0x02 Networking

Day 2 – IPs, Subnetting, Important Services

Setup

- Please boot up your Kali VMs
- We will be running some tools to help us view services and network traffic in a bit

Review of Day 1

- OSI Model
- What is an IP address?
- Public vs. Private IP address?
- What is a MAC address?
- What is a packet?

Easy Subnetting

(short and sweet)

Subnetting Basics

- This is a crucial skill to be able to do by hand
- CCNA and other certification exams will require that you know how to do it
- “In the real world, I’m going to use a calculator”
  - Probably, but you really do need to understand how it works and do it in your head

Subnetting Basics

- Having one huge network is not a good idea
  - Segmenting hosts makes networks more manageable
  - Cut down on broadcast traffic
- Take bits from the host portion of an address, and reserve them to define a subnet address instead

IP Address

- 192.168.1.10
  - Remember this is a representation of binary (1, 0)
  - Bit: 1 or a 0
  - Byte: Combination of 8 bits
- Each field or octet is a byte long
  - byte.byte.byte.byte
- So if we can have 8 bits, what is the maximum number we can put into an octet? (11111111)

Creating Subnets

- Determine the number of required network IDs
  - One for each LAN subnet
  - One for each WAN connection
- Determine the number of required host IDs per subnet
  - One for each TCP/IP host
  - One for each router interface
- Based on the above, create:
  - Unique subnet mask for entire network
  - Unique subnet ID for each physical segment
  - Range of host IDs for each subnet

Subnet Masks

- Each machine on a network must know which part of a host address will be the subnet mask
- Subnet mask is 32-bit binary value
- We read them in decimal format
  - 255.255.255.0 rather than 11111111.11111111.11111111.00000000

Default Subnet Masks

Class	Format	Default Subnet Mask
A	network.node.node.node	255.0.0.0
B	network.network.node.node	255.255.0.0
C	network.network.network.node	255.255.255.0

Classless Inter-Domain Routing (CIDR)

- Also referred to as *slash notation*
- Simple way to summarize a subnet mask
- Format looks like **/<number>** where the number represents how many bits are in a subnet mask
- Example: subnet mask of 255.255.255.0
  - In binary, it looks like 11111111.1111111.11111111.00000000
  - Count the 1's and you get 24
  - CIDR notation is **/24**

CIDR Notation

- /8 through /15 can be used with class A
- /16 through /23 can be used with class A & B
- /24 through /30 work for any class A, B, or C network

Subnetting Made Easy

- Make an excel spreadsheet
  - Know how to write this out by hand too
- If you can draw this table, you will have 0 problems getting your subnetting right

Subnet Chart

- Block size: **2^n**
- Usable hosts: **block size – 2**
- CIDR – **Start at /24** (255.255.255.0)
  - Smaller block size = higher CIDR
  - Bigger block size = smaller CIDR
- Subnet mask: **256 – block size**

Example 1

- Given the subnet **255.255.255.128(/25)** and the network **192.168.10.0**
- How many subnets?
  - 2 (256/128)
- How many hosts per subnet?
  - 126
- Valid subnets?
  - 0 and 128
- Broadcasts?
  - 127 and 255

Example 1

Subnet	0	128
First Host	1	129
Last Host	126	254
Broadcast	127	255

Example 2

- Given the Subnet mask of **255.255.255.192** and the network address of **192.168.10.0**
- How many subnets are there?
  - 4 (256/64)

Subnet	0	64	128	192
First Host	1	65	129	193
Last Host	62	126	190	254
Broadcast	63	127	191	255

Example 3

- Given the network **127.16.0.0/17**
- How many subnets?
  - **2**

Subnet	0.0	128.0
First Host	0.1	128.1
Last Host	127.254	255.254
Broadcast	127.255	255.255

Example 4

- Given host **192.168.10.10/30**
  - What is the block size of the subnet?
    - 4
  - What subnet does the host belong to?
    - 192.168.0.0 to 192.168.0.3
    - 192.168.0.4 to 192.168.0.7
    - **192.168.0.8 to 192.168.0.11**
- Fill out the other information about the subnet (usable hosts, subnet mask, broadcast, etc.)

Public vs. Private IP

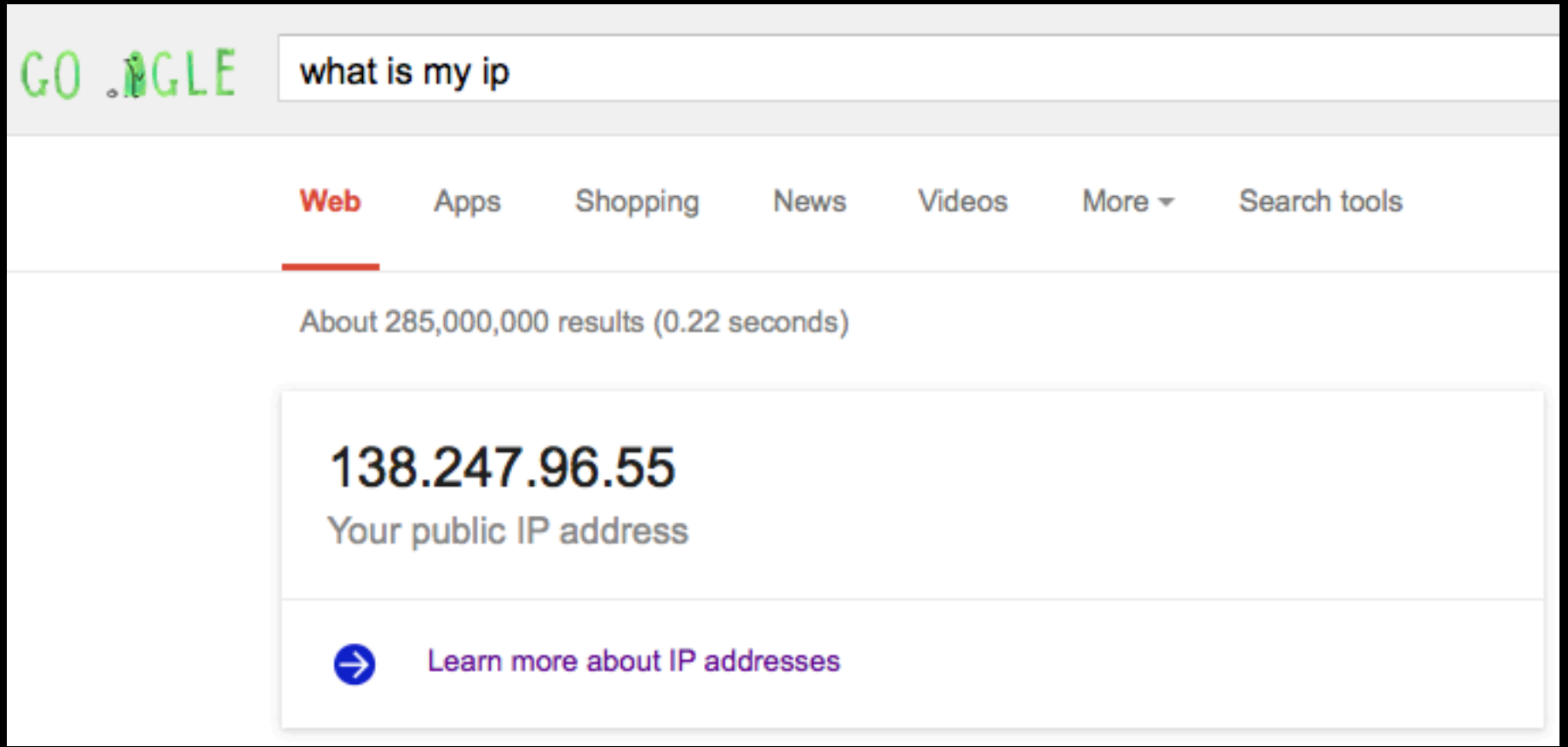
- What is your home IP address?
  - We've probably all seen 192.168.1.X somewhere
- If we all have the same internal IP address scheme, how can we communicate?
  - There are some ranges of IPs that cannot communicate over the internet, they are reserved for internal use

IP Ranges

- Internal ranges are not routable over the internet
- You need to communicate with other devices that are not on your same network with a public IP address

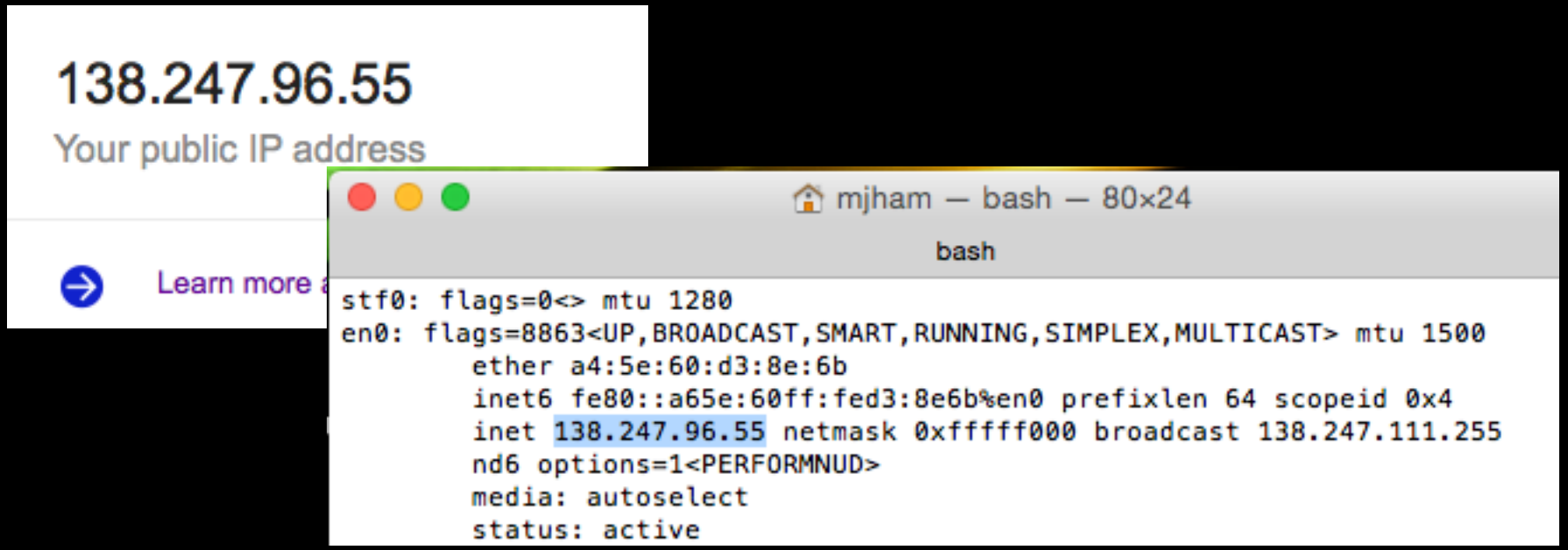
RFC1918 name	IP address range	number of addresses	largest CIDR block (subnet mask)	host id size	mask bits	*classful* description[Note 1]
24-bit block	10.0.0.0 - 10.255.255.255	16,777,216	10.0.0.0/8 (255.0.0.0)	24 bits	8 bits	single class A network
20-bit block	172.16.0.0 - 172.31.255.255	1,048,576	172.16.0.0/12 (255.240.0.0)	20 bits	12 bits	16 contiguous class B networks
16-bit block	192.168.0.0 - 192.168.255.255	65,536	192.168.0.0/16 (255.255.0.0)	16 bits	16 bits	256 contiguous class C networks

What is my public IP?



Hang on…

- I’m on the DSU network and my public and private IPs are the same?



DSU is Special

- We have a full class B network at our disposal
  - 138.247.0.1 - 138.247.255.254
- 65,535 available IP addresses
- Every client device on campus is issued a publicly facing IP address
  - There is still a firewall in front of us all
  - Devices aren't sitting wide open to the world

Network Devices

- Hubs
- Switches
- Bridges
- Routers

Hubs

- Hubs were the main interconnection for older Ethernet networks
- Any incoming signal on any port on a hub is re-created (repeated)
- Everyone can see everyone else's traffic
- All connected devices have to share the total bandwidth
- Replaced by switches

Hub

Switches

- Current most common interconnection for Ethernet networks
- Look like hubs
- Separating every connection, each computer can use the full bandwidth of the switch
- Traffic is segmented so you have a point-to-point connection to the switch

Switches


NETGEAR
ProSafe 8 Port Gigabit Switch
MODEL GS108
NETGEAR
GS108
Gigabit Ethernet
Auto Uplink


Catalyst 2960-S Series

Bridges

- Used to link Ethernet network media together
- Not very common to see
- Can link Ethernet to fiber, vice versa

Bridges


TX
RX
100M
100M
TXL
FXL
FDX
PWR
Fiber/T Transceiver™
10/100/1000 Base-Tx & 1000Base-Fx Converter

Routers

- A *router* connects LANs together using the TCP/IP protocol
- Router must have at least two connections—one into a network, and one out to another network
  - Most, especially in enterprise environments have many more

What is this?

What is DHCP?

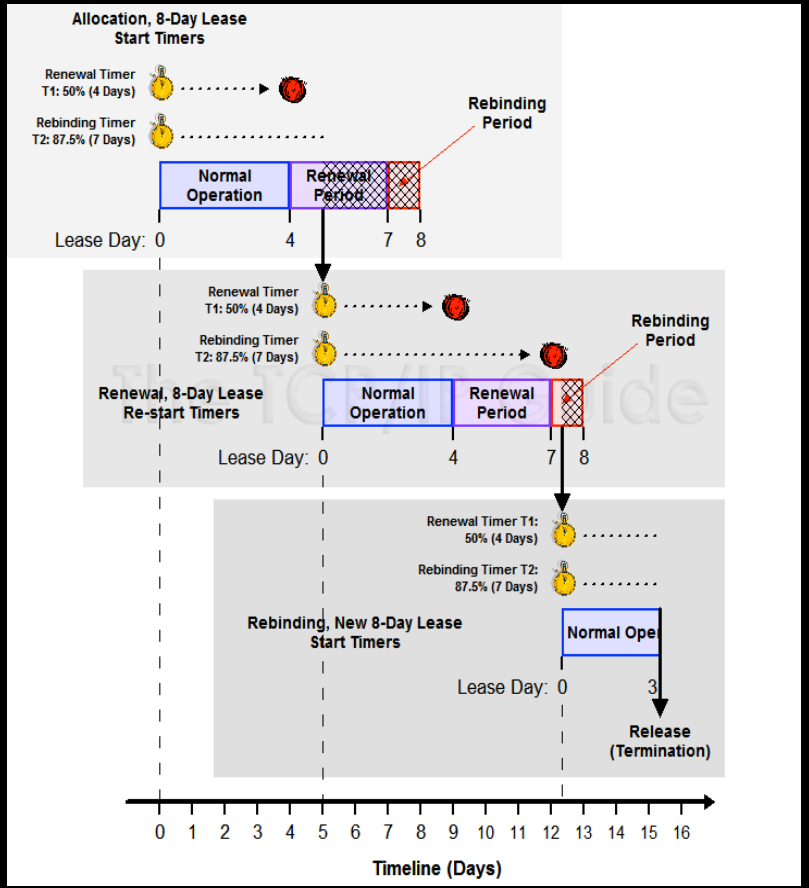
- Dynamic Host Configuration Protocol
- When you connect to Wifi you “just get an IP”
- DHCP assigns any host that connects an IP address
  - We don’t have to take the time to assign these manually
  - We don’t have to worry about 2 hosts using the same IP
- Configuring DHCP you can set a pool
  - Range(s) of IP’s that are allowed to be automatically assigned

Activity: Release & Renew

- Release and renew your DHCP assigned IP address
  - You may get the same address back
  - Why?
  - What does release actually do?
- Windows: **ipconfig /release && ipconfig /renew**
- Linux: **dhclient –r eth0 ; dhclient eth0**
- Wireshark: **udp.port == 68**

DHCP Lease

- How long you can keep an IP for
  - Admins can set this



Sauce: http://www.tcpipguide.com/free/t_DHCPLeaseLifeCycleOverviewAllocationReallocationRe.htm

What is DNS?

- Domain Name System
  - The internet’s address book
  - Map’s domain names to IP addresses
    - i.e. google-public-dns-a.google.com → 8.8.8.8

Types of DNS Records

- MX Record
  - Mail exchange record that points to a domains mail servers
- CNAME Record
  - Canonical record - link to aliases (e.g. www.google.com → google.com
- A Record
  - Address - links to the ip address (e.g. www.google.com → 172.194.64.147
- NS Record
  - Nameserver - Shows the nameserver(s) for the given domain

Activity: nslookup

- Use nslookup to find the following records from www.dsu.edu
  - A
  - CNAME
  - MX
  - NS

DNS Zone

- Pretty much like a folder for DNS entries
- Way to organize records by domain name

DNS AXFR

- DNS servers need to stay in sync
  - What if I light up a new web server, I want everyone else to know about it
- Authorized servers should be able to perform a “zone transfer” on each other to learn about new changes
  - Also called AXFR
- You effectively retrieve all of the zones another server knows about

Performing Zone Transfer

- In Kali, you can use a tool called **dnsenum**
- Perform a transfer on **zonetransfer.me**
  - Server someone stood up for testing
- Can we find it in Wireshark?