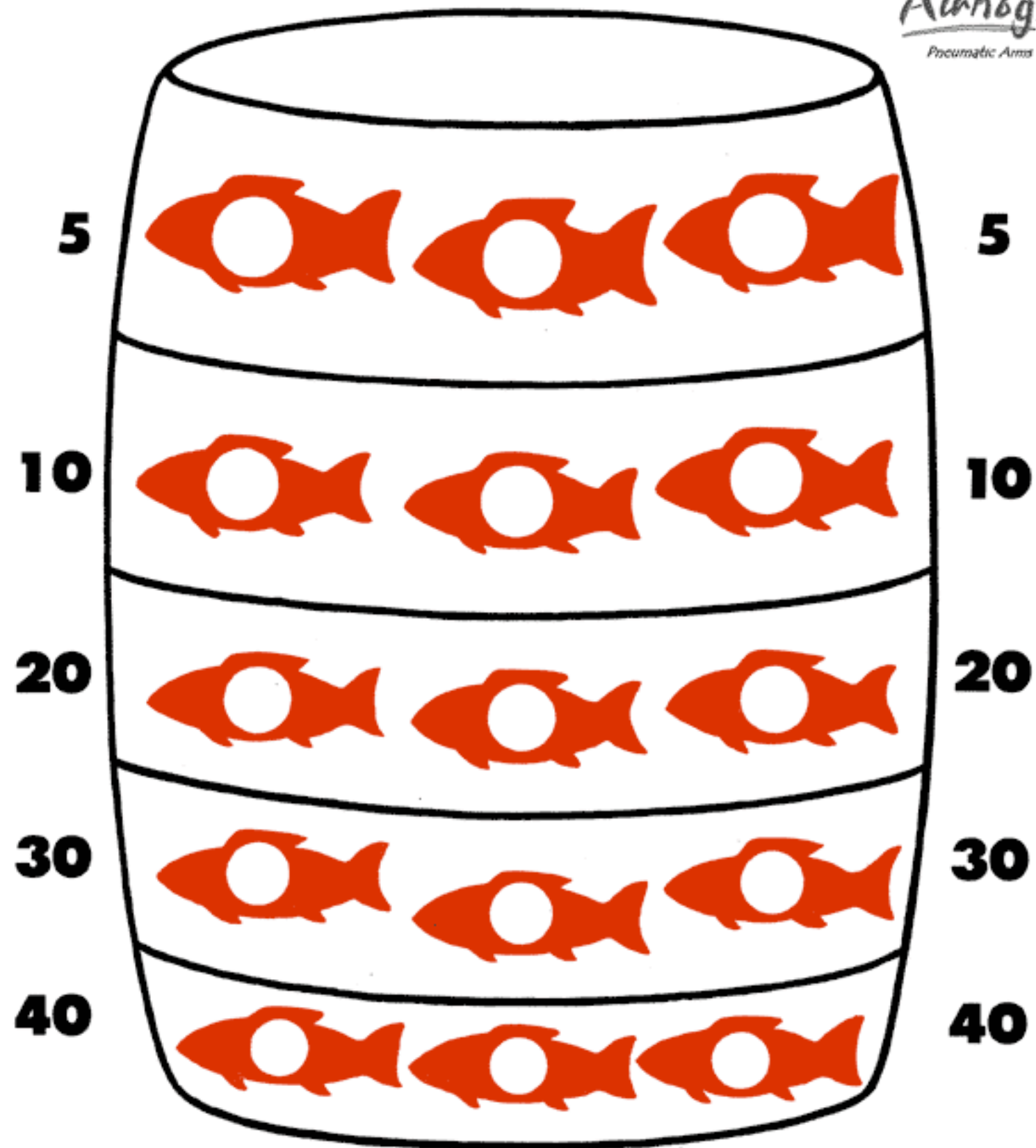


Surprise!

*Randy Bush, Bill Fenner, Rob Thomas,
Russ Housley, Steve Bellovin, Jose Nazario*

FISH IN A BARREL

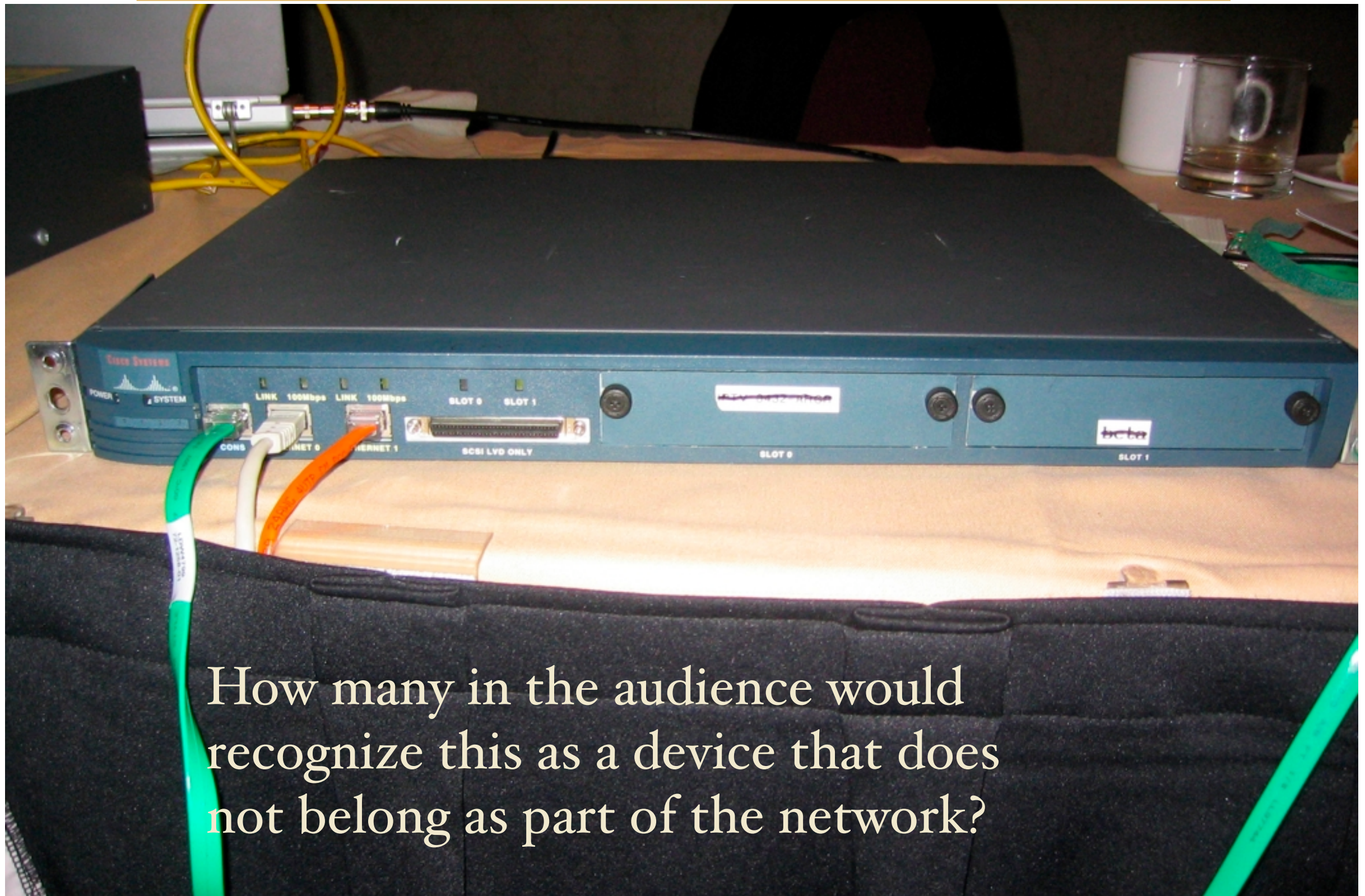
Presented
by
Airhog
Pneumatic Arms



What?

- Sniffing the network
 - Capturing passwords, URLs, email messages, some IM traffic.

How?



How many in the audience would recognize this as a device that does not belong as part of the network?

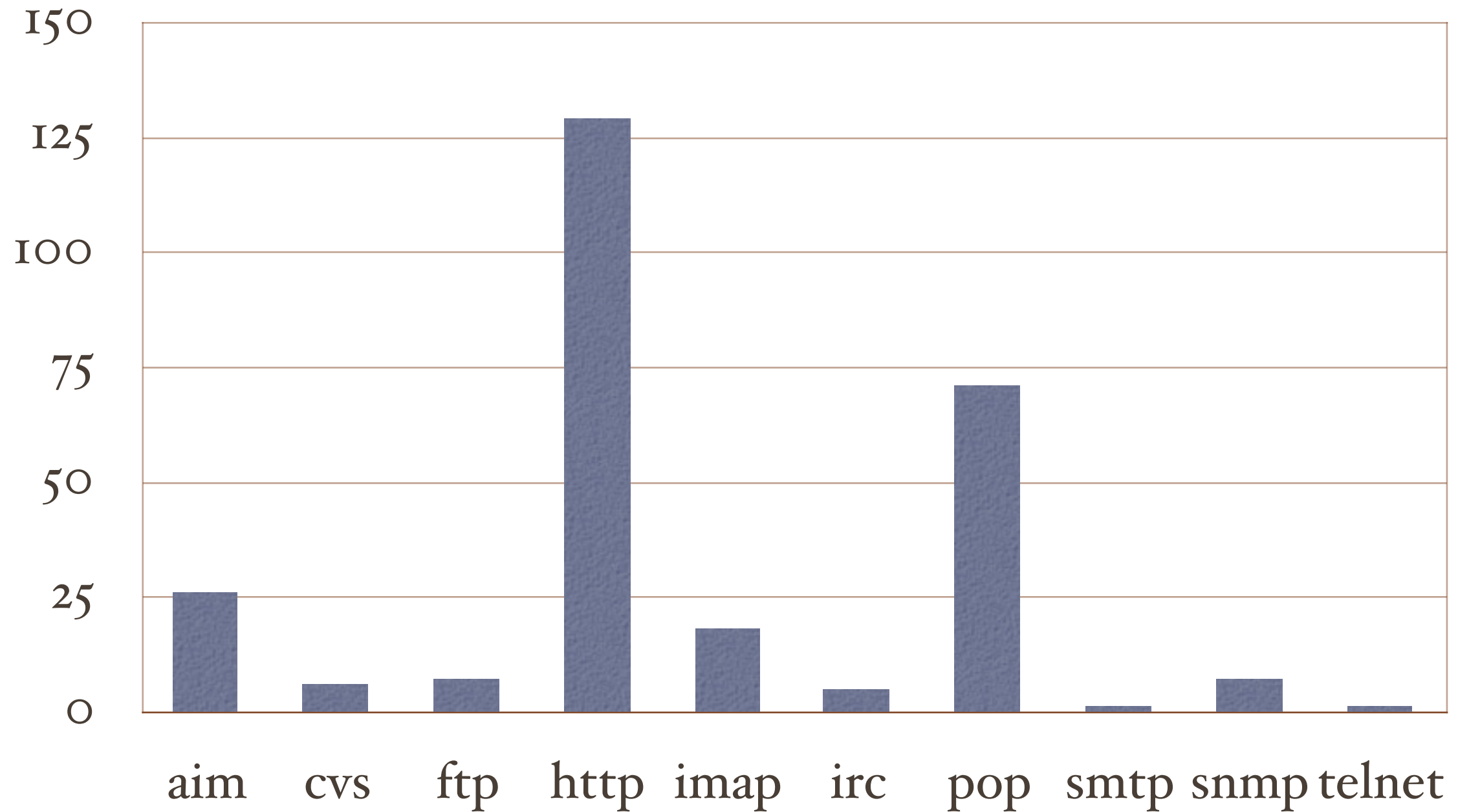
How did we get the traffic?

- SPAN switch port, set to monitor all traffic.

That's cheating!

- Some say that monitoring the wired network this way isn't fair, since only the wireless is sniffable.
- Black hats have their own ways to cheat:
 - CLUS: run ettercap
 - Physically insert sniffer at uplink to main switch

How many?



What else?

- 2341 email messages
- 264,820 web URLs

Plaintext passwords seen at NANOG 22 (May 2001)

«passwords deleted for
web presentation»

Password List

«passwords deleted for
web presentation»

Password for account “fenner”:

■ «deleted»

Most-seen passwords

«passwords deleted for
web presentation»

What about that telnet?

(IP addresses and user name edited)

10/21/03 15:13:12 tcp xx.xx.xx.xx.4013 -> xx.xx.xx.xx.23 (telnet)
cico

joeisuzu

cisco

en

«deleted»

Things sent through email

- POP password “«deleted»”
 - Twice in 2 different messages...
- Password “«deleted»”
 - In 5 different messages...
- Someone's cisco config with “encrypted” passwords:
 - «deleted»
 - «deleted»
- What was your server name? I also don't have the username password. Don't send it over the net. I am at a conference of network operators and I'm sure someone is sniffing the network.

Webalizer Results

User Agents

63561 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
40801 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1
22468 Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en-us) AppleWebKit/8
21010 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
11813 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.5) Gecko
6826 Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.4) Gecko
6053 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; .NET CLR 1
4873 Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)
4587 Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en) AppleWebKit/103u
4383 Mozilla/5.0 (Macintosh; U; PPC Mac OS X; en-us) AppleWebKit/1
4303 Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.4) Gecko
3927 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; T312461)
3500 Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1) Opera 7.11
3394 Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US; rv:1.5a) Geck
3361 Mozilla/4.0 (compatible; MSIE 5.22; Mac_PowerPC)
3157 Mozilla/5.0 (X11; U; Linux i386; en-US; rv:1.5b) Gecko/200309

More Webalizer Results

Search Strings

20	bruce sterling
8	802.16
8	fiber ethernet converter
6	cost of living
6	junko
6	multicast flooding IGMP
6	nanog
6	xioop
5	Ron Of Japan Inc Chicago IL
5	rancid
5	team cymru
4	OSPF multipath routing
4	Parking at Gatwick
4	airo: max tries
4	cisco intellectual property
4	default argument given
4	export LD_LIBRARY_PATH

Referrers

6893	http://www.cnn.com/
4122	http://cgi.ebay.com/ws/eBayISAPI.dll
3828	http://www.shacknews.com/ja.zz
3381	http://www.nanog.org/mtg-0310/agenda.html
2887	http://news.google.com/
2787	http://www.nanog.org/
2785	http://www.usatoday.com/money/front.htm
2258	http://www.google.com/search
1704	http://search.ebay.com/search/search.dll