Defending Computer Networks
Lecture 7: Port Scanning

Stuart Staniford

Adjunct Professor of Computer Science

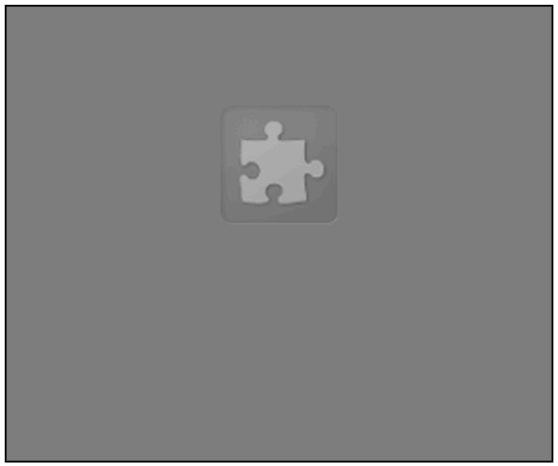
Logistics

- First quiz will Tuesday September 23rd.
  - Half hour quiz at start of class.
  - Covering everything in class through Thursday
    - and all readings assigned to date.
  - Shorter lecture after quiz.

Latest News

Netanyahu: Iran behind cyber attacks on Israel

Iran is behind cyber attacks against Israel, including during this summer's Gaza conflict, Prime Minister Binyamin Netanyahu said on Sunday evening. He spoke of the significance of Internet security both in the fight against terrorism and for the country's future economy.



"I want to make clear that the party behind the cyber attacks against Israel is first and foremost Iran," Netanyahu said as he addressed the fourth international cyber security conference at Tel Aviv University.

This includes cyber attacks by Hamas and other terrorist groups, Netanyahu added.

"Iran and its proxies take advantage of the security and anonymity of cyber space" to attack Israel and other countries, Netanyahu said.

http://www.jpost.com/Israel-News/Watch-Live-Netanyahu-addresses-cyber-security-conference-375290

Latest News

Many IT professionals still not confident of preventing a cyber attack

Despite the number of high profile attacks in recent months, many organisations are still lacking confidence in their ability to prevent a cyber attack or data breach.

These are the findings of a new survey from risk consultancy firm **Protiviti**, which also shows that companies aren't properly preparing for crises and often don't have adequate core data policies.

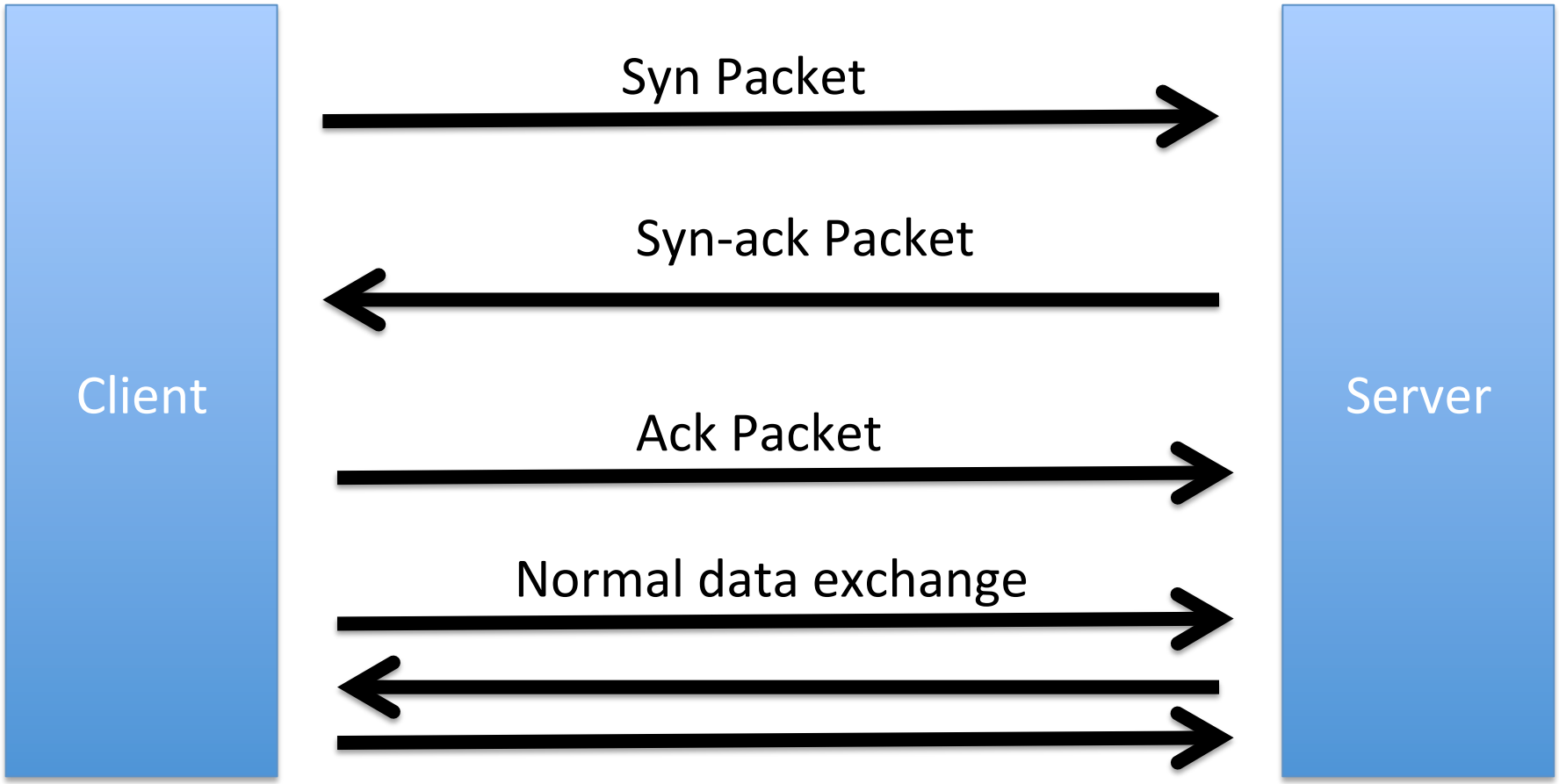
"Our survey results tell a story of gaps between where companies currently stand and where they should be in relation to fundamental elements of IT security. Some progress has been made since our last survey, yet many organisations still fall short of important standard protocols for IT security and privacy," says Ryan Rubin, managing director with Protiviti and UK leader of the firm's IT security and privacy practice.

http://www.itproportal.com/2014/09/16/many-it-professionals-still-not-confident-of-preventing-a-cyber-attack

Main Goals for Today

- TCP Portscanning
- Detection of Portscanning

Refresh: 3-way handshake



Refresh: IP Address Space

- Different organizations get different amounts
  - Class A: x.0.0.0/8 (2^{24} = 16,777,216)
    - x.1.1.1 is in, as is x.254.254.254)
    - Huge org eg (DOD is 11.0.0.0/8 IBM is 9.0.0.0/8)
  - Class B: x.y.0.0/16 (2^{16} = 65536)
    - Mid-sized organization
      - eg Cornell has 128.253.0.0/16, 128.84.0.0/16, 132.236.0.0/16 and 140.251.0.0/16
  - Class C: x.y.z.0/24 (2^{8} = 256)
    - Small organizations.
  - Can also have intermediate bitmasks.
    - eg /22

Port Scan Scenarios

- Bad guy wants to map an address space
  - Old style: across the internet
    - Still happens for internet facing servers
    - But rarely can map entire networks any more
  - Newer style: has a compromised machine on an internal network
  - Wants to know “what servers are here?”
  - Specifically, which machines have open ports?

Class B Portscan Example

- 2^16 addresses
- Say bad guy just scans on port 80
  - Eg say he knows an IIS or Apache exploit.
  - Send out 2^{16} syn packets to port 80
    - x.y.0.0, x.y.0.1, x.y.0.2,… x.y.255.254
  - "Horizontal scan on port 80"
  - See who sends back a syn-ack.
    - Means they have a process answering on port 80.
  - Find all the web servers this way.
  - Attack em!
    - Start with sending an ack pkt to establish conn.
    - Or not – if we don't send the 3rd handshake, system typically won't log.
      - Half-open connection

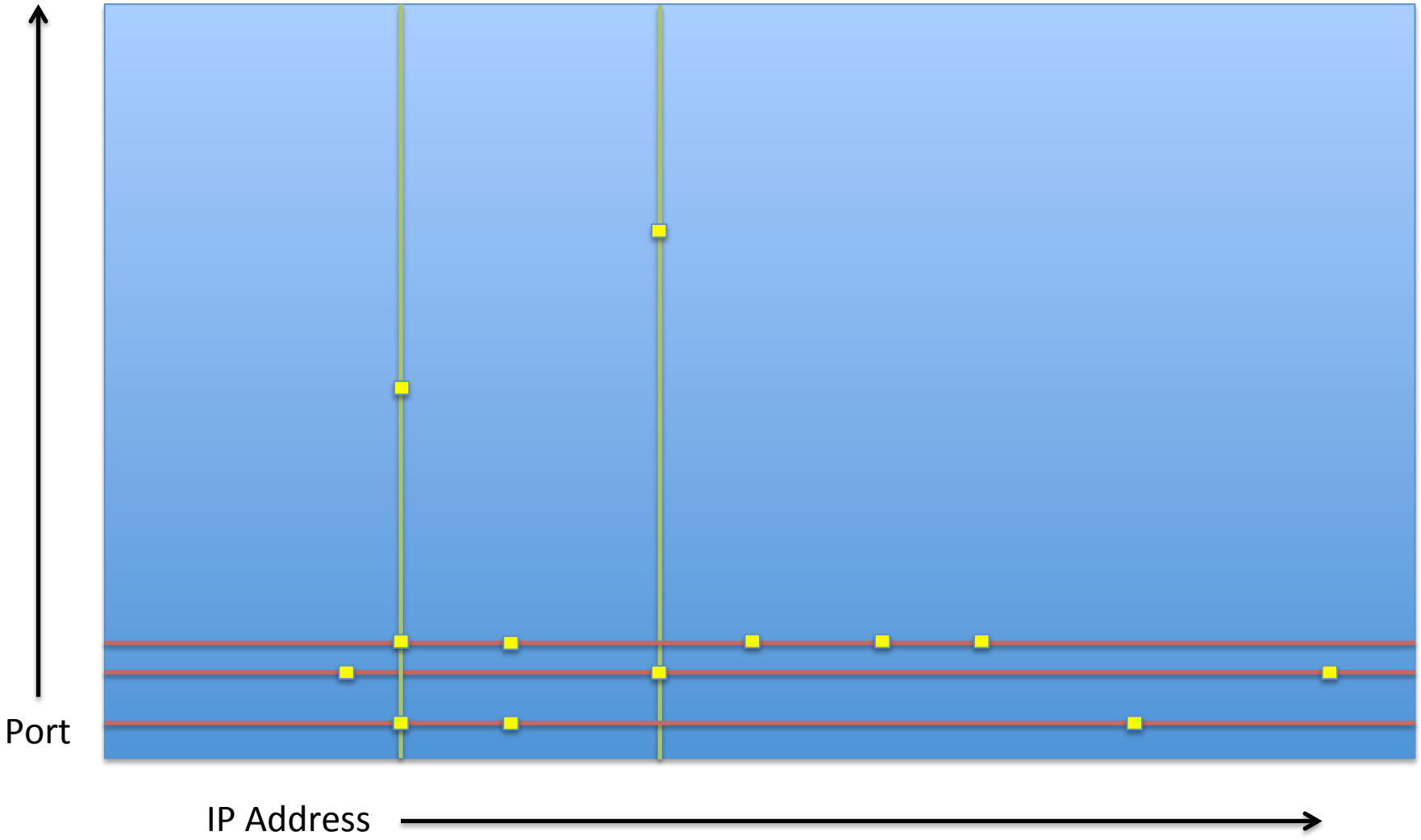
Vertical Port Scan of 1 IP

- Targetting a single IP address.
- Scan all 2^{16} ports.
- Find all ports answering

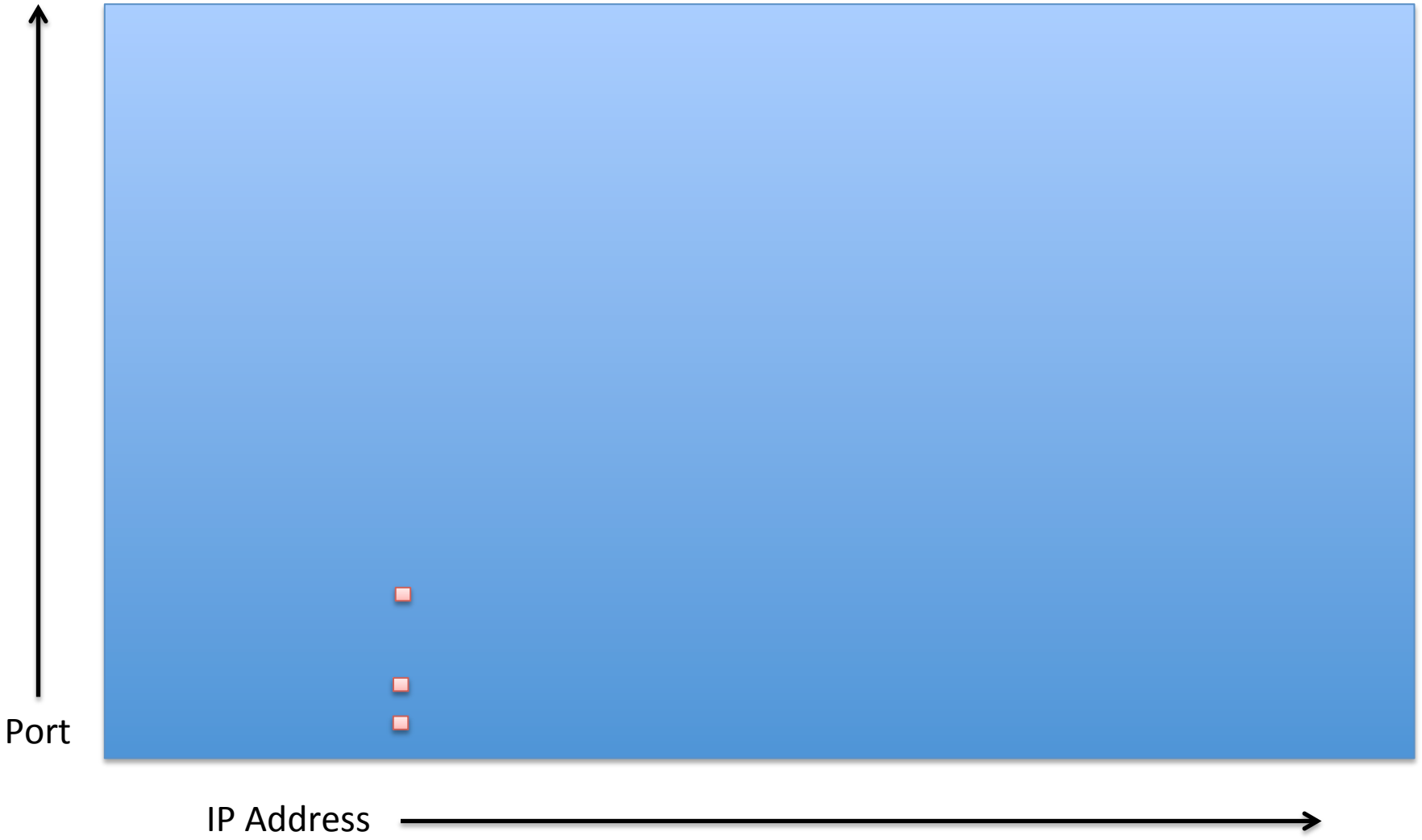
What Happens if Port Not Open

- No machine at all.
  - Typically get an ICMP response from a router
    - Special protocol for Internet error message packets
    - Saying no host at this address
- Machine but with closed port
  - Typically get a reset packet
  - Like a syn-ack, but with R set instead of S and A
  - Semantics – "stop this immediately"
- Security system (firewall)
  - Silence (depending on configuration)

Visualizing Scans



Small Piece of a Large Random Scan



Let’s try it

- sudo nmap -n –sS 10.0.0.2

What’s Happening on The Wire

- sudo tcpdump -n -i en3
- sudo nmap -n –sS 10.0.0.2

TCP Fin Flag

- Used to indicate orderly close of a connection.
  - Fin (F) 0x0x in TCP header flags field
- Either side may issue a packet with FIN in.
  - Can be a data packet.
- Other side should respond with a FIN pkt.
- Connection is then over and no more pkts should be sent.

FIN Scanning

`-sN`; `-sF`; `-sX` (TCP NULL, FIN, and Xmas scans)

These three scan types (even more are possible with the `--scanflags` option described in the next section) exploit a subtle loophole in the TCP RFC to differentiate between `open` and `closed` ports. Page 65 of RFC 793 says that "if the [destination] port state is CLOSED .... an incoming segment not containing a RST causes a RST to be sent in response." Then the next page discusses packets sent to open ports without the SYN, RST, or ACK bits set, stating that: "you are unlikely to get here, but if you do, drop the segment, and return."

When scanning systems compliant with this RFC text, any packet not containing SYN, RST, or ACK bits will result in a returned RST if the port is closed and no response at all if the port is open. As long as none of those three bits are included, any combination of the other three (FIN, PSH, and URG) are OK. Nmap exploits this with three scan types:

Null scan (`-sN`)

Does not set any bits (TCP flag header is 0)

FIN scan (`-sF`)

Sets just the TCP FIN bit.

Xmas scan (`-sX`)

Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.

Let's try these and compare

- tcpdump -n -i en0
- nmap -n –sS 10.0.0.2
- nmap -n –sF 10.0.0.2
- If time
  - nmap -n –sX 10.0.0.2
  - nmap -n –sN 10.0.0.2

What is Advantage

- Some early packet filters
  - Network access control devices
  - Would just examine syns to enforce policy
  - Eg if we want to block inbound email,
    - No syns to port 25.
  - Allow all non-syn pkts through
    - on the theory that end-host will not actually allow a connection with no syn.
  - But, end-host might respond to FIN scan, allowing attacker to portscan it through filter.

Let's look at everything nmap can do

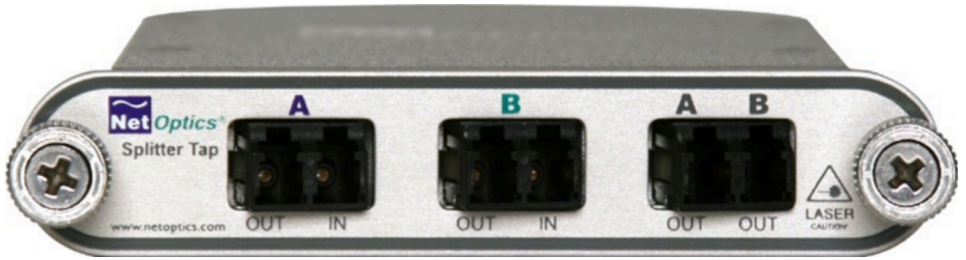
- Just for kicks
  - May not work, is slow/flaky at times
- sudo nmap -n –A –T4 10.0.0.2

Algorithms to Detect Portscans

- First brush with Network Intrusion Detection
  - General art/science of detecting badness by watching packets fly by.
  - Invented at UC Davis
    - Todd Heberlein et al circa 1989
    - "Network Security Monitor"
  - Portscan detection is a nice sample problem.
  - Illustrates many of the issues in an easy-to-follow context.

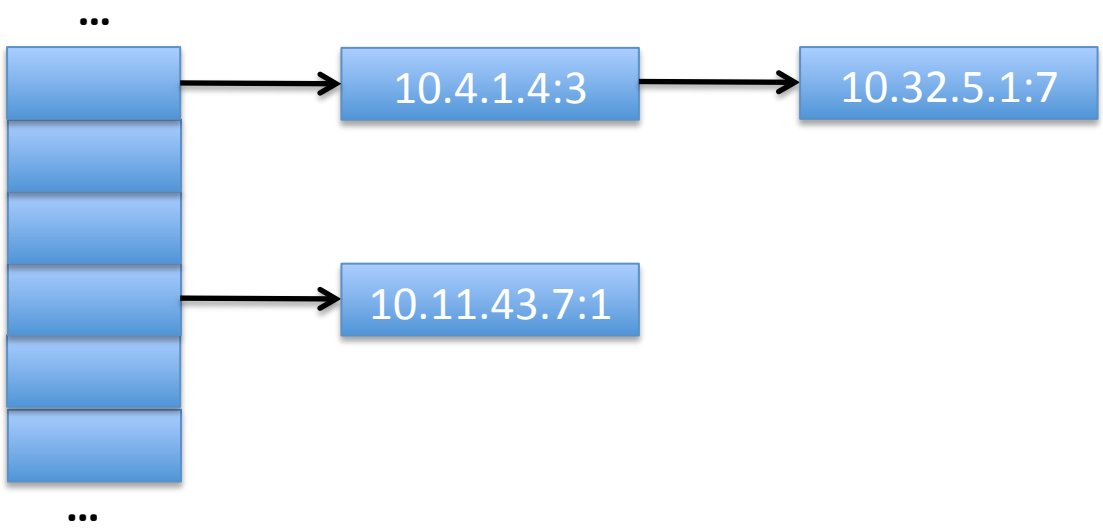
Firstly We Need to Get Packets

- Old
  - Promiscuously monitor a hub/wire
- Modern
  - Span port on switch
  - Network tap device
  - Detection device itself inline
    - IPS – Intrusion Prevention System
- For CS 5434 purposes, libpcap
  - 'man pcap' will get you started.



Then we need a data structure

- Simplest possible thing is a hash table
  - keyed on client IP
  - With per-connection counts of relevant stuff
  - Eg just count syns
  - Portscanners will issue more syns than average.
    - Alert when count goes over threshold
    - But what's likely to go wrong?



Another possibility

- Look for the actual sequential behavior
  - Syn->10.4.35.1
  - Syn->10.4.35.2
  - Syn->10.4.25.3
  - …
- Implement by having a “last dest” field in table entry
  - Keep counts of “number of increment-by-ones”
- Fragile
  - What could go wrong?