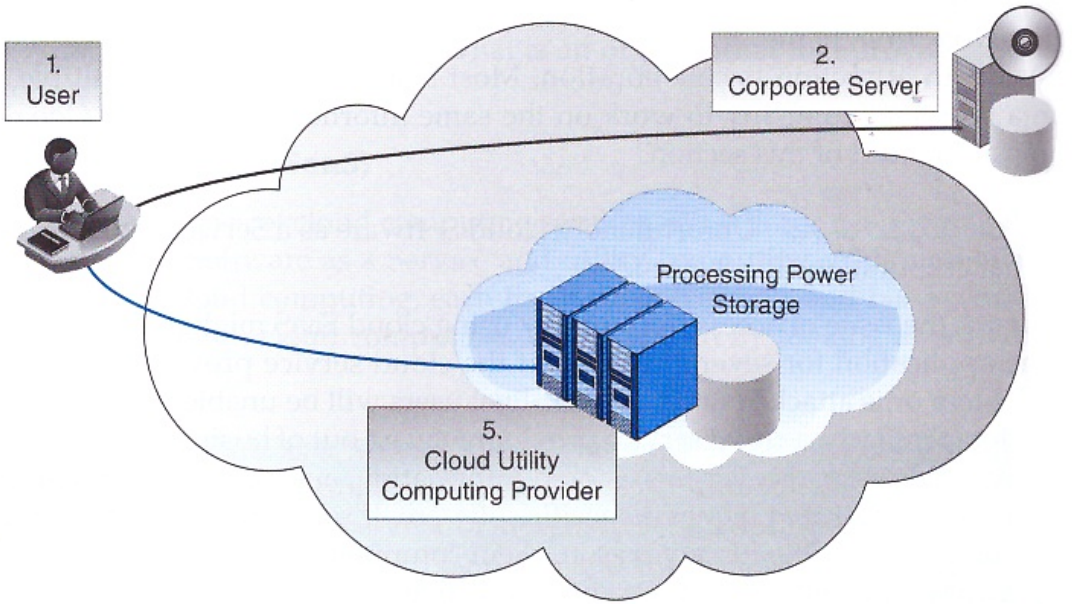


Cloud SaaS (Software as a Service):
application and data are stored in the Cloud.



Cloud computing

In **cloud utility computing**, the company offloads server processing work to a cloud service provider, and the data is sent over the Internet to be processed.



Factors that made the success of cloud computing:

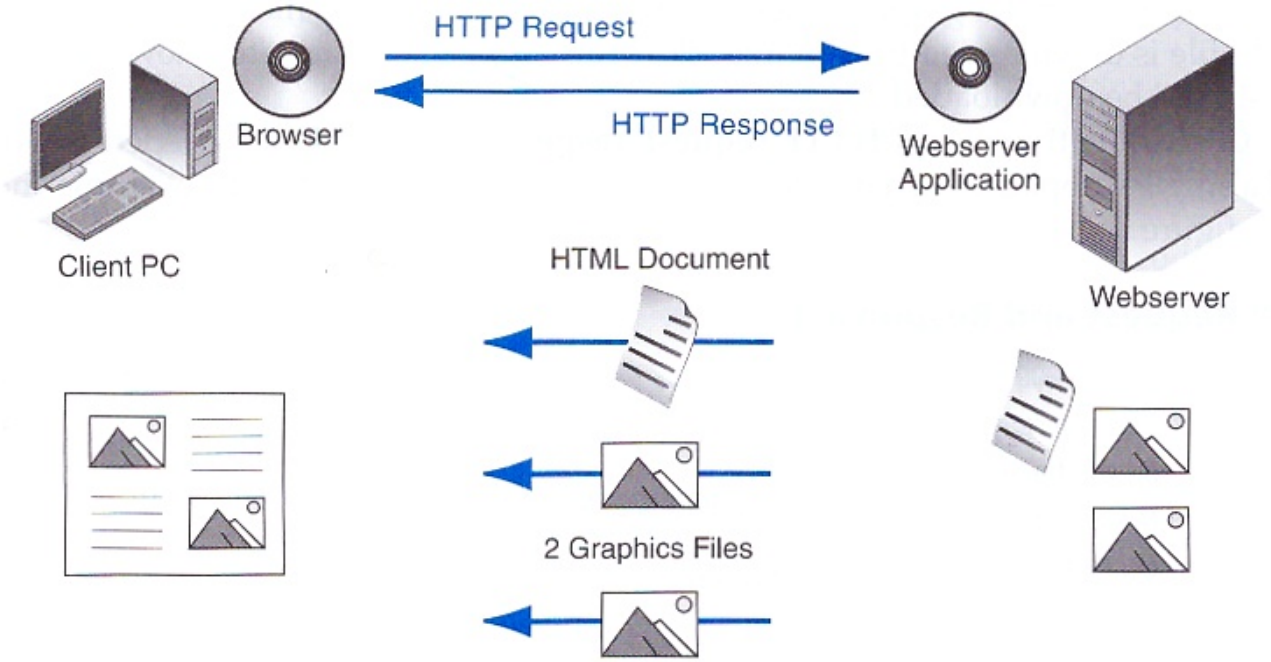
- Speed, accessibility, and reliability of the Internet
- Web services allowed remote machines to communicate easily
- **Virtualization** of machines

World Wide Web

The **World Wide Web** was created by Sir Tim Berners-Lee at CERN in 1991.

It is based on two standards:

- **HyperText Markup Language (HTML)** for document format
- **HyperText Transfer Protocol (HTTP)** for file transfer



HTTP session

client

```
GET /index.html HTTP/1.1
Host: students.webster.edu
```

server

```
HTTP/1.1 200 OK
Date: Mon, 19 May 2014 22:38:34 GMT
Server: Apache/1.3.3.7 (Unix) (Red-Hat/Linux)
Last-Modified: Wed, 07 Mar 2012 23:11:55 GMT
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
Content-Length: 131
Accept-Ranges: bytes
Connection: close

<html>
<head>
   <title>An Example Page</title>
</head>
<body>
   <h1>Hello!!!</h1>
   Hello World, this is a very simple HTML document.
</body>
</html>
```

HTTP session

The client issues a HTTP command GET to download content. Other commands are POST, PUT, ...

The server replies with a HTTP status code, e.g.:

200 OK
403 Forbidden
404 Not Found
500 Internal Server Error

The **MIME (Multipurpose Internet Mail Extension)** standard specifies the format of the file being delivered as the body of the response message.

Service-Oriented Architecture

A **program-oriented architecture** is build on individual large programs interacting with each other.

In **Service-Oriented Architecture** the programs are replaced by **service objects**, each one providing one or more services to callers.

Each service object can be **reused** simultaneously by several callers.

Service objects and callers are **language-independent**.

Web services implement SOA using WWW standards, for instance using XML-encoded **SOAP (Simple Object Access Protocol)**.

SOAP

A client sends a GetStockPrice request.
The request has a StockName parameter, and a Price parameter that will be returned in the response:

```
POST /InStock HTTP/1.1
Host: www.example.org
Content-Type: application/soap+xml; charset=utf-8
Content-Length: nnn

<?xml version="1.0"?>
<soap:Envelope
xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
soap:encodingStyle="http://www.w3.org/2001/12/soap-encoding">

<soap:Body xmlns:m="http://www.example.org/stock">
   <m:GetStockPrice>
      <m:StockName>IBM</m:StockName>
   </m:GetStockPrice>
</soap:Body>

</soap:Envelope>
```

SOAP

The server replies with a GetStockPriceResponse:

```
HTTP/1.1 200 OK
Content-Type: application/soap+xml; charset=utf-8
Content-Length: nnn

<?xml version="1.0"?>
<soap:Envelope
xmlns:soap="http://www.w3.org/2001/12/soap-envelope"
soap:encodingStyle="http://www.w3.org/2001/12/soap-encoding">

<soap:Body xmlns:m="http://www.example.org/stock">
   <m:GetStockPriceResponse>
      <m:Price>34.5</m:Price>
   </m:GetStockPriceResponse>
</soap:Body>

</soap:Envelope>
```

BitTorrent

BitTorrent is a P2P protocol for file sharing.

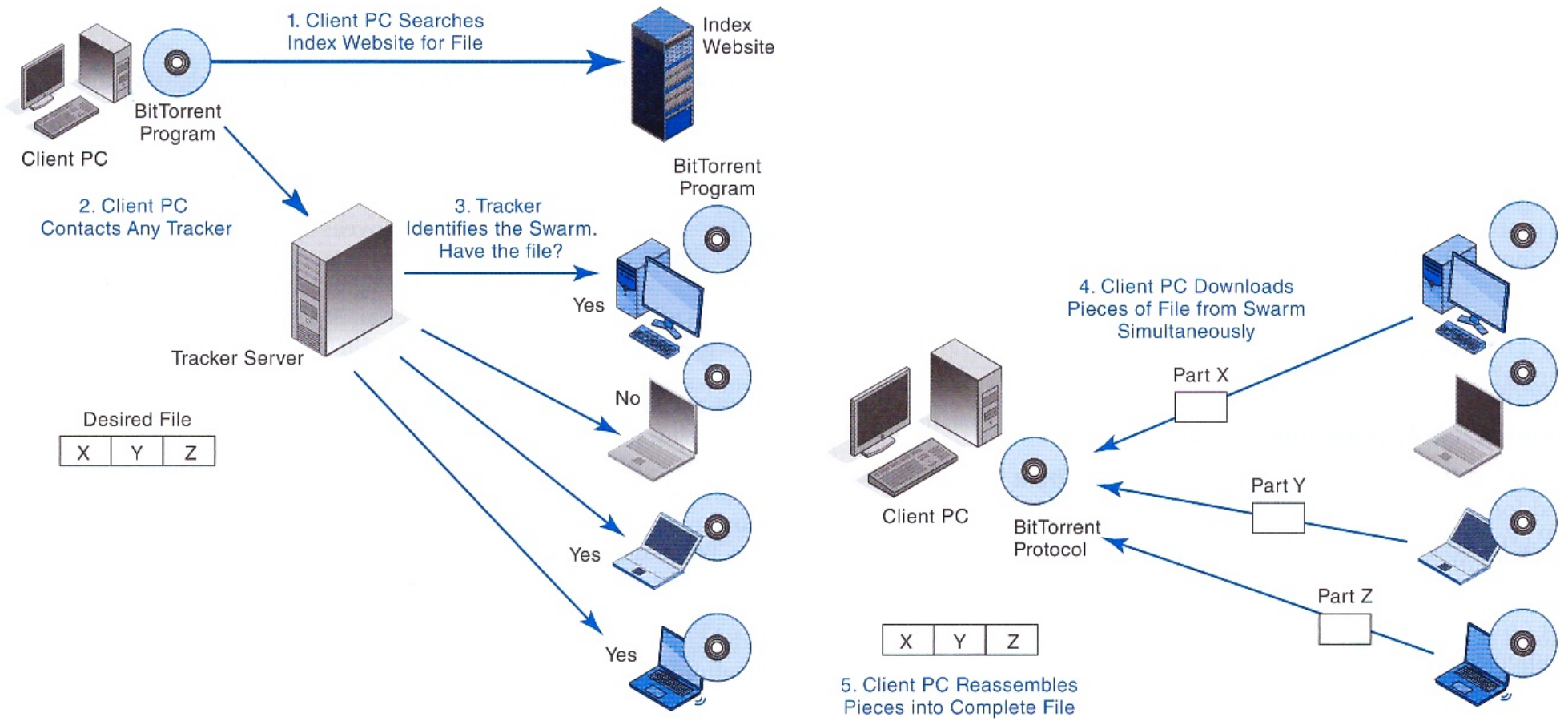
The file being shared is divided into segments.
The requesting node (**leecher**) downloads each segment from another BitTorrent node (**seeder**).

An index webserver provides a **.torrent** file, which contains metadata about the file to be shared, the cryptographic hashes of all segments, and the URL of the **tracker** computer that will coordinate the sharing of that file.

The tracker identifies the **swarm**, composed of the BitTorrent seeder nodes having a copy of the file segments.

The leecher downloads all file segments in random order and reassembles them once the download is complete.
The leecher also seeds a segment as soon as it has downloaded it.

BitTorrent


1. Client PC Searches Index Website for File
Index Website
BitTorrent Program
Client PC
2. Client PC Contacts Any Tracker
3. Tracker Identifies the Swarm. Have the file?
BitTorrent Program
Yes
Tracker Server
No
Desired File
X Y Z
Yes
Yes
4. Client PC Downloads Pieces of File from Swarm Simultaneously
Part X
Part Y
Part Z
Client PC
BitTorrent Protocol
X Y Z
5. Client PC Reassembles Pieces into Complete File

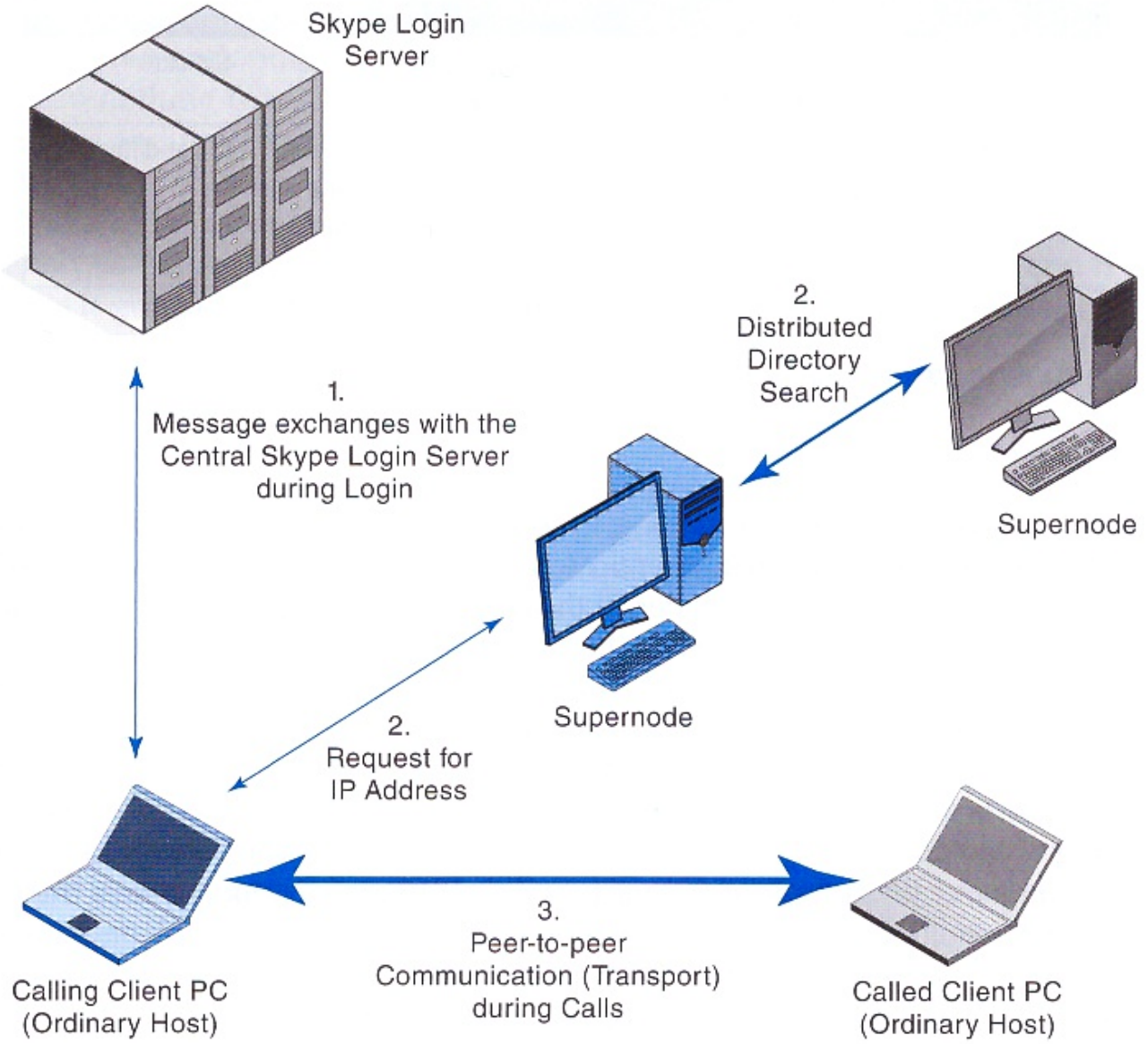
Skype

Skype is currently the most popular P2P VoIP service.

The user logs in to the central **Skype login server** that takes note of the user's host IP address.
Signaling is not done by a SIP proxy but by **supernodes** instead, which perform a P2P directory search for the username and IP the caller wants to contact.
After the call is established, the calling host communicates directly via P2P with the called host (VoIP transport).

Supernodes are chosen amongst Skype hosts that have enough memory, CPU, and network bandwidth.

Skype


Skype Login Server
1. Message exchanges with the Central Skype Login Server during Login
2. Distributed Directory Search
Supernode
Supernode
2. Request for IP Address
3. Peer-to-peer Communication (Transport) during Calls
Calling Client PC (Ordinary Host)
Called Client PC (Ordinary Host)

SETI@home

SETI@home is a P2P processing application that uses the computing power of the peer host when idle for the SETI project (Search for Extra-Terrestrial Intelligence).
This processing power is used to analyze chunks of radio data transmissions from deep space and look for non-noise signals.