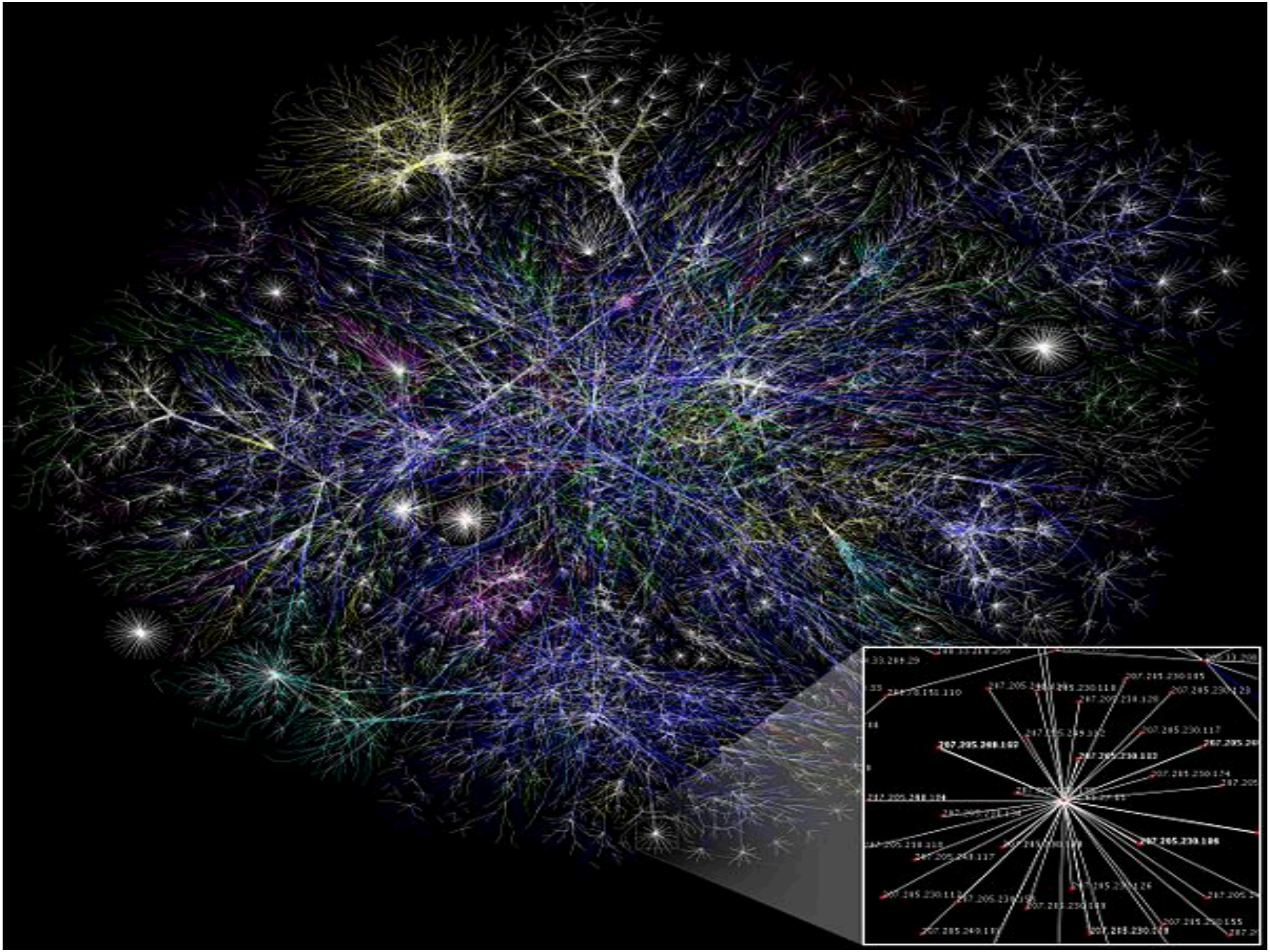
Firewalls

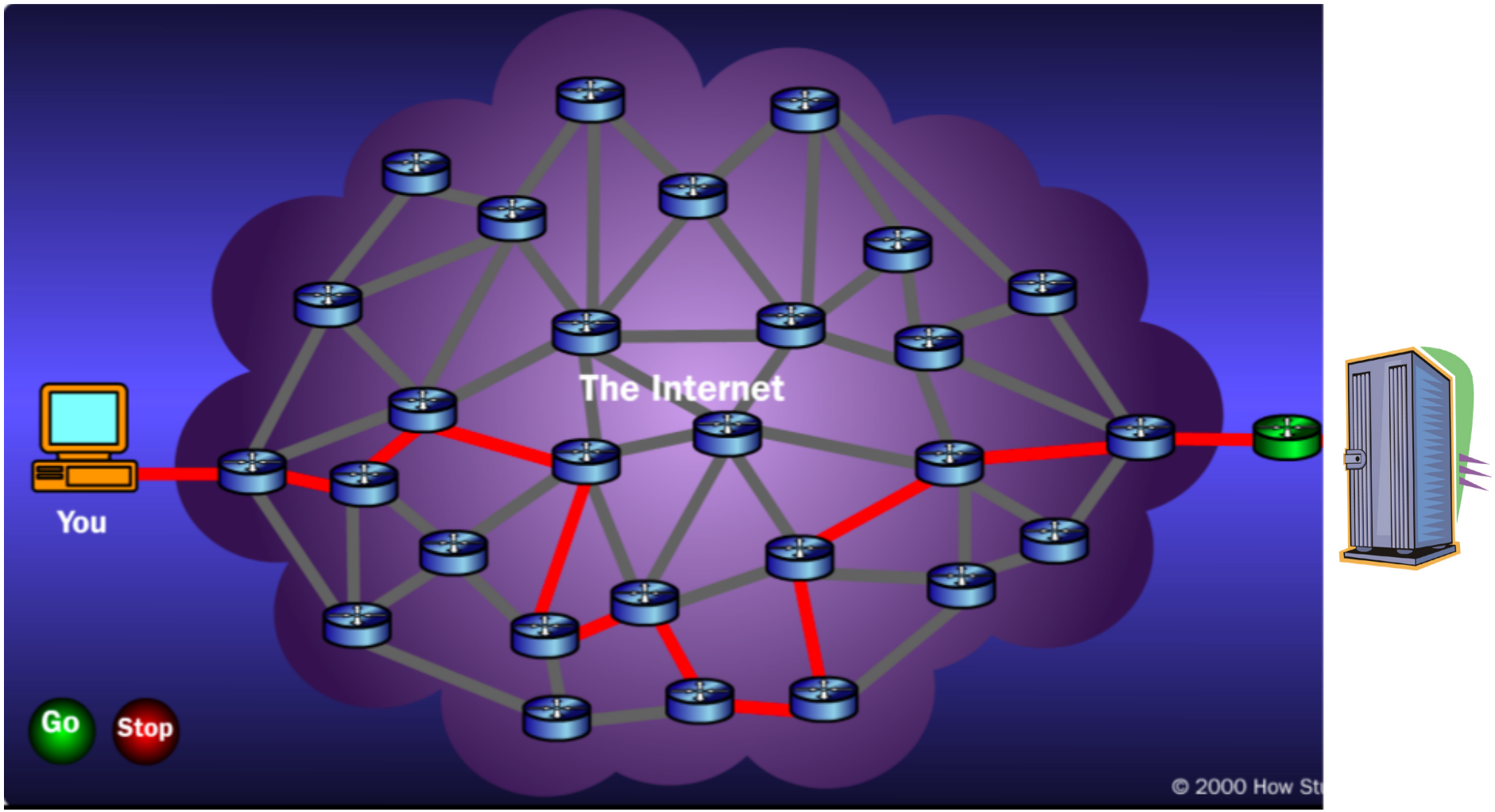
Securing the Network Perimeter

Network Preliminaries

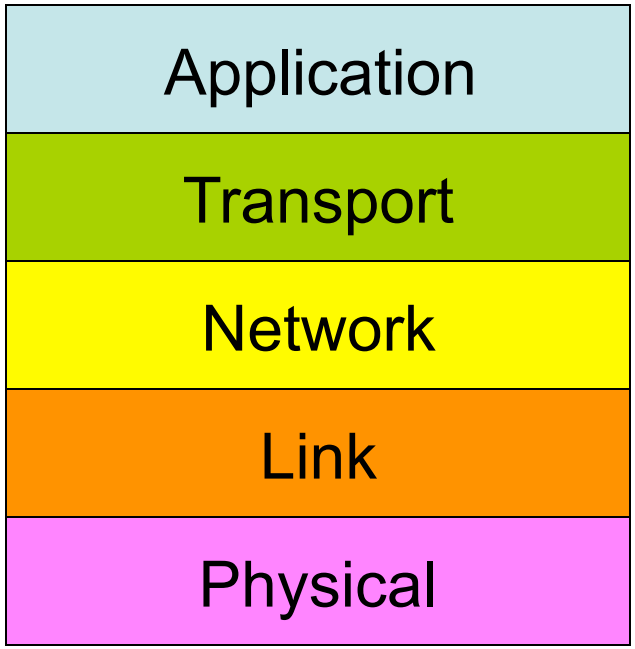
- Layers
- Headers
- IP addresses
- Ports



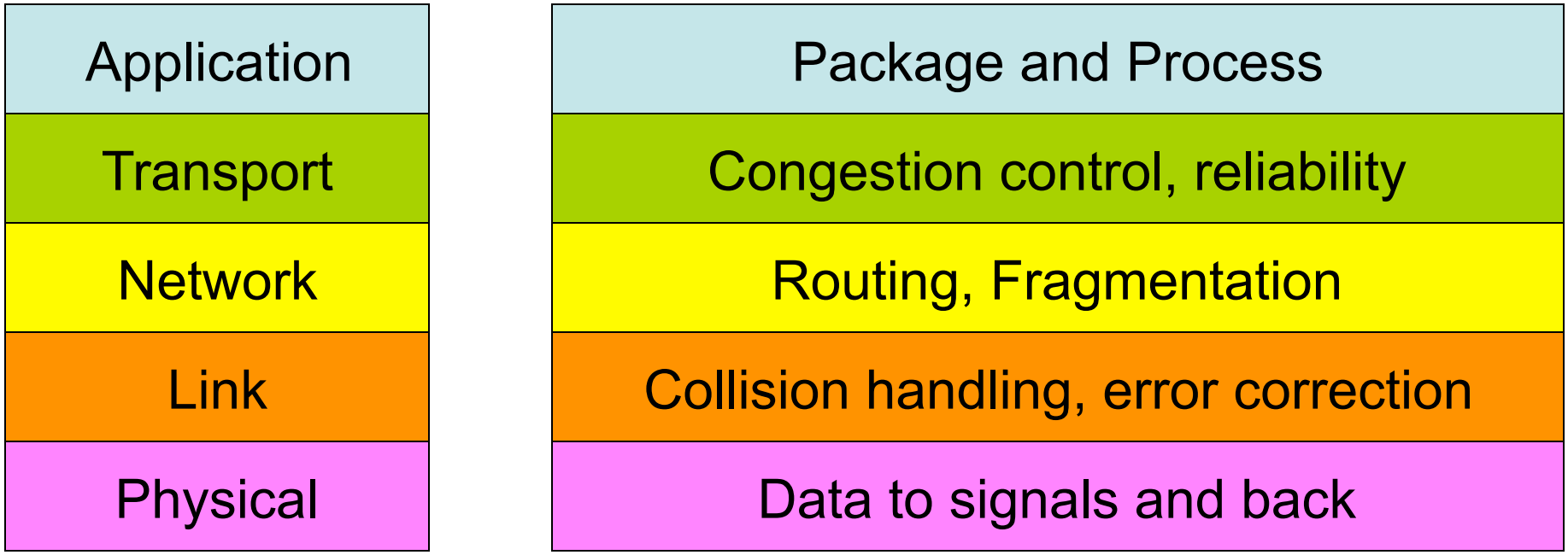
Many Steps



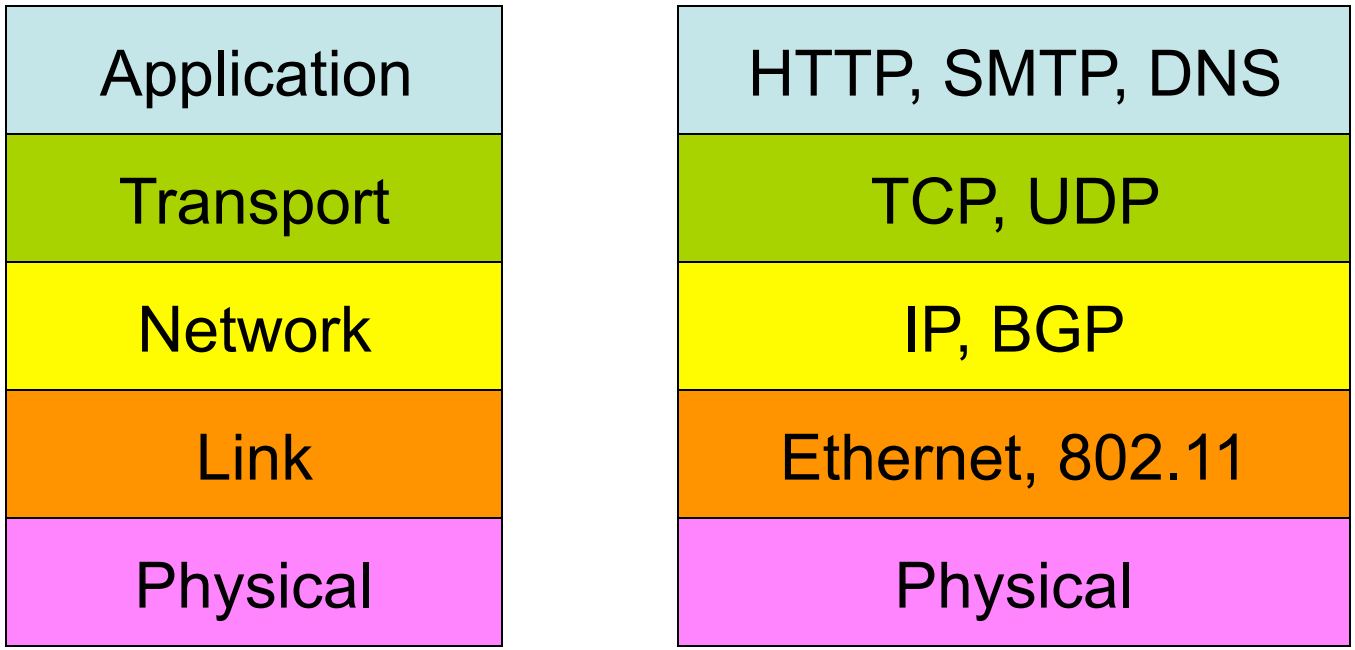
Layers



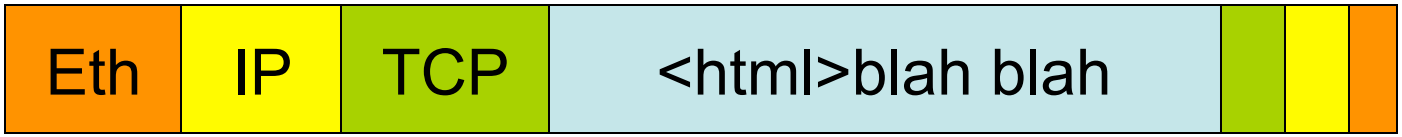
Layers


Application
Transport
Network
Link
Physical
Package and Process
Congestion control, reliability
Routing, Fragmentation
Collision handling, error correction
Data to signals and back

Layers


Application
Transport
Network
Link
Physical
HTTP, SMTP, DNS
TCP, UDP
IP, BGP
Ethernet, 802.11
Physical

Headers



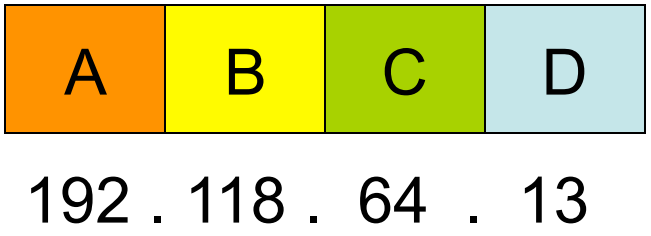
TCP Header: Sequence no., ACK no.

IP Header: IP address, port no.

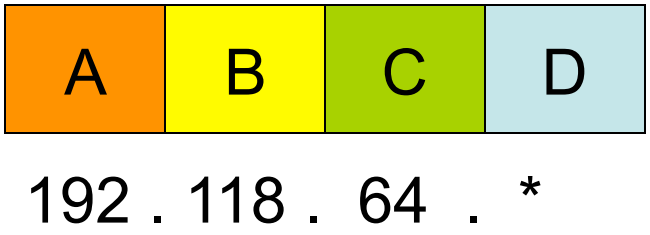
Eth Header: Ethernet address

IP Addresses

- 32 bits
  - Four parts



- Ownership
  - A *C-class* network
  - Starting bits: 110
    - What values?



Classes

ipindex.net

- Class A

```
  0.  0.  0.  0 = 00000000.00000000.00000000.00000000
127.255.255.255 = 01111111.11111111.11111111.11111111
                  0nnnnnnn.HHHHHHHH.HHHHHHHH.HHHHHHHH
```

- Class B

```
128.  0.  0.  0 = 10000000.00000000.00000000.00000000
191.255.255.255 = 10111111.11111111.11111111.11111111
                  10nnnnnn.nnnnnnnn.HHHHHHHH.HHHHHHHH
```

- Class C

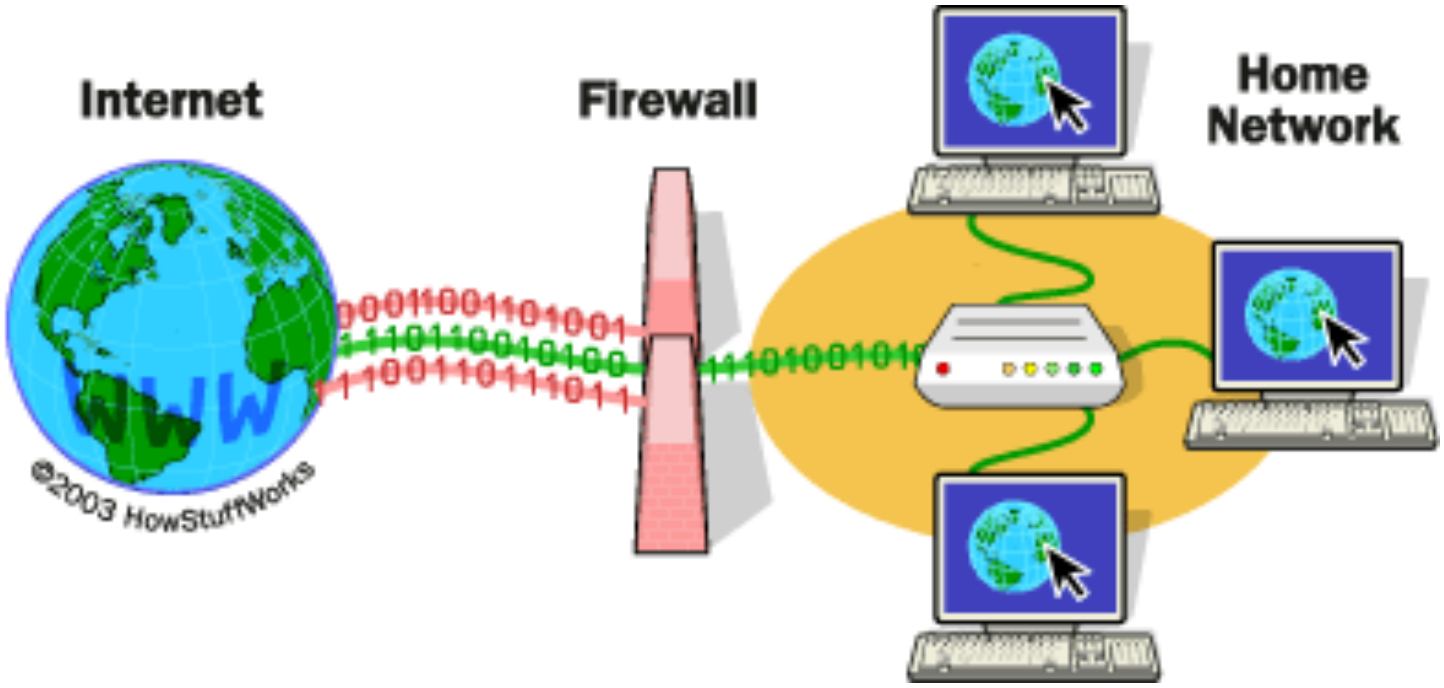
```
192.  0.  0.  0 = 11000000.00000000.00000000.00000000
223.255.255.255 = 11011111.11111111.11111111.11111111
                  110nnnnn.nnnnnnnn.nnnnnnnn.HHHHHHHH
```

Also reserve two addresses: first and last

Perimeter Security

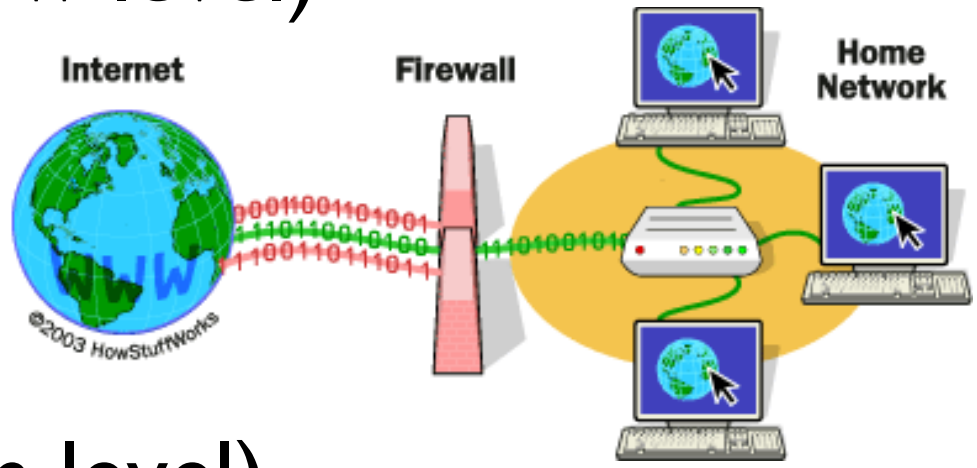
- Barriers keep others out
- Examples?

Network Firewalls

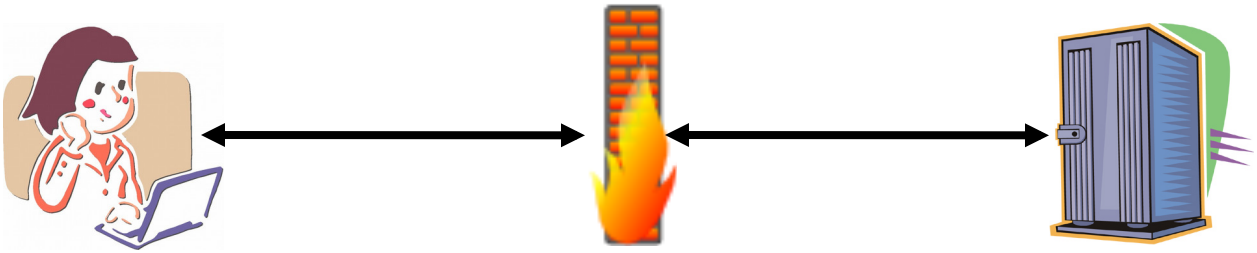


Methods

- Packet Filtering (low level)

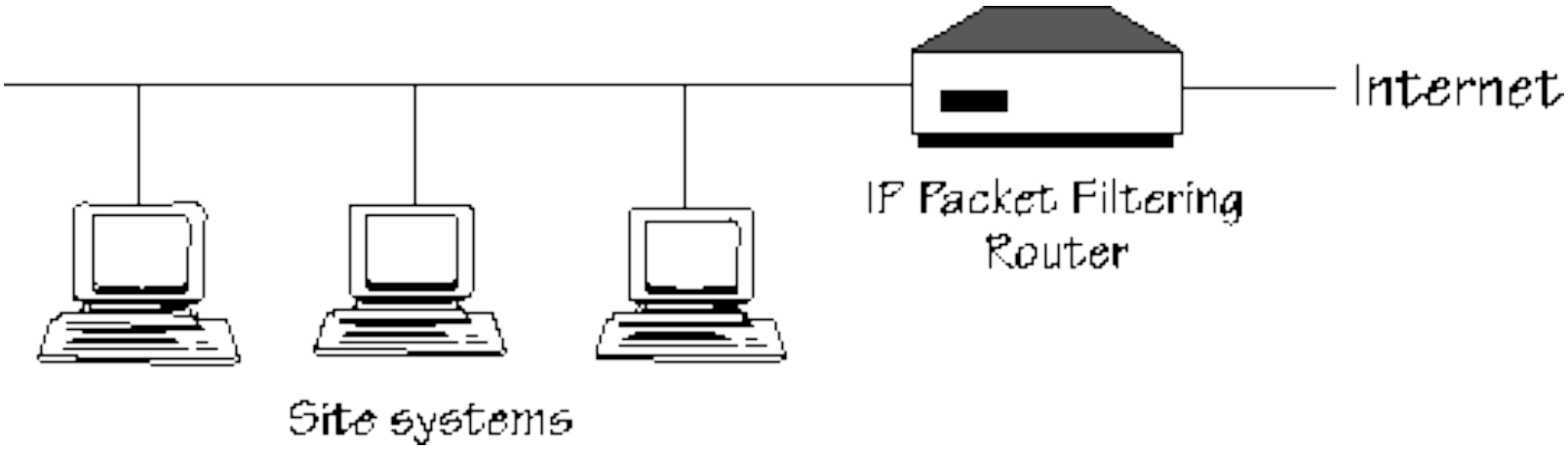


- Proxy service (high level)
  - The firewall handles transactions with the outside



Basic Packet Filtering

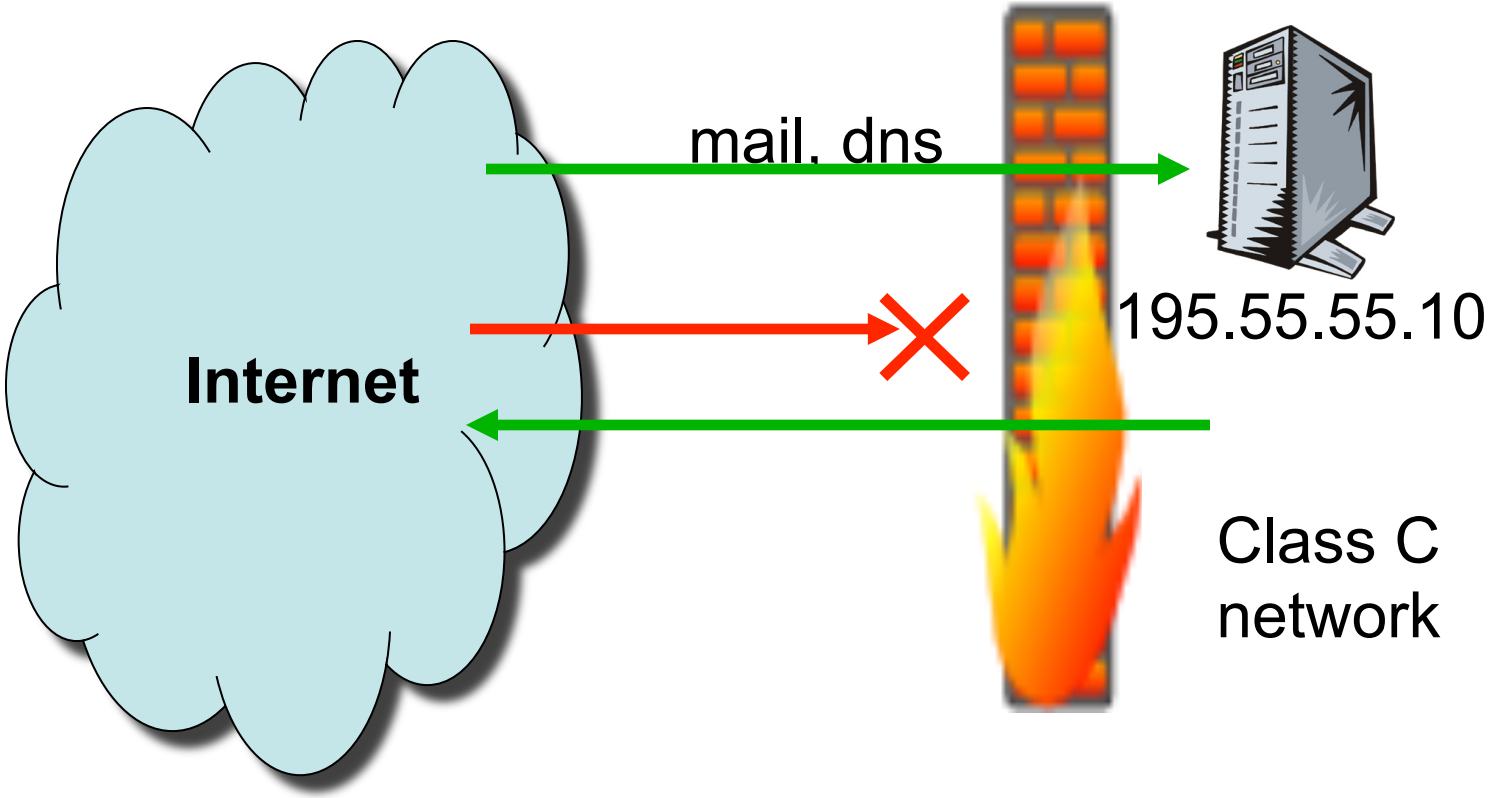
- Direct Access
  - simple to setup
  - But rules can be complex
    - Hard to verify
    - Exceptions are hard to manage
    - Flexible rule sets needed



Filtering Example

- Security policy
  - Allow FTP access to the download server
  - Otherwise no FTP access is allowed.
- Rules
  - Deny list: * * 21
  - Allow list: * 128.119.245.66 21
- Outgoing
  - * *.badstuff.com *

UNIX Filtering



UNIX Filtering

```
ipfwadm -F -f
```

flush (-f) the Forwarding (-F) rules

```
ipfwadm -F -p deny
```

Policy is set to *default deny*

Input: masq.

Match bi-dir.

TCP

Source

Ports

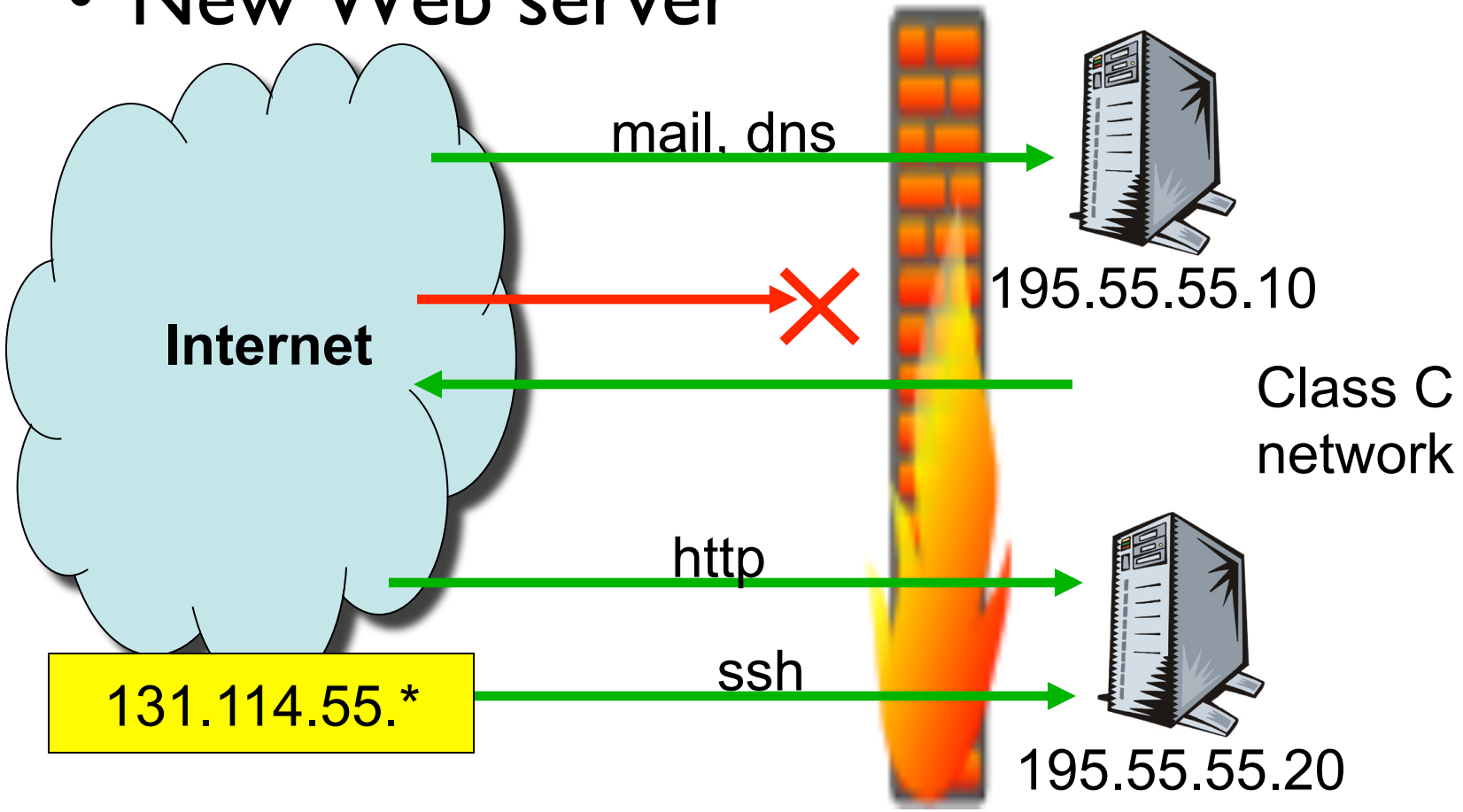
Destination

```
ipfwadm -F -i m -b -P tcp -S 0.0.0.0/0 1024:65535 -D 195.55.55.10 25
ipfwadm -F -i m -b -P tcp -S 0.0.0.0/0 1024:65535 -D 195.55.55.10 53
ipfwadm -F -i m -b -P udp -S 0.0.0.0/0 1024:65535 -D 195.55.55.10 53
ipfwadm -F -a m -S 195.55.55.0/24 -D 0.0.0.0/0 -W eth0
```

Append

Making a change

- New Web server

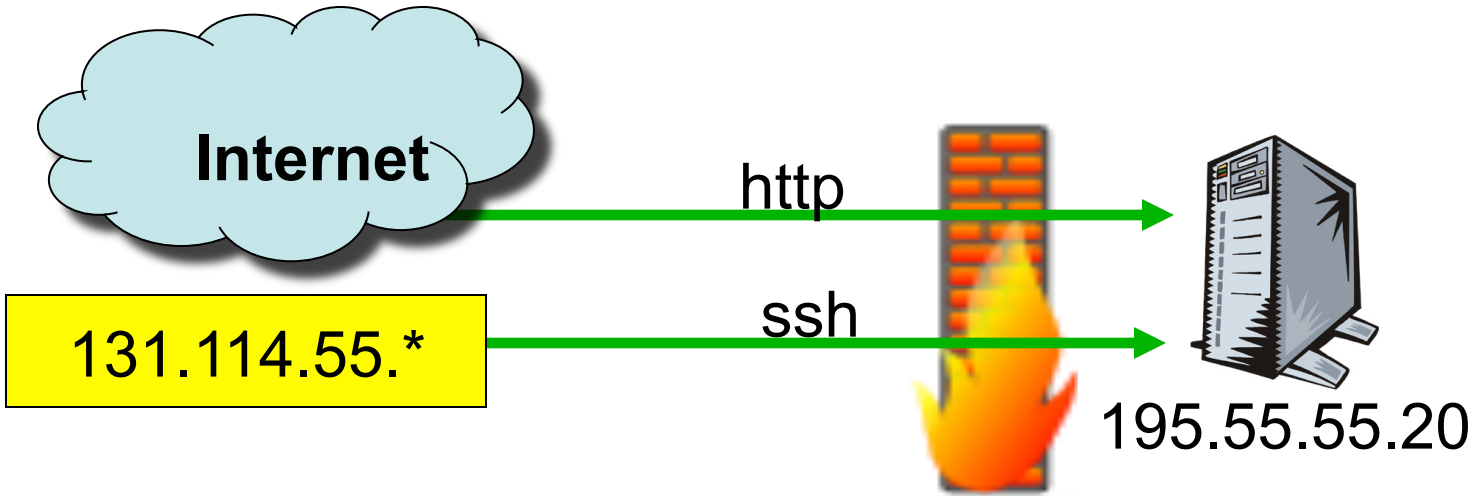


Let's update the rules

```
ipfwadm -F -f
ipfwadm -F -p deny

ipfwadm -F -i m -b -P tcp -S 0.0.0.0/0 1024:65535 -D 195.55.55.10 25
ipfwadm -F -i m -b -P tcp -S 0.0.0.0/0 1024:65535 -D 195.55.55.10 53
ipfwadm -F -i m -b -P udp -S 0.0.0.0/0 1024:65535 -D 195.55.55.10 53
ipfwadm -F -a m -S 195.55.55.0/24 -D 0.0.0.0/0 -W eth0
```

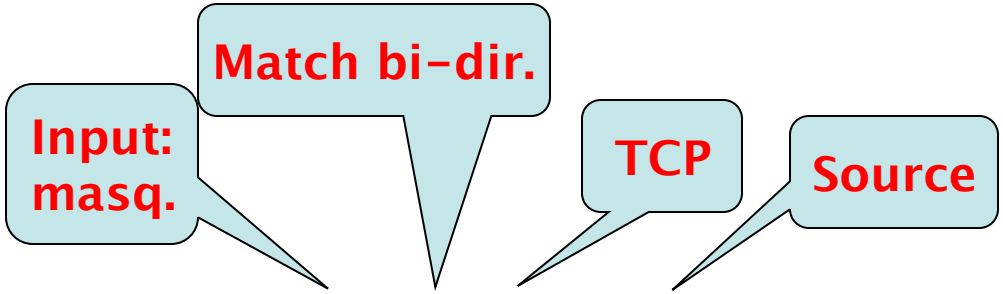
PUT COMMANDS HERE




Marcus J. Ranum Certified
Apparently
OK
Firewall

The End

Cisco Rules



- access-list 101 permit tcp any host 195.55.55.10 eq smtp
- access-list 101 deny ip 195.55.55.0 0.0.0.255

Benefits

- Enforcement point
  - Corporate policies
  - Security policies
- A single point of observation
  - Logging and auditing
  - Forensics
  - IDS

Benefits

- Cost & Complexity
  - A single point of focus
  - Reduced need for specialized security internally
- Simple security principle
  - Don't give away more information than necessary
  - Is this security by obscurity?

Limitations

- Obvious work-arounds
  - physical media
  - other networks (POTS)
  - attacks over allowed protocols
  - insider attacks
- Central point of failure
- Hard tasks
  - malware ID

Policies

- Heart of firewall
  - What services are available?
  - In which directions?

- Basics
  - Default Allow
    - Explicitly dis-allow "dangerous" services
    - Far too easy to circumvent
  - Default Deny
    - Explicitly allow OK services

Address Mask

- Rules
  - Class A
    - First bit 0
    - 8 total bits
  - Class B
    - First bits 10
    - 16 total bits
  - Class C
    - First bits 110
    - 24 total bits
- How many networks?
- Available addresses per n/w?

Ports

- Different services
  - Web, email, ssh, etc.
- Known server ports
  - HTTP (80), ssh (22), DNS (53)
- Client ports
  - Anything between 1024 and 65535