System Administration & Security

COMP 175 | Fall 2021 | University of the Pacific | Jeff Shafer

Networking Essentials

COMP 177 compressed?

Agenda

- Goal: **High level summary** of **networking topics** relevant to introductory sysadmin work
- Topics
  - IP Addresses
  - Subnets
  - DNS & Hostnames
  - Network Address Translation (NAT)
  - Dynamic Host Configuration Protocol (DHCP)

Identification

Identification

- How can we distinguish between all the systems running on our network?
- Need a **unique name / address** for each one
- Human-friendly: **DNS hostname**
  - `cyberlab.pacific.edu`
- Machine-friendly: **IP address**
  - `54.148.163.48` (IPv4)
  - `2600:1f14:536:b01:9cda:64e:15a9:da0` (IPv6)

*Want **both** in most cases!*

IP Addresses

Internet Protocol (IP)

- **Challenge**: How can we uniquely identify computers on the global Internet?
- Solution: **IP** ("Internet Protocol") **Addresses**
  - Using IP, a packet can be delivered from any arbitrary computer to any other as long as the two hosts are publicly accessible
- IP addresses are assigned to network interfaces
  - If a host has multiple network interfaces, that host needs multiple IP addresses

Internet Protocol (IP)

- IP addresses for the **`cyberlab`** server
  - IPv4: `54.148.163.48`
  - IPv6: `2600:1f14:536:b01:9cda:64e:15a9:da0`
- Dig deeper…
  - How do I find (or set) my IP address?
  - Where did these addresses come from?
  - Do they have a special meaning?

What is My IP?

- Linux

```
$ ip addr
$ ifconfig  # Legacy
```

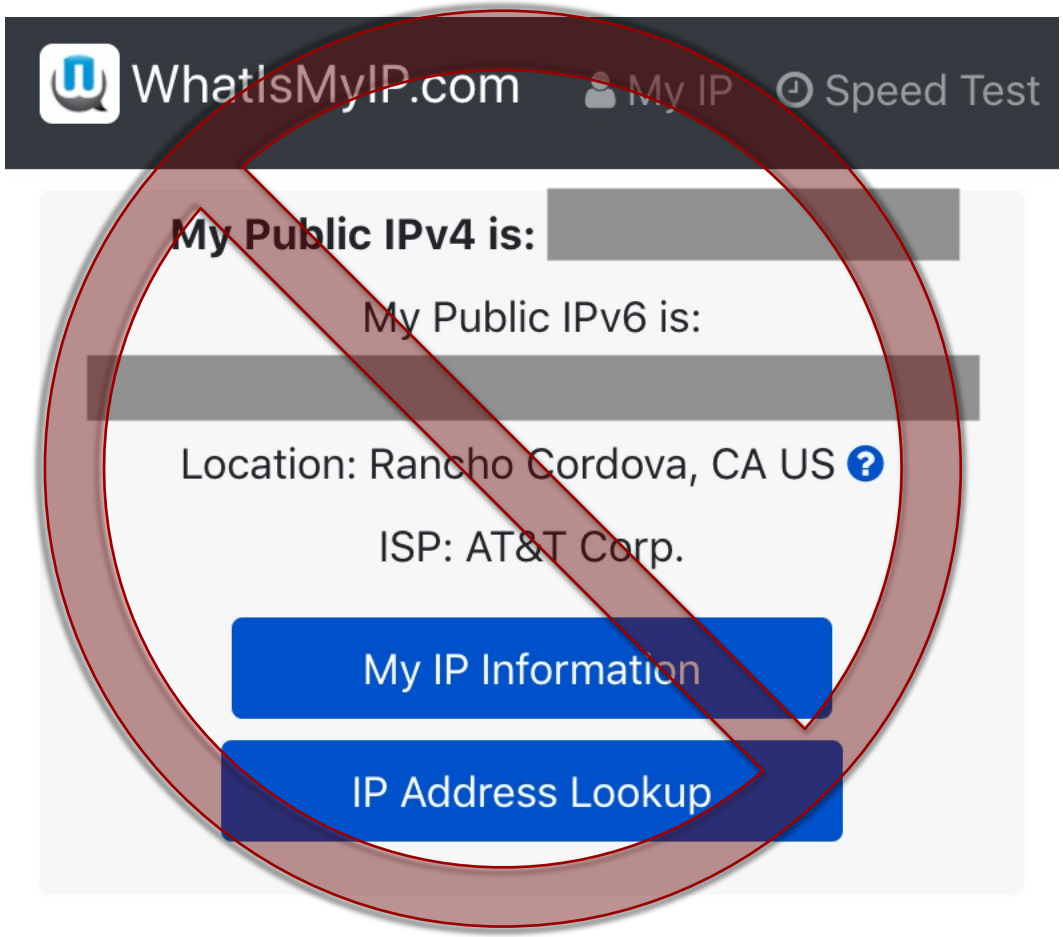
- Mac

```
$ ifconfig
```

- Windows CMD prompt

```
> ipconfig
```

What is My IP?

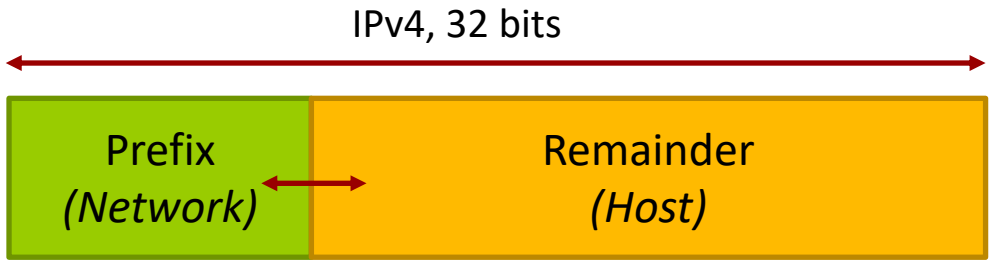

WhatIsMyIP.com
My IP
Speed Test
My Public IPv4 is:
My Public IPv6 is:
Location: Rancho Cordova, CA US
ISP: AT&T Corp.
My IP Information
IP Address Lookup

IP Address Format

- IPv4 addresses are usually displayed in dotted decimal notation
  - Each byte represented by decimal value
  - Bytes are separated by a period
  - IP address `0x8002C2F2 = 128.2.194.242`
- Computers use the 32-bit binary number **internally**
- Dotted-decimal notation is only for human display

IP Address Format

- An IP address consists of two parts:
  - *Network* part (prefix)
  - *Host* (interface) part (remainder)



- The size of the prefix can **vary!**
  - Classless Inter-Domain Routing (CIDR)

IP Address Format

- The network part is assigned by the *ISP*
- The host part is usually configured by the *network administrator*
- As a result, IP addresses identify both
  - What network is this specific address part of?
  - What computer on that network should receive the message?

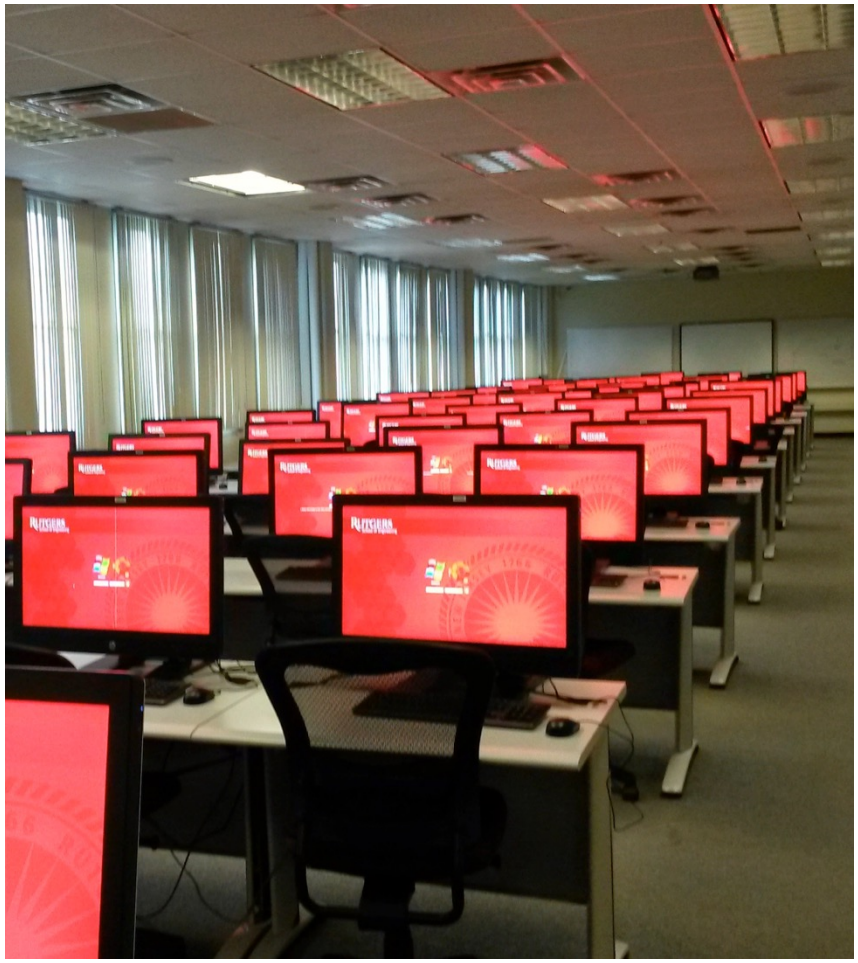
Specifying Network Prefix

- **CIDRized** notation: Use `/n` at the end of IP address, where `n` is the length of the network prefix
  - Example: `9.126.5.125/`**8** specifies
    - Prefix bits = Upper **8** bits
      - *Which network?*
    - Host bits = Lower 24 bits
      - *Which computer on network?*

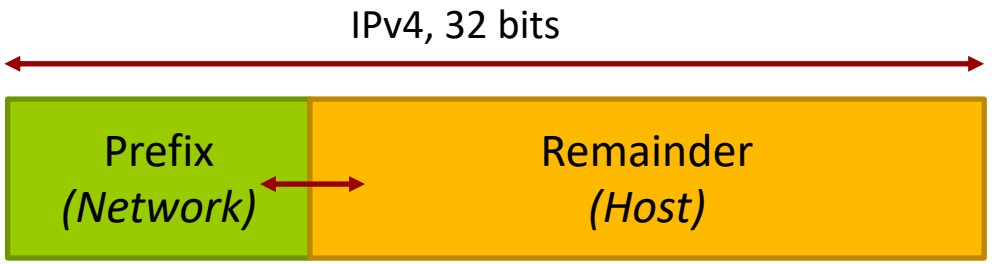
IP Subnets

Subnets

- Imagine we are designing the network for an "engineering building"
- How many hosts (max) will be connected to the building network?
  - Estimate: **800 hosts**
- **How big should our subnet be?**



Subnets



- How big should the host address field be?
  - 8 bits? ($2^8 = 256$)
  - 9 bits? ($2^9 = 512$)
  - 10 bits? ($2^{10} = 1024$)
    - **Sufficiently large for "800 hosts"**

Subnet Naming

- Imagine you could use any IP address range for this network
- **Will `192.168.1.0/24` work?**
  Definitely not!

Subnet Naming

- **Problem 1:**
  - The length of the subnet address is 22 bits, not 24 bits
  - This address should be of the form **`a.b.c.d/22`**

Subnet Naming

- **Problem 2:**
  - The bits don't fit in the fields any more…
  - Decimal: `192.168.1.0/22`
  - Binary:
    `11000000.10101000.000000`**`01`**`.00000000`

You have "prefix address" bits in the host address field…

What addresses would work?

- Host field needs to be all 0's

11000000.10101000.00000000.00000000

192.168.0.0/22

11000000.10101000.00000100.00000000

192.168.4.0/22

11000000.10101000.00001000.00000000

192.168.8.0/22

11000000.10101000.00001100.00000000

192.168.12.0/22

...

11000000.10101000.11111100.00000000

192.168.252.0/22

Subnet Naming

- Let's choose `192.168.252.0/22`
- **What addresses are available for hosts within the subnet?**

11000000.10101000.111111xx.xxxxxxxx

- 11000000.10101000.111111**00.00000000**
  - **192.168.252.0**
  - All **zeros** in host field = "**Subnet Name**"
  - Not allowed for host address
- 11000000.10101000.111111**00.00000001**
  - **192.168.252.1** – **Lowest possible** IP address
- . . .
- 11000000.10101000.111111**11.11111110**
  - **192.168.255.254** – **Highest possible** IP address
- 11000000.10101000.111111**11.11111111**
  - **192.168.255.255**
  - All **ones** in host field = "**Broadcast Address**"
  - Not allowed for host address

Domain Name System

Motivation

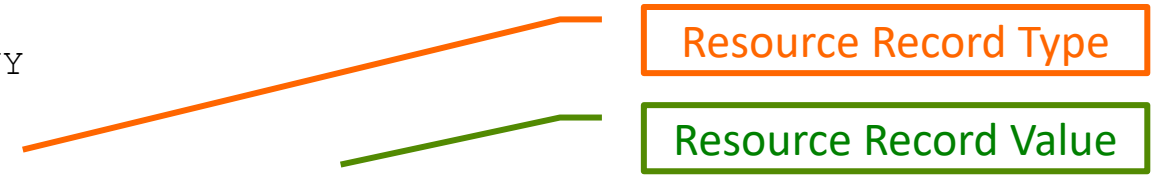
- IP addresses are hard to remember
  - `54.148.163.48`? Or was it `.84`?
- Human-friendly names are much better
  - `cyberlab.pacific.edu`
- How can we translate between the two?

Domain Name System (DNS)

- **Distributed database** implemented in hierarchy of many **name servers**
  - No single point of failure
  - No distant centralized database
  - Easier maintenance
    - Take one or a dozen servers offline without issue
  - Support high traffic volume
  - *** **Scalable** ***

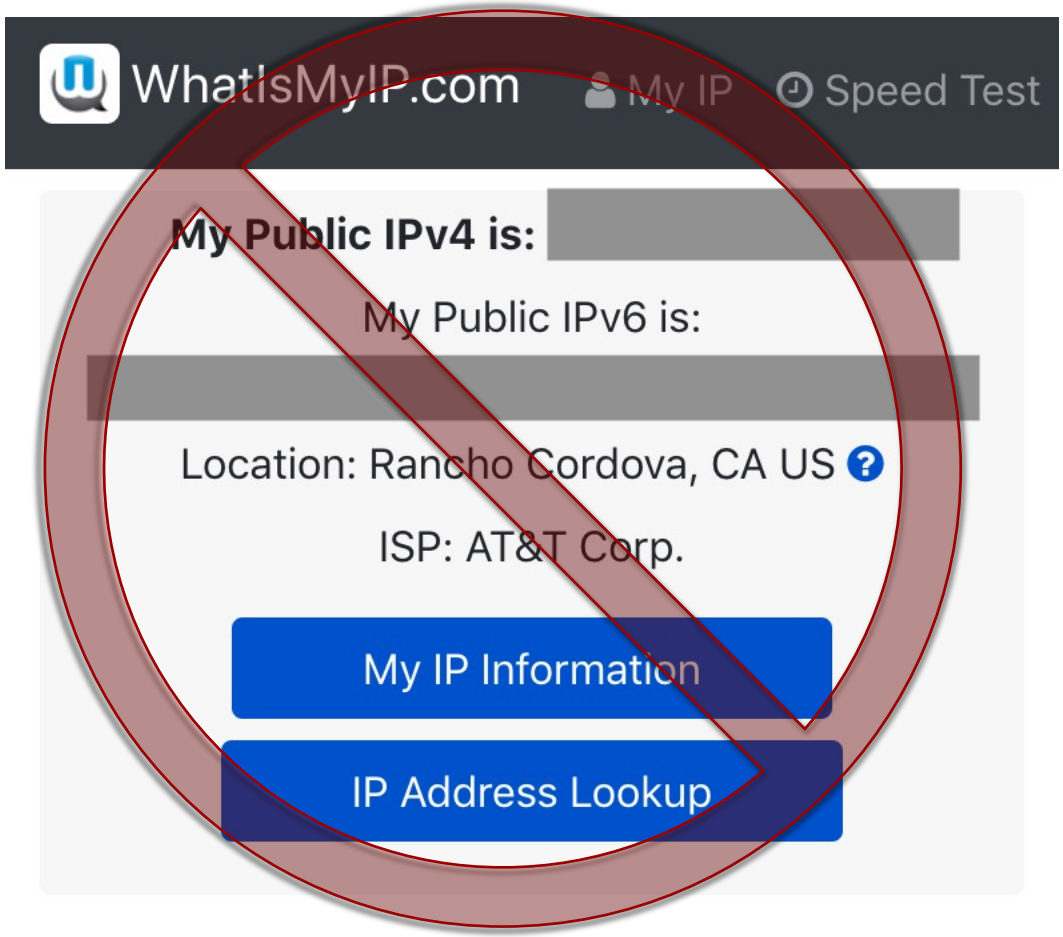
DNS: Example

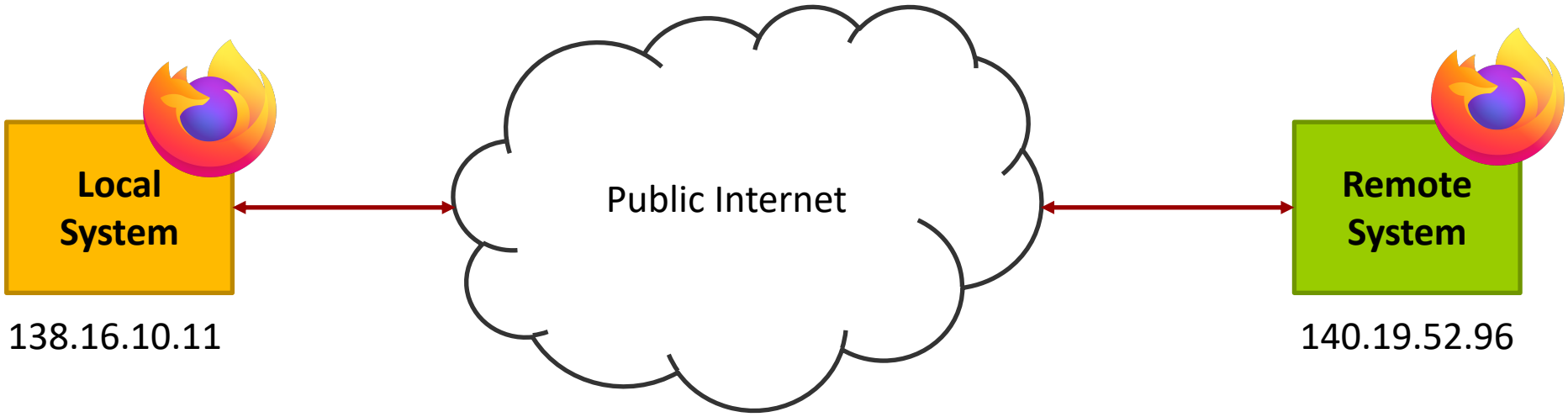
```
$ dig cyberlab.pacific.edu any

; <<>> DiG 9.10.6 <<>> cyberlab.pacific.edu any
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38914
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;cyberlab.pacific.edu. IN ANY

;; ANSWER SECTION:
cyberlab.pacific.edu. 299 IN A 54.148.163.48
cyberlab.pacific.edu. 299 IN AAAA 2600:1f14:536:b01:9cda:64e:15a9:da0

;; Query time: 93 msec
;; SERVER: 2600:1700:b810:b988::1#53(2600:1700:b810:b988::1)
;; WHEN: Tue Jul 13 22:42:43 PDT 2021
;; MSG SIZE  rcvd: 93
```

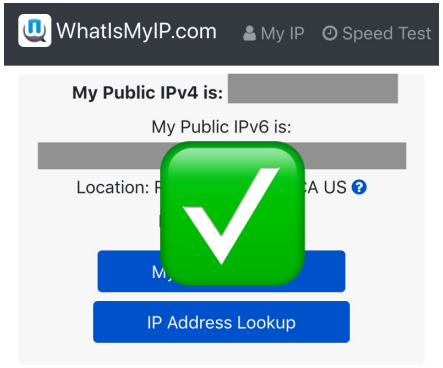


Network Address Translation (NAT)

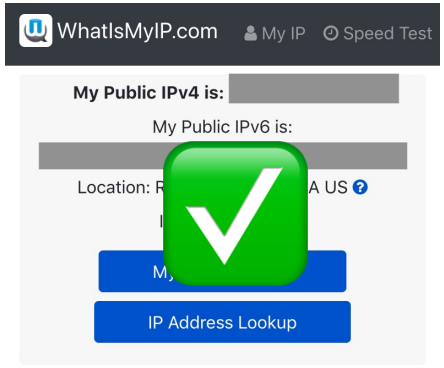
What is My IP?


WhatIsMyIP.com
My IP
Speed Test
My Public IPv4 is:
My Public IPv6 is:
Location: Rancho Cordova, CA US
ISP: AT&T Corp.
My IP Information
IP Address Lookup





***Design Goal* of Internet – Every system is publicly accessible (public IP)**

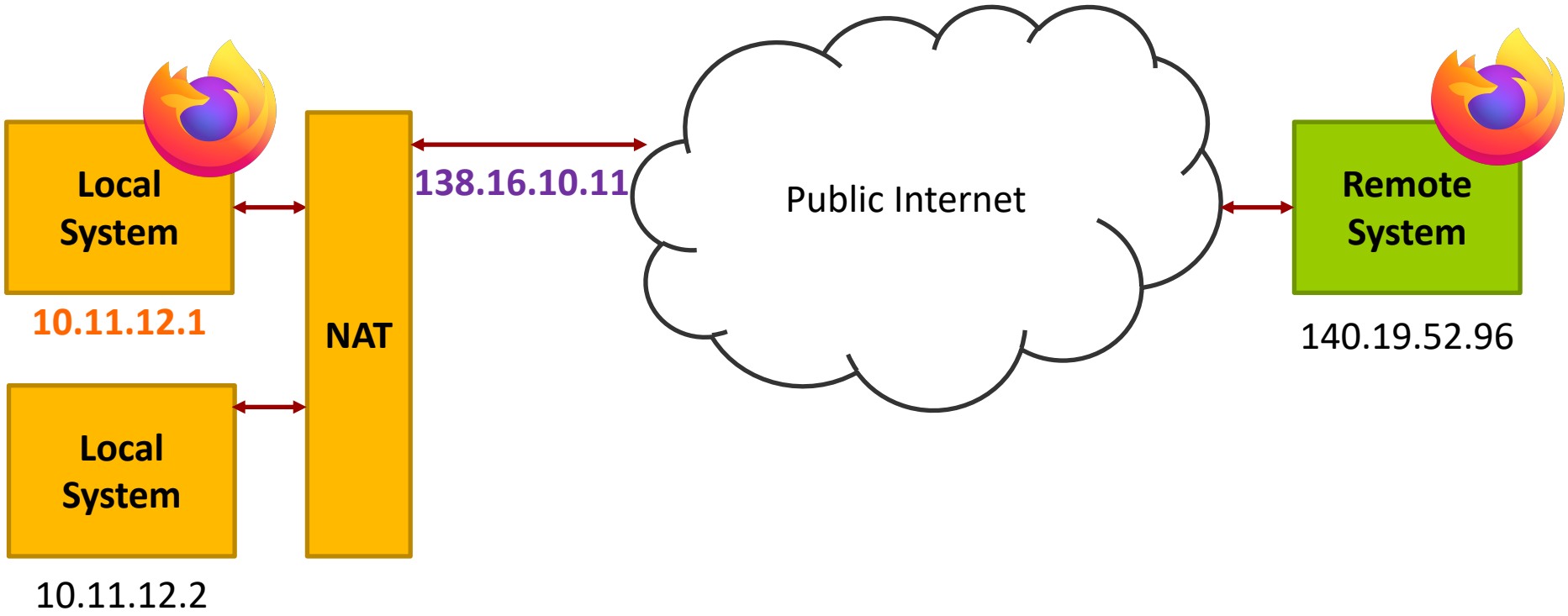


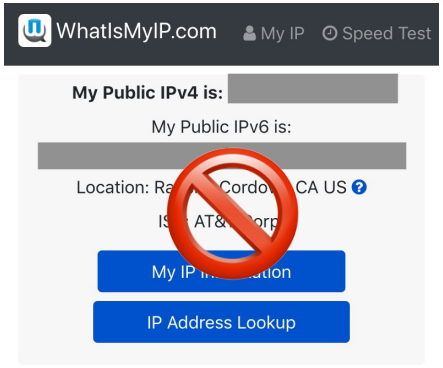
Private Addresses

- 32-bit address space for IPv4 is not enough for today's Internet ($2^{32} \simeq$ 4billion addresses)
- Many of the IP addresses are for internal / private use
  - The address for a corporate file server
  - The address of each interfaces of an internal router
  - The address of the PCs and laptops handed to employees
- Private IP addresses can be used *arbitrary number of times* in different networks
- **Public routers (e.g., ISP's) cannot forward packets with a destination address in the private ranges**
- Private IP address blocks
  - `10.0.0.0/8`
  - `172.16.0.0/12`
  - `192.168.0.0/16`

Network Address Translation (NAT)

- Network address translation (NAT) is a capability of routers that enables multiplexing large number of individual hosts behind a single IPv4 public address
- Benefits of NAT
  - Conserves *limited address space of IPv4*
  - Enables a form of *firewall-based security* in LANs
    - Internal devices can *initiate* connections to external devices, but not vice versa

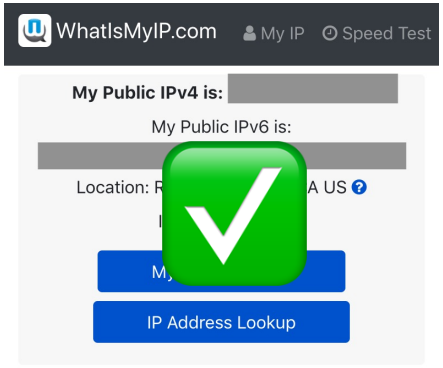




The WhatIsMyIP.com site (and similar) will only see the public IP of your NAT (gateway), not the private IP of your internal device.

Sometimes this is what you want.

Other times it is not.

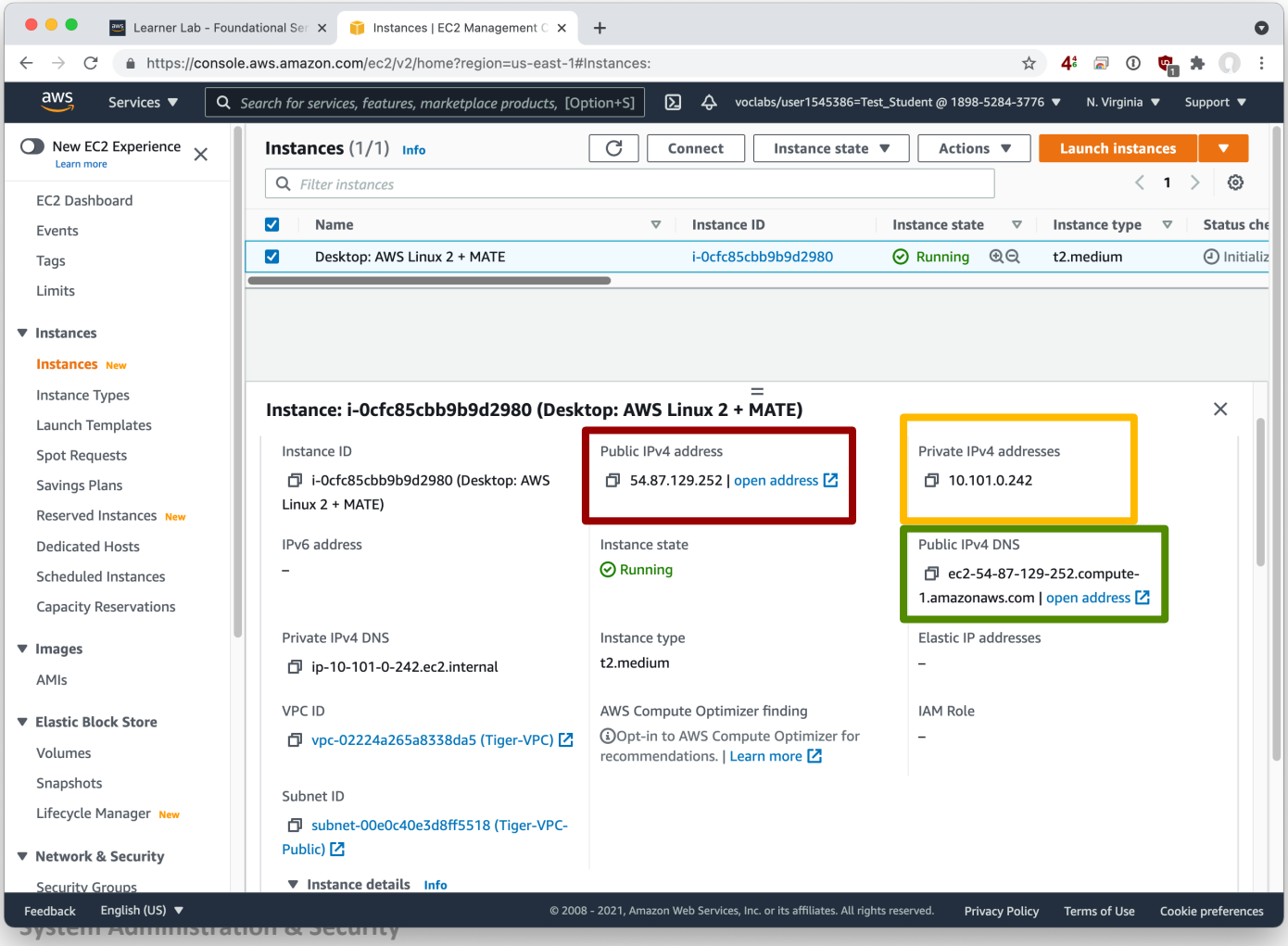


What is My IP? AWS Example

- Started a virtual machine in AWS EC2 and SSH'd into it…

```
$ ip addr
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc
mq state UP group default qlen 1000
    link/ether 12:7c:6d:a6:5c:eb brd ff:ff:ff:ff:ff:ff
    inet 10.101.0.242/24 brd 10.101.0.255 scope global
dynamic eth0
```

What is My IP? AWS Example



- **Private IP**
  - 10.101.0.242
  - Matches "ip addr" command
- **Public IP**
  - 54.87.129.252
  - Won't see this on command line! (*Unless you use AWS-specific command*)
- **Public IPv4 DNS**
  - ec2-54-87-129-252.compute-1.amazonaws.com

Dynamic Host Configuration Protocol (DHCP)

Network Configuration

- How does a host get its network interface configured?
  - IP address
  - Network mask (“Subnet”)
  - Default gateway (“Router to leave subnet”)
  - DNS servers
  - …

Dynamic Host Configuration Protocol (DHCP)

- Goals of DHCP
  - Plug and play!
  - Allow host to *dynamically* obtain its IP address from network server when it joins network
  - Allow host to renew its lease on in-use address
  - Allow reuse of addresses (if you disconnect your host, someone else can use that address)

IPv6

IP Versions

Version	Description
0-3	Unused: Development versions of IP
4	**Current network-layer protocol**
5	Unused: Experimental stream protocol – ST
6	**New network-layer protocol (1996)**
7-9	Unused: Experimental protocols – TP/IX, PIP, TUBA
10-15	Not allocated

Motivation for IPv6: Scarcity! (Of IP addresses…)

Why Replace IPv4?

- The problem
  - IPv4 has ~4.3 billion addresses
  - World has ~6.6 billion people!
    - How many internet-capable devices per person?
- IP address exhaustion
  - Internet will not “collapse”, but new devices / networks will not be able to join(*)
- When? **YEARS AGO!** Final rate of consumption was one /8 block (16.78 million addresses) per month
  - Feb 1st, 2011 – Five final /8 blocks handed out to Regional Internet Registries (RIRs)
  - RIR supply ran out within months

(*) Except via address translation…

Comparison – IPv4 vs IPv6

	IPv4	IPv6
Deployed	1981 *[RFC 791]*	1999 *[RFC ~~2460~~, 8200]*
Address Size	32-bit number	128-bit number

Address Format	Dotted Decimal Notation:
	`192.149.252.76`
		Hexadecimal Notation:
		`3FFE:F200:0234:AB00:`
		`0123:4567:8901:ABCD`

Prefix Notation	`192.149.0.0/24`	`3FFE:F200:0234::/48`
Number of Addresses	2^{32} = ~4,294,967,296 (~4 billion)	**2^{128} = ~340,282,366,920,938,463,463,374,607,431,768,211,456**

https://biotech.law.lsu.edu/blog/ipv4_ipv6.pdf (ARIN Fact Sheet)

IPv6 Address Notation

- 128 bits – 8 groups of 4 hex digits
  - `2001:0db8:85a3:08d3:1319:8a2e:0370:7334`
- "User friendly!" "Easy to remember!"
- "Helpful" Shortcuts:
  - Omit leading zeros in a group (`0005:0db8:...` is equivalent to `5:db8:...`)
  - Collapse groups of all-zeros with :: (`2001:0000:0000:0000:0000:8a2e:0370:7334` is equivalent to `2001::8a2e:0370:7334`)

But we couldn't just stop with a larger address space….

IPv4 vs IPv6 - Differences

IPv6 is *not* just IPv4 with 128-bit long addresses…

It's a different network protocol that should be configured (and secured) separately but runs over the same data link layer.

"Dual Stack"