PROTECTING INFORMATION ASSETS

UNIT 4B

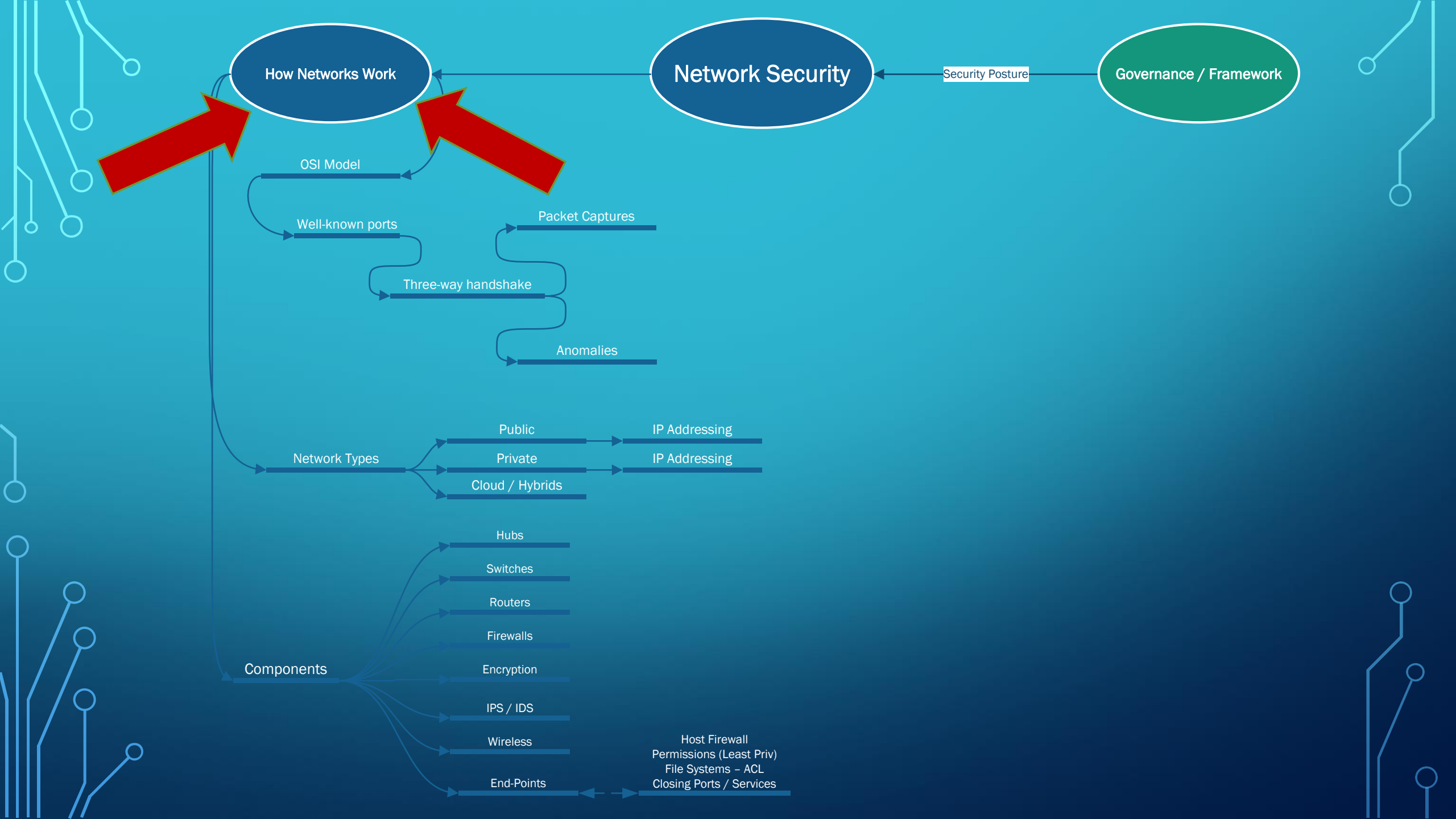
NETWORK SECURITY

AGENDA

- Network security definition
- Models and protocols
- Switched environments
- Access control lists
- Firewalls
- Intrusion detection and prevention systems

SIMPLE DEFINITION OF NETWORK SECURITY

The purpose of network security is to protect the network of information systems from unauthorized access and misuse


How Networks Work
Network Security
Security Posture
Governance / Framework
OSI Model
Well-known ports
Packet Captures
Three-way handshake
Anomalies
Network Types
Public
IP Addressing
Private
IP Addressing
Cloud / Hybrids
Components
Hubs
Switches
Routers
Firewalls
Encryption
IPS / IDS
Wireless
End-Points
Host Firewall
Permissions (Least Priv)
File Systems – ACL
Closing Ports / Services

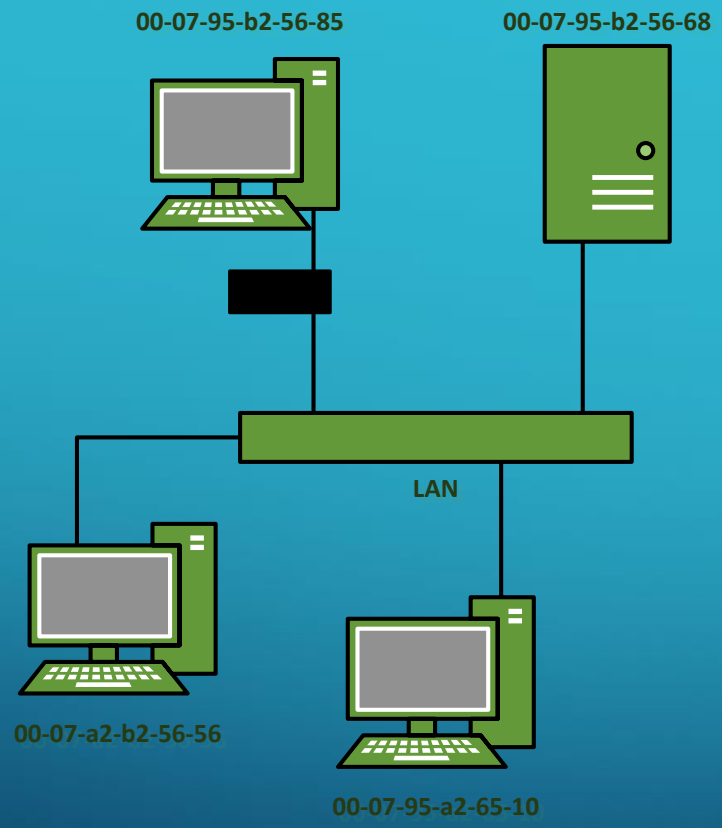
MOVING DATA

Data Packets

Addressing

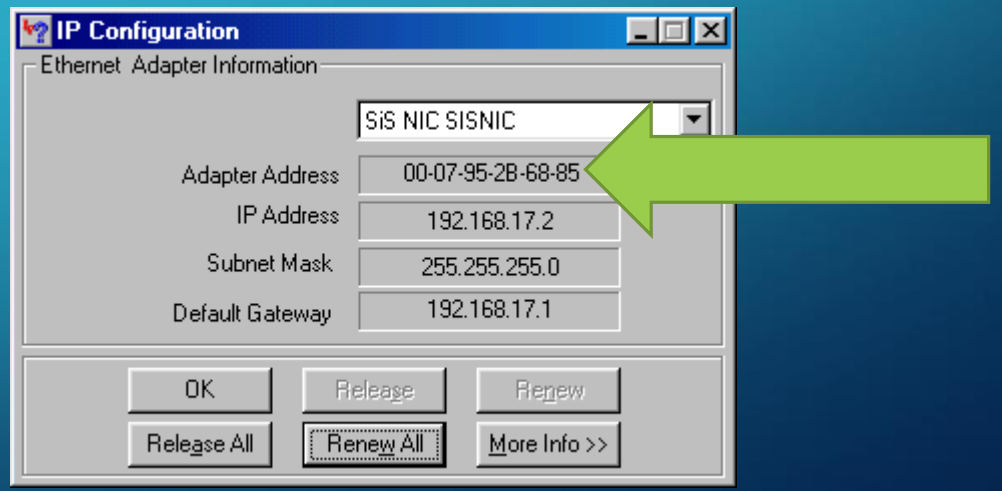
Delivery Method

BASIC NETWORKING - MAC ADDRESSES



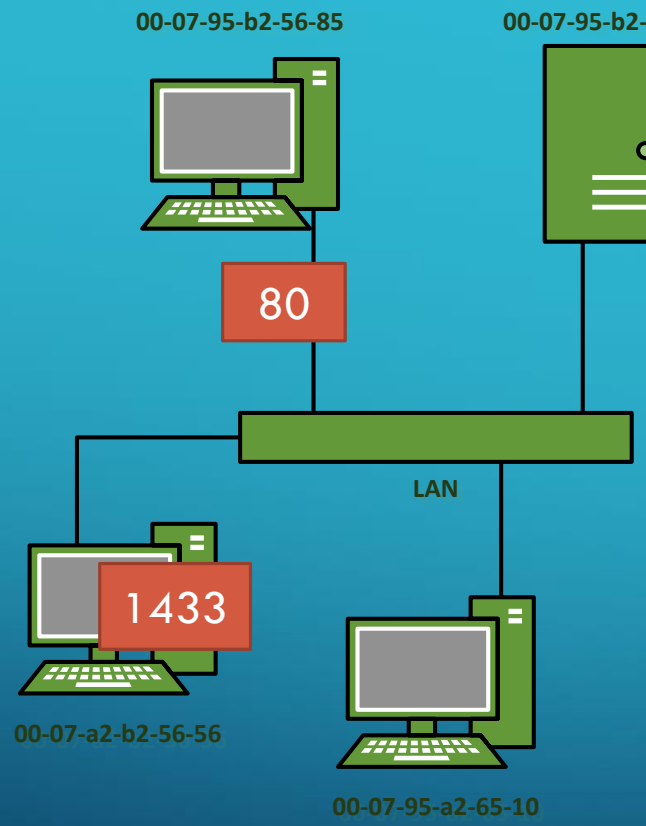
A **M**edia **A**ccess **C**ontrol address (**MAC address**) is a unique identifier assigned to network interfaces for communications on the physical network segment.

The **A**ddress **R**esolution **P**rotocol (**ARP**) is a telecommunication protocol used for discovering the MAC Addresses of known **I**nternet **P**rotocol (**IP**) addresses



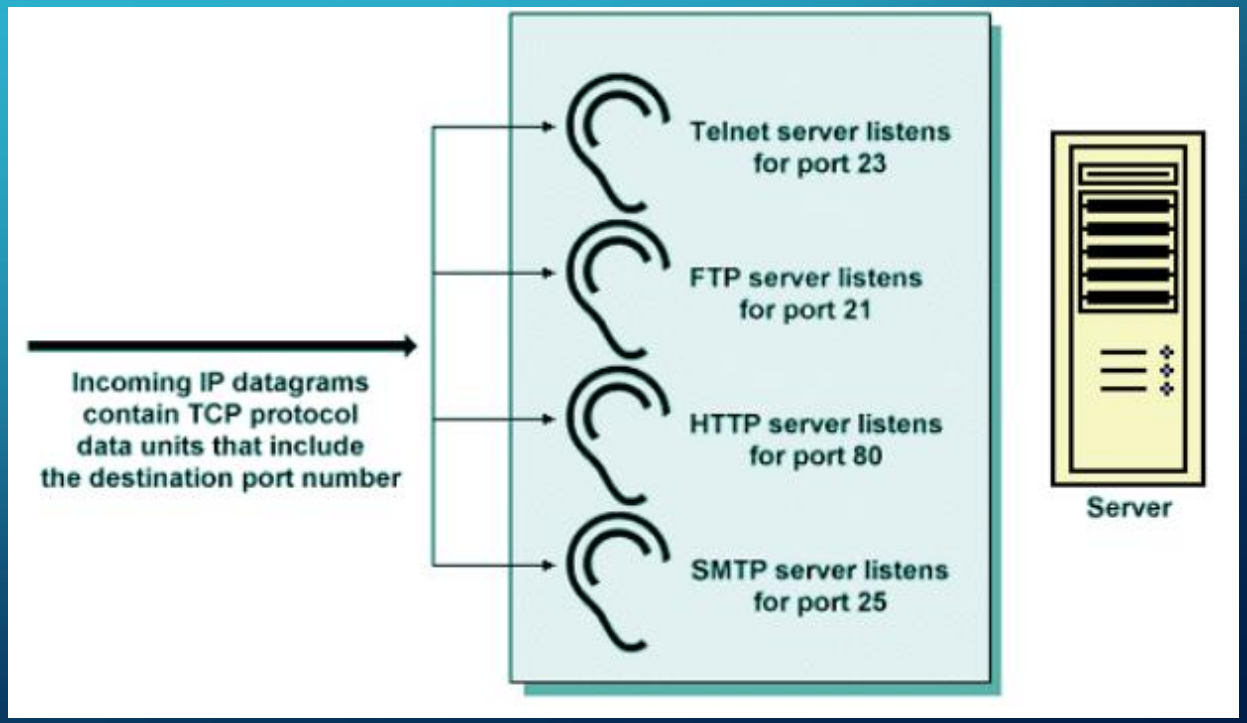
ARP spoofing is a type of attack in which a malicious actor sends falsified **ARP** (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network.

BASIC NETWORKING – PORTS *MACHINES LISTEN TO FOR DATA TRAFFIC*

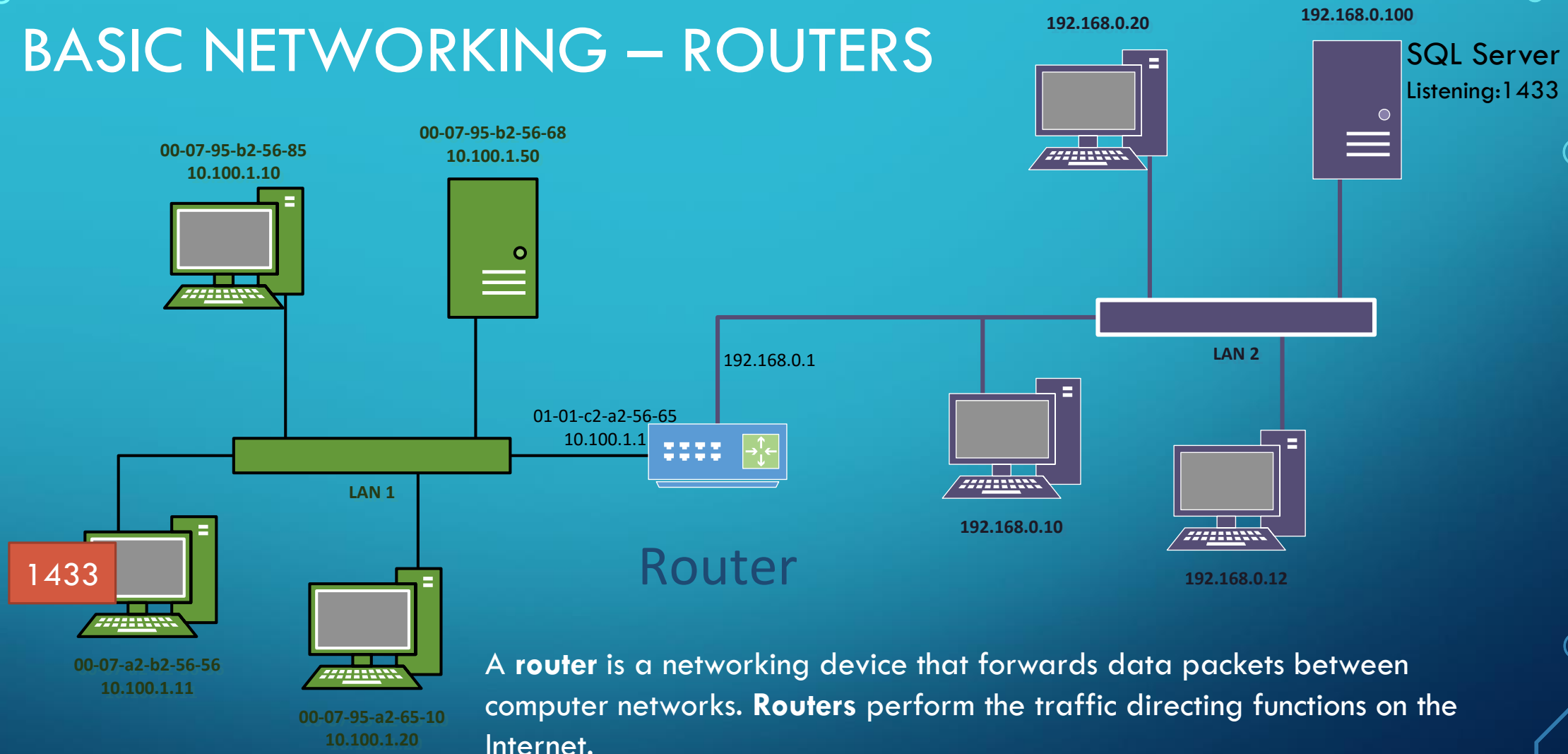


Port 80: Web
Port 443: Secure web
Port 1433: SQL Database
Port 1521: Oracle Database

Scan networks for these ports to identify which servers are offering which services



BASIC NETWORKING – ROUTERS



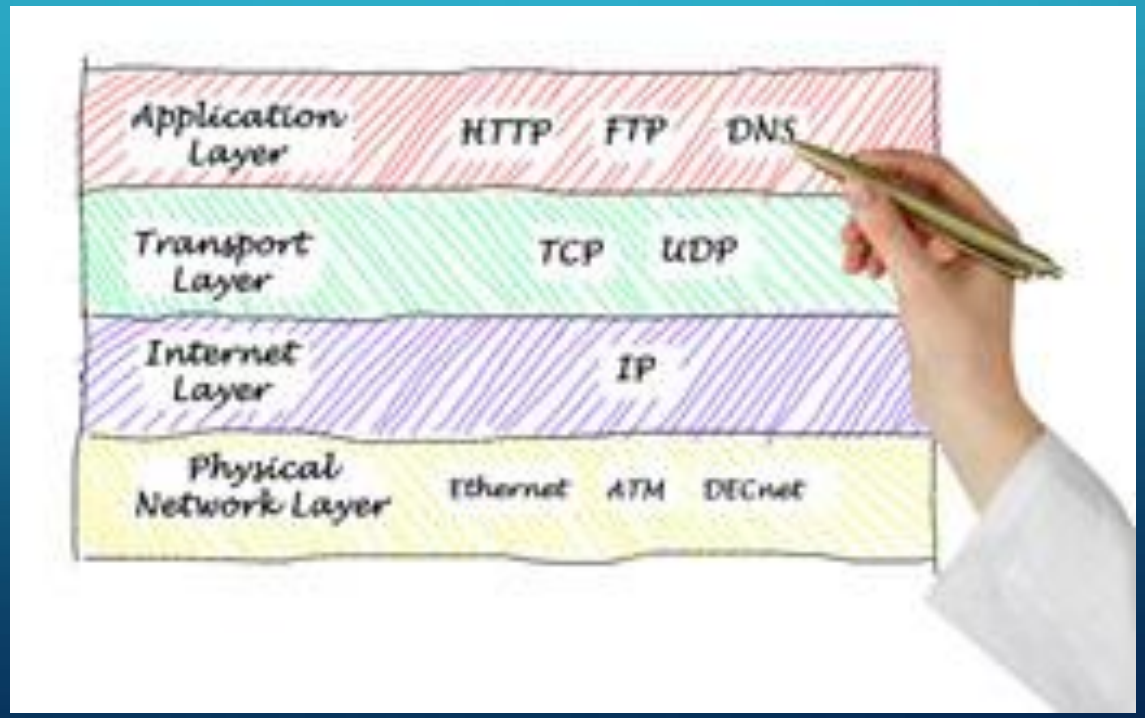
A **router** is a networking device that forwards data packets between computer networks. **Routers** perform the traffic directing functions on the Internet.

A data packet is typically forwarded from one **router** to another through the networks that constitute the internetwork until it reaches its destination node.

MODELS AND PROTOCOLS

OSI MODEL

- Developed by ISO – International Organization of Standardization
- Layered, each level sends to the layer above or below.

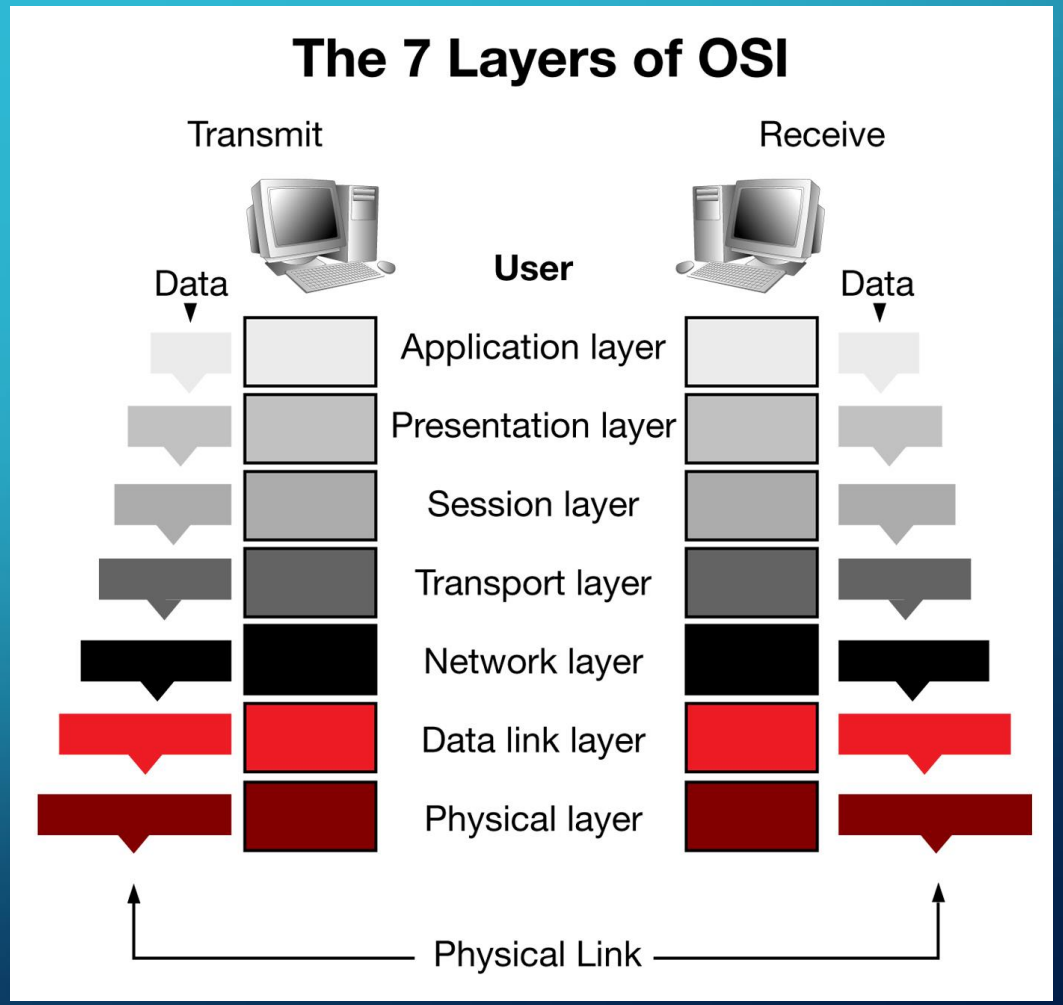


BENEFITS OF OSI MODEL

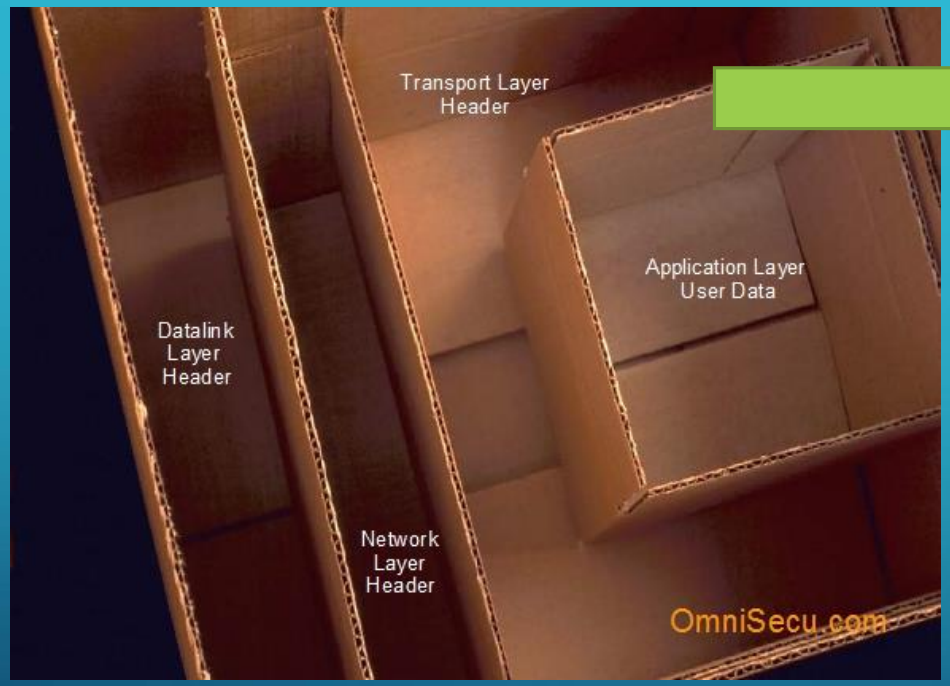
- Common Language
- Acceptable Behavior
- Protocols: set of rules that dictates how computers communicate over networks
- TCP/IP is a suite of protocols - de facto standard of the internet

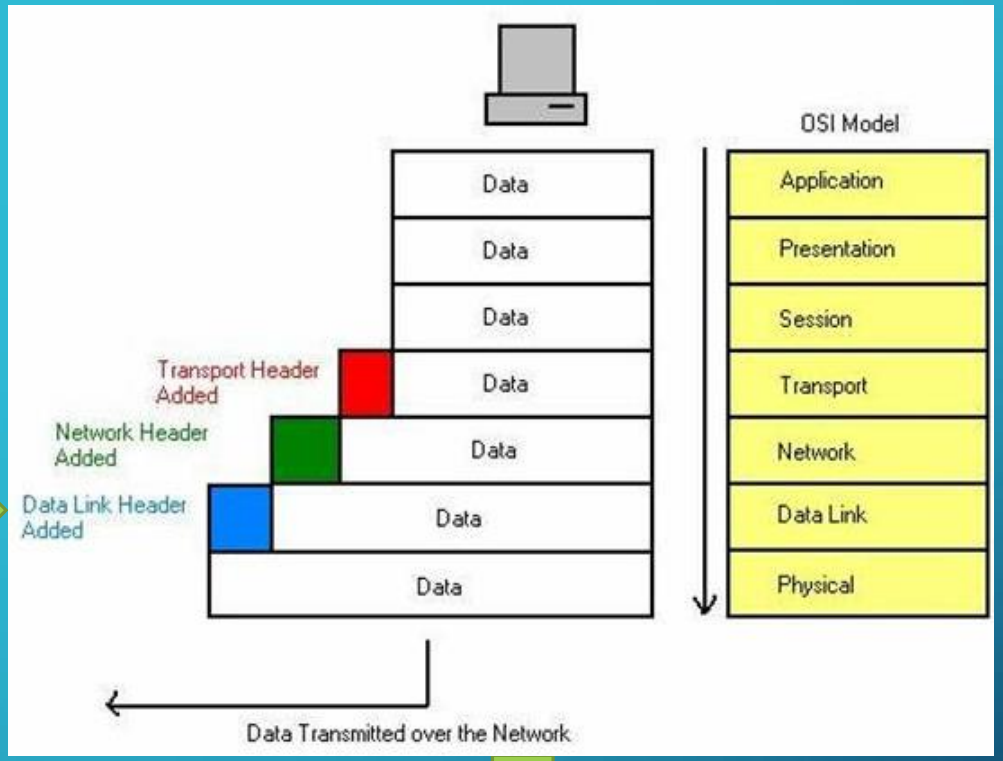
DATA FLOW – OSI MODEL

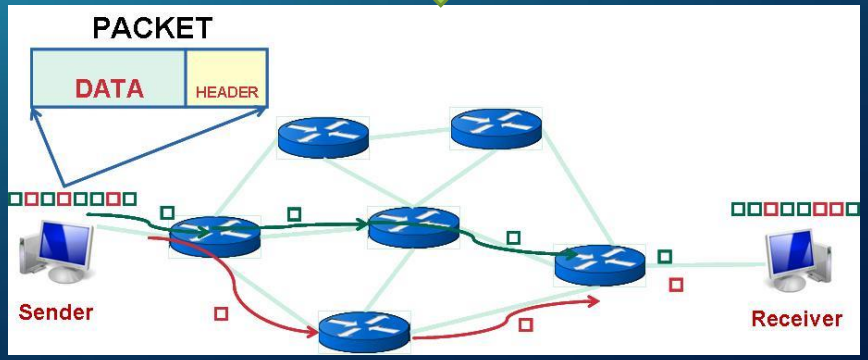
- Data encapsulation occurs as data travels down the stack.
- Data DE-capsulation = stripping off layers as the data travels up the stack.



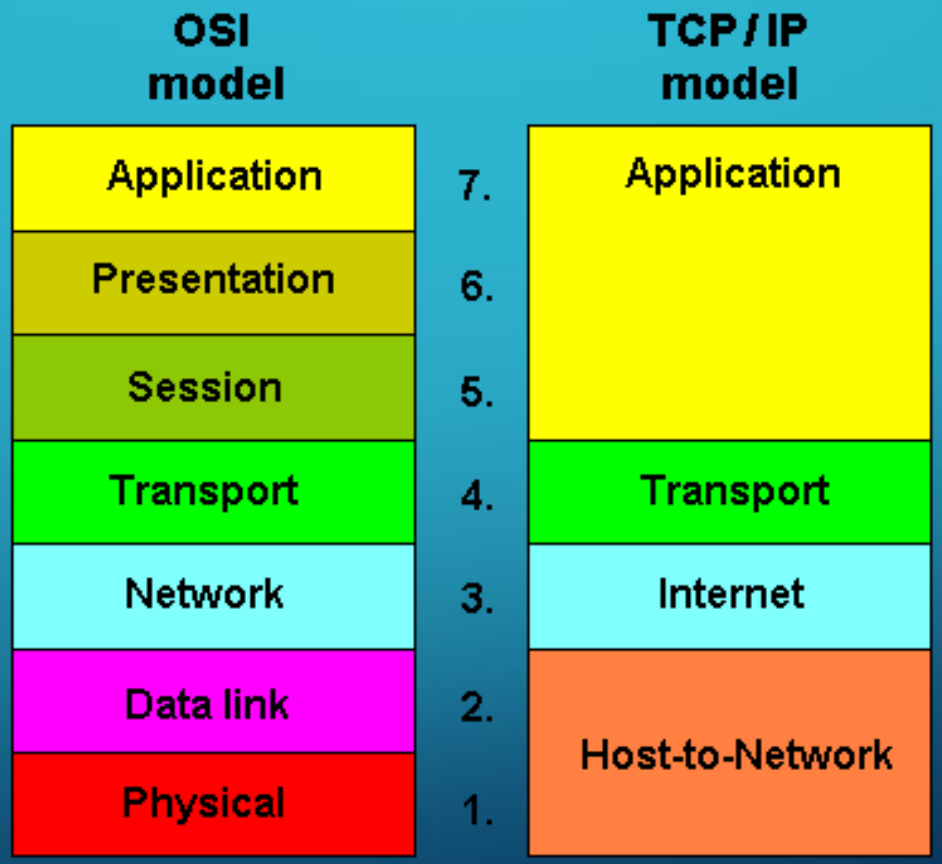
PACKETS


Transport Layer Header
Application Layer User Data
Datalink Layer Header
Network Layer Header
OmniSecu.com

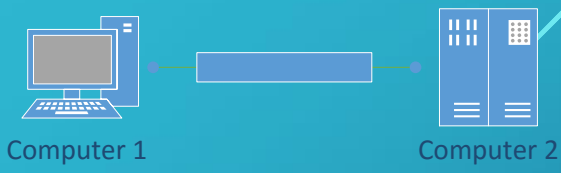

OSI Model
Data
Data
Data
Data
Data
Data
Data
Transport Header Added
Network Header Added
Data Link Header Added
Application
Presentation
Session
Transport
Network
Data Link
Physical
Data Transmitted over the Network


PACKET
DATA
HEADER
Sender
Receiver

TWO MODELS

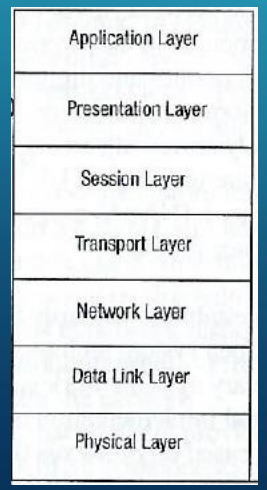

OSI model
TCP/IP model
Application
Presentation
Session
Transport
Network
Data link
Physical
7.
6.
5.
4.
3.
2.
1.
Application
Transport
Internet
Host-to-Network

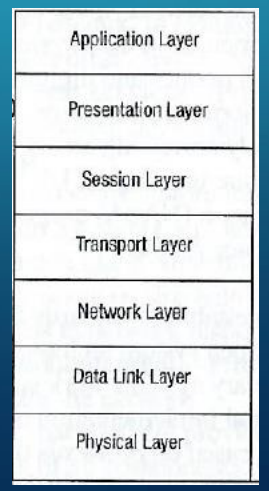
OPEN SYSTEMS INTERCONNECTION(OSI) REFERENCE MODEL – ISO STANDARD 7498-1

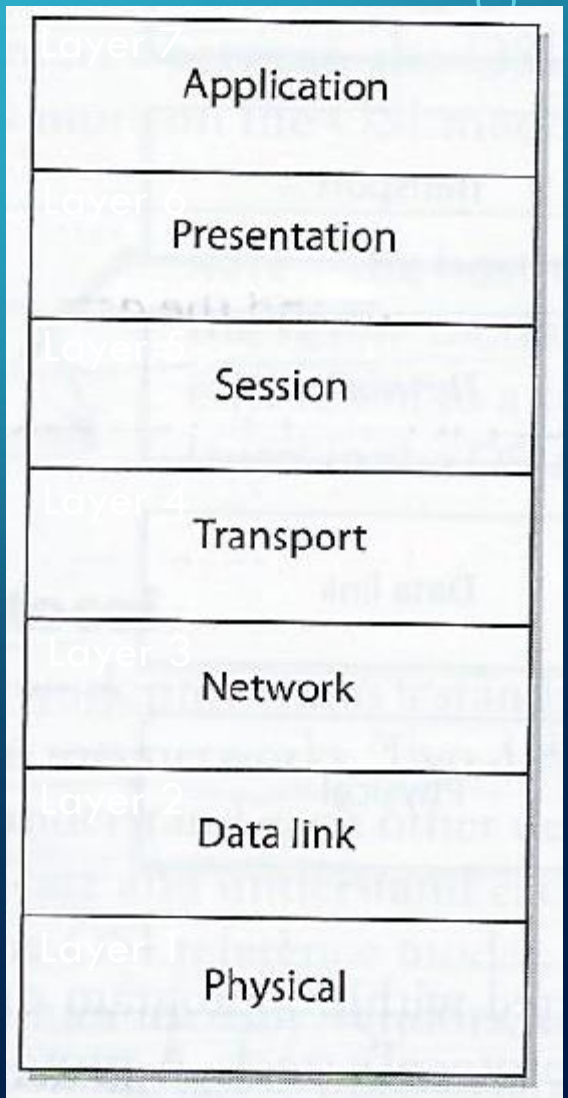


OSI Model

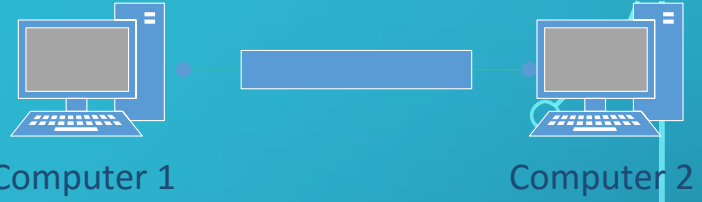
- Guidelines used by vendors, engineers, developers to enable their systems to interoperate
- Layers networking tasks, protocols and services into different layers
- Each layer has its own responsibilities regarding how two computers communicate over a network



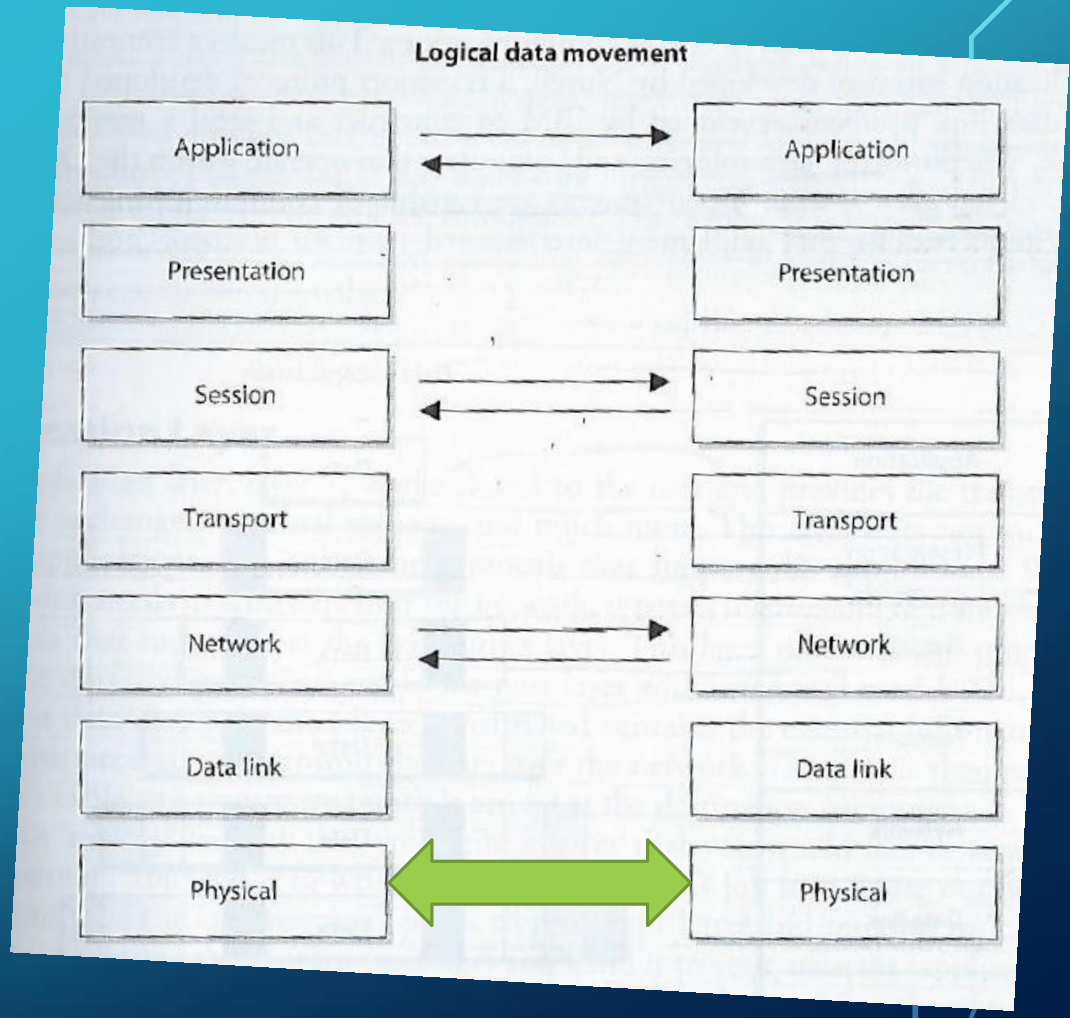




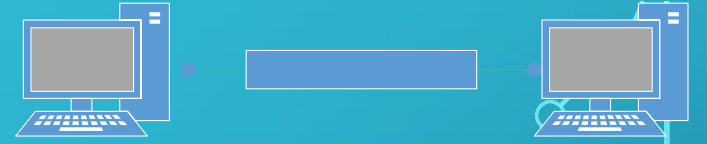
COMPUTERS COMMUNICATE VIA NETWORK



- Protocols function in specific OSI layers
- Each protocol on one computer communicates with the same corresponding protocol within the same OSI layer on another computer
- Via logical channels
- At the physical layer electronic/light signals are passed from one computer over a wire/fiber optic cable to the other computer



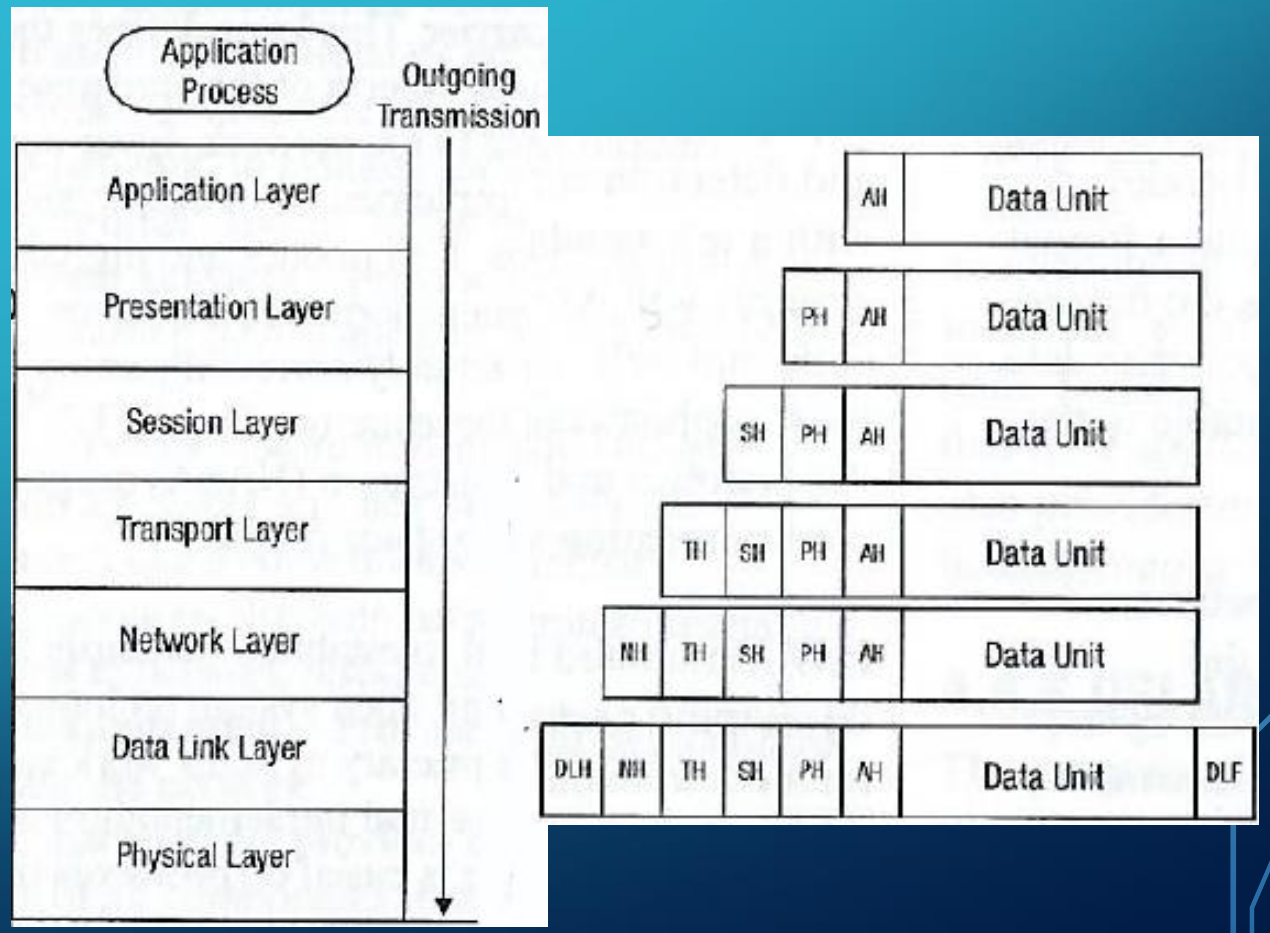
ENCAPSULATION



Process by which a protocol is used to enable two computers to communicate with each other within a specific OSI layer on each

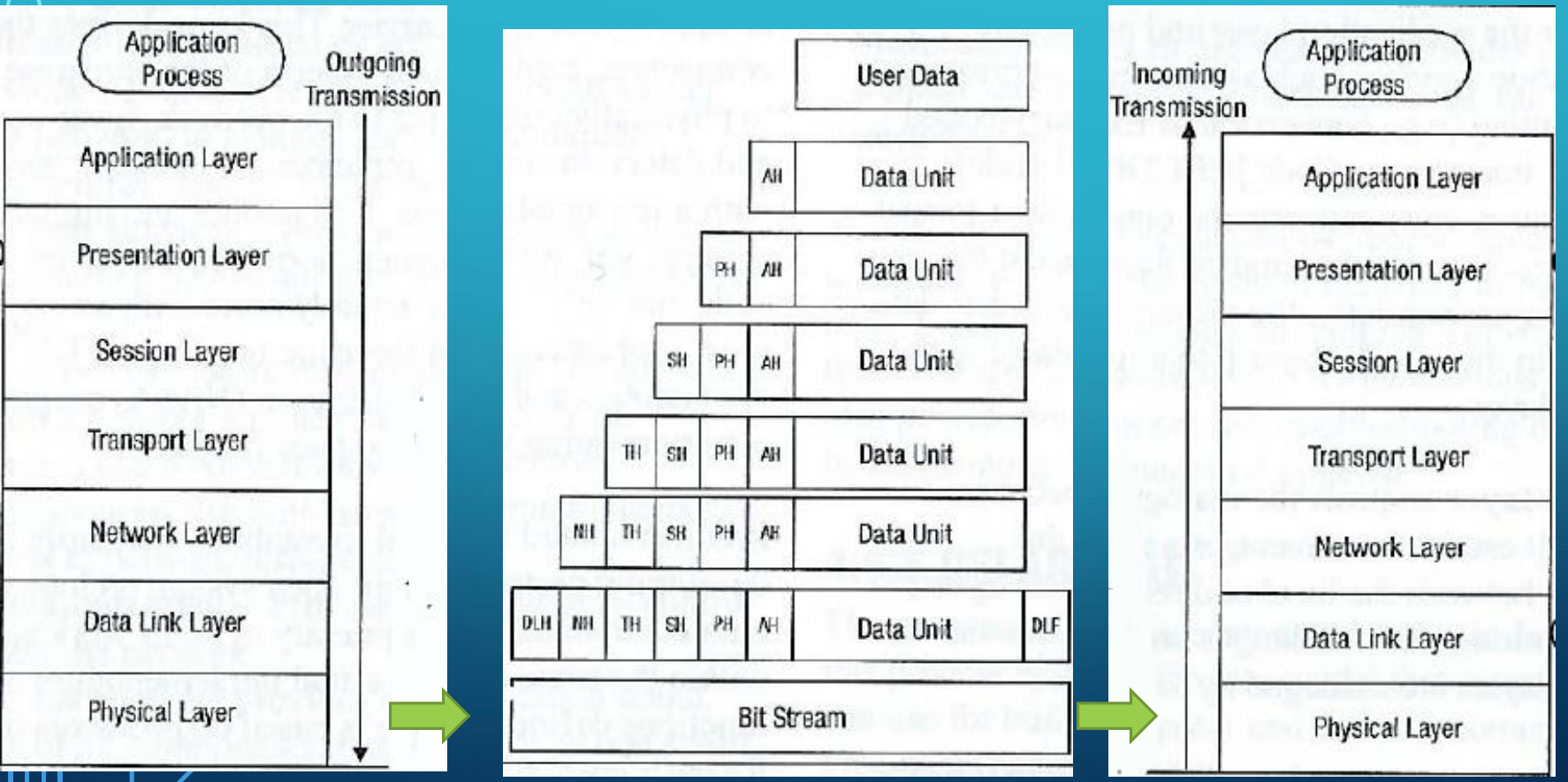
1. A message is constructed within a program on one computer and passed down through the network protocol's stack…

   A protocol at each layer adds its own information to the message, and the message grows in size as it does down the protocol stack



ENCAPSULATION

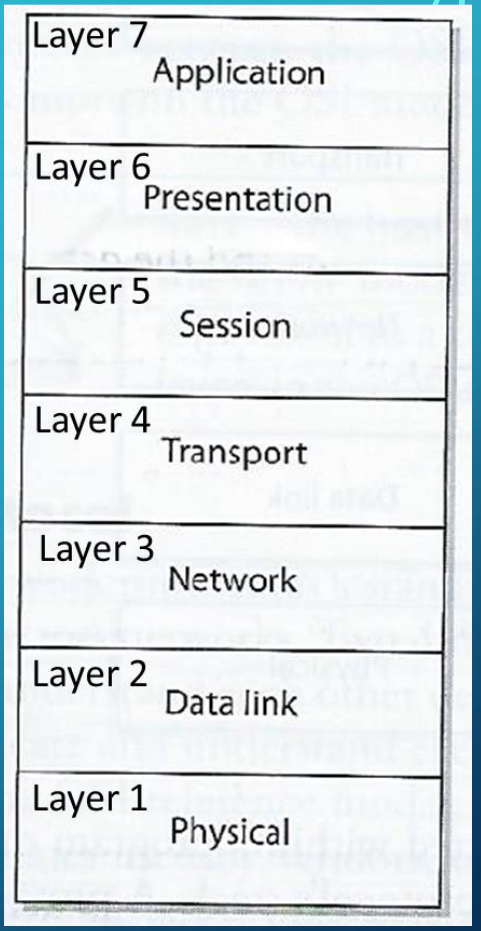
2. At the physical layer of the network the message is passed by the sending computer as bits via electronic or light pulses (on/off) across the network to the destination computer



3. At the destination computer the encapsulation is reversed taking the message apart via the protocols of each layer until the data is ready for the application processing

OSI LAYERS

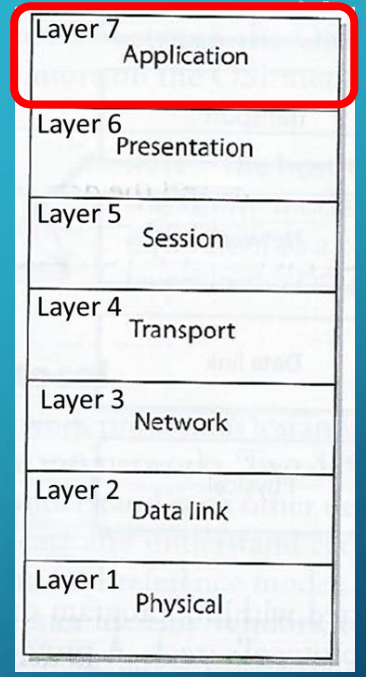
- Implementing international standard protocols and interfaces makes them part of an "open system" in which different vendor's technologies can communicate with one another
- Being part of an open system of common protocols makes the different OSI layers vulnerable and targets of attack



A network can be:

1. Used as a channel of an attack – i.e. as a resource for an attacker
   - For example: *Attacker sends a virus via a network channel from one system to another*
2. The target of an attack
   - For example: *Attacker carries out a denial-of-service (DoS) attack which sends a large volume of badly formed protocol message traffic over a network link to bog it down*

LAYER 7: APPLICATION LAYER



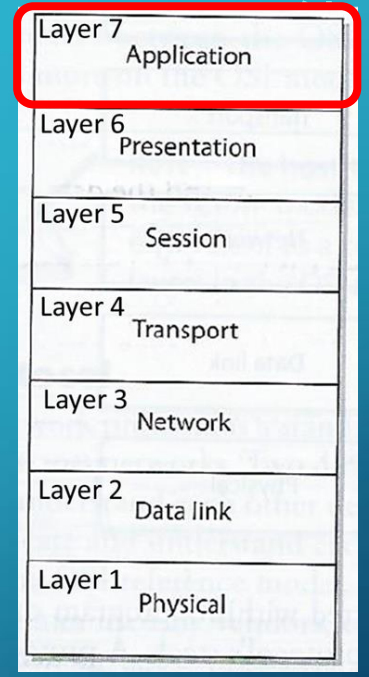
Works closest to the user – providing protocols that support the user's applications

For example: File transmissions, message exchanges, terminal sessions…

- When an application needs to send data over the network, it uses application layer protocols to prepare and communicate its instructions and data

Application layer properly formats the data and sends it down to the presentation layer… (after data makes it through all the layers it has all the information needed to transmit it over the network)

LAYER 7: APPLICATION LAYER

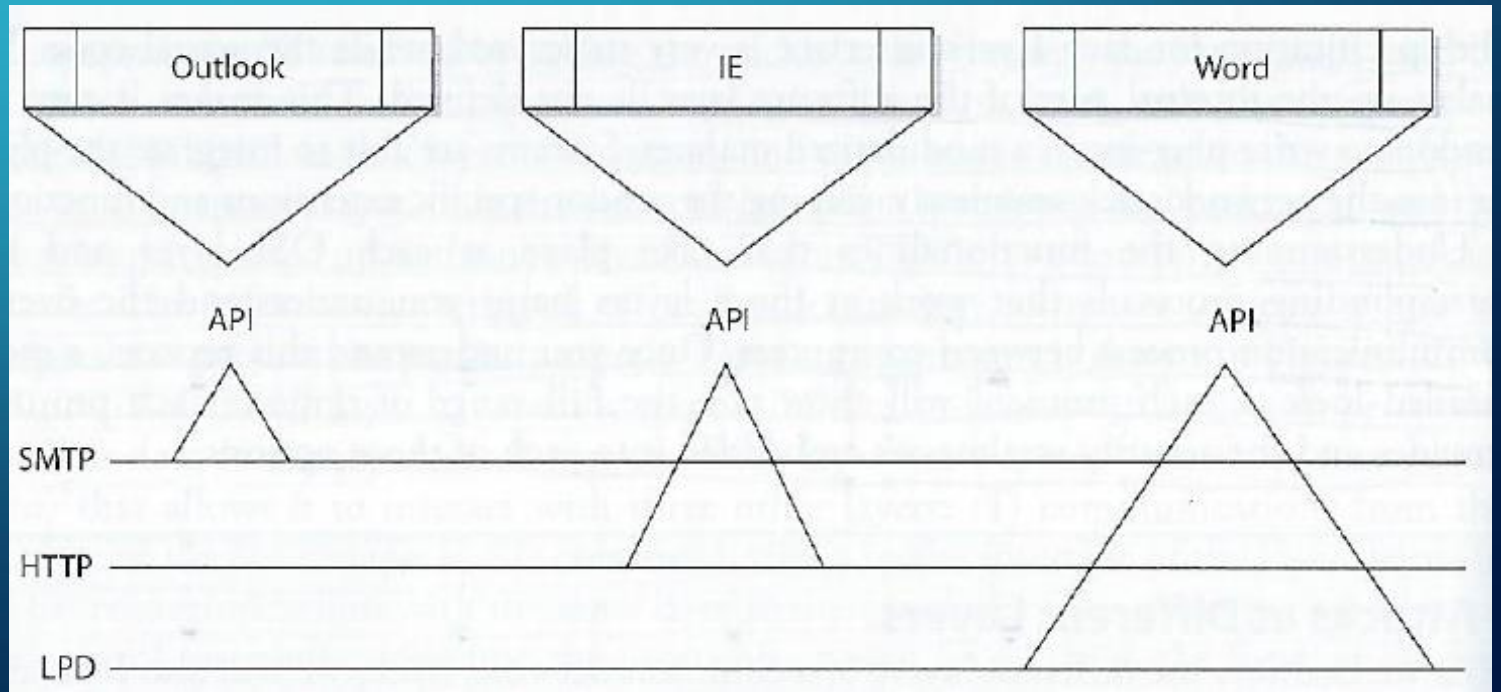


Protocols functioning at this layer communicate include:

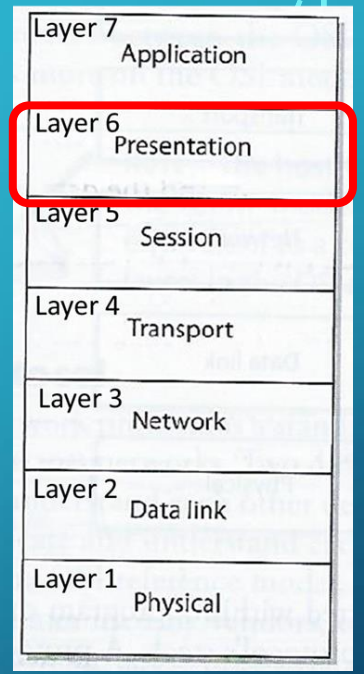
- SMTP – Simple Mail Transfer Protocol
- HTTP – Hyper Text Transfer Protocol
- DNS – Domain Name System
- IRC – Internet Relay Chat
- LPD – Line Printer Daemon

Applications communicate with Layer 7 protocols by sending requests using Application Program Interface (API) libraries

E.g. Outlook user clicks send, and the email client sends this information to SMTP which adds information to the user's message and passes it down to the Presentation Layer



LAYER 6: PRESENTATION LAYER

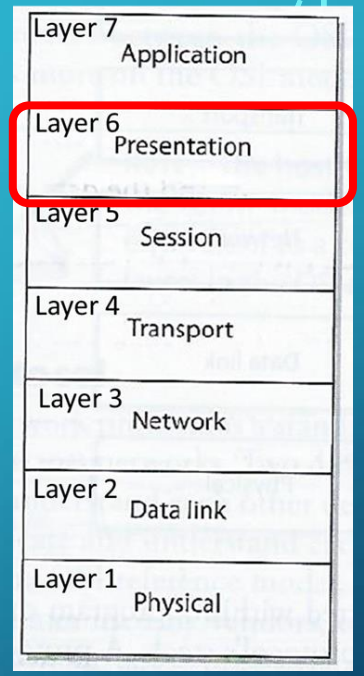


Receives data from the application layer protocol and puts it in a standard format with annotation that enables any process operating at Layer 6 on destination computer can understand

Presentation layer

1. Translates the format of data an application is using into a standard format used for passing messages over a network
2. Adds file type data to tell destination computer the file type and how to process and present it
3. Handles compression and encryption requests and adds data that enables the receiving computer to know how to decompress and decrypt the data

LAYER 6: PRESENTATION LAYER



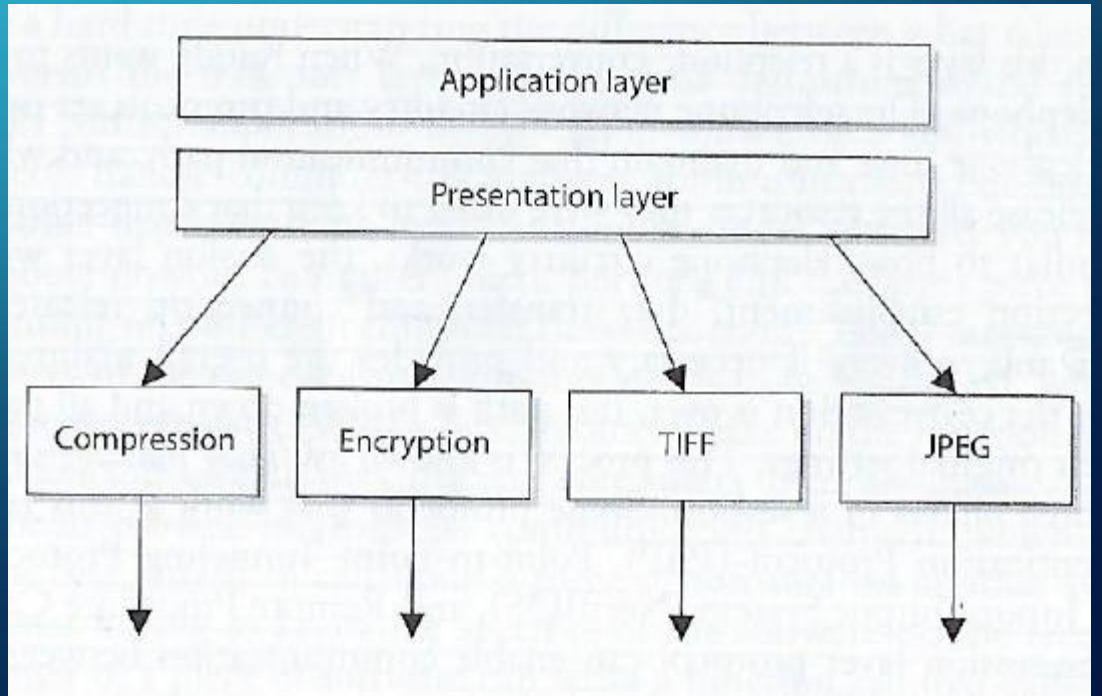
Protocols functioning at this layer communicate include:

- MIME – Multipurpose Internet Main Extensions standards
- TIFF - Tagged Image File Format
- GIF – Graphic Interchange Format
- JPEG – Joint Photographic Experts Group

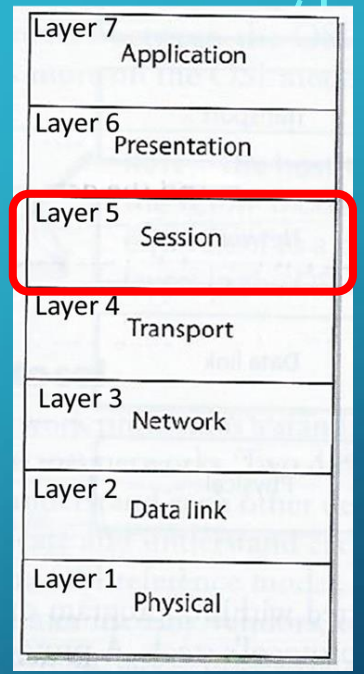
For example, user compresses file on Windows computer with WinZip sends it to someone on Linux computer

When the Linux computer receives the file, it looks at the file header, interprets the header's MIME type (Content-Type: application/zip) and knows what application can decompress the file

If systems does not have WinZip or other program that understands the compression/decompression instructions, the file will be presented to the user with an unassociated icon



LAYER 5: SESSION LAYER



When two applications need to communicate or transfer data between themselves, Layer 5 is responsible for:

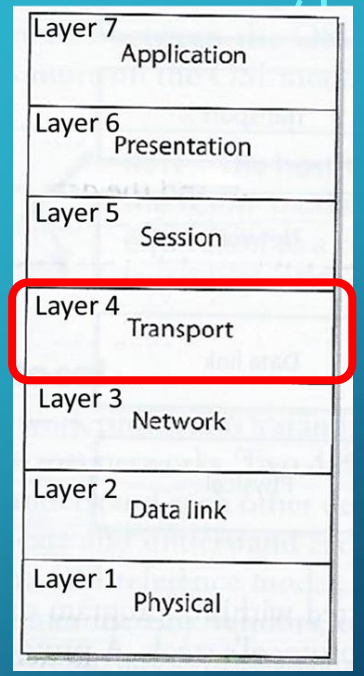
1. Establishing a connection between two applications
2. Dialog management to maintain the connection during the transfer of data
   - *Restarts and recovers the session to maintain the connection if needed*
3. Controlling release of the connection

- Provides inter-process communication channels, enables one software module on a local system to call a second software module running on a remote system. The results of the second module are retuned to the first system over the same session protocol channel

The session layer protocol enables 3 different modes of communications between 2 applications running on different computers across the network:

1. ***Simplex:*** *Communication takes place in one direction (very seldom used)*
2. ***Half-duplex:*** *Communication takes place in both directions, but only one application can send information at a time*
3. ***Full-duplex:*** *Communication takes place in both directions , and both applications can send information at the same time*

LAYER 4: TRANSPORT LAYER

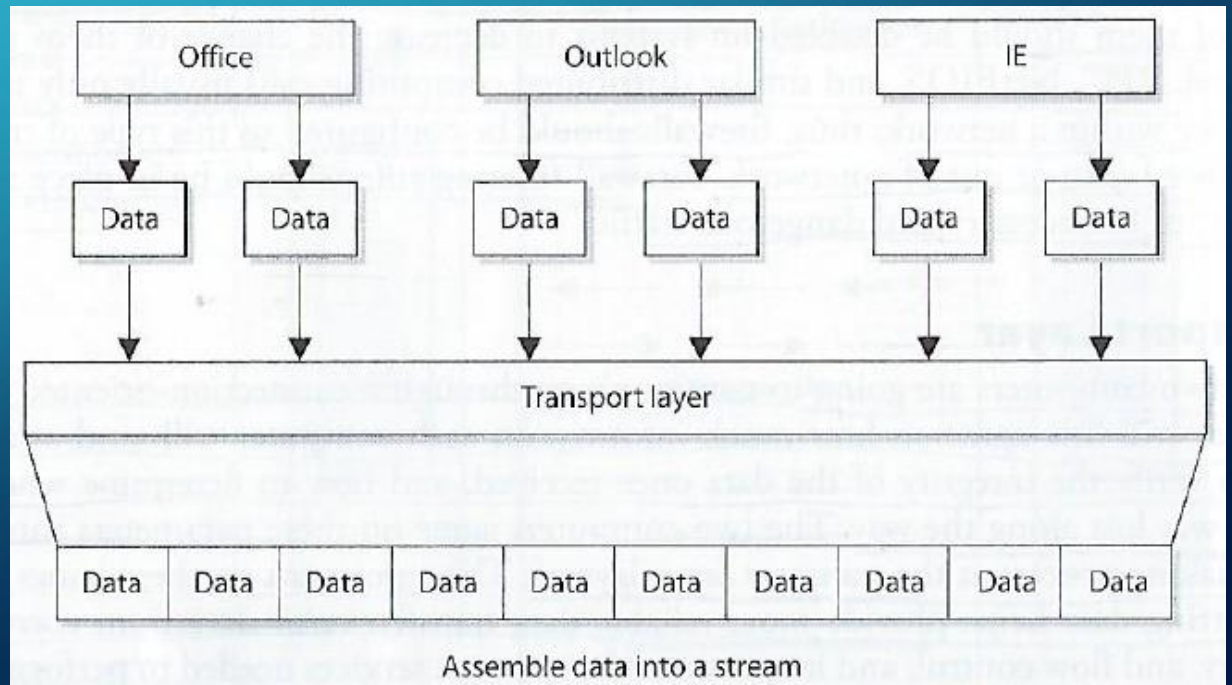


Establishes a logical connection between two computer systems and provides end-to-end data transport services

Provides connection level protocols for two computers to engage in a "handshaking process" and agree on parameters for:

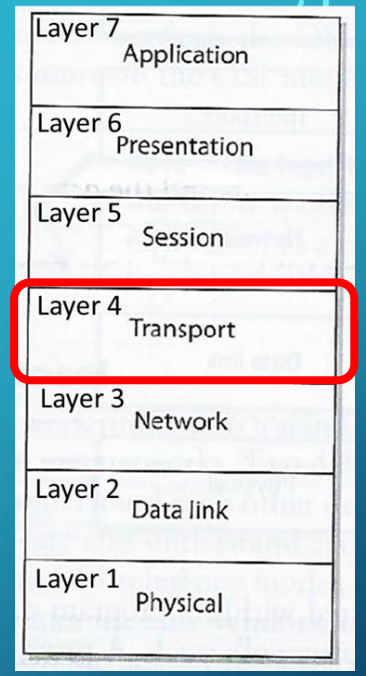
1. How much data each computer will send at a time
2. How to verify data integrity once received
3. How to determine if a data packet was lost

Receives data from different applications and assembles their data into a stream for transmission over the network



LAYER 4: TRANSPORT LAYER

Transport layer protocol controls data flow across computer to computer connections without tracking connections between individual pairs of applications communicating across the network



Protocols:

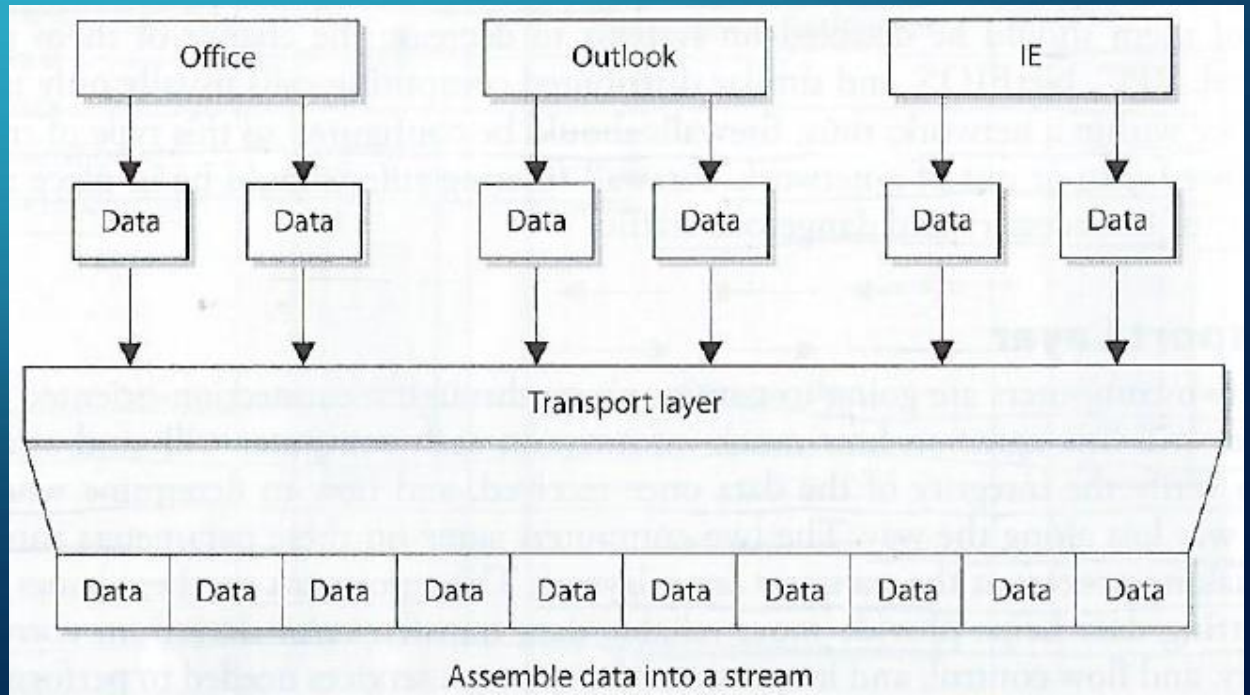
- TCP – Transmission Control Protocol

  Connection-oriented provides reliable data transmission

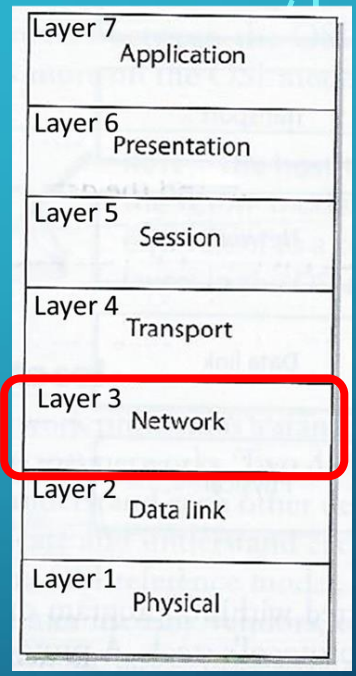
- UDP – User Datagram Protocol

  Connectionless

TLS – Transport Layer Security protocol, straddles both Session and Transport layers



LAYER 3: NETWORK LAYER'S



Routing protocols

- Build and maintain routing tables

  Routing tables are maps of the network
- Determine best route to send packet from source computer to destination computer
- Inserts information into the data packet's header consisting of addresses (source and destination) and routes to their destination
- Do not guarantee delivery of packets

  Transport layer protocols catch problems and resend packets as needed (TCP not UDP)

Protocols

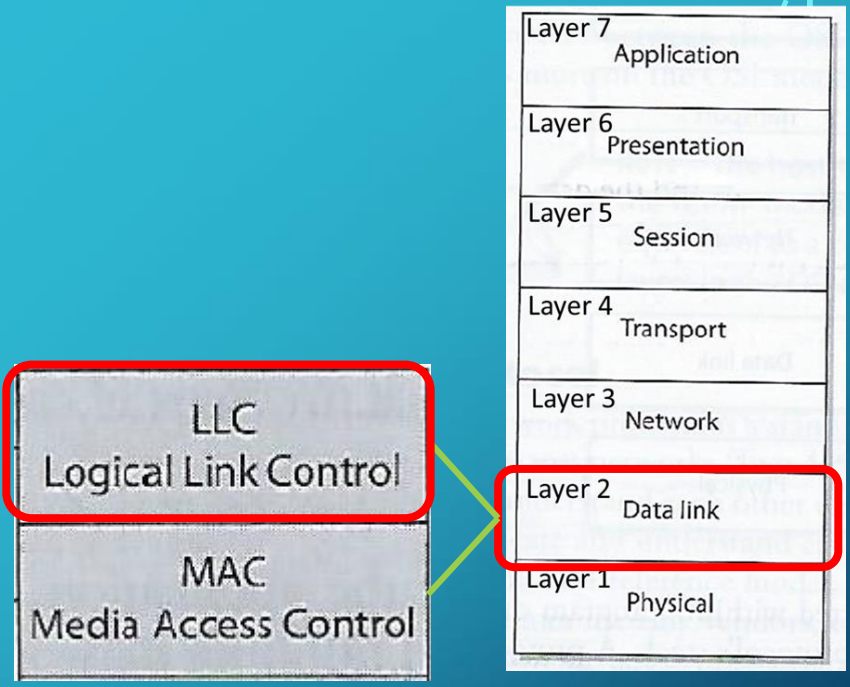
- IP – Internet Protocol
- ICMP – Internet Control Message Protocol
- RIP – Routing Information Protocol
- OSPF – Open Shortest Path First
- IPX – Internet Packet Exchange

Routers operate on OSI Layer 3

LAYER 2: DATA LINK LAYER

Translates the data packet with header/footer information accumulated from layers above into

LAN (Local Area Network) or WAN (Wide Area Network) binary format for transmission over the network transmission line



After the network layer adds its routing information into the data packet, it passes the packet to the Data Link Layer's LCC sublayer

LCC sublayer takes care of flow of control and error checking and passes it to the MAC sublayer

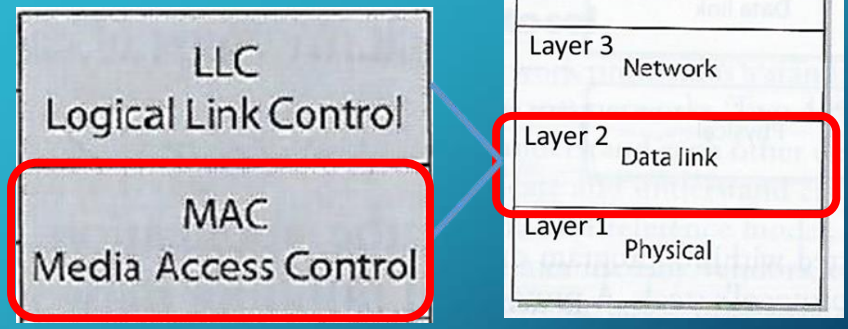
Switches operation on OSI Layer 2

LAYER 2: DATA LINK LAYER

The MAC sublayer determines if the data will be transmitted over a LAN or WAN, the network type and protocols and puts the last header and trailer on the packet before it is "put on the wire" and transmitted

Each network type has a different:

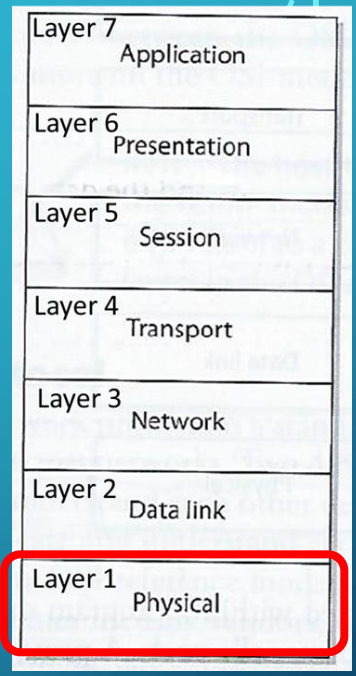
- *Header data format structure*
- *Protocol for physical transmission across the network type (coaxial, twisted pair, fiber optic cable; or wireless)*



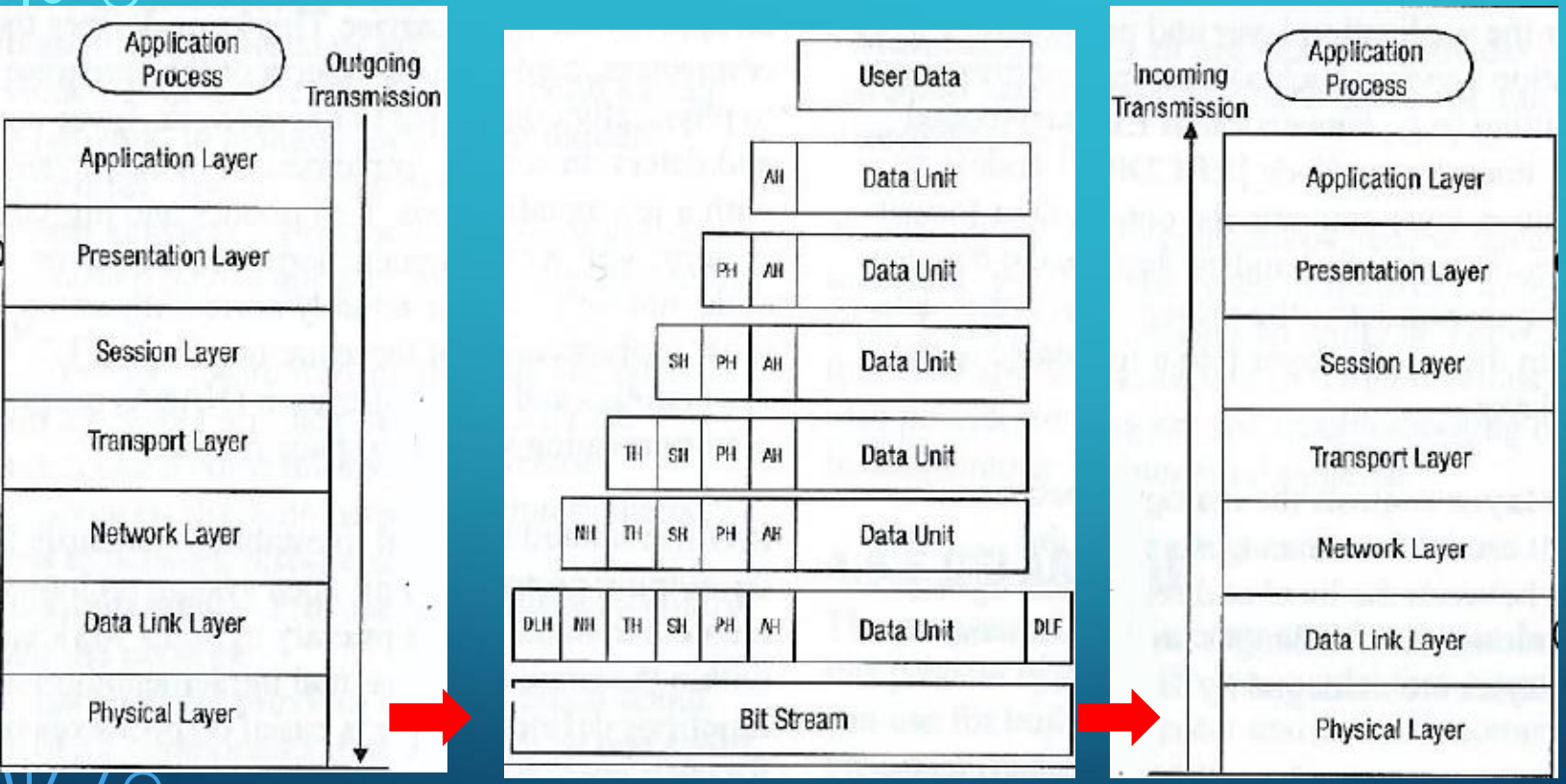
LAYER 1: PHYSICAL LAYER

The Network Interface Card (NIC)

- Produces and interprets electromagnetic signals
- Converts bits into signals or voltages suitable for transmission across the LAN or WAN technology it is connected
- Determines synchronization, data transfer rates, line noise and transmission techniques based on the physical connection to electrical, optical or mechanical equipment



LAYER 1: PHYSICAL LAYER



Data/file requests and terminals

Standard formats, encryption, compression

Applications communicating data

Computers communicating

Routing packets formed

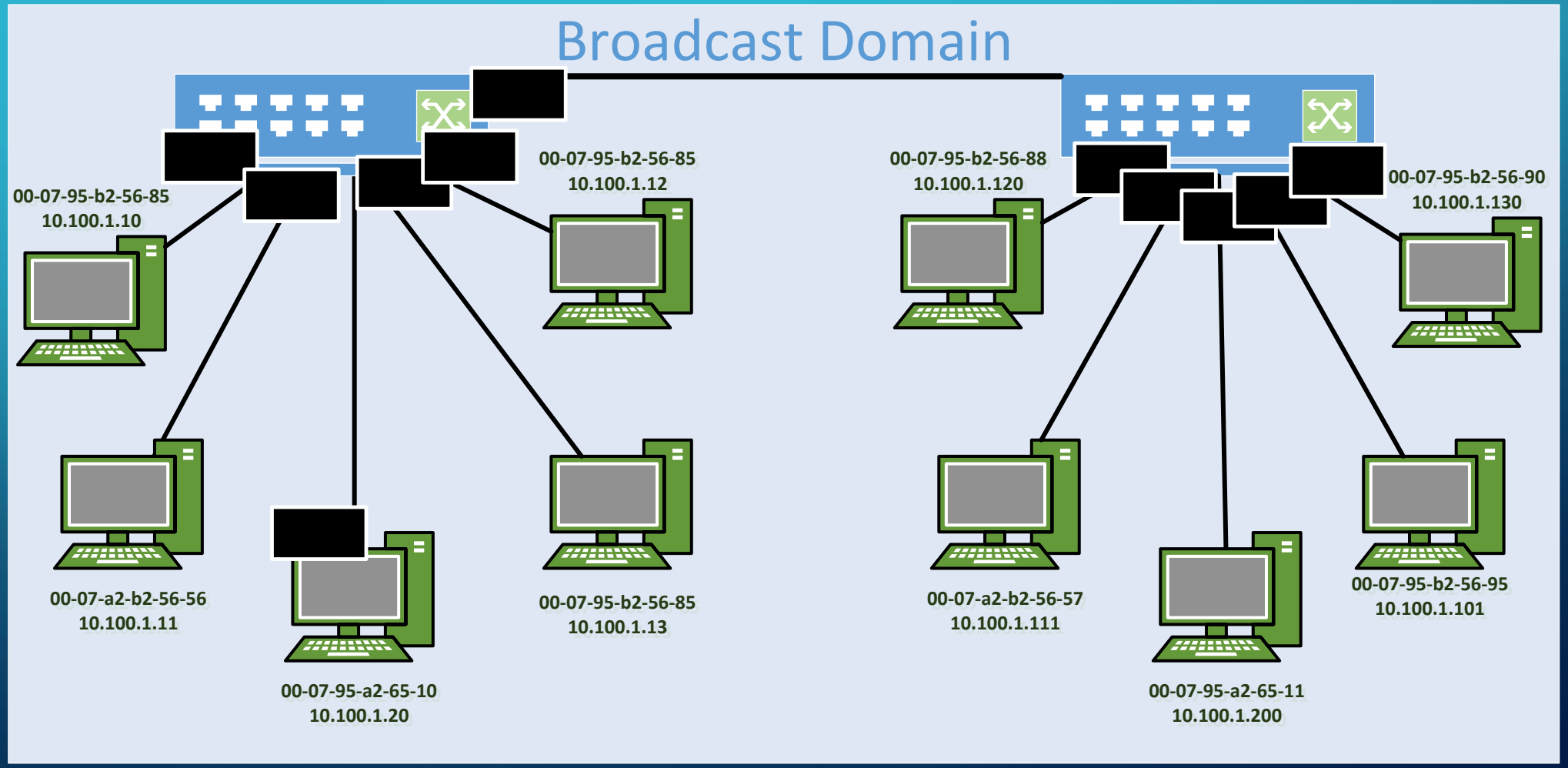
Data frames ready for transfer

Signal processing

SWITCHED ENVIRONMENTS

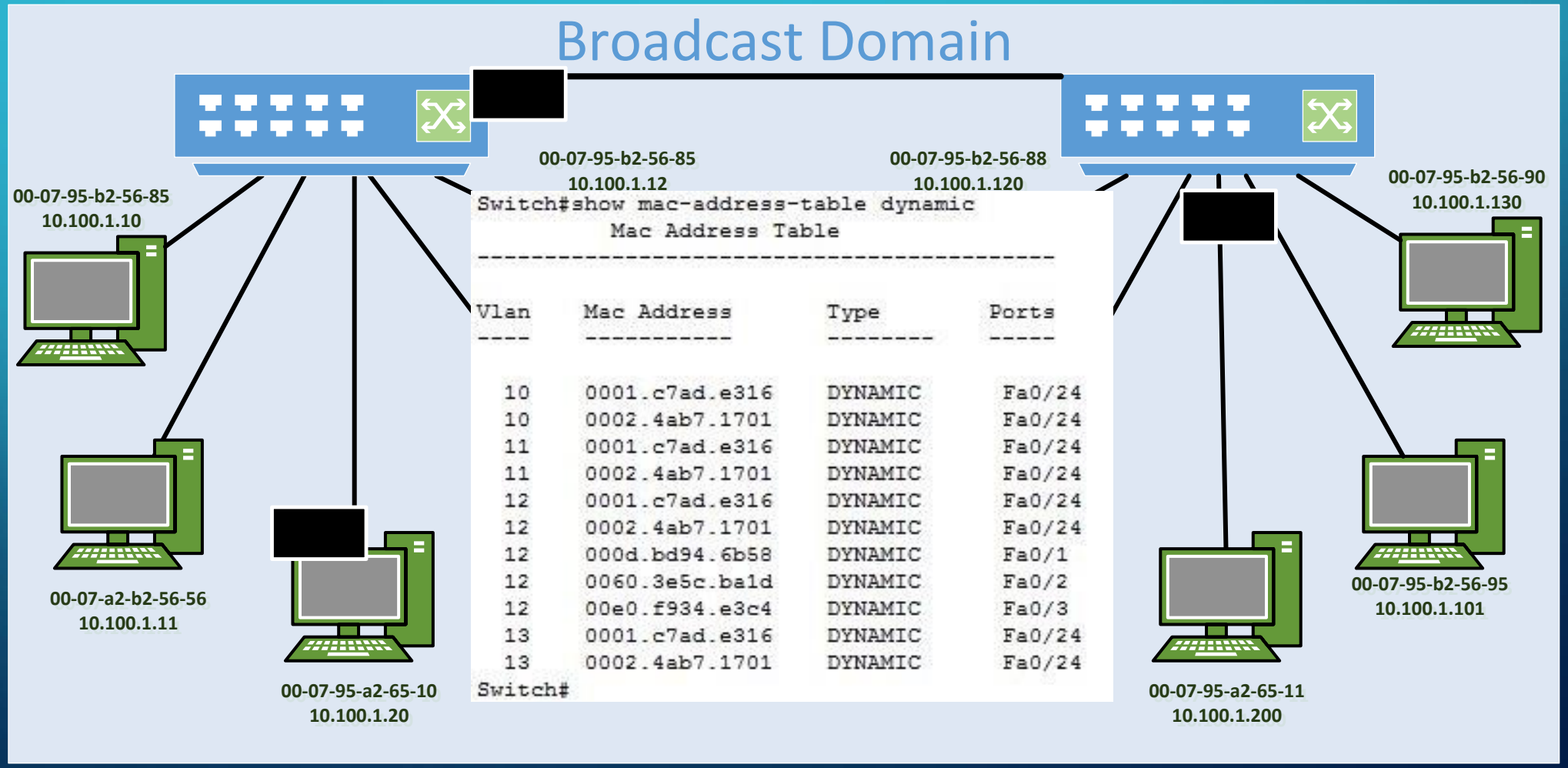
NONE-SWITCH ENVIRONMENTS

All packets received by the hub are transmitted out all ports.

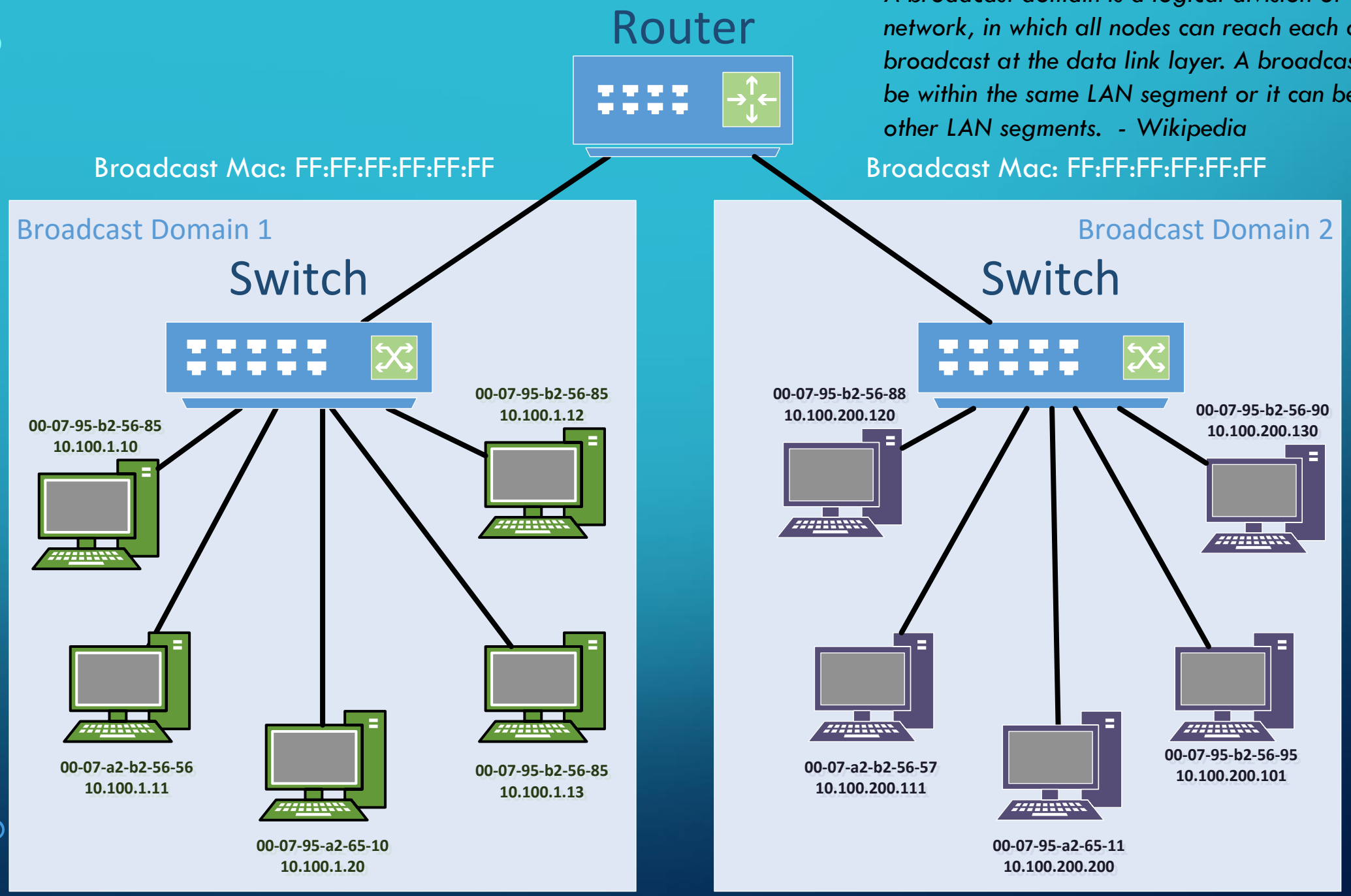


SWITCH ENVIRONMENTS

Packets received by the switch are transmitted out ports based on destination mac addresses

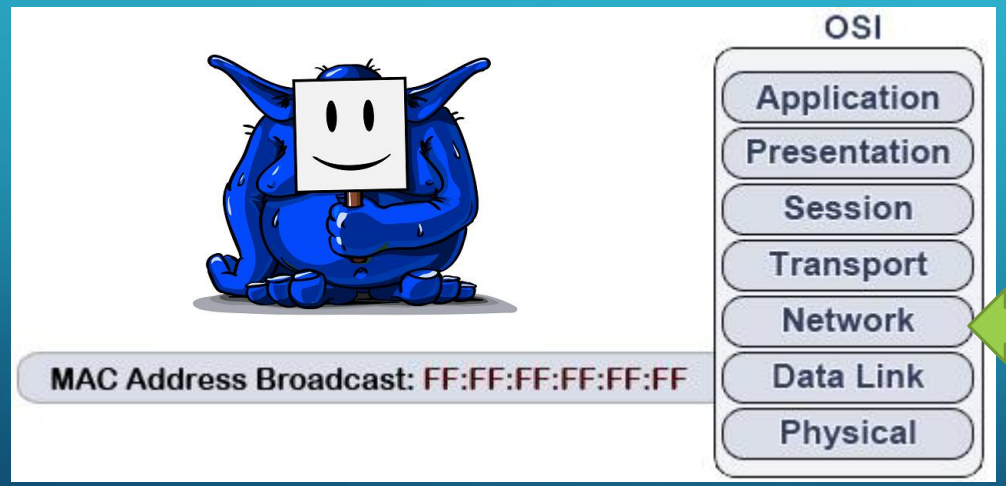


A broadcast domain is a logical division of a computer network, in which all nodes can reach each other by broadcast at the data link layer. A broadcast domain can be within the same LAN segment or it can be bridged to other LAN segments. - Wikipedia

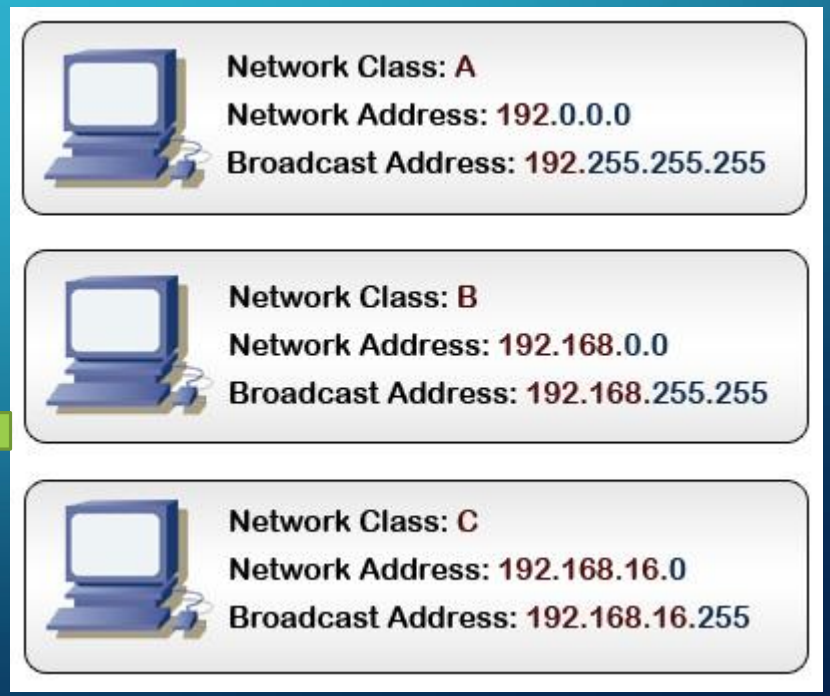


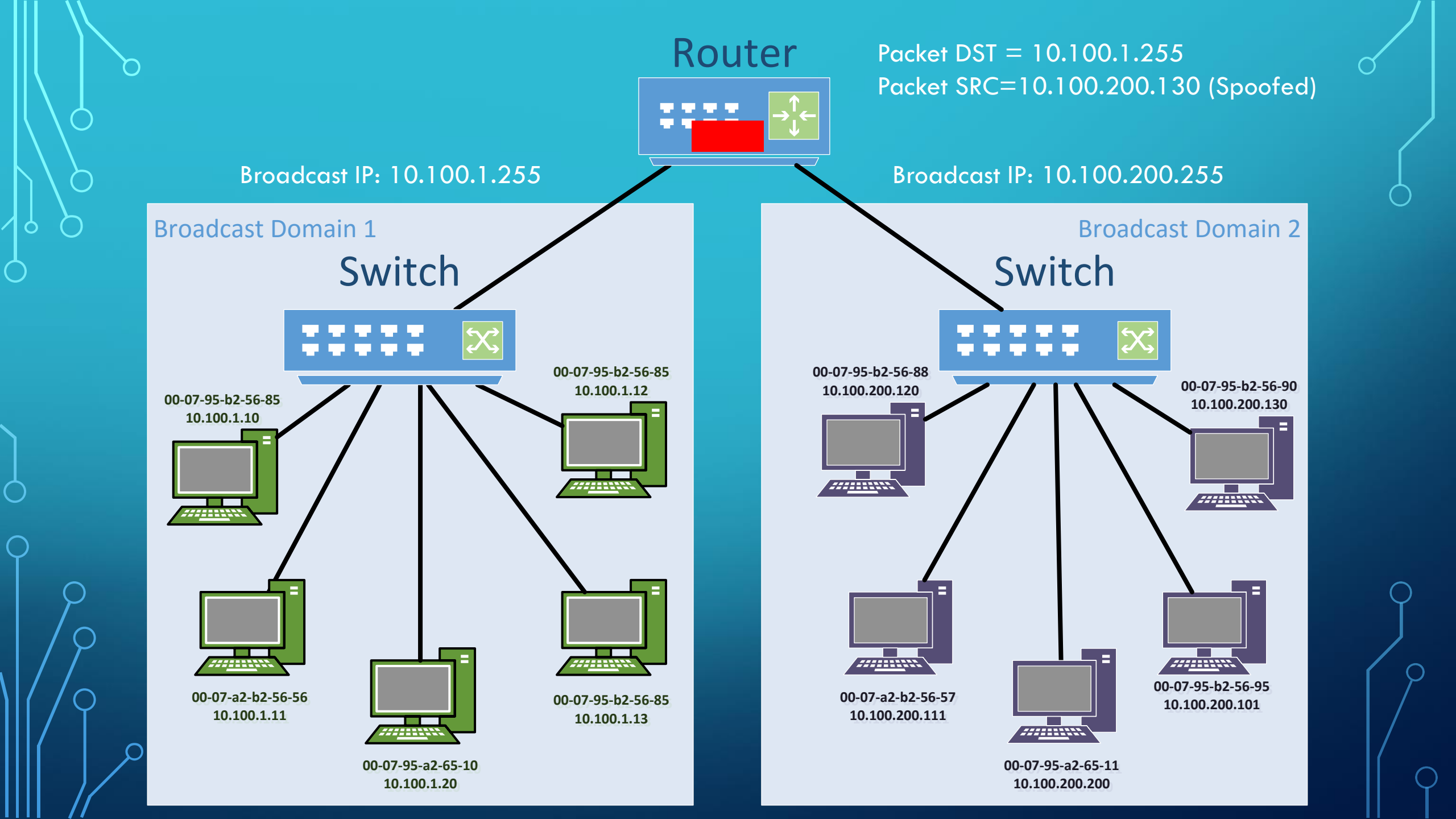
BROADCAST DOMAIN

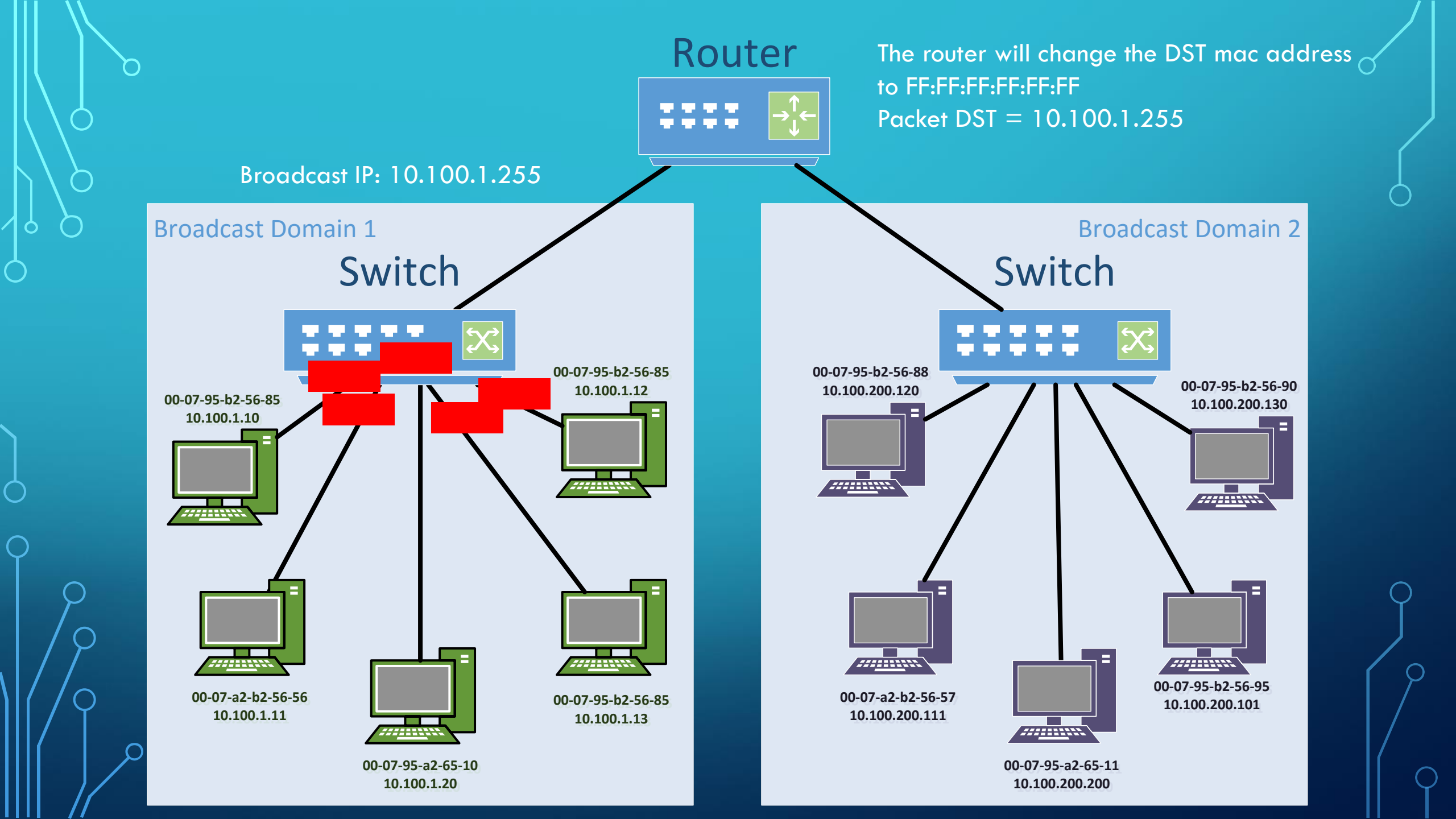
Attack type: ARP SPOOFING

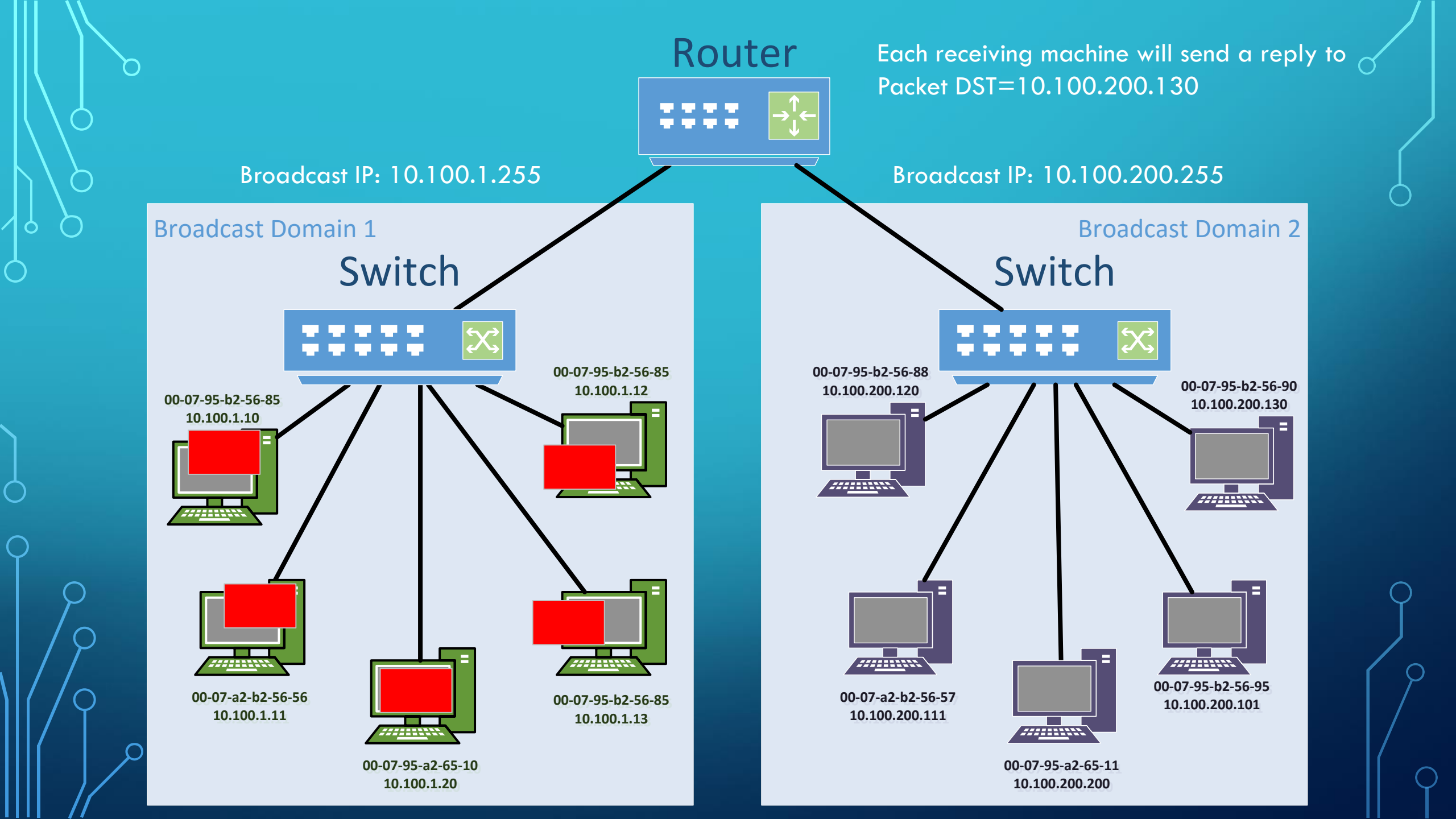


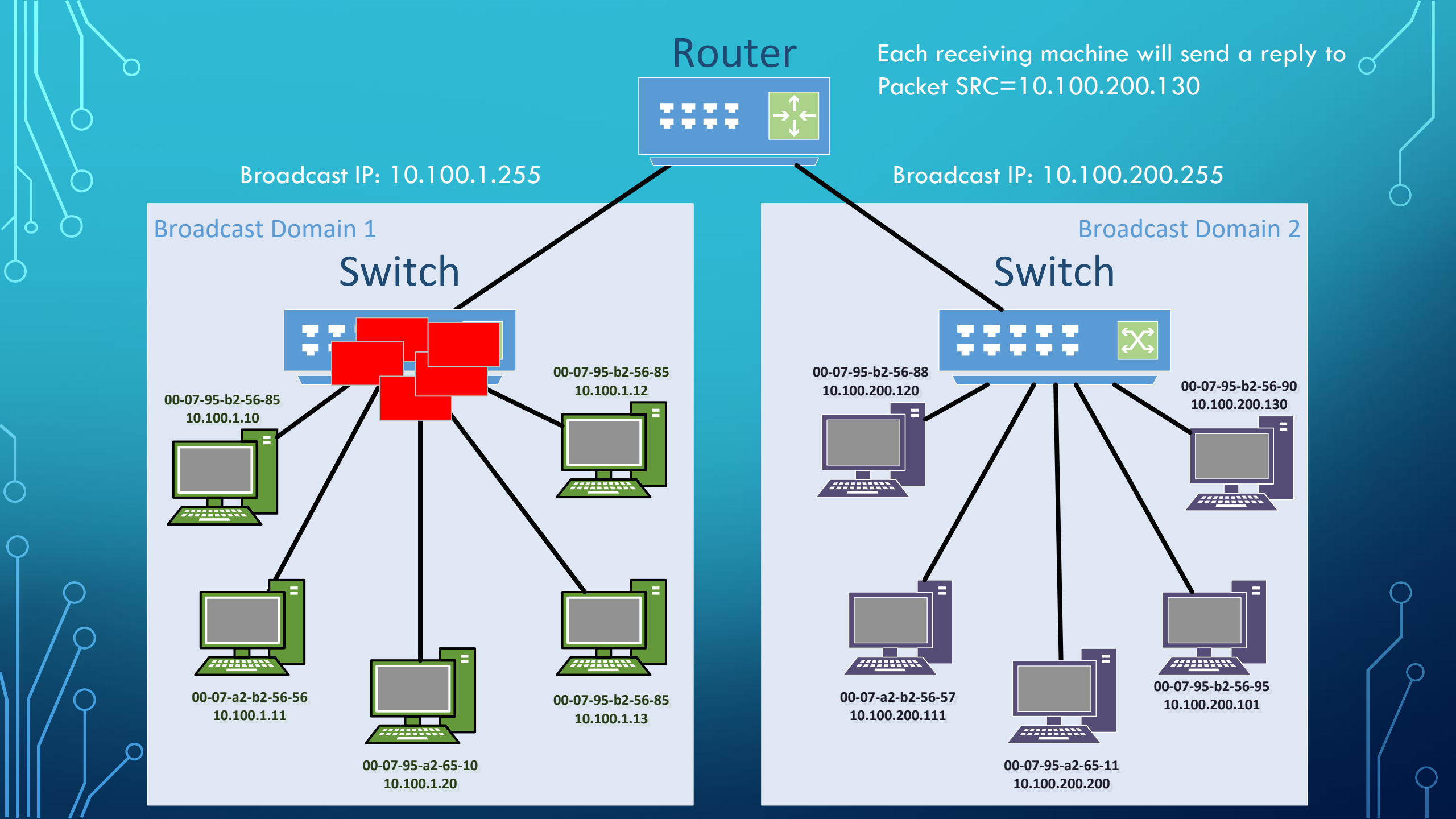
Attack type: Smurf Attacks




Router
Packet DST = 10.100.1.255
Packet SRC=10.100.200.130 (Spoofed)
Broadcast IP: 10.100.1.255
Broadcast IP: 10.100.200.255
Broadcast Domain 1
Broadcast Domain 2
Switch
Switch
00-07-95-b2-56-85
10.100.1.10
00-07-95-b2-56-85
10.100.1.12
00-07-a2-b2-56-56
10.100.1.11
00-07-95-a2-65-10
10.100.1.20
00-07-95-b2-56-85
10.100.1.13
00-07-95-b2-56-88
10.100.200.120
00-07-95-b2-56-90
10.100.200.130
00-07-a2-b2-56-57
10.100.200.111
00-07-95-a2-65-11
10.100.200.200
00-07-95-b2-56-95
10.100.200.101

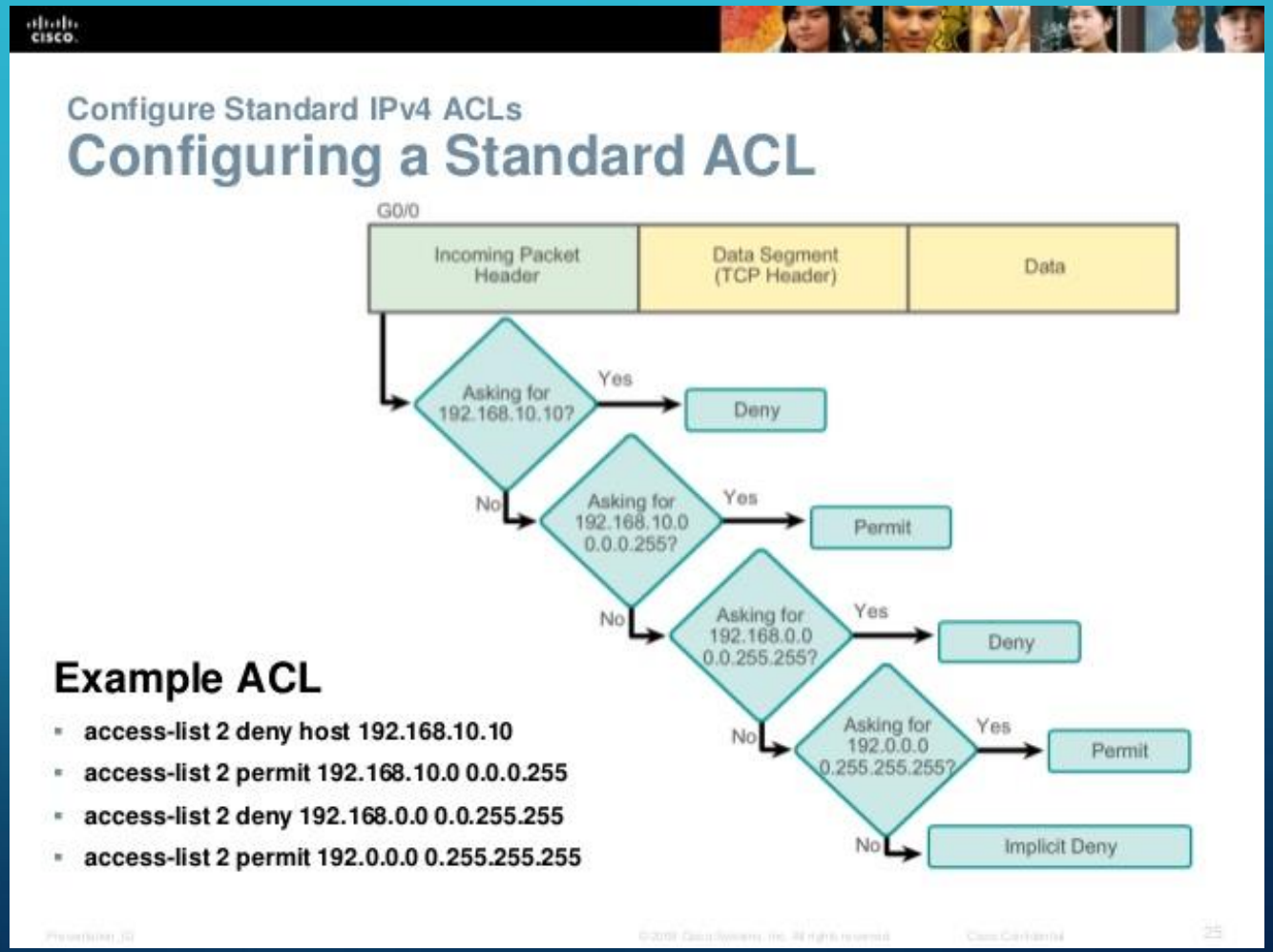

Router
The router will change the DST mac address to FF:FF:FF:FF:FF:FF
Packet DST = 10.100.1.255
Broadcast IP: 10.100.1.255
Broadcast Domain 1
Switch
00-07-95-b2-56-85
10.100.1.10
00-07-95-b2-56-85
10.100.1.12
00-07-a2-b2-56-56
10.100.1.11
00-07-95-a2-65-10
10.100.1.20
00-07-95-b2-56-85
10.100.1.13
Broadcast Domain 2
Switch
00-07-95-b2-56-88
10.100.200.120
00-07-95-b2-56-90
10.100.200.130
00-07-a2-b2-56-57
10.100.200.111
00-07-95-a2-65-11
10.100.200.200
00-07-95-b2-56-95
10.100.200.101

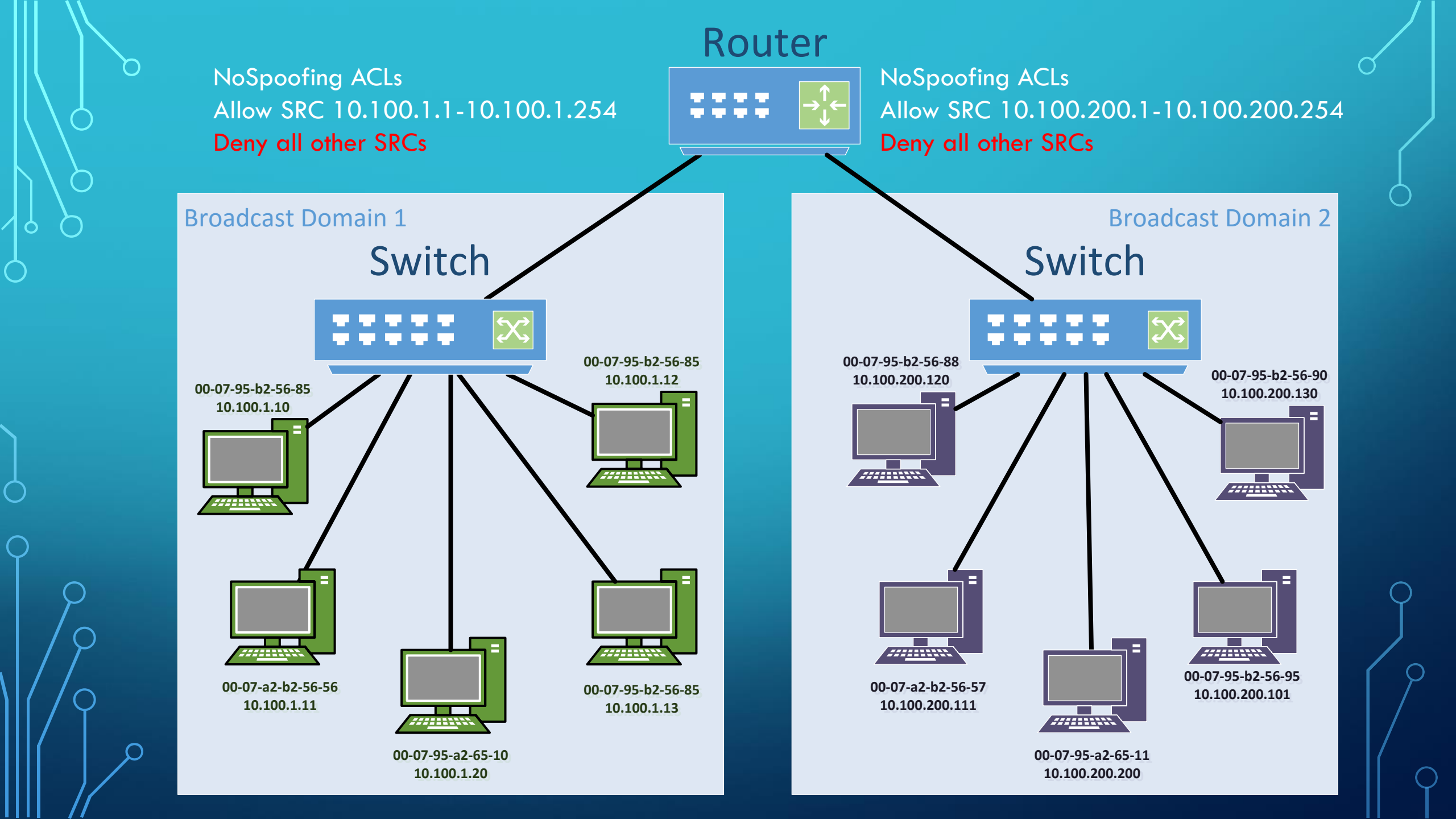

Router
Each receiving machine will send a reply to
Packet DST=10.100.200.130
Broadcast IP: 10.100.1.255
Broadcast IP: 10.100.200.255
Broadcast Domain 1
Broadcast Domain 2
Switch
Switch
00-07-95-b2-56-85
10.100.1.10
00-07-95-b2-56-85
10.100.1.12
00-07-a2-b2-56-56
10.100.1.11
00-07-95-a2-65-10
10.100.1.20
00-07-95-b2-56-85
10.100.1.13
00-07-95-b2-56-88
10.100.200.120
00-07-95-b2-56-90
10.100.200.130
00-07-a2-b2-56-57
10.100.200.111
00-07-95-a2-65-11
10.100.200.200
00-07-95-b2-56-95
10.100.200.101


Router
Each receiving machine will send a reply to
Packet SRC=10.100.200.130
Broadcast IP: 10.100.1.255
Broadcast IP: 10.100.200.255
Broadcast Domain 1
Broadcast Domain 2
Switch
Switch
00-07-95-b2-56-85
10.100.1.10
00-07-95-b2-56-85
10.100.1.12
00-07-a2-b2-56-56
10.100.1.11
00-07-95-a2-65-10
10.100.1.20
00-07-95-b2-56-85
10.100.1.13
00-07-95-b2-56-88
10.100.200.120
00-07-95-b2-56-90
10.100.200.130
00-07-a2-b2-56-57
10.100.200.111
00-07-95-a2-65-11
10.100.200.200
00-07-95-b2-56-95
10.100.200.101

ACCESS CONTROL LISTS (ACL)

ROUTER ACCESS CONTROL LIST

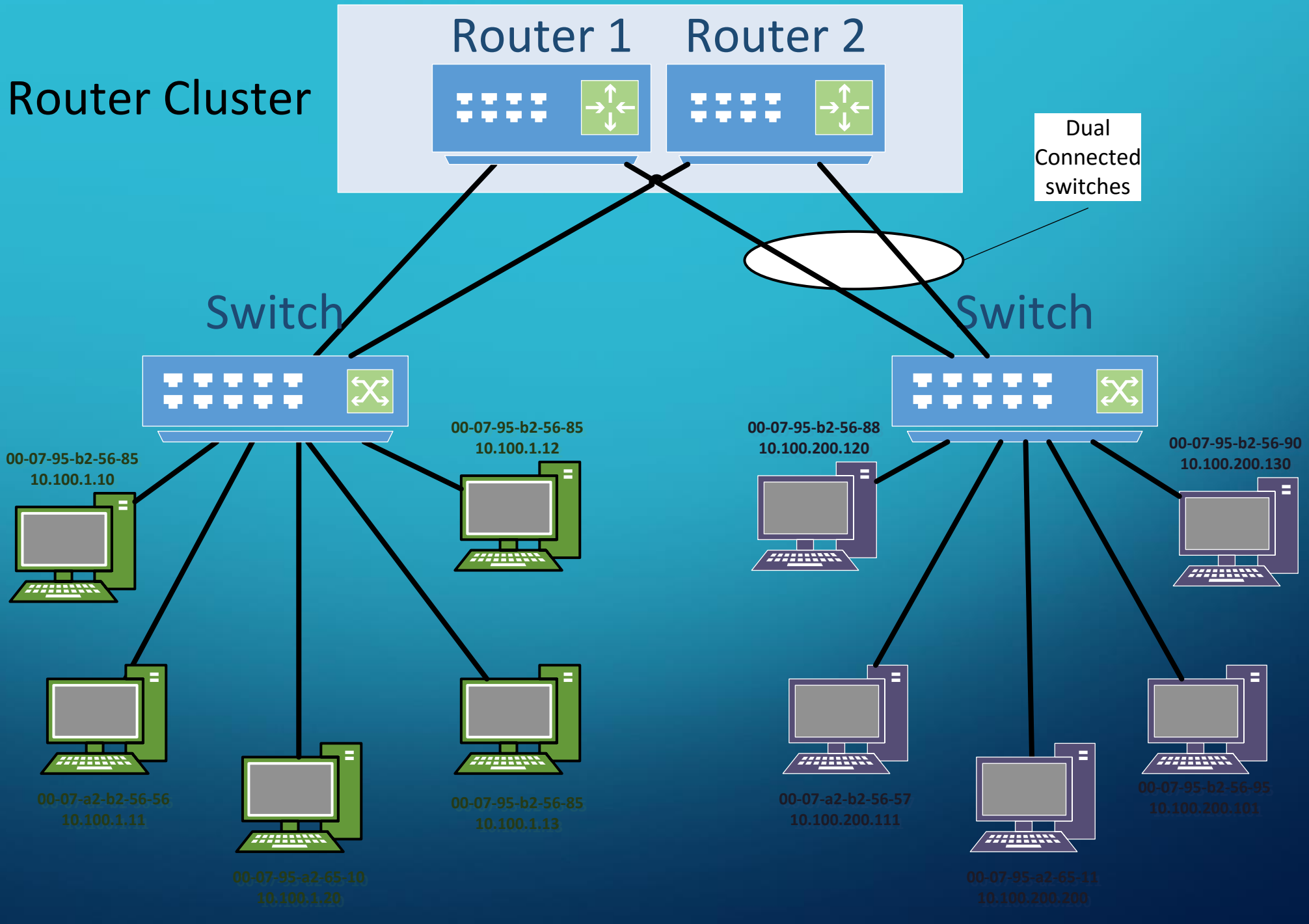



Router
NoSpoofing ACLs
Allow SRC 10.100.1.1-10.100.1.254
Deny all other SRCs
NoSpoofing ACLs
Allow SRC 10.100.200.1-10.100.200.254
Deny all other SRCs
Broadcast Domain 1
Switch
00-07-95-b2-56-85
10.100.1.10
00-07-95-b2-56-85
10.100.1.12
00-07-a2-b2-56-56
10.100.1.11
00-07-95-a2-65-10
10.100.1.20
00-07-95-b2-56-85
10.100.1.13
Broadcast Domain 2
Switch
00-07-95-b2-56-88
10.100.200.120
00-07-95-b2-56-90
10.100.200.130
00-07-a2-b2-56-57
10.100.200.111
00-07-95-a2-65-11
10.100.200.200
00-07-95-b2-56-95
10.100.200.101

NETWORK ARCHITECTURES

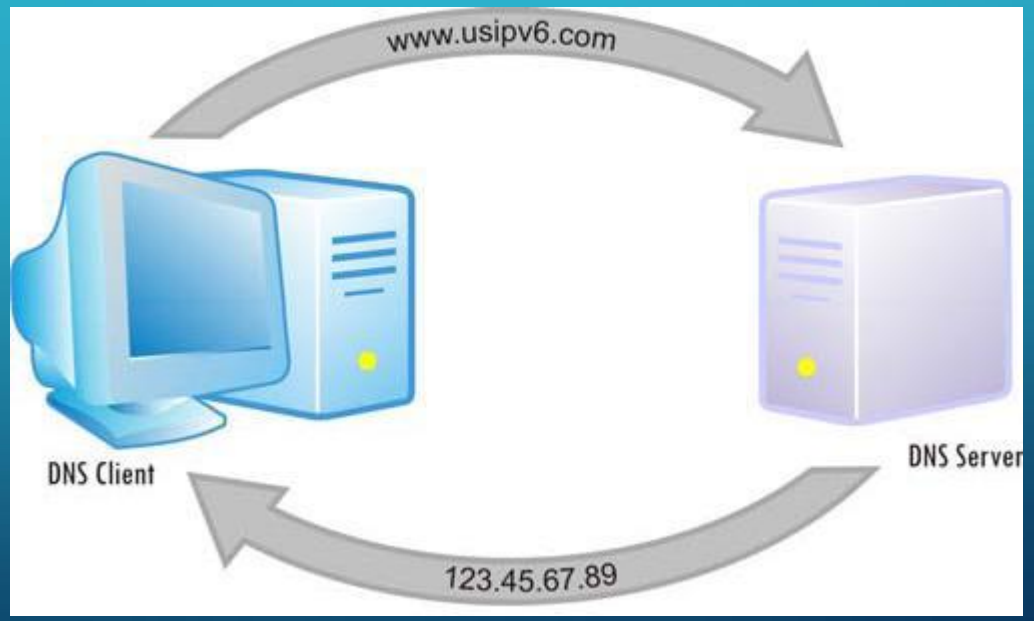
- **Access costs, speed, flexibility and reliability**
- **Critical infrastructure**
  - *Risk of downtime (loss of availability) ?*
  - *Impact of downtime?*
- **Business Continuality Planning**
  - *Role of Highly Available and Redundant networks*

Router Cluster



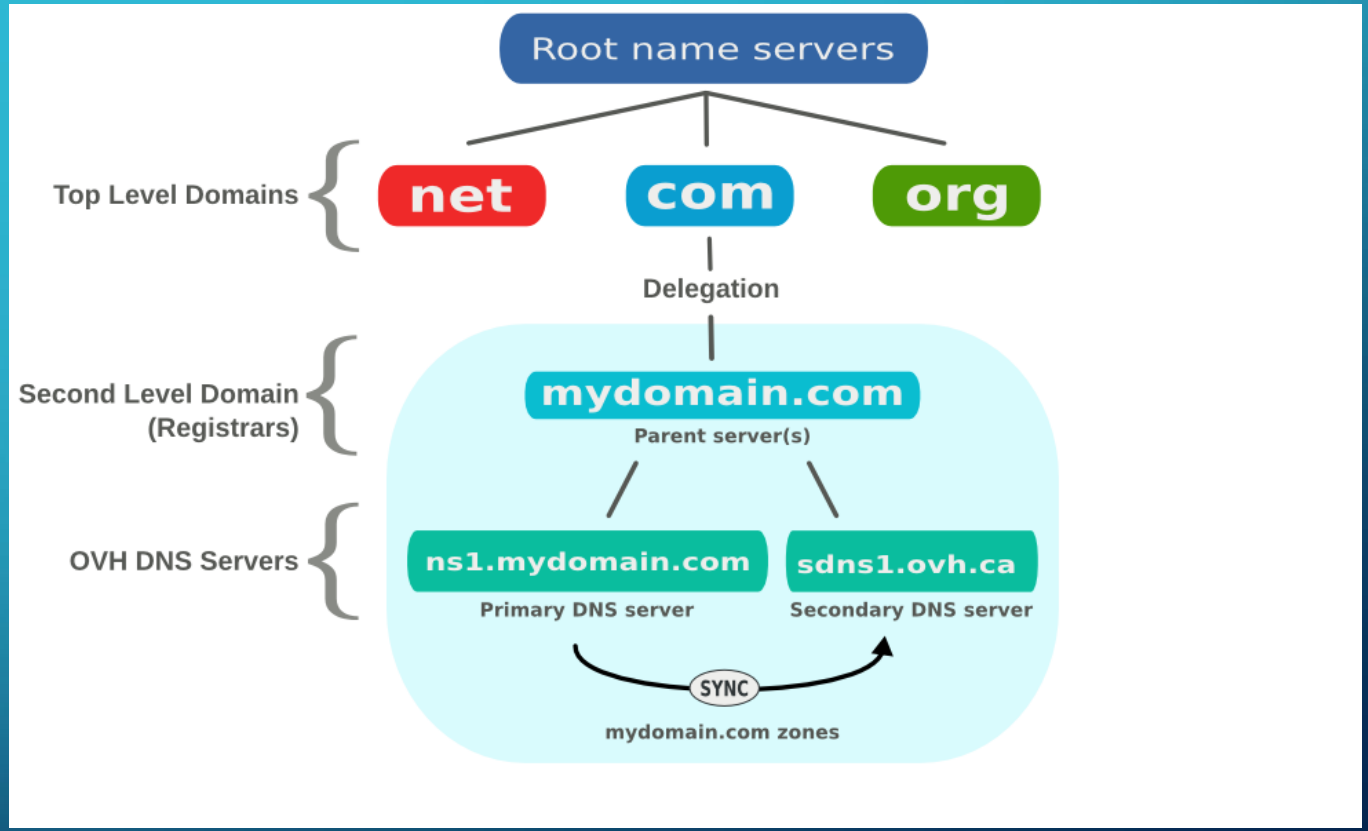
DOMAIN NAME SYSTEM (DNS)

- Hostname-to-IP addressing translation: www.cnn.com to 151.101.32.73



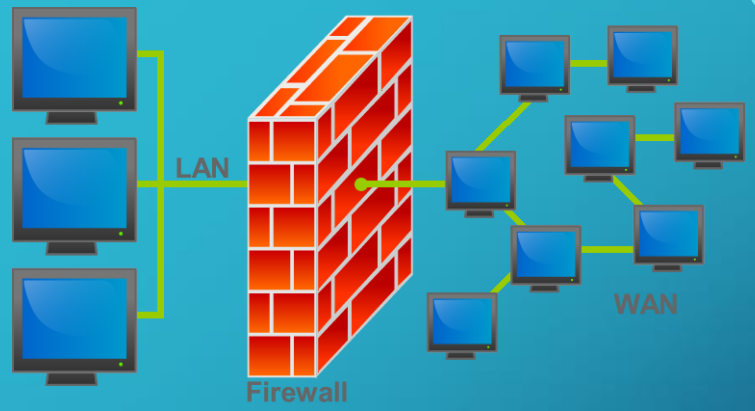
DOMAIN NAME SERVER (DNS)

- Hierarchical structure
- Root Servers
- Top-level domains
- Split-DNS
  - Internal vs External facing
- Vulnerability to attack



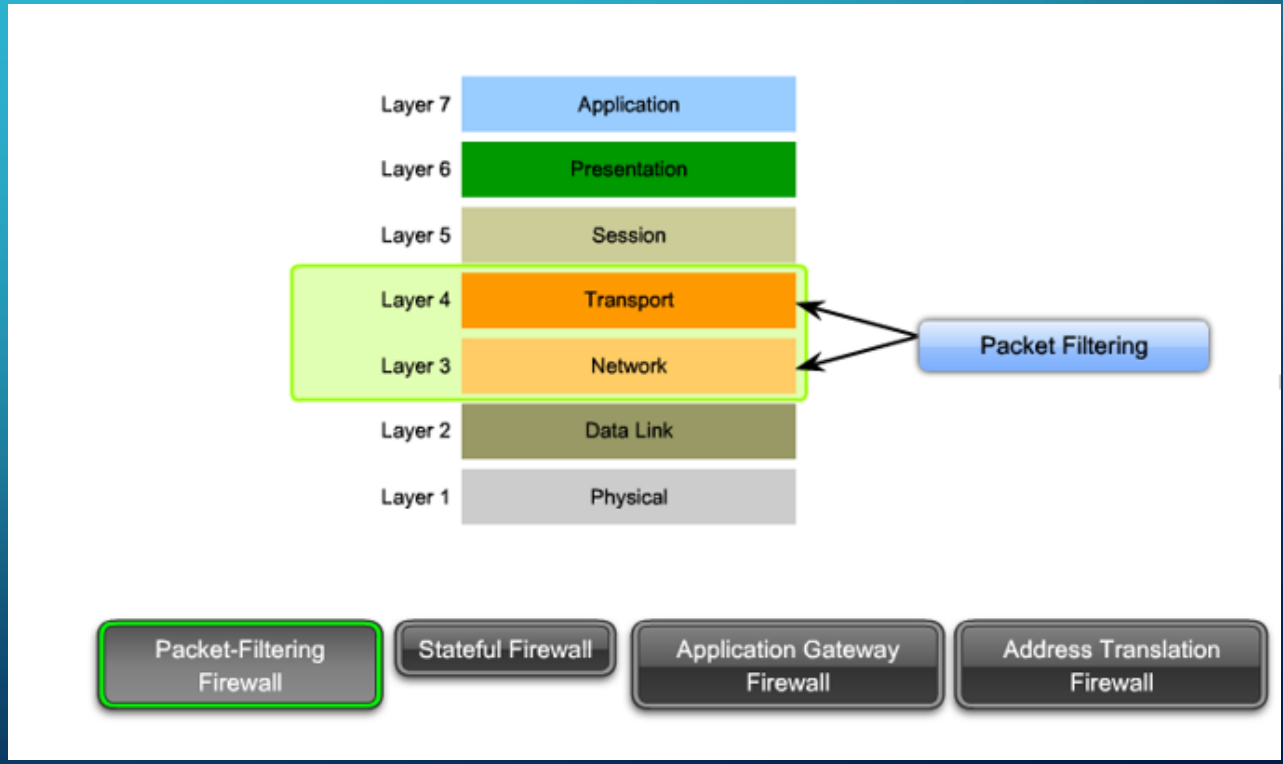
FIREWALLS

FIREWALL ROLES AND PLACEMENT



- Placed at network borders
  - Network Address Translation (NAT)
- Packet filtering
  - IP-Address
  - Port
- Application based
- Stateful inspection
  - Reassembling packets first
- IPS Inspections

- **All equal "overhead" processing**

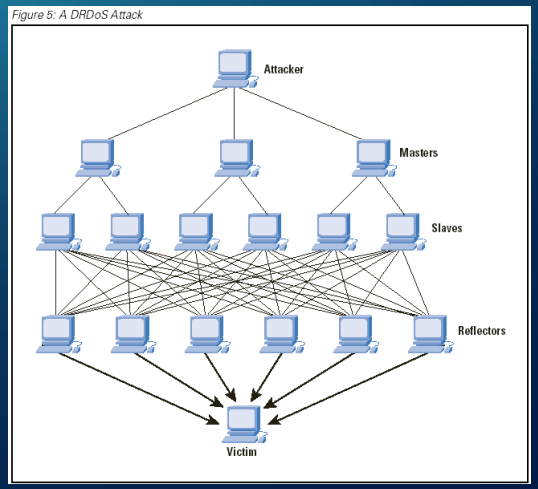


ATTACK METHODOLOGY

ATTACK METHODOLOGY/COUNTER MEASURES

DENIAL OF SERVICE ATTACKS (DOS)

- Rather than gaining access, deny access to others!
  - Two Types DoS or **Distributed** DoS
- By preventing networks and servers from handling legitimate traffic, attackers deny service.
- Overwhelm firewalls or servers with invalid traffic patterns that consume bandwidth, memory or CPU resources.
- Distributed means leveraging others in the attack.



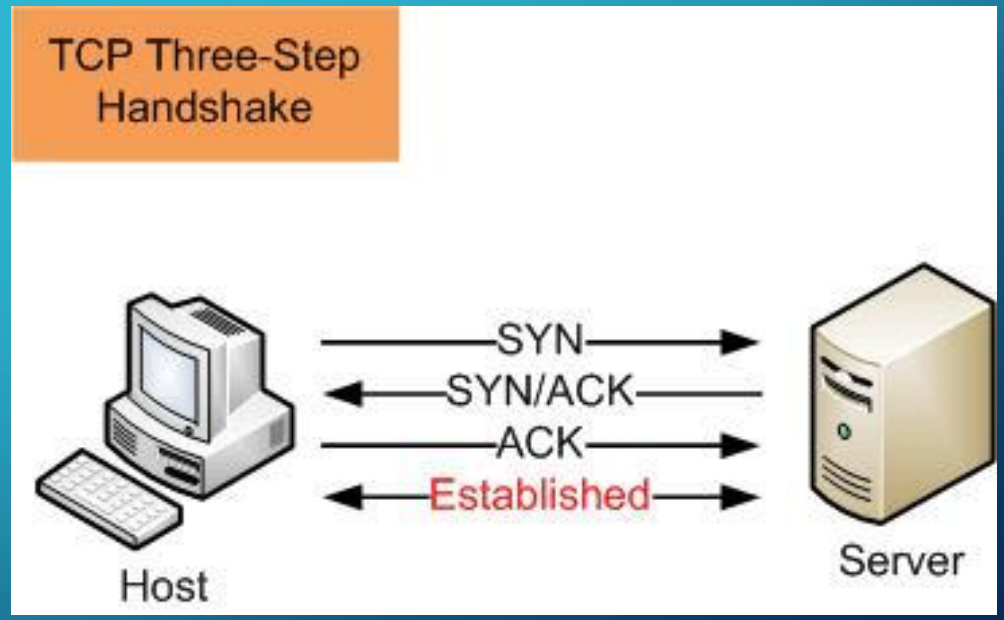
HOW DOS WORKS

SYN attack: attacker ignored "syn/ack" return, each SYN takes up a TCP connection on the server. Goal is to exhaust TCP connection table.

Reflective DoS: spoof the sending IP address so return syn/ack traffic attacks another IP.

Distributed DoS: Have multiple Zombie machines in a BOT Net attack a single IP.

UDP attacks: flooding the pipes or links with traffic
Which does not need Three-Way Handshake.
Forces routers and firewalls to process useless traffic.



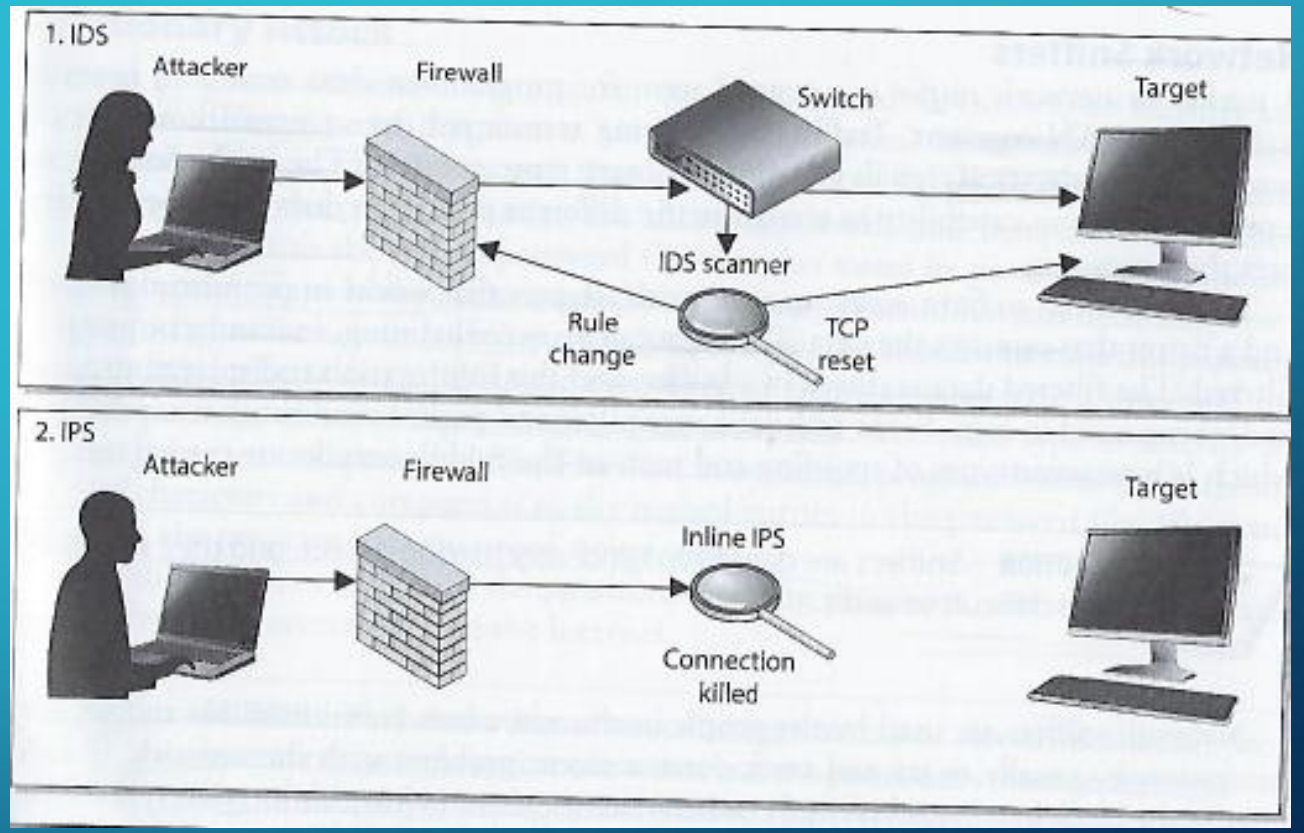
HOW TO COUNTER DOS

- Anomaly detection
- Usual traffic patterns
- Network traffic which breaks rules
- Install an Anomaly detection appliance
- Turn on features on firewalls
- Not the same a signature based Intrusion Detection (IPS)

INTRUSION DETECTION AND PREVENTION SYSTEMS (IDS & IPS)

INTRUSION DETECTION VS PREVENTION

- IDS – Detect something bad may be taking place and send an alert
  - *Detective and "after the fact" response*
- IPS – Detect something bad may be taking place and block traffic from gaining access to target
  - *Preventive and proactive response*



SUMMARY OF BEST PRACTICE STEPS

- Know where your data is and classify it (Data classification standards, policy)
- Segment Hosts and Broadcast Domains (vlans, switches, routers)
- Control which hosts can talk. (Router Access Control Lists or Firewall rules)
- Reduce exposure to untrusted networks (Firewalls)
- Good host hygiene. (Patch Management, vulnerability management)
- Know your own network (Discover scans to look for new hosts … usually not patched!)
- Next time: Protecting Data (Encryption at rest and Encryption in-transit)

Network Security

How Networks Work

- OSI Model
- Well-known ports
- Three-way handshake
- Packet Captures
- Anomalies
- Network Types
  - Public → IP Addressing
  - Private → IP Addressing
  - Cloud / Hybrids
- Components
  - Hubs
  - Switches
  - Routers
  - Firewalls
  - Encryption
  - IPS / IDS
  - Wireless
  - End-Points

Concepts

- Perimeter Defense
- Defense In Depth
- Continuous Monitoring
- Least Privledge

Host Firewall
Permissions (Least Priv)
File Systems – ACL
Closing Ports / Services

Security Posture

Governance / Framework

- Confidentiality/Integrity/Access (CIA)
- Asset Classification
- Law Compliance
  - HIPAA
  - FERPA
  - Sarbanes Oxley
  - PCI-DSS
  - FISMA
  - GLBA

Risks

- Mitigation
- Tolerance
- Transfer
- Evaluation
- “Likelihood”

Attacks/ Countermeasures

- Recon
- OS Vulnerabilities
- DDoS / DOS
- Sniffers
- Social Engineering
- Data Harvesting

AGENDA

- ✓Network security definition
- ✓Models and protocols
- ✓Switched environments
- ✓Access control lists
- ✓Firewalls
- ✓Intrusion detection and prevention systems