Network forensic
& ?

An ounce of prevention is worth a pound of detection

Forensics

- The art of gathering evidence during or after a crime
  - Reconstructing the criminal's actions
  - Providing evidence for prosecution
- Forensics for computer networks is ***extremely*** difficult and depends completely on the quality of information you maintain

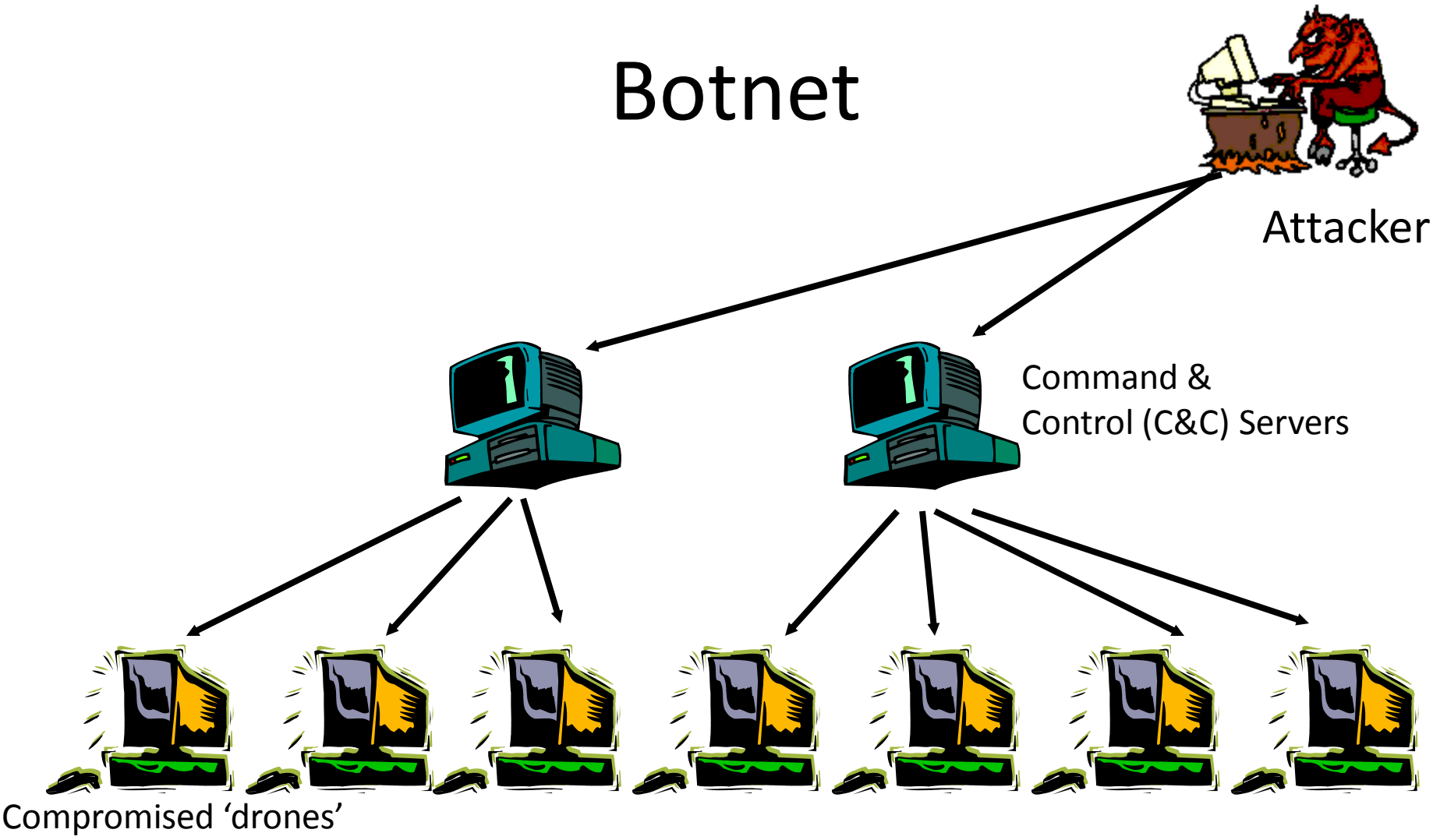
Network forensics

- What does it mean?
  - Network forensics is the analysis of network events in order to discover the source of problem incidents.

What sort of “problem incidents?”

- Aka “network badness”
- Lots of things – for this discussion, let’s talk primarily about botnets

Botnet



Types: agobot, forbot, gtbot, phatbot, rbot, rxbot, sdbot, phatbot, storm, etc, etc.

Creation of a botnet

- Scan & sploit
  - It still works
  - Many, many vulnerabilities and more every day
  - Scanning entire /8 takes approximately 32 hours
  - Bad neighbourhoods most popular – cable & DSL ranges – home users are less protected…how about that VPN connection?
  - Malware attached to emails (i.e. socially-engineered spreading)
  - Files transferred via Instant Messaging programs
  - Flaws in Internet Explorer, Firefox, and many, many others
  - Etc. etc. etc…attacks are against all platforms (NIX, Windows, XP/2000/98 etc, Mac OS), in many ways…not one is safe!

Botnet scan & sploit

sdbot


```
<@SourceX> .hello 72570478 n0d
<@PFool> you are now logged in!
<@SourceX> .scan 142.59.170.1
<@PFool> rpc scan started on 142.59.170.1 using universal offset 0x0100139d
<@PFool> Offset(0x0100139d)->VulnerableIP(142.59.170.11)
<@PFool> Offset(0x0100139d)->VulnerableIP(142.59.170.34)
<@PFool> Offset(0x0100139d)->VulnerableIP(142.59.170.36)
<@PFool> Offset(0x0100139d)->VulnerableIP(142.59.170.40)
<@PFool> Offset(0x0100139d)->VulnerableIP(142.59.170.67)
<@PFool> Offset(0x0100139d)->VulnerableIP(142.59.170.85)
<@PFool> Offset(0x0100139d)->VulnerableIP(142.59.170.101)
<@PFool> Offset(0x0100139d)->VulnerableIP(142.59.170.138)
<@PFool> Offset(0x0100139d)->VulnerableIP(142.59.170.205)
<@PFool> Offset(0x0100139d)->VulnerableIP(142.59.170.221)
<@PFool> Offset(0x0100139d)->VulnerableIP(142.59.170.225)
<@PFool> Offset(0x0100139d)->VulnerableIP(142.59.170.234)
<@PFool> Offset(0x0100139d)->VulnerableIP(142.59.170.252)
<@PFool> Offset(0x0100139d)->VulnerableIP(142.59.171.3)
<@PFool> Offset(0x0100139d)->VulnerableIP(142.59.171.18)
```

Creation of a botnet

- “phone home”, usually using DNS, sometimes a hard-coded IP
- Bots join a channel on the IRC server and wait to accept commands
- HTTP-based bots increasing – harder to detect
- P2P bots: Phatbot, Superbot, Storm
- Increasingly encrypted & obfuscated connections to C&C
- Distributed C&Cs – need for coordinated takedown

Preventative measures

- Social factor
  - How do you get users to stop clicking on bad attachments and protect against social engineering attacks?
- Administrative factor – how do you get admins to install and stay up-to-date with necessary patches?
- Engineering factor – how do you get software developers to write secure code?
- Criminal factor – how do you remove the motivation to commit on-line crime?

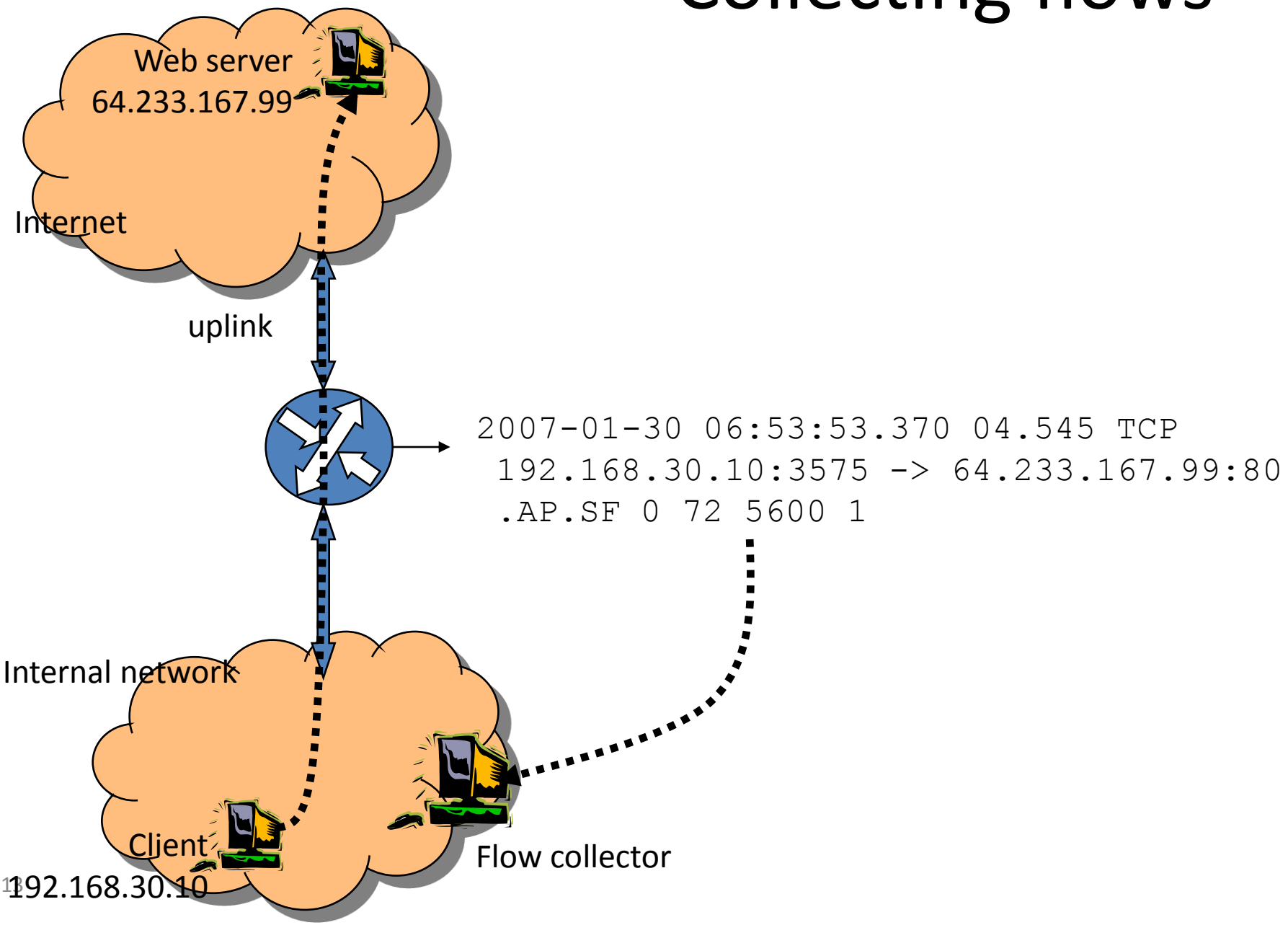
So for now…

- We need to make the bad guy's life more difficult
  - Objective: deter miscreants from committing online crime

Botnets – how do you find them?

- Watch flows
- Watch DNS
- Effectively use darknets
- Sniffing
- Sandboxing
- Malware analysis

Collecting flows



Collecting flows – enabling collection

A generic Cisco IOS configuration example:

```
interface fastethernet 0/0
ip route-cache flow
```

Set to netflow version 5 and set timeout:

```
ip flow-export <ip> <port>
ip flow-export version 5
```

Break-up long flows into 5 minute segments (should be less than your file rotation time):

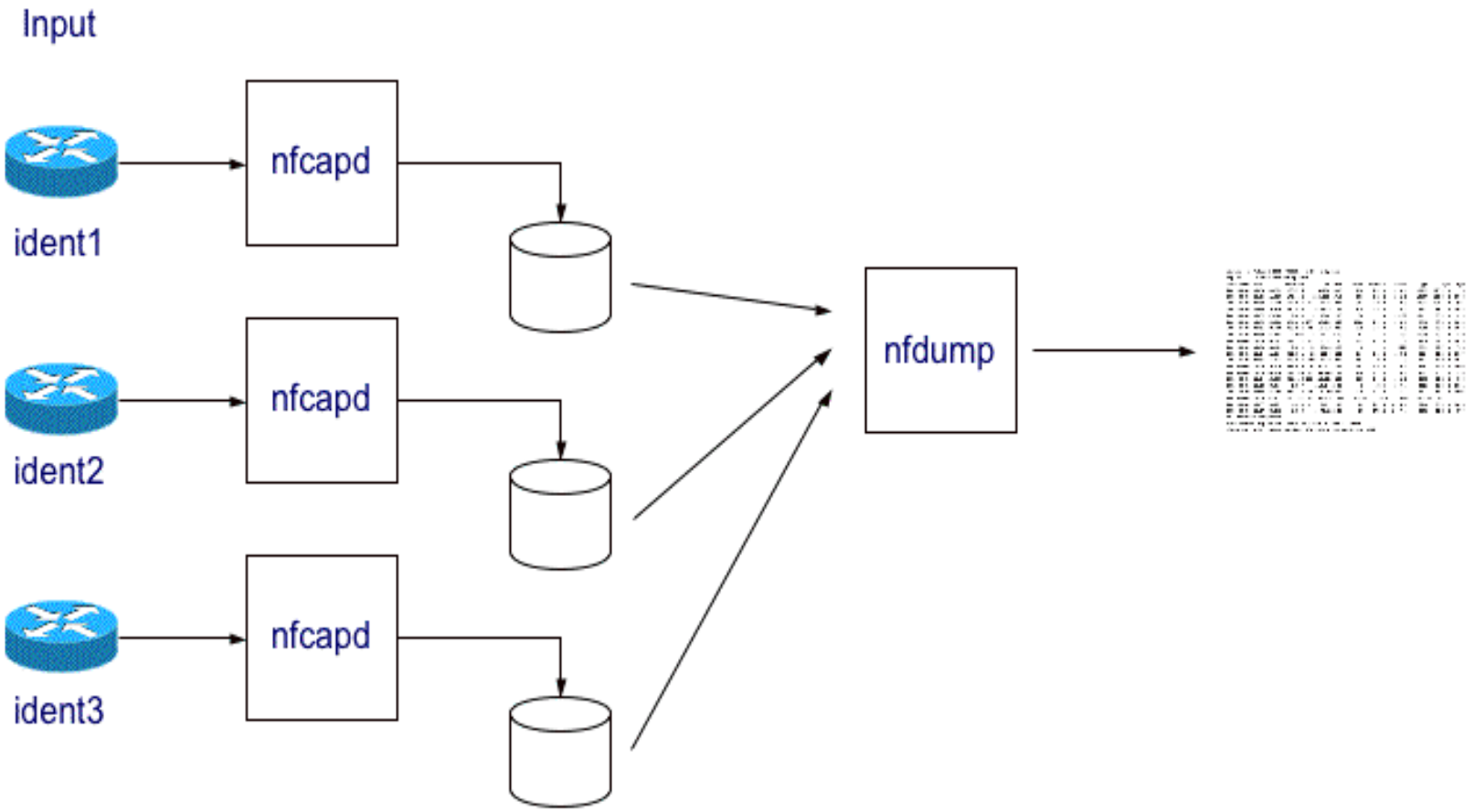
```
ip flow-cache timeout active 5
```

Collecting flows – enabling collection

- nfcapd
  - netflow capture daemon
  - Reads the netflow data from the network and stores the data into files. Automatically rotate files every n minutes. (typically ever 5 min)
  - nfcapd reads netflow v5, v7 and v9 flows transparently
  - You need one nfcapd process for each netflow stream

http://nfdump.sourceforge.net/

Nfcapd – principle of operation



http://nfdump.sourceforge.net/

Collecting flows – enabling collection

- nfcapd
  - Flow collector
  - Listens for flows on a given port and stores the data into files that are rotated a pre-set number of minutes
  - One nfcapd per flow stream
  - Example:

```
nfcapd -w -D -l /var/log/flows/router1 -p 23456
nfcapd -w -D -l /var/log/flows/router2 -p 23457
```

-w: sync file rotation with next 5 minute interval

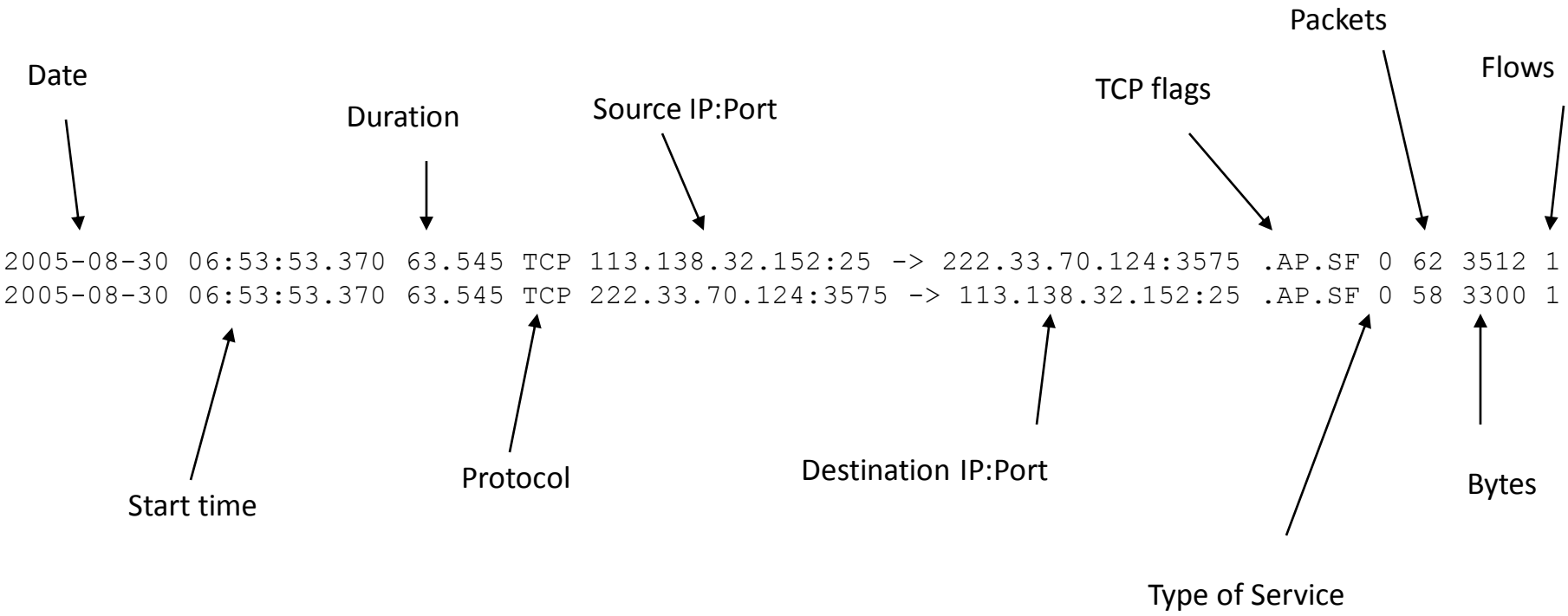
-D: fork to background

-l: location of log file

Watching flows

- nfdump
  - Reads the netflow data from the files stored by nfcapd
    - http://nfdump.sourceforge.net/
  - Its syntax is similar to tcpdump
    - Four different formats
    - Displays netflow data, staticstics of flows, IPaddresses, ports and etc.
    - Can be sorted in various ways

nfdump – long format



http://nfdump.sourceforge.net/

Nfdump – extended format

```
Packets Bytes   pps   bps   Bpp   Flows
1.4 M   2.0 G  2023 5.6 M 1498       1
```

Sort flows by total number of bytes

```
# nfdump -r nfcapd.200508300700
    -o extended -s srcip -s ip/flows
    -s dstport/pps/packets/bytes
    -s record/bytes
```

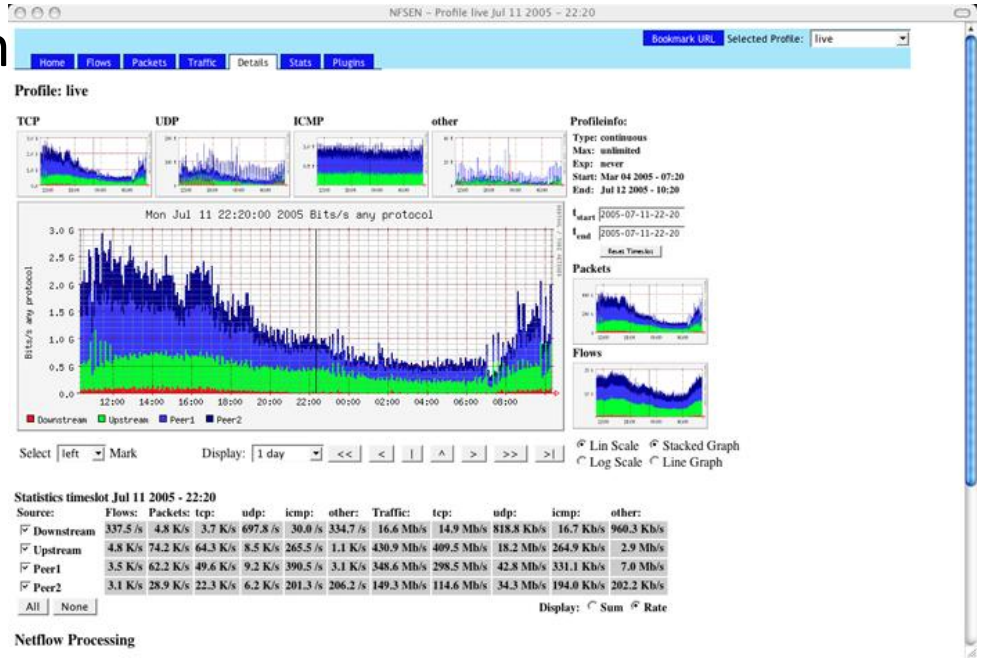
```
Top 10 flows ordered by bytes:
Date flow  Prot Src IP Addr:Port     Dst IP Addr:Port    Flags Tos Packets Bytes pps bps Bpp Flows
2005-08-30 TCP 126.52.54.27:47303 -> 42.90.25.218:435     ...... 0 1.4 M   2.0 G 2023 5.6 M 1498 1
2005-08-30 TCP 198.100.18.123:54945 -> 126.52.57.13:119   ...... 0 567732 795.1 M 627 2.5 M 1468 1
2005-08-30 TCP 126.52.57.13:45633 -> 91.127.227.206:119   ...... 0 321148 456.5 M 355 4.0 M 1490 1
2005-08-30 TCP 126.52.57.13:45598 -> 91.127.227.206:119   ...... 0 320710 455.9 M 354 4.0 M 1490 1
2005-08-30 TCP 126.52.57.13:45629 -> 91.127.227.206:119   ...... 0 317764 451.5 M 351 4.0 M 1489 1
2005-08-30 TCP 126.52.57.13:45634 -> 91.127.227.206:119   ...... 0 317611 451.2 M 351 4.0 M 1489 1
2005-08-30 TCP 126.52.57.13:45675 -> 91.127.227.206:119   ...... 0 317319 451.0 M 350 4.0 M 1490 1
2005-08-30 TCP 126.52.57.13:45619 -> 91.127.227.206:119   ...... 0 314199 446.5 M 347 3.9 M 1490 1
2005-08-30 TCP 126.52.54.35:59898 -> 132.94.115.59:2466   ...... 0 254717 362.4 M 322 3.7 M 1491 1
2005-08-30 TCP 126.52.54.35:59773 -> 55.107.224.187:11709 ...... 0 272710 348.5 M 301 3.1 M 1340 1
```

…the possibilities are endless…

http://nfdump.sourceforge.net/

Nfsen - watching flows

- Nfsen
  - NfSen is a graphical web based front end for the nfdump netflow tools.
    - http://nfsen



http://nfsen.sourceforge.net/

Watching flows

- By examining flows to/from known C&C servers, you'll identify machines compromised in your network and other networks.
  - it greatly helps to be a part of a trusted community that shares this sort of info
- Useful flow-related tools:
  - nfsen/nfdump (http://nfdump.sourceforge.net/)
  - fprobe (http://fprobe.sourceforge.net/)
  - SiLK (http://silktools.sourceforge.net/)
  - Stager (http://software.uninett.no/stager)
  - flow-tools (http://www.splintered.net/sw/flow-tools/)
  - InMon (www.inmon.com)
  - ntop (www.ntop.org)
  - Argus (http://www.qosient.com/argus/)

Watch DNS

- To find compromised devices and identify C&Cs
  - Known bad DNS names – very useful
  - DNS query logging is essential
- Short TTLs in a DNS A record are indicative of a C&C
  - TTLs are used to determine how long to cache the record before updating it
  - dnswatch/dig

```
# dig hackerdomain.com A
hackerdomain.com        60    IN    A    <ip address>
```

- Repetitive A queries – a bot?
- Repetitive MX queries – a spam bot?
- Know bad DNS names
  - It helps to be a part of a community that finds & shares known bad DNS names

Watching DNS

To find compromised devices & identify C&Cs

- known bad DNS names – *very useful*
- DNS query logging is essential

- short TTLs in a DNS A record are indicative of a C&C
  - TTLs are used to determine how long to cache the record before updating it
  - dnswatch/dig

```
# dig hackerdomain.com A
hackerdomain.com          60       IN       A        <ip address>
```

- Repetitive A queries - a bot?
- Repetitive MX queries - a spam bot?

- **known bad DNS names - it helps to be a part of a community that finds & shares known bad DNS names ...but more on that in a minute.**

Darknets

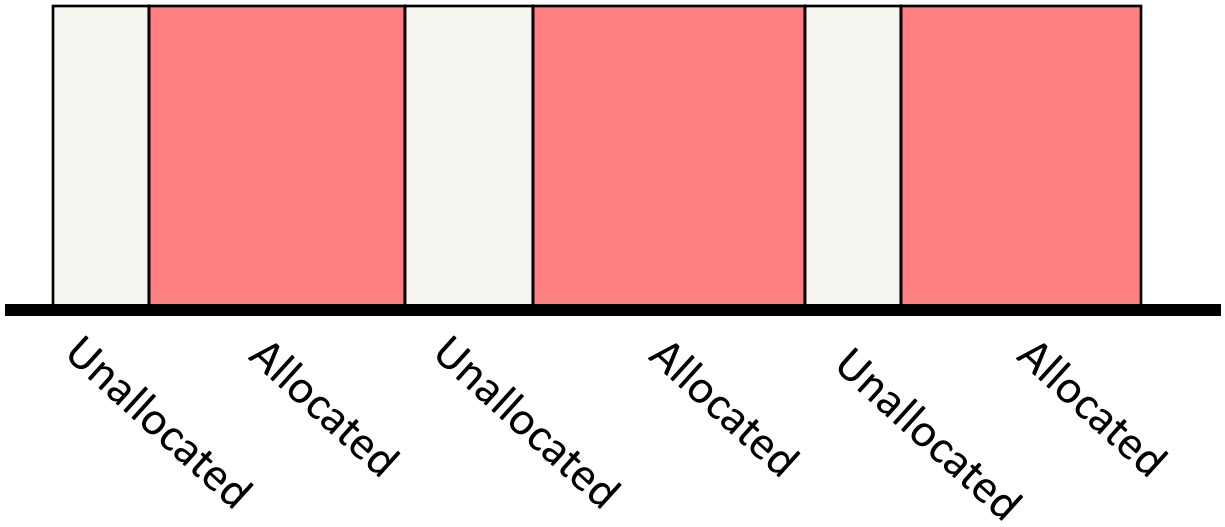
What is a Darknet?

- Routed, allocated IP space in which *(seemingly)* no active servers or services reside
- Any traffic that enters a Darknet is *aberrant*; little chance of false positives
- Can use flow collectors, sniffers and/or IDS boxes for further analysis
- Similar ideas: CAIDA *(Network Telescope)* and University of Michigan *(Internet Motion Sensor)*

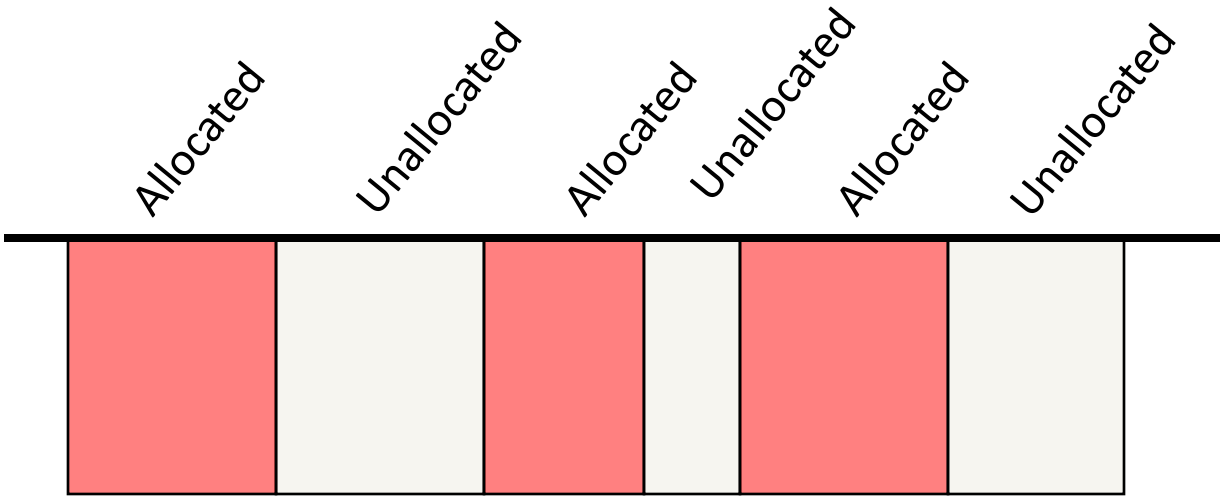
Darknets

Watch your Dark Space!

allocations of external IP space

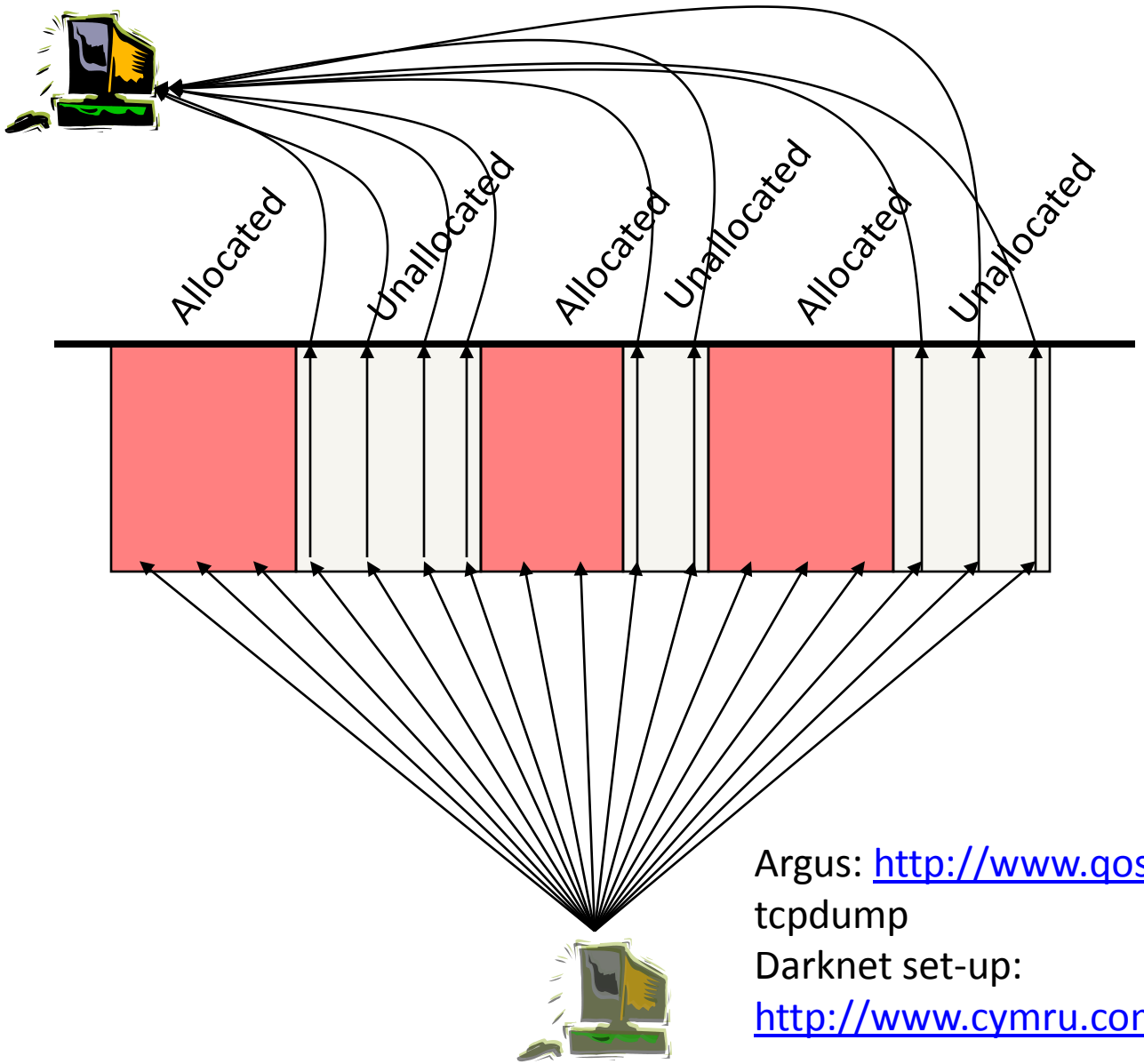


allocations of internal IP space



Darknets

Watch your Dark Space!



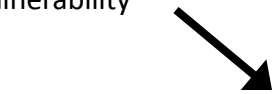
Argus: http://www.qosient.com/argus/
tcpdump
Darknet set-up:
http://www.cymru.com/Darknet/

Darknets

Watch your Dark Space!

ra – program to analyze Argus output (http://www.qosient.com/argus/ra.1.htm)

Looking for dameware vulnerability



Find connections characteristic of dameware:

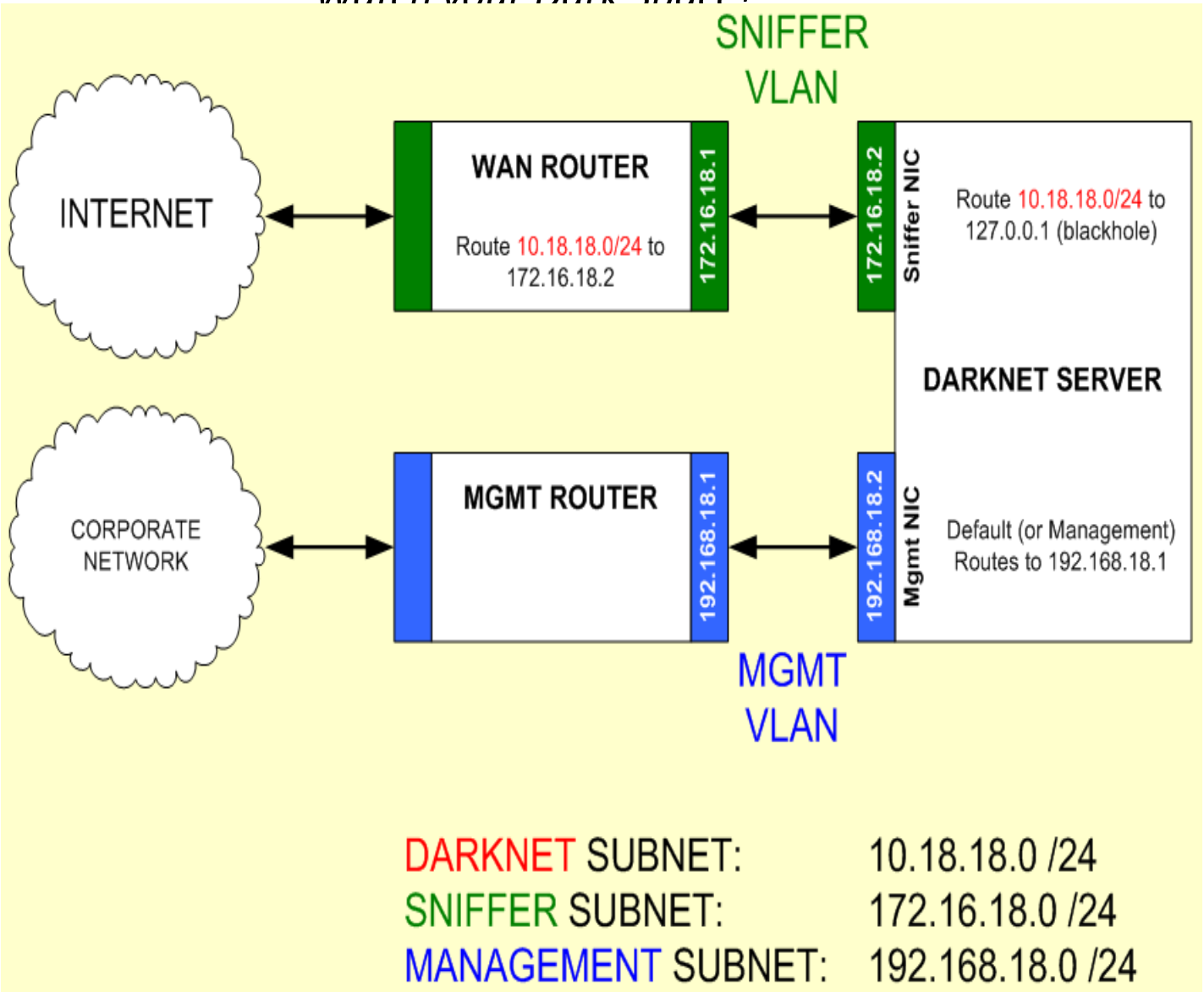
```
# ra -r ./argus.out.9 -n tcp and dst port 6129
22 Aug 06 07:24:28   tcp  82.50.1.222.2688   ->    xxx.yyy.210.32.6129  RST
22 Aug 06 07:24:28   tcp  82.50.1.222.2689   ->    xxx.yyy.210.33.6129  RST
22 Aug 06 07:24:28   tcp  82.50.1.222.2692   ->    xxx.yyy.210.34.6129  RST
22 Aug 06 07:24:28   tcp  82.50.1.222.2690   ->    xxx.yyy.210.35.6129  RST
22 Aug 06 07:24:28   tcp  82.50.1.222.2693   ->    xxx.yyy.210.36.6129  RST
22 Aug 06 07:24:28   tcp  82.50.1.222.2691   ->    xxx.yyy.210.37.6129  RST
22 Aug 06 07:24:28   tcp  82.50.1.222.2694   ->    xxx.yyy.210.38.6129  RST
22 Aug 06 07:24:28   tcp  82.50.1.222.2645   ->    xxx.yyy.210.39.6129  RST

# whois –h whois.cymru.com 82.50.1.222
[Querying whois.cymru.com]
[whois.cymru.com]
AS      | IP               | AS Name
3269    | 82.50.1.222      | ASN-IBSNAZ TELECOM ITALIA
```

CANINE: converts from Argus to netflow format. (http://security.ncsa.uiuc.edu/distribution/CanineDownLoad.html)

Darknets

Watch your Dark Space!



Darknets

Watch your Dark Space!

inward-facing AND outward-facing

If you ran a bank -- would you put security cameras inside your bank, in the parking lot, or both?

Darknets

inward-facing

- most malware scans the compromised host's /16 for vulnerabilities.
- allows you to identify hosts within your network that are scanning your local address space
- in other words, compromised hosts WITHIN your local address space.
- something you'd like to know about, right?

Darknets

inward-facing

- Unless you're conducting a pentest or vulnerability scan, you shouldn't see scans inside your own network.
- Things to watch for inside your network:
  - Attempted connections to ports associated with known vulnerabilities
  - Attempted connections to known malware "listening" ports
  - Any scanning activity.
  - …not to mention the obvious, but wherever this activity is originating from, you have a problem.

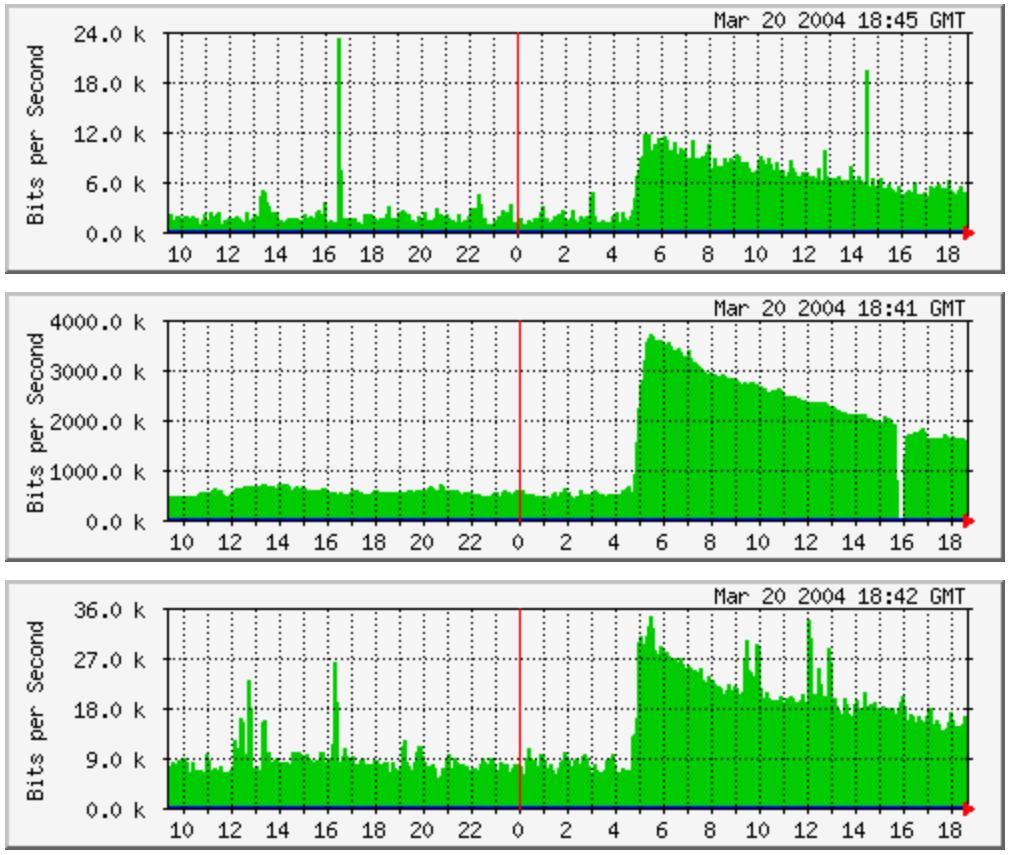
Darknets

outward-facing

3 different darknets. Spike at same time.
Indicative of spread of Witty Worm.

Witty Worm

- allows you to see who is scanning you
- who is trying to cause you pain?
- with what?
- Internet “garbage meter”

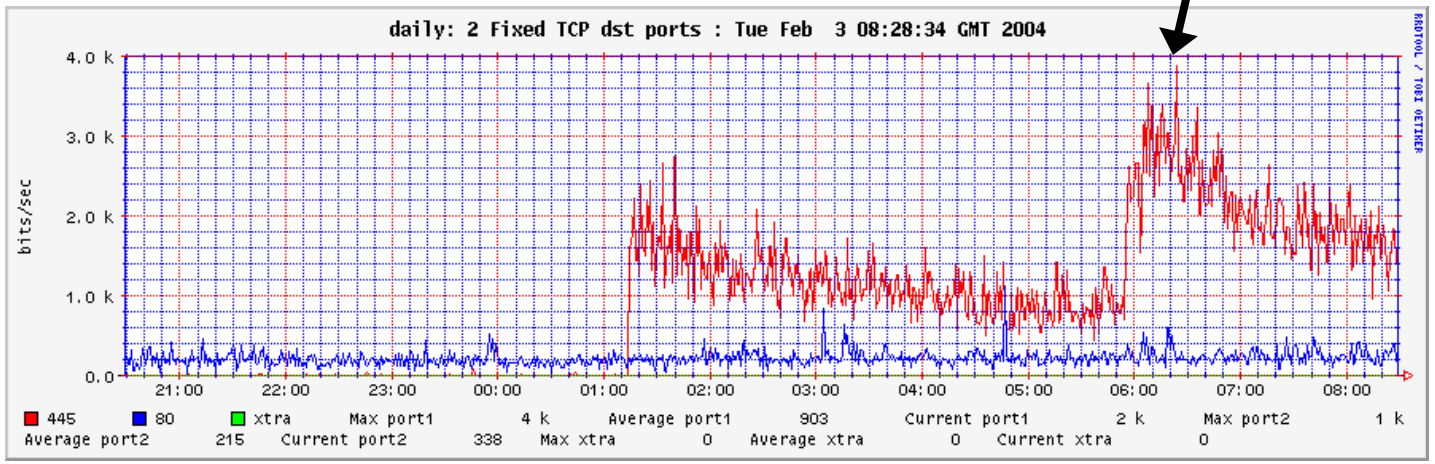


Darknets

outward-facing

Spike = port 445 scans. This was indicative of the first outbreak of the LSASS vulnerability

Signature Recognition
Dest TCP/445 = Scanning for Win2K Open Shares
Dest UDP/1434 and size 404 bytes = Slammer Scans



New malware – catch it in beta!

Sandboxing

- run malware in a virtual environment to determine actions
  - what domain name does the malware look-up, or what IP does it try to connect to?
  - Identify modified files, registry entries, and other changes to the system
  - Identify patterns of network activity – which can then be applied to the darknets & flow collectors to identify this malware.
  - Identify new trends in malware development – see where the miscreants are headed!
  - http://www.cwsandbox.org/, Norman (http://sandbox.norman.no/)

- to make this work, also need to collect malware
  - http://nepenthes.mwcollect.org/

- some malware detects some sandboxing environments and will cease execution

- economies of scale
  - he with the biggest collection has the best security
  - or, he with the best community has the best security
  - …but more on that in a minute.

Watch Network Traffic

- sniff network traffic for common botnet commands & return traffic.
- In capture files can look for patterns in data

SDBot: `advscan|asc [port|method] [threads] [delay] [minutes]`
Agobot: `cvar.set spam_aol_channel [channel]`

```
000 : 50 52 49 56 4D 53 47 20 23 6D 65 73 73 61 67 65 PRIVMSG #message
010 : 73 23 20 3A 5B 6C 73 61 73 73 5F 34 34 35 5D 3A s# :[lsass_445]:
020 : 20 45 78 70 6C 6F 69 74 69 6E 67 20 49 50 3A 20 Exploiting IP:
030 : 31 39 32 2E 31 36 38 2E 34 2E 32 32 39 2E 0D 0A 192.168.4.229...
```

List of AgoBot, SDBot, & UrXBot commands:
http://www.honeynet.org/papers/bots/botnet-commands.html

Watch Network Traffic

- Use snort signatures to identify common bot C&C traffic

```
alert tcp any any -> any 6667
(msg:"IRC BOT 1 - lsass";
 flow:to_server,established;
 content:"lsass";
 nocase:; classtype:bad-unknown; sid:3011381; ev:1;)
```

http://www.bleedingsnort.com/
http://www.giac.org/practicals/GSEC/Chris_Hanna_GSEC.pdf

- Increasing trend in encrypted IRC channels for C&Cs, which makes either of these techniques problematic

Malware Analysis

- also works, but:

```
.text:004014D1    push    0                ; hTemplateFile
.text:004014D3    push    80h              ; dwFlagsAndAttributes
.text:004014D8    push    3                ; dwCreationDisposition
.text:004014DA    push    0                ; lpSecurityAttributes
.text:004014DC    push    1                ; dwShareMode
.text:004014DE    push    80000000h        ; dwDesiredAccess
.text:004014E3    mov     eax, [ebp+arg_4]
.text:004014E6    push    dword ptr [eax] ; lpFileName
.text:004014E8    call    CreateFileA
.text:004014ED    mov     edi, eax
```

- miscreant countermeasures (packing, etc) can make this especially difficult
- Wouldn't you rather analyze flows or tump ? :-)

Collaboration

- If your organization is doing these:
  1) watching flows to identify C&Cs
  2) discovering rogue domain names
  3) using Darknets to identify compromised devices
  4) sandboxing to analyze malware
  5) sniffing traffic to find bots
  6) doing malware analysis

- Then you produce these:
  - C&C IPs & domain names (within and **outside** your network)
  - IPs of compromised devices (within and **outside** your network)

We highly suggest collaborating with your communities of choice to share the above information!

Useful Network components
or
Desining your network for

How do I connect to sniffing/monitoring solution to the Network?

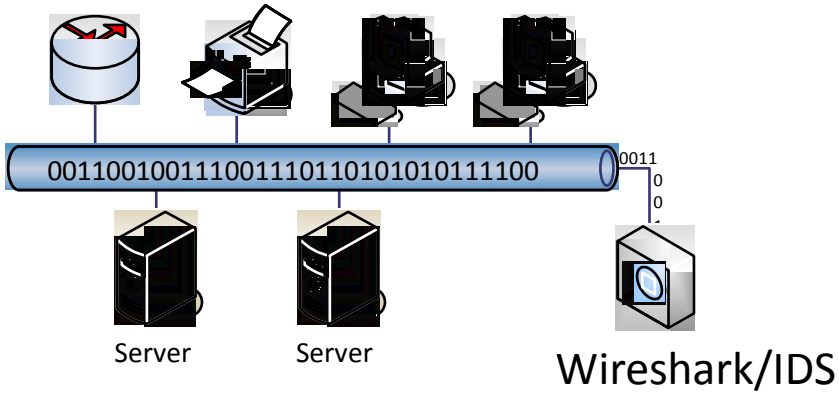
- 10/100 Hub
- SPAN or Mirrored Ports (switches)
- TAP – Traffic Access Point

It's simple, I need access to the data!

How do I connect to sniffing solution to the Network?

- 10/100 Ethernet Hub
- Shared 10/100 collision based topology
- Cannot monitor full duplex traffic
- Drop Packets
- Does not support gigabit or fiber applications
- Hard find a hub
- Single port makes it easy when using with a laptop or portable application with sniffing solution

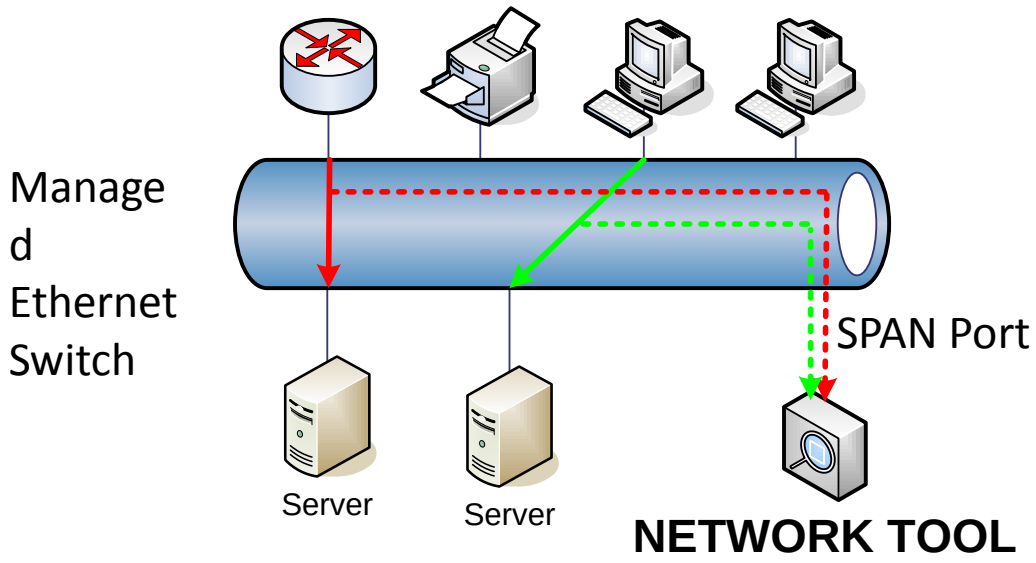
SHARED ETHERNET 10/100MB TOPOLOGY



How do I connect to sniffing solution to the Network?

Mirrored Port or Cisco Term SPAN (**S**witch **P**ort **An**alyzer)

- With SPAN, traffic from any port on the network switch can be mirrored or copied to another port, which is designated as the SPAN port. You can then connect the SPAN port to the Network Tool



Connect to designated SPAN or Mirrored Port
to get a copy of the traffic between the two network devices

SPAN/Mirrored Switch Port

Benefits

- Included in the cost of your managed switch
- Internal Switch Traffic Visible
- VLAN's are visible
- Single port makes it easy when using with a laptop or portable application with Sniffer

Limitations

- Groomed data (change timing, add delay)
- Extract bad frames as well as ignore all Layer 1 &2 information
- Dropped frames: Monitoring device is missing packets due to port over-subscription
- Full Duplex monitoring is not supported
- Not secure and transporting monitored traffic through the production network may not acceptable
- Not Priority
- Degraded network switch performance when monitoring a busy segment
- Contention for SPAN Ports
  - Engineers, Security, VoIP, etc
  - *I have no SPAN Ports Available*
- Requires re-configuration of the network switch
  - Authorization Problems
  - Switch Configuration Errors can cause major Network Problems

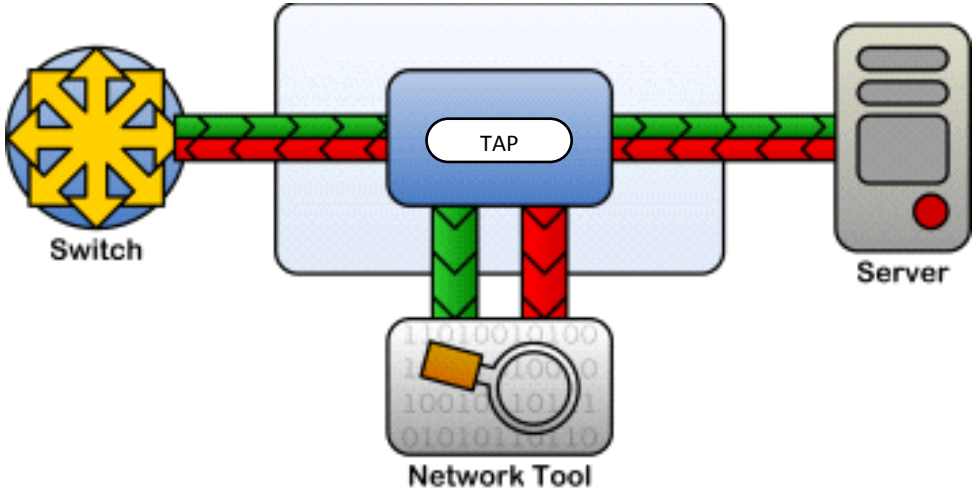
SPAN/Mirrored Switch Port

- **Data Monitoring Access: SPAN Port or Passive TAP? What's on your Network?**
- **Part 1**
- **Is SPAN port a viable data access technology for today's business critical networks especially with today's access needs for Data Security Compliance and Lawful Intercept requirements?**
- **Not really, see why !**
- **by Tim O'Neill from BT Solutions**
- From Cisco' on SPAN port usability –From Cisco's White Paper – Using the Cisco Span port for SAN analysis
- "Cisco warns that the switch treats SPAN data with a lower priority than regular port-to-port data. In other words, if any resource under load must choose between passing normal traffic and SPAN data, the SPAN loses and the mirrored frames are arbitrarily discarded. This rule applies to preserving network traffic in any situation. For instance, when transporting remote SPAN traffic through an Inter Switch Link (ISL) which shares the ISL bandwidth with regular network traffic, the network traffic takes priority. If there is not enough capacity for the remote SPAN traffic, the switch drops it.
- Knowing that the SPAN port arbitrarily drops traffic under specific load conditions, what strategy should users adopt so as not to miss frames? According to Cisco, the best strategy is to make decisions based on the traffic levels of the configuration and when in doubt to use the SPAN port only for relatively low-throughput situations. "

- **Read the entire article by accessing**
- **http://www.lovemytool.com/blog/2007/08/span-ports-or-t.html**

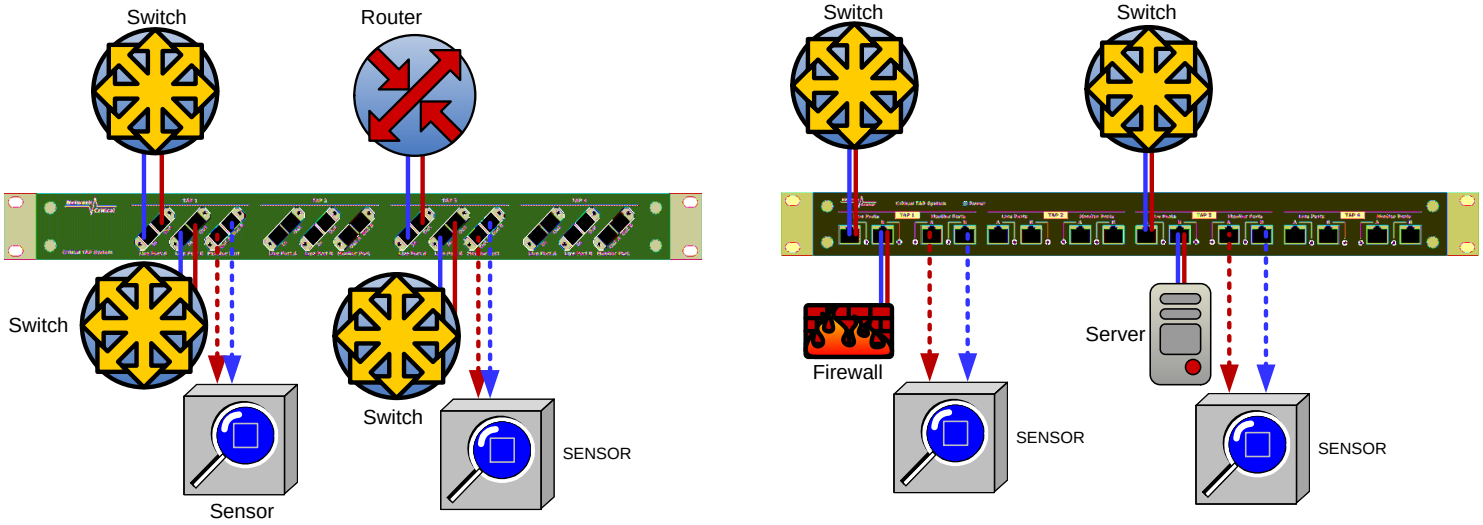
How do I connect to sniffing solution to the Network?

- **Traffic Access Port (TAP)**
  - Provides a copy of the traffic flowing between two (2) Network Devices
  - Fail Safe Technology - 100% Network Availability even in an event of power loss
  - 100 % Visibility of the Full Duplex Network Traffic including Layer 1 & Layer 2 Errors
  - Sensor are 100% Isolated & Secure
  - TAPs are a layer 1 device – Easy to install & Manage
  - Creates a Permanent Access Point for Network Tools



TAP Benefits

- Provide Easy Network Access (hardware only solution)
- Eliminates the need for SPAN / Mirrored Ports
- Permanent 24/7/365 Access
- 10/100/1000 Copper, Fiber 100Base-FX, OC3 – OC192, Gigabit, 10 Gigabit, Fiber to Copper Gigabit TAPs



TAP Benefits

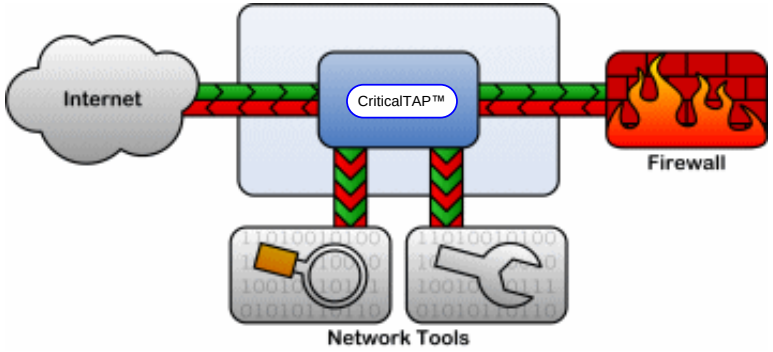
- Simple Layer 1 Passive Hardware Device
- Easy to Install
- Provides Permanent Access
- 100% Network Availability
  - No Single Point of Failure
- 100% Visibility to Network Traffic
- Eliminate the need for a SPAN Port
- Cost effective
- Save $$$$, No Network Downtime

Make your life easier when deploying & managing Sniffer

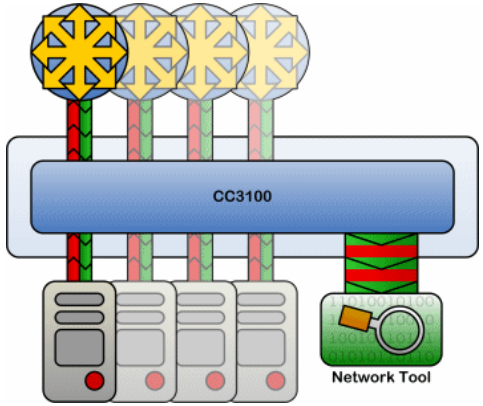
Tapping Technology

Many-to-One or One-to-Many TAPs

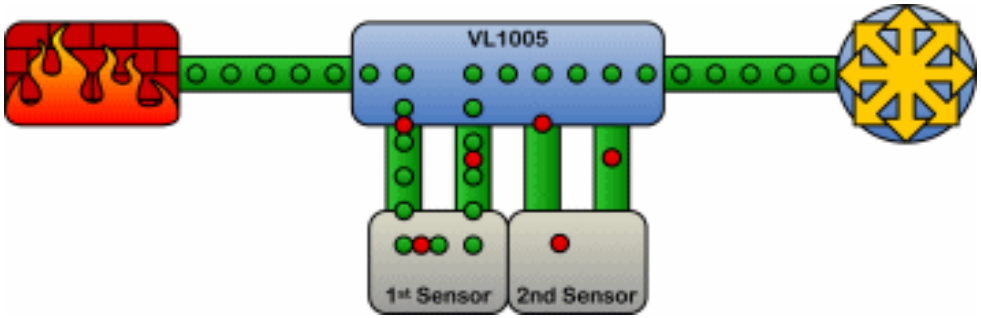
Aggregating TAP



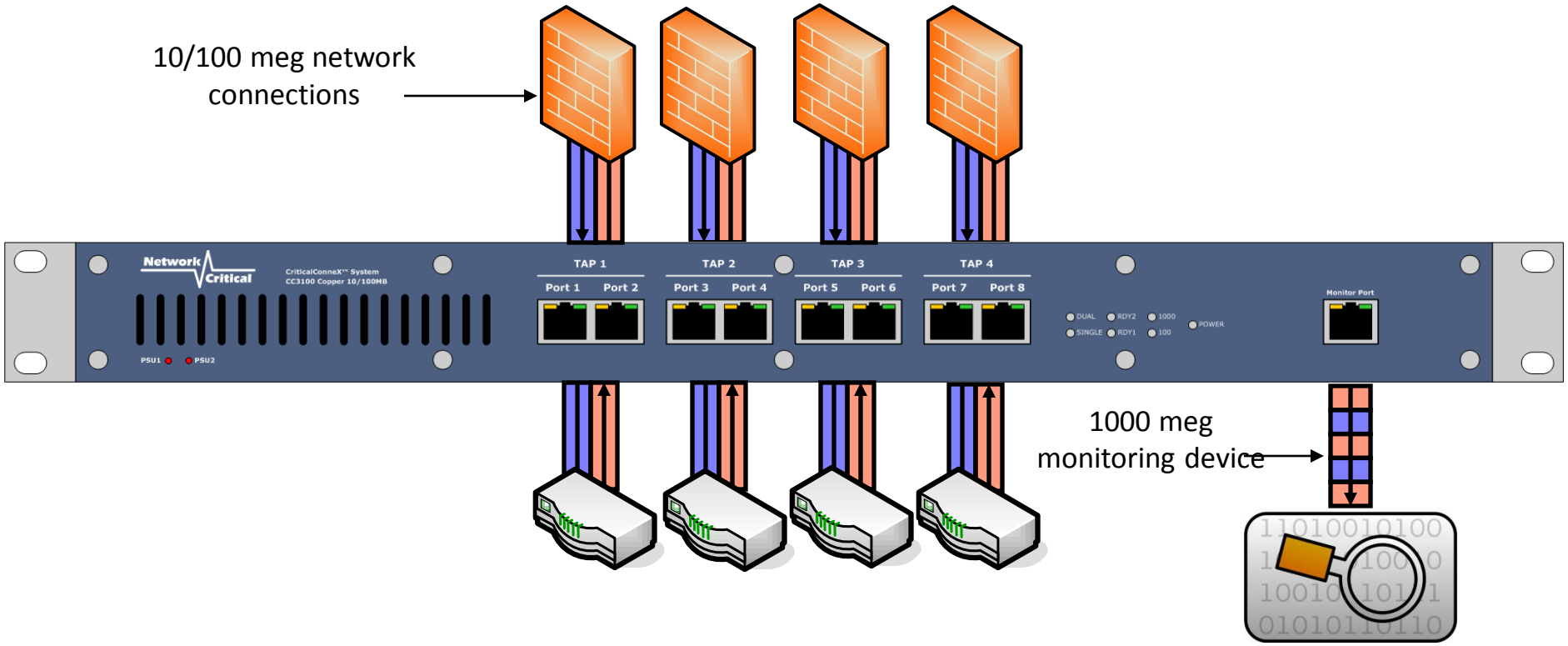
Aggregation or Regeneration

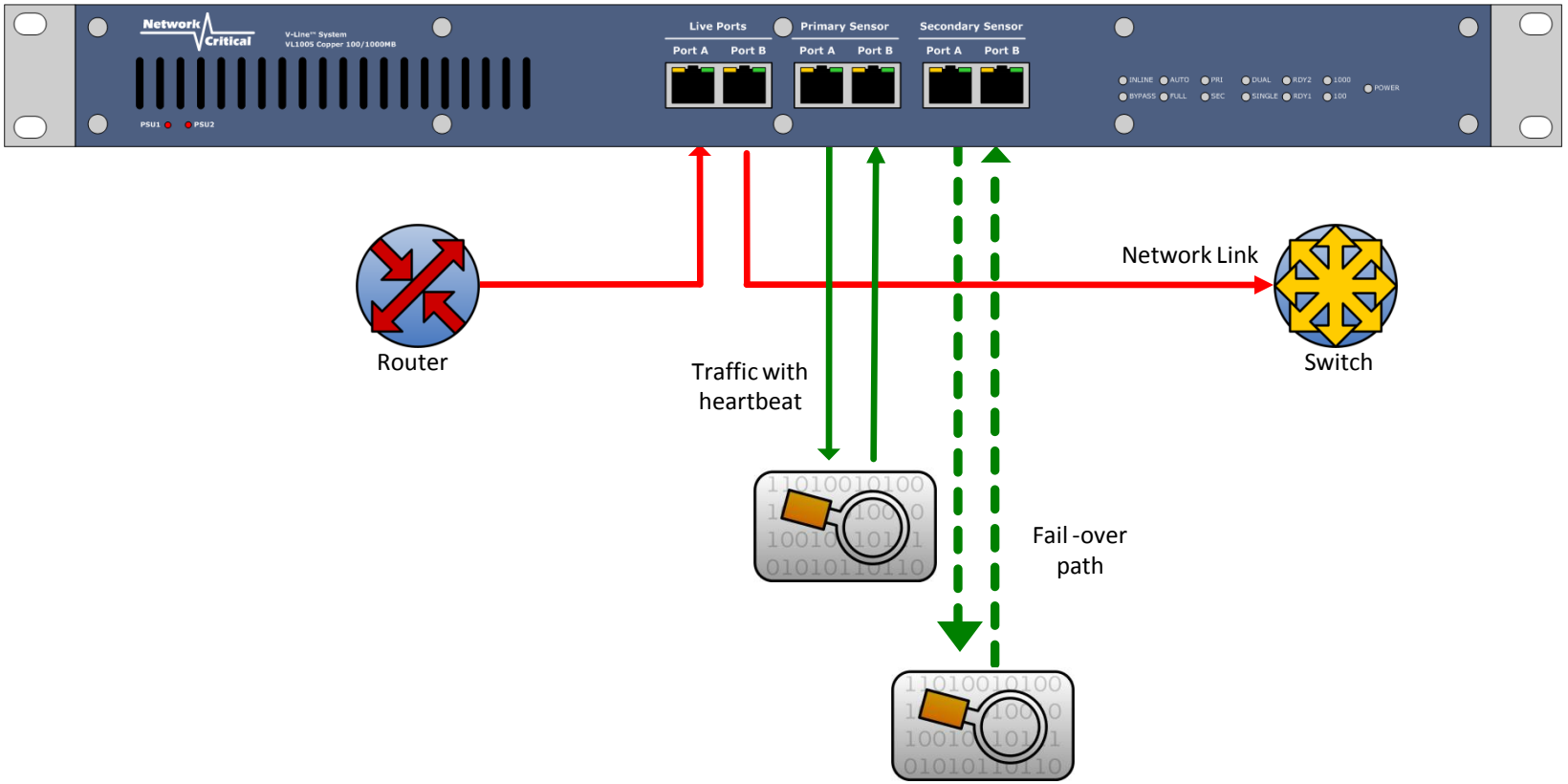


V-Line (Virtually In-Line) By-pass TAPs



Aggregation / Many-to-One / One-to-Many




Network Critical
V-Line™ System
VL1005 Copper 100/1000MB
PSU1
PSU2
Live Ports
Port A
Port B
Primary Sensor
Port A
Port B
Secondary Sensor
Port A
Port B
INLINE
BYPASS
AUTO
FULL
PRI
SEC
DUAL
SINGLE
RDY2
RDY1
1000
100
POWER
Router
Network Link
Switch
Traffic with heartbeat
Fail -over path

TAP Your Network for sniffing/ monitoring solution

- Easily connect your sniffing solution Analyzer
  - 10/100/1000 Copper
  - Multi-mode Gigabit Fiber
  - Single Mode Gigabit Fiber
  - Provide a single copper monitoring port for laptops & single port mobile devices
  - Install & Monitor

Network Design

- What about it ?
- Where to put TAP ?