Review Question

Examine the packet headers below

```
> Frame 48: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits) on interface 0
> Ethernet II, Src: Vmware_e3:cd:12 (00:50:56:e3:cd:12), Dst: Vmware_3e:42:6b (00:0c:29:3e:42:6b)
> Internet Protocol Version 4, Src: 134.115.4.231, Dst: 192.168.112.128
> Transmission Control Protocol, Src Port: 80, Dst Port: 50488, Seq: 2921, Ack: 1060, Len: 286
> [3 Reassembled TCP Segments (3206 bytes): #46(1460), #47(1460), #48(286)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (439 lines)
```

- What application layer protocol is in use and what is it used for?
- What transport layer protocol has been used to encapsulate this packet and why has it been used?

Murdoch UNIVERSITY

Review Question

Examine the packet headers below

```
Frame 48: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits) on interface 0
Ethernet II, Src: Vmware_e3:cd:12 (00:50:56:e3:cd:12), Dst: Vmware_3e:42:6b (00:0c:29:3e:42:6b)
Internet Protocol Version 4, Src: 134.115.4.231, Dst: 192.168.112.128
Transmission Control Protocol, Src Port: 80, Dst Port: 50488, Seq: 2921, Ack: 1060, Len: 286
[3 Reassembled TCP Segments (3206 bytes): #46(1460), #47(1460), #48(286)]
Hypertext Transfer Protocol
Line-based text data: text/html (439 lines)
```

- What application layer protocol is in use and what is it used for?

The packet contains a Hypertext Transfer Protocol (HTTP) message. HTTP is usually used to request and load web content.

Murdoch UNIVERSITY

Review Question

Examine the packet headers below

```
> Frame 48: 340 bytes on wire (2720 bits), 340 bytes captured (2720 bits) on interface 0
> Ethernet II, Src: Vmware_e3:cd:12 (00:50:56:e3:cd:12), Dst: Vmware_3e:42:6b (00:0c:29:3e:42:6b)
> Internet Protocol Version 4, Src: 134.115.4.231, Dst: 192.168.112.128
> Transmission Control Protocol, Src Port: 80, Dst Port: 50488, Seq: 2921, Ack: 1060, Len: 286
> [3 Reassembled TCP Segments (3206 bytes): #46(1460), #47(1460), #48(286)]
> Hypertext Transfer Protocol
> Line-based text data: text/html (439 lines)
```

- What transport layer protocol has been used to encapsulate this packet and why has it been used?

HTTP is encapsulated using Transmission Control Protocol (TCP) which is used to ensure that the web content is reliably delivered.

Murdoch UNIVERSITY

The Network Layer

ICT169

Foundations of Data Communications

Admin

- Participation quiz 1 was due yesterday (Sunday, 12 Aug)
    - Expect to receive marks and feedback Wednesday / Thursday
- Participation quiz 2 due this Sunday (19 Aug)
    - No further reminders about participation quizzes

Murdoch UNIVERSITY

Last Week

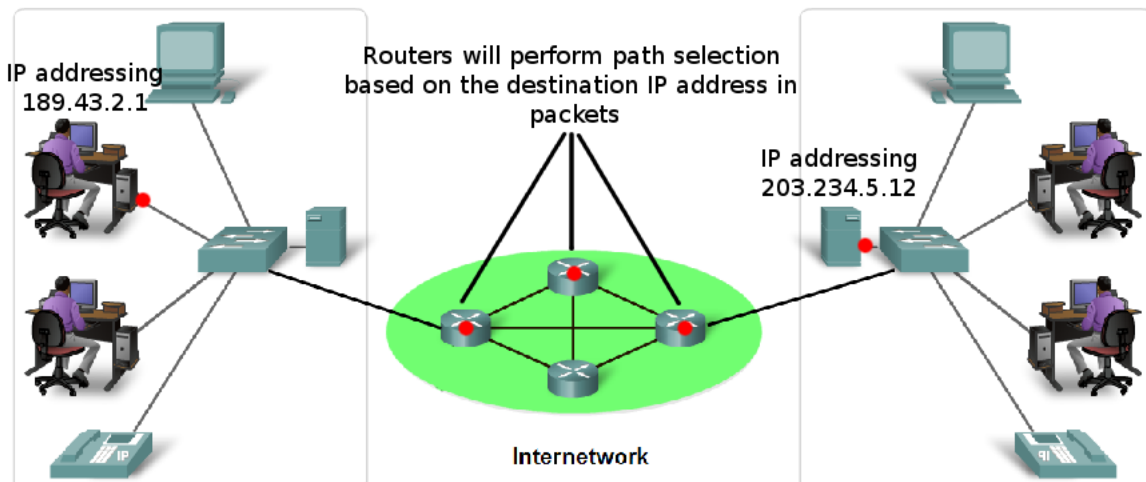
- An overview of the Application layer and a look at some common application layer protocols
- Examined the operation of the transport layer, looking closely at two protocols: TCP and UDP
- Closer look at network traffic in the labs using Wireshark

Lecture Overview

- The role of the Network layer and the encapsulation process
- Network layer protocols
- Internet Protocol (version 4)
- Binary maths
- IPv4 addressing and subnet masks
- Subnetting and Variable Length Subnet Masks (VLSM)

Network Layer

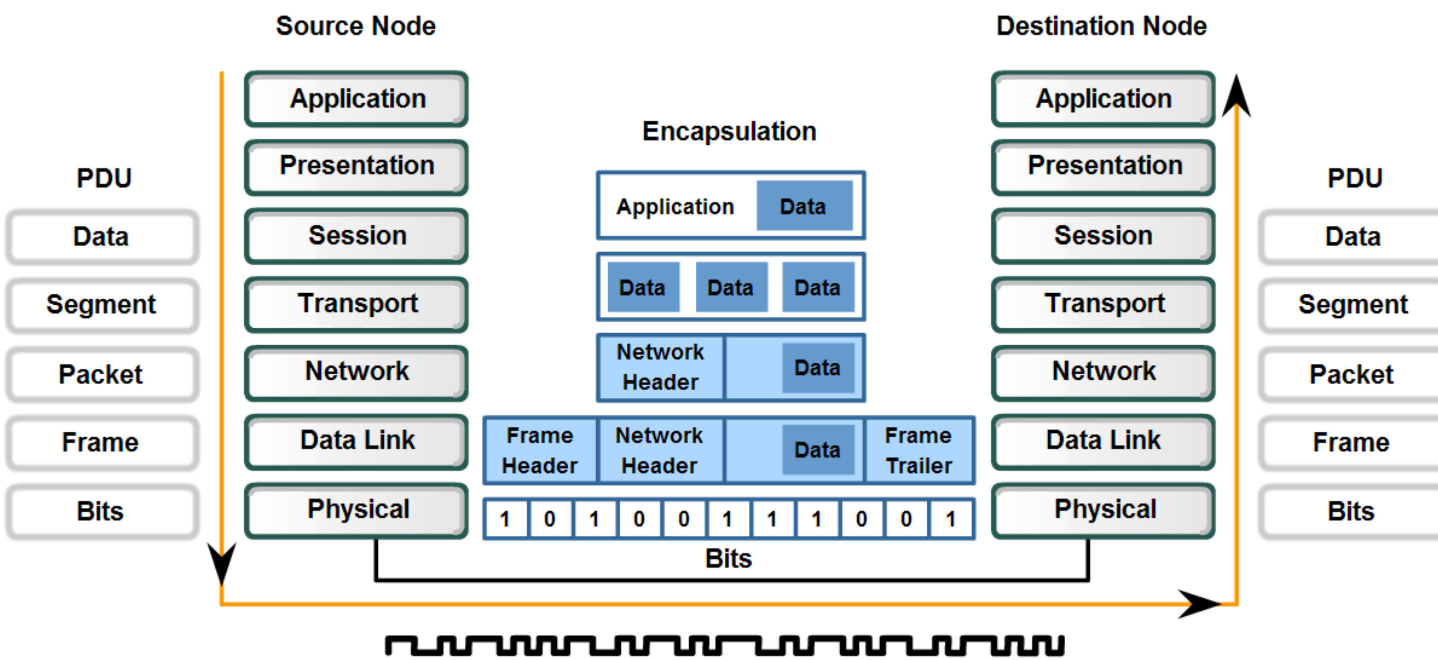
- Specifies an **addressing scheme** for the network (IP addressing), and how packets should be **routed** through the network
- Like the Transport layer, the Network layer is also responsible for end-to-end delivery of packets (from the source to destination)



Individual parts of the system can be designed independently, but still work together seamlessly.

Encapsulation

- Recall that encapsulation occurs as data travels down the networking stack
- Each layer adds information (headers) required to ensure that the transmission reaches its intended destination
- Remember: Data → Segment → Packet → Frame → Bits

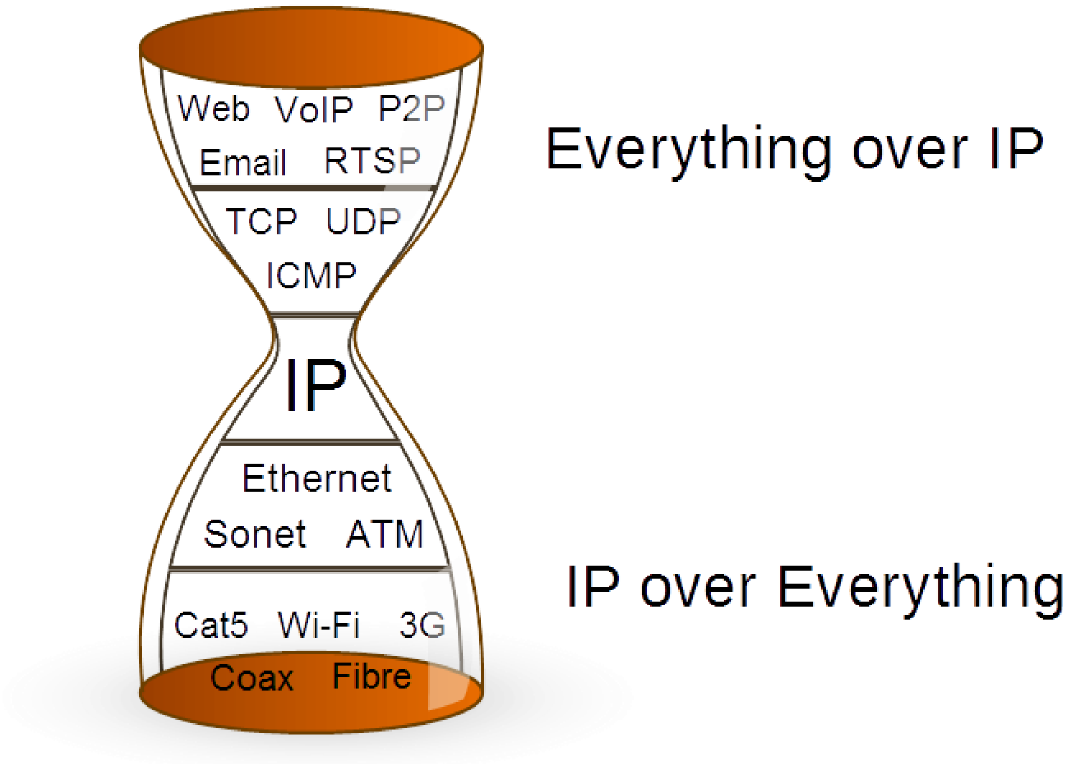


Network Layer Protocols

- There are a few network layer protocols:
  - Internet Protocol version 4 (IPv4)
  - Internet Protocol version 6 (IPv6)
  - IPX
  - AppleTalk
- IPv4 is the most widely used and will be the focus of today's lecture
- We'll come back to IPv6 later
- You'll also have encountered another network layer protocol: Internet Control Message Protocol (ICMP)

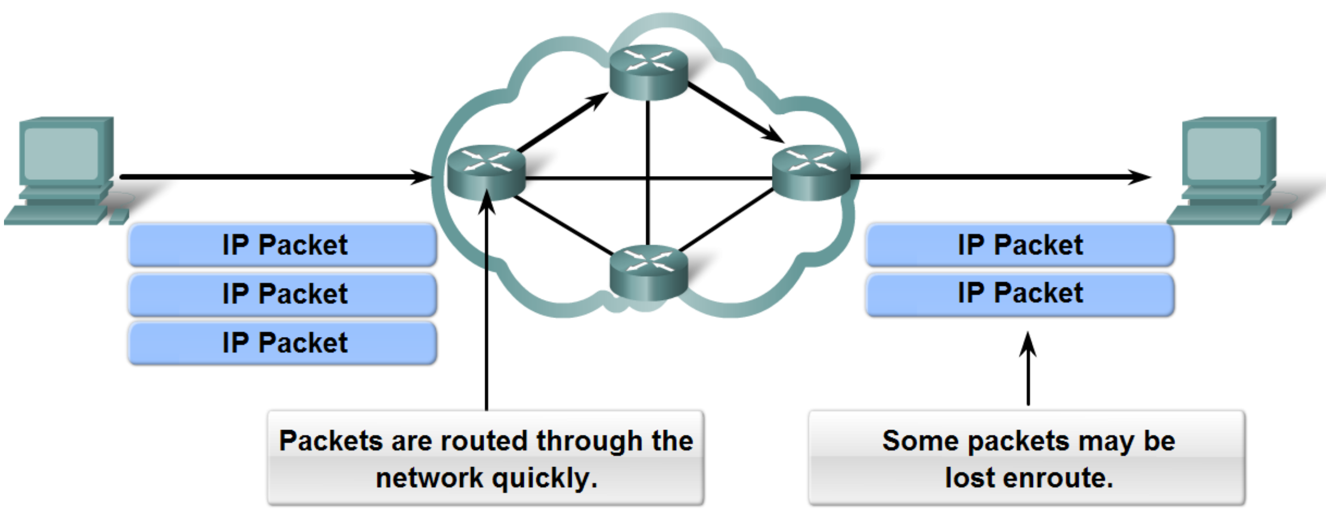
The IP Hourglass Model

- IP has become the dominant protocol at the Network layer, and is now central to the stack



Internet Protocol (IP)

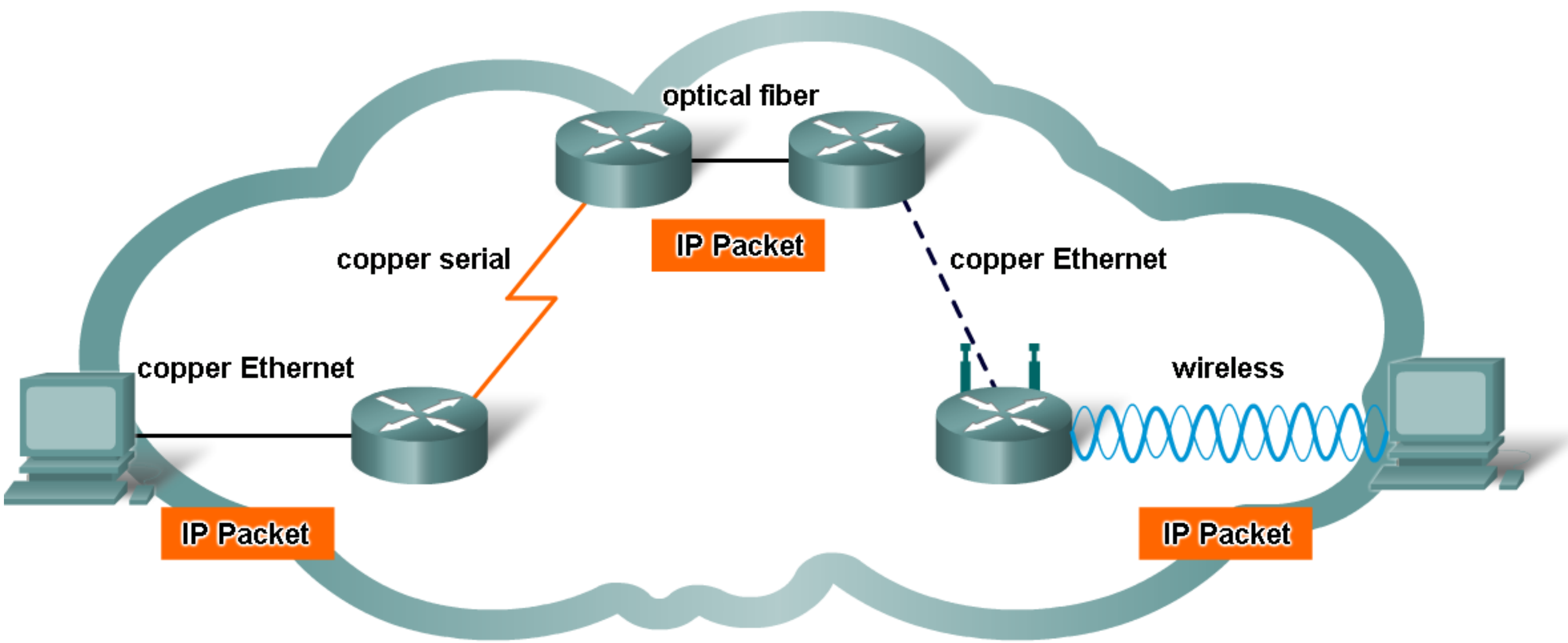
- IP communications are **connectionless**; no setup required
- Like UDP, IPv4 is a 'best effort' protocol;
  - Like UDP, this doesn't mean that IP is unreliable
  - Reliability must come from another layer of the networking stack



As an unreliable Network layer protocol, IP does not guarantee that all sent packets will be received.

Internet Protocol (cont.)

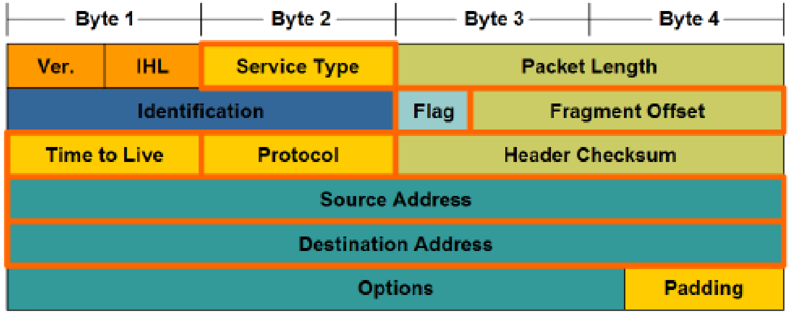
- IPv4 is also media independent
- This means that it can function over copper, fiber, air (or any combination of the three)



IP packets can travel over different media.

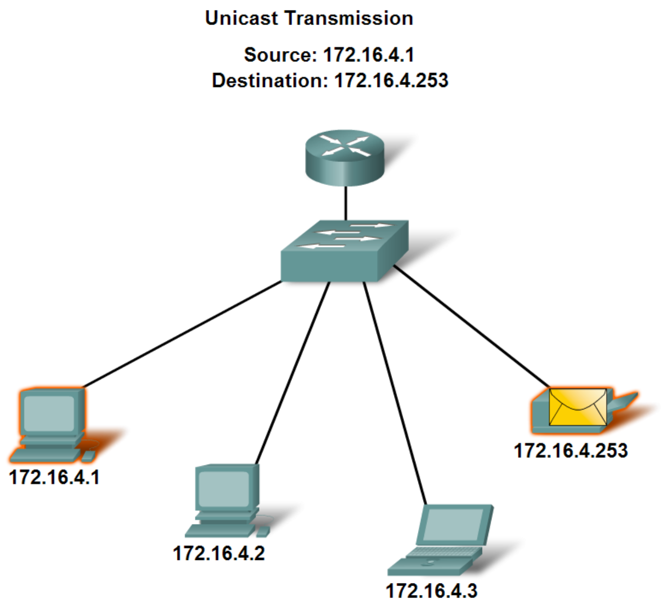
IP Protocol Header

- IPv4 and IPv6 packet headers differ, but share some commonalities
- Some fields to remember:
  - Source Address – The originating host address.
  - Destination Address – The destination host address.
  - Version – Which IP version is being used (v4 / v6).
  - Protocol – What transport layer protocol is being encapsulated.
  - Time to Live (TTL) – The maximum number of hops the packet can traverse before being dropped.



Types of Transmissions

- **Unicast** transmissions are packets destined for only one host
- **Multicast** transmissions will reach more than one (but not all) hosts
- **Broadcast** transmissions are packets destined for all other hosts within the subnet



IP Addresses – Addressing at the Network Layer

- A 32 bit address, broken up into 4 numbers separated by dots (referred to as **dotted decimal notation**)
- Each of these numbers is known as an **octet** and represents 8 bits (binary digits)
- These eight bits can represent decimal numbers ranging between 0 and 255

Dotted decimal	192	.	168	.	10	.	10
Binary	11000000		10101000		00001010		00001010

Public and Private IP Addressing

- Some address blocks are reserved for private networks:
  - 10.0.0.0 – 10.255.255.255
  - 169.254.0.0 – 169.254.255.255
  - 172.16.0.0 – 172.31.255.255
  - 192.168.0.0 – 192.168.255.255
- These address ranges are used inside private networks, and packets addressed to these ranges cannot be routed on the Internet
- Packets originating from a private IP address must undergo Network Address Translation (NAT) to be routed over the Internet (more on this in a later lecture)

Murdoch UNIVERSITY

Other Reserved Addresses

- Other ranges of reserved addresses include:
  - **Local identification:** 0.0.0.0 – 0.255.255.255
    - Only used in source addresses
  - **Loopback:** 127.0.0.1 – 127.255.255.255
    - Used for virtual network interfaces for testing
    - Send data to yourself only
  - **Link-local:** 169.254.0.1 – 169.254.255.255
    - Can only be used to communicate in local subnet
  - **Documentation:** 192.0.2.0 – 192.0.2.255
  - **Testing:** 198.18.0.0 – 198.19.255.255

Murdoch UNIVERSITY

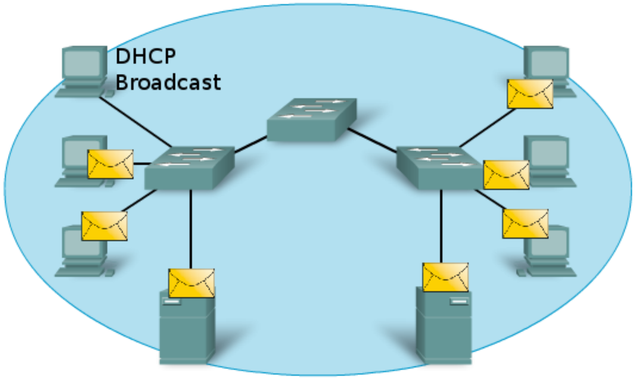
Assigning IP Addresses

- IP addresses can either be assigned manually (**static**) or automatically (**dynamic**)
- Dynamic addressing uses DHCP to automatically assign devices an IP address
- Static addressing is usually used for devices that should have a fixed IP address such as servers, printers, and routers

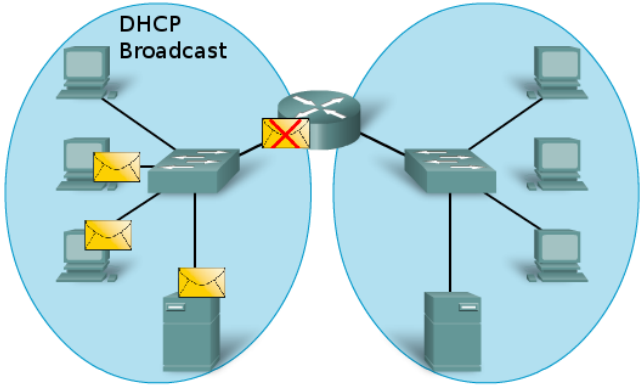
Murdoch UNIVERSITY

Broadcast Propagation

- Broadcasts are transmitted to all hosts within the source host's subnet
- A network switch moves packets within a subnet, and will propagate broadcasts
- Each interface on a router belongs to a **different** subnet, and will contain broadcasts



All devices in this network are connected in one broadcast domain when the switch is set to the factory default settings. Since switches forward broadcasts by default, broadcasts are processed by all devices

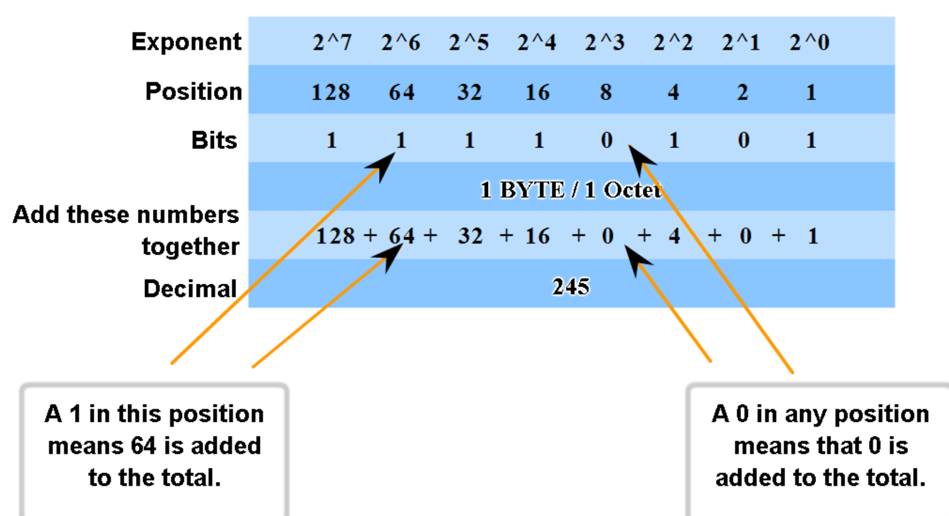


Replacing the middle switch with a router creates 2 IP subnets, hence, 2 distinct broadcast domains. All devices are connected but local broadcasts are contained.

Understanding IP Addressing – Converting Binary and Decimal

To be able to divide networks into subnets, we must be first convert IP addresses from their decimal representation to binary

Binary To Decimal Conversion

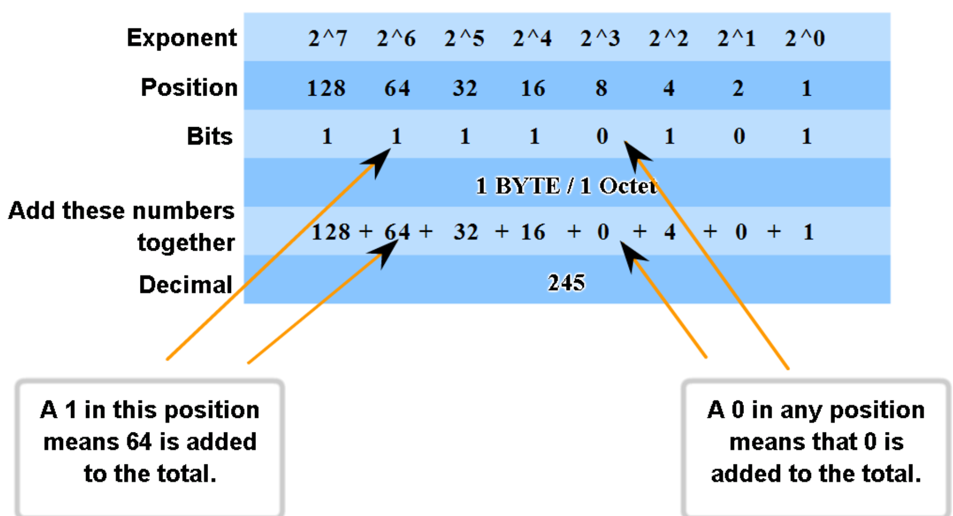


11110101 in Binary = Decimal Number 245

Converting from Decimal to Binary

- We can convert decimal numbers to binary by trying to add the different powers of two together, but this isn't very intuitive
- Easier to subtract powers of two instead

Binary To Decimal Conversion



11110101 in Binary = Decimal Number 245

Converting from Decimal to Binary – Problems

Convert the following binary numbers to decimal:

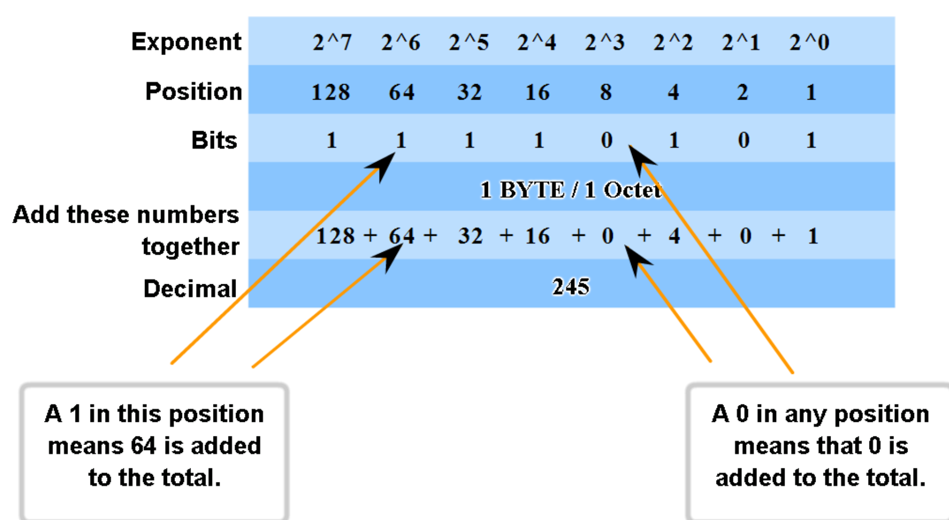
10	~~0000~~1010
212	11010100
112	01110000
12	~~0000~~1100

Murdoch University

Converting from Binary to Decimal

- In binary numbers, each bit represents a power of two
- We can convert binary numbers to decimal by adding all of the powers of two together

Binary To Decimal Conversion



11110101 in Binary = Decimal Number 245

Converting from Binary to Decimal – Problems

Convert the following binary numbers to decimal:

10101	16 + 4 + 1 = 21
1011001	64 + 16 + 8 + 1 = 89
101110	32 + 8 + 4 + 2 = 46
1011111	64 + 16 + 8 + 4 + 2+ 1 = 95

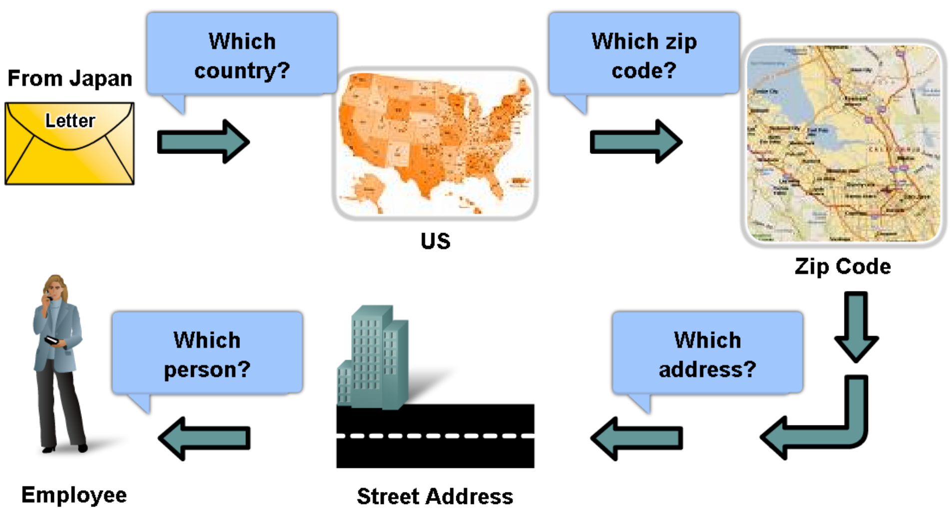
Break

When we return: More on Subnets and Subnetting!

Hierarchical IP Addressing

- IP uses a hierarchical addressing system based around subnetworks (groups of IP addresses)
- Summarisation is used to route packets around the network (or Internet)

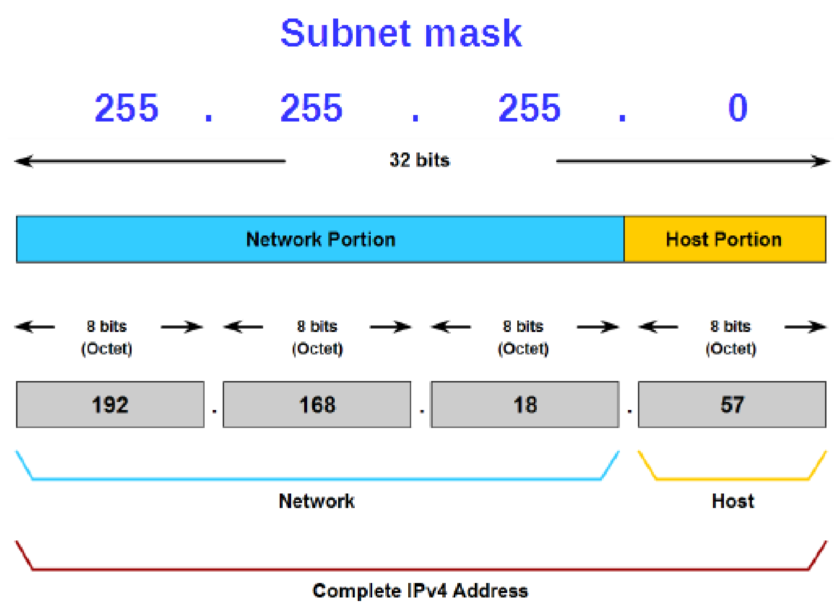
TO: Jane Doe 170 West Tasman Drive, San Jose, CA 95134, USA



At each step of delivery, the post office need only examine the next hierarchical level.

Hierarchical IP Addressing (cont.)

- IP uses the **subnet mask** to provide hierarchy by dividing addresses into a **network** and **host** portion
- The subnet mask uses bits set to 1 to represent the network portion of an address
- Each host is only aware of other hosts within its own subnet
- Hosts pass packets to the **default gateway** to be routed outside of the local network



The Subnet Mask – Representation

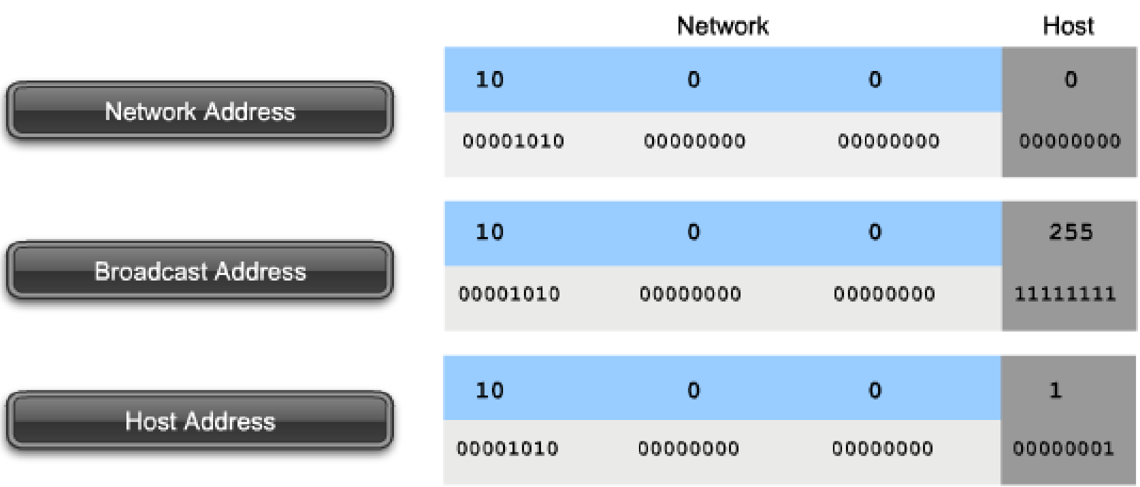
- Subnet mask can be written in **dotted decimal** or **slash** notation
- Slash notation is an abbreviated form and is more commonly used (but not by operating systems)
- Convert the subnet mask to slash notation by counting the number of '1' bits in the dotted decimal representation

255.255.255.0 =
11111111.11111111.11111111.00000000

= /24

Types of IP Addresses

- A **network address** is the first address on the network used to identify a network or subnet
    - All host bits set to 0
- A **broadcast address** is the final address on the network, used to address a transmission to all hosts within the subnet
    - All host bits set to 1
- **Host addresses** are the IP addresses in between



Murdoch University

The Subnet Mask – Implementation

- Operating systems evaluate a subnet mask using logical AND operations to figure out the network address
- This information is then used in the packet forwarding process

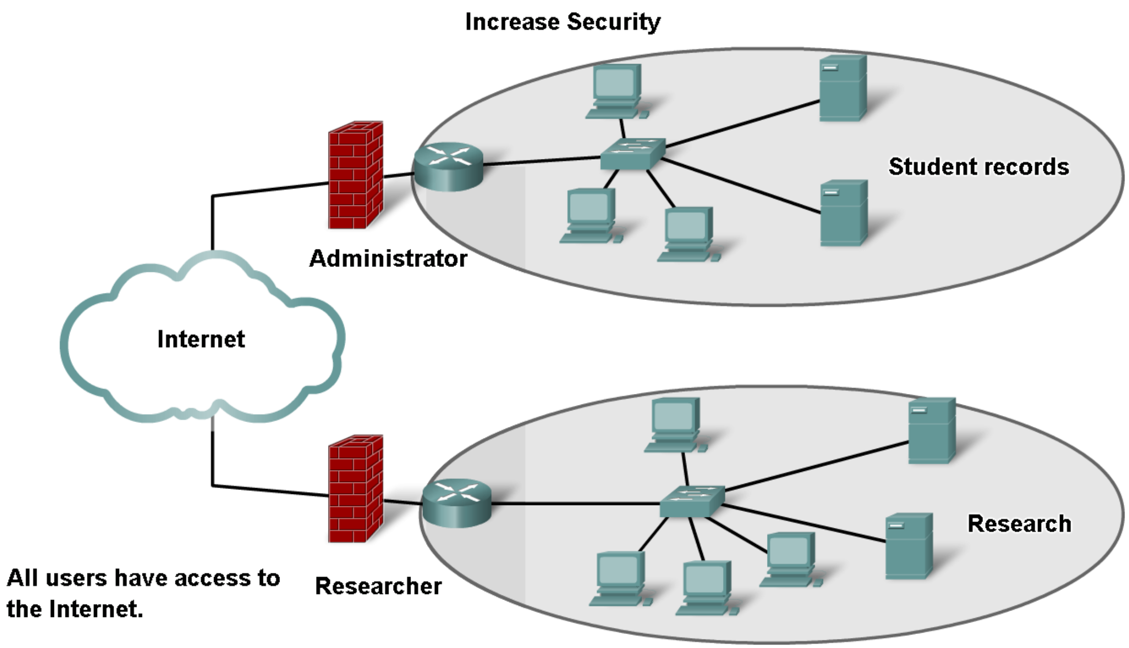
	High order bits Prefix /16		Low order bits	
	192 .	0 .	0 .	1
Host	11000000	00000000	00000000	00000001
Subnet	255 11111111	255 11111111	0 00000000	0 00000000
Network	11000000	00000000	00000000	00000000
	192 .	0 .	0 .	0

1 AND 1 = 1
0 AND 1 = 0
0 AND 0 = 0
1 AND 0 = 0

Murdoch UNIVERSITY

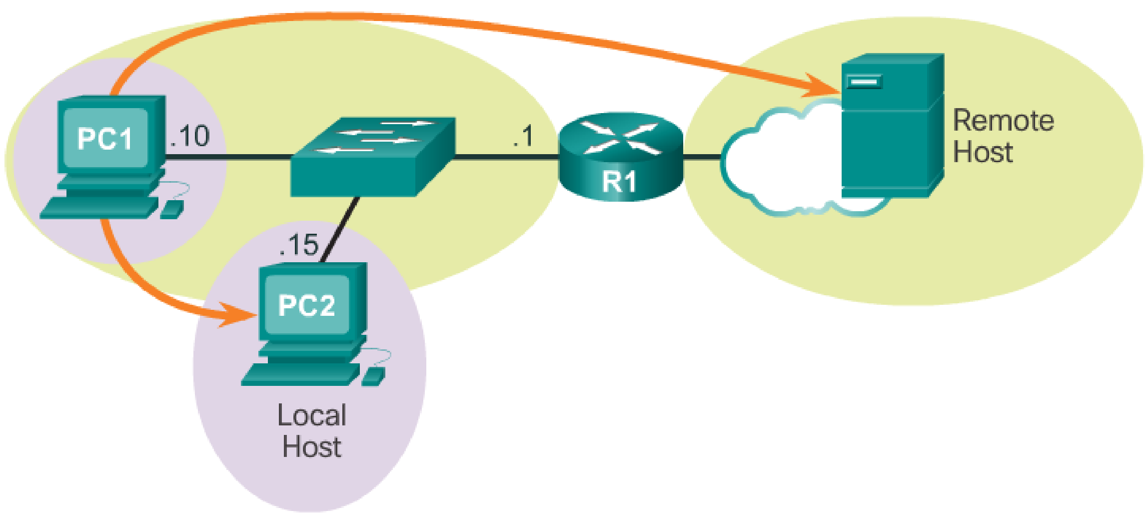
Why Subnet?

- In one administrative domain, we divide up large range of IP addresses into smaller subnetworks/subnets
  - Reduce performance overheads caused by excessive broadcasts
  - Allow different security policies to be applied to groups of users (in different subnets)



Packet Forwarding

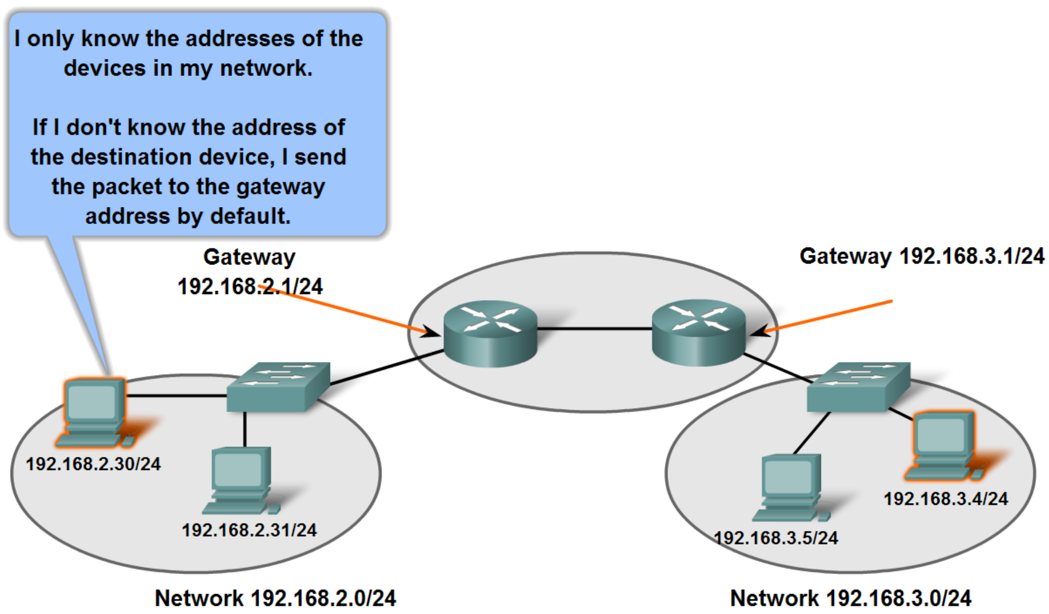
- When a device is readying a packet for submission, it first checks whether the destination is in its local subnet
- If the destination is in the local subnet, the devices will use Layer 2 addressing
- Otherwise, the packet will be forwarded to the default gateway



The Default Gateway

- The default gateway is the router responsible for forwarding traffic outside of the local subnet
- Packets are forwarded to the gateway using its Layer 2 address

Gateways Enable Communications between Networks



Classful Networks – A History Lesson

- Until 1993, IP addressing was classful; the subnet mask used was based solely on the IP address
- Classful addressing is extremely inefficient due to the size of each block of IP addresses
- Classes A, B, and C are now deprecated
- Classes D and E are still in use, but are referred to as **ranges**

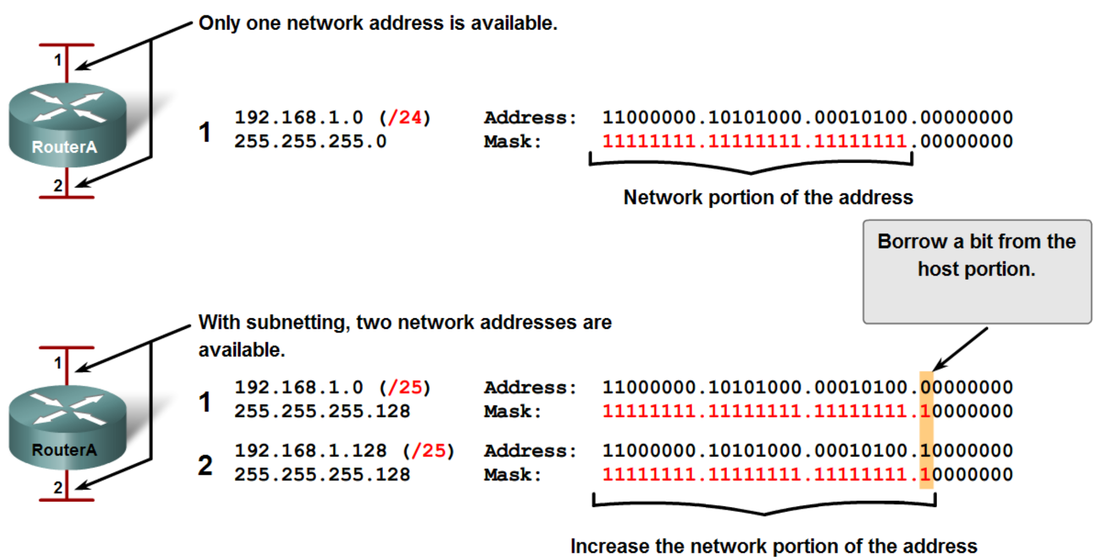
Address Class	First Octet Range	First Octet Bits	Subnet Mask	Network / Host Portions	Number of Hosts
A	1—127	**0**0000001—**0**1111111	255.0.0.0	N.H.H.H	16,777,214
B	128—191	**10**000000—**10**111111	255.255.0.0	N.N.H.H	65,534
C	192—223	**110**00000—**110**11111	255.255.255.0	N.N.N.H	254
D	224—239	**1110**0000—**1110**1111	-	N/A (Multicast)	-
E	240—255	**1111**0000—**1111**1111	-	N/A (Experimental)	-

Classless Addressing

- Because of the finite number of IPv4 addresses, the Internet has moved to a 'classless' addressing scheme.
- Classless addressing allows blocks of IP addresses to be assigned to an organisation based on their size.
- These blocks can be further subdivided at the discretion of the network administrator.

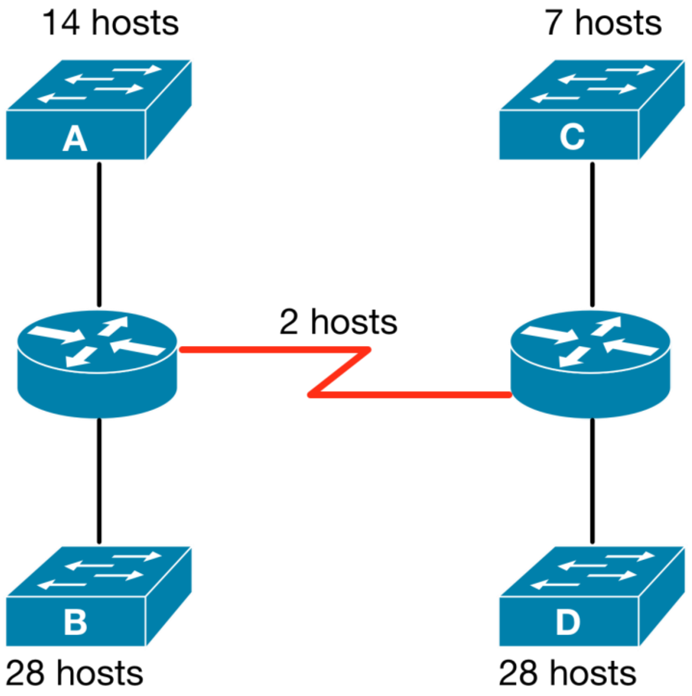
Subnetting using VLSM

- We borrow bits from the host portion to create subnets
- Traditionally subnets were all the same size, but this approach is wasteful
- Instead, we now use an approach called **Variable Length Subnet Masks (VLSM)**
    - Allows each subnet to be provisioned to the most appropriate size



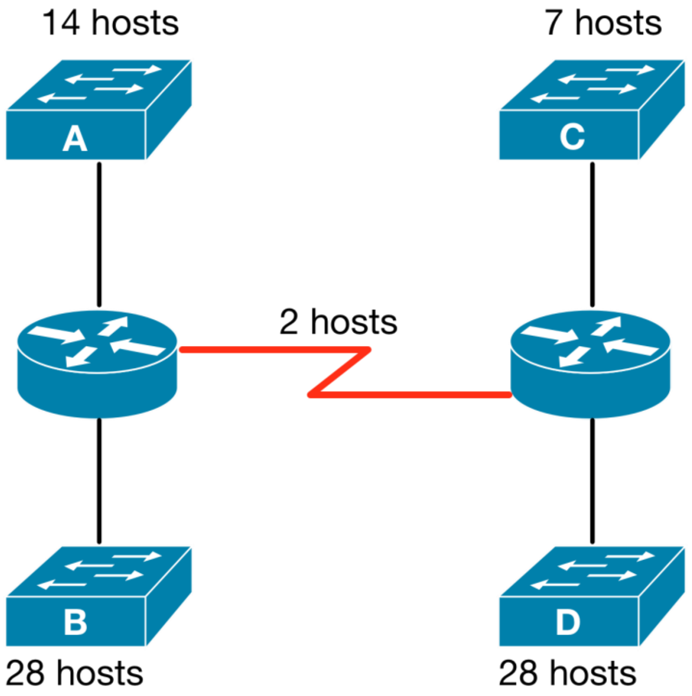
Subnetting using VLSM – An Example

- Consider this network topology and design an addressing scheme using the 192.168.1.0/24 range
- How many subnets are there in this topology?
- Order them from largest to smallest



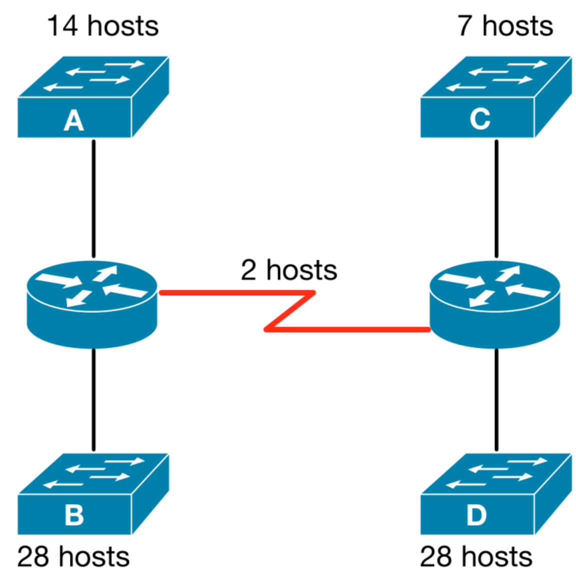
Subnetting using VLSM – An Example

- 5 subnets shown in diagram of:
  - 28 hosts
  - 28 hosts
  - 14 hosts
  - 7 hosts
  - 2 hosts
- How many bits are required to accommodate each subnet?



Subnetting using VLSM – An Example

- We can figure this out using the formula:
  - $2^n - 2$
  - n represents the number of host bits needed
- Host bits required for each subnet:
  - 28 hosts → 5 bits
  - 28 hosts → 5 bits
  - 14 hosts → 4 bits
  - 7 hosts → 4 bits
  - 2 hosts → 2 bits



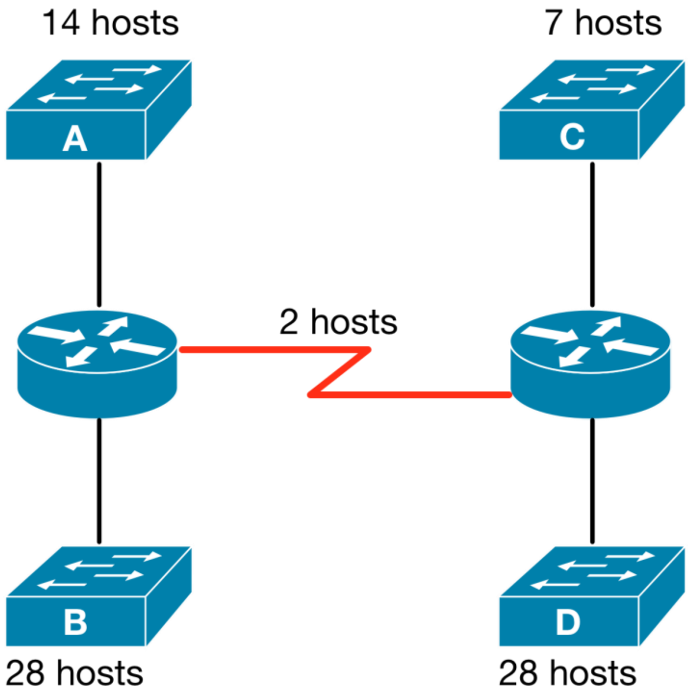
2^0	1
2^1	2
2^2	4
2^3	8
2^4	16
2^5	32
2^6	64
2^7	128

Murdoch UNIVERSITY

Subnetting using VLSM – An Example

- Where to from here?
- There are different methods for VLSM, but we'll use the binary method
- We should ultimately end up with:

B	192.168.1.0/27
D	192.168.1.32/27
A	192.168.1.64/28
C	192.168.1.80/28
WAN	192.168.1.96/30



Murdoch UNIVERSITY

Alternative Approaches to VLSM

- People learn to 'count' subnets
  - Simply add x number to the previous subnet address
  - OK, but potentially error-prone
- Another approach is to use a VLSM chart
  - Not recommended; you won't ever get one in an assessment
- There are also subnetting calculators
  - Also won't be available in assessments

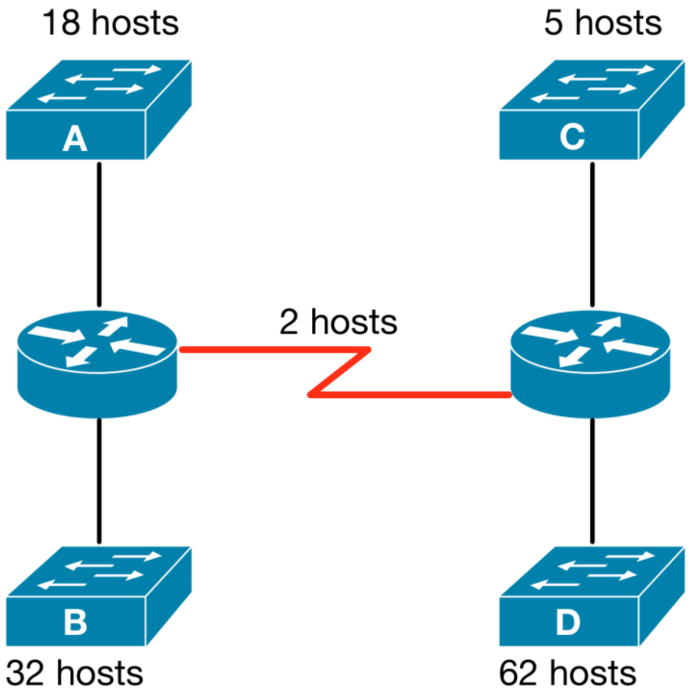
4/13/2007

Subnet Addressing for Last Octet	/25 (1 subnet bit) 2 subnets 126 hosts	/26 (2 subnet bits) 4 subnets 62 hosts	/27 (3 subnet bits) 8 subnets 30 hosts	/28 (4 subnet bits) 16 subnets 14 hosts	/29 (5 subnet bits) 32 subnets 6 hosts	/30 (6 subnet bits) 64 subnets 2 hsots
.0	.0	.0 (.1- .62)	.0 .1- .30)	.0 (.1- .14)	.0 (.1- .6)	.0 (.1- .2)
.4						.4 (.5- .6)
.8					.8 (.9- .14)	.8 (.9- .10)
.12						.12 (.13- .14)
.16				.16 (.17- .30)	.16 (.17- .22)	.16 (.17- .18)
.20						.20 (.21- .22)
.24					.24 (.25- .30)	.24 (.25- .26)
.28						.28 (.29- .30)
.32			.32 33- .62)	.32 (.33- .46)	.32 (.33- .38)	.32 (.33- .34)
.36						.36 (.37- .38)
.40					.40 (.41- .46)	.40 (.41- .42)
.44						.44 (.45- .46)
.48				.48 (.49- .62)	.48 (.49- .54)	.48 (.49- .50)
.52						.52 (.53- .54)
.56					.56 (.57- .62)	.56 (.57- .58)
.60						.60 (.61- .62)
.64		.64 (.65- .126)	.64 (.65- .94)	.64 (.65- .78)	.64 (.65- .70)	.64 (.65- .66)
.68						.68 (.69- .70)
.72					.72 (.73- .78)	.72 (.73- .74)
.76						.76 (.77- .78)
.80				.80 (.81- .94)	.80 (.81- .86)	.80 (.81- .82)
.84						.84 (.85- .86)
.88					.88 (.89- .94)	.88 (.89- .90)
.92						.92 (.93- .94)
.96			.96 (.97- .126)	.96 (.97- .110)	.96 (.97- .102)	.96 (.97- .98)
.100						.100 (.101- .102)
.104					.104 (.105- .110)	.104 (.105- .106)
.108						.108 (.109- .110)
.112				.112 (.113- .126)	.112 (.113- .118)	.112 (.113- .114)
.116						.116 (.117- .118)
.120					.120 (.121- .126)	.120 (.121- .122)
.124						.124 (.125- .126)
.128	.128	.128 (.129- .190)	.128 (.129- .158)	.128 (.129- .142)	.128 (.129- .134)	.128 (.129- .130)
.132						.132 (.133- .134)
.136					.136 (.137- .142)	.136 (.137- .138)
.140						.140 (.141- .142)
.144				.144 (.145- .158)	.144 (.145- .150)	.144 (.145- .146)
.148						.148 (.149- .150)
.152					.152 (.153- .158)	.152 (.153- .154)
.156						.156 (.157- .158)
.160			.160 (.161- .190)	.160 (.161- .174)	.160 (.161- .166)	.160 (.161- .162)
.164						.164 (.165- .166)
.168					.168 (.169- .174)	.168 (.169- .170)
.172						.172 (.173- .174)
.176				.176 (.177- .190)	.176 (.177- .182)	.176 (.177- .178)
.180						.180 (.181- .182)
.184					.184 (.185- .190)	.184 (.185- .186)
.188						.188 (.189- .190)
.192		.192 (.193- .254)	.192 (.193- .222)	.192 (.193- .206)	.192 (.193- .198)	.192 (.193- .194)
.196						.196 (.197- .198)
.200					.200 (.201- .206)	.200 (.201- .202)
.204						.204 (.205- .206)
.208				.208 (.209- .222)	.208 (.209- .214)	.208 (.209- .210)
.212						.212 (.213- .214)
.216					.216 (.217- .222)	.216 (.217- .218)
.220						.220 (.221- .222)
.224			.224 (.225- .254)	.224 (.225- .238)	.224 (.225- .230)	.224 (.225- .226)
.228						.228 (.229- .230)
.232					.232 (.233- .238)	.232 (.233- .234)
.236						.236 (.237- .238)
.240				.240 (.241- .254)	.240 (.241- .246)	.240 (.241- .242)
.244						.244 (.245- .246)
.248					.248 (.249- .254)	.248 (.249- .250)
.252						.252 (.253- .254)
	/25 (1 subnet bit) 2 subnets 126 hosts	/26 (2 subnet bits) 4 subnets 62 hosts	/27 (3 subnet bits) 8 subnets 30 hosts	/28 (4 subnet bits) 16 subnets 14 hosts	/29 (5 subnet bits) 32 subnets 6 hosts	/30 (6 subnet bits) 64 subnets 2 hsots

Originally Authored by Dale Henninger
Compiled by Lee Toderick

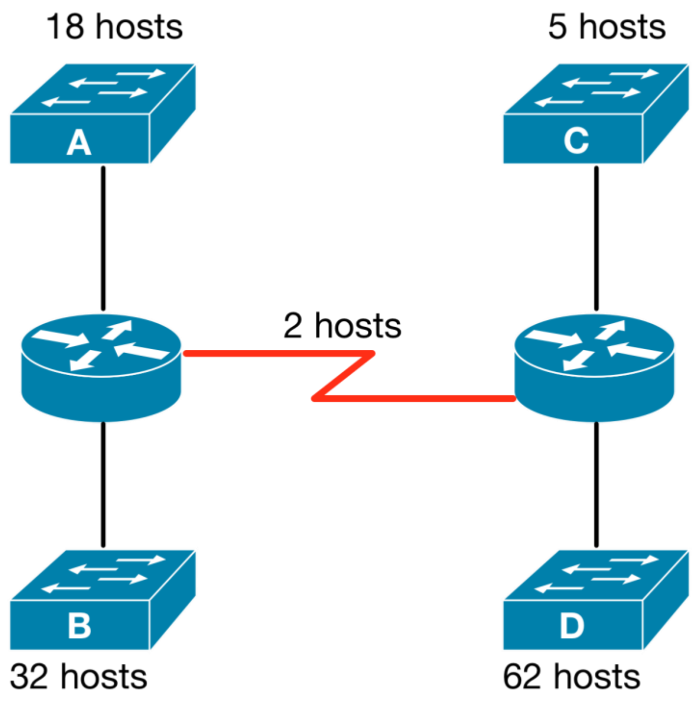
Subnetting using VLSM – A Problem

- Consider this network topology and design an addressing scheme using the 192.168.1.0/24 range
- How many subnets are there in this topology?
- Remember, subnets should be ordered them from largest to smallest



Subnetting using VLSM – A Problem

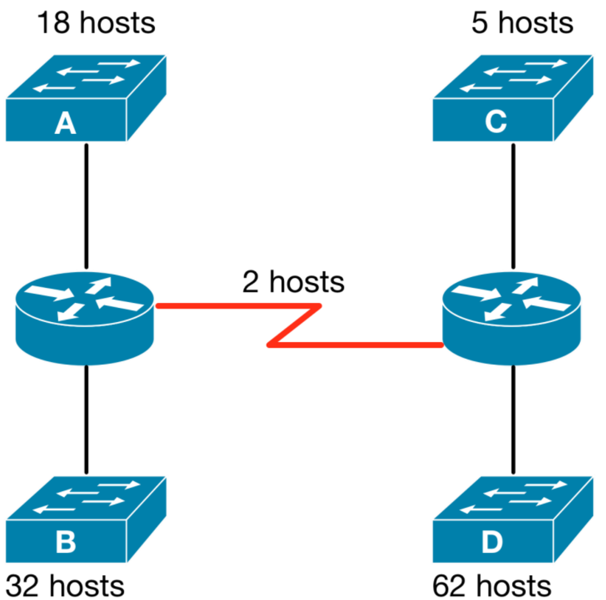
- 5 subnets shown in diagram of:
  - 62 hosts
  - 32 hosts
  - 18 hosts
  - 5 hosts
  - 2 hosts
- How many bits are required to accommodate each subnet?



Murdoch UNIVERSITY

Subnetting using VLSM – A Problem

- Remember, we can figure this out using our powers of two
- Host bits required for each subnet:
    - 62 hosts → 6 bits
    - 32 hosts → 6 bits
    - 18 hosts → 5 bits
    - 5 hosts → 3 bits
    - 2 hosts → 2 bits



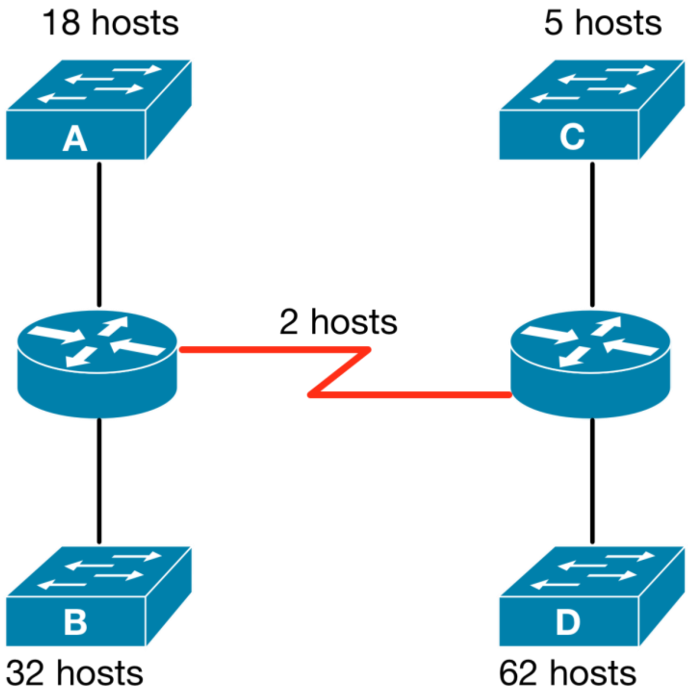
2^0	1
2^1	2
2^2	4
2^3	8
2^4	16
2^5	32
2^6	64
2^7	128

Murdoch UNIVERSITY

Subnetting using VLSM – A Problem

- Now back to the binary
- We should end up with:

D	192.168.1.0/26
B	192.168.1.64/26
A	192.168.1.128/27
C	192.168.1.144/29
WAN	192.168.1.152/30



Internet Control Message Protocol (ICMP)

- Network layer protocol used for managing Internet connections
- Adjunct to (runs on top of) IP
- Used by routers to send error messages to senders (eg. When TTL expires)
- Also used by *ping* and *traceroute* for testing network connectivity

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	Type								Code								Checksum															
4	32	Rest of Header																															

Source: Wikipedia

Lecture Objectives

You should now be able to:

- Describe the purpose of the network layer
- Describe the encapsulation process
- Identify network layer protocols
- Identify an IP version 4 address
- Describe the components of an IP version 4 address
- Describe the different types of IP transmissions
- Represent binary numbers in decimal
- Represent decimal numbers in binary
- Describe the purpose of the subnet mask
- Differentiate between classful and classless IP addressing

Lecture Summary and the Week Ahead

- Today's lecture has examined the role of the OSI network layer with specific focus on IPv4
- We also looked at converting between binary and decimal, as well as subnetting using VLSM
- The readings for this week are Introduction to Networks Chapters 6, 7, and 8
- Binary maths and VLSM handouts available on LMS
- In the labs: More Subnetting!
    - Make sure you attend; subnetting is a vital skill in data communications!

Murdoch UNIVERSITY

Additional Subnetting Resources

Binary to Decimal Conversion:

https://static-course-assets.s3.amazonaws.com/ITN51/en/index.html#7.1.1.4

Decimal to Binary Conversion:

https://static-course-assets.s3.amazonaws.com/ITN51/en/index.html#7.1.1.7

Binary Game:

https://learningnetwork.cisco.com/docs/DOC-1803

Next Week

- We’ll move down the OSI model once again and take a closer look at the Data Link and Physical layers
- Data Link sublayers: Medium Access Control (MAC) and Logical Link Control (LLC)
- Different media for data transmission
    - Coaxial cable
    - Twisted pair
    - Fibre
    - Radio frequencies

Murdoch UNIVERSITY