Basic Networking Design and Configuration

Understanding networks

- What happens when you type “www.google.com” into the browser URL bar and hit enter?

Understanding networks

- What happens when you type “www.google.com” into the browser URL bar and hit enter?
  - Client sends a DNS request to determine the IP address of the web server called www.google.com
  - Client sends an HTTP GET request to web server’s IP address
  - Server responds with the code for the Google homepage
  - Browser renders the code in a graphical interface

Understanding networks

- What happens when you type “www.google.com” into the browser URL bar and hit enter?
  - Client sends a DNS request to determine the IP address of the web server called www.google.com
  - Client sends an HTTP GET request to web server’s IP address
  - Server responds with the code for the Google homepage
  - Browser renders the code in a graphical interface

- How does the client know which DNS server to use?
- How does the request get to the DNS server and back?
- How does the client know how to talk to the network?

OSI Model

OSI Model

- OSI Model is a conceptual model that describes the functions of a communication system by dividing it into *abstraction layers*

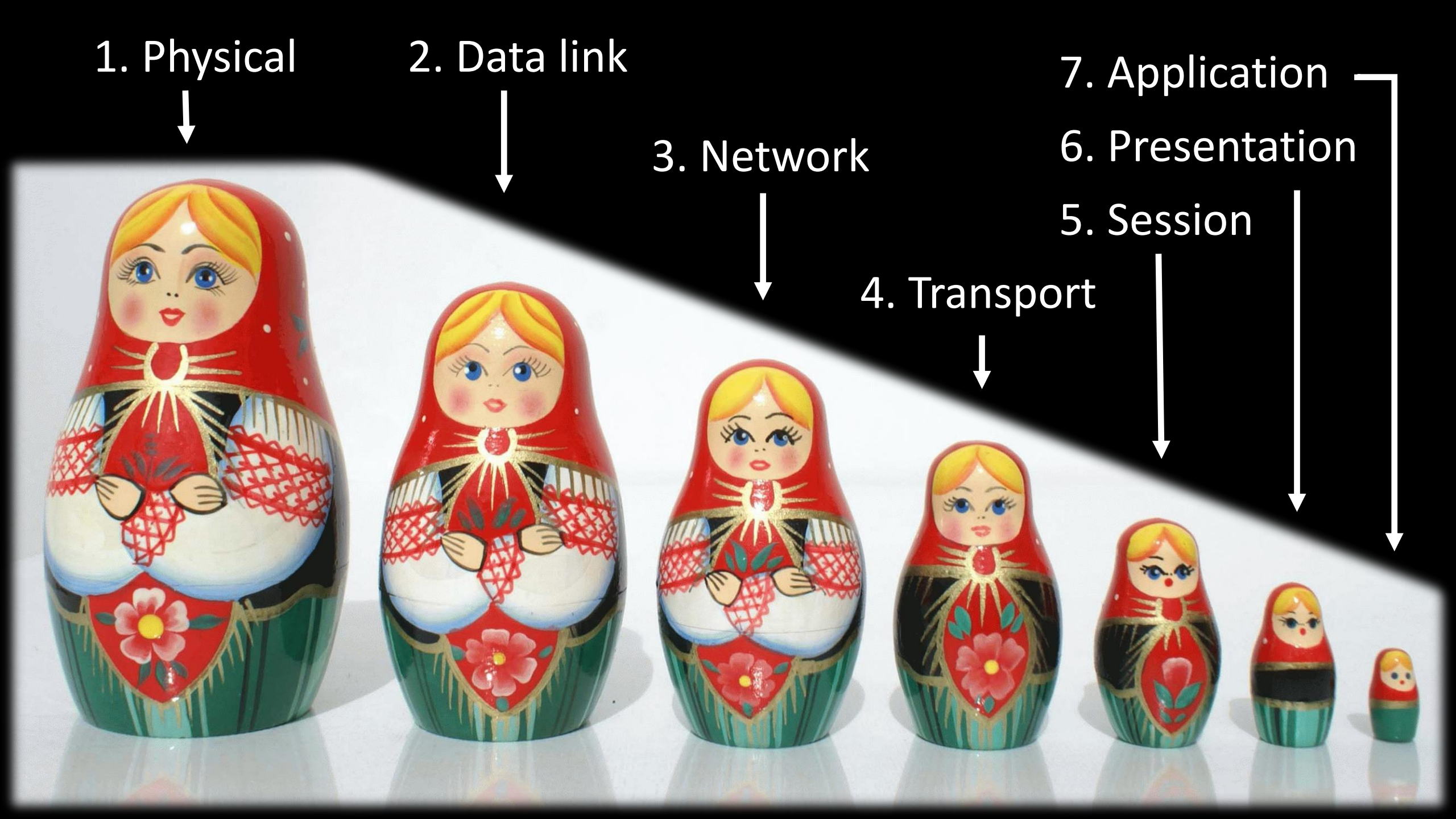
What is the OSI Model?

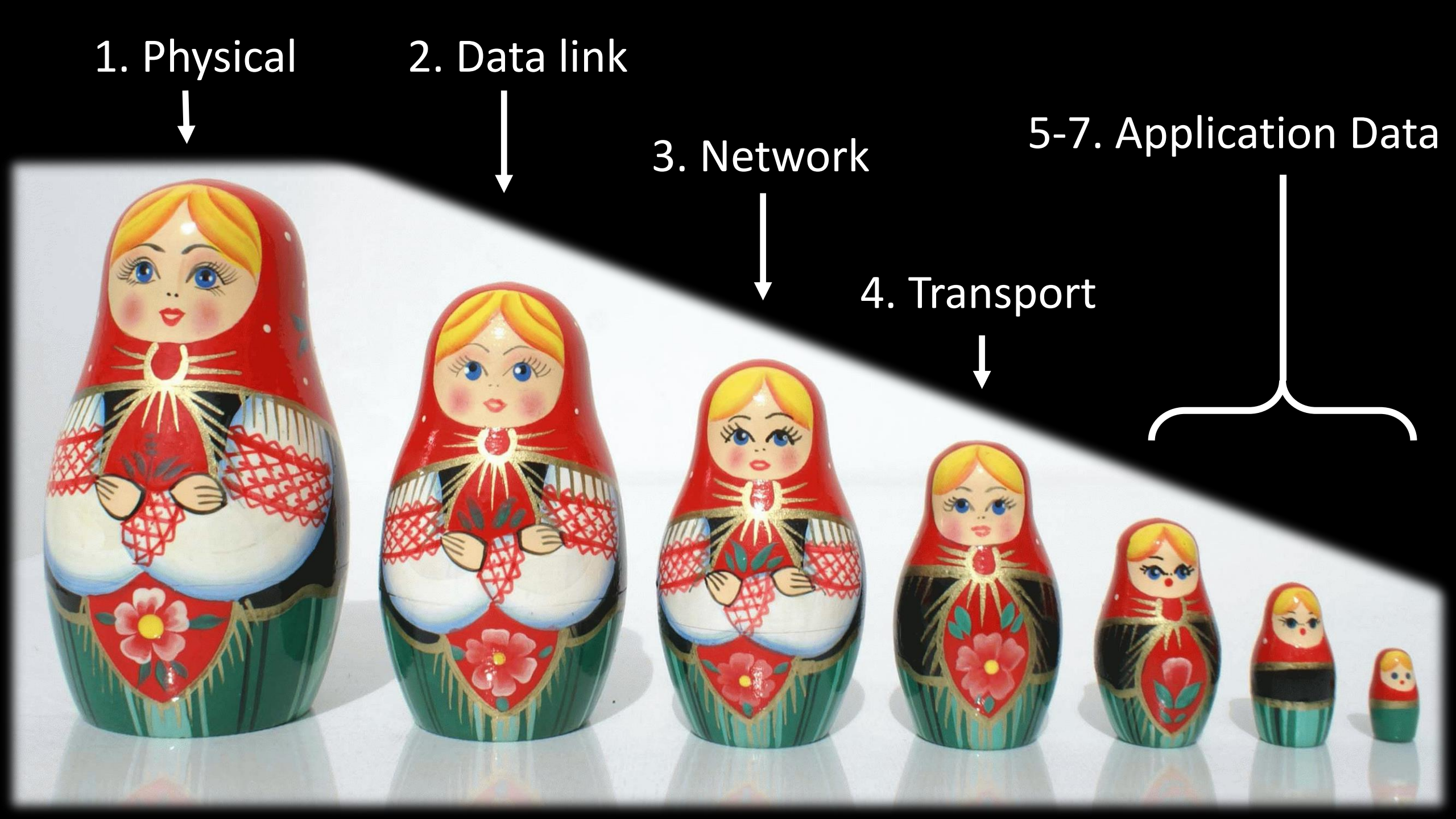
- OSI Model is a conceptual model that describes the functions of a communication system by dividing it into *abstraction layers*
- Abstraction layers – each layer has a function that depends on the layer below, but doesn’t have to know how that lower layer works
- Abstraction allows for easy interoperability between systems
  - Web browser does not have to know what a MAC address is
  - Network switch does not have to interpret HTTP
  - Fiber patch cable doesn’t need to have an IP address

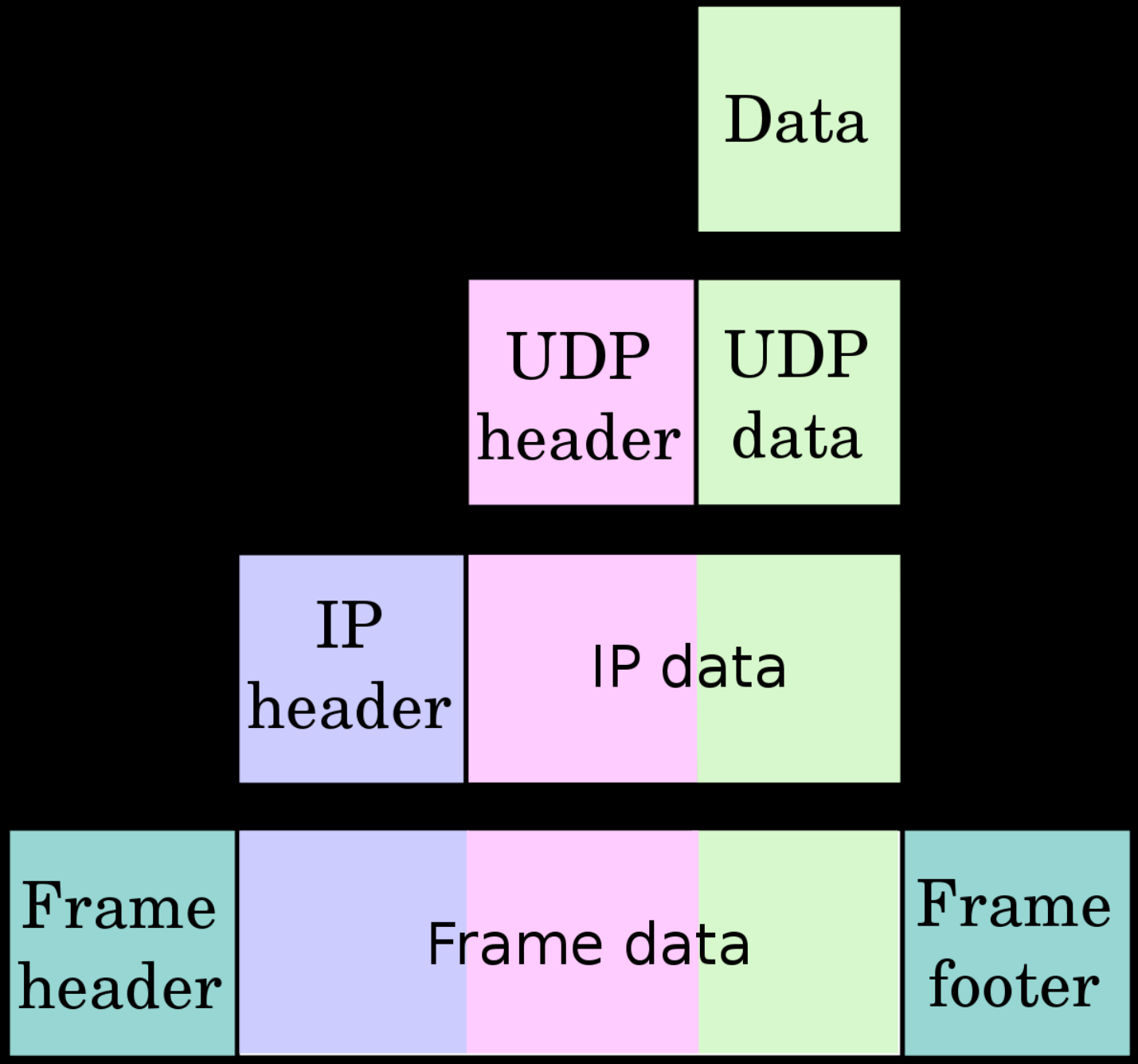
Layers of the OSI Model

Layers of the OSI Model

7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data link
1. Physical


1. Physical
2. Data link
3. Network
4. Transport
5. Session
6. Presentation
7. Application

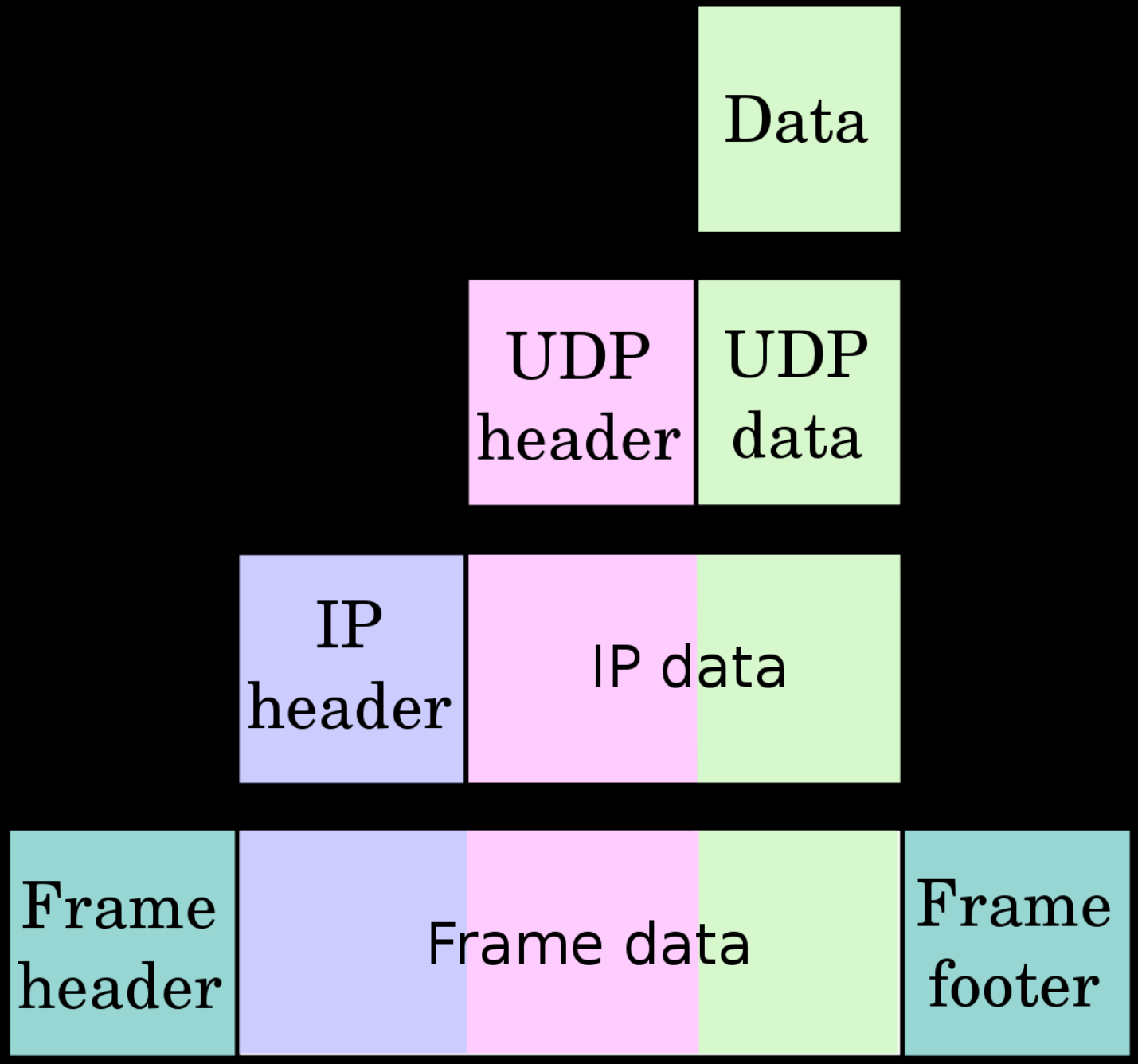

1. Physical
2. Data link
3. Network
4. Transport
5-7. Application Data

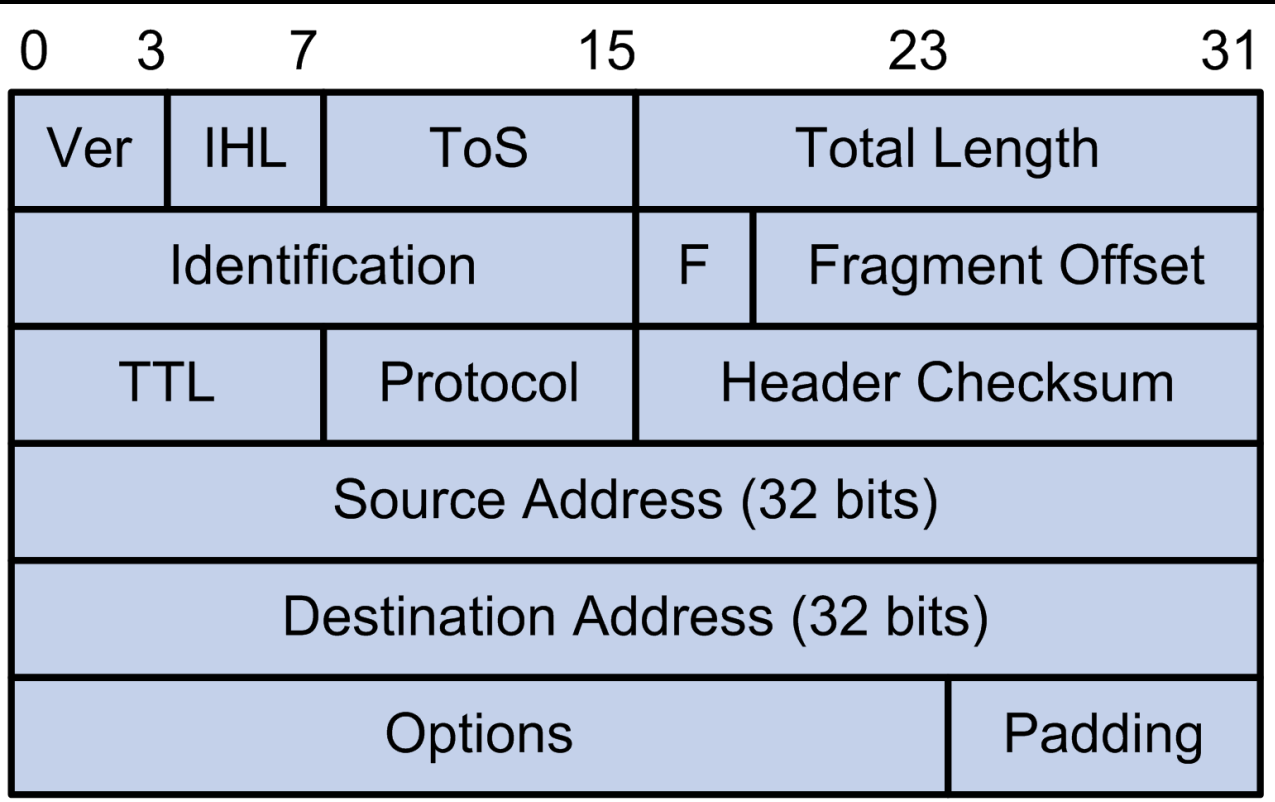

Data
UDP header
UDP data
IP header
IP data
Frame header
Frame data
Frame footer
Layer 5+ - Application
Layer 4 - Transport
Layer 3 - Network
Layer 2 - Link

UDP header

UDP datagram header

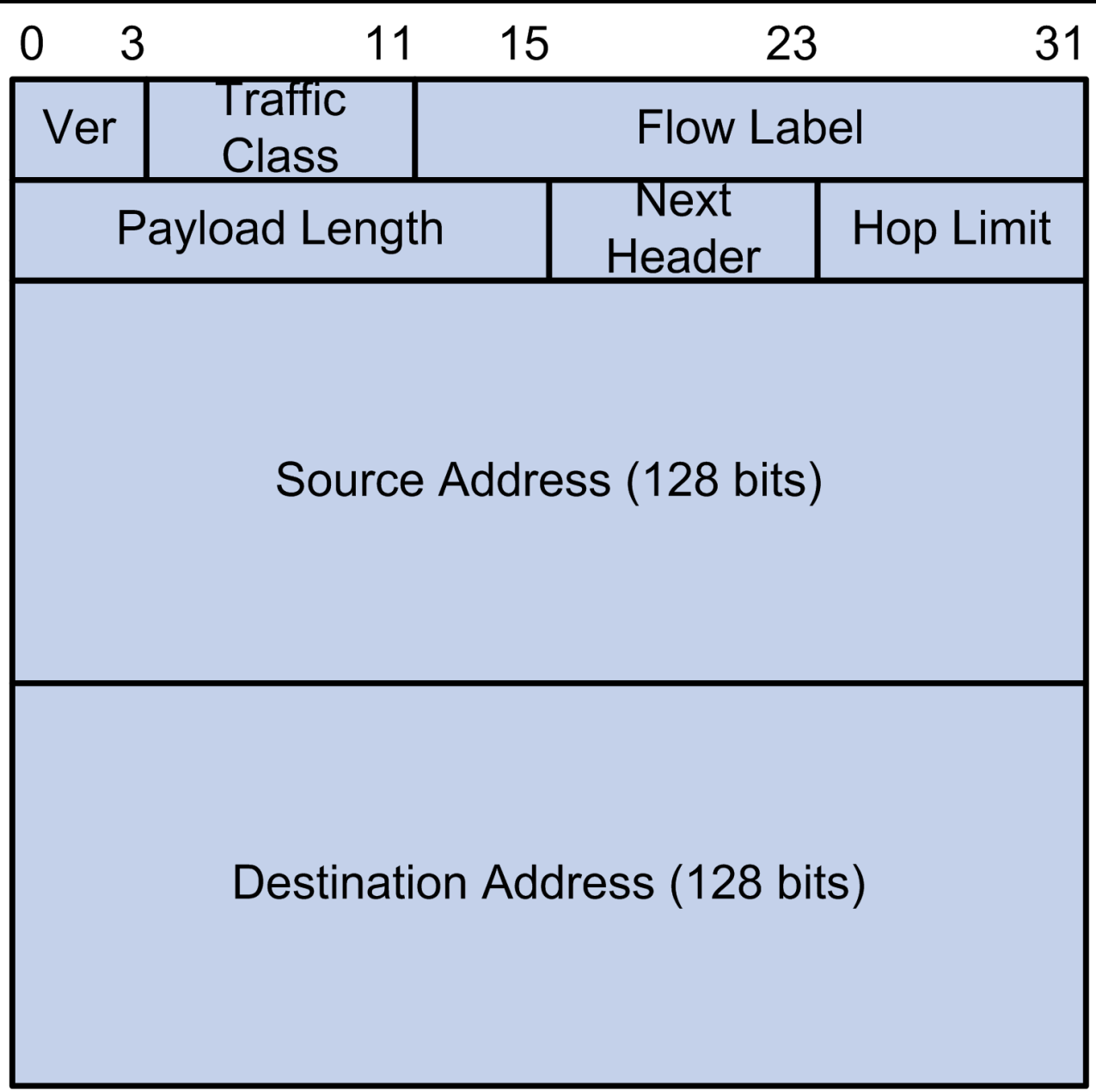
Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Length																Checksum															


Data
UDP header
UDP data
IP header
IP data
Frame header
Frame data
Frame footer
Layer 5+ - Application
Layer 4 - Transport
Layer 3 - Network
Layer 2 - Link

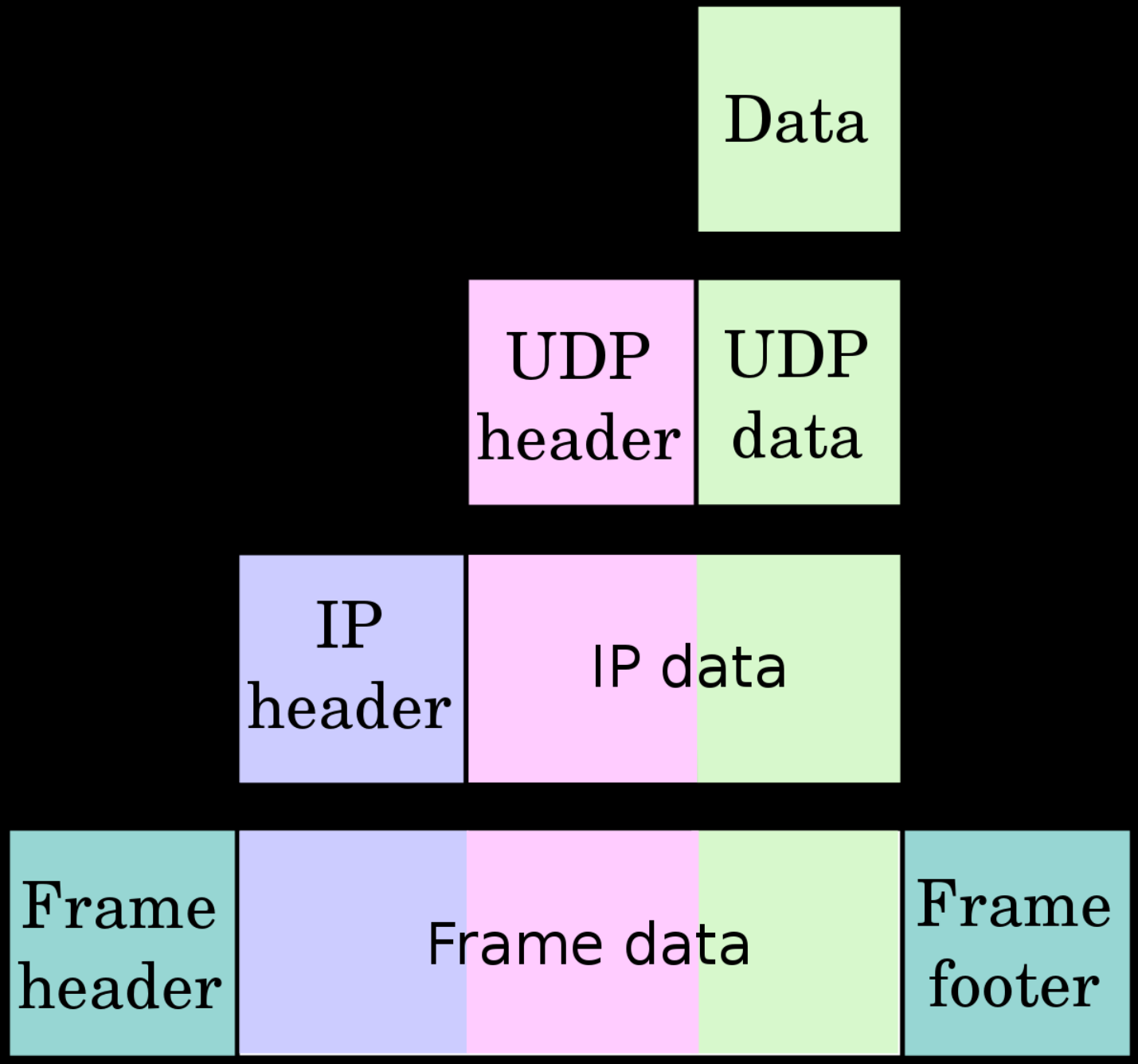


IPv4 header

IP header



Basic IPv6 header


Data
UDP header
UDP data
IP header
IP data
Frame header
Frame data
Frame footer
Layer 5+ - Application
Layer 4 - Transport
Layer 3 - Network
Layer 2 - Link

Ethernet frame

802.3 Ethernet packet and frame structure

Layer	Preamble	Start frame delimiter	MAC destination	MAC source	802.1Q tag (optional)	Ethertype (Ethernet II) or length (IEEE 802.3)	Payload	Frame check sequence (32-bit CRC)	Interpacket gap
	7 octets	1 octet	6 octets	6 octets	(4 octets)	2 octets	46-1500 octets	4 octets	12 octets
Layer 2 Ethernet frame			← 64–1522 octets →						
Layer 1 Ethernet packet & IPG	← 72–1530 octets →								← 12 octets →

	Layer	Data unit	Protocols / Related terms
7	Application		
6	Presentation		
5	Session	Session	
4	Transport	Segment / Datagram	
3	Network	Packet	
2	Data link	Frame	
1	Physical	Symbol / Bits	

	Layer	Data unit	Protocols / Related terms
7	Application		HTTP, SMTP, IMAP, LDAP, FTP, DNS
6	Presentation		TLS, SSL, AFP, MIME, Character Set, Compression
5	Session	Session	SMB, SOCKS, NetBIOS, Session control
4	Transport	Segment / Datagram	TCP, UDP, iSCSI, NetBIOS, IPsec, ESP, AH, TCP/IP, Ports
3	Network	Packet	IPv4, IPv6, ICMP, IPX, TCP/IP, ARP, NDP, Routing
2	Data link	Frame	MAC, ARP, VLAN, LLDP/CDP/FDP, Ethernet (802.3), Wi-Fi (802.11), L2TP, STP, VTP, Token ring, LACP, Switching
1	Physical	Symbol / Bits	Electrical signals, RF waves, light impulses, 100BASE-TX, 1000BASE-T, modulation, duplex, DSL, ISDN, T1, RS-232

	Layer	Data unit	Network equipment
7	Application		
6	Presentation		
5	Session	Session	
4	Transport	Segment / Datagram	
3	Network	Packet	
2	Data link	Frame	
1	Physical	Symbol / Bits	

	Layer	Data unit	Network equipment
7	Application		Firewall (application)
6	Presentation		
5	Session	Session	
4	Transport	Segment / Datagram	Router, Firewall (port)
3	Network	Packet	Router (IP)
2	Data link	Frame	Switch (MAC)
1	Physical	Symbol / Bits	PHY, network interface controller, transceiver

	Layer	Ingredients	Scope
3	Network	Source and destination IP address	Global / universal * *Example: your computer connecting to Google through the Internet* *sort of
2	Data link	Source and destination MAC address	A single Layer 2 segment, commonly called a LAN, VLAN, or broadcast domain. *Example: several computers connected by an unmanaged switch (not VLAN-aware)*
1	Physical	Electrical signals in copper or light in an optical fiber (ignoring Wi-Fi for now)	A single cable or physical connection between two devices. *Example: two computers connected by a Category 6 Ethernet cable*

Address types

MAC Address

- 48-bit interface address written in hexadecimal, usually with a colon or hyphen between each byte
- `E0-4F-43-8B-8F-4D`
- `E0:4F:43:8B:8F:4D`
- `E04F438B8F4D`
- `11100000 01001111 01000011 10001011 10001111 01001101` (binary)
- 281.5×10^{12} permutations (281.5 trillion)

Address types

IPv4 Address

- 32-bit address written as 4 bytes (“octets”) in decimal, separated by periods
- `192.168.1.101`
- `11000000 10101000 00000001 01100101` (binary)
- 4.3×10^9 permutations (4.3 billion)

Address types

IPv6 Address

- 128-bit address written in hexadecimal as 8 two-byte “chunks” separated by colons
- `2620:01d5:0001:1148:7598:0af6:a6c0:c68e`
- `00100110 00100000 00000001 11010101`
  `00000000 00000001 00010001 01001000`
  `01110101 10011000 00001010 11110110`
  `10100110 11000000 11000110 10001110` (binary)
- 340×10^{36} permutations (340 undecillion)

  (that’s about 80 billion billion billion times the number of IPv4 addresses)

Address types

IPv6 Address

- IPv6 addresses may be abbreviated:
  - Leading zeros may be omitted from each chunk
  - The longest sequence of adjacent zeros may be compressed to ::

- 2620:01d5:0001:1148:7598:0af6:a6c0:c68e
- 2620:1d5:1:1148:7598:af6:a6c0:c68e (leading zeros omitted)

- 2620:01d5:0001:1148:0000:0000:0000:0001
- 2620:15d:1:1148::1 (leading zeros omitted, sequential zeros compressed)

IP networks and subnets

What defines an IP network?

- An IPv4 network is defined by a network ID and a subnet mask or mask length
- An IPv6 network is defined by a network prefix and a prefix length

network ID ⇔ network prefix mask length ⇔ prefix length

Network ID / Prefix	Subnet mask	Prefix length
`192.168.1.0`	`255.255.255.0`	24
`2620:1d5:1:1148::`	`ffff:ffff:ffff:ffff::`	64

IP networks and subnets

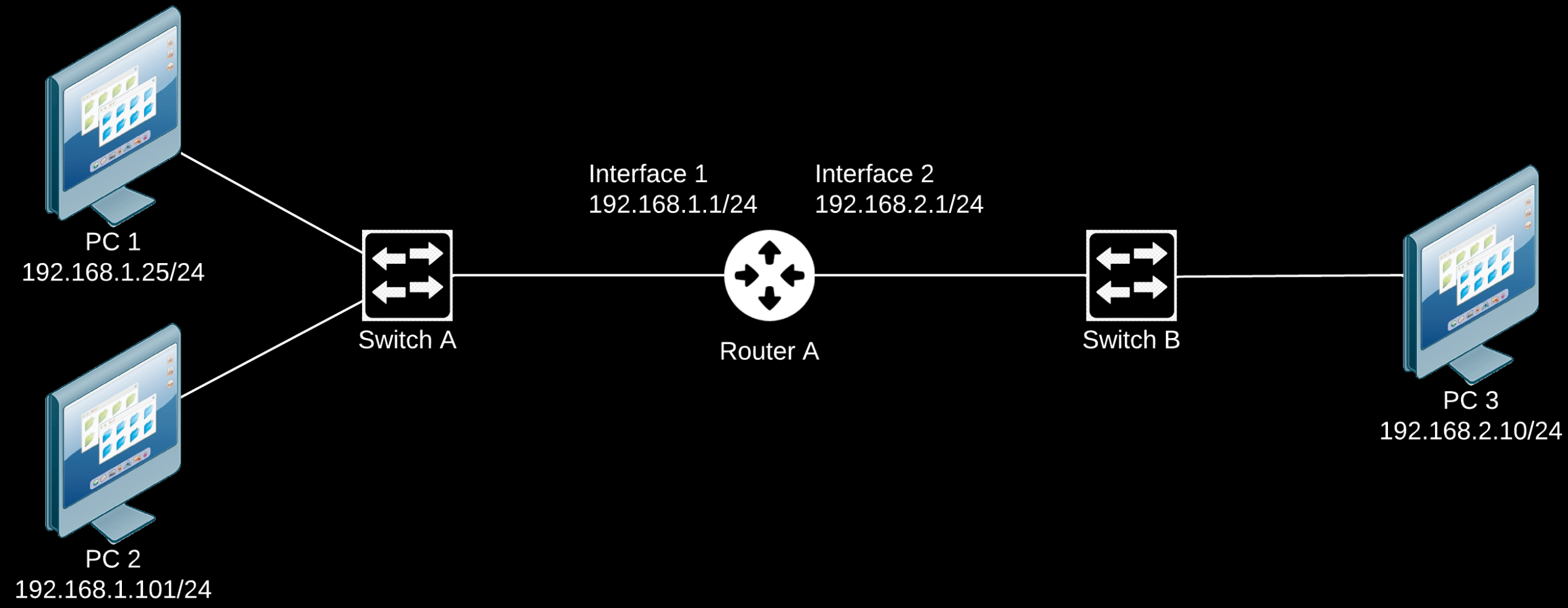
Subnet mask and mask length

- Network engineers often use CIDR notation (mask length) to describe IPv4 subnet masks more concisely
- `255.255.255.0` to binary → `11111111 11111111 11111111 00000000`
- Count the ones to find that the mask length is 24

255.255.255.0	11111111 11111111 11111111 00000000	24
255.255.254.0	11111111 11111111 11111110 00000000	23
255.255.252.0	11111111 11111111 11111100 00000000	22
255.255.248.0	11111111 11111111 11111000 00000000	21
255.255.240.0	11111111 11111111 11110000 00000000	20
...		
255.255.0.0	11111111 11111111 00000000 00000000	16

Communication between IP addresses

- Hosts can communicate directly with other hosts in the same IP network/subnet
- To communicate with another host outside the subnet, the host will need the help of a router
- To determine if an IP address is local to its subnet, the host performs a *bitwise and* operation with the IP addresses and subnet mask


PC 1
192.168.1.25/24
PC 2
192.168.1.101/24
Switch A
Interface 1
192.168.1.1/24
Router A
Interface 2
192.168.2.1/24
Switch B
PC 3
192.168.2.10/24

Communication between IP addresses

```
Source IP              192.     168.       1.      25 -> binary
                   11000000 10101000 00000001 00011001
Subnet mask            255.     255.     255.       0 -> binary
                   11111111 11111111 11111111 00000000
Bitwise AND        11000000 10101000 00000001 00000000 -> decimal
Network ID             192.     168.       1.       0
```

Communication between IP addresses

```
Source IP              192.     168.       1.      25 -> binary
                   11000000 10101000 00000001 00011001
Subnet mask            255.     255.     255.       0 -> binary
                   11111111 11111111 11111111 00000000
Bitwise AND        11000000 10101000 00000001 00000000 -> decimal
Network ID             192.     168.       1.       0

Destination IP         192.     168.       1.     101
Subnet mask            255.     255.     255.       0
Network ID             192.     168.       1.       0
```

Subnet mask of *source* host!

Network ID of source and destination are the same, so they are in the same subnet!

Communication between IP addresses

Network ID of source and destination are the same, so they are in the same subnet, and the hosts can communicate directly within the subnet.

The source host will generate layer 3 packets with the destination IP of the target host, and layer 2 frames with the destination MAC of the target host.

In IPv4, the source host will use ARP (address resolution protocol) to learn the MAC address corresponding with the target IP address.

Communication between IP addresses

Source IP	192.	168.	1.	25
Subnet mask	255.	255.	255.	0
Network ID	192.	168.	1.	0
Destination IP	192.	168.	2.	10
Subnet mask	255.	255.	255.	0
Network ID	192.	168.	2.	0

Subnet mask of *source* host!

Network ID of source and destination are different, so they are not in the same subnet!

Communication between IP addresses

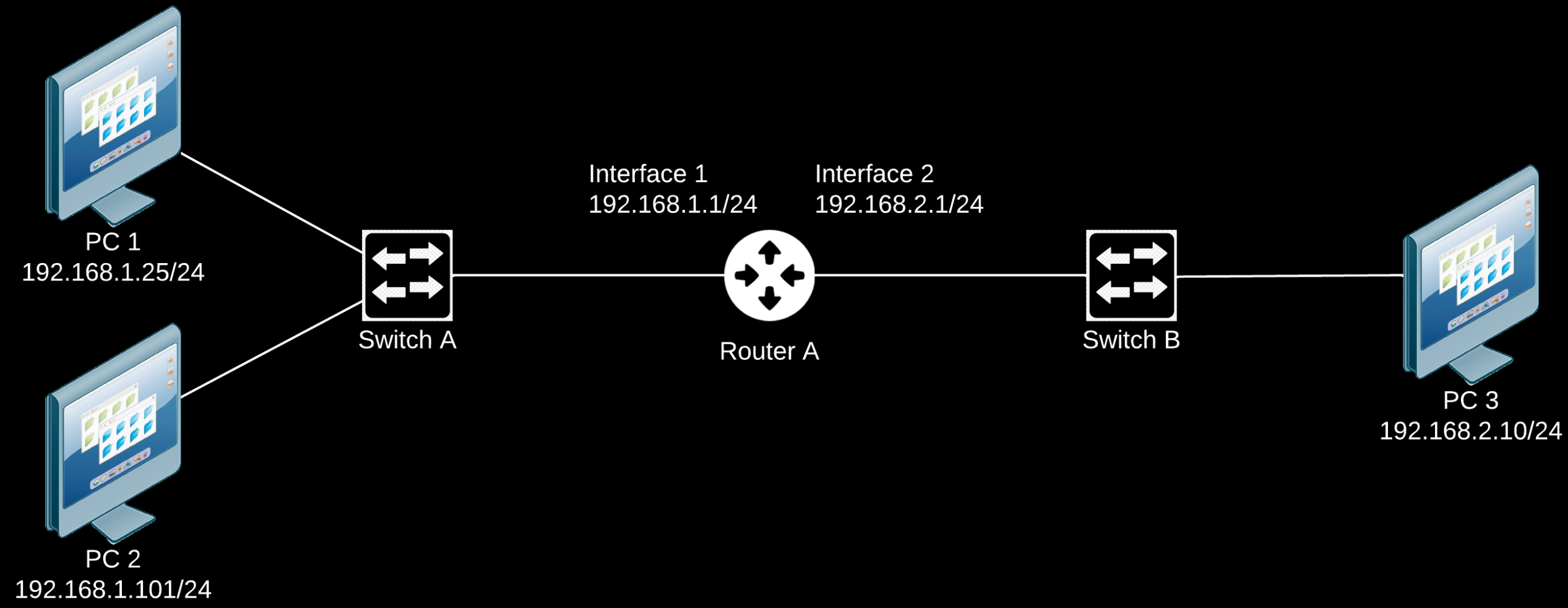
Network ID of source and destination are not the same, so they are not in the same subnet.

The source host checks its routing table to see if it has a route to 192.168.2.10.

On a computer, the only route is typically a default route, called the “default gateway”.

The source host will generate layer 3 packets with the destination IP of the target host, and layer 2 frames with the destination MAC of the default gateway.

In IPv4, the source host will use ARP (address resolution protocol) to learn the MAC address corresponding with the default gateway.


PC 1
192.168.1.25/24
PC 2
192.168.1.101/24
Switch A
Interface 1
192.168.1.1/24
Router A
Interface 2
192.168.2.1/24
Switch B
PC 3
192.168.2.10/24

Communication between IP addresses

PC 1 generates a layer 3 packet with its own source IP of 192.168.1.25 and a destination IP of 192.168.2.10 (PC 3)

PC 1 compares the source and destination subnets. The destination is in a different subnet, so PC 1 checks its routing table to find a next hop that can reach PC 3. The packet will be forwarded to the default gateway, Router A Interface 1.

At layer 2, PC 1 wraps the packet in a frame with its own MAC address as the source, and a destination MAC address of Router A Interface 1

When the L2 frame reaches Router A, the L3 packet is unwrapped (L2 frame header is discarded), and Router A examines the destination IP of the packet

Router A checks its routing table for a route to 192.168.2.10, and finds one pointing to Interface 2

Router A wraps the packet in a frame with its own Interface 2 MAC address as the source, and a destination MAC address of PC 3, and forwards the frame out Interface 2

Communication between IP addresses

What did you notice?

Communication between IP addresses

What did you notice?

- Source and destination IP address of the layer 3 packet remained the same for the entire journey
- Source and destination MAC address changed each time the packet got encapsulated in a new layer 2 frame

Conclusions?

- MAC address is only valid/helpful within a layer 2 segment
- Source and destination IP addresses are valid for end-to-end communication across multiple subnets and layer 2 segments (aka, through routers)

Routers

How do routers know where to forward packets?

- A router has a “connected route” for every router interface that is in a subnet, so it knows how to route those packets
- For packets with a destination that is not directly connected to the router, the router must have a route in its routing table for the destination (or the packet is discarded):
  - Might be a default route, just like the PC has for its default gateway
  - Might be a static route, when the engineer has specified where to send packets for a certain destination
  - Might be a route learned from a routing protocol, a mechanism that routers use to share routing information with other routers automatically

Why segment?

Why segment?

Efficiency and reliability

- Layer 2 segments are broadcast domains
  - A broadcast is message that must be delivered to every host in the broadcast domain
  - Broadcasts are used by ARP and DHCP, and other protocols
  - Putting many hosts in a single layer 2 segment can create a large volume of broadcast traffic, and can even make the network too busy to handle user traffic
  - Carving layer 2 segments limits broadcast domains to manageable sizes
- Switches must learn and store the MAC address of every device in the layer 2 segment
  - Switches have finite memory resources and can only learn a certain number of MAC addresses
  - Creating layer 2 segments limits the number of MAC address each switch needs to learn
- Segmenting creates smaller failure domains
  - It is easier to troubleshoot an issue when you an identify the scope

Why segment?

Security

- Segmentation makes it easier to control communication between hosts
  - Rather than being able to communicate directly, hosts in different subnets must communicate through a router (and possibly a firewall), which may apply security policy.
- Segmentation helps avoid spoofing or impersonation
  - Hosts in one subnet cannot easily impersonate hosts in another subnet

Organization and management

- Segmentation helps to keep the network organized
- Grouping similar devices or users together makes it easier to apply the correct policies

How to segment?

Layer 2 – VLAN

- VLAN allows a single switch to handle multiple separate layer 2 segments
- VLAN is implemented as an additional header in the layer 2 frame
- 12-bit header field, permitting 4094 VLAN IDs (0 and 4095 are reserved)

VLAN Tagging

- Frames may be tagged or untagged
- An untagged frame has no VLAN ID in the frame header
- A tagged frame has a VLAN ID in the range of 1 - 4094 in the header

How to segment?

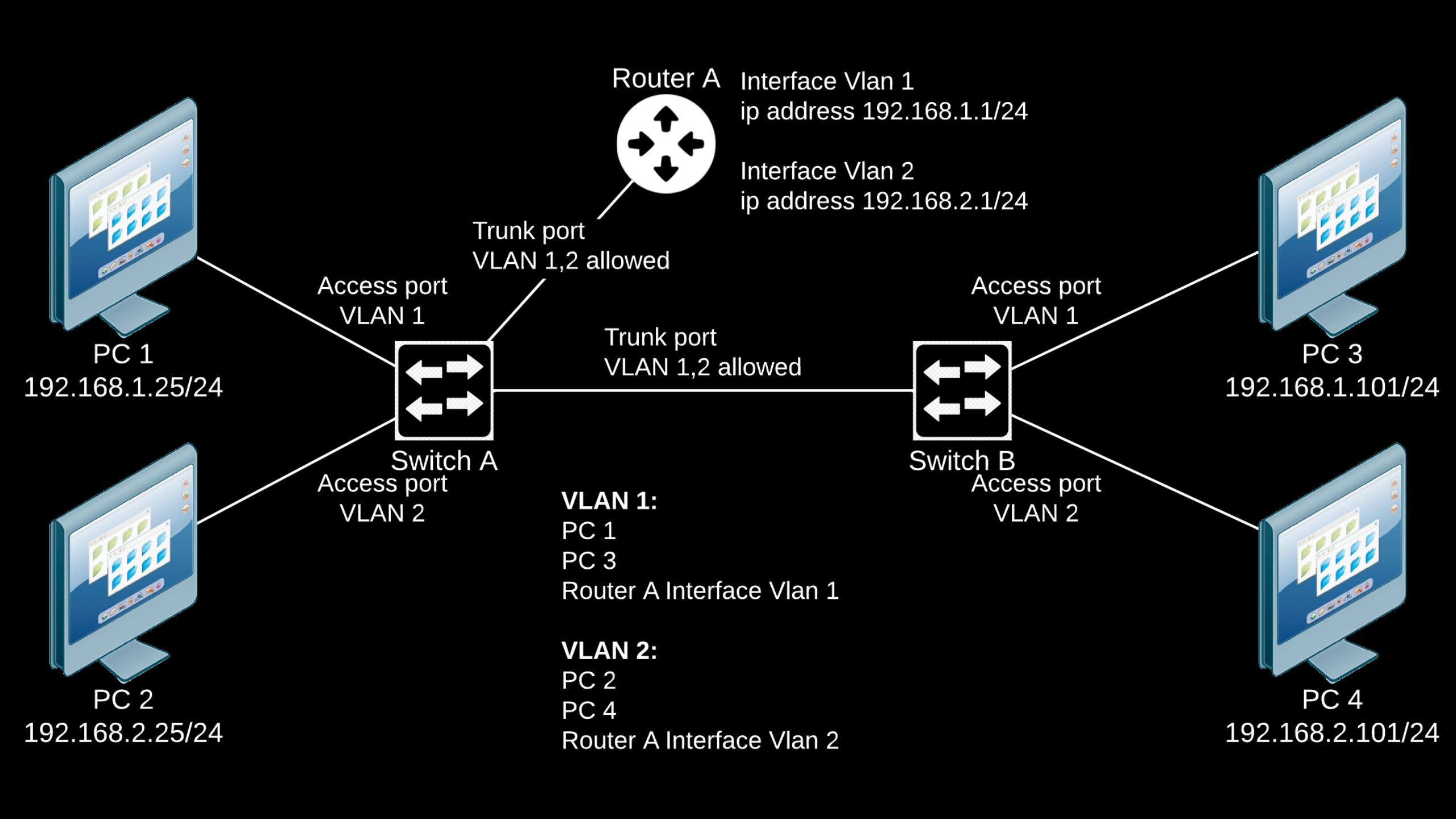
Layer 3 – IP subnetting

- A unique IP subnet is defined and assigned to each layer 2 segment
- A router is required for communication between subnets

How to segment?

Managed Layer 2 Switching

- Unmanaged (“dumb”) switches treat all frames as if they have no VLAN information. All ports on an unmanaged switch are in the same layer 2 segment
- Managed switches are VLAN-aware. Each port may be configured with different VLAN settings
  - Access ports
    - An access port accepts untagged frames (from a computer or printer, for example)
    - When an untagged frame ingresses the switchport, it is assigned to a VLAN (layer 2 segment) inside the switch according to the access port’s VLAN membership
    - If a tagged frame ingresses the switchport, it is discarded
    - When a frame egresses the switchport, it has no VLAN tag
  - Trunk ports
    - A trunk port accepts tagged frames (from another switch or router, for example)
    - When a tagged frame ingresses the switchport, it is assigned to a VLAN inside the switch according to its VLAN tag
    - If an untagged frame ingresses the switchport, it is either discarded or assigned to a native VLAN, depending in the port config. Default behavior for untagged frames is not standardized and varies widely among different manufacturers.


Router A
Interface Vlan 1
ip address 192.168.1.1/24
Interface Vlan 2
ip address 192.168.2.1/24
Trunk port
VLAN 1,2 allowed
Access port
VLAN 1
Trunk port
VLAN 1,2 allowed
Access port
VLAN 1
PC 1
192.168.1.25/24
PC 3
192.168.1.101/24
Switch A
Switch B
Access port
VLAN 2
Access port
VLAN 2
PC 2
192.168.2.25/24
PC 4
192.168.2.101/24
VLAN 1:
PC 1
PC 3
Router A Interface Vlan 1
VLAN 2:
PC 2
PC 4
Router A Interface Vlan 2

How to segment?

IP Address Management / Subnet Planning

Functions that should be segmented:

- Network management
- Server management
- DMZ servers
- Internal servers
- Printers
- Security cameras
- Security devices / building access control
- HVAC and building automation
- Phones and phone systems
- Administrative users – wired
- Administrative users – wireless
- Faculty/staff – wired
- Faculty/staff – wireless
- Students – wired
- Students – wireless
- Guests – wired
- Guests – wireless

How to segment?

IP Address Management / Subnet Planning

Functions that should be segmented:

- Network management
- Server management
- DMZ servers
- Internal servers
- Printers
- Security cameras
- Security devices / building access control
- HVAC and building automation
- Phones and phone systems

per building / campus

- Administrative users – wired
- Administrative users – wireless
- Faculty/staff – wired
- Faculty/staff – wireless
- Students – wired
- Students – wireless
- Guests – wired
- Guests – wireless

How to segment?

IP Address Management / Subnet Planning

Subnet size

- IPv4
  - Large enough to accommodate all unique devices that will connect to the subnet within 24-48 hours
  - Typically no smaller than /24 (253 host addresses)
  - Ideally no larger than /20 (4093 host addresses)
- IPv6
  - Always /64 (18 billion billion host addresses)

Example IPAM

VLAN ID	Name	IPv4	IPv6
101	Network Management	10.95.1.0/24	2620:1d5:c04:101::/64
102	Wireless Management	10.95.2.0/24	2620:1d5:c04:102::/64
103	Hypervisor Management	10.95.3.0/24	2620:1d5:c04:103::/64
104	Servers	10.95.4.0/24	2620:1d5:c04:104::/64
105	DMZ	10.95.5.0/24	2620:1d5:c04:105::/64
106	Security Devices	10.95.6.0/24	2620:1d5:c04:106::/64
107	Security Cameras	10.95.7.0/24	2620:1d5:c04:107::/64
108	HVAC Controls	10.95.8.0/24	2620:1d5:c04:108::/64
109	Phones	10.95.9.0/24	2620:1d5:c04:109::/64
110	IT Staff	10.95.10.0/24	2620:1d5:c04:110::/64
111	Administrative Staff	10.95.11.0/24	2620:1d5:c04:111::/64
112	Staff	10.95.12.0/24	2620:1d5:c04:112::/64
113	Student Wired	10.95.13.0/24	2620:1d5:c04:113::/64
114	Student Wireless	10.95.14.0/23	2620:1d5:c04:114::/64

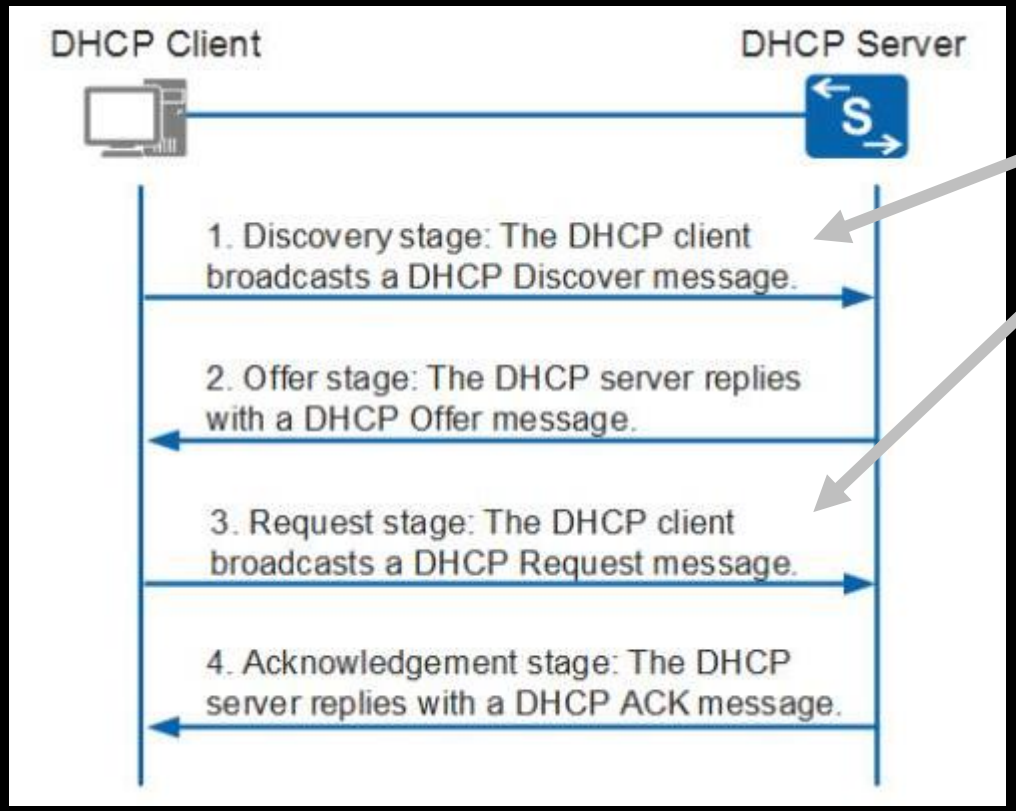
How do clients connect to the network?

How does the client learn what IP address, subnet mask, and gateway to use when it connects to the network?

- The user can manually configure these details
  - Not user-friendly
  - Usually necessary for infrastructure components – network equipment, servers, printers, cameras
- The host can use DHCP to configure itself automatically
  - Allows clients to move from one network to another easily
  - Does not require user intervention
  - DHCP server is configured with subnet information and a pool of addresses to “lease” to clients
  - Client IPs may change over time based on available addresses in the DHCP server’s lease pool
  - DHCP server can provide additional information, like DNS server addresses, using DHCP options
- In IPv6, clients can autoconfigure using SLAAC – stateless address autoconfiguration
  - No DHCP server is required, but the router must be configured to send router advertisements containing subnet information
  - DHCP may also be used for address assignment in IPv6 (but why would you?)

How do clients connect to the network?

The DHCP process

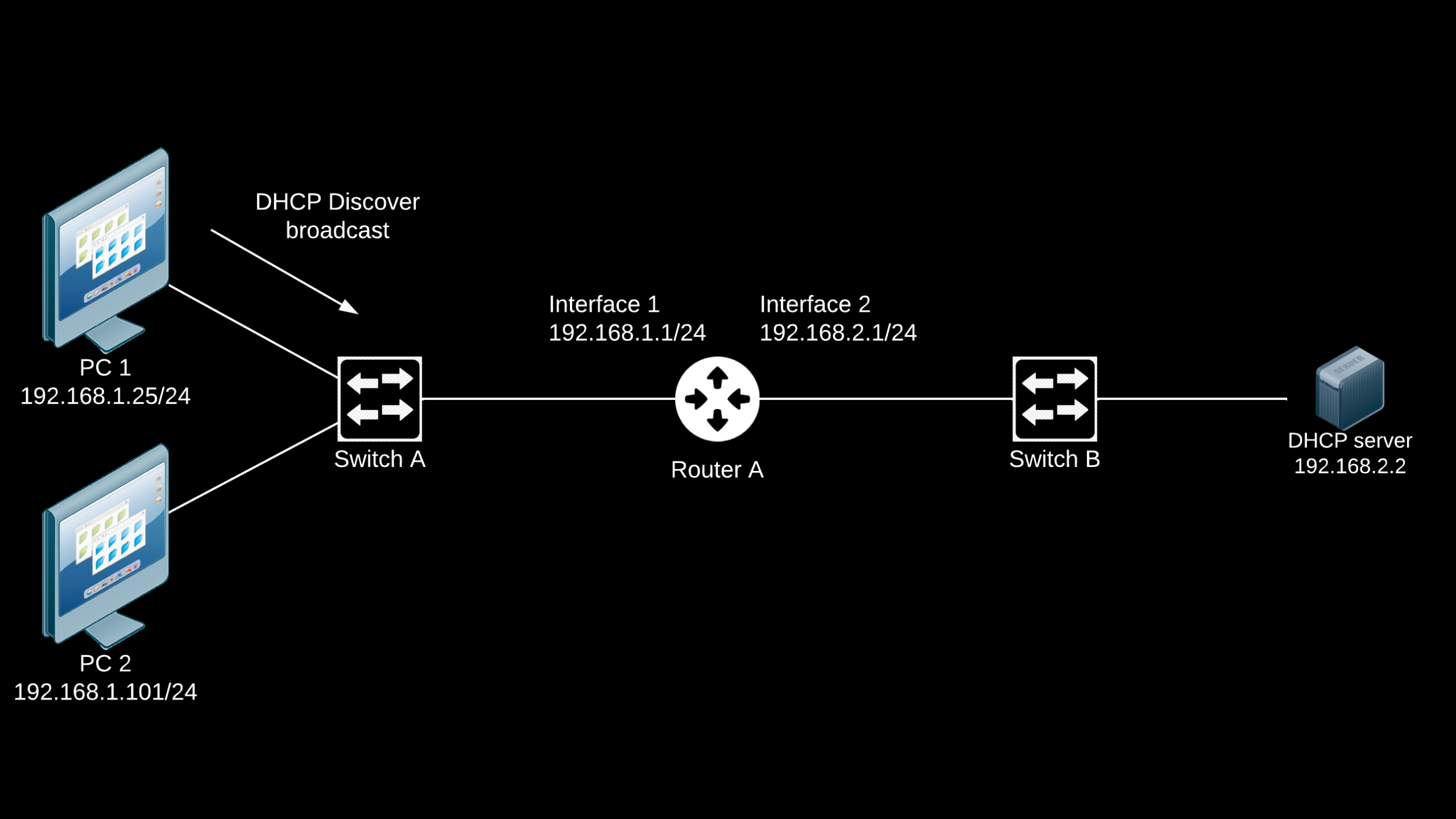


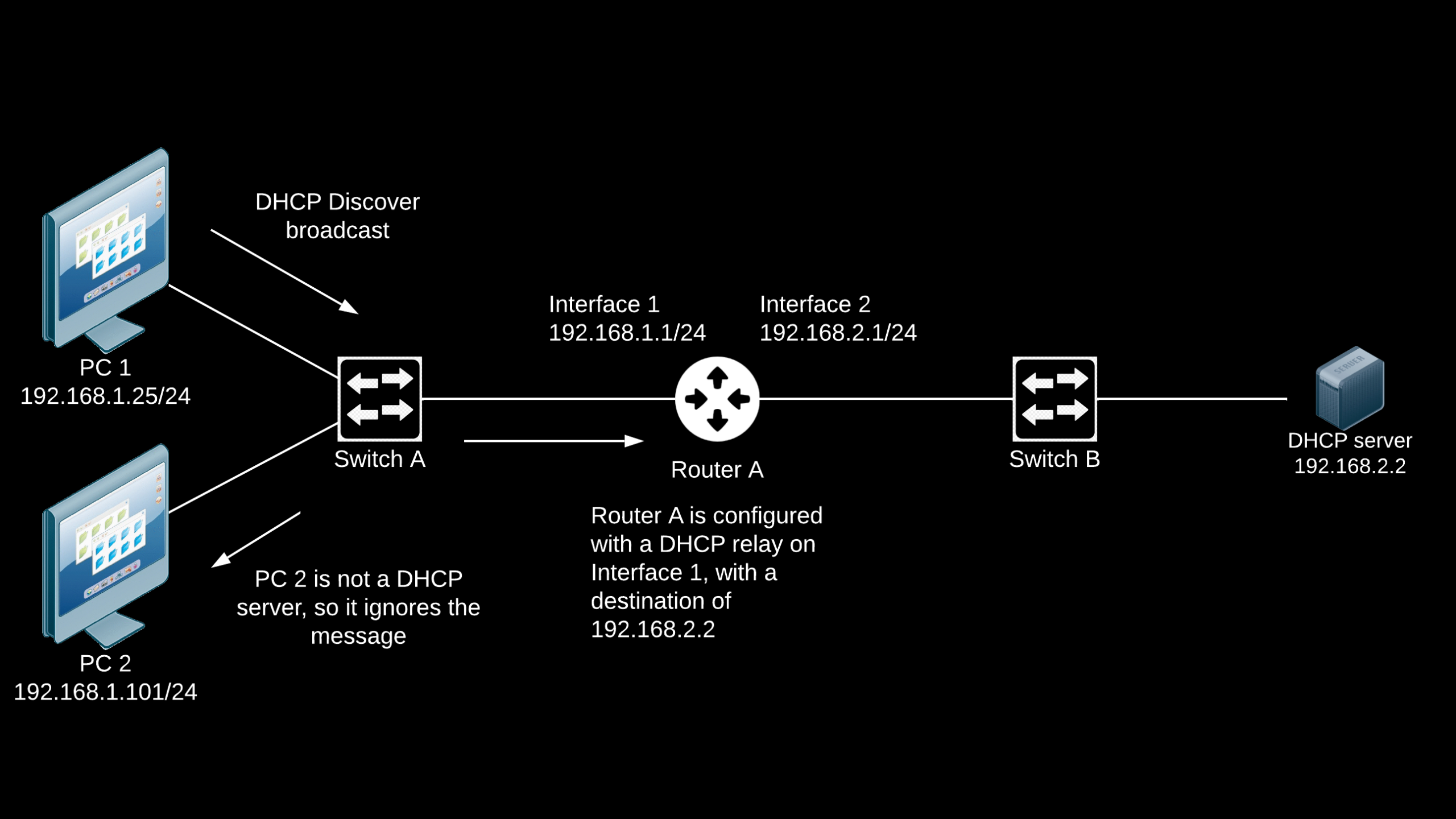
Broadcast!

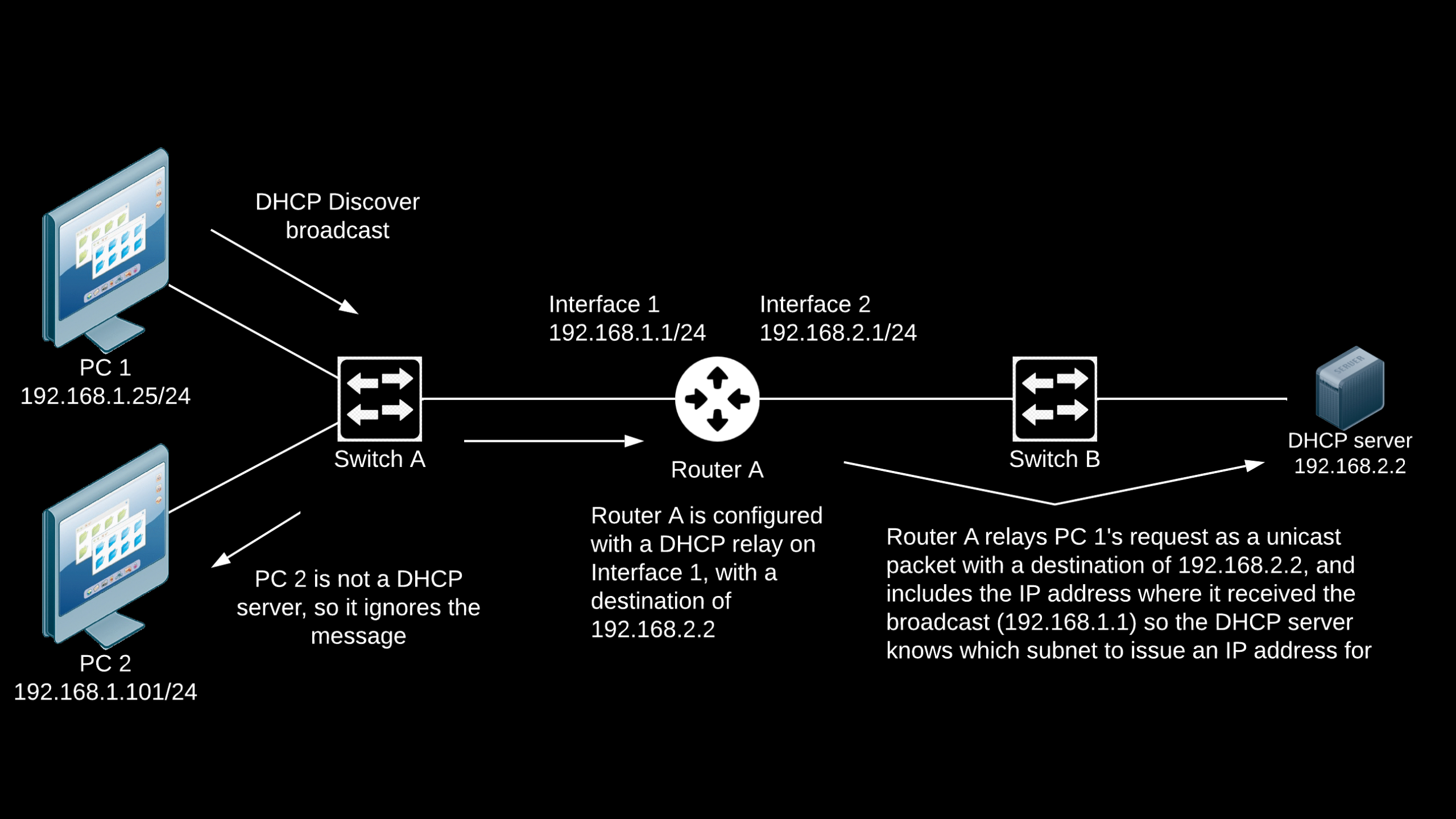
What's a broadcast again?
- A message that is delivered to *every host* in the layer 2 segment

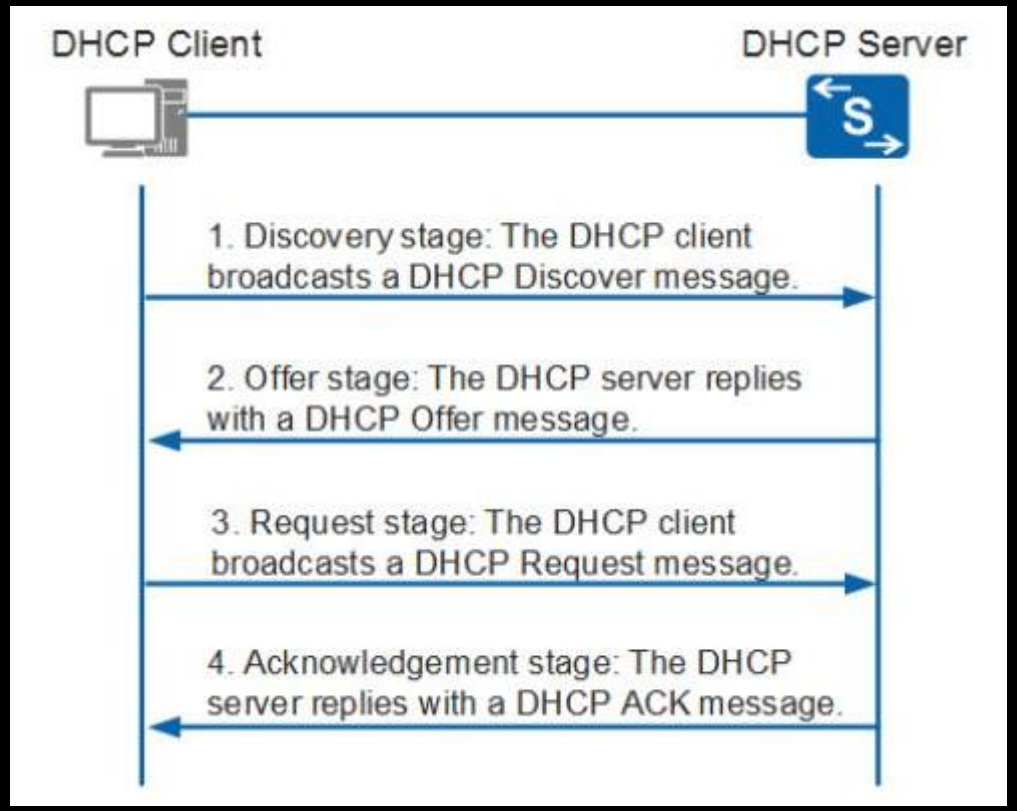
What if the DHCP server does not live in the same layer 2 segment / subnet as the client?
- The router must be configured to relay DHCP broadcasts to the server in another subnet

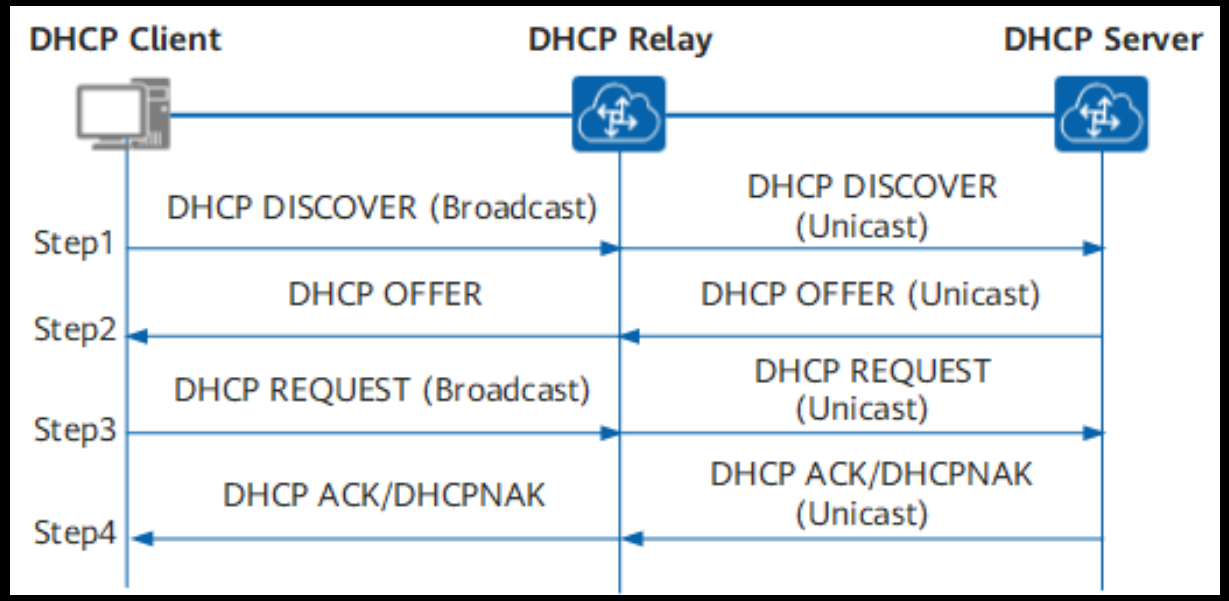
In addition to IP address, the DHCP server can inform the client of subnet mask, default gateway, DNS server addresses, local domain name, time servers, time zone, and many other DHCP options


DHCP Discover
broadcast
Interface 1
192.168.1.1/24
Interface 2
192.168.2.1/24
PC 1
192.168.1.25/24
Switch A
Router A
Switch B
DHCP server
192.168.2.2
PC 2
192.168.1.101/24


DHCP Discover
broadcast
Interface 1
192.168.1.1/24
Interface 2
192.168.2.1/24
PC 1
192.168.1.25/24
Switch A
Router A
Switch B
DHCP server
192.168.2.2
Router A is configured with a DHCP relay on Interface 1, with a destination of 192.168.2.2
PC 2 is not a DHCP server, so it ignores the message
PC 2
192.168.1.101/24


DHCP Discover
broadcast
Interface 1
192.168.1.1/24
Interface 2
192.168.2.1/24
PC 1
192.168.1.25/24
Switch A
Router A
Switch B
DHCP server
192.168.2.2
PC 2
192.168.1.101/24
PC 2 is not a DHCP server, so it ignores the message
Router A is configured with a DHCP relay on Interface 1, with a destination of 192.168.2.2
Router A relays PC 1's request as a unicast packet with a destination of 192.168.2.2, and includes the IP address where it received the broadcast (192.168.1.1) so the DHCP server knows which subnet to issue an IP address for


DHCP Client
DHCP Server
1. Discovery stage: The DHCP client broadcasts a DHCP Discover message.
2. Offer stage: The DHCP server replies with a DHCP Offer message.
3. Request stage: The DHCP client broadcasts a DHCP Request message.
4. Acknowledgement stage: The DHCP server replies with a DHCP ACK message.


DHCP Client
DHCP Relay
DHCP Server
Step1
DHCP DISCOVER (Broadcast)
DHCP DISCOVER (Unicast)
Step2
DHCP OFFER
DHCP OFFER (Unicast)
Step3
DHCP REQUEST (Broadcast)
DHCP REQUEST (Unicast)
Step4
DHCP ACK/DHCPNAK
DHCP ACK/DHCPNAK (Unicast)

SLAAC

- Client sends a *multicast* router solicitation message
  - To all routers: “I’m looking for a router.”
- Router(s) respond with a router advertisement
  - “I am a router. The subnet for this segment is 2001:db8:beef:cafe::/64, and you should autoconfigure an address using that prefix.”
- Client picks an address to use and performs duplicate address detection
  - “Is anybody using the address 2001:db8:beef:cafe::1234/64?”
- If radio silence, the address is available to use. If somebody responds that the address is already in use, the client generates a new one and tries again.
- The router advertisement may also contain DNS server addresses and local domain names. Or, these options may be requested from a DHCPv6 server without using the DHCPv6 server for address assignment.

Why IPv6?

Why IPv6?

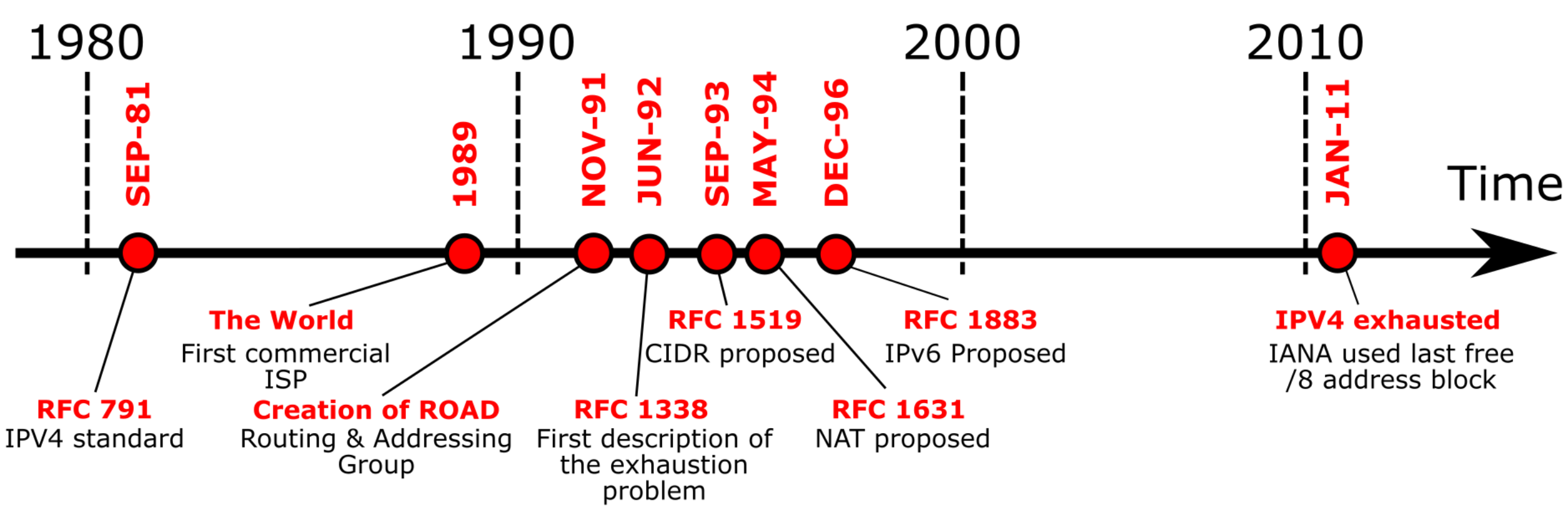
	Layer	Ingredients	Scope
3	Network	Source and destination IP address	Global / universal * *Example: your computer connecting to Google through the Internet* *sort of
2	Data link	Source and destination MAC address	A single Layer 2 segment, commonly called a LAN, VLAN, or broadcast domain. *Example: several computers connected by an unmanaged switch (not VLAN-aware)*
1	Physical	Electrical signals in copper	A single cable or physical connection between two

Address types

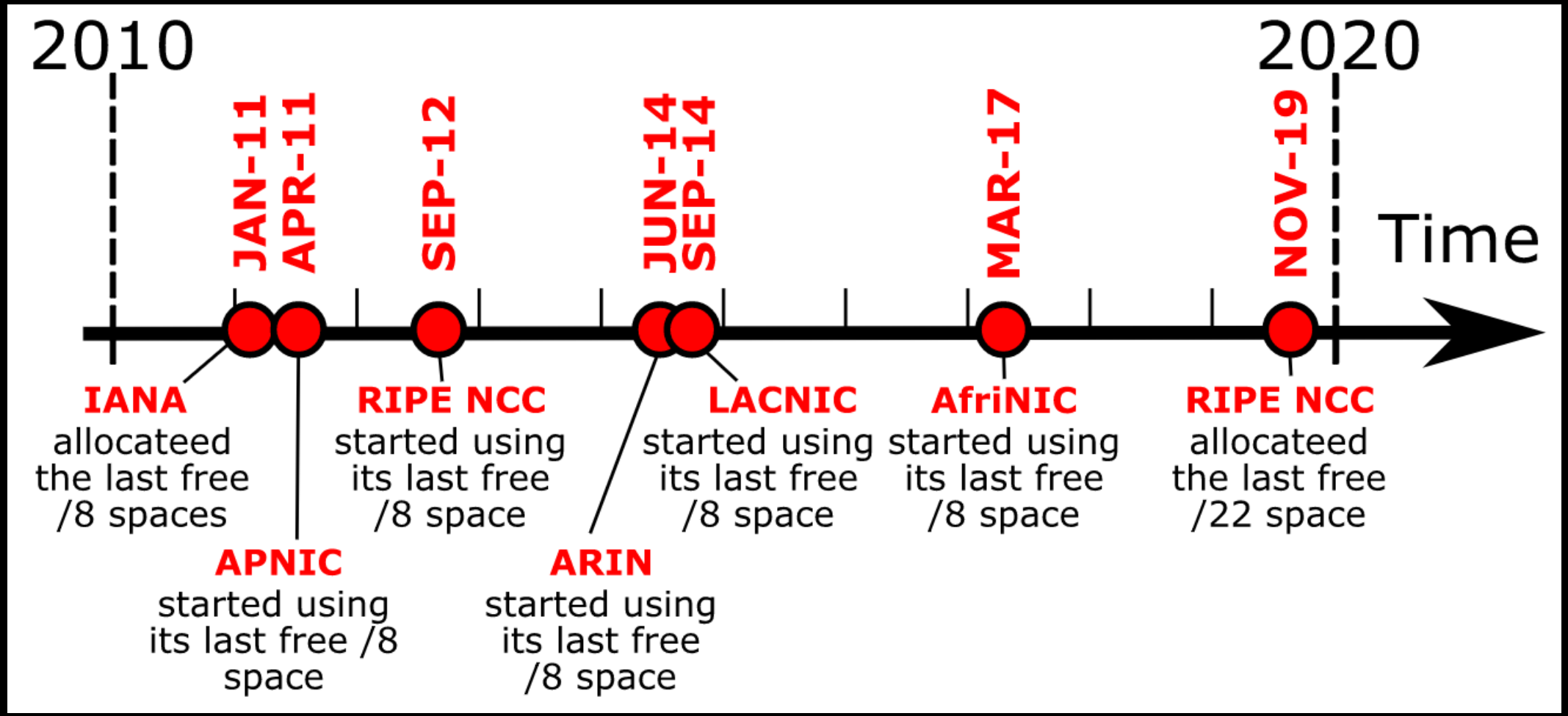
IPv4 Address

- 32-bit address written as 4 bytes (“octets”) in decimal, separated by periods
- `192.168.1.101`
- `11000000 10101000 00000001 01100101` (binary)
- 4.3×10^9 permutations (4.3 billion)

IPv4 Exhaustion



IPv4 Exhaustion



NAT

Network Address Translation

- Translates one IP address to another
- Can be S-NAT (translate source IP) or D-NAT (translate destination IP), or both
- Can be PAT (port address translation) or NAT overload

NAT

Benefits of NAT

- Allows many hosts share one public IP address
- That’s it

NAT

Drawbacks of NAT

- Makes troubleshooting more difficult
  - IP packets no longer use keep the same source and destination address for the whole journey
- Expensive in terms of hardware resources, difficult to scale
  - Each exchange must be tracked in memory so the translating device can deliver the response to the correct private IP
- Increases overhead
  - The translating device must spend additional computation time manipulating the packet
- Breaks some types of traffic
  - Higher level protocols, like SIP, may relay on knowing the source or destination IP address, which might get changed by a router upstream

IPv6 – back to basics

- IPv6 provides a *vast* address space
- *Every device* in the world can have a globally unique IPv6 address – or a billion billion billion addresses!
- An IPv6 packet keeps the same source and destination for its whole journey – the way IPv4 was meant to work
- IPv6 reduces overhead by avoiding NAT and improving efficiency in routers
- IPv4 is not going away tomorrow, but it is time to add IPv6 to our networks, because it is becoming the preferred protocol on the Internet
  - Dual-stack will likely be the standard for many years

Questions

Lab

- Dual stack campus network with a core and 12 buildings
- Palo Alto firewall providing security policy and NAT
- Windows DNS and DHCP server
- IP ranges in use:
  - 10.95.0.0/16, subnetted as /20 for each building
  - 206.82.17.64/28, one PAT addresses per building
  - 2620:1d5:c04::/48, subnetted as /52 per building
- Configure your building switch to provide some client subnets that can communicate with the rest of the campus
- https://bit.ly/TTL2022Lab