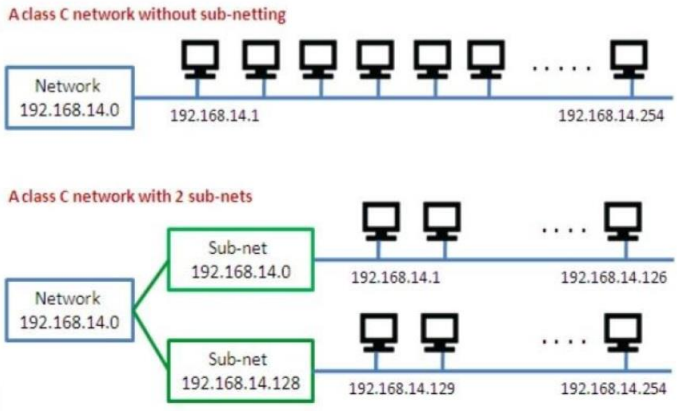
IP Subnetting and Introduction to NAT

CLARUSWAY©
WAY TO REINVENT YOURSELF

Subnetting Basics

- The process of taking an extensive network and splitting into smaller networks is known as subnetting



CLARUSWAY©
WAY TO REINVENT YOURSELF

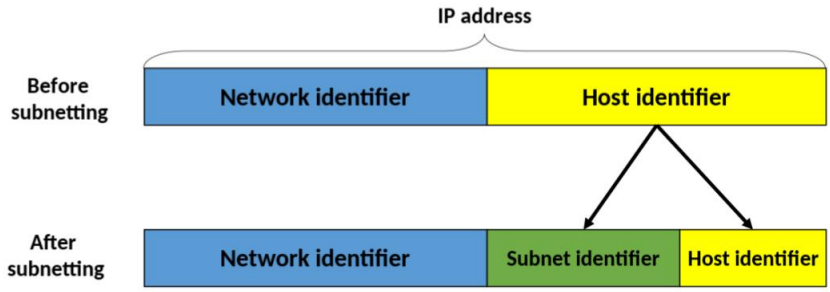
Subnetting Basics

Why to use subnetting?

- Reduced Network Traffic
- Optimized Network Performance
- Simplified Management - Easier to identify and isolate network problems
- Facilitated Spanning of Large Geographical Distances - Connecting multiple smaller networks makes the system more efficient

Subnetting Basics

- IPv4 address is divided into network ID and host ID by using octets
- In subnetting we can borrow some bits from host ID to use as subnetwork



Subnetting Basics

Subnetting IPv4 Address:

- A **Class A**, **B**, or **C** TCP/IP network can be further divided, or subnetted, by a system administrator
- For example, you have 150 hosts on three networks that are connected by a router
- You are allocated a **Class C** address: 192.168.123 Network ID | .0 Host ID
- You can use from 192.168.123 .1 to 192.168.123 .254
  (Just remember that the first and last address in any network or subnet cannot be assigned to any individual host, so you cannot use 192.168.123.0 and 192.168.123.255)

CLARUSWAY© WAY TO REINVENT YOURSELF

7

Subnetting Basics

Subnetting IPv4 Address:

- With the allocated Class C IP address we can map 254 hosts on one network
- But our 150 hosts are located on **three** separate networks
- Instead of requesting more address blocks for each network, we can divide our block into three subnets

CLARUSWAY© WAY TO REINVENT YOURSELF

8

Subnetting Basics

Subnetting IPv4 Address:

- Remember we can create subnets by borrowing bits from Host ID
- We need 3 subnets in total, so if we borrow 1 bit we will get 2 subnets which is not enough
- So we need more bits, if we borrow 2 bits we will get 4 subnets and our subnet mask will be:
  11111111.11111111.11111111.11000000 → 255.255.255.192

Subnetting Basics

Subnetting IPv4 Address:

- Since we borrowed 2 bits, there are only 6 bits left for Host ID which makes 2^6 - 2 = 62 hosts *(first and last numbers are reserved)*
- Our company has **3 networks** and **50 hosts** on each network
- We have **4 subnets**, and **62 host IDs** for each subnet *(that means 1 subnet with 62 host IDs will be reserved for future use)*

Subnetting Basics

Subnetting IPv4 Address:

- Using subnet mask 255.255.255.192, our 192.168.123.0 network will become 4 networks:
  - 192.168.123.0 — 11111111.11111111.11111111.00 000000
  - 192.168.123.64 — 11111111.11111111.11111111.01 000000
  - 192.168.123.128 — 11111111.11111111.11111111.10 000000
  - 192.168.123.192 — 11111111.11111111.11111111.11 000000

- Valid host addresses will be:

  192.168.123.1-62 192.168.123.129-190

  192.168.123.65-126 192.168.123.193-254

(Remember, again, that binary host addresses with all 1s or all 0s are reserved, so you cannot use addresses with the last octet of 0, 63, 64, 127, 128, 191, 192, and 255)

Subnetting Basics

Let's see how this works:

- Assume we have two IP addresses:
  - 192.168.123.71 and 192.168.123.133

- If we used default subnet mask of Class C which is 255.255.255.0 both addresses should be on the same network.

- However we use subnet mask of 255.255.255.192 so
  - 192.168.123.71 host will be on the 192.168.123.64 network
  - 192.168.123.133 host will be on the 192.168.123.128 network

Well done!

Subnetting Basics

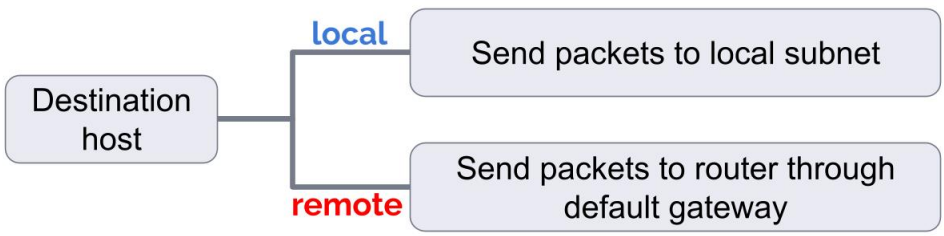
Default gateways

- If a host needs to communicate with a host on another network, it will communicate through a router
- A router specified on a host is called **default gateway**
- So how does TCP/IP knows if the destination host is on the same network or not?

Subnetting Basics

Default gateways

When a host wants to communicate with another device, it performs a comparison process using the defined subnet mask with the destination IP address and its own IP address



Subnetting Basics

- Source host : 192.168.123.72
- Subnet mask : 255.255.255.192
- Destination host : 192.168.123.109

Source IP : 11000000.10101000.01111011.01001000
Subnet mask : 11111111.11111111.11111111.11000000 Logical AND
Network ID 11000000.10101000.01111011.01000000 (192.168.123.64)

Destination IP : 11000000.10101000.01111011.01101101
Subnet mask : 11111111.11111111.11111111.11000000 Logical AND
Network ID 11000000.10101000.01111011.01000000 (192.168.123.64)

Same result! Two hosts are on the same network.

CLARUSWAY© WAY TO REINVENT YOURSELF

15

Subnetting Basics

- Source host : 192.168.123.46
- Subnet mask : 255.255.255.192
- Destination host : 192.168.123.202

Source IP : 11000000.10101000.01111011.00101110
Subnet mask : 11111111.11111111.11111111.11000000 Logical AND
Network ID 11000000.10101000.01111011.00000000 (192.168.123.0)

Destination IP : 11000000.10101000.01111011.11001010
Subnet mask : 11111111.11111111.11111111.11000000 Logical AND
Network ID 11000000.10101000.01111011.11000000 (192.168.123.192)

Not the same! Two hosts are on different networks.

CLARUSWAY© WAY TO REINVENT YOURSELF

16

Subnetting Basics

Classless Inter-Domain Routing (CIDR)

- In order to reduce the wastage of IP addresses, a new concept of **CIDR** is introduced
- CIDR provides the flexibility of borrowing bits of Host part of the IP address
- By using subnetting, one single Class A address can be used to have smaller sub-networks which provides better network management capabilities

Subnetting Basics

- **CIDR** notation examples:

IP address: 192.168.1.142
Subnet mask: 255.255.255.0 or 11111111.11111111.11111111.00000000

CIDR: 192.168.1.142 /24 ← 24 turned on bits (1s)

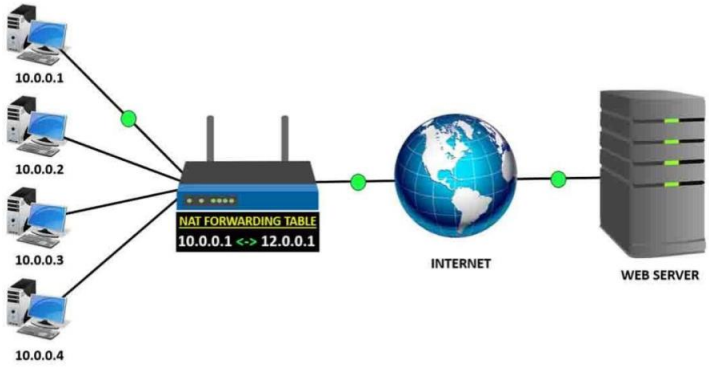
IP address: 172.16.56.140
Subnet mask: 255.255.255.240 or
11111111.11111111.11111111.11110000

← 28 turned on bits (1s)

CIDR: 172.16.56.140 /28

Introduction to NAT

- NAT is a process in which one or more local IP addresses are translated into one or more global IP address and vice versa to provide Internet access to the local hosts
- NAT allows multiple devices to access the Internet through a single public address



Introduction to NAT

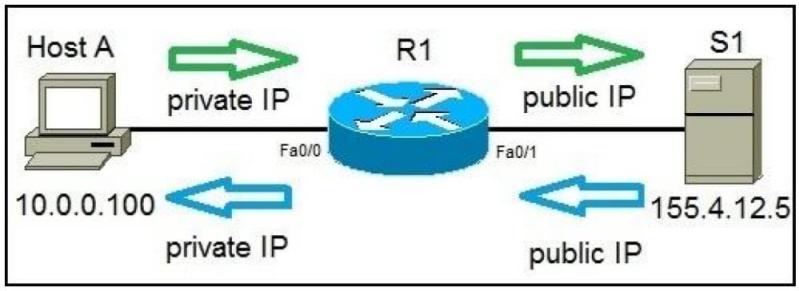
- Advantages:
  - Hides internal structure of the network from the outsider and thus increases network security
  - Eliminates address renumbering when a network evolves
  - Allows unlimited private IP address range

- Disadvantages:
  - Changes the IP addresses, thus troubleshooting becomes more complex
  - Translation results in switching path delays
  - Certain applications will not function while NAT is enabled
  - Complicates tunneling protocols such as IPsec

Introduction to NAT

Types of NAT:

- **Static NAT (SNAT):**
  - One-to-one mapping (A single private IP with a single global IP)
  - Each device needs a public IP address
  - Generally used for web hosting



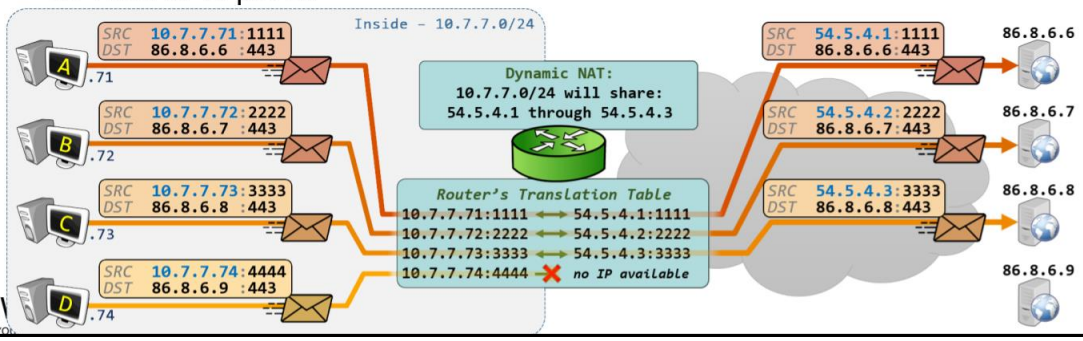
CLARUSWAY©
WAY TO REINVENT YOURSELF

22

Introduction to NAT

Types of NAT:

- **Dynamic NAT (DNAT):**
  - Public IP is picked from a pool of IP addresses
  - If no IP is left, data packet is dropped by the NAT
  - Very costly as many global IP addresses have to be bought to make a pool



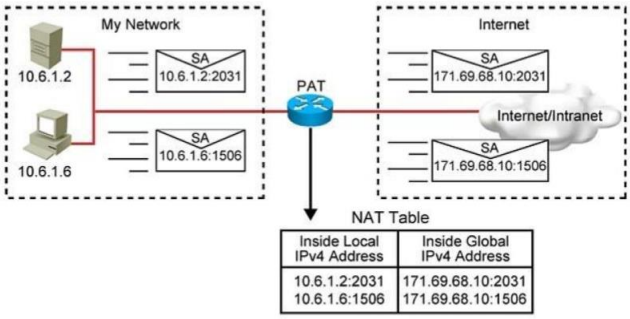
CLARUSWAY©
WAY TO REINVENT YOURSELF

23

Introduction to NAT

Types of NAT:

- **Overloading or Port Address Translation (PAT)**:
  - Most popular type of NAT
  - Port numbers are used to distinguish the traffic
  - Cost-effective as lots of users can be connected by using only one public IP address



NAT Table

Inside Local IPv4 Address	Inside Global IPv4 Address
10.6.1.2:2031	171.69.68.10:2031
10.6.1.6:1506	171.69.68.10:1506