System and Network Administration

Network Essentials

Configuring for Network Services

Networks are made of

- Hosts that act as clients and servers
  - **Servers share resources with AUTHORISED Clients**
- Media and Equipment that interconnect hosts
- Protocols that govern connections
- Users

Networks allow cooperation

Cooperation leads to communities of users

Network Components

Component	Description
Device	Any piece of hardware such as a computer, server, printer, or smartphone.
Media	Connects devices to the network and carries data between devices.
Network adapter	Hardware that translates data between the network and a device.
Operating system	Software that controls network traffic and access to network resources.
Protocol	Software that controls network communications using a set of rules.


Q
&
A

ISO OSI Reference Model

Understanding the abstract architecture is key to understanding the concrete network

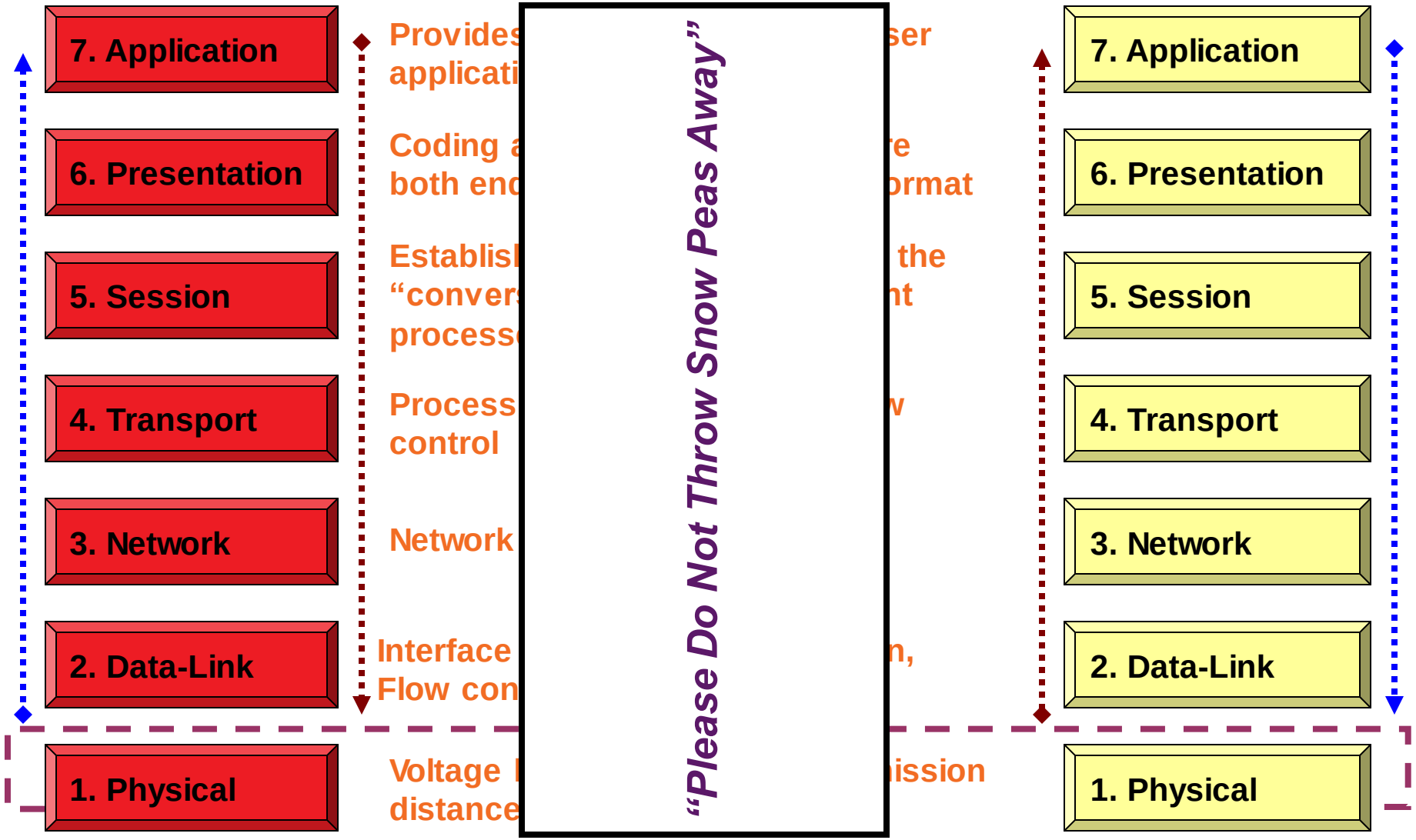
The ISO Seven "layer" OSI Model is a Conceptual model that describes many types of network.

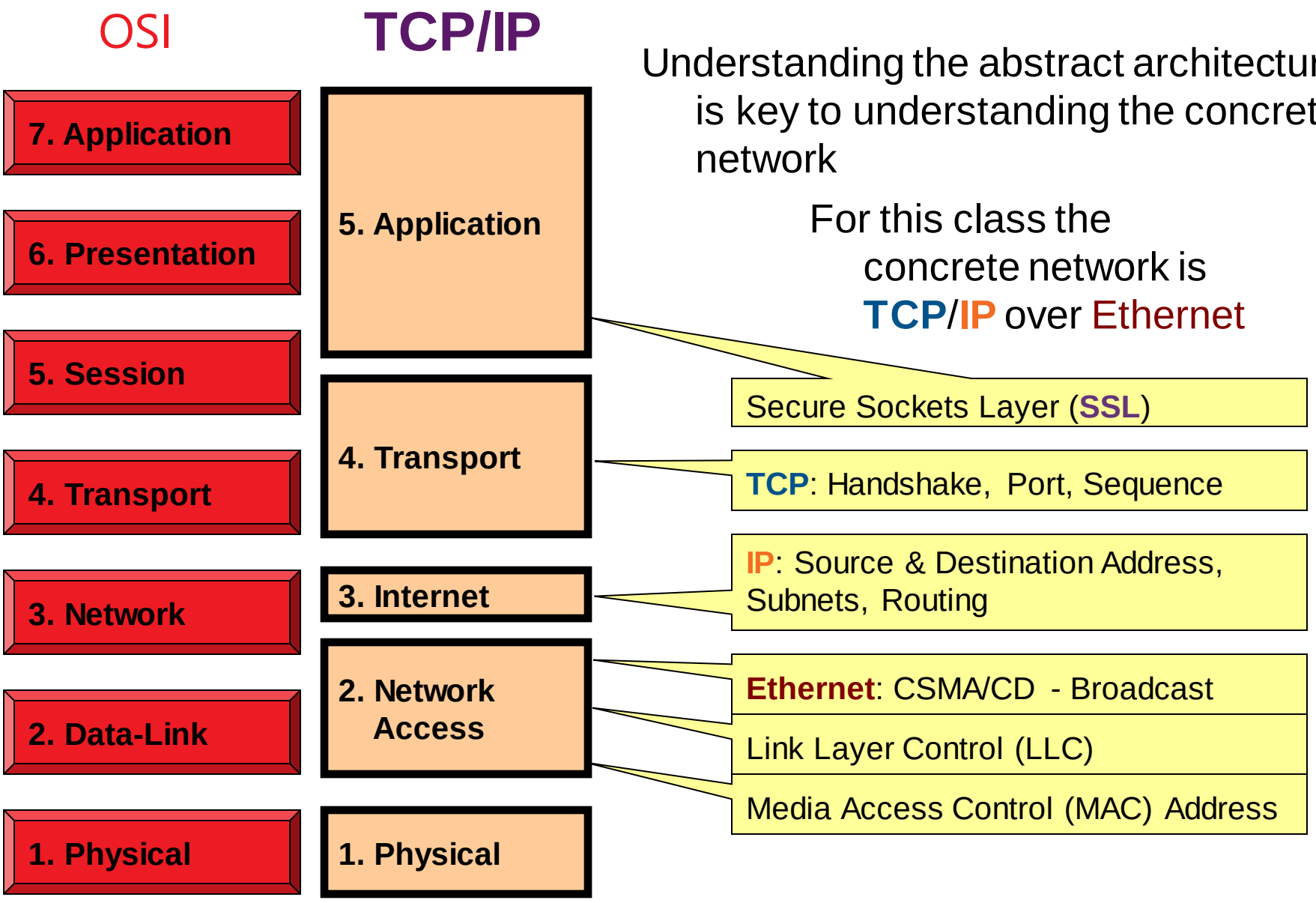
The Internet is a fairly unsophisticated example.

Each layer represents a higher level of abstraction in the process of data communications

- Complexities of low level transmission of signals representing the data are hidden from users at the application level (top layer)

OSI Model: Information Flow






Q
&
A

Packets and Encapsulation

Packets: Header and payload

- Header tells where the packet came from and where it's going
- Payload is the data

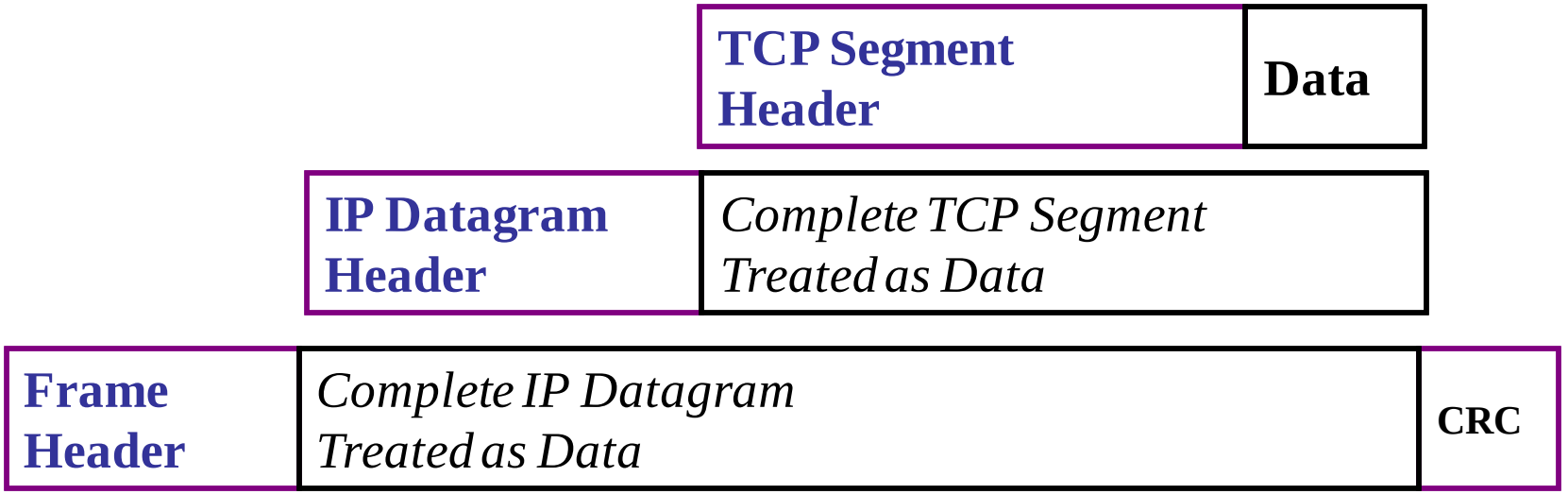
- TCP layer it's called a *segment*
- IP layer it's called a *packet*
- Link layer it's called a *frame*

Cultural Sensitivity

Encapsulation

- A packet is a structured message.
- The control information of a given protocol must be treated strictly as data by the next "lower" protocol.
- As a packet moves *down* the protocol stack, it gets bigger as information relevant to the layer is added to the beginning and the end.
- Any given layer is allowed to work only with the data relevant to that layer, and nobody else's.
- As a packet moves up the stack it gets smaller, as the information from the current level is removed.

Ethernet, IP, and TCP



Remember, this is really just a stream of bits

00111101010101011100001010101010100010101101010010010101001011100101 00

Ethernet Frame Format

Preamble (64 bits)
Destination Address (48 bits)
Source Address (48 bits)
Packet type (16 bits)
Data (368-12,000 bits)
CRC (32 bits)

Key Fields

- *Preamble:* Alternating *1's* and *0's* to help receiving nodes synchronise
- *Address:* Unique identifier assigned by the hardware manufacturer **(MAC Address)**
- *Packet Type:* identifies this as an Ethernet frame (allows mutiple protocols and versions)
- *CRC:* Error detection (Cyclic Redundancy Check)

Remember, this is really just a stream of bits

00111101010101011100001010101010100010101101010010010101001011100101 00

Datagram Format

Each row represents 4 octets (32 bits)

Version - Length - QOS - Total Length
Unique ID - Flags - Fragment Offset
Time to Live - Protocol - Checksum
Source IP Address
Destination IP Address
Options - Padding
Data *(up to 4416 bits)*

Key Fields

- IP is version 4 or 6
- QOS requests priority
- Second Row controls Fragmentation (e.g., "2 of 4")
- Gateways decrement **TTL** and discard the datagram if zero
- Protocol is analogous to Ethernet Type, Header Checksum to CRC
- Options are included for network testing (not required)

Remember, this is really just a stream of bits

00111101010101011100001010101010100010101101010010010101001011100101 00

TCP Segment Format

Each row represents 4 octets (32 bits)

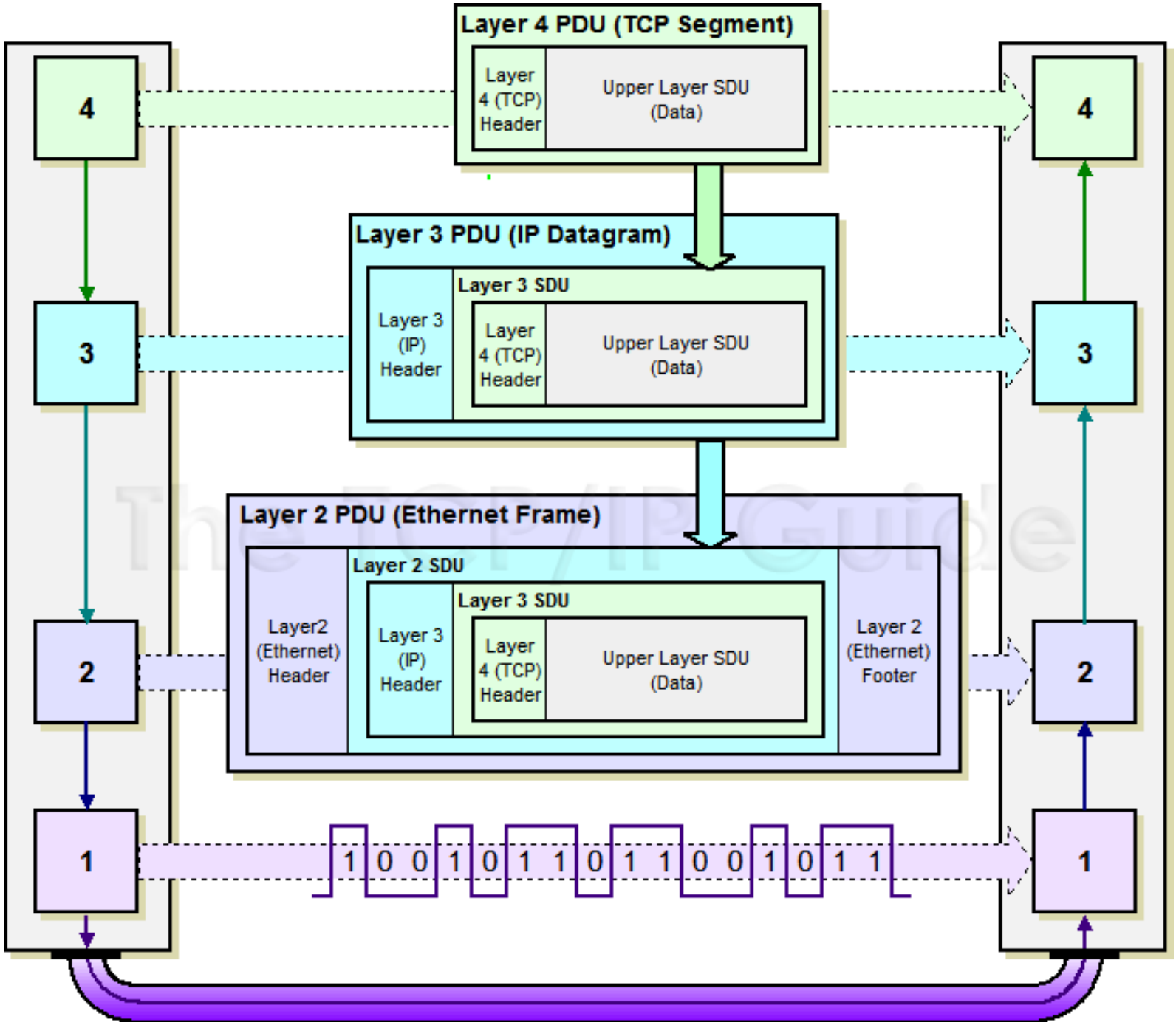
Source Port - Destination Port
Sequence Number
Acknowledgement Number
Offset - Code - Window
Checksum - Urgent
Options - Padding
Data *(up to 4224 bits)*

Key Fields

- Port number specifies service
- Sequence is position in sender's byte stream
- Acknowledgement of position in sender's byte stream
- Some segments carry only ACK, others carry data, and others a request to establish or close a connection (Code)
- Window and Options negotiate maximum segment size

Remember, this is really just a stream of bits

00111101010101011100001010101010100010101101010010010101001011100101 00


Layer 4 PDU (TCP Segment)
Layer 4 (TCP) Header
Upper Layer SDU (Data)
Layer 3 PDU (IP Datagram)
Layer 3 (IP) Header
Layer 3 SDU
Layer 4 (TCP) Header
Upper Layer SDU (Data)
Layer 2 PDU (Ethernet Frame)
Layer2 (Ethernet) Header
Layer 2 SDU
Layer 3 (IP) Header
Layer 3 SDU
Layer 4 (TCP) Header
Upper Layer SDU (Data)
Layer 2 (Ethernet) Footer
4
3
2
1
1 0 0 1 0 1 1 0 1 1 0 0 1 0 1 1

Ethernet, IP, and TCP

Is there a service on this port? **Yes: Pass up the DATA part** No: discard it

TCP Segment Header	**Data**

Is this my IP address? **Yes: Pass up the DATA part** No: discard it

Am I a Router? **Yes: Pass the whole packet to all interfaces** No: ~

IP Datagram Header	*Complete TCP Segment Treated as Data*

Is this my MAC address? **Yes: Pass up the DATA part** No: discard it

Frame Header	*Complete IP Datagram Treated as Data*	**CRC**

Is this an ethernet frame? **Yes: Pass it up** No: discard it

Data Link Layer: stream of bits

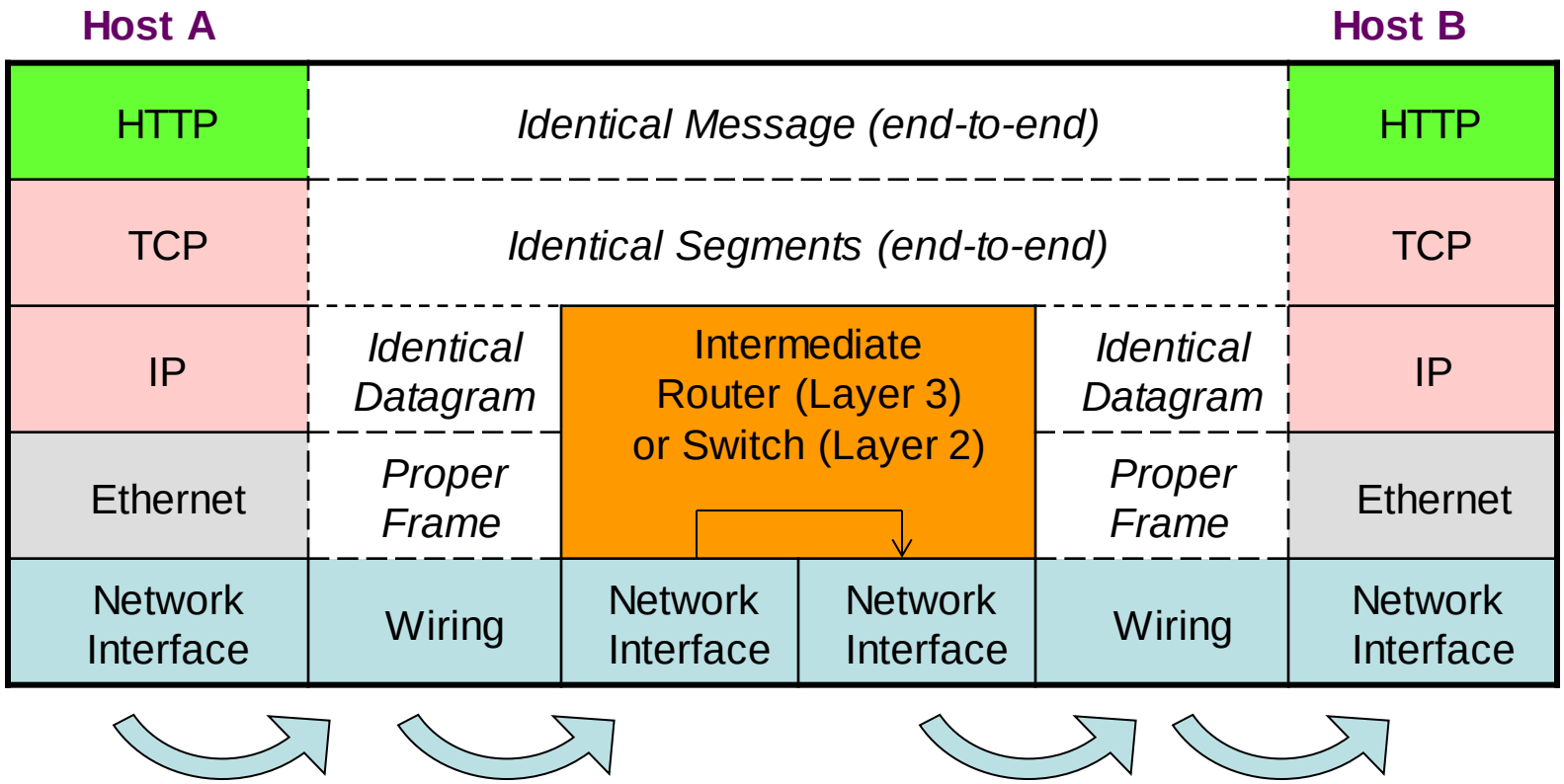
00111101010101011100001010101010100010101101010010010101001011100101000


Q
&
A

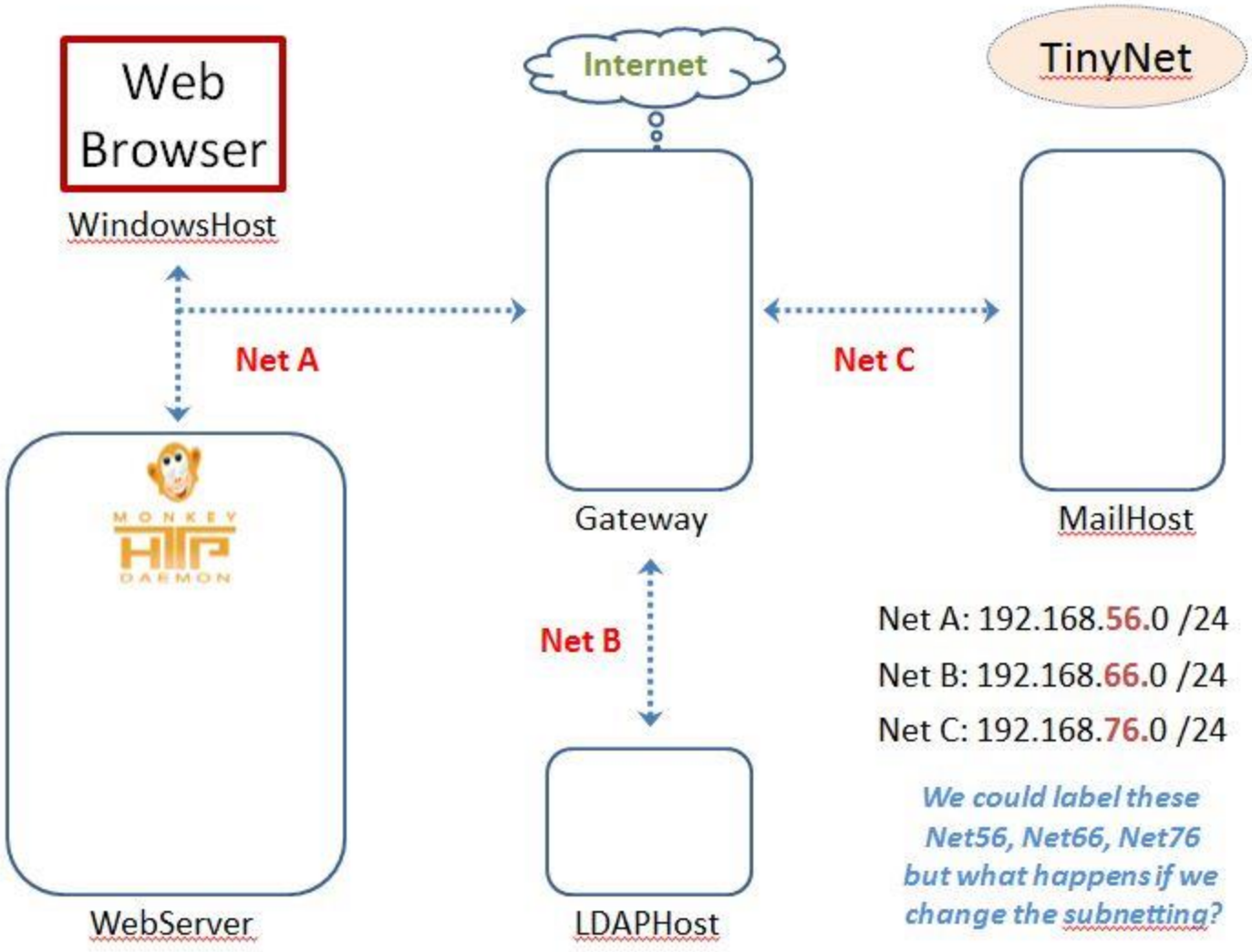
Beyond a **broadcast domain**, communication is typically through a network of intermediate switching nodes.

Switching is the process of taking an incoming frame from one interface and delivering it out through another interface.

- At **Layer 2** frames are switched based on ***MAC address***
- At **Layer 3** packets are switched based on ***IP address***



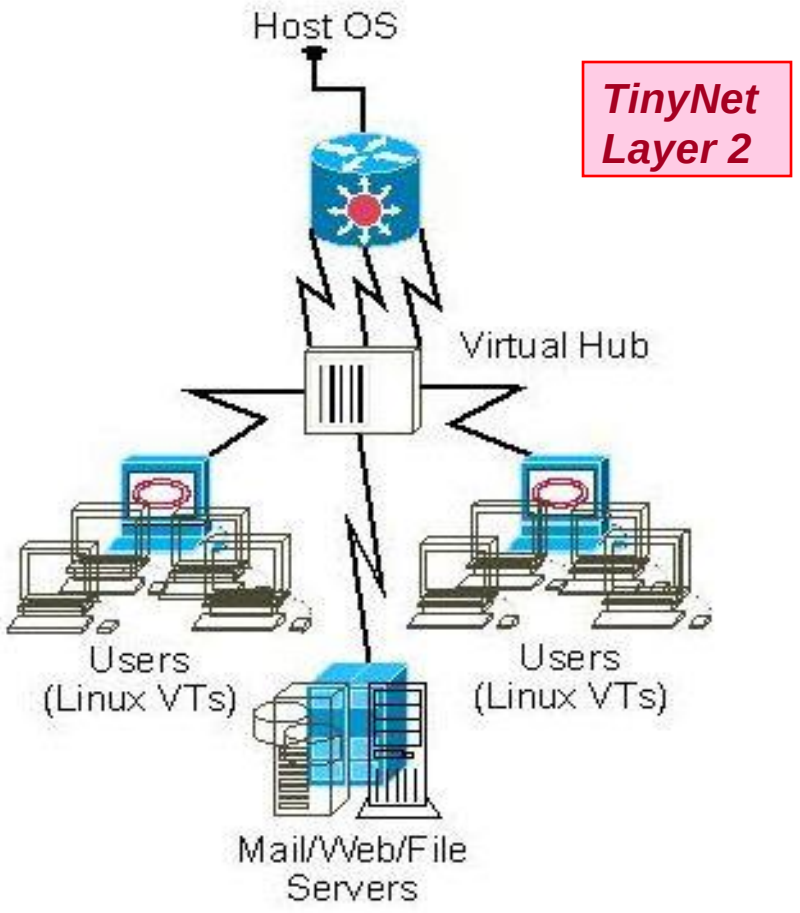
TinyNet in practice



Virtual Networking

VirtualBox provides **Layer 2** (Network Access) interconnection

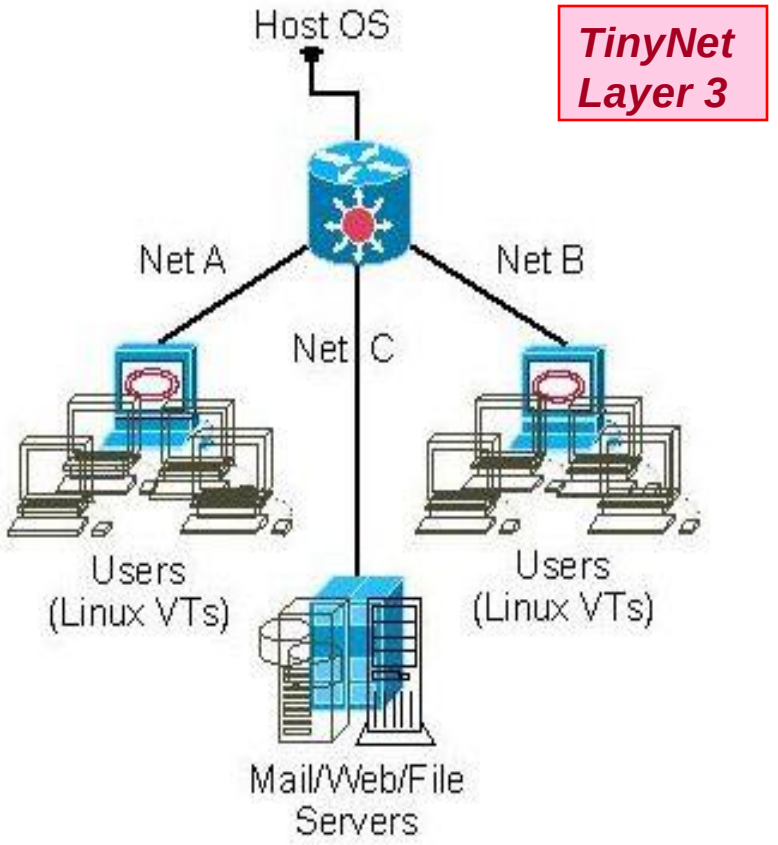
- **A *hub* broadcasts every message to every interface**
- We can watch this with a *packet sniffer* when we put the interface into *promiscuous mode*



Virtual Networking

Layer 3 (Internet) interconnection is more useful

1. **Assign an IP address to each interface**
2. **Configure a *default* or *static* route to the gateway**
3. **Gateway interconnects subnets**



Addresses

- Layer 2 addresses are put into the interface ROM by the hardware manufacturer
- Layer 3 addresses are assigned by the network administrator
  - **If users move to another building (or WAP), their device may get a new Layer 3 address, but the Layer 2 address remains the same.**

The broadcast domain is everyone who can hear a broadcast.

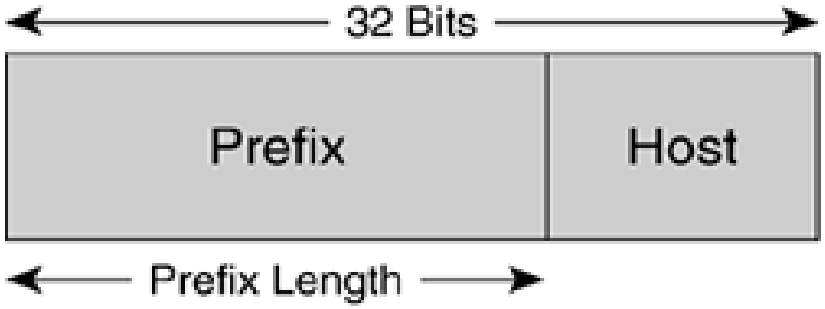
It is important to limit the size of the broadcast domain because too many broadcast frames can overwhelm endpoints, switches and routers

At layer 3 the broadcast domain is defined by the subnet mask.

At layer 2 a hub is a single broadcast domain, or switch ports are configured to define the broadcast domain (vlan tagging).

IP Addressing & Subnet Masks

- Subnet Mask is like an IPv4 Address: 32 bits long
- Specifies which part of an IP address is the network/subnet field and which part is the host field



- **The prefix portion of the mask is all 1s in binary.**
- **The host portion of the mask is all 0s in binary.**

Classless Addressing (VLSM)

- Extend the network prefix by borrowing bits from host address range
  - a Variable Length Subnet Mask (VLSM)
- An IP address is accompanied by an indication of the prefix length

  192.168.11.0 255.255.255.0

  Convert the binary expression to dotted-decimal notation

  192.168.11.0/24

  / specifies the number of ones “up front”

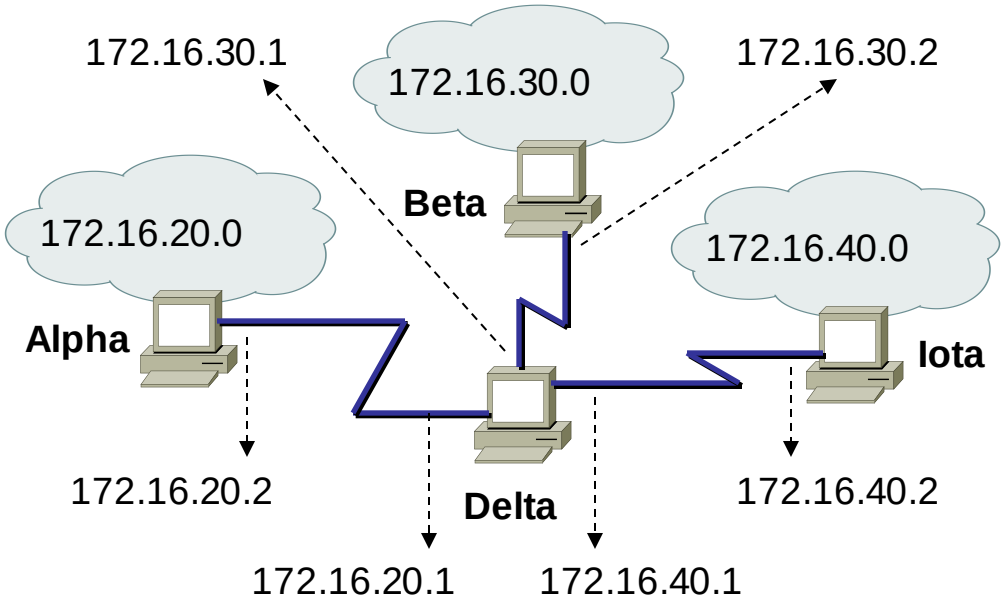
- *Contiguous subnet mask*: no 1 bit appears to the right of any 0 bit

The routing table actually has both the IP address and the netmask

You cannot tell what subnet an address belongs to without knowing the netmask!

Network	*Netmask*
172.16.20.0	255.255.255.0
172.16.30.0	255.255.255.0
172.16.40.0	255.255.255.0

This network has 3 subnets



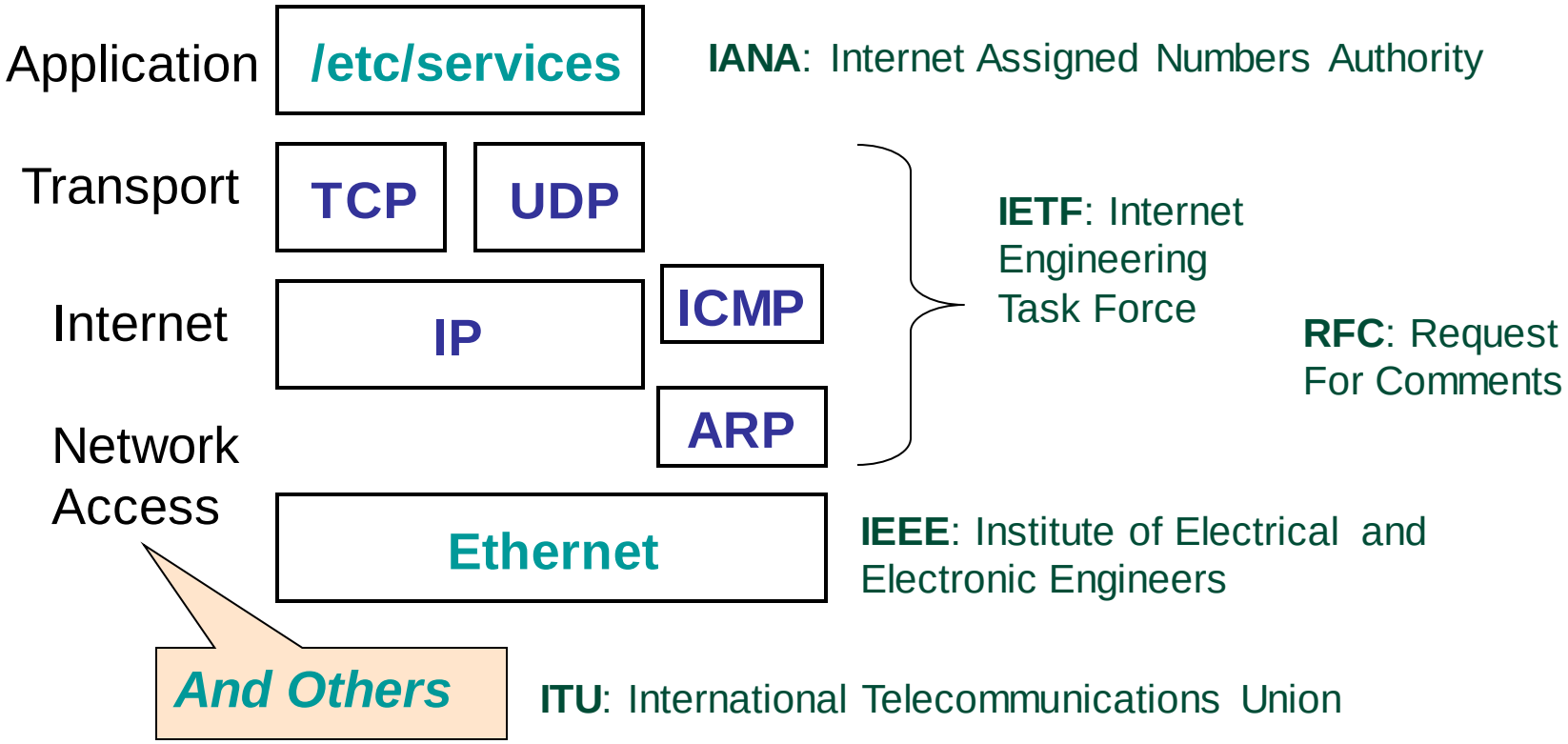
Virtual Local Area Networks (VLANs)

A logical method of segmenting a network at the data link layer (layer 2) – Also called VLAN Tagging.

- Similar to subnets.
  - However, subnets are network layer (layer 3).
- VLANs enable grouping of network hosts not on the same physical switch or multiple VLANs on the same physical switch.
- If network configuration changes, the physical cabling and devices don't need to.
- VLANs can be configured with one or more subnets.


Q
&
A

Internet Protocols and Standards



ARP - Address Resolution Protocol

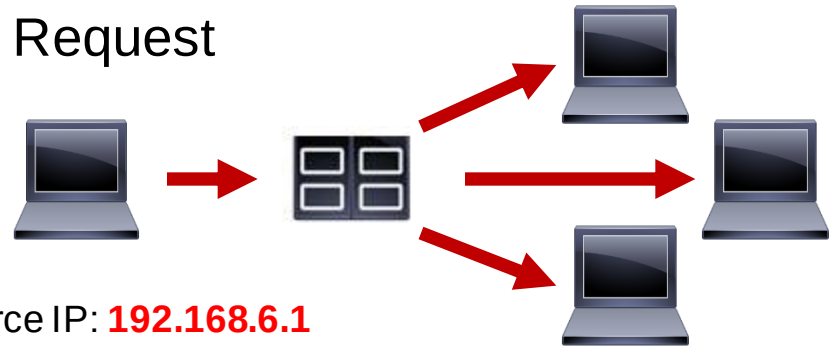
- Concerned with mapping layer 2 to layer 3 addresss, e.g., MAC address to IP address.
- The source host sends an ARP request by broadcast, asking “who has IP address A.B.C.D?”

  If the destination host (which owns A.B.C.D) sees the ARP query, it responds and sends its MAC address.

  If the destination host is not on the same local network, the router/gateway will respond and send its own MAC address.
- The source host registers the MAC address obtained and a data-link (layer 2) connection is established between the two hosts.

ARP - Address Resolution Protocol

arp Request

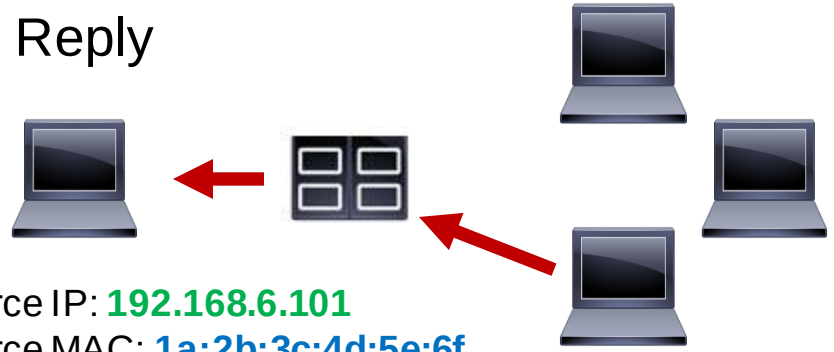


Source IP: **192.168.6.1**
Source MAC: **a1:b2:c3:d4:e5:f6**
Target IP: **192.168.6.101**
Target MAC: **00:00:00:00:00:00**

ARP Spoofing relies on the decentralized, unauthenticated, and completely trusting nature of ARP

Any reply is cached, even if no request was sent. Attackers can easily substitute their MAC and divert traffic.

arp Reply



Source IP: **192.168.6.101**
Source MAC: **1a:2b:3c:4d:5e:6f**
Target IP: **192.168.6.1**
Target MAC: **a1:b2:c3:d4:e5:f6**

ICMP - Internet Control Message Protocol

Used for gateway management:

- congestion control (source quench)
- route-change notification (redirect)
- **subnet addressing (address mask request/reply)**

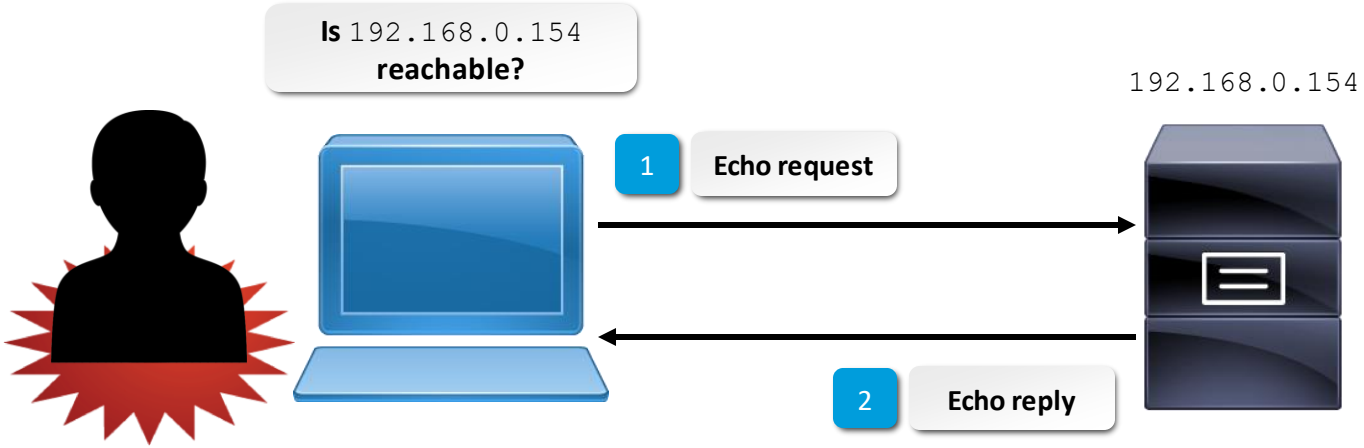
Also for general network management:

- reachability testing (echo request/reply)
- performance measuring (timestamp)

ping

Uses ICMP “echo request” and “echo reply” to check network connectivity.

- Used to check a target host for a response.
- Many systems block ICMP to prevent attacks:
  - Flood system in a Smurf attack.
  - Reconfigure routing tables with forged packets.



UDP - User Datagram Protocol

- **Connectionless** service for application level procedures
  - **Unreliable**: delivery not guaranteed & no duplication control
- Reduced overhead, least common denominator service
- **Used when one IP packet is sufficient for the whole message**
  - DNS tries to use UDP first, fallback to TCP

TCP: Transmission Control Protocol

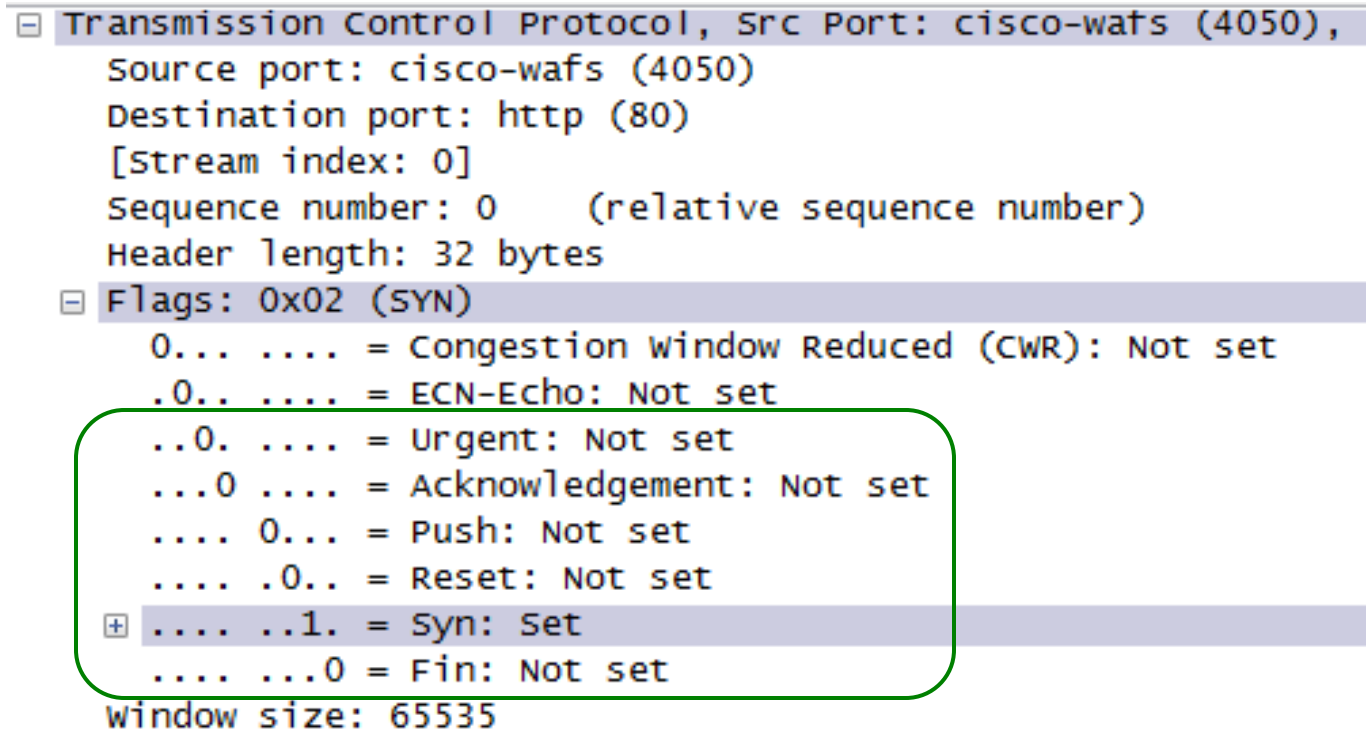
- TCP connections provide reliable delivery for messages that are too big for a single packet
- The message is broken into a number of packets before it is sent
- Packets can arrive in any order, missing packets are re-sent
- Packet sequence numbers are established during the initial connection using a “3-Way Handshake”.

- Other initial connection setup messages establish parameters of channel e.g., buffer sizes, error detection & recovery procedures.

Background: TCP

- The TCP segment (packet) header has six **flag bits** that can be set independently.
- to remember them in order

  Unskilled **A**ttackers **P**ester **R**eal **S**ecurity **F**olks.



http://www.lovemytool.com/blog/2010/07/practical-tcp-series-tcp-flags-by-chris-greer.html

Background: TCP

Four flag bits can be set to describe the state of the connection:

- SYN (SYNchronise) is used for starting a connection
- ACK (ACKnowledge) is used to confirm packets are received
- FIN (FINish) is used for ending a connection
- RST (ReSeT) is used to denote no service on the port (closed)

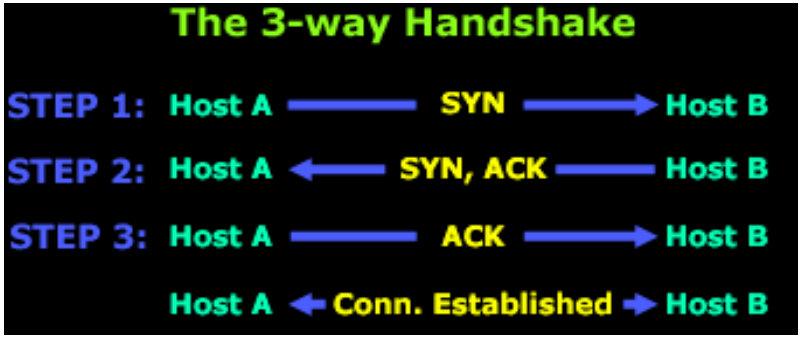
- PSH (PuSH) and URG (URGent) are used to ensure priority over other packets for processing when a packet is received.
- The CWR and ECN bits may be used together by a client and server that can use RFC 3168 Explicit Congestion Notification.

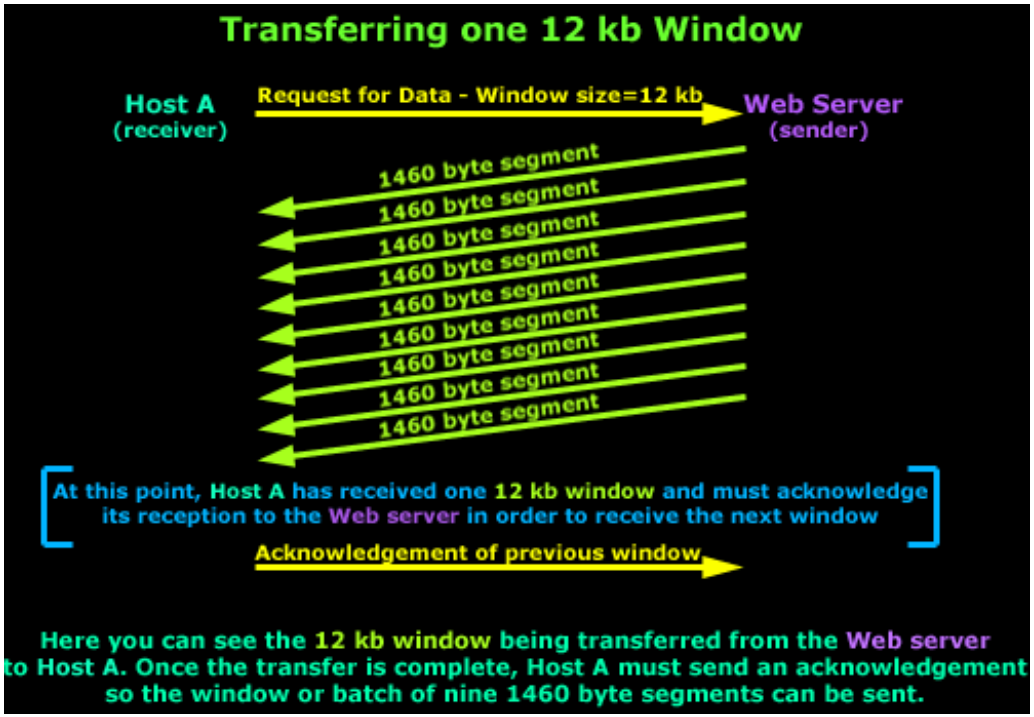
Background: TCP

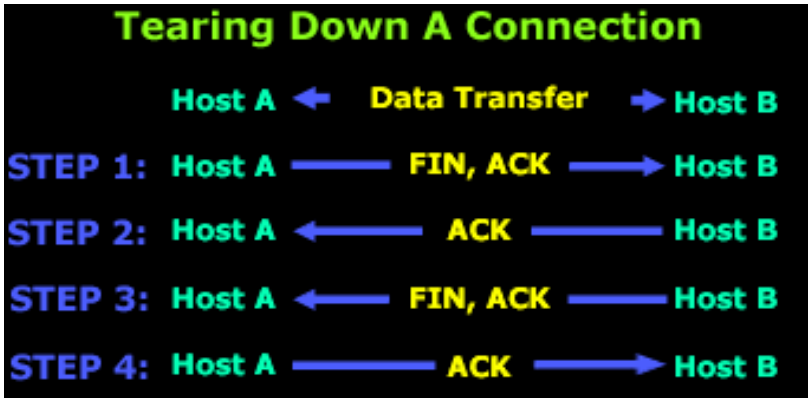
The initial connection with a TCP service is established with the "TCP 3 way handshake".

- First a SYN is sent to a port that has a service bound to it (an open port). Typical examples are HTTP (port 80), SMTP (port 25), or SSH (port 22).
- The server side will see the SYN and respond with SYN + ACK, with the client answering with an ACK. This completes the set up and the data of the service protocol can now be communicated.
- After this, an ACK is sent after receiving each "window size" group of packets (details are beyond our scope, we have nice graphic).
- When a host sends a FIN to close a connection, it may continue to receive data until the remote host has also closed the connection, although this only occurs under certain circumstances.

Background: TCP







http://www.firewall.cx/networking-topics/protocols/tcp/136-tcp-flag-options.html
http://www.firewall.cx/networking-topics/protocols/tcp/137-tcp-window-size-checksum.html


Q
&
A

Ports and Port Ranges

Port: The endpoint of a logical network connection.

- Client computers connect to server programs through a designated port.
- Port is a "Layer 4" concept – TCP header
- All ports assigned are between the numbers 0 and 65535.

Port	Service	Secure	Port
20	Telnet	SSH	**22**
25	SMTP	SMTPS	**465**
80	HTTP	HTTPS	**443**
143	IMAP	IMAPS	**993**
389	LDAP	LDAPS	**636**

Port	Service
53	DNS
67	DHCP (server)
68	DHCP (client)
587	Submission

Service names and port numbers

- Service names and port numbers are used to distinguish between different services that run over TCP and UDP (transport layer)
- A port is actually just a 16 bit number used as an identifier
- The registration procedures for service names and port numbers are described in [RFC6335].
- Service names are assigned by IANA with a first-come, first-served process.

Transport Protocol Addresses: TCP & UDP Port Numbers

/etc/services

```
# This file contains port numbers for well-known services defined by IANA
# Format:
# <service name>  <port number>/<protocol>  [aliases...]   [#<comment>]
discard             9/tcp    sink null
discard             9/udp    sink null
qotd               17/tcp    quote          #Quote of the day
qotd               17/udp    quote          #Quote of the day
ftp-data           20/tcp                   #FTP, data
ftp                21/tcp                   #FTP. control
telnet             23/tcp
smtp               25/tcp    mail           #Simple Mail Transfer Protocol
time               37/tcp    timserver
time               37/udp    timserver
domain             53/tcp                   #Domain Name Server
domain             53/udp                   #Domain Name Server
bootps             67/udp    dhcps          #Bootstrap Protocol Server
bootpc             68/udp    dhcpc          #Bootstrap Protocol Client
tftp               69/udp                   #Trivial File Transfer
finger             79/tcp
http               80/tcp    www www-http   #World Wide Web
```

- Port numbers are assigned based on three ranges:
- The Well Known or System Ports (0-1023)
  - **Ports under 1024 restricted to root**
- The Registered or User Ports (1024-49151),
- The Dynamic and/or Private Ports (49152-65535);

System Ports are assigned by IETF for standards-track protocols, User Ports are assigned by IANA, and dynamic ports are not assigned.


Q
&
A

netstat – Network Statistics

netstat –a	(connections)
netstat –i	(interfaces)
netstat –nr	(routing)
netstat –tulp	(tcp+udp listening ports)

Consulting the man pages for lsof and netstat is highly recommended.

These tools are flexible and can provide a wealth of information about network services and configuration.

Finding Listening Sockets

- If you want to know what process has a connection open to or from the Internet host aaa.bbb.ccc

```
lsof -i@aaa.bbb.ccc
```

- You can add in a particular protocol and a specific port number or service name

```
lsof -iTCP@aaa.bbb.ccc:http
```

Listing Open Files

- If you're interested in knowing what files the processes owned by a particular login name have open

  `lsof -u<login>` ***or*** `lsof -u<User ID number>`

- Run this on an NFS client to list all files open by processes on the client that are on remote NFS file systems

  `lsof -N`

  – Note that lsof can only examine the processes running on the machine where it is called, so if this is run on the server it will not list files opened by clients.


Q
&
A