Chapter

Overview of TCP/IP

Reference

- Highly Recommended:
  - TCP/IP White Paper by Microsoft

Questions

- How many layers are there in the TCP/IP model? How do they relate to the ISO-OSI model?
- What are some of the TCP/IP related protocols?
- Explain the purpose and function of the above protocols?
- What are ports? Explain the implication of keeping the ports open. How can the ports be protected from hacker attacks?
- Where would one use the UDP protocol in place of the TCP protocol?

Chapter Modules

- TCP/IP Overview and Layers
- TCP/IP Related Protocols
- TCP/IP Ports and Windows API

Module

Overview of TCP/IP

TCP/IP

- A highly standardized protocol used widely on the Internet
- Standards area available in the form of RFC documents
  - Request For Comments (RFC)
- Standards are overseen by the Internet Engineering Task Force (IETF)

Layers of TCP/IP Reference Model

- There are four layers of the TCP/IP reference model (DARPA model as named by the US Government Agency)
  - The ISO-OSI reference model is composed of seven layers
- The next slide shows the mapping of the ISO/OSI model to the TCP/IP model
- Note that the ISO/OSI model is more widely used and accepted but the TCP/IP model is easy to comprehend

ISO-OSI Seven Layer Model Recalled

Layer 7	**Application**
Layer 6	**Presentation**
Layer 5	**Session**
Layer 4	**Transport**
Layer 3	**Network**
Layer 2	**Data Link**
Layer 1	**Physical**

Source: http://starter.sdsu.edu/remote/demo/osi-tcp.html

Comparison of ISO-OSI Model and the DOD (TCP/IP) Model

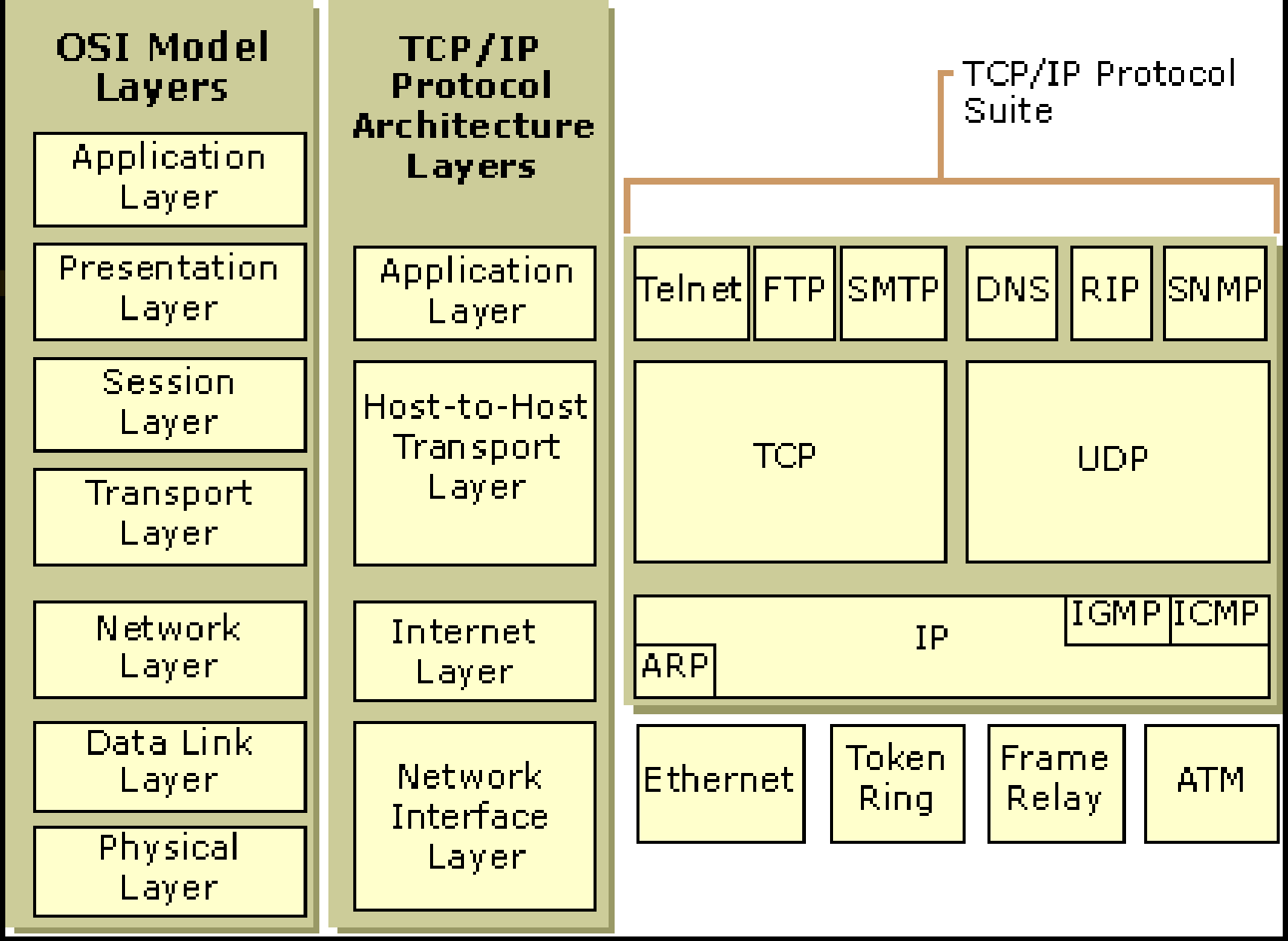
Source: http://starter.sdsu.edu/remote/demo/osi-tcp.html

Application	**Application**
Presentation	
Session	
Transport	**Host-to-Host**
Network	**Internet**
Data Link	**Network Access**
Physical	

Layer Reference to Protocol Recalled

Application	**Application**	**FTP, Telnet, SMTP, HTTP..**
Presentation		
Session		
Transport	**Host-to-Host**	**TCP, UDP**
Network	**Internet**	**IP, ICMP, IGMP**
Data Link	**Network Access**	**Ethernet, Token-Ring ...**
Physical		

Source: http://starter.sdsu.edu/remote/demo/osi-tcp.html



Source: TCP/IP White Paper by Microsoft

TCP/IP Layers

- Network interface layer
- Internet layer
- Host-to-host transport layer
- Application layer

Layer Properties

- In the following slides, the following is described for each layer
  - Layer function
  - Core protocols
  - Relationship to ISO/OSI model

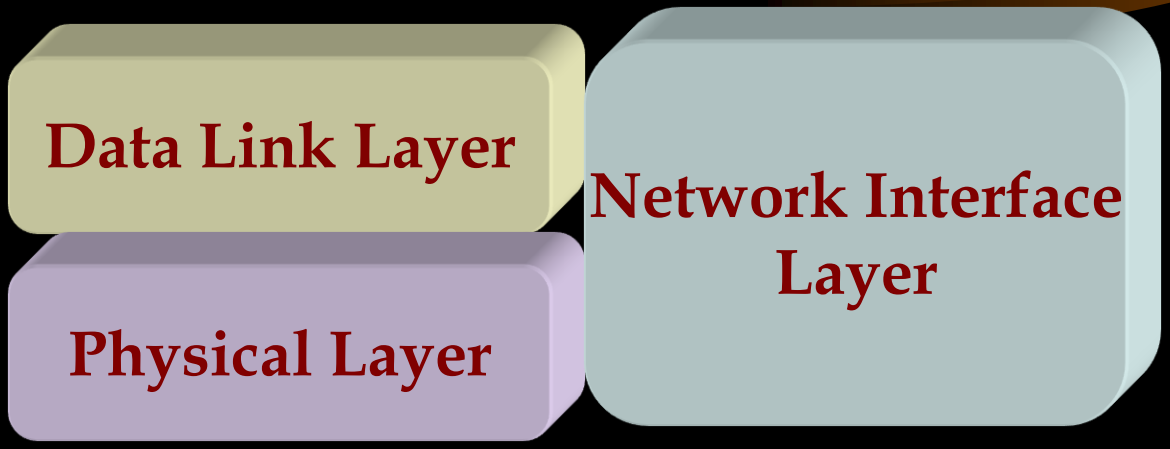
Network Interface Layer

- Responsible for sending and receiving TCP/IP packets on the network medium (physical/Data Link)
- Applicable LAN technologies
  - Ethernet, Token Ring, FDDI etc.
- Applicable WAN technologies
  - X.25 (old), Frame Relay, ATM etc.
- Note that some technologies such as ATM and FDDI may be used at both the WAN and the LAN levels

Some Core Protocols

- IEEE 802.3, IEEE 802.5 and IEEE 802.11 series of protocols

Relationship to OSI Model



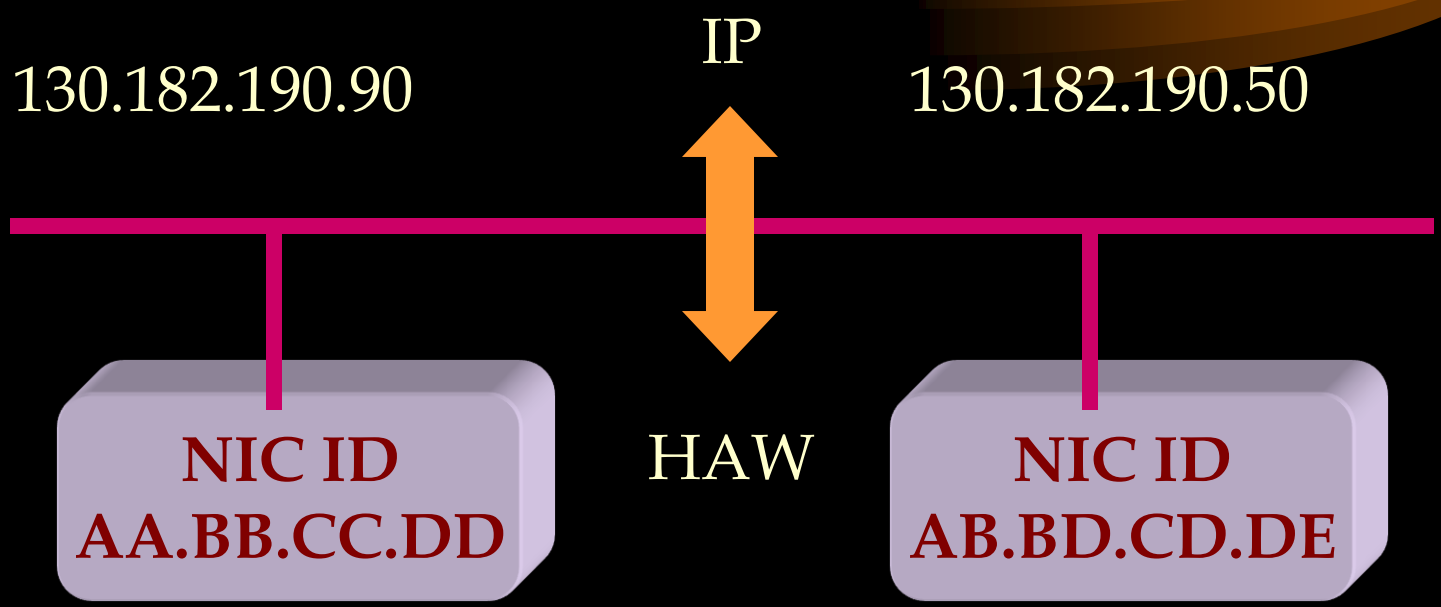
Internet Layer

- Packaging
- Addressing
- Routing

Core Internet Layer Protocols

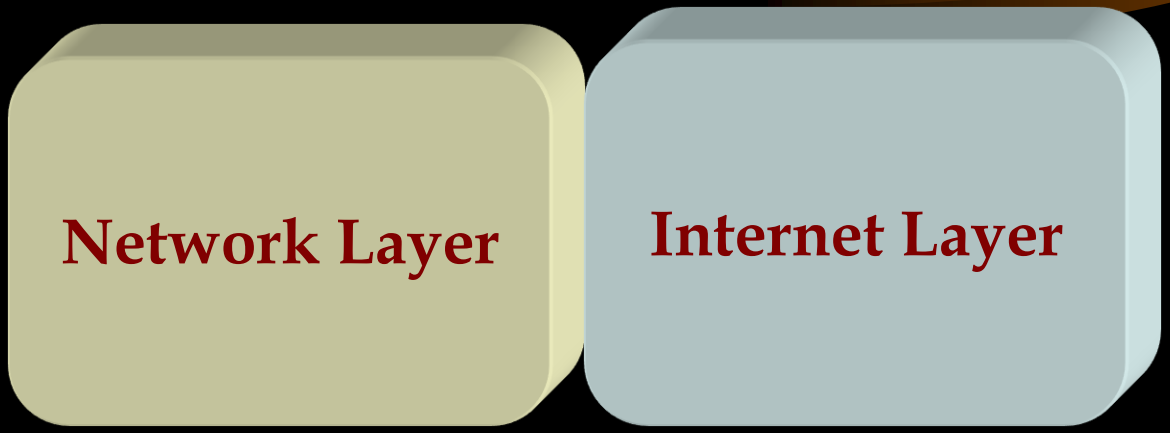
- IP
  - A connectionless unreliable protocol that is part of the TCP/IP protocol suite
- ARP (Address Resolution Protocol)
  - Resolves IP addresses to MAC addresses
- ICMP (Internet Control Message Protocol)
  - Diagnostics and error reporting
- (IGMP) Internet Group Management Protocol
  - Management of group multicast

More on Address Resolution Protocol (ARP)



Resolves, for example, IP addresses to the corresponding MAC level hardware address by for instance broadcasting.

Relationship to ISO Model

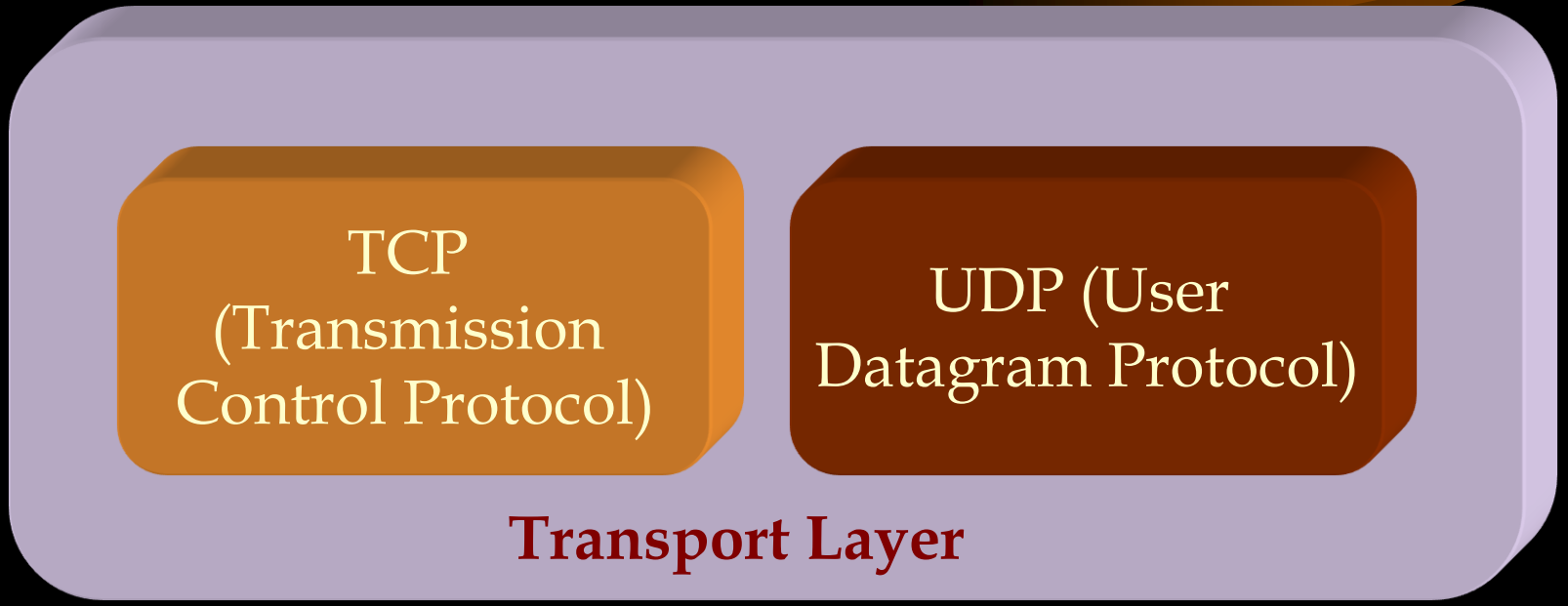


ISO Model **TCP/IP Model**

Transport Layer

- Sequencing and transmission of packets
- Acknowledgment of receipts
- Recovery of packets
- Flow control
- In essence, it engages in host-to-host transportation of data packets and the delivery of them to the application layer

Core Protocols of the Transport Layer



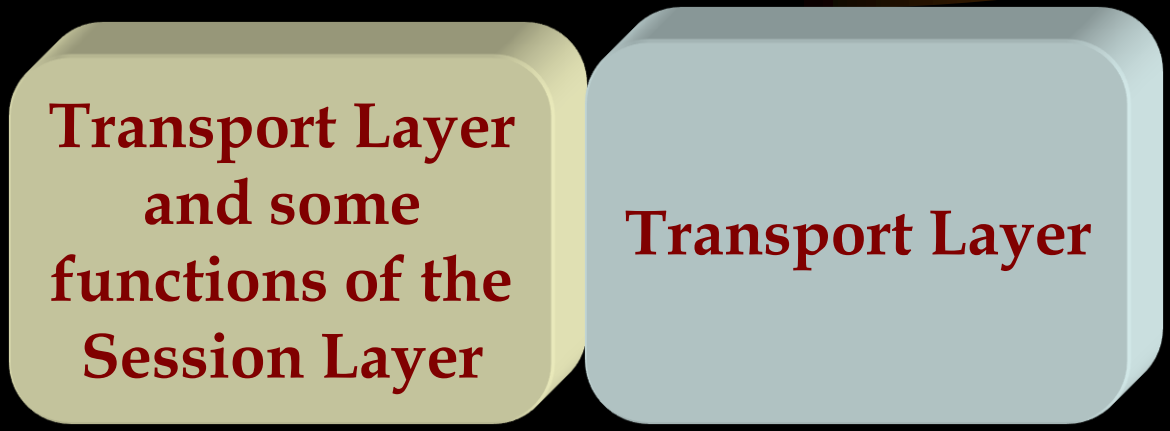
TCP

- Transmission Control Protocol (TCP)
- One-to-one and connection-oriented reliable protocol
- Used in the accurate transmission of large amount of data
- Slower compared to UDP because of additional error checking being performed

UDP

- User Datagram Protocol (UDP)
- One-to-one or one-to-many,connectionless and unreliable protocol
- Used for the transmission of small amount of data
  - Accuracy is not of prime concern
  - The overhead of establishing a TCP connection is not warranted
- Used in video and audio casting
  - Multicasting
  - Broadcasting
- Also used for multimedia transmission
- Faster compared to TCP

Relationship to ISO Model



Application Layer

- Provides applications with the ability to access the services of the other layers
- New protocols and services are always being developed in this category

Some Core Protocols

- HTTP
- FTP
- Telnet
- SMTP
- POP3
- IMAP
- SNMP etc.

End of Module

Module

More on TCP/IP Application Layer Protocols

Some Application Related Application Layer Protocols

- HTTP
- FTP
- SMTP
- Telnet

Some LAN Management/Operation Related Application Layer Protocols

- DNS
- RIP
- SNMP

Hyper Text Transfer Protocol (HTTP)

- Protocol relating to web applications
- Current version of HTTP 1.1 has additional features
  - Upload information to the server
  - Etc.
- Default port number is 80

File Transfer Protocol (FTP)

- File Transfer Protocol
  - Used for downloading from most MP3 sites, for example
- Designed for faster file transfer over the Internet compared to using the HTTP protocol
- FTP sites can be configured alongside a web site to support FTP file transfer
- FTP default ports are 20 and 21

HTTP and FTP

- File transfer under FTP is faster than file transfer under HTTP
- Choose an FTP site if there is one for downloading files etc.

Simple Mail Transfer Protocol (SMTP)

- Governs the transmission of mail messages and attachments
- SMTP is used in the case of outgoing messages
- More powerful protocols such as POP3 and IMAP4 are needed and available to manage incoming messages

POP3/IMAP4

- Used for incoming mail
- POP3 is the older protocol
- IMAP4 is the more advanced protocol

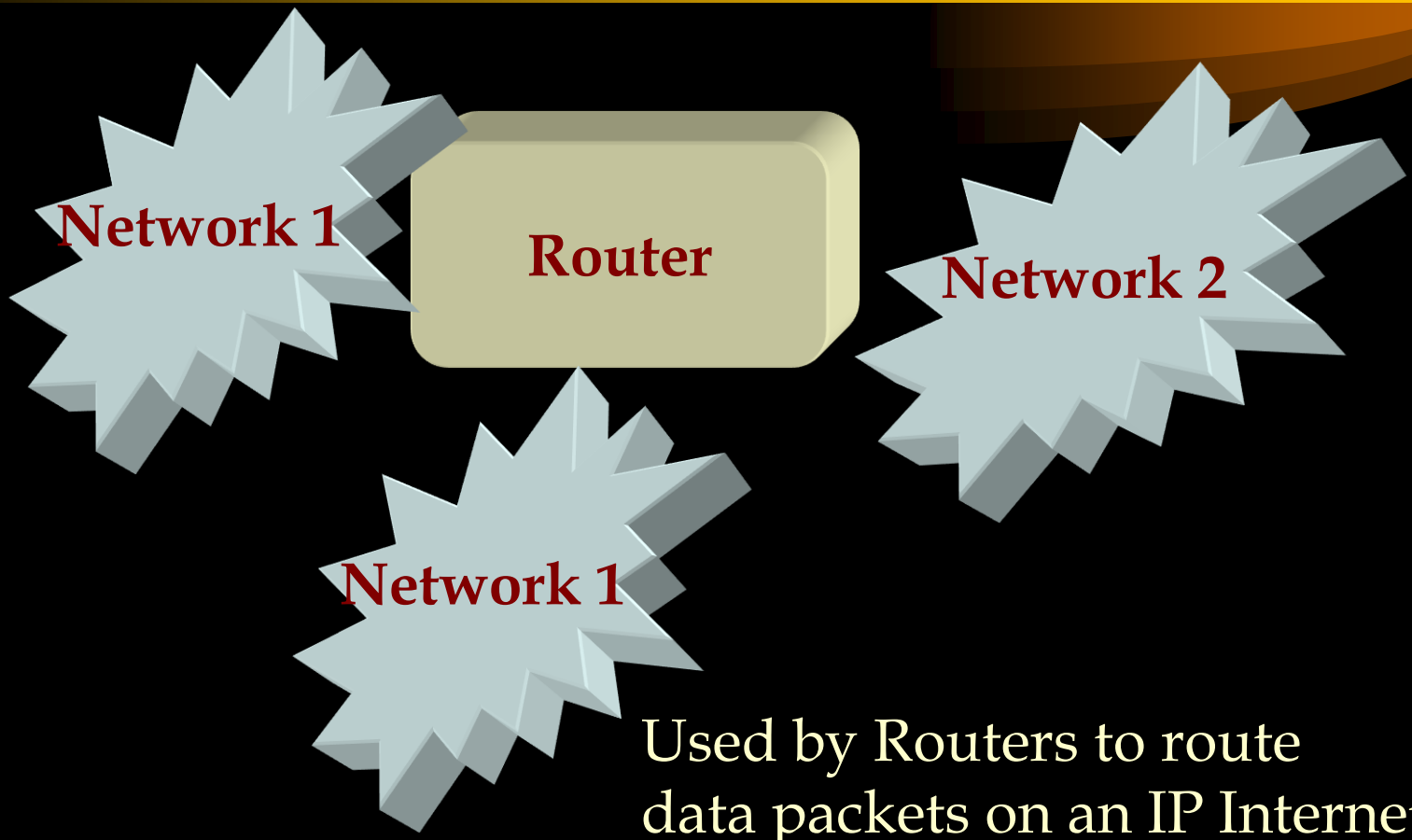
Telnet

- Supports terminal emulation or host sessions
- For example, Telnet can be used for accessing a Unix machine and emulating a terminal attached to the Unix computer

Domain Name System (DNS)

Resolves domain names to IP addresses
and vice versa

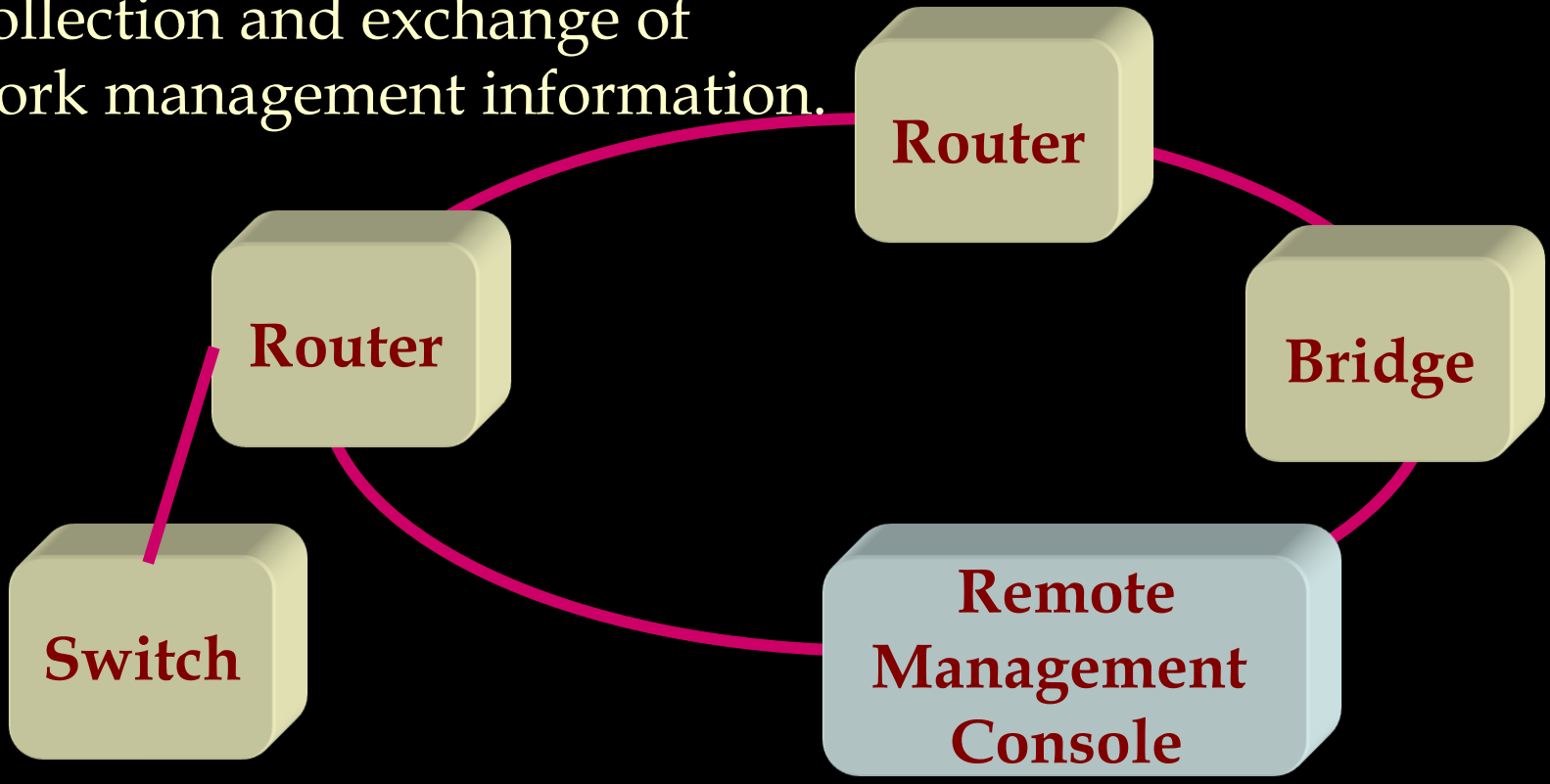
Routing Information Protocol (RIP)



Used by Routers to route data packets on an IP Internet.

Simple Network Management Protocol (SNMP)

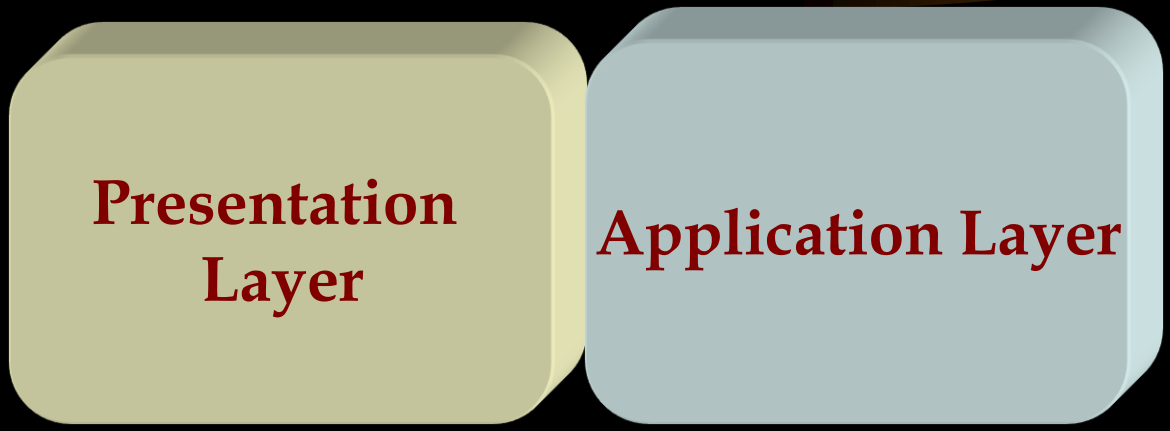
Facilitates the management of SNMP compliant routers, bridges, switches etc. by enabling the collection and exchange of network management information.



SNMP

- Used by network management utilities to manage network devices
- For example, a manageable hub that support SNMP can be managed from a remote location using a SNMP based LAN management software

Relationship to ISO Model



End of Module

Module

TCP/IP Client and Windows API

Ports

- TCP requires port numbers on the host and destination for communication
  - Different port numbers are assigned to different protocols by default
    - HTTP 80, Telnet 23, FTP 20/21, RPC 135, NetBIOS 139 etc.
- Standard port numbers have been assigned by the Internet Assigned Number Authority (IANA)

Using Port Numbers on Addresses

- Standard access for web browsing
  - Ganesan.calstatela.edu
  - Default port of 80 is used in this case
- Non-standard access
  - http://ganesan.calstatela.edu:5002
  - The port number 5002 is used in this case to host the above web server

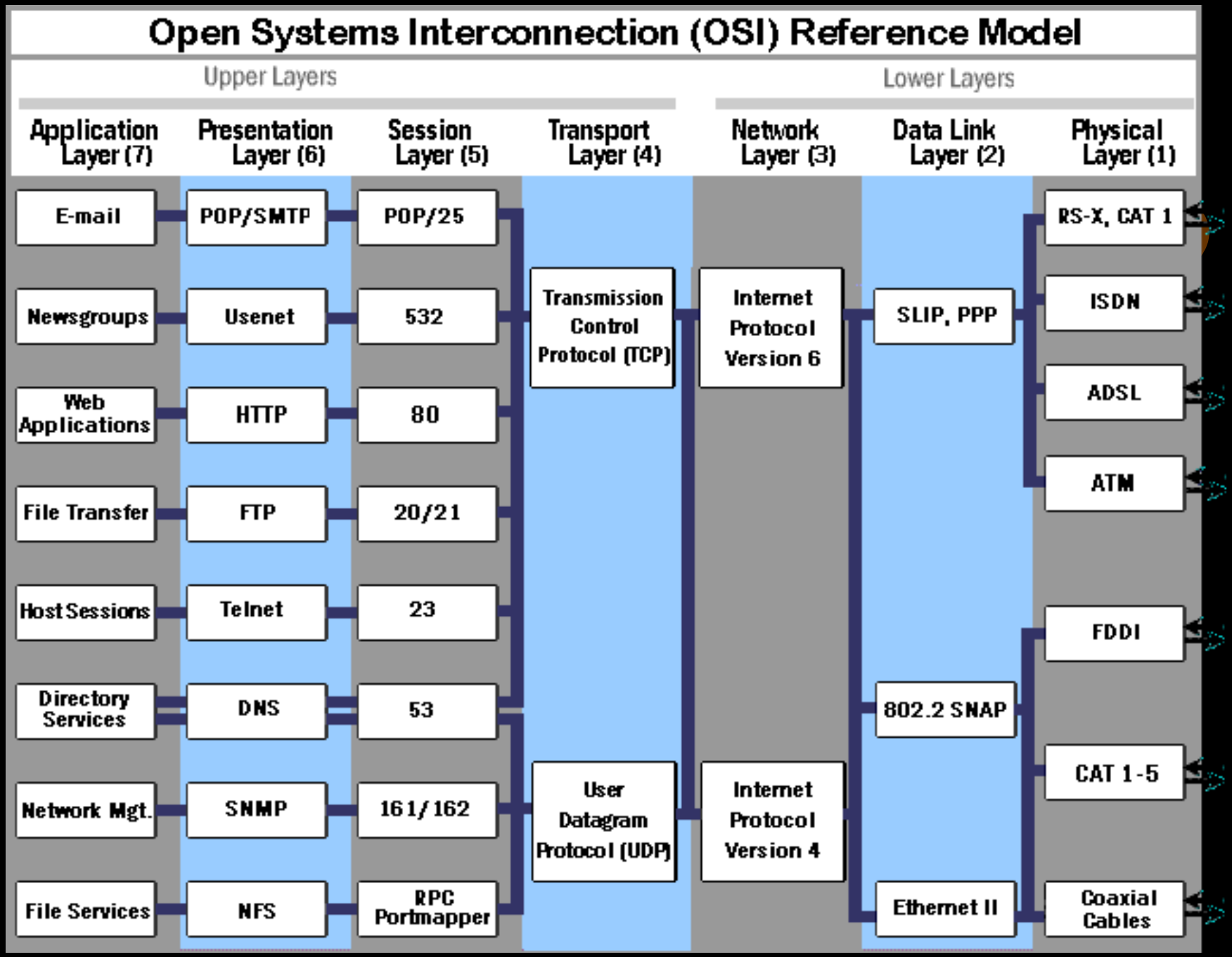
Sample TCP Port Numbers

20	FTP Data Channel
21	FTP Control Channel
23	Telnet
80	HTTP on WWW
135	RPC
139	NetBIOS Session Services

Note: There are port numbers applicable to UDP as well.

More Ports Information

- http://www.networkice.com/advice/exploits/ports


Open Systems Interconnection (OSI) Reference Model
Upper Layers
Lower Layers
Application Layer (7)
Presentation Layer (6)
Session Layer (5)
Transport Layer (4)
Network Layer (3)
Data Link Layer (2)
Physical Layer (1)
E-mail
POP/SMTP
POP/25
Newsgroups
Usenet
532
Web Applications
HTTP
80
File Transfer
FTP
20/21
Host Sessions
Telnet
23
Directory Services
DNS
53
Network Mgt.
SNMP
161/162
File Services
NFS
RPC Portmapper
Transmission Control Protocol (TCP)
User Datagram Protocol (UDP)
Internet Protocol Version 6
Internet Protocol Version 4
SLIP, PPP
802.2 SNAP
Ethernet II
RS-X, CAT 1
ISDN
ADSL
ATM
FDDI
CAT 1-5
Coaxial Cables

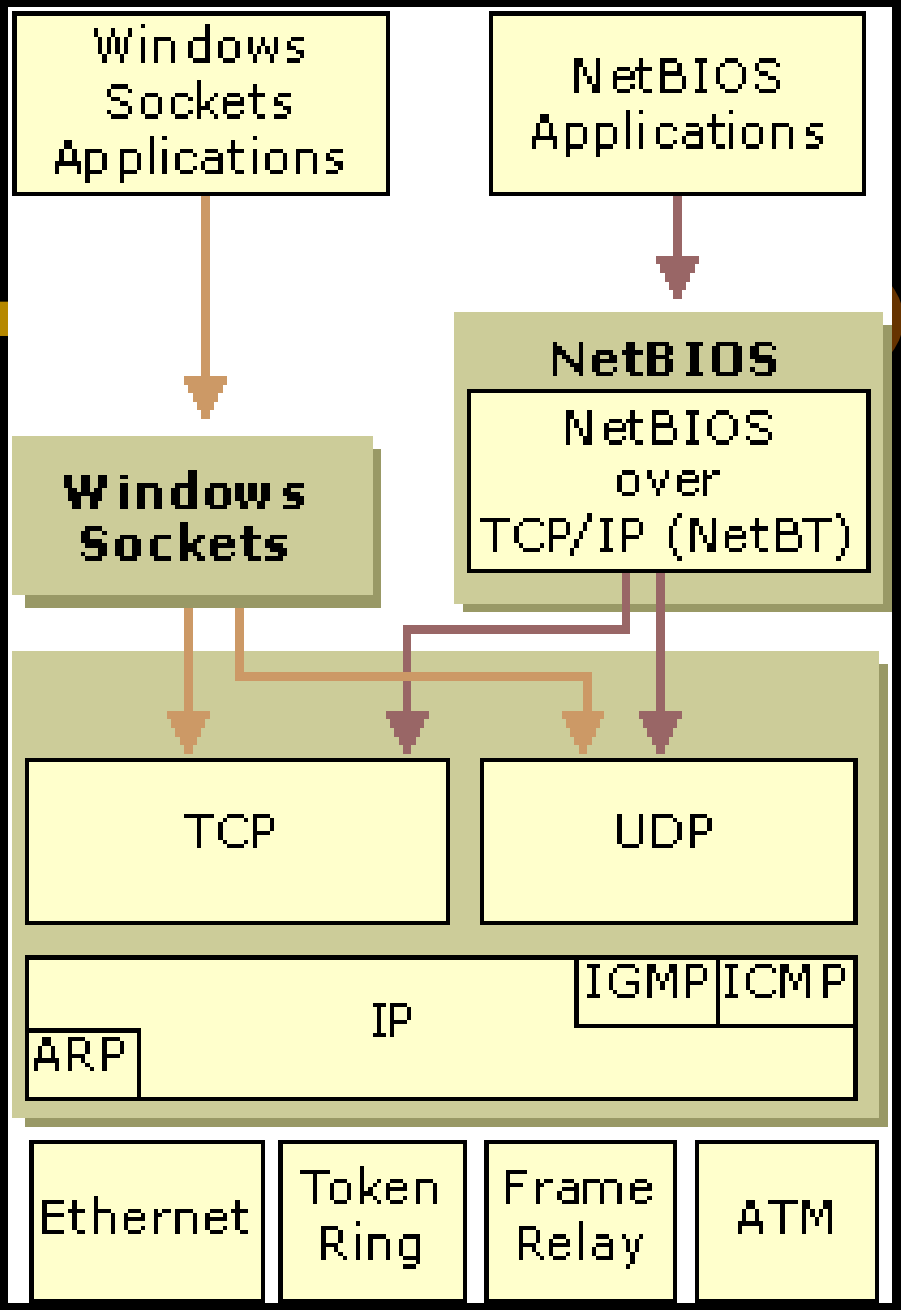
Port Scanning

- To test the security of a computer, its ports can be scanned and the port status can be displayed
- Access Shieldup in www.grc.com to scan your computers port
- Ports
  - Open is insecure
  - Closed is somewhat secure
  - Stealth is most secure

TCP/IP Application Interface

- Applications require an Application Programming Interface (API) to use the services of TCP/IP
- API is a standardized interface between the applications and the TCP/IP services
- Windows Sockets interface and NetBIOS interface are two of the prominent examples of Windows API

Windows API with TCP/IP



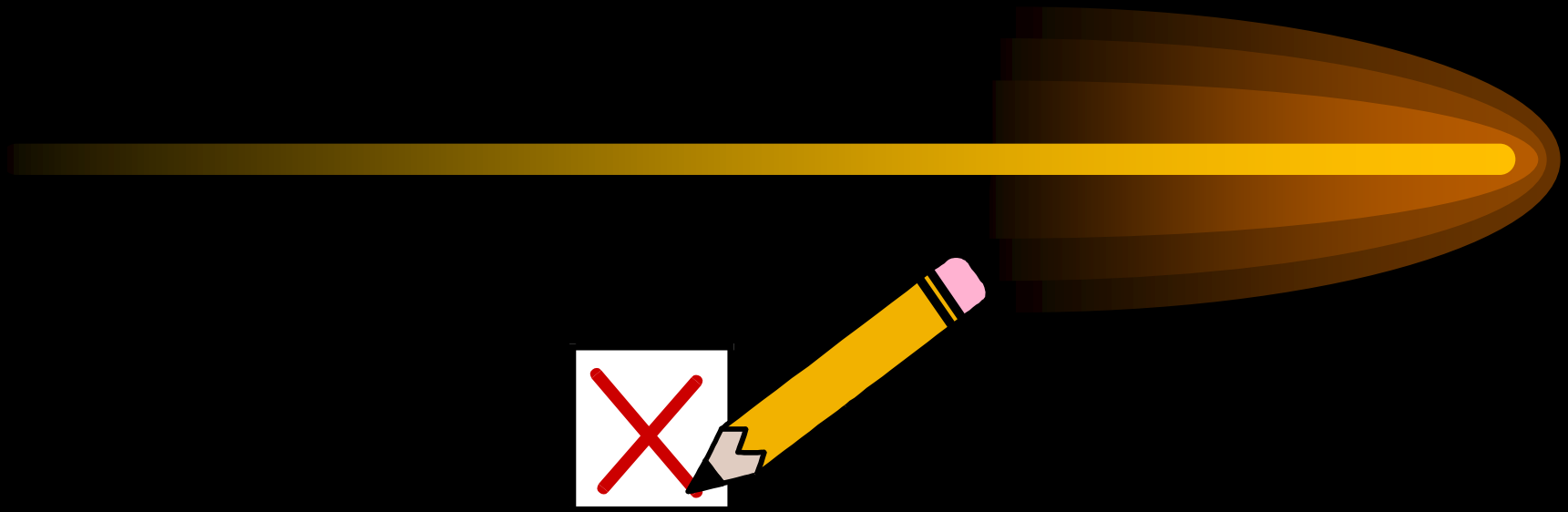
Windows APIs

- Windows socket
  - Protocol, IP Address and Port number
- NetBIOS interface
  - NetBIOS over TCP/IP (NetBT)
  - Supports NetBIOS Name Management, NetBIOS Datagram and NetBIOS sessions
  - If support is required for older NetBIOS applications, then NetBIOS over TCP/IP must be invoked in the TCP/IP properties tab

Other References

- TCP/IP, MCSE Examcram, Tittel Ed., Hudson Kurt and Stewart Michael J., The Coriolis Group, 1998.

End of Module



End of Module

END OF CHAPTER