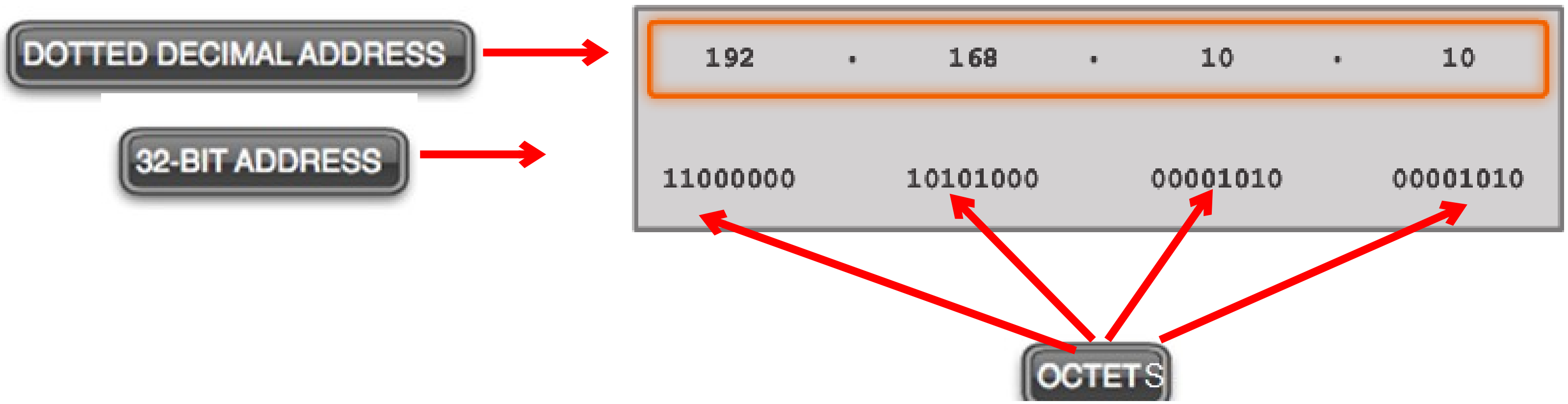
IP addressing & Subnet

Dr. Md. Shohrab Hossain
Professor, CSE, BUET

Slide Source: Cisco Networking

- IP addressing
- Public / Private IP address
- Network Address Translation
- Subnetting

Binary Number System



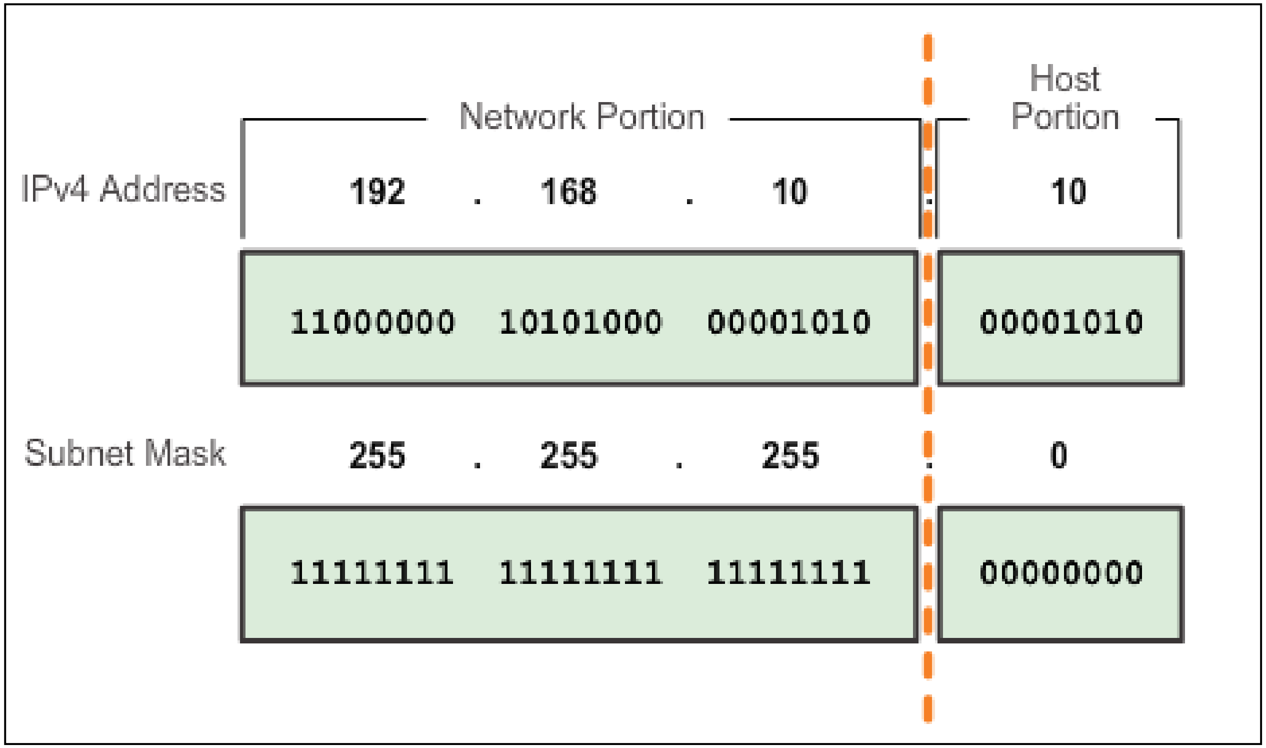
Radix	2	2	2	2	2	2	2	2
Exponent	7	6	5	4	3	2	1	0
Octet Bit Values	128	64	32	16	8	4	2	1
Binary Address	1	1	0	0	0	0	0	0
Binary Bit Values	128	64	0	0	0	0	0	0

Add the binary bit values.

128 + 64 = 192

Network Portion and Host Portion of an IPv4 Address

- The subnet mask just says where to look for the network portion in a given IPv4 address



Bitwise AND Operation

IPv4 Address	192	168	10	10
	11000000	10101000	00001010	00001010
Subnet Mask	255	255	255	0
	11111111	11111111	11111111	00000000
Network Address	192	168	10	0
	11000000	10101000	00001010	00000000

IPv4 Subnet masks

Valid Subnet Masks

Subnet Value	128	64	32	16	8	4	2	1
255	1	1	1	1	1	1	1	1
254	1	1	1	1	1	1	1	0
252	1	1	1	1	1	1	0	0
248	1	1	1	1	1	0	0	0
240	1	1	1	1	0	0	0	0
224	1	1	1	0	0	0	0	0
192	1	1	0	0	0	0	0	0
128	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

(Bit Value header spans columns 128 through 1.)

Network Address and Broadcast address

- For a network, 192.168.10.0/24 network

  There are 8-bit allocated for host part.

- Network Address:
  - All 0’s in the host part: 0000 0000 = 0
  - So, network address = 192.168.10.0
- Broadcast address:
  - All 1’s in the host part: 1111 1111 = 255
  - So, broadcast address = 192.168.10.255
- IP range: 1- 254

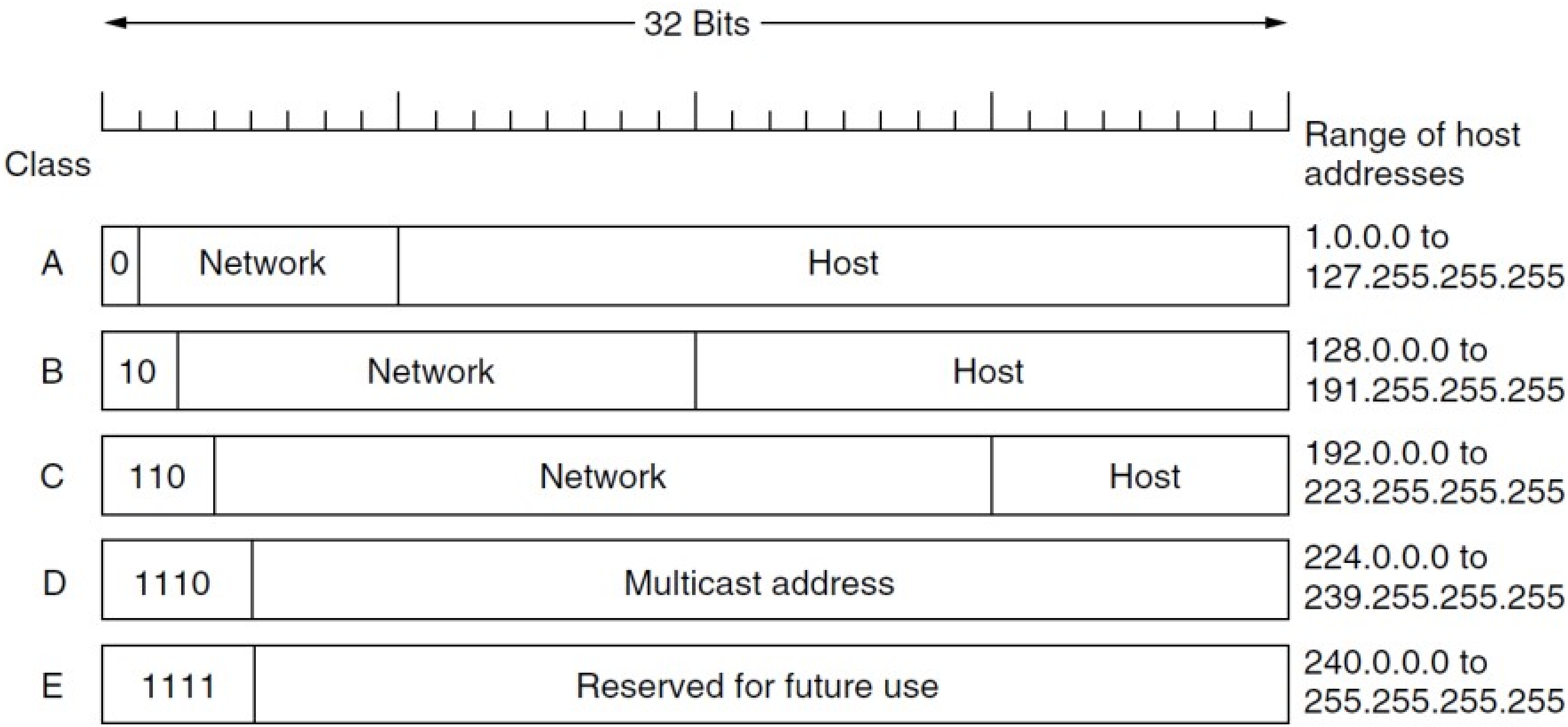
Types of IPv4 Address

Legacy Classful Addressing

IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

Classful Addressing



Classless Addressing

- Formal name is Classless Inter-Domain Routing (CIDR)

- Created a new set of standards that allowed service providers to allocate IPv4 addresses on any address bit boundary (prefix length) instead of only by a class A, B, or C address

- Example:
  192.168.10.0/23

Examining the Prefix Length

	Dotted Decimal	Significant bits shown in binary
Network Address	**10.1.1.0/24**	**10.1.1.00000000**
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.254	10.1.1.11111110
Broadcast Address	10.1.1.255	10.1.1.11111111
Number of hosts: 2^8 – 2 = 254 hosts		

Network Address	**10.1.1.0/25**	**10.1.1.00000000**
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.126	10.1.1.01111110
Broadcast Address	10.1.1.127	10.1.1.01111111
Number of hosts: 2^7 – 2 = 126 hosts		

Network Address	**10.1.1.0/26**	**10.1.1.00000000**
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.62	10.1.1.00111110
Broadcast Address	10.1.1.63	10.1.1.00111111
Number of hosts: 2^6 – 2 = 62 hosts		

Examining the Prefix Length (cont.)

	Dotted Decimal	Significant bits shown in binary
Network Address	**10.1.1.0/27**	**10.1.1.00000000**
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.30	10.1.1.00011110
Broadcast Address	10.1.1.31	10.1.1.00011111
Number of hosts: 2^5 – 2 = 30 hosts		

Network Address	**10.1.1.0/28**	**10.1.1.00000000**
First Host Address	10.1.1.1	10.1.1.00000001
Last Host Address	10.1.1.14	10.1.1.00001110
Broadcast Address	10.1.1.15	10.1.1.00001111
Number of hosts: 2^4 – 2 = 14 hosts		

Private IP address

Public and Private IPv4 Addresses

Private address blocks are:

- Hosts that do not require access to the Internet can use private addresses
  - 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
  - 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
  - 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)

- Not globally routable
- Address translation is done at Router to convert private IP into Public IP address and vice versa

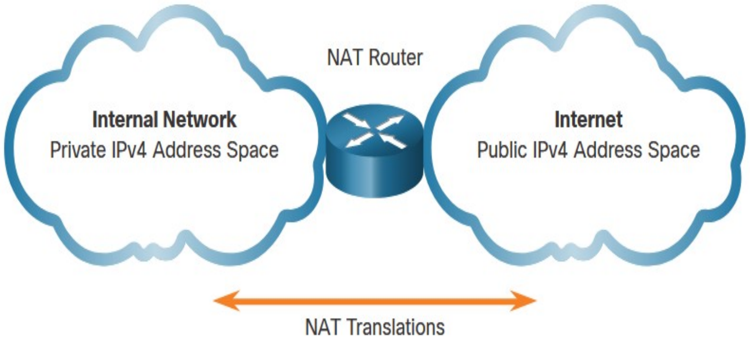
What is NAT?

- NAT is a process used to translate network addresses.
- NAT's primary use is to conserve public IPv4 addresses.
- NAT is usually implemented at border network devices, such as firewalls or routers.
- NAT allows the networks to use private addresses internally, only translating to public addresses when needed.
- Devices within the organization can be assigned private addresses and operate with locally unique addresses.
- When traffic must be sent or received to or from other organizations or the Internet, the border router translates the addresses to a public and globally unique address.

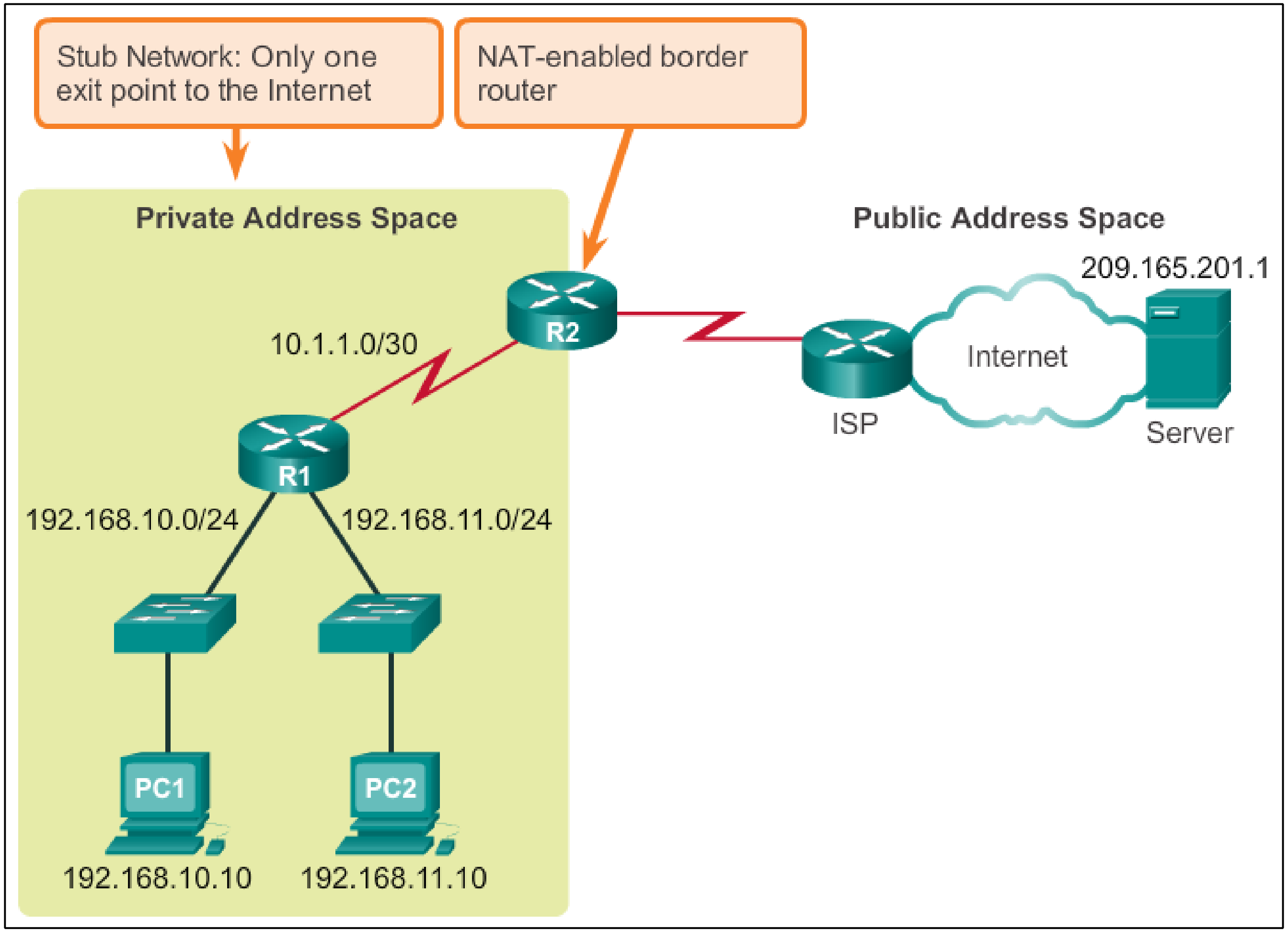
NAT Characteristics
IPv4 Address Space

- Networks are commonly implemented using private IPv4 addresses, as defined in RFC 1918.
- Private IPv4 addresses cannot be routed over the internet and are used within an organization or site to allow devices to communicate locally.
- To allow a device with a private IPv4 address to access devices and resources outside of the local network, the private address must first be translated to a public address.
- NAT provides the translation of private addresses to public addresses.

Class	Activity Type	Activity Name
A	10.0.0.0 – 10.255.255.255	10.0.0.0/8
B	172.16.0.0 – 172.31.255.255	172.16.0.0/12
C	192.168.0.0 – 192.168.255.255	192.168.0.0/16



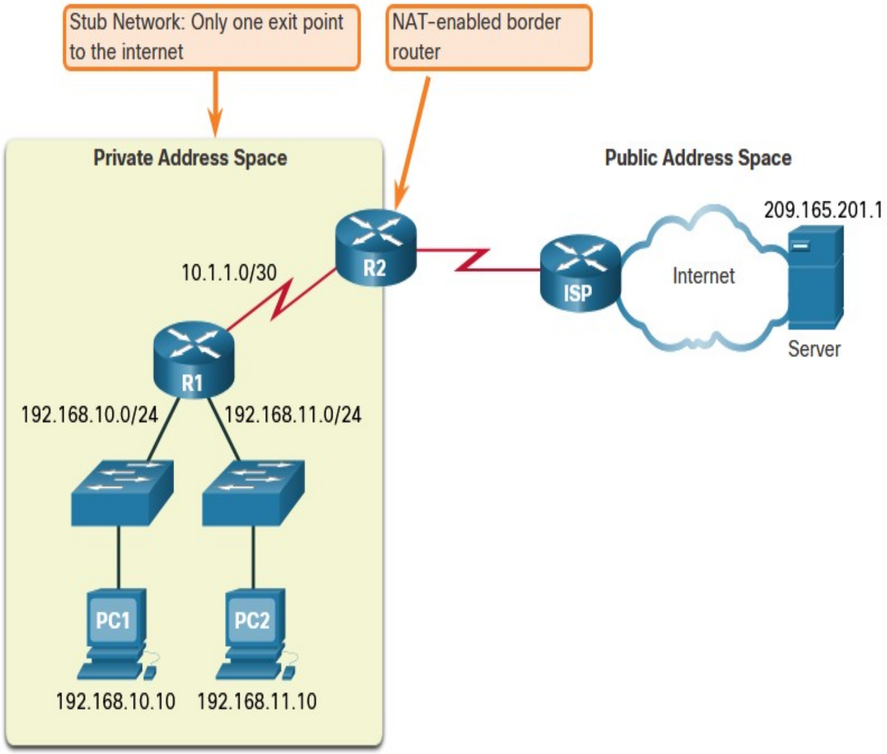
NAT



Stub Network: Only one exit point to the Internet
NAT-enabled border router
Private Address Space
Public Address Space
209.165.201.1
R2
10.1.1.0/30
Internet
ISP
Server
R1
192.168.10.0/24
192.168.11.0/24
PC1
PC2
192.168.10.10
192.168.11.10

NAT Characteristics
What is NAT

- The primary use of NAT is to conserve public IPv4 addresses.
- NAT allows networks to use private IPv4 addresses internally and translates them to a public address when needed.
- A NAT router typically operates at the border of a stub network.
- When a device inside the stub network wants to communicate with a device outside of its network, the packet is forwarded to the border router which performs the NAT process, translating the internal private address of the device to a public, outside, routable address.



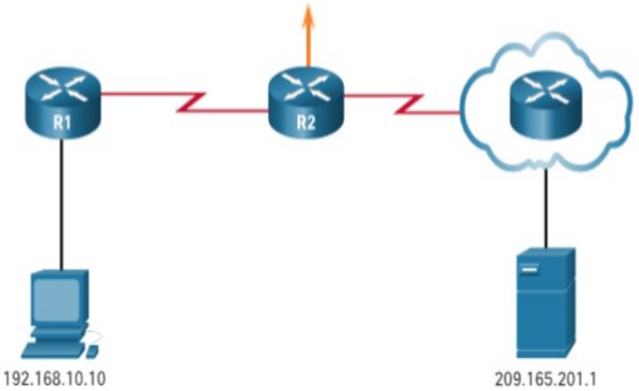
How NAT Works

PC1 wants to communicate with an outside web server with public address 209.165.201.1.

1. PC1 sends a packet addressed to the web server.
2. R2 receives the packet and reads the source IPv4 address to determine if it needs translation.
3. R2 adds mapping of the local to global address to the NAT table.
4. R2 sends the packet with the translated source address toward the destination.
5. The web server responds with a packet addressed to the inside global address of PC1 (209.165.200.226).
6. R2 receives the packet with destination address 209.165.200.226. R2 checks the NAT table and finds an entry for this mapping. R2 uses this information and translates the inside global address (209.165.200.226) to the inside local address (192.168.10.10), and the packet is forwarded toward PC1.

NAT Table

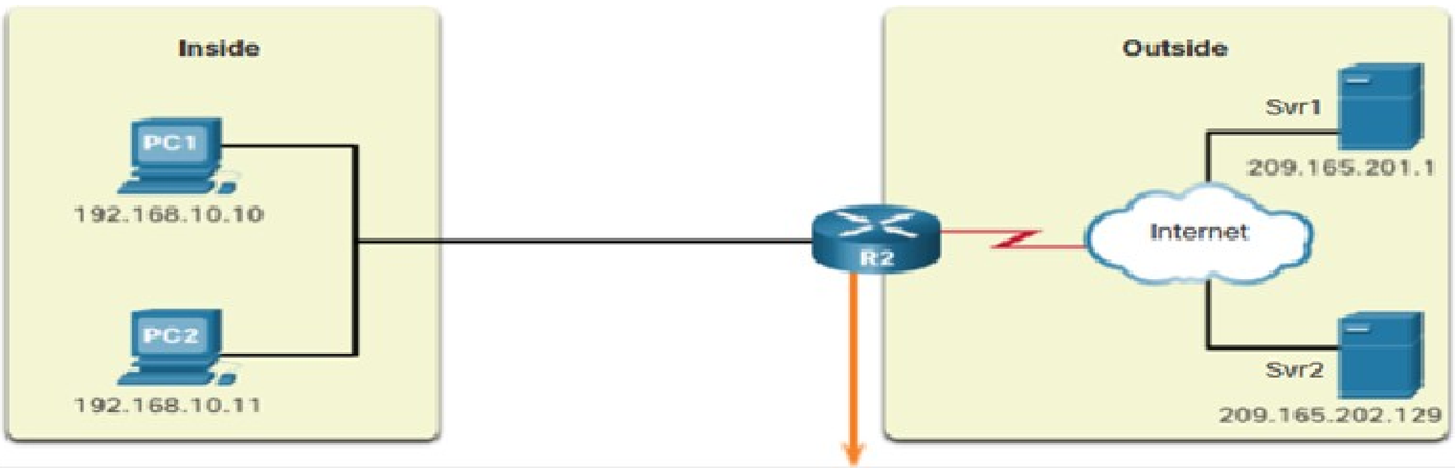
Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



Port Address Translation (PAT)

Port Address Translation (PAT), also known as NAT overload, maps multiple private IPv4 addresses to a single public IPv4 address or a few addresses.

- With PAT, when the NAT router receives a packet from the client, it uses the source port number to uniquely identify the specific NAT translation.
- PAT ensures that devices use a different TCP port number for each session with a server on the internet.



NAT Table with Overload

Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global IP Address
192.168.10.10:1555	209.165.200.226:1555	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1331	209.165.200.226:1331	209.165.202.129:80	209.165.202.129:80

Subnetting

Network Segmentation

Reasons for Subnetting

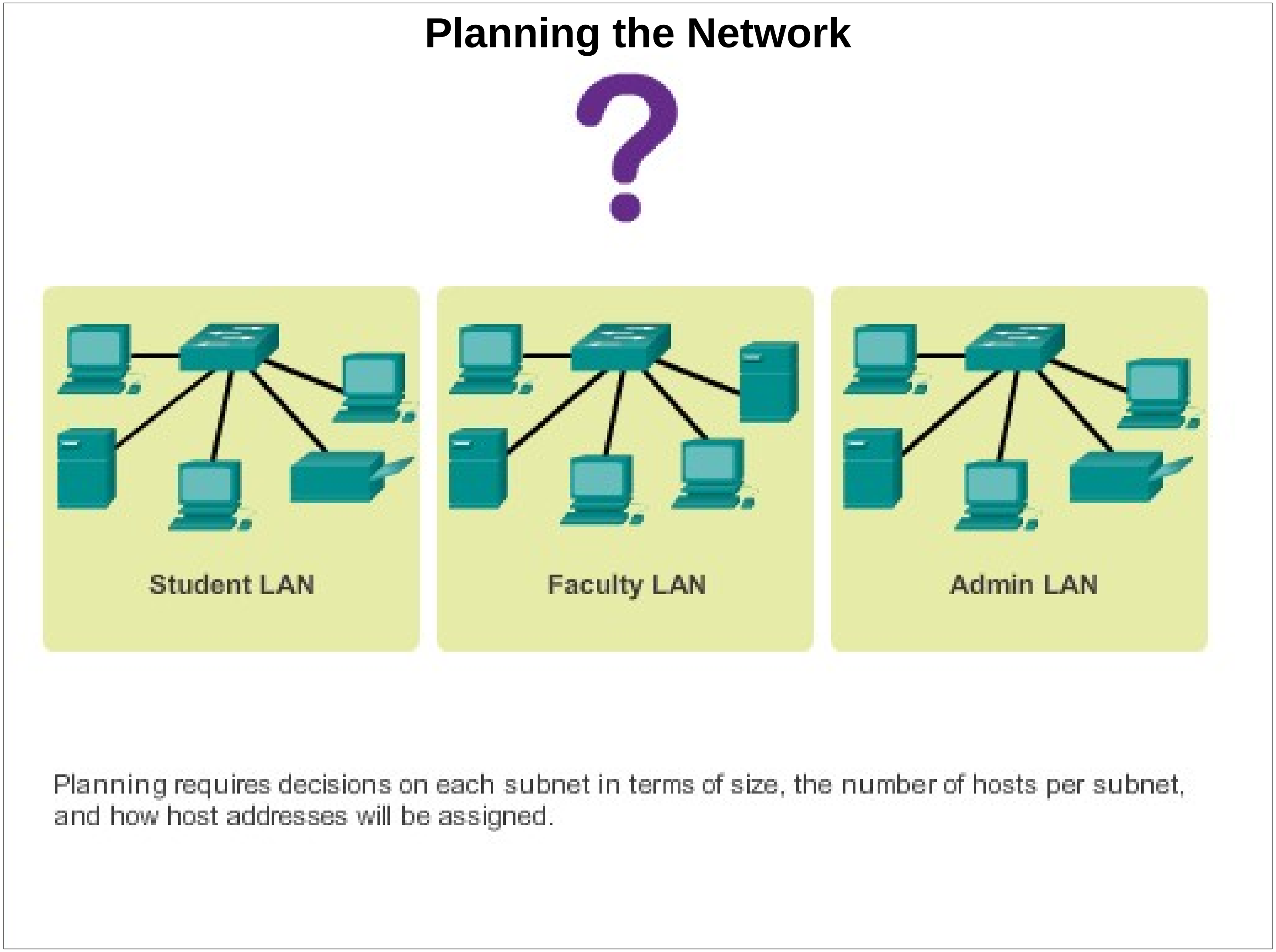
Subnetting is the process of segmenting a network into multiple smaller network spaces called subnetworks or subnets.

- Large networks must be segmented into smaller subnetworks, creating smaller groups of devices and services to:
  - Control traffic by containing broadcast traffic within each subnetwork.
  - Reduce overall network traffic and improve network performance.

Communication Between Subnets

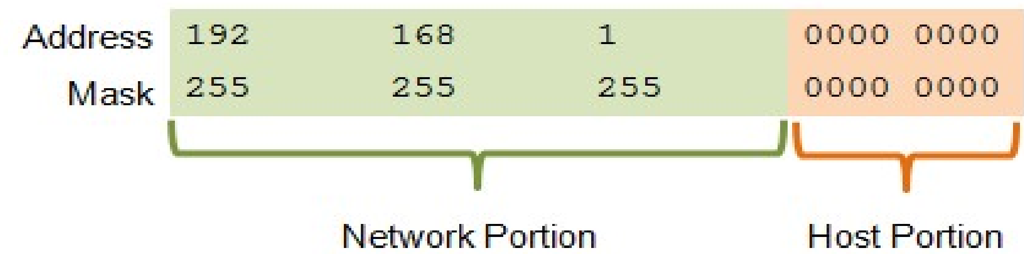
- A router is necessary for devices on different networks and subnets to communicate.
- Devices on a network and subnet use the router interface attached to their LAN as their default gateway.

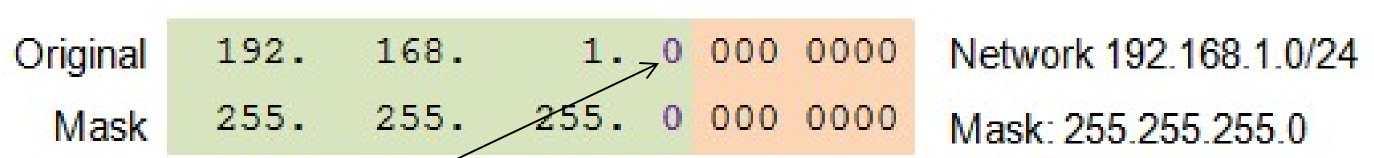
Different networks for different groups



Basic Subnetting

- Borrowing Bits to Create Subnets
- Borrowing 1 bit $2^1 = 2$ subnets





Borrowing 1 Bit from the host portion creates 2 subnets with the same subnet mask

Subnet 0

Network 192.168.1.**0-127**/**25**

Mask: 255.255.255.**128**

Subnet 1

Network 192.168.1.**128-255**/**25**

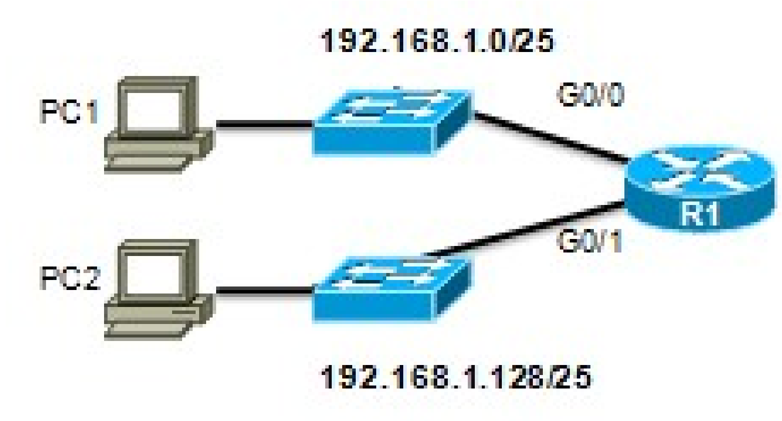
Mask: 255.255.255.**128**

Subnets in Use

Subnets in Use

Subnet 0

Network 192.168.1.**0-127**/**25**



Subnet 1

Network 192.168.1.**128-255**/**25**

Address Range for 192.168.1.0/25 Subnet

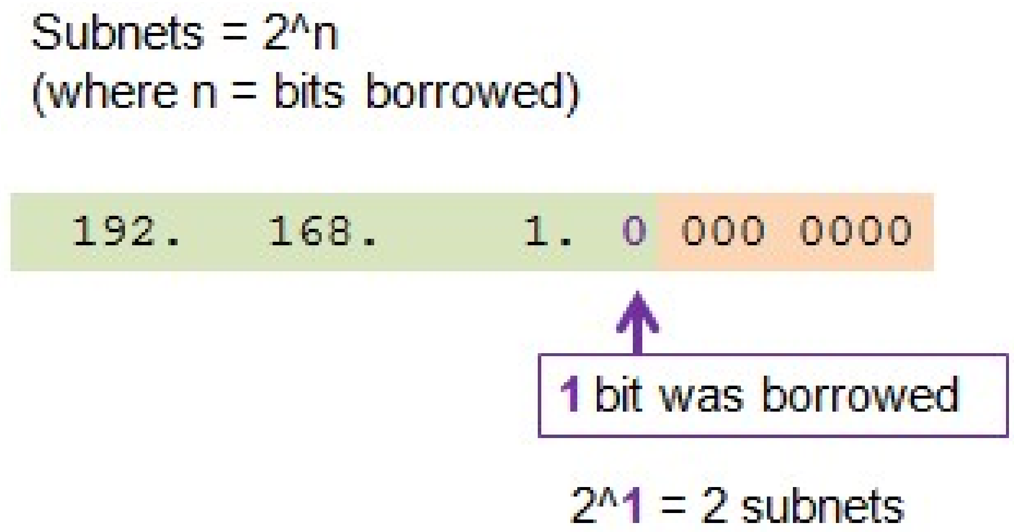
Network Address					
192.	168.	1.	0	000 0000	= 192.168.1.0
First Host Address					
192.	168.	1.	0	000 0001	= 192.168.1.1
Last Host Address					
192.	168.	1.	0	111 1110	= 192.168.1.126
Broadcast Address					
192.	168.	1.	0	111 1111	= 192.168.1.127

Address Range for 192.168.1.128/25 Subnet

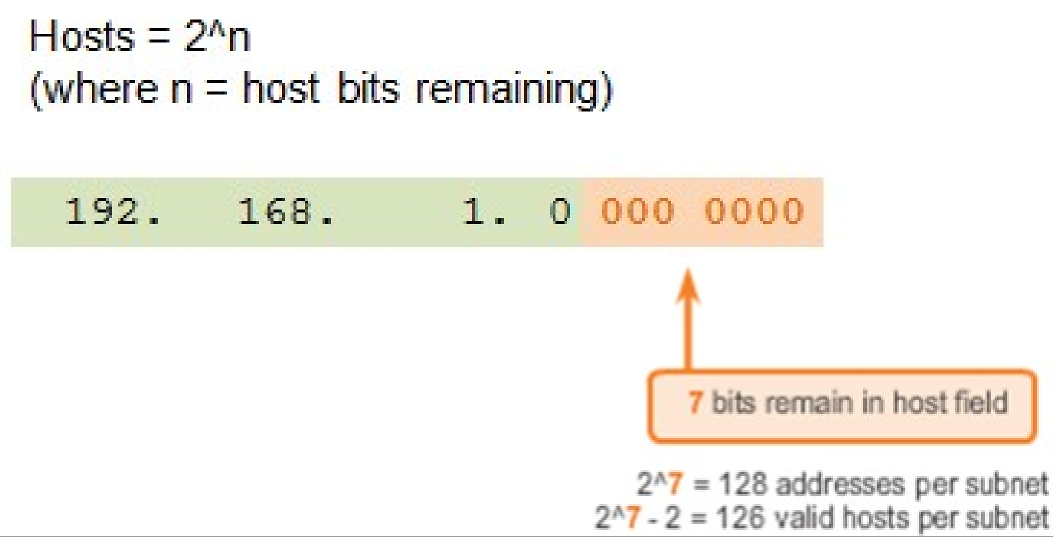
Network Address					
192.	168.	1.	1	000 0000	= 192.168.1.128
First Host Address					
192.	168.	1.	1	000 0001	= 192.168.1.129
Last Host Address					
192.	168.	1.	1	111 1110	= 192.168.1.254
Broadcast Address					
192.	168.	1.	1	111 1111	= 192.168.1.255

Subnetting Formulas

Calculate number of subnets

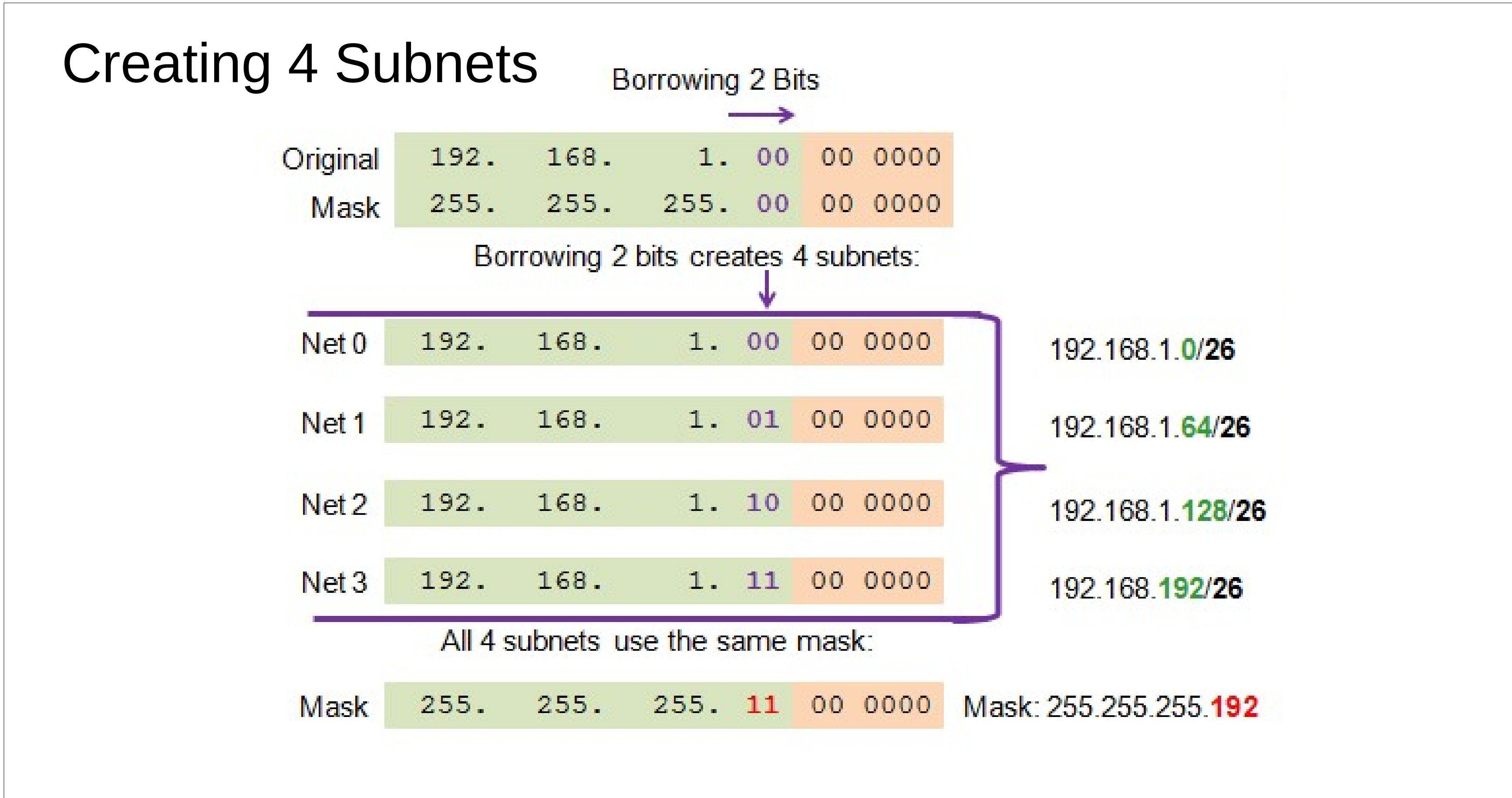


Calculate number of hosts



Creating 4 Subnets

Borrowing 2 bits to create 4 subnets. **2^2 = 4 subnets**



Creating Eight Subnets

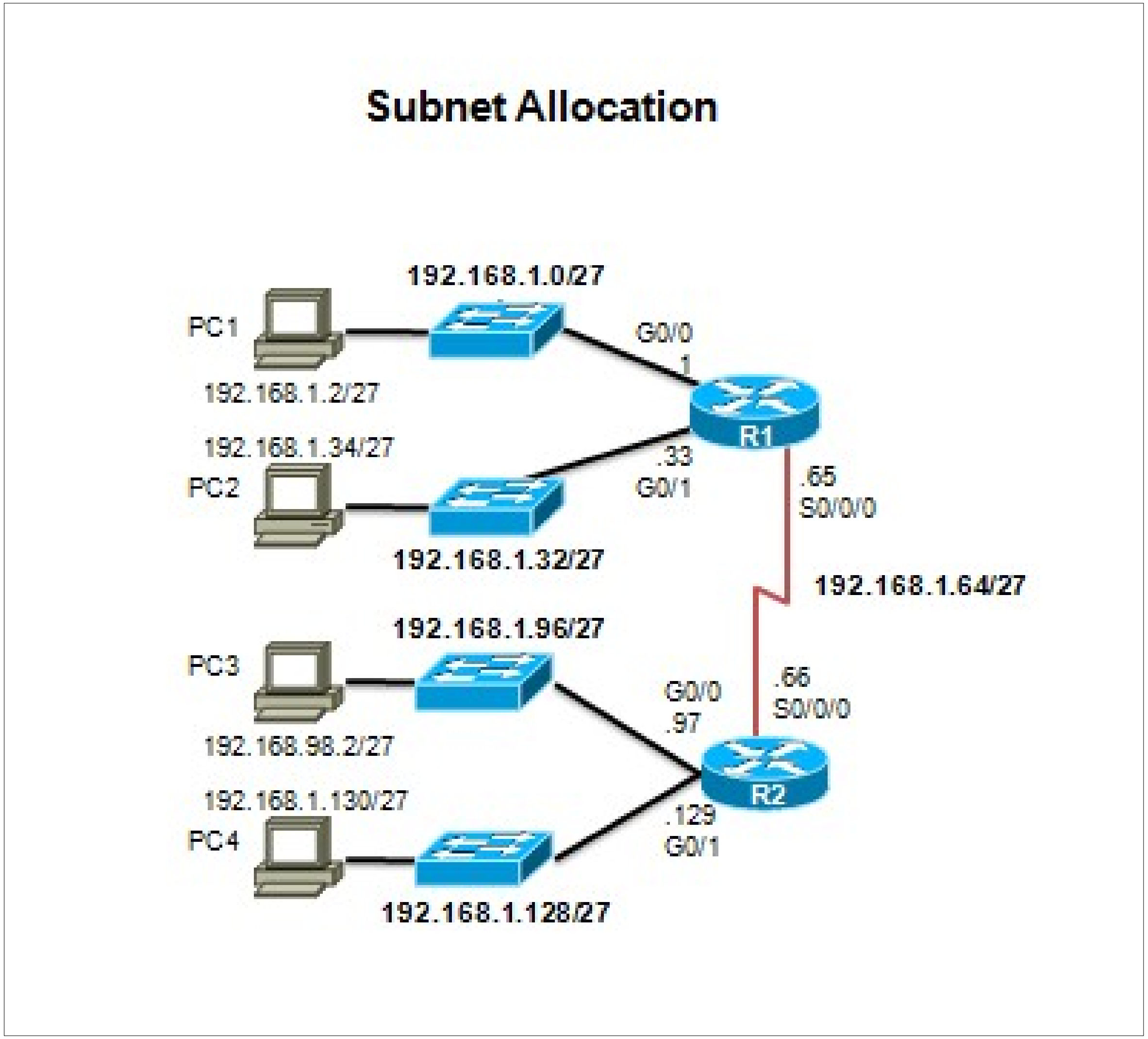
Borrowing 3 bits to **Create 8 Subnets**. **2^3 = 8 subnets**

Net 0	Network	192.	168.	1.	000	0 0000	192.168.1.0
	First	192.	168.	1.	000	0 0001	192.168.1.1
	Last	192.	168.	1.	000	1 1110	192.168.1.30
	Broadcast	192.	168.	1.	000	1 1111	192.168.1.31
Net 1	Network	192.	168.	1.	001	0 0000	192.168.1.32
	First	192.	168.	1.	001	0 0001	192.168.1.33
	Last	192.	168.	1.	001	1 1110	192.168.1.62
	Broadcast	192.	168.	1.	001	1 1111	192.168.1.63
Net 2	Network	192.	168.	1.	010	0 0000	192.168.1.64
	First	192.	168.	1.	010	0 0001	192.168.1.65
	Last	192.	168.	1.	010	1 1110	192.168.1.94
	Broadcast	192.	168.	1.	010	1 1111	192.168.1.95
Net 3	Network	192.	168.	1.	011	0 0000	192.168.1.96
	First	192.	168.	1.	011	0 0001	192.168.1.97
	Last	192.	168.	1.	011	1 1110	192.168.1.126
	Broadcast	192.	168.	1.	011	1 1111	192.168.1.127

Creating Eight Subnets (Cont.)

Net 4	Network	192.	168.	1.	100	0	0000	192.168.1.128
	Fist	192.	168.	1.	100	0	0001	192.168.1.129
	Last	192.	168.	1.	100	1	1110	192.168.1.158
	Broadcast	192.	168.	1.	100	1	1111	192.168.1.159
Net 5	Network	192.	168.	1.	101	0	0000	192.168.1.160
	Fist	192.	168.	1.	101	0	0001	192.168.1.161
	Last	192.	168.	1.	101	1	1110	192.168.1.190
	Broadcast	192.	168.	1.	101	1	1111	192.168.1.191
Net 6	Network	192.	168.	1.	110	0	0000	192.168.1.192
	Fist	192.	168.	1.	110	0	0001	192.168.1.193
	Last	192.	168.	1.	110	1	1110	192.168.1.222
	Broadcast	192.	168.	1.	110	1	1111	192.168.1.223
Net 7	Network	192.	168.	1.	111	0	0000	192.168.1.224
	Fist	192.	168.	1.	111	0	0001	192.168.1.225
	Last	192.	168.	1.	111	1	1110	192.168.1.254
	Broadcast	192.	168.	1.	111	1	1111	192.168.1.255

Creating Eight Subnets (Cont.)



Subnetting Based on Host Requirements

Two considerations when planning subnets:

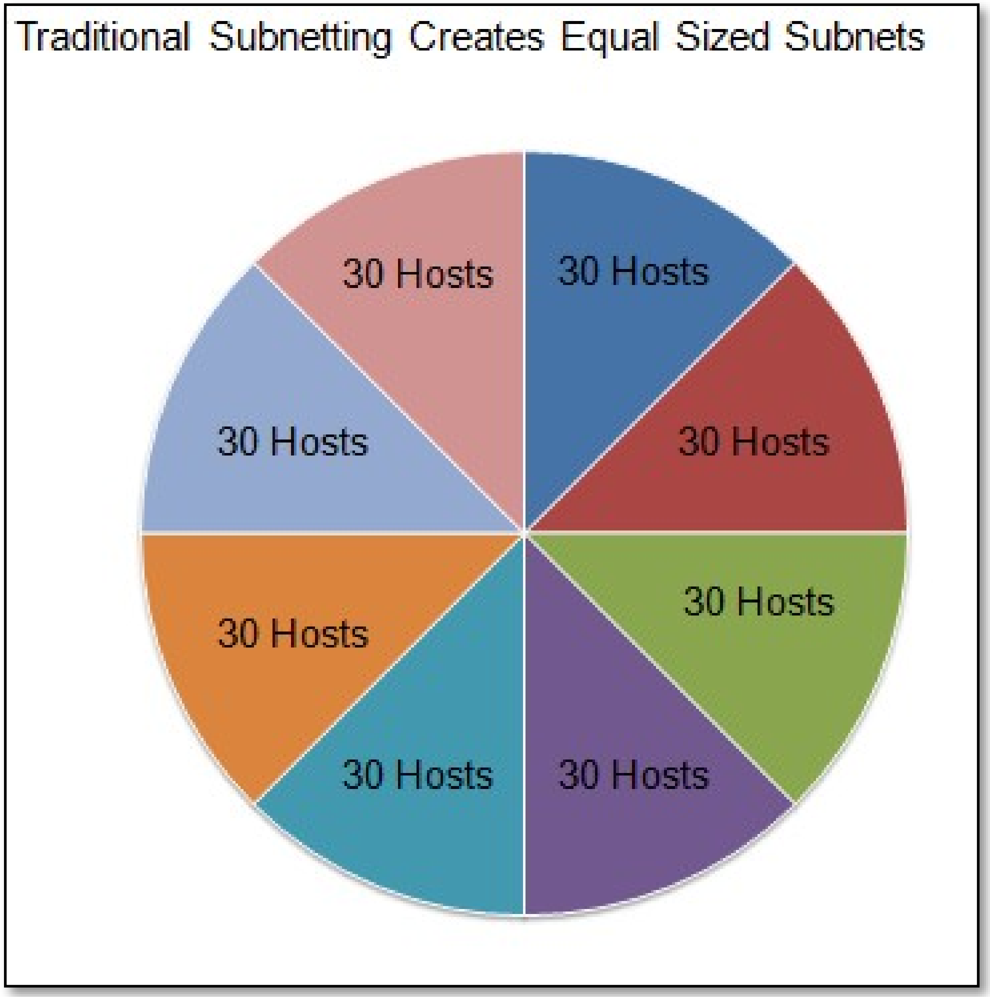
- Number of subnets required
- Number of host addresses required

Formula to determine number of usable hosts: 2^n-2

- 2^*n* (where *n* is the number of remaining host bits) is used to calculate the number of hosts.
- -2 (The subnetwork ID and broadcast address cannot be used on each subnet.)

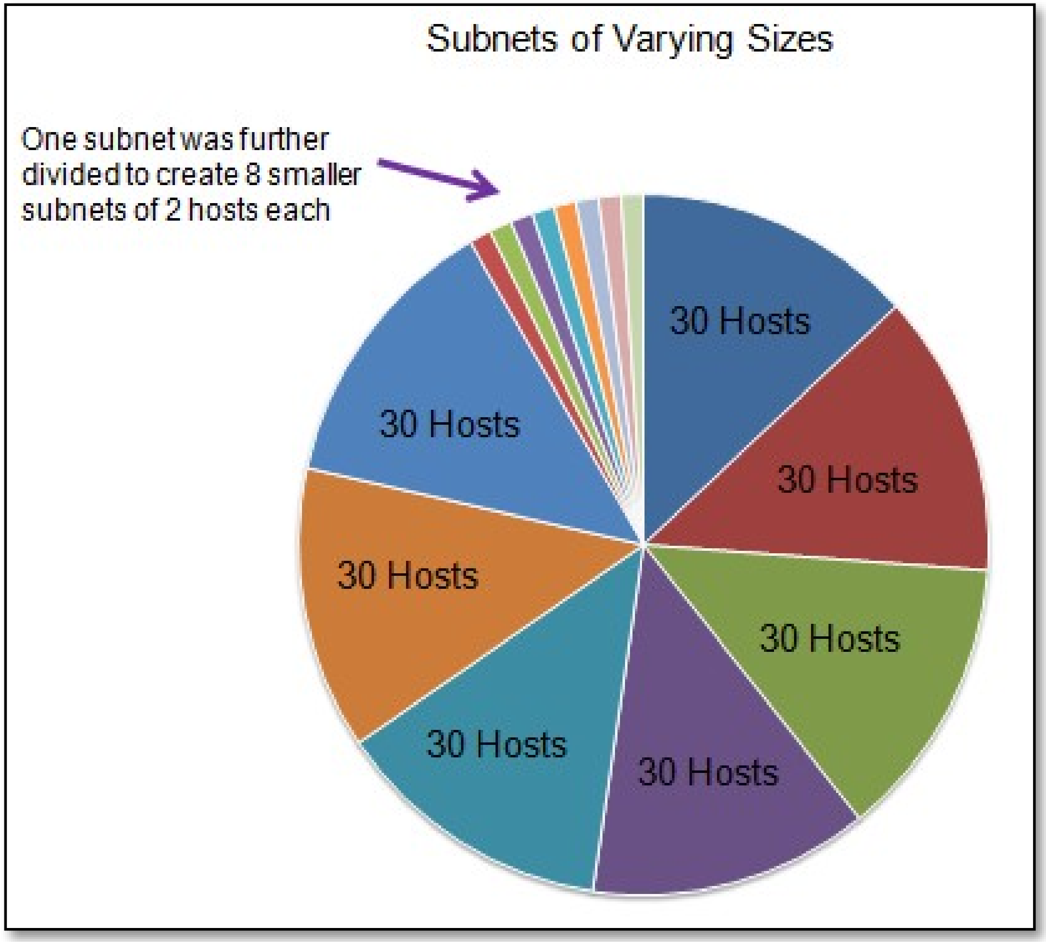
Traditional Subnetting: Equal Addresses

- Subnets that require fewer addresses have unused (wasted) addresses
- For example, WAN links only need two addresses.



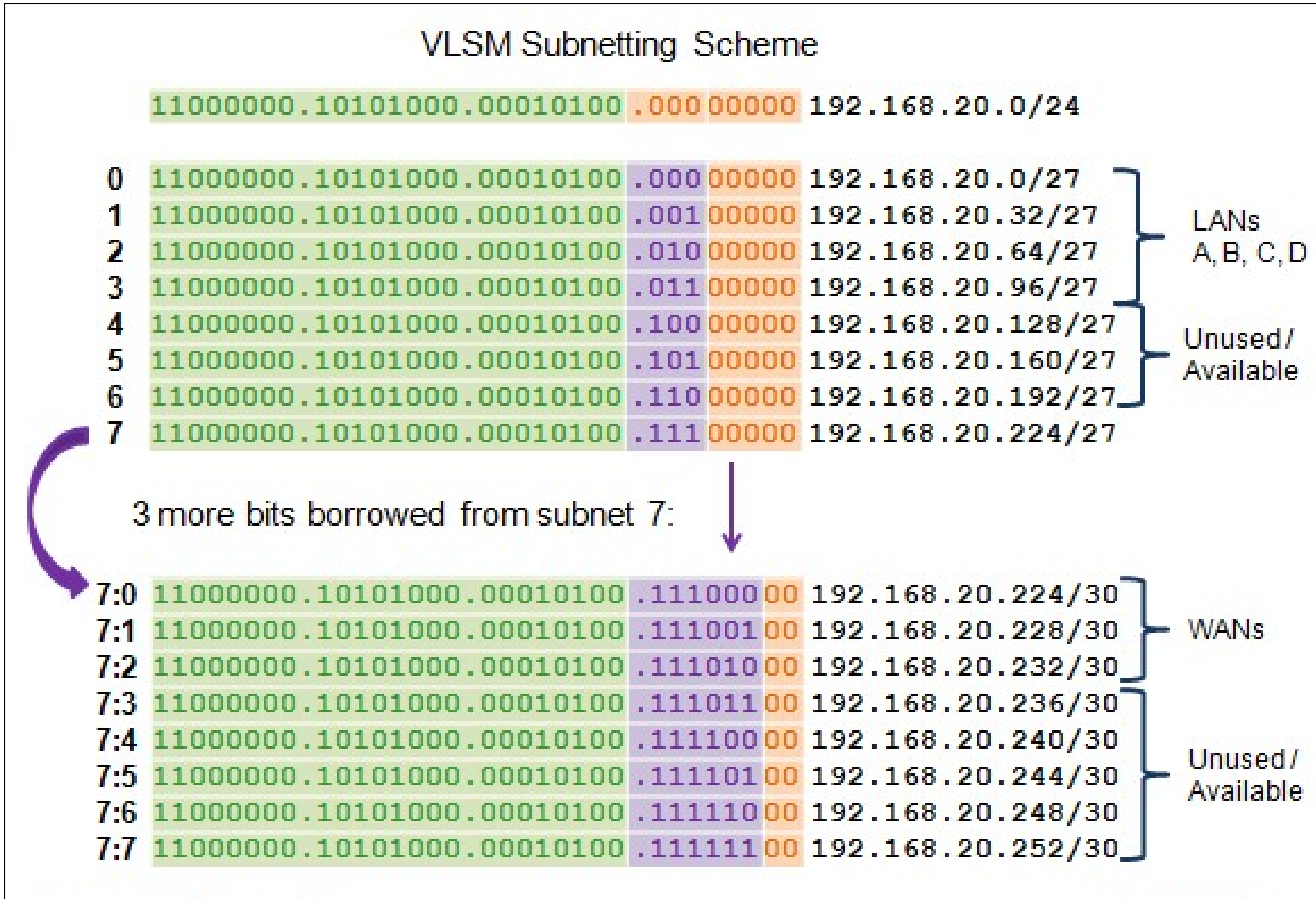
Variable Length Subnet Masks (VLSM)

- The variable-length subnet mask (VLSM) or subnetting a subnet provides more efficient use of addresses.
- VLSM allows a network space to be divided in unequal parts.
- Subnet mask varies, depending on how many bits have been borrowed for a particular subnet.
- Network is first subnetted, and then the subnets are resubnetted.

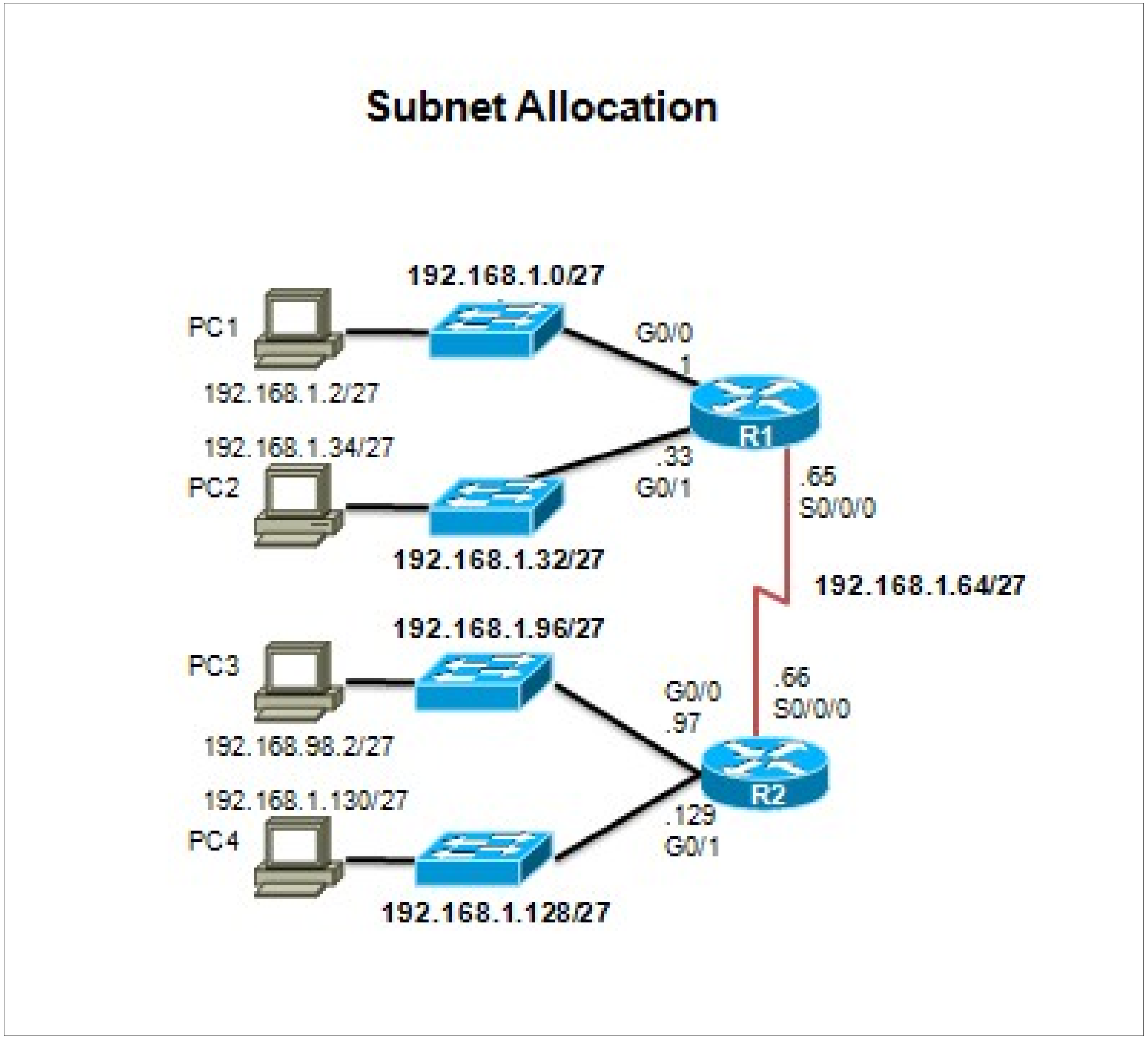


Benefits of Variable Length Subnet Masking

Basic VLSM



Creating Eight Subnets (Cont.)



Let us do another example ..