Open Systems Interconnection
(OSI)
Reference Model
(by the ISO)

Client

| Application |
| Presentation |
| Session |
| Transport |
| Network |
| Data Link |
| Physical |

Router

| Network |
| Data Link |
| Physical |

Server

| Application |
| Presentation |
| Session |
| Transport |
| Network |
| Data Link |
| Physical |
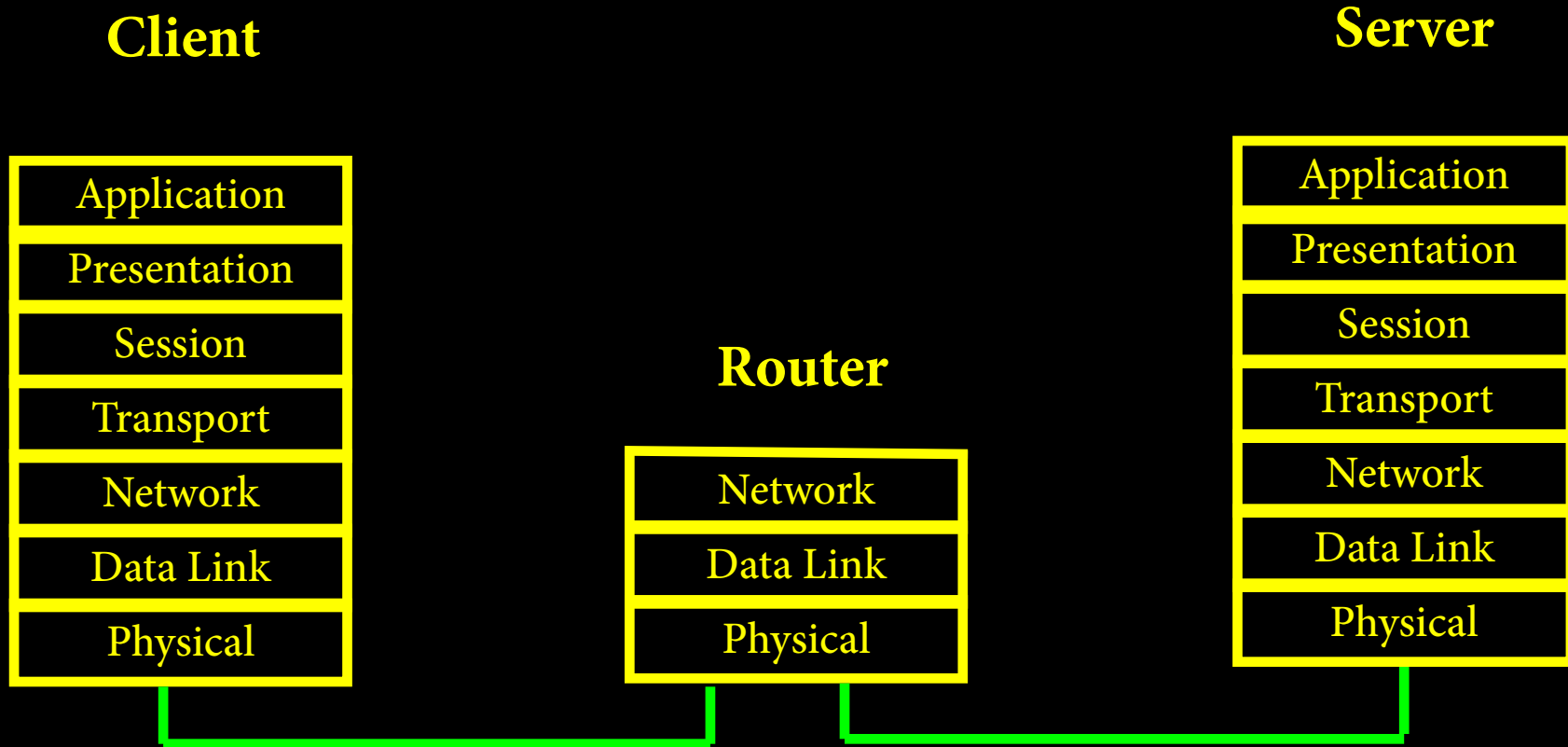
OSI Reference Model Layer Attributes

Layer k + 1

Interface Specifications

Service Provided by layer k

Interface Specifications

Layer k

Protocol

Layer k

Layer k - 1

Layer k + 1

Layer k - 1
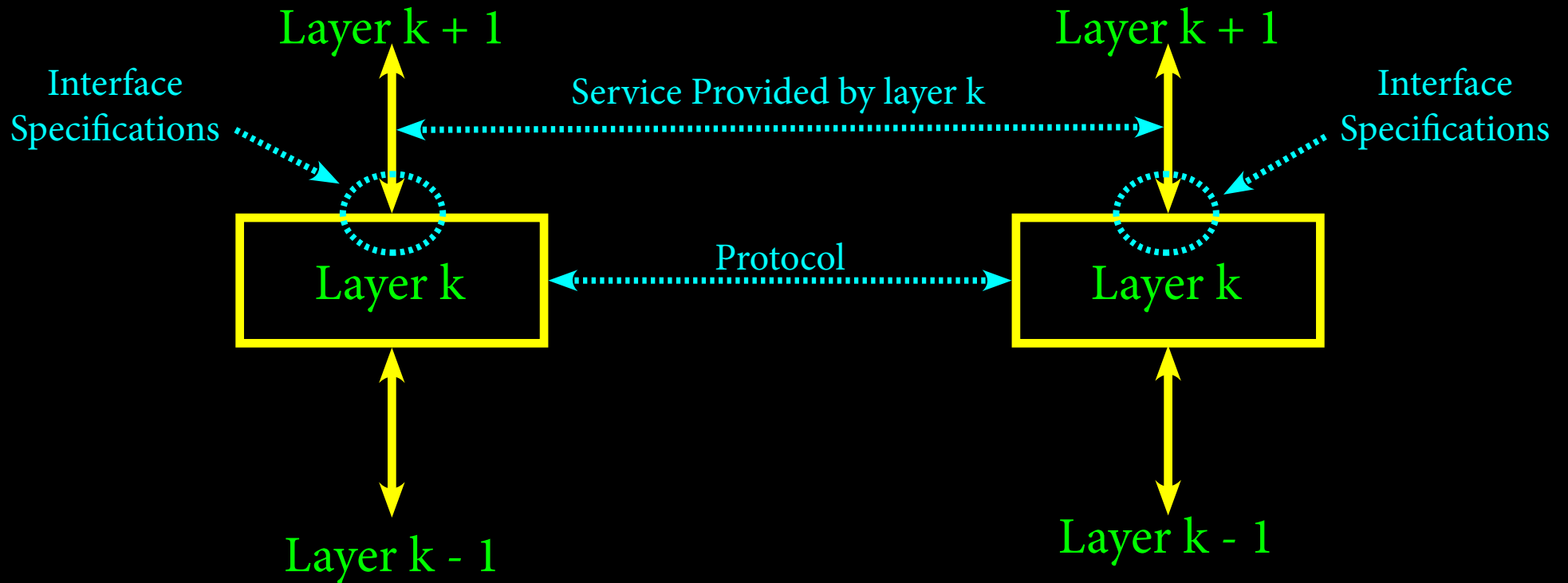
OSI Reference Model *Physical* Layer Attributes

Data Link Layer   Data Link Layer

Service Provided by Physical Layer

Physical Layer   Protocol   Physical Layer

Interface Specifications   Interface Specifications

Physical Transmission Medium   Physical Transmission Medium

Cable
Optical
Wireless

Cable
Optical
Wireless
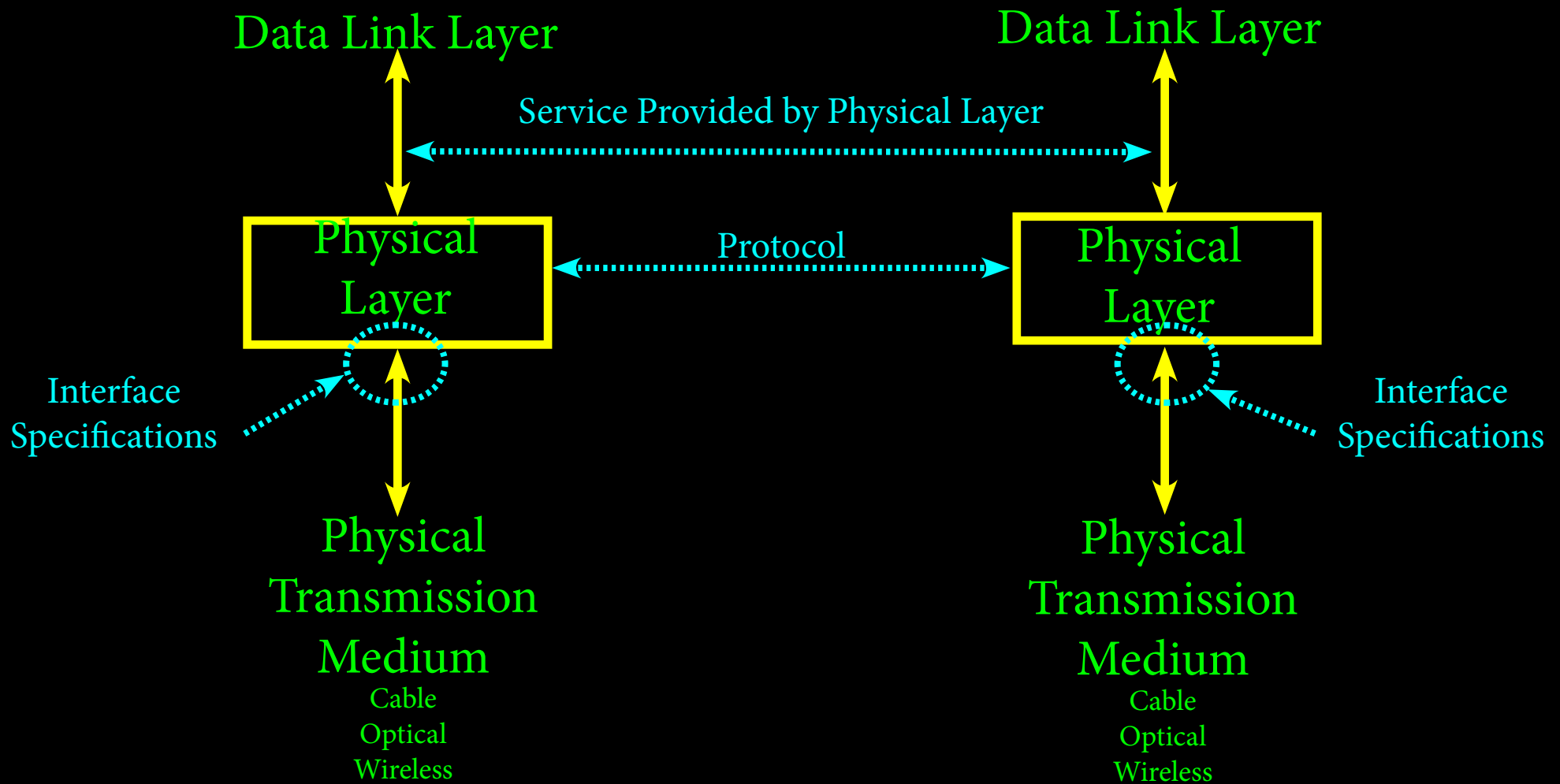
Physical Layer Attribute Detail

Service Attribute:

1. Transportation of bits (ones and zeros) between sender and receiver.

2. (sender) Conversion of bits into the electrical, optical, or radio signal accepted by the transmission medium.

3. (receiver) Conversion of transmission medium's signal into bits.

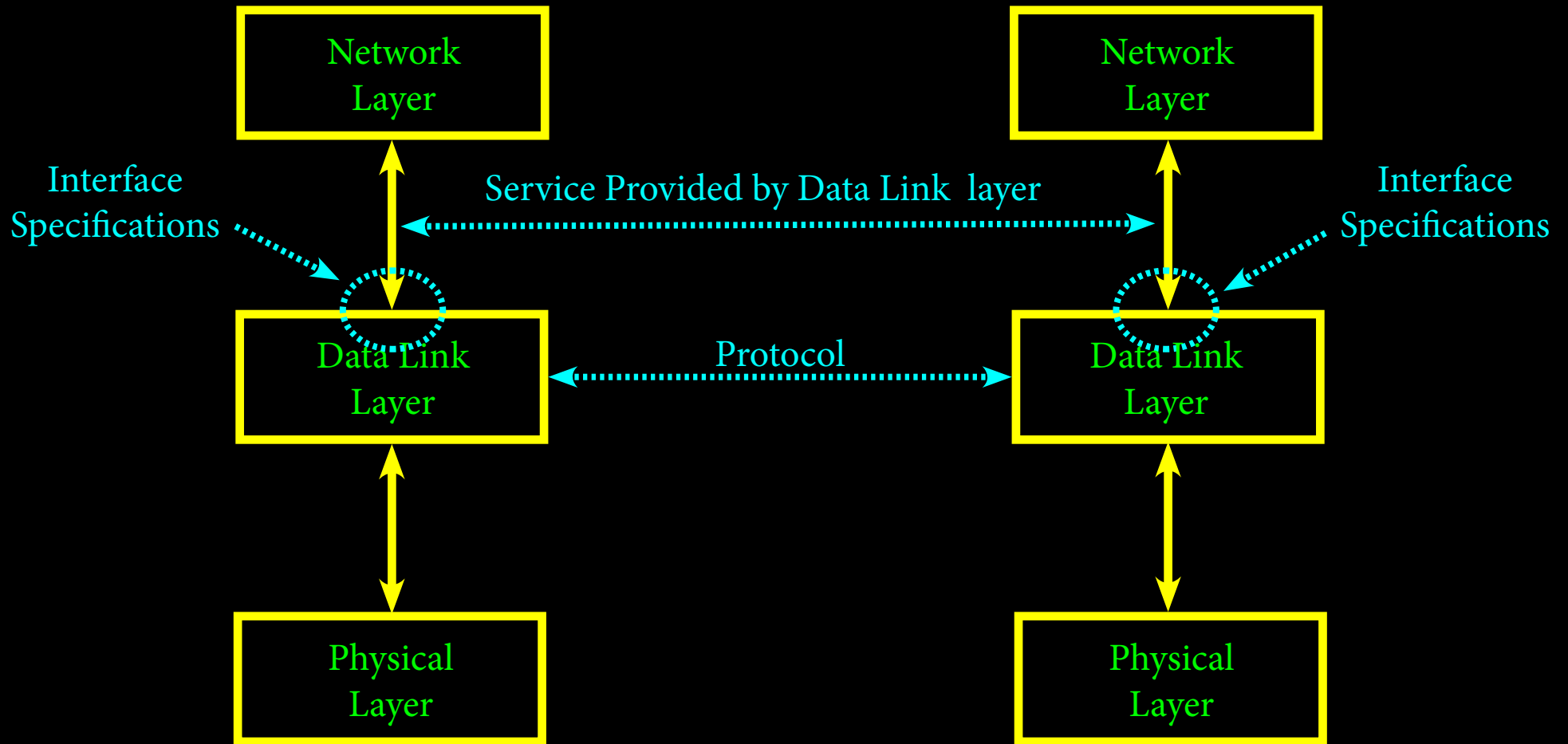# Physical Layer Attribute Detail

Protocol Attribute:

1. Electrical, optical, or radio signal as defined by the transmission medium

2. Modulation and demodulation or digital signal conversion in compliance with the transmission medium.

Physical Layer Attribute Detail

Interface Attribute:

1. Physical jack specifications, or

2. Wireless card interface spcifications

3. Speed, and "plexing" technique:
   Simplex
   Half duplex
   Full duplex, etc.

OSI Reference Model *Data Link* Layer Attributes

Network Layer

Network Layer

Interface Specifications

Service Provided by Data Link layer

Interface Specifications

Data Link Layer

Protocol

Data Link Layer

Physical Layer

Physical Layer

Data Link Layer Attribute Detail

Service Attribute:

1. Framing

2. Error checking

3. Switching

4. Virtual LAN (VLAN)

Data Link Layer Attribute Detail
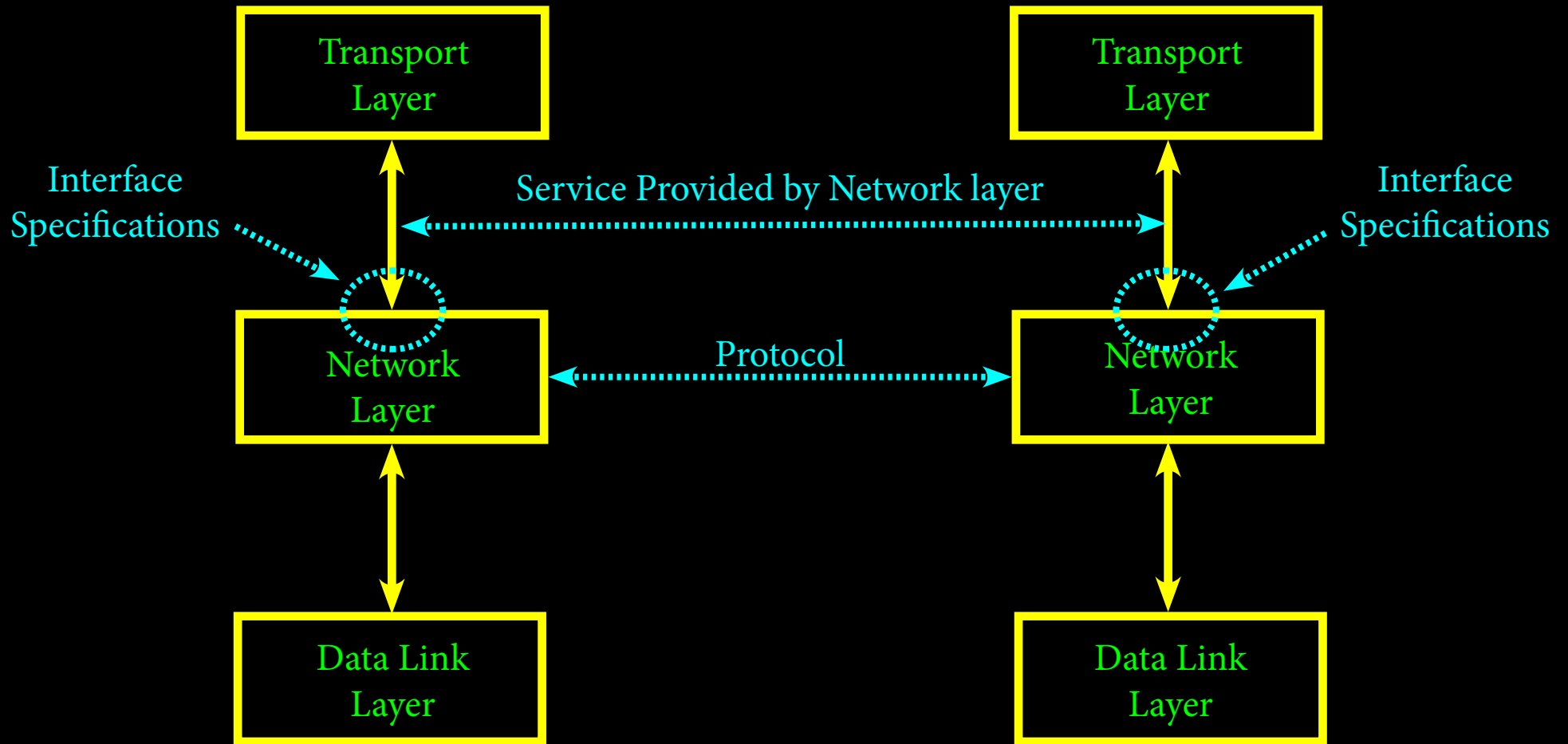
Protocol Attribute:

1. Logical Link Control (Ethernet framing) IEEE 802.2

2. Logical Access Procedure Balanced (LAPB), used in X.25

3. Logical Access Procedure for D channel (LAPD), used ISDN

4. Layer 2 Tunnel Protocol (L2TP), used by some VPNs

5. For a complete list, visit the IANA site:
   http://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.xhtml#ieee-802-numbers-1

Data Link Layer Attribute Detail

Interface Attribute:

1. Encapsulating (sending):
    Formatted frame passed down to physical layer as a
    serialized bit stream

2. De-capsulating (receiving):
    Network layer protocol number from Ethernet type
    field and PDU passed up to network layer

OSI Reference Model *Network* Layer Attributes

Transport Layer

Transport Layer

Interface Specifications

Service Provided by Network layer

Interface Specifications

Network Layer

Protocol

Network Layer

Data Link Layer

Data Link Layer

Network Layer Attribute Detail

Service Attribute:

1. Address Resolution

2. Routing

3. Congestion Control

4. Quality of Service

5. Internetworking

6. NAT

Network Layer Attribute Detail

Protocol Attribute:

Popular Network Layer Protocols:
IPv4
IPv6
ARP
MPLS

For a complete list, visit the IANA table:

http://www.iana.org/assignments/protocol-num-bers/protocol-numbers.xhtml#protocol-num-bers-1

Network Layer Attribute Detail

Interface Attribute:

1. Encapsulating (sending):
   Network protocol number and PDU passed down to data link layer

2. De-capsulating (receiving):
   Transport protocol number from 8-bit protocol value field, and PDU passed up to transport layer

OSI Reference Model *Transport* Layer Attributes

Session Layer · Transport Layer · Network Layer

Interface Specifications

Service Provided by Transport layer

Protocol
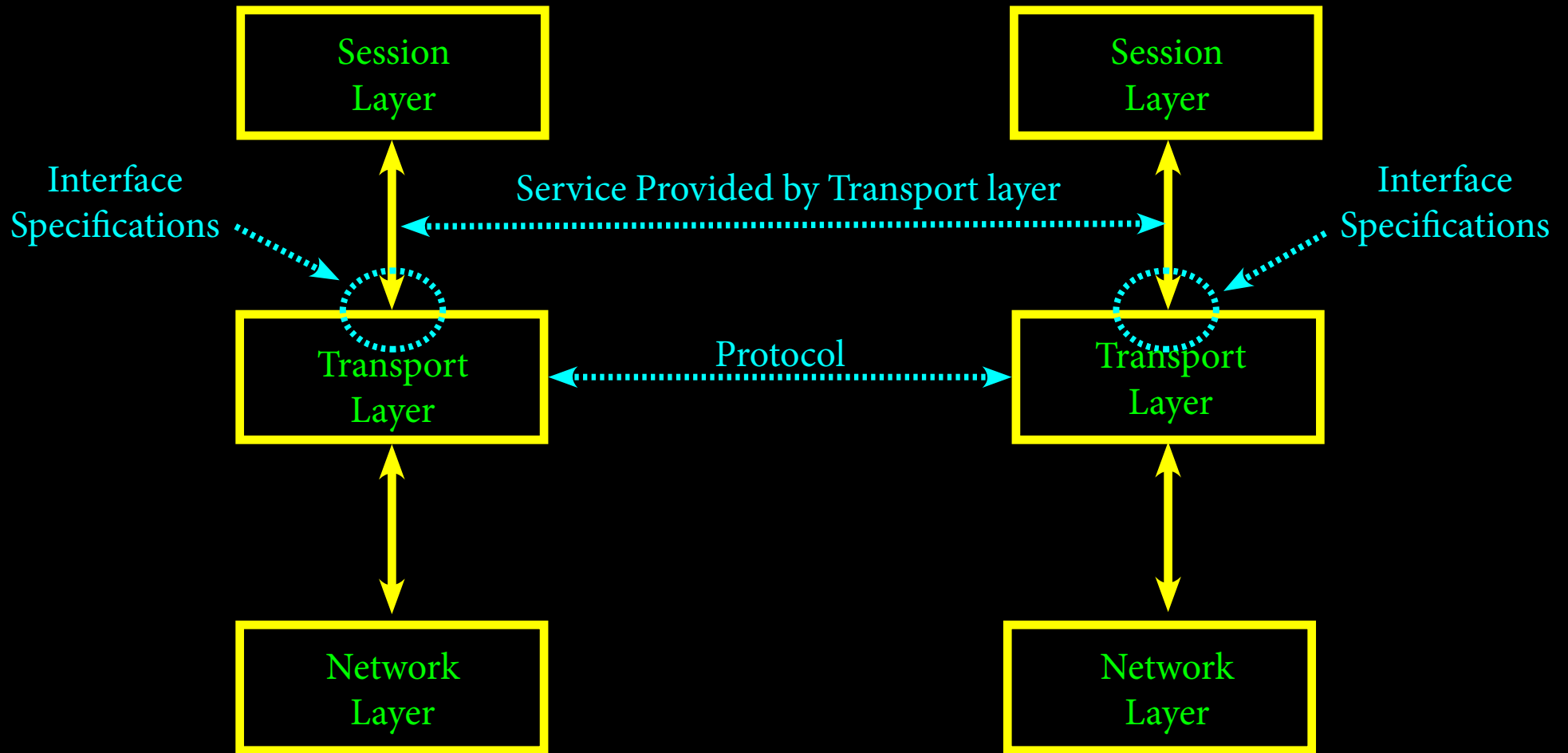
Transport Layer Attribute Detail

Service Attribute:

1. End-to-end connectivity
   Connection-oriented
   Connectionless-oriented

2. Data transfer management:
   Sequencing
   Blocking
   Concatenation
   Segmenting
   Multiplexing/splitting
   Flow control
   Error dectection/recovery
   Expedited data transfer

3. Port Address Translation (PAT)

Transport Layer Attribute Detail
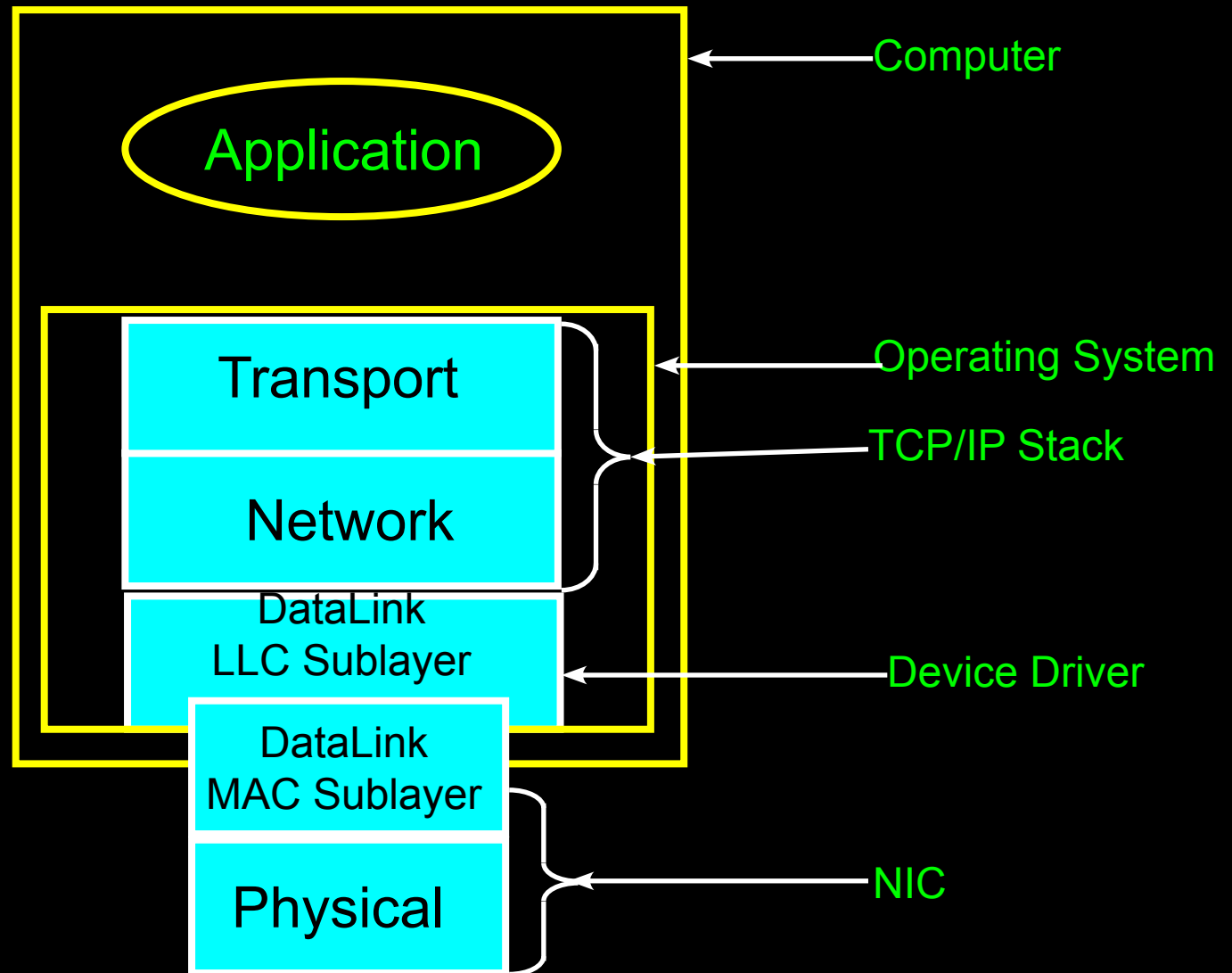
Protocol Attribute:

Popular Protocols:

1. TCP - Connection Oriented

2. UDP - Connectionless Oriented

3. For a complete list visit the IANA site:
   http://www.iana.org/assignments/service-names-port-numbers/
   service-names-port-numbers.xhtml

Transport Layer Attribute Detail

Interface Attribute:

1. Encapsulating (sending):
   Transport protocol number and PDU passed down to network layer

2. De-capsulating (receiving):
   Destination service port (aka. application protocol number) and socket number passed up to application layer

Typical Implementation
of
Physical, Data Link, Network and Transport Layers

TCP/IP Layer-to-Layer Interface Identifications
aka The Demultiplexing of an Ethernet Frame

Application Threads

Socket Number

Application

Destination Service Port

Transport

Protocol Value

Network

Ethernet Type Value

Data Link

MAC

Physical
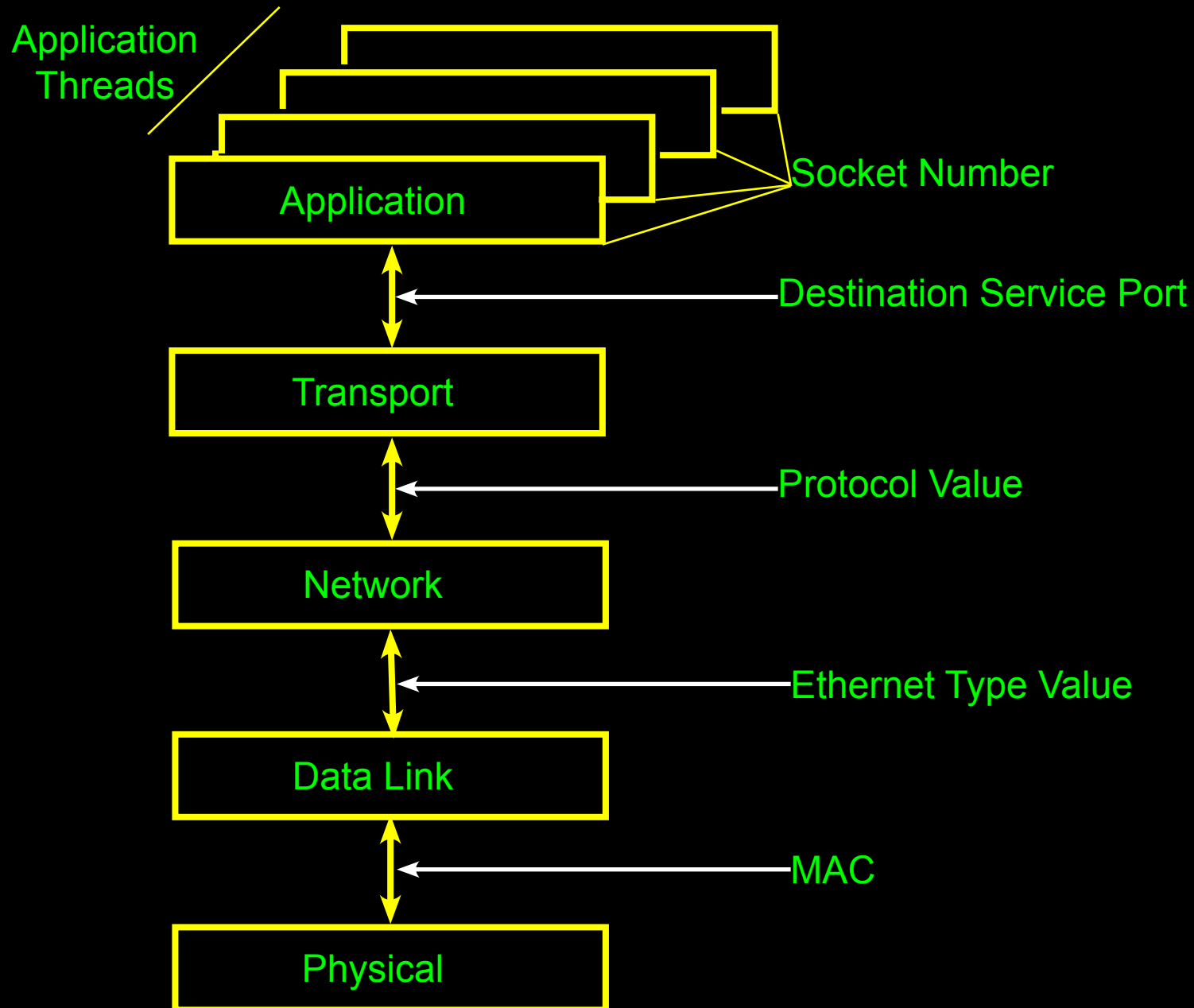
Demultiplexing of received Ethernet frame

Demultiplexing based on socket number

Application   Application   Application   Application

Demultiplexing based on destnation port number

ICMP   IGMP   TCP   UDP

Demultiplexing based on protocol value in IP header

ARP   IP   RARP

Demultiplexing based on type field in Ethernet header

Ethernet Driver

MAC

Incoming Frame
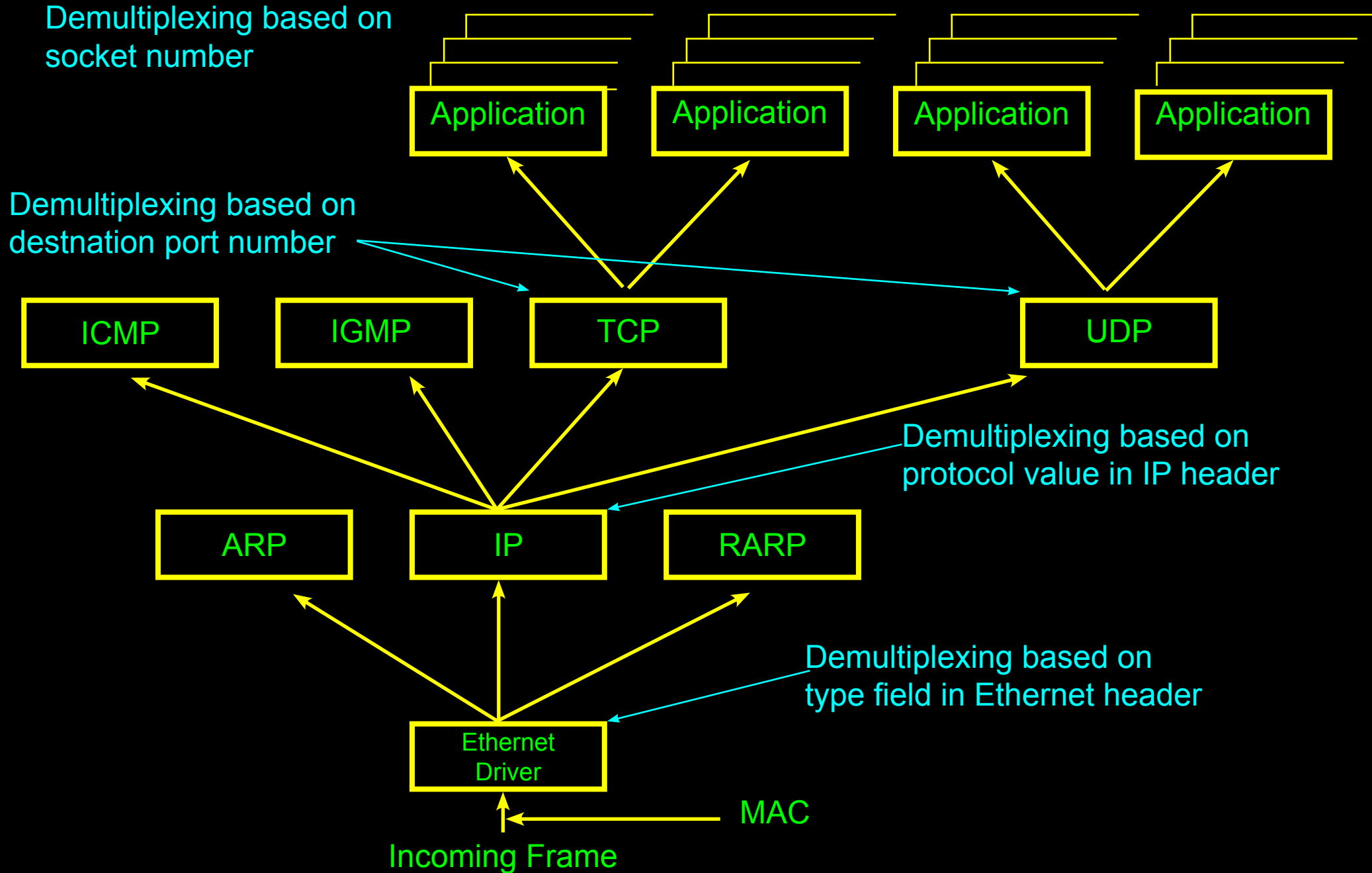
Classful and Special IPv4 Addressing

32 bits

	1st Octet	2nd Octet	3rd Octet	4th Octet

Dotted Decimal Range

Class

A

7 bits	24bits
0 Network ID	Host ID

1.0.0.0 to
127.255.255.255

B

14 bits	16bits
10 Network ID	Host ID

128.0.0.0 to
191.255.255.255

C

21bits	8 bits
110 Network ID	Host ID

192.0.0.0 to
223.255.255.255

D

28 bits
1110 Multicast Address

224.0.0.0 to
239.255.255.255

E

28 bits
1110 Reserved

240.0.0.0 to
255.255.255.255
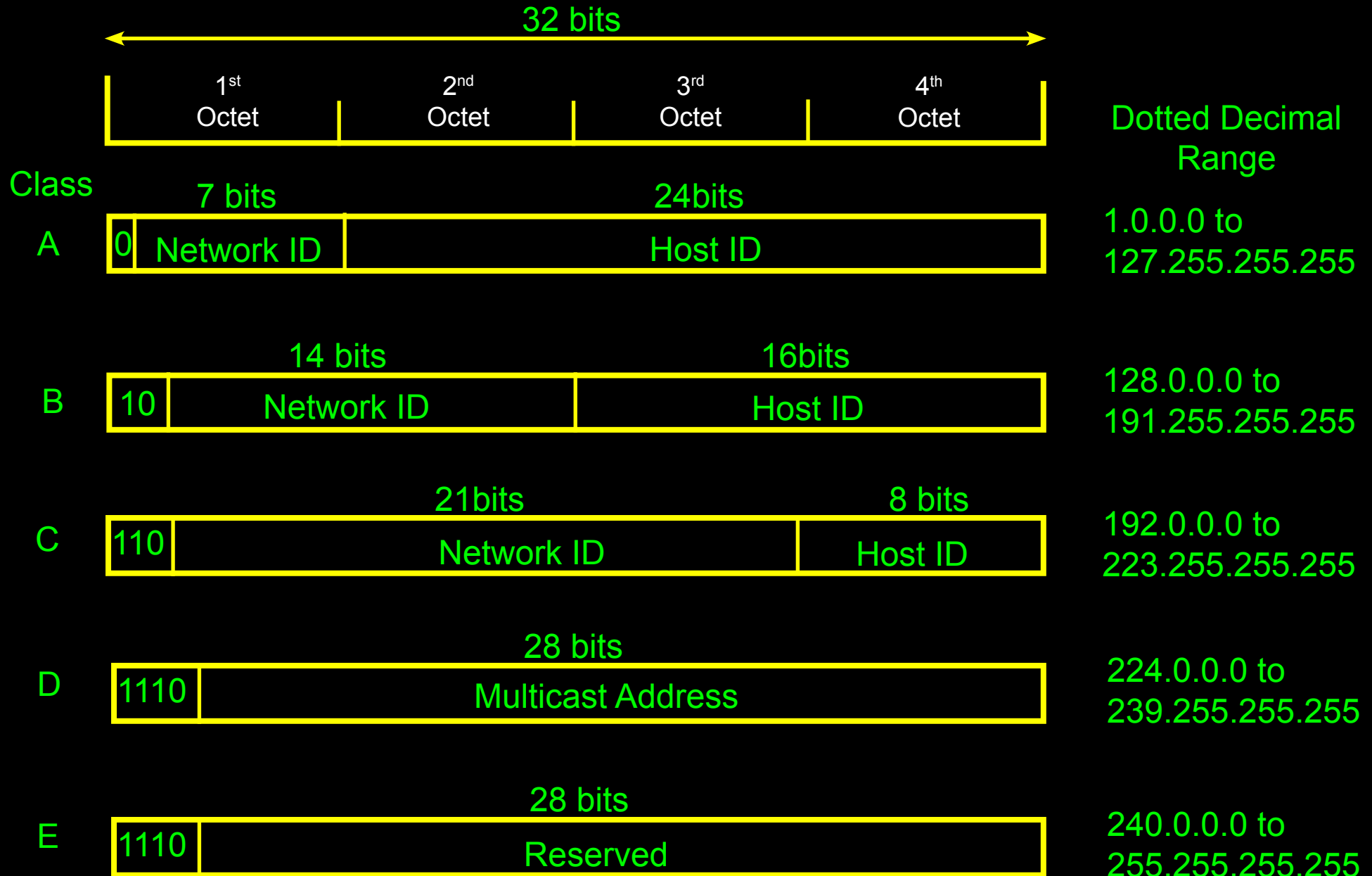
How Subnet Masks Work (same subnet)

	Dotted Decimal
Source Host IP	192.168.101.217
Subnet /Notation	192.168.101/24
Subnet Mask Notation	255.255.255.0
Destination Host IP	192.168.101.210

	Binary
Source Host IP	11000000.10101000.01100101.11011001
Subnet Mask	11111111.11111111.11111111.00000000
Destination Host IP	11000000.10101000.01100101.11010010
Source & Mask	11000000.10101000.01100101.00000000
Dest. & Mask	11000000.10101000.01100101.00000000

How Subnet Masks Work (different subnet)

Dotted Decimal

Source Host IP	192.168.101.217
Subnet /Notation	192.168.101/24
Subnet Mask Notation	255.255.255.0
Destination Host IP	192.168.110.217

Binary

Source Host IP	11000000.10101000.01100101.11011001
Subnet Mask	11111111.11111111.11111111.00000000
Destination Host IP	11000000.10101000.01101110.11010010

Source & Mask	11000000.10101000.01100101.00000000
Dest. & Mask	11000000.10101000.01101110.00000000

Network Protocol Attributes

Autonomous Systems (AS):

   An independently operated network. Operational policies apply to only the boundries of the AS, and not to foreign ASes

Intra-domain networking refers to networking inside the AS

Inter-domain networking refers to networking across multiple ASes

Examples?

Network Protocol Attributes

Router Protocols:

Open Shortest Path First (OSPF) : An Intra-Domain routing protocol. Also called: Interior Gateway Protocol

Algorithm Requirments
Open : Non-proprietary algorithm
Supports multiple distance metrics such as delay and cost
Supports type of service routing
Supports load balancing
Supports hierarchical systems (legacy routers)
Sensitive to security

Network Protocol Attributes

Router Protocols:

Border Gateway Protocol (BGP): An Inter-Domain routing pro-
tocol. Also called Exterior Gateway Protocol

Sample Requirments
Do not carry commerical traffic on the educational network
Do not send Pentagon traffic via an Iraqi route
Use TeliaSonera instead of Verizon because it's lower cost
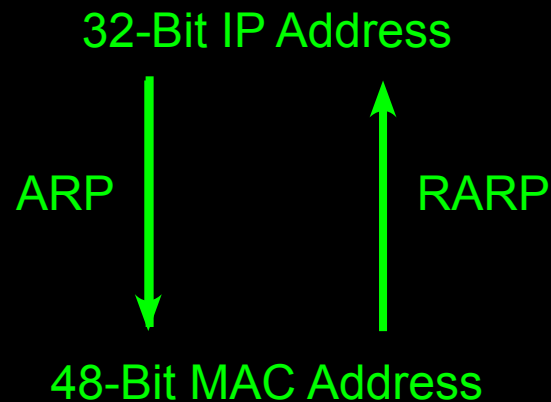Do not use Australian AT&T due to poor performance
Traffic for Apple is not to traverse through Google
etc. etc. etc.

Network Protocol Attributes
Intra- and Inter- Networking Protocols

Address Resolution Protocol (ARP)
and
Reverse Address Resolution Protocol (RARP)

32-Bit IP Address

ARP   RARP

48-Bit MAC Address

Network Protocol Attributes
Networking Protocols

ARP Packet Format

All '1' bits to Broadcast

Populated by Target 0x00000000 in Req.

0x0806

Hdw Size

Pro Size

MAC Destination	MAC Source	Fr. Typ	Hdw Typ	Pro Typ		Op	Sender MAC	Sender IP Addr	Target MAC	Target IP Addr
6	6	2	2	2	1 1	2	6	4	6	4

Ethernet Frame Header

28 Byte ARP Request/Reply

Frame Type	= 0x0806	==>	ARP request or reply
Hardware Type	= 0x0001	==>	Ethernet
Protocol Type	= 0x0800	==>	IEEE 802.3
Hardware Size	= 0x06	==>	Size of MAC addresses
Protocol Size	= 0x04	==>	Size of IP Addresses
Op Code	= 0x0001	==>	ARP Request
	= 0x0002	==>	ARP Response

Network Protocol Attributes
Networking Protocols

Address Resolution Protocol (ARP)

Proxy ARP - When one host, such as a router, stands-in for the target

Gratuitous ARP - When a host sends and ARP request asking for its own MAC

ARP Request to nonexistent Host - Eventually times out. Time out value varies by system.

ARP Reply available to any host that can "hear" it.

Cached ARP data refreshed frequently

Network Protocol Attributes
Networking Protocols

Reverse Address Resolution Protocol (RARP)

Purpose is to obtain an IP address from a destination

Destination must have knowledge of source's MAC address

RARP Packet format nearly same as ARP:

Frame Type = 0x035   ==> RARP Request or Reply
Op Code   = 0x0002   ==> Request
            = 0x0003   ==> Reply

Network Protocol Attributes
Networking Protocols

IP Header Format

4-bit version	4-bit Hdr length	8-bit Type Of Service (TOS)	16-bit total byte length	
16-bit Identification			3-bit flags	16-bit Identification
8-bit Time To Live (TTL)		8-bit protocol	16-bit header checksum	
32-bit Source IP Address				
32-bit Destination IP Address				
Options if any				
Data				

Transport Protocol Attributes
Networking Protocols

TCP Header Format

16-bit Source Port	16-bit destination port

32-bit sequence no.	

32-bit Ack. no.	

32-bit Source IP Address	

4-bit hdr length	reserved	U R G	A C K	P S H	R S T	S Y N	F I N	16-bit window size

16-bit TCP Checksum	16-bit urgent pointer

Options if any	

Data	
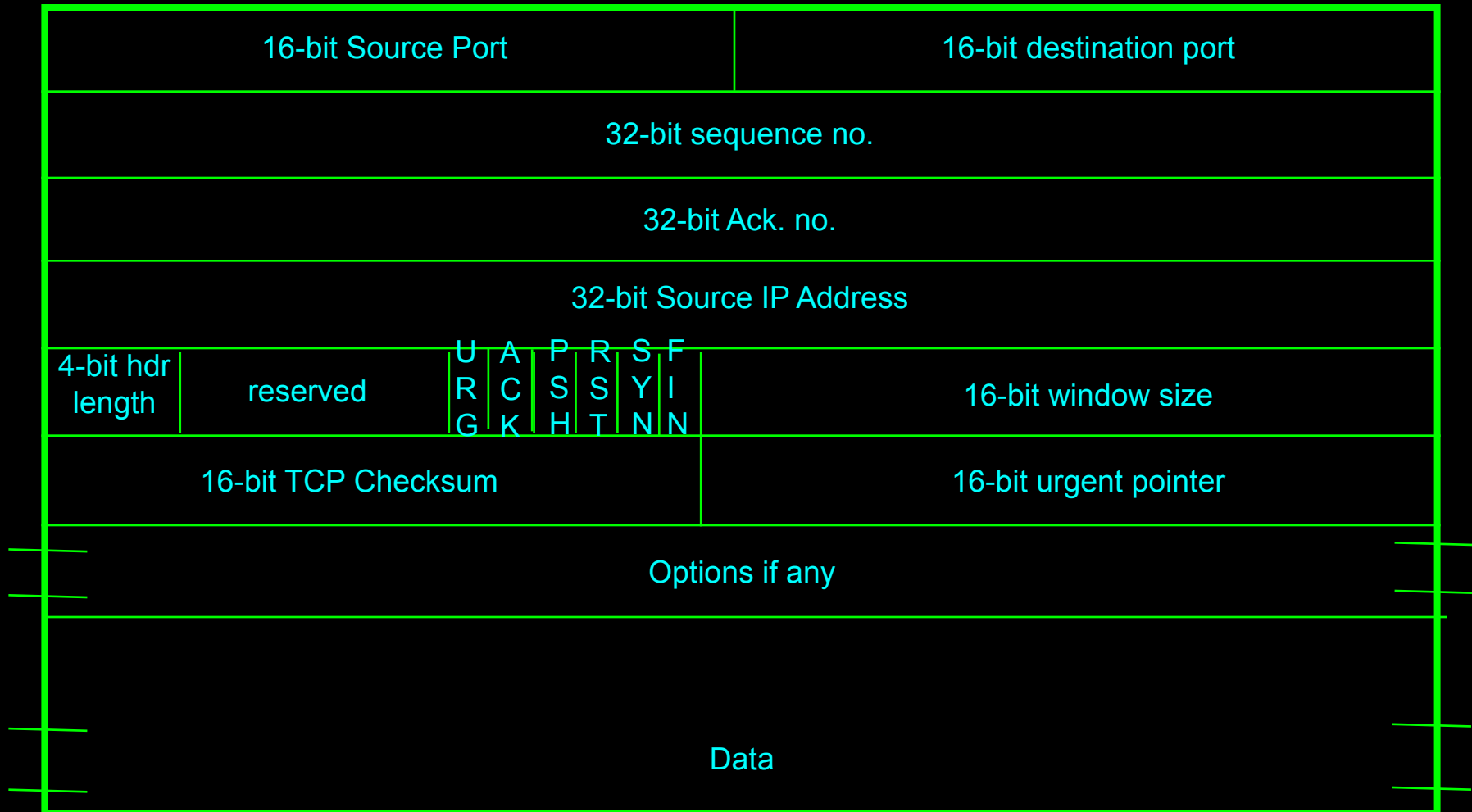
Typical TCP Socket Session

Client

Create stream socket 's'

Bind s to local address

CONNECT s to foreign host

SEND & RECV data on socket s

SHUTDOWN socket s xmt
then rcv

CLOSE socket s

Server

Create stream socket 's'

Bind s to local address

LISTEN for client connect

ACCEPT connect &
LISTEN for next

RECV & SEND data on socket s

SHUTDOWN socket s rcv
then xmt

ACCEPT another connect on s, or
CLOSE s