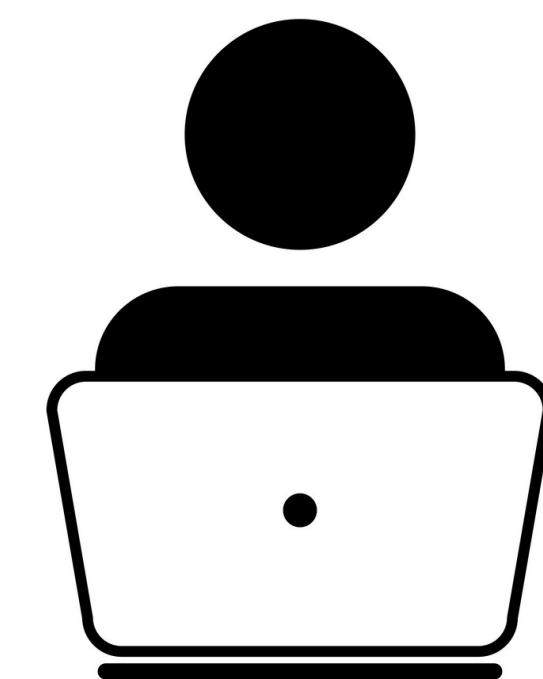
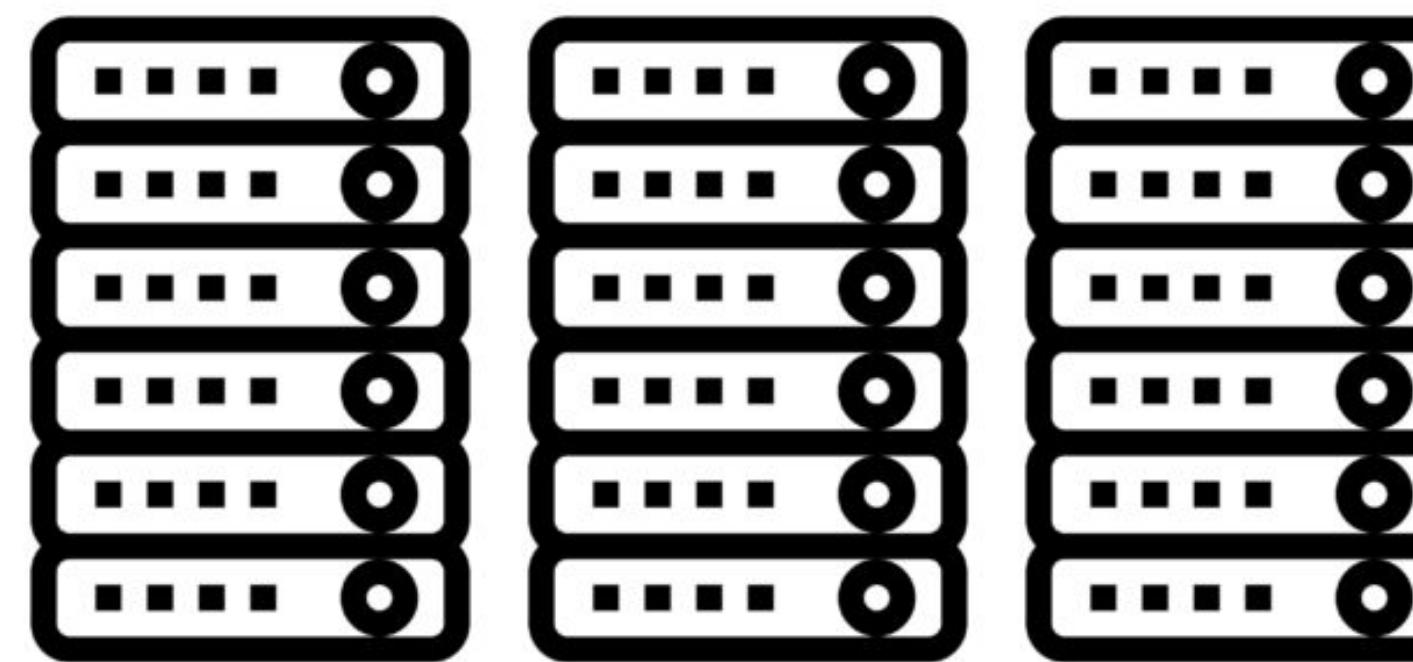
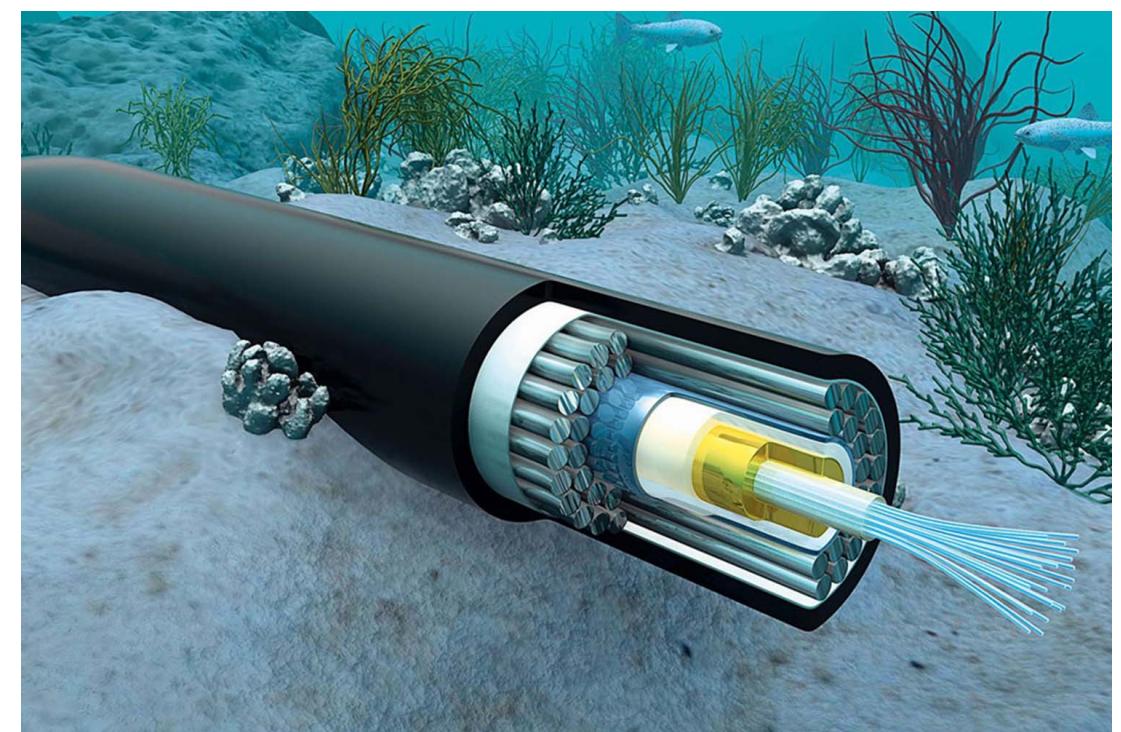
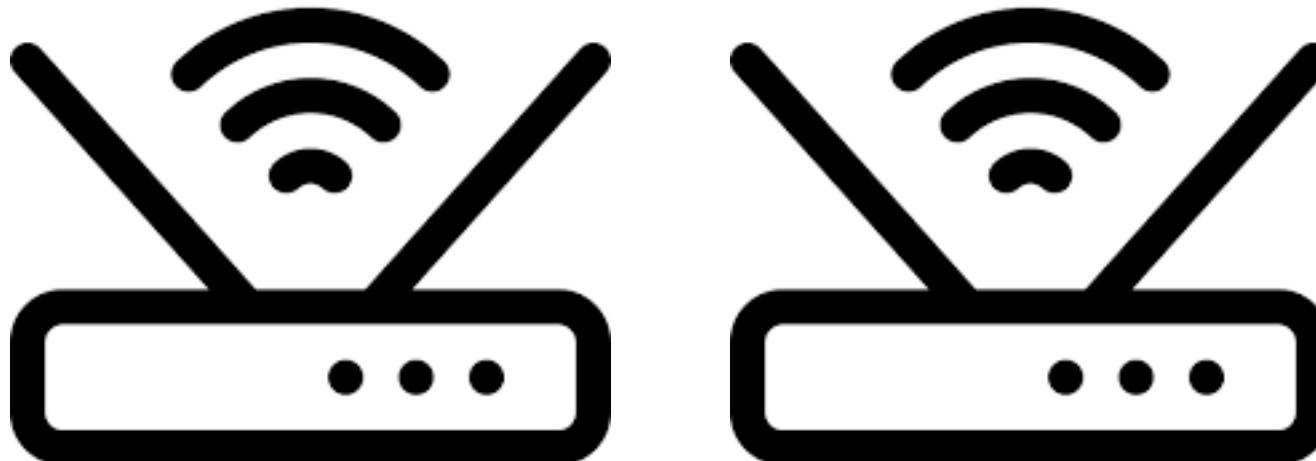


# **Computer Network Measurement and Security**

## **ECE 239AS**

**Liz Izhikevich**

# The Internet is composed of multiple constituents

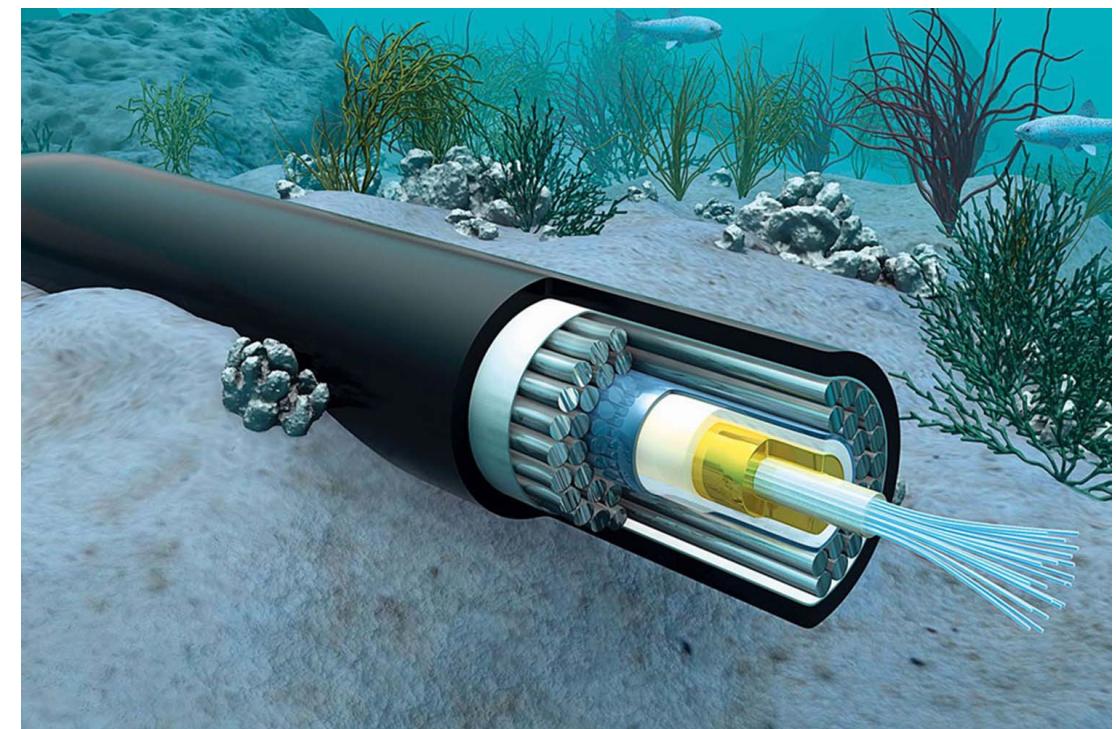


Networks

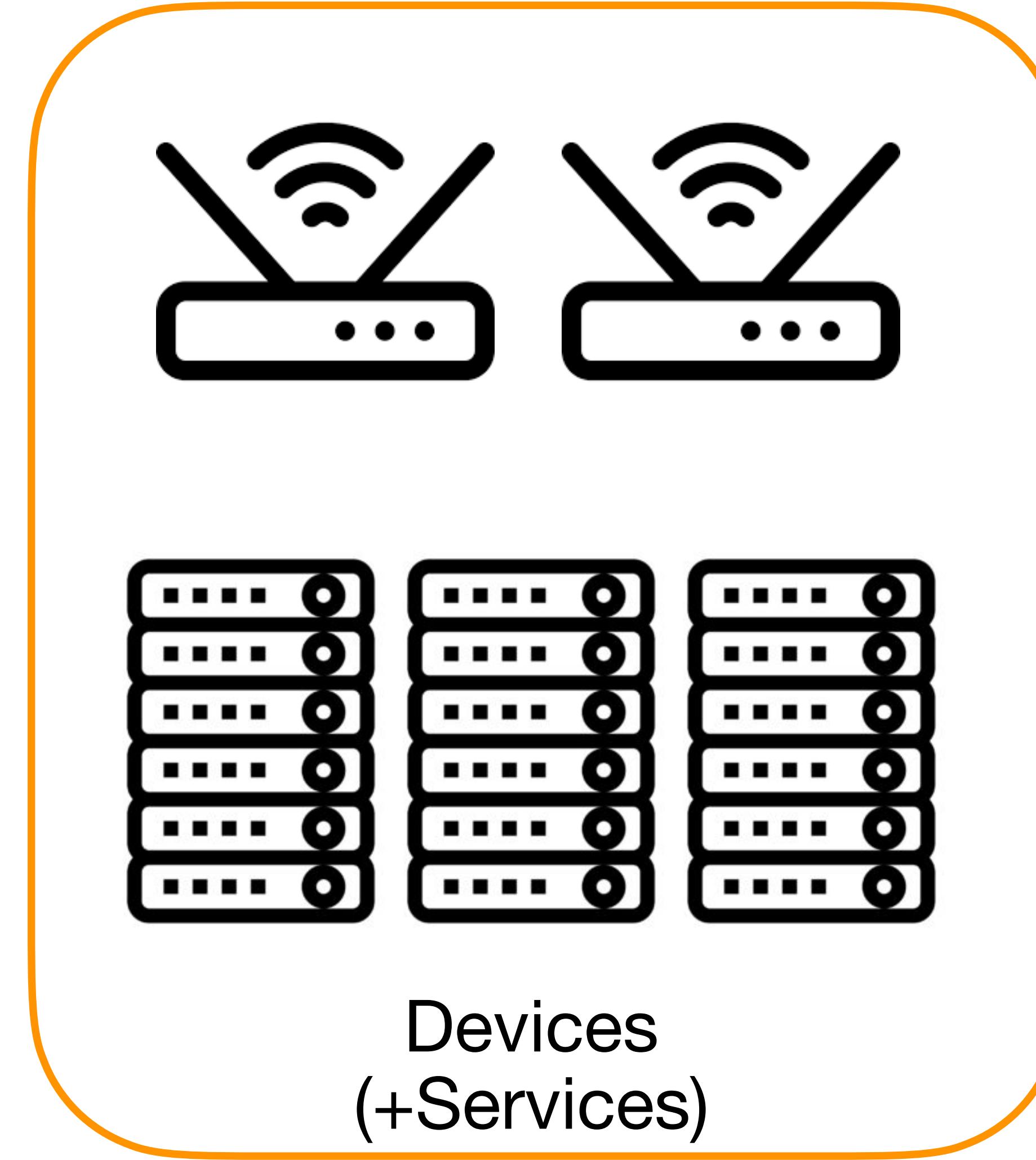
Devices  
(+Services)

Users  
(+Attackers)

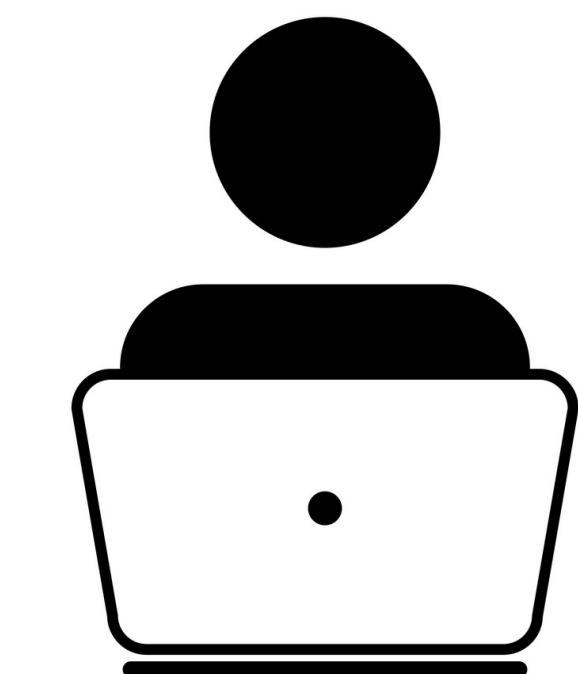
# The Internet is composed of multiple constituents



Networks



Devices  
(+Services)

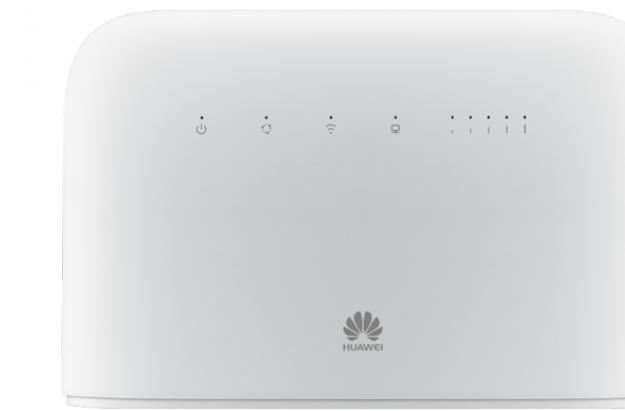


Users  
(+Attackers)

# The Internet consists of many devices



# The Internet consists of many devices...that are (unintentionally) publicly-accessible



# Attackers are finding and abusing Internet exposed devices



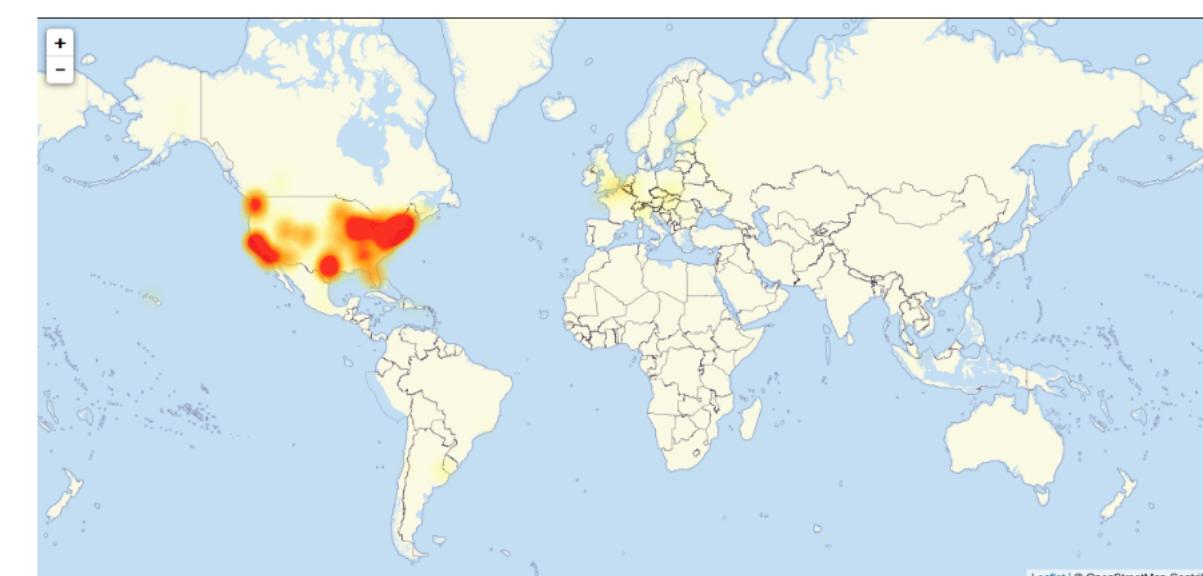
# Attackers are finding and abusing Internet exposed devices



The New York Times

**Hackers Used *New Weapons* to Disrupt Major Websites Across U.S.**

[Share full article](#) [Email](#) [Bookmark](#)



A map of the areas experiencing problems, as of Friday afternoon, according to downdetector.com.

# Attackers are finding and abusing Internet exposed devices



The New York Times

Hackers Used *New Weapons* to Disrupt Major Websites Across U.S.

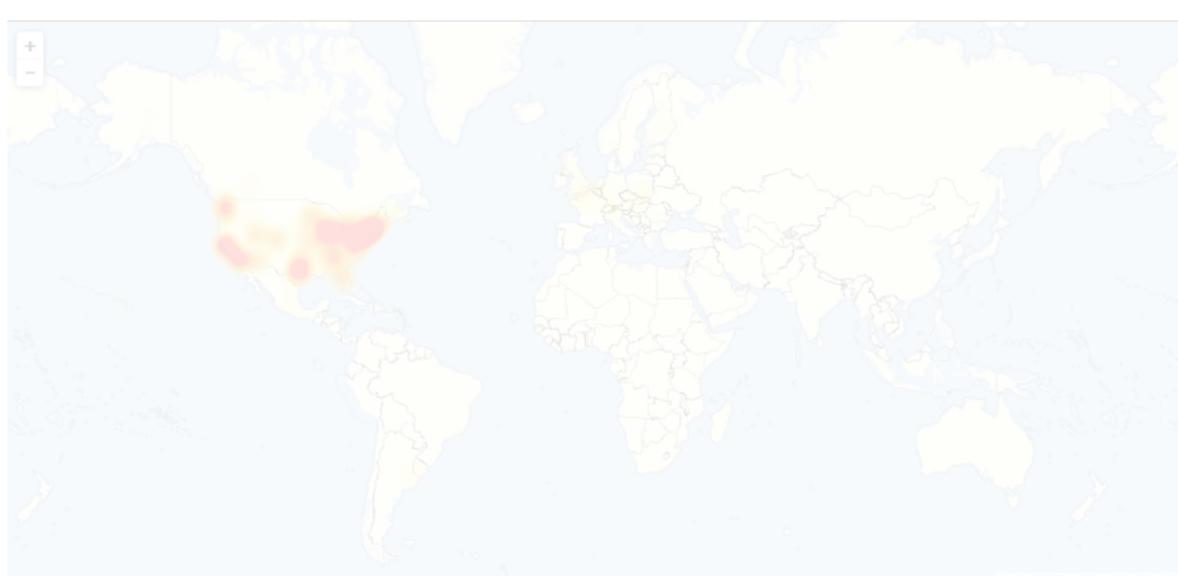
Share full article

AP

WORLD U.S. ELECTION 2024 POLITICS SPORTS ENTERTAINMENT BUSINESS SCIENCE FACT CHECK

U.S. NEWS

States and Congress wrestle with cybersecurity after Iran attacks small town water utilities



# Why are operators not securing their devices?



# Why are operators not securing their devices?

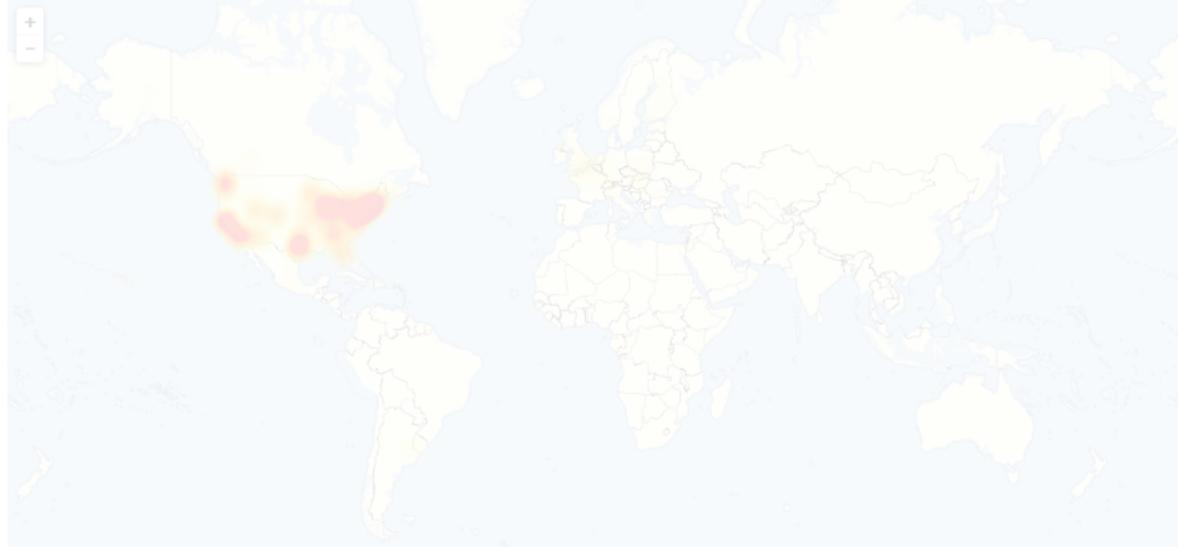
Operators often do not know their devices are

- publicly accessible
- vulnerable

The New York Times

## Hackers Used *New Weapons* to Disrupt Major Websites Across U.S.

Share full article



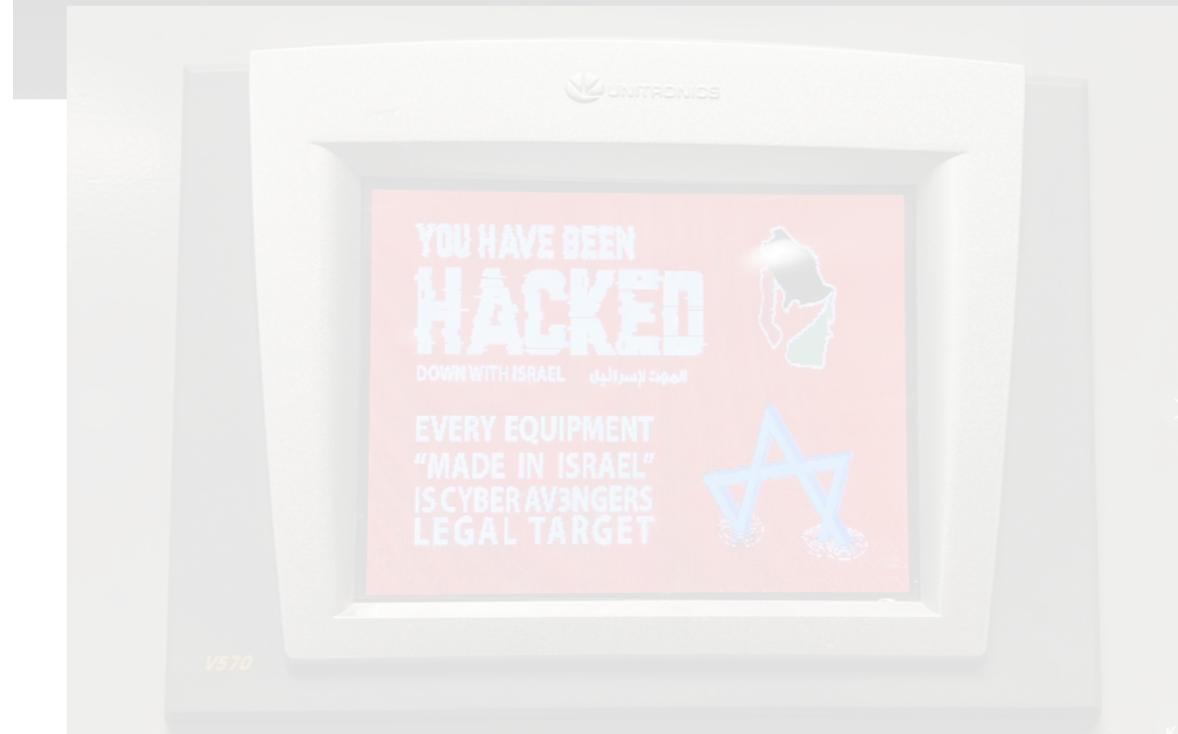
A map of the areas experiencing problems, as of Friday afternoon, according to downdetector.com.

AP = WORLD U.S. ELECTION 2024 POLITICS SPORTS ENTERTAINMENT BUSINESS SCIENCE FACT CHECK

Israel-Hamas war Nevada primary King Charles Marvel crewmember dies Taylor

U.S. NEWS

## States and Congress wrestle with cybersecurity after Iran attacks small town water utilities



# Why are operators not securing their devices?

Operators often do not know their devices are

- publicly accessible
- vulnerable



The New York Times

Hackers Used *New Weapons* to Disrupt Major Websites Across U.S.

Share full article

A map of the areas experiencing problems, as of Friday afternoon, according to downdetector.com.

This screenshot shows a news article from The New York Times. The headline reads "Hackers Used *New Weapons* to Disrupt Major Websites Across U.S." The word "New Weapons" is highlighted with a red oval. Below the headline is a world map showing yellow and orange dots indicating affected areas, primarily concentrated in North America. A caption at the bottom states, "A map of the areas experiencing problems, as of Friday afternoon, according to downdetector.com."

AP

WORLD U.S. ELECTION 2024 POLITICS SPORTS ENTERTAINMENT BUSINESS SCIENCE FACT CHECK

Israel-Hamas war Nevada primary King Charles Marvel crewmember dies Taylor

U.S. NEWS

States and Congress wrestle with cybersecurity after Iran attacks small town water utilities

This screenshot shows a news article from AP. The headline reads "States and Congress wrestle with cybersecurity after Iran attacks small town water utilities". The word "cybersecurity" is highlighted with a red oval. The background of the page is dark, and there is a small image of a computer monitor displaying a message about being hacked.



# Why are operators not securing their devices?

Operators often do not know their devices are

- publicly accessible
- vulnerable

Protecting the Internet requires visibility  
into devices, networks, and their users

# Why are operators not securing their devices?

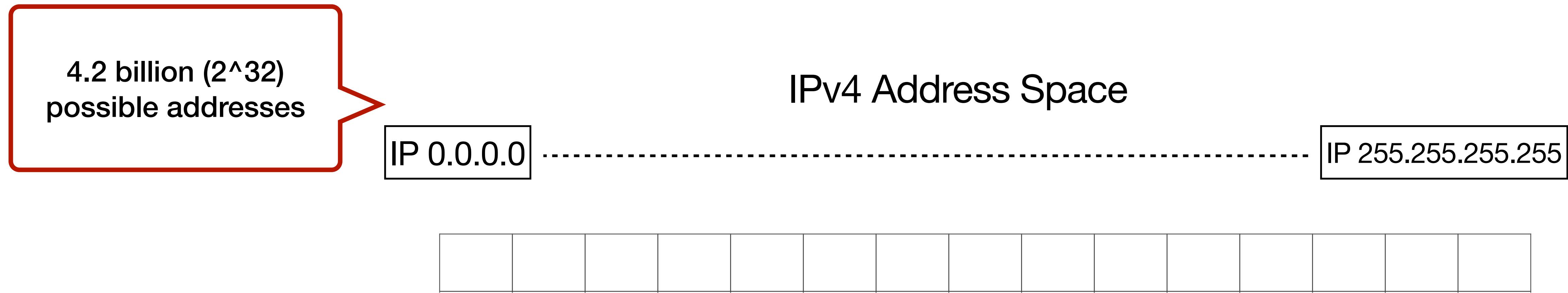
Operators often do not know their devices are

- publicly accessible
- vulnerable

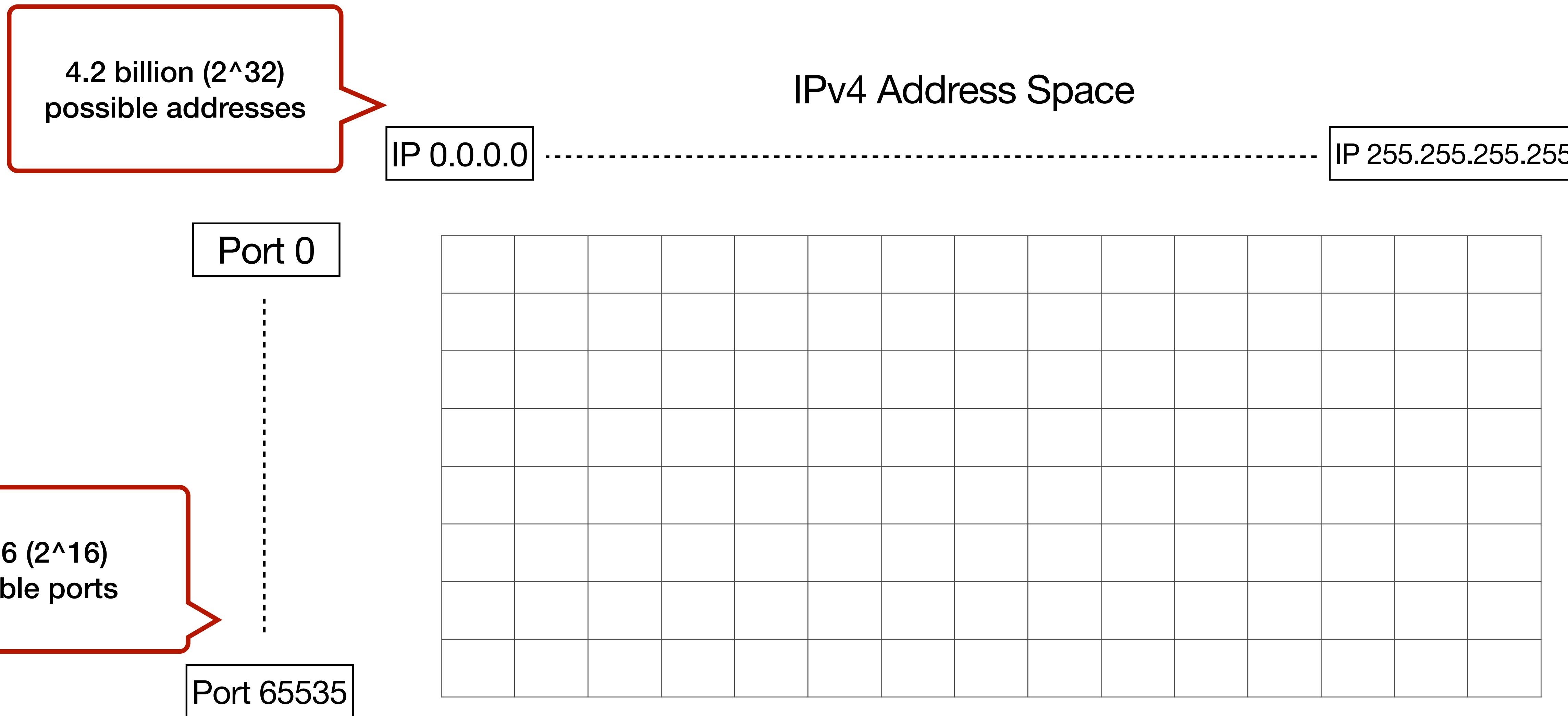
Internet Measurement!

Protecting the Internet requires visibility  
into devices, networks, and their users

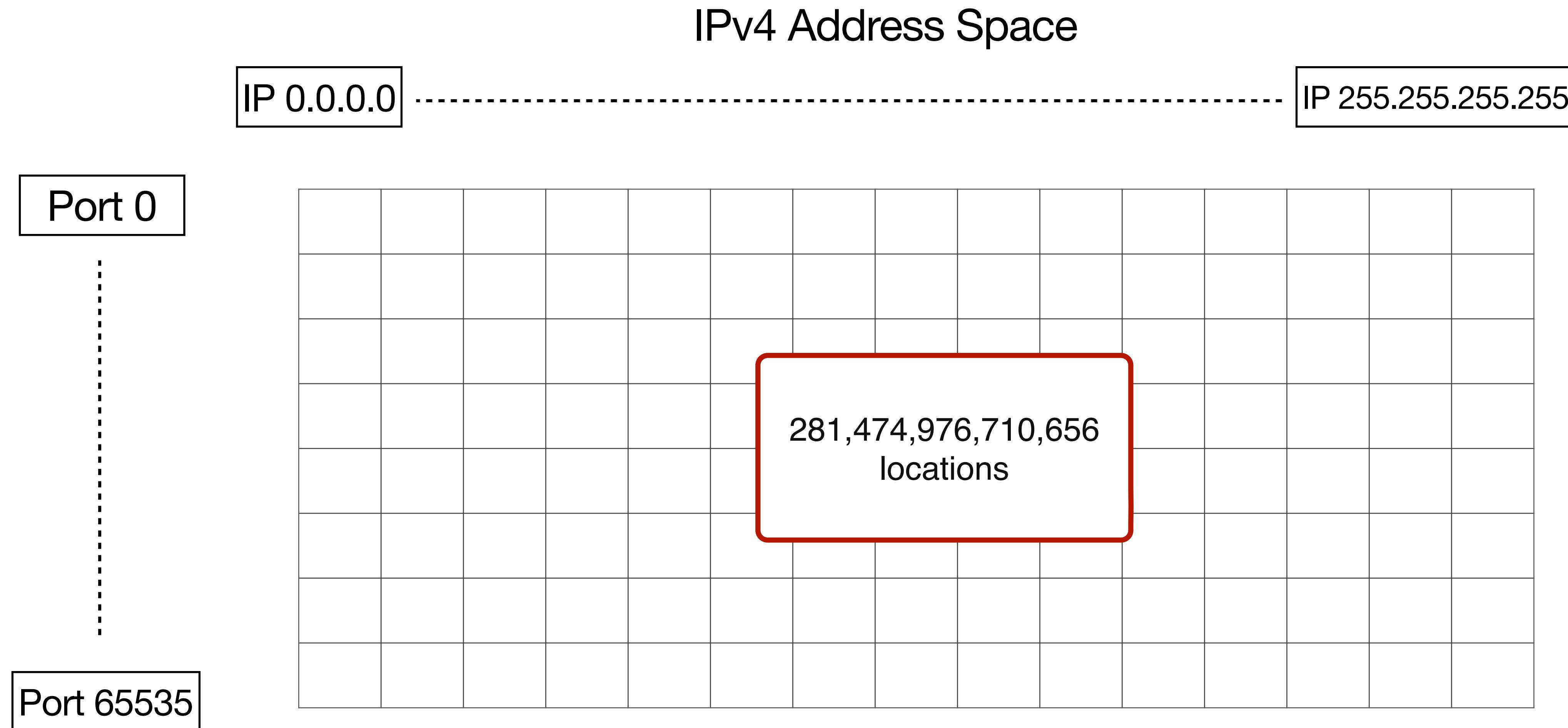
# Visibility is challenging because the Internet is large and sparse



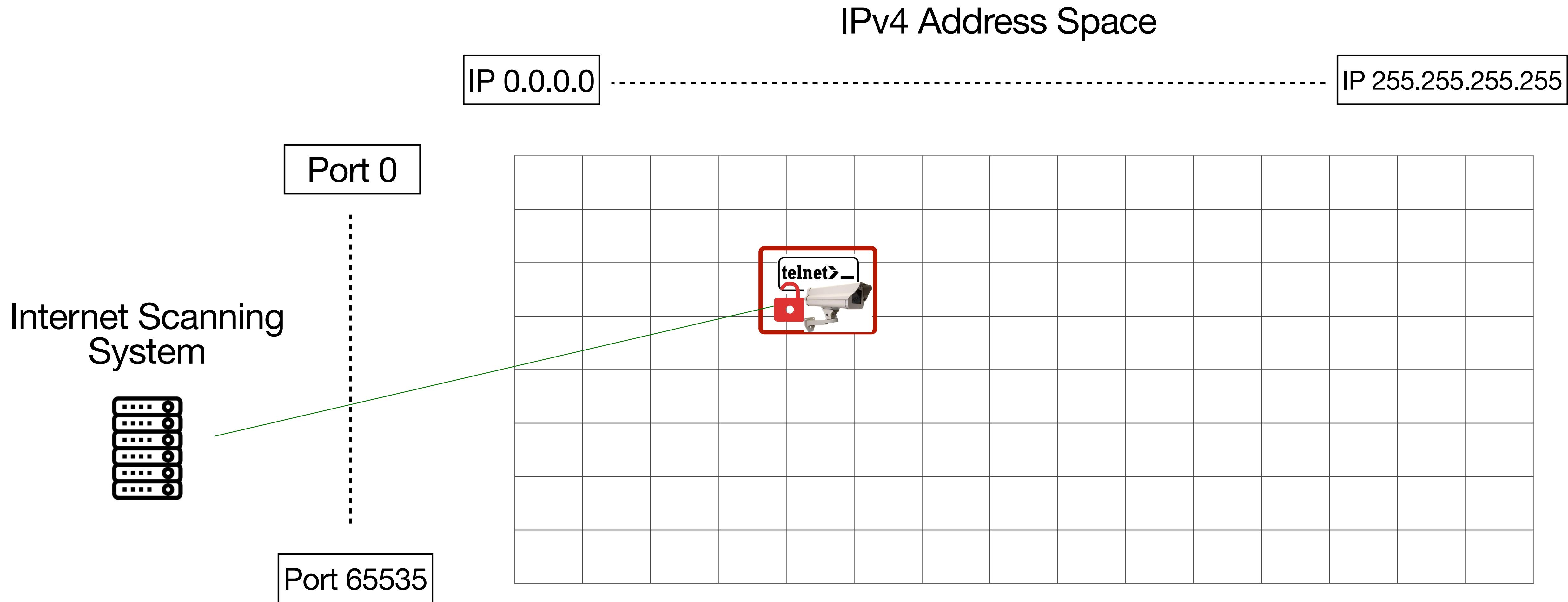
# Visibility is challenging because the Internet is large and sparse



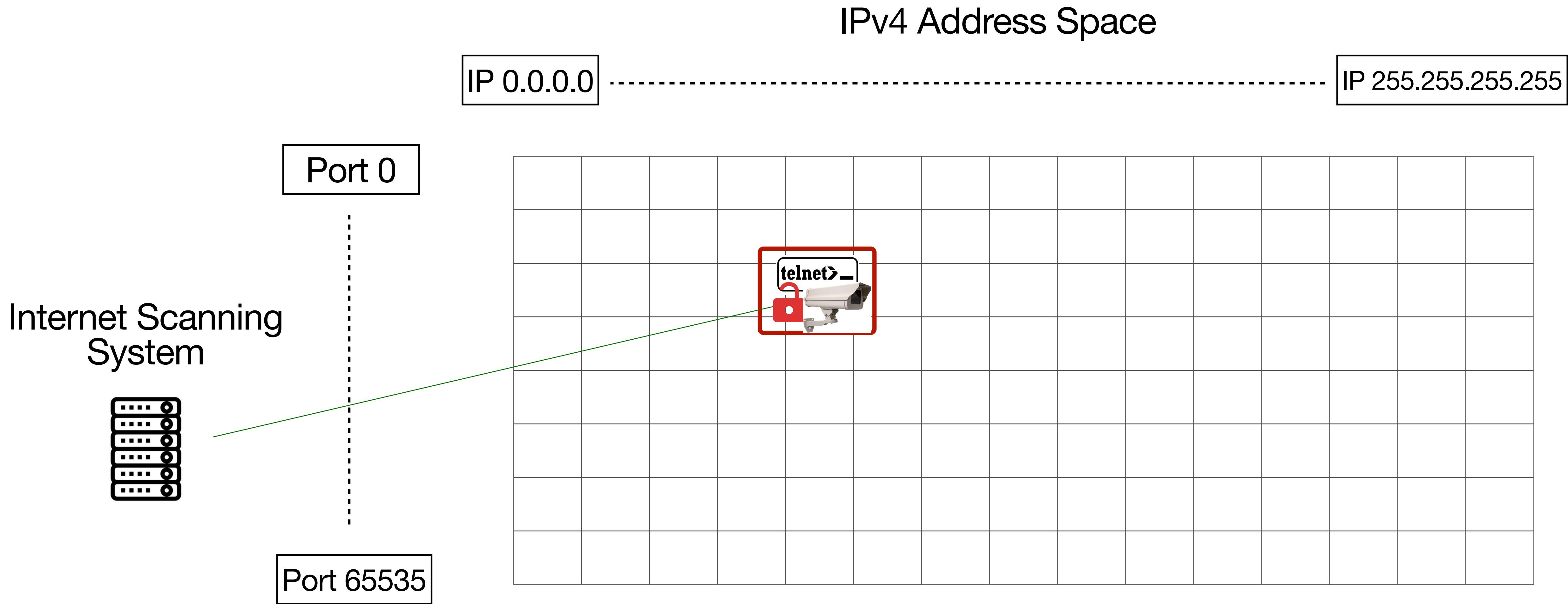
# Visibility is challenging because the Internet is large and sparse



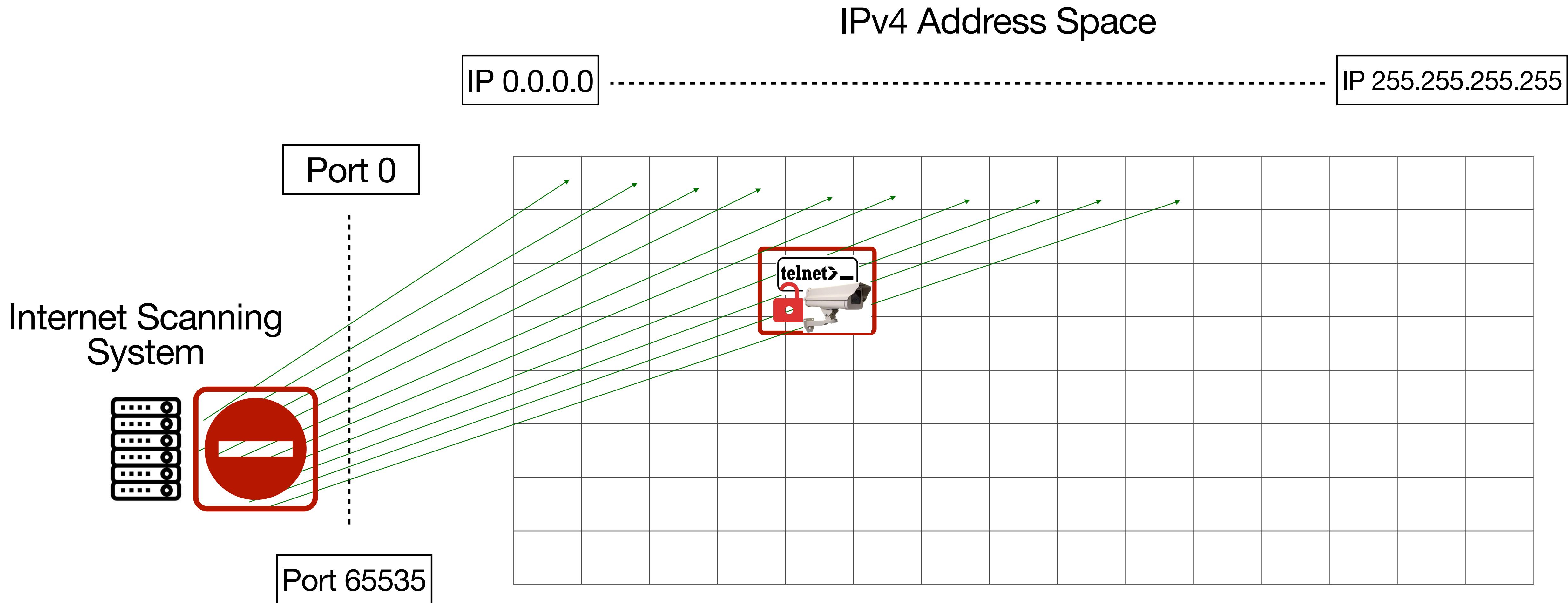
# To detect services, “Internet scanning” probes (IP,Port) pairs



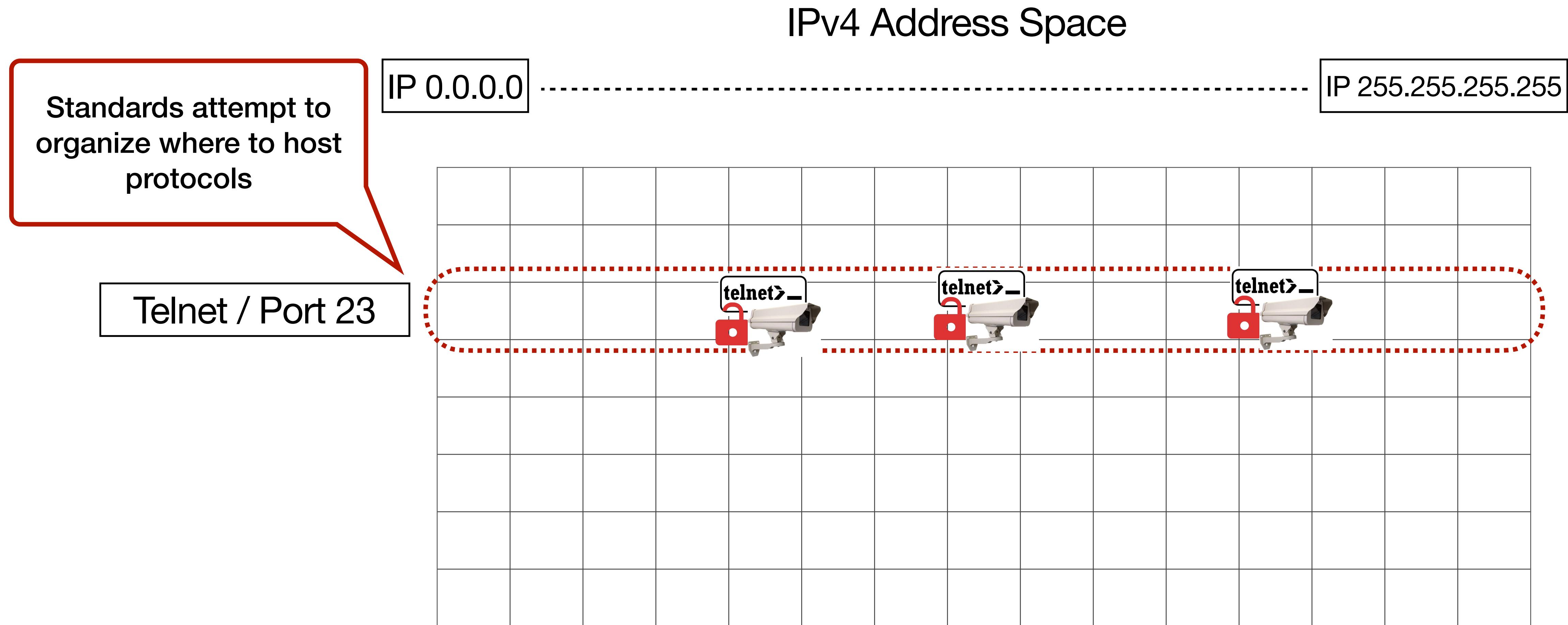
# How do scanning systems know where to find services?



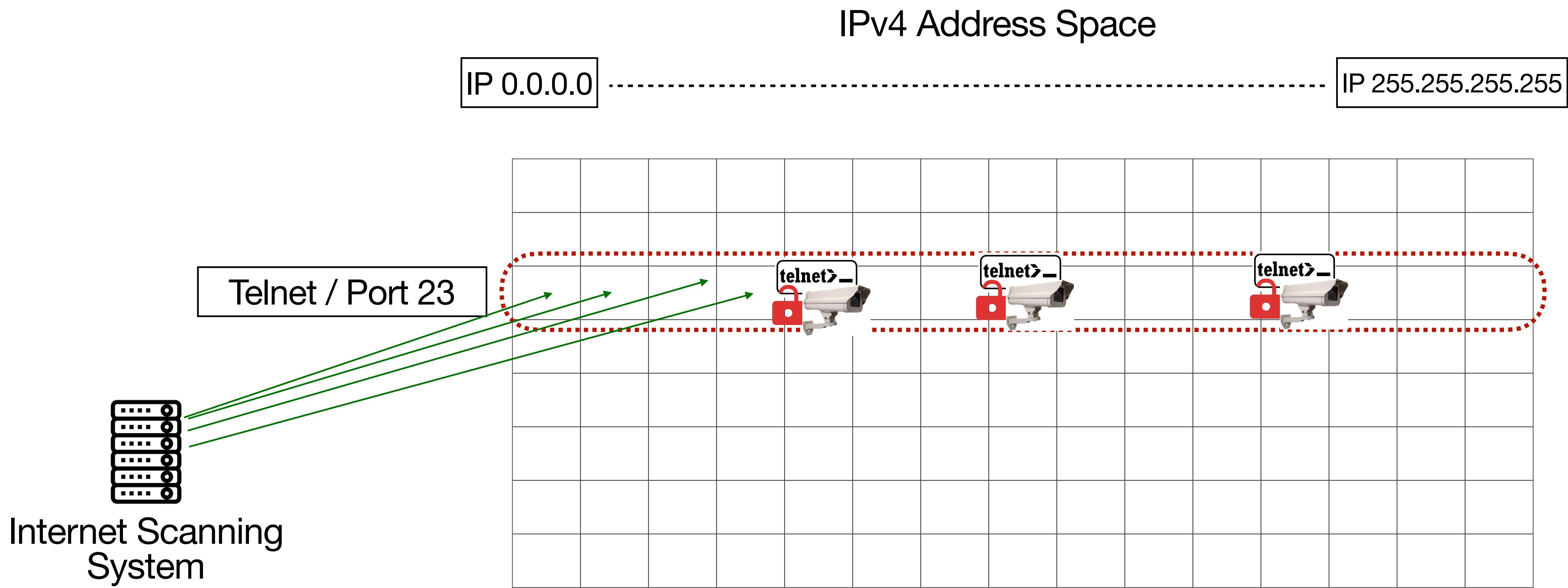
# The Internet is too large to exhaustively search



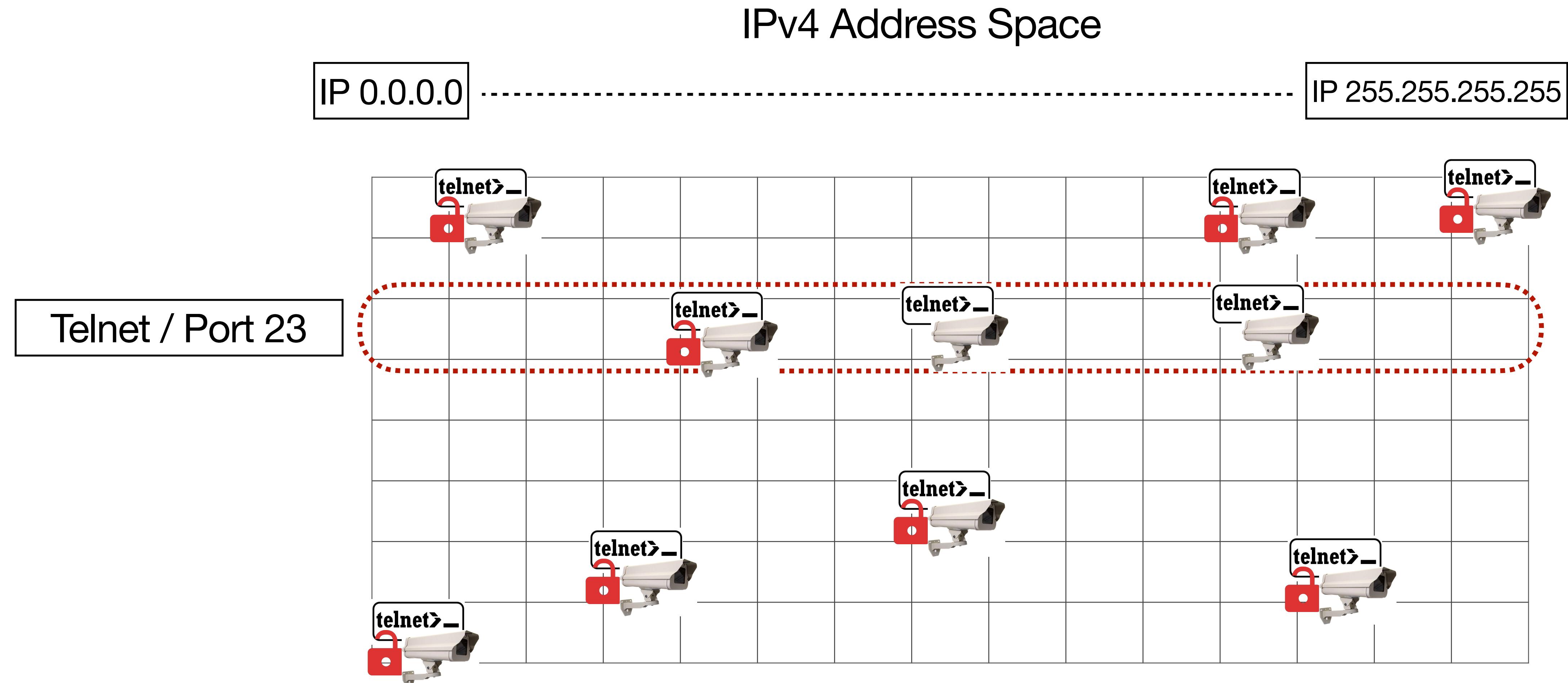
# Existing Internet scanning systems use standards to find services



# Existing Internet scanning systems use standards to find services



# But, the majority of services are non-compliant!



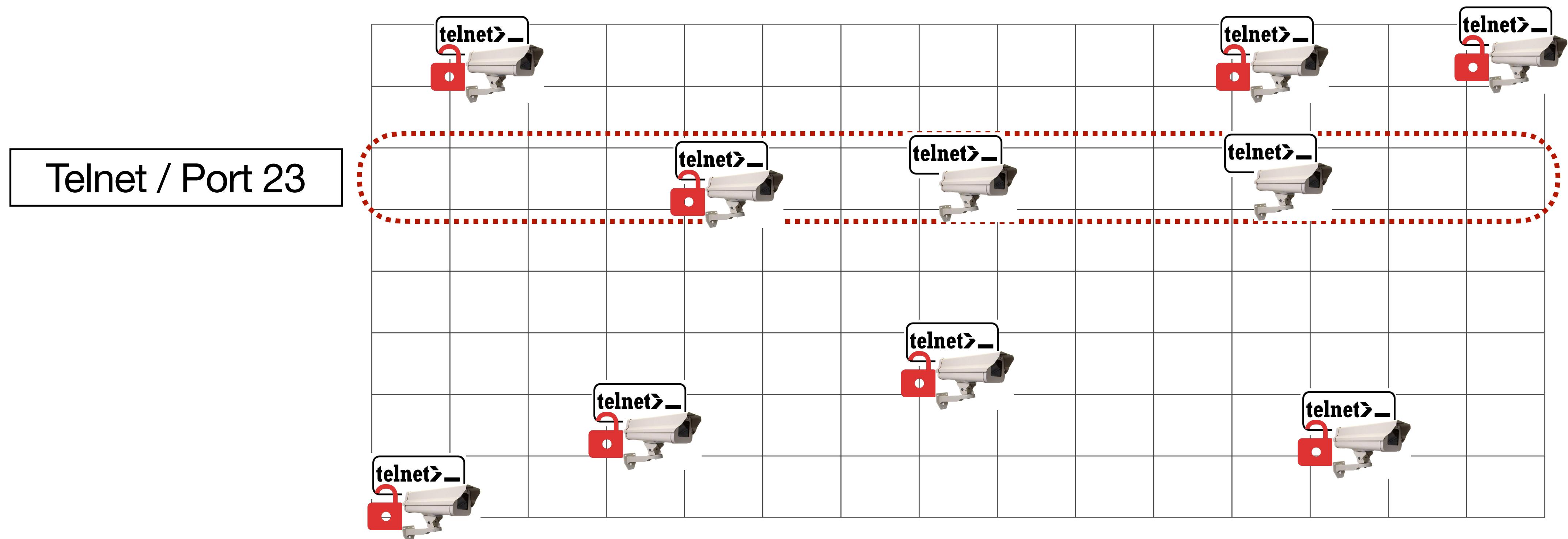
# But, the majority of services are non-compliant!

95% of Telnet is not on port 23

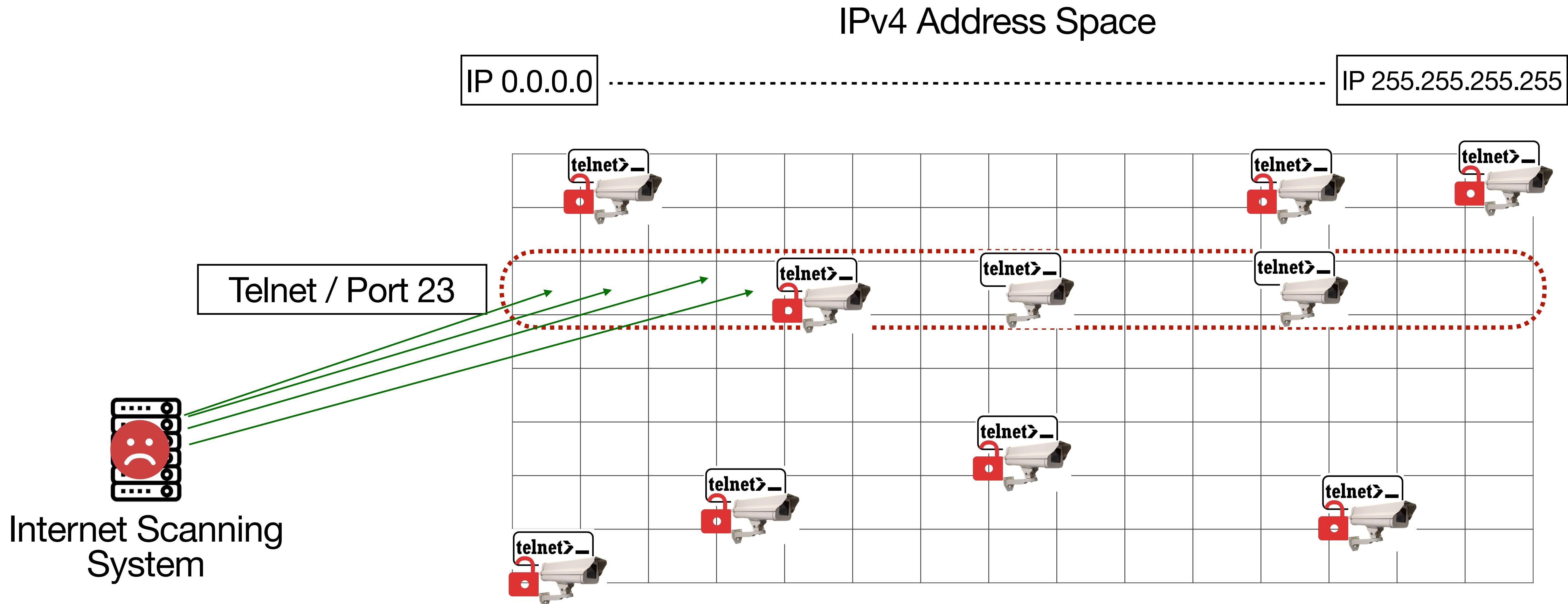
IPv4 Address Space

IP 0.0.0.0

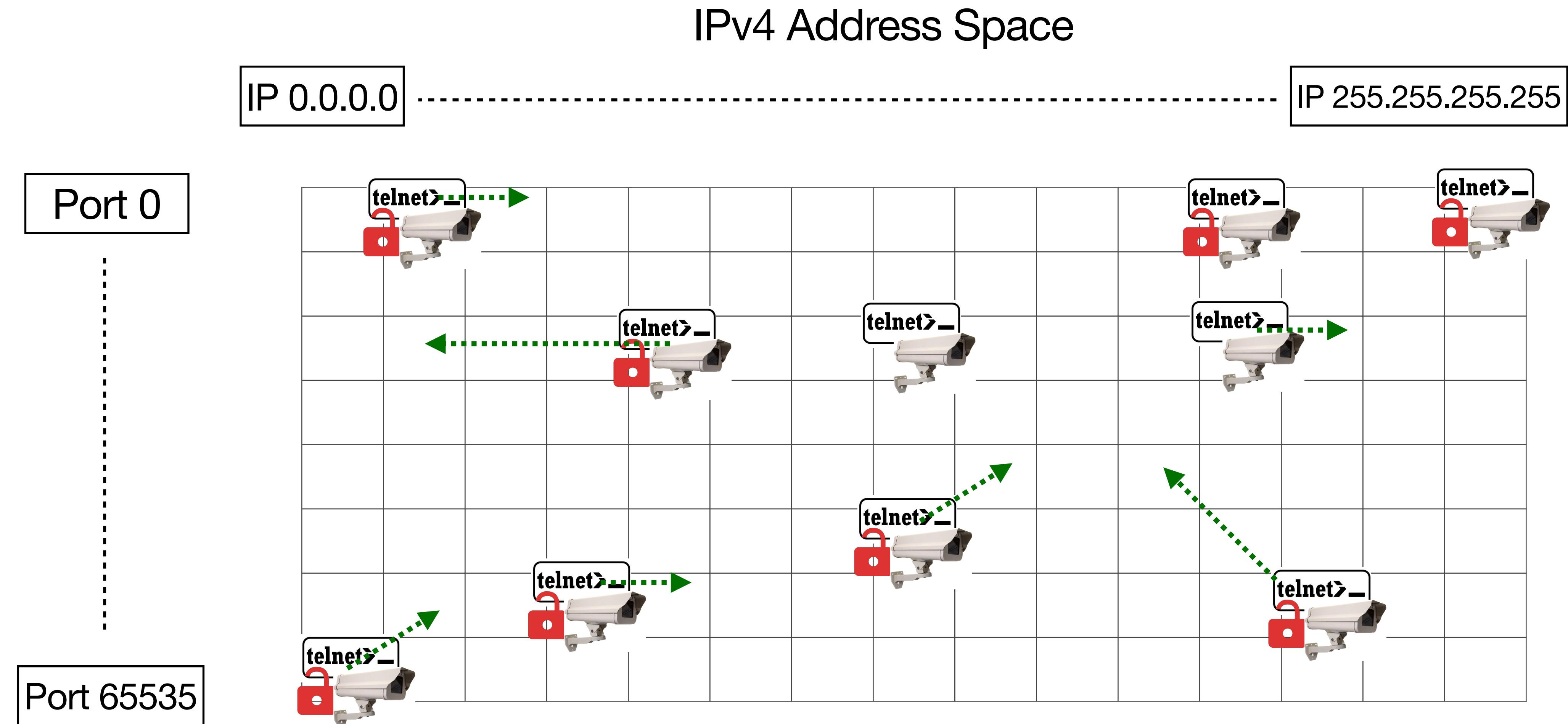
IP 255.255.255.255



# Existing systems miss the *majority* of devices

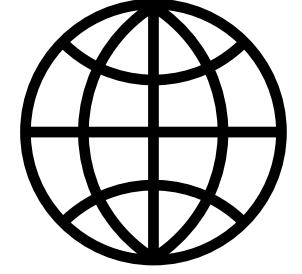


# Internet service location constantly changes



# The Internet is Complex

Internet



Inconsistent

Large

Ephemeral

# This course covers many aspects the Internet and its Security



Internet Scanning Techniques

Abusing Internet Scanning (Botnets)



Internet Scanning Techniques



Scanning and Abuse of Storage

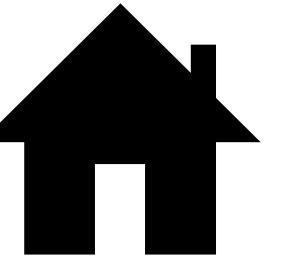
Abuse of Compute



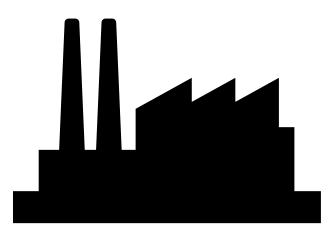
Satellites

Insecure GEO Satellite Networks

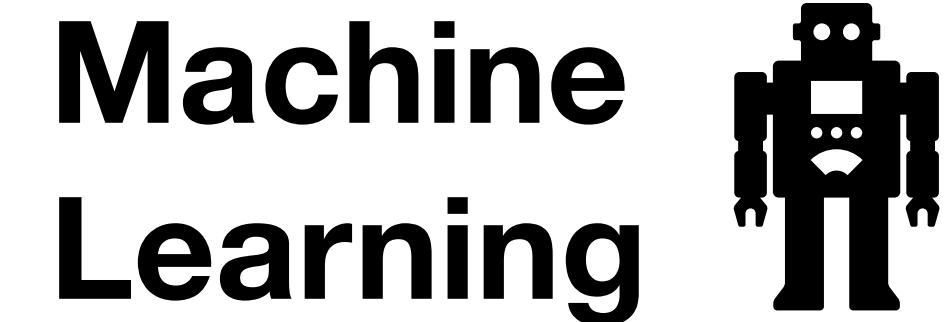
Measuring LEO Satellite Networks



Internet of Things (IoT)



Industrial Control  
Systems (ICS)



Machine Learning

Applications for Network Security

Large Language Models

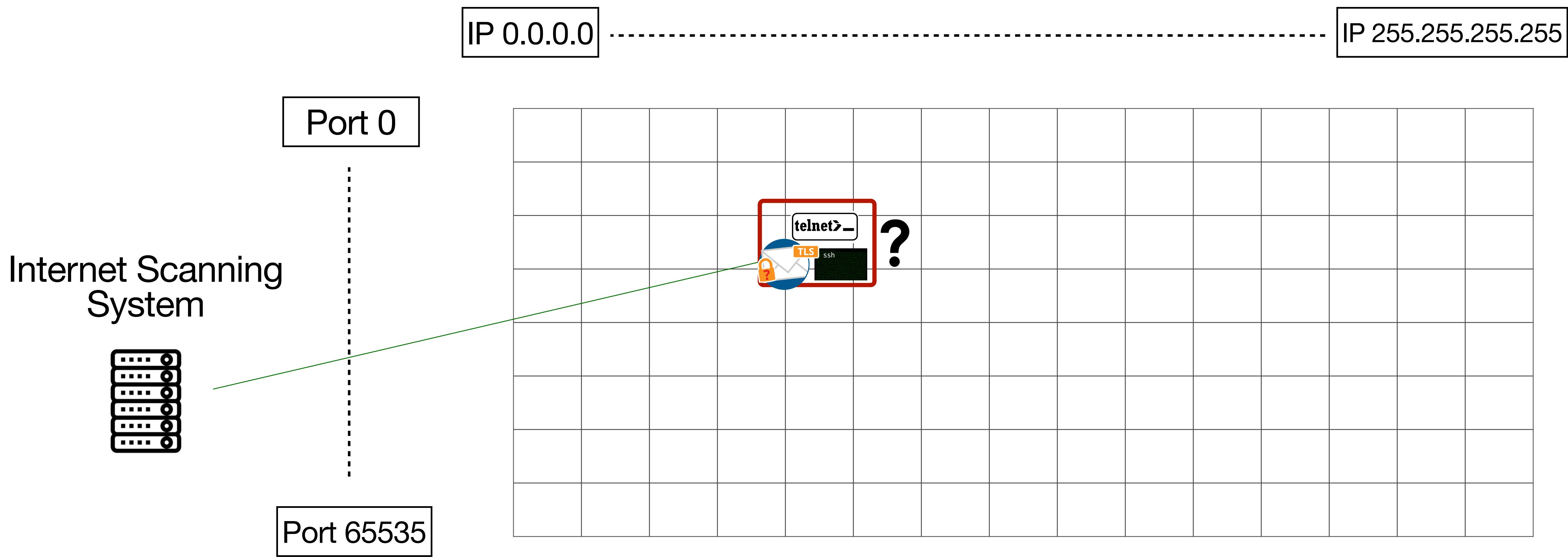


Internet Criminals

# LZR: Identifying Unexpected Internet Services

USENIX  
SECURITY SYMPOSIUM

# How do we efficiently identify services on unexpected ports?



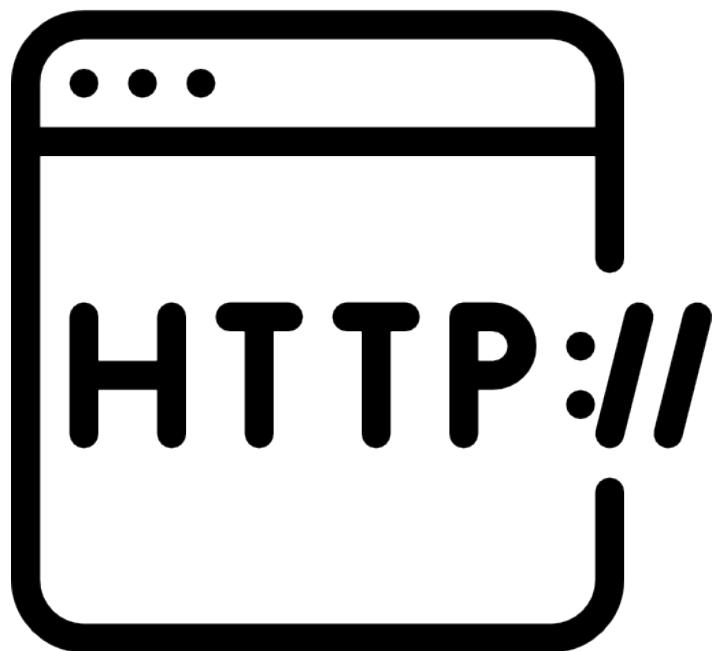
# Community Standards assigns services to ports



-----BEGIN RSA PRIVATE KEY-----  
MIIIEpAIBAAKCAQEcaycIxxvf/DAPLnNTEVU/HedHXHmrHgZa/6/WnaxZCvz3  
7C/CQDagP8rJ5Kjw/D.../23Iy5AdkI9LRNNJfyAgidc0rqzMvu/uEwghGfeN  
FmWgq9nk6Ku...XKd.../4f1TE2uXfJqMoW5wNqHuYSMonEpNCL3OZYxOzI4ywM  
TnEdqJbi2+.../Ew.../1.../20.../dbSUC1t7G2T3Iu2JyphGRx6RUQX0mgTtAycsFmu5  
qtOPHQqlNRBc7qL0M0XAjGcVbUtB7xVs5mg5YTDguEHuWgdj/VIPB0kY9B8uSle...  
hEgMFnzsdEFxr5ID2RfwMyPmrwd8Wq-hwlIjeQIDAQABaObAeavTaVkyZgUv1FTh  
sqPQMKrTtPuBYEF+KGKWoK3PEUYB929FUGiBghVJBFHm2NqDONG1W867C4s8Hg  
L7o52Bz9/NSoDkazykZxNySEHf3oIaki2V52s8z1hky7J0C12tnk71N5o6S/1  
blfEqfnJ7jzWpWSnTimsGgs9T8sBkLRW89UoxoyQ410sgrdtcWh7E7PFKhn  
k0sJhs2CET7KJmndBla08EZ1ZT2ljhMrn5u4RaJnnms5rdVz0Bz2fZtcIec9tRoA  
AvdPEnMLTgD2Hnf55//9YrGj1jYUDw4P8gDWFqHfpY01QK0h/CpbSyQdpLoXG82  
NncVFSECGyEA9dHqLkqHgLVd9f678juH+UiQXz5uFtEvLxDpAfEE11lhVfk4JH  
0Si10gbze/k3SJ7V0WnhmmAVNPKFauXm3wXvbaWtZuJ1Lz1SusG6lXp0w/nAAy  
Ck2f/0/7AfuiwyGwAb0Umy0JrgSp/wJuL6Zf6DdfM0sK32zPxclry1...00CgYeAwude  
GzgDLG+8ssFZZBt+FyrWNdVLWR0B650h+K7jZpJgQd0QzqXDU09kLJ9rUrADRXCP  
7vAxU10d8t+BH99PD+r-JPC5V5Asca0R8BA1LHRw5eu5V9453+j4rJrxVHrbkEzHn  
goHsh8ed8NyDz8e4rDU0j0t2kRf6Byfz05a6N0CgyEAvdtwW3xNqLuJcJri/Q5ie  
n4G4-c4Pm7t6IK+bh2caY6G7nWxV8mf6...GmNSW...hge/...r0n1k4MXz...p0...h2...hC

IP 1.2.3.4

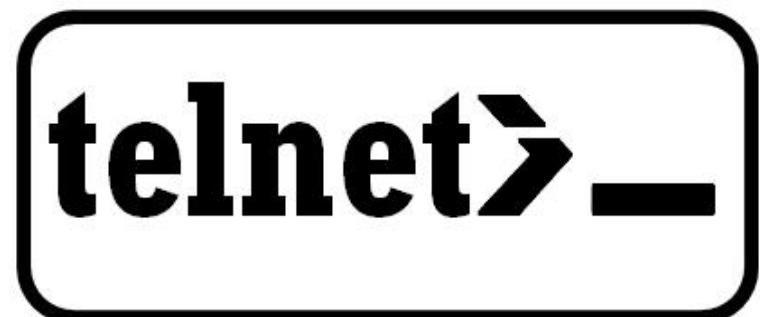
# Port 22



# Port 80

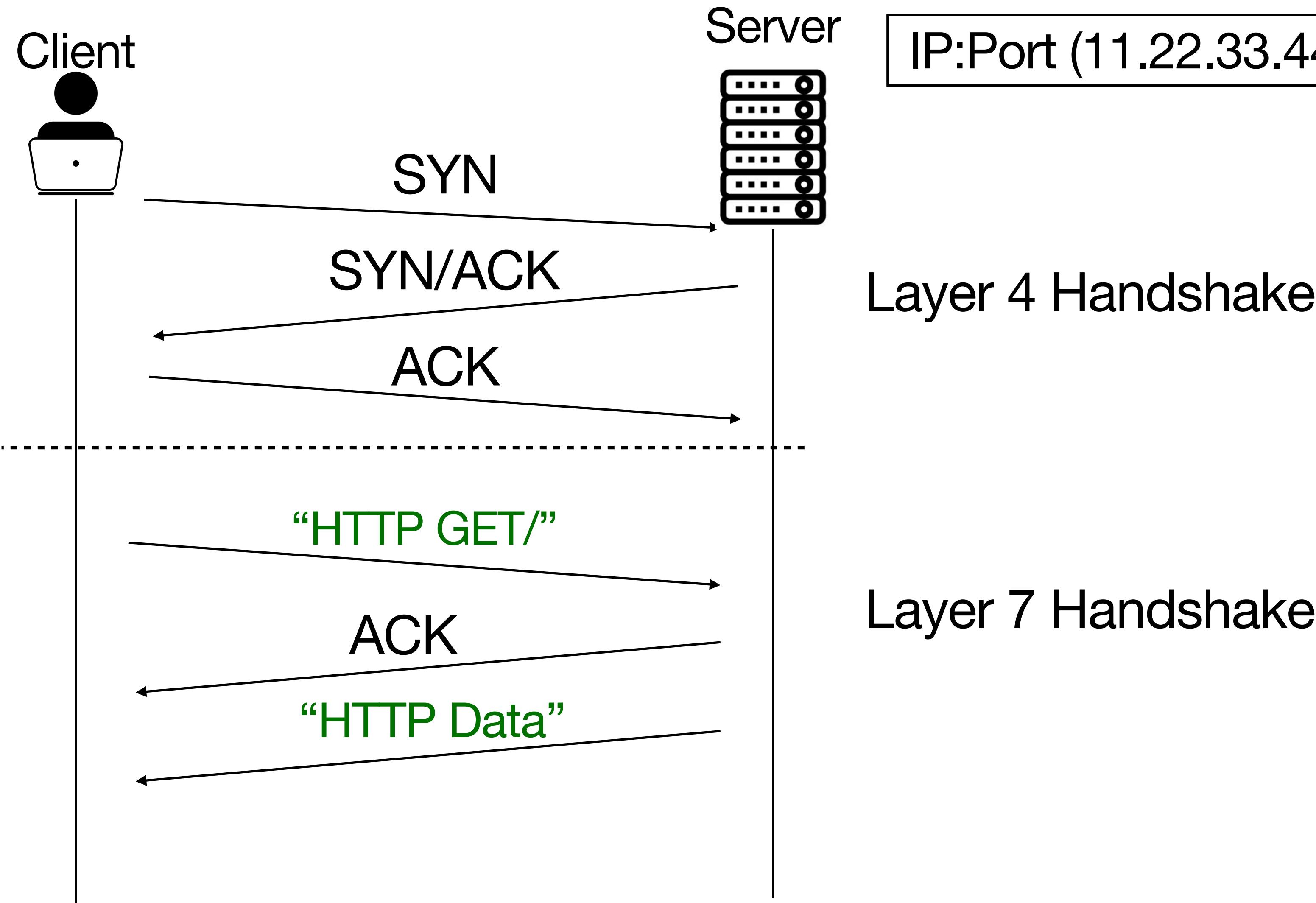


**https://**



# Port 23

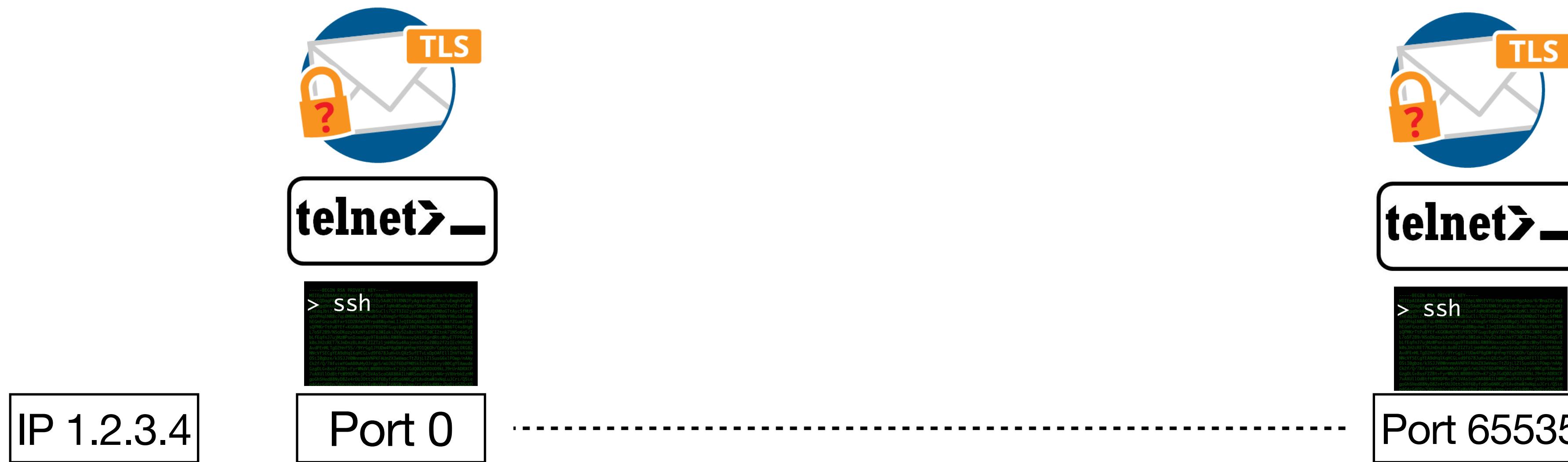
# Traditional TCP Handshake Assumes Service



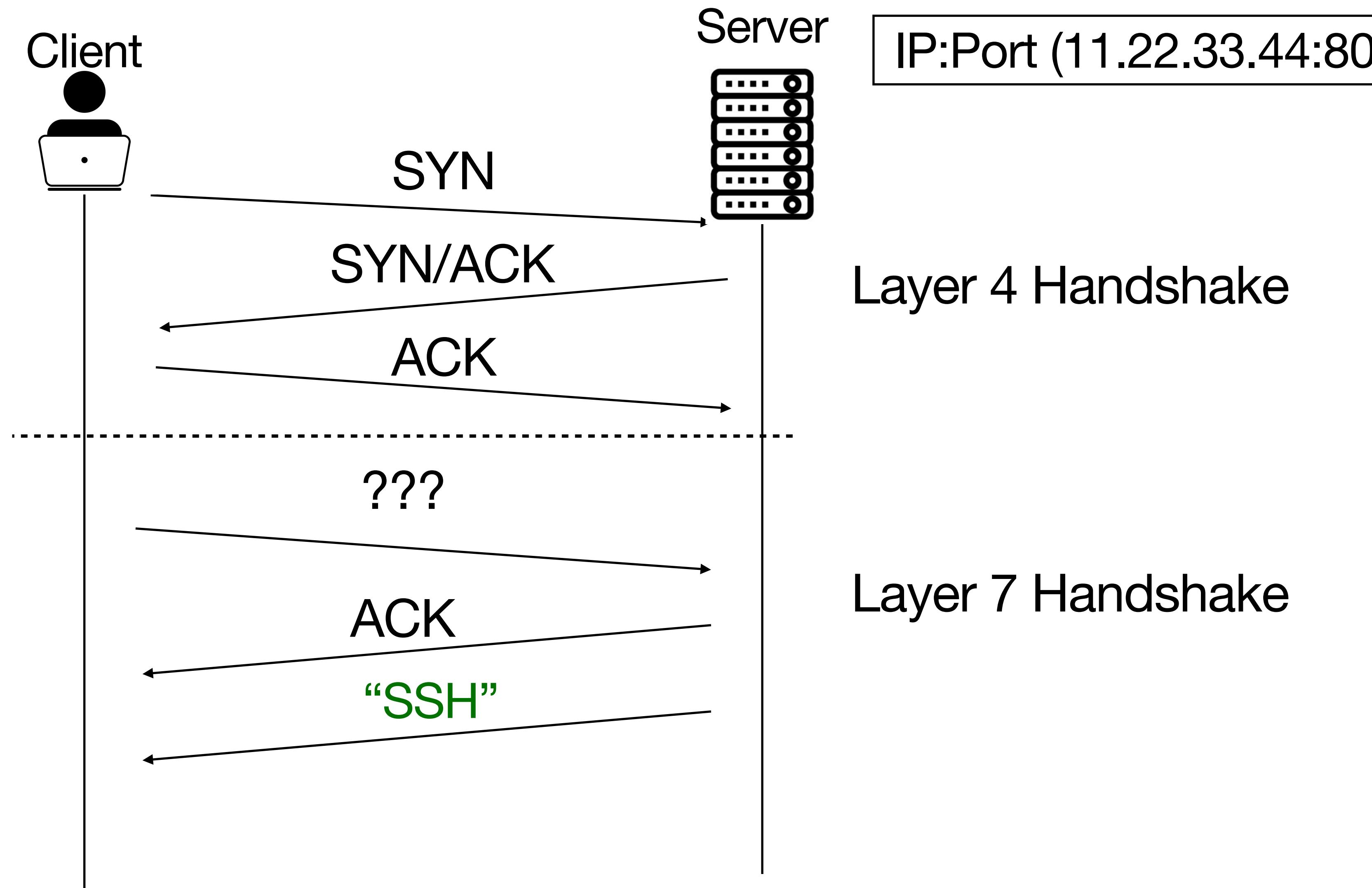
IP:Port (11.22.33.44:80)

Data	Layer
Data	Application Network Process to Application
Data	Presentation Data Representation and Encryption
Data	Session Interhost Communication
Segments	Transport End-to-End Connections and Reliability
Packets	Network Path Determination and IP (Logical Addressing)
Frames	Data Link MAC and LLC (Physical addressing)
Bits	Physical Media, Signal, and Binary Transmission

# But technically, any service can be hosted on any port



# Traditional TCP Handshake Does Not Know True Service



```
--BEGIN RSA PRIVATE KEY--  
MIIEpaTBAAKzA0fEAnyc...xyF/D4p1NNtEVYU/HedHxmrgHzo/6/WneZCzv3  
c/CC0opPn...23TySA4KJ9LRMJu...yAgidc0pqzMu.../uEwghGfENj  
E...ap9hk...TE2uxf1gMolSwNaHuYS...Monenp...CL30ZY...OZ1...YmMF  
n...d...Jb1Z...L...dbS...1.7G2T3TU2...jyp...Grx...6RU...XM...o...GT...Ay...c...FM...US  
q...OPH...1...N...B...c...7...q...0...M...Y...A...1...G...e...Y...u...R...t...7...s...X...V...m...g...5...r...Y...D...B...e...H...u...W...d...3.../V...P...B...0...k...Y...B...u...S...h...l...em...w...  
h...C...m...G...n...z...d...f...E...x...s...T...D...2...R...f...w...M...Y...r...p...d...w...q...h...w...1...1...1...0...Q...D...A...0...B...a...t...B...A...e...T...V...A...k...Y...G...w...1...F...H...  
s...Q...P...M...K...c...T...P...u...Y...F...+...K...G...w...a...P...E...U...Y...B...9...2...F...u...g...1...B...h...v...1...B...F...H...m...2...n...q...D...N...G...1...W...B...G...T...4...4...8...l...g...B...  
L...7...5...F...2...B...9.../...N...s...d...k...z...k...y...X...N...Y...e...H...f...c...2...t...l...a...k...1...2...v...y...5...2...s...2...1...h...k...y...7...2...0...C...2...t...n...k...7...1...N...s...o...q...5.../...1...  
b...l...F...e...q...f...n...1...7...1...j...M...z...w...P...s...n...1...c...m...c...g...9...7...8...s...b...k...l...R...W...9...l...o...x...o...y...0...4...1...0...S...g...d...R...t...c...w...y...7...7...P...F...K...h...x...  
k...o...s...J...H...2...c...R...E...T...7...X...1...m...n...z...B...l...a...o...E...Z...1...2...t...1...j...h...l...R...m...u...d...R...c...i...m...p...5...r...d...v...2...0...b...2...f...2...2...1...f...-9...1...R...O...A...C...  
A...v...d...P...t...H...M...T...g...0...2...l...n...f...5.../...9...Y...g...1...1...Y...D...w...4...8...g...W...f...h...f...m...p...Y...0...1...0...Q...O...h.../...C...p...S...y...d...p...0...O...G...8...2...  
N...N...c...V...F...S...E...C...g...Y...E...9...d...h...1...k...q...l...G...l...v...d...9...F...7...8...J...u...l...1...U...O...x...S...u...F...T...v...L...x...0...p...0...A...F...1...1...h...V...F...k...4...J...H...  
0...5...1...I...0...g...b...z...e.../...k...3...3...1...V...0...h...n...m...m...A...V...P...F...K...A...U...n...7...3...w...a...c...t...1...2...1...j...1...2...1...s...u...s...G...x...t...P...0...n...A...y...  
C...k...2...F.../...Q.../...7...A...f...u...w...Y...w...A...B...0...M...y...0...J...r...p...s.../...w...J...6...2...f...6...d...f...M...0...5...3...2...z...c...x...1...r...1...0...0...g...Y...e...w...d...  
G...z...d...l...G...-...8...s...F...Z...B...t...-...F...v...r...W...N...V...L...W...0...8...6...5...0...h...-...K...7...z...p...1...G...0...0...7...2...x...0...0...9...k...1...j...9...v...0...A...D...R...X...C...P...  
7...V...A...X...U...1...0...d...t...t...w...9...9...0...P...-...P...C...S...V...A...S...c...c...0...A...R...8...B...A...T...L...W...R...5...e...v...5...4...3...1...M...-...V...K...h...b...E...H...M...  
g...p...G...h...S...h...e...d...8...8...N...0...8...2...6...4...r...D...U...0...t...+...2...k...F...G...b...Y...r...0...5...d...G...N...C...y...E...A...v...d...w...3...N...q...l...u...C...r...1...Q...5...1...e...  
g...g...g...-...c...d...h...s...0...7...0...8...t...h...1...2...-...p...y...6...3...t...w...k...v...0...d...t...1...0...w...1...s...0...1...4...0...v...>.../...5...0...1...3...5...2...0...x...0...>
```

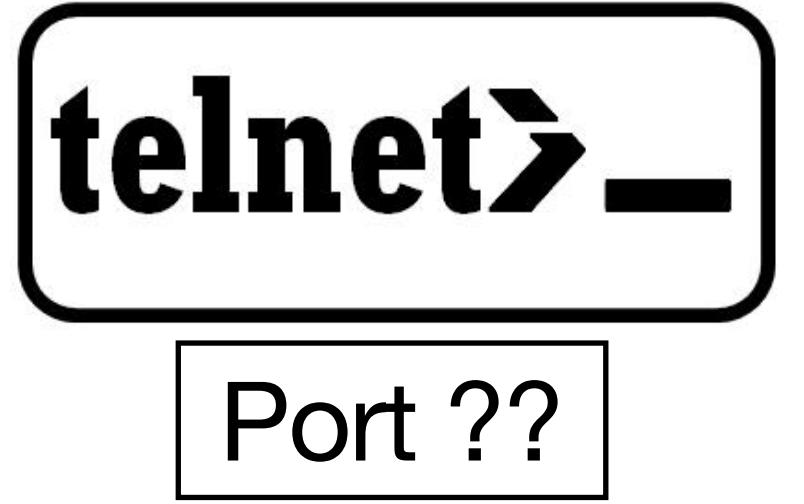


- Where are Internet services deployed in practice?

### LZR: Identifying Unexpected Internet Services

Liz Izhikevich, Stanford University; Renata Teixeira, Inria;  
Zakir Durumeric, Stanford University

<https://www.usenix.org/conference/usenixsecurity21/presentation/izhikevich>

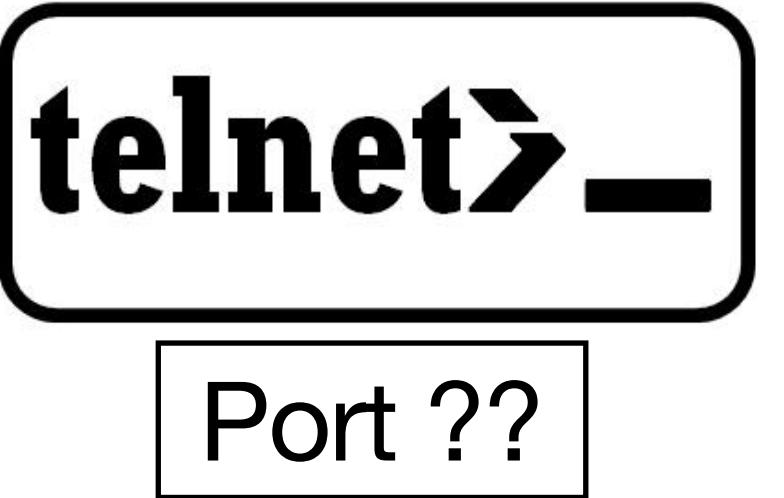


- Where are Internet services deployed in practice?

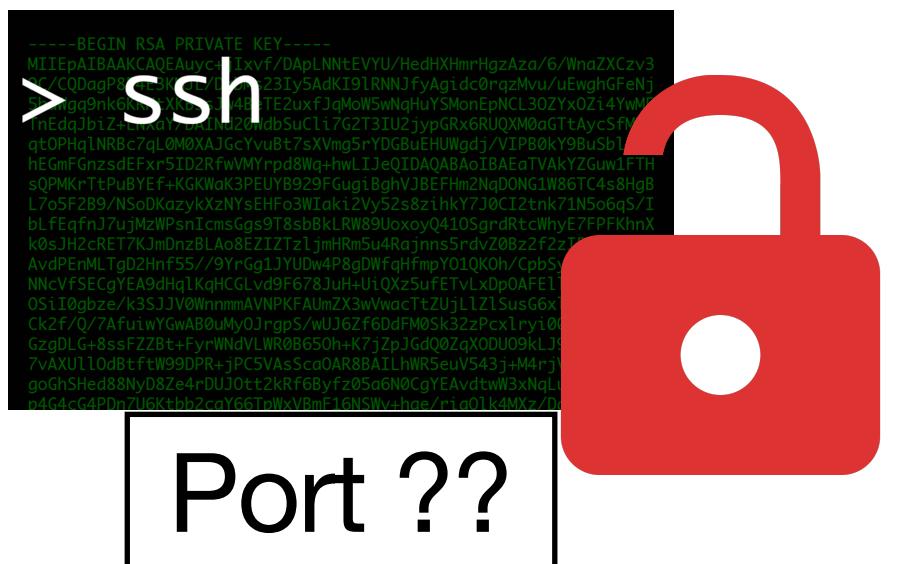
### LZR: Identifying Unexpected Internet Services

Liz Izhikevich, Stanford University; Renata Teixeira, Inria;  
Zakir Durumeric, Stanford University

<https://www.usenix.org/conference/usenixsecurity21/presentation/izhikevich>



- What is the security posture of services on unexpected ports?

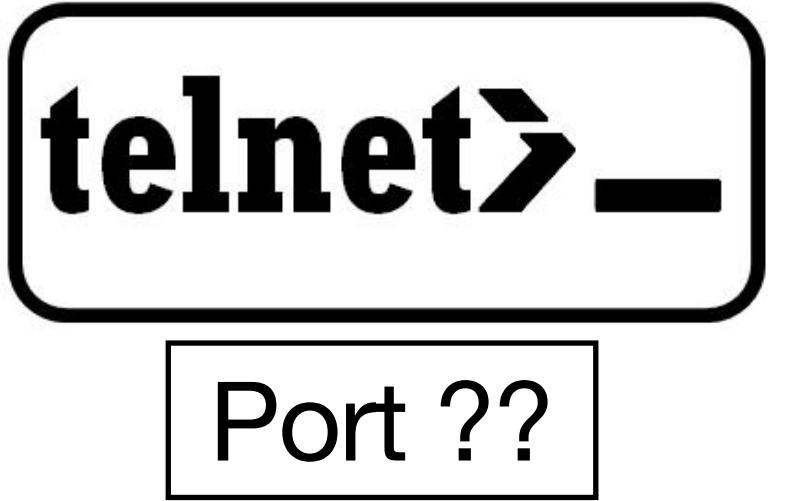


- Where are Internet services deployed in practice?

### LZR: Identifying Unexpected Internet Services

Liz Izhikevich, Stanford University; Renata Teixeira, Inria;  
Zakir Durumeric, Stanford University

<https://www.usenix.org/conference/usenixsecurity21/presentation/izhikevich>



- What is the security posture of services on unexpected ports?



- How do we efficiently identify services on unexpected ports?

# Questions?