Lessons From Stuxnet

Bill Cheswick

http://www.cheswick.com/ches/talks/

Introduction

- New worm discovered in the wild in 2010
- Sophisticated, elaborate, mostly benign
- Named by one of the worm analysts
- Reports of trouble in the Iranian nuclear program
- No one has claimed credit for the attacks
  - see below

Some details

- **Analysis showed use of four unknown day 0 exploits in Windows (since repaired)**
- **Compromised certificates allowed silent installation of kernel modules**
  - **new MD5 collision code in the worm**
    - unknown crypto

Will you ever face a nation/state level of attack?

- **ehg at Google**

This talk

- **What does a sophisticated attack look like?**
  - **(answer, not much, usually.)**
- **What are the goals?**
- **What tools are used?**
- **How might one detect such attacks, as a defender?**

“Security people are paid to think bad thoughts”

- Bob Morris

Disclaimer

I have never mounted a sophisticated cyber attack, nor have I been cleared for official training in the subject.

The speculations here come from twenty five years of evil thoughts and pondering offensive cyber activities.

Some speculations have been confirmed, off the record, sometimes by strangers.

Offensive cyberwar and me

- **Hackers Workbench**
  - **Unix-style filters for the wily hacker**
- **Anonymous packet traceback in 1996**
- **I've had spook friends since the mid-1980s**
  - **US offensive cyber was a black op at least as early as 2000.**
- **Internet mapping project, 1998 - 2011**
  - **some results give a hint of what is possible**

MAP NET

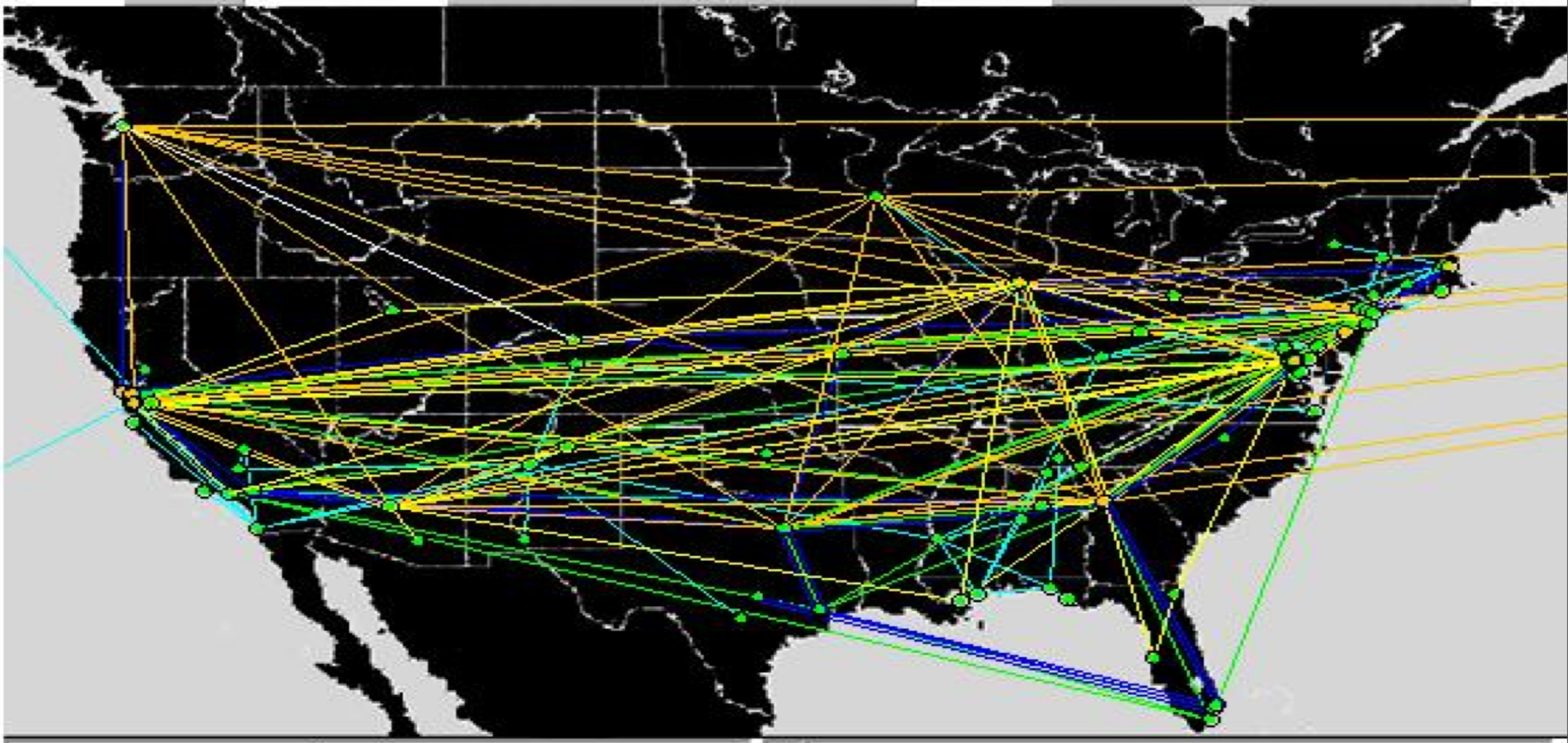
Show the Map

Clear the map

Size: 1

Both Backbones

Color by ISP



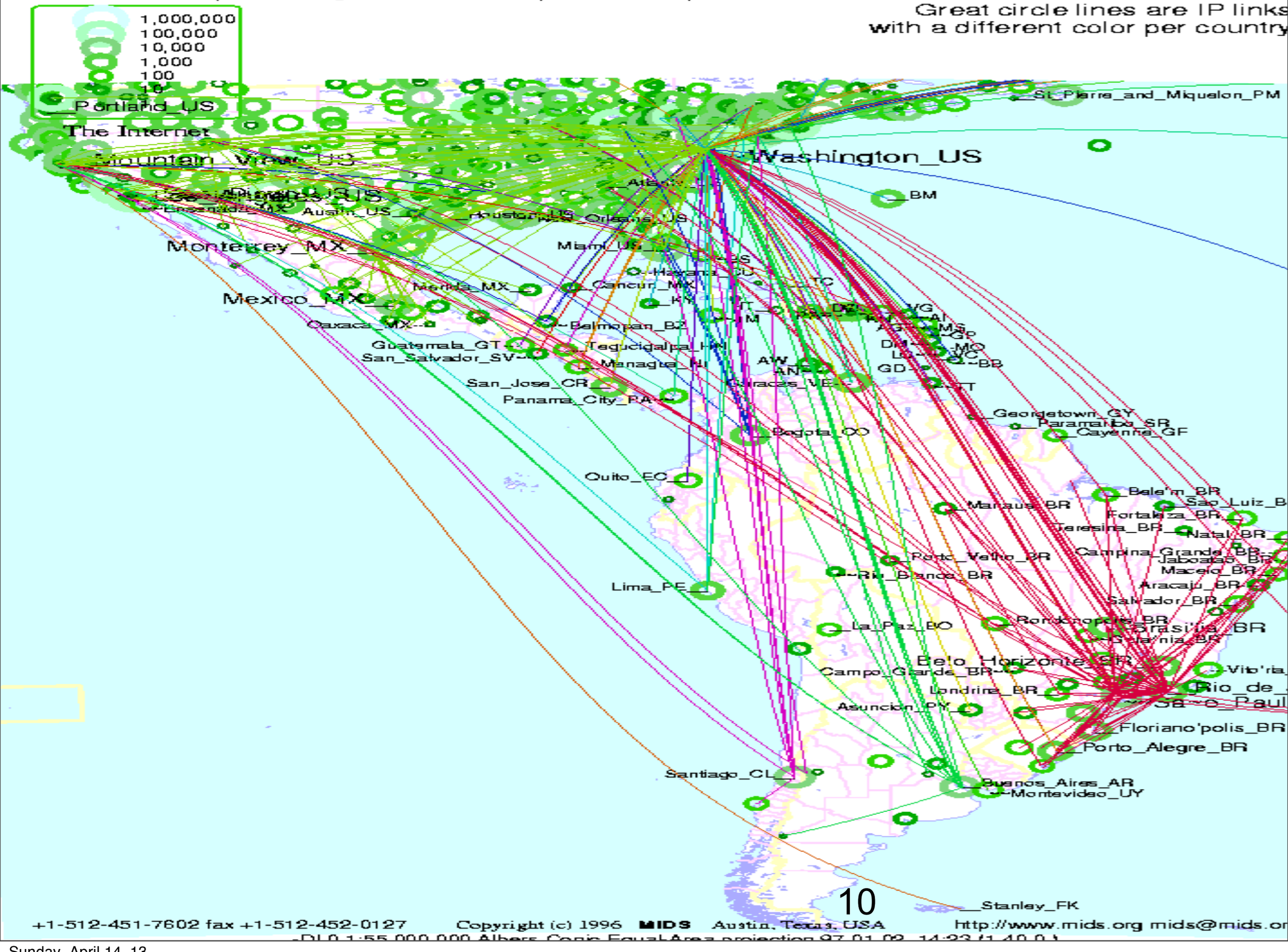
GeoNet Communications, Inc.
GetNet International
orange – GlobalCenter
yellow – GoodNet
green – GridNet International
IBM Global Network
cyan – IDREN
IDT Corp
blue – internetMCI
iSTAR Internet Inc.

Pipes
---
45 internetMCI
Seattle, WA<->Denver, CO

The Internet (hosts July 1996 links Sep-Oct 1996)

LatIn AmerIca and CarIbbean

Great circle lines are IP links
with a different color per country



DLO 1:55,000,000 Albers Conic Equal-Area projection 97.01.09 14:23 (1.40.0)

The Internet Mapping Project

- **Highlands Forum "Day After Scenario"**
- **a personal profile by Jerry Post for Fred Cohen and me.**
- **Started with Hal Burch in 1997. Continued with Lumeta through the 2000s.**
- **350,000 traceroutes per day**
- **Long-term analysis of data**

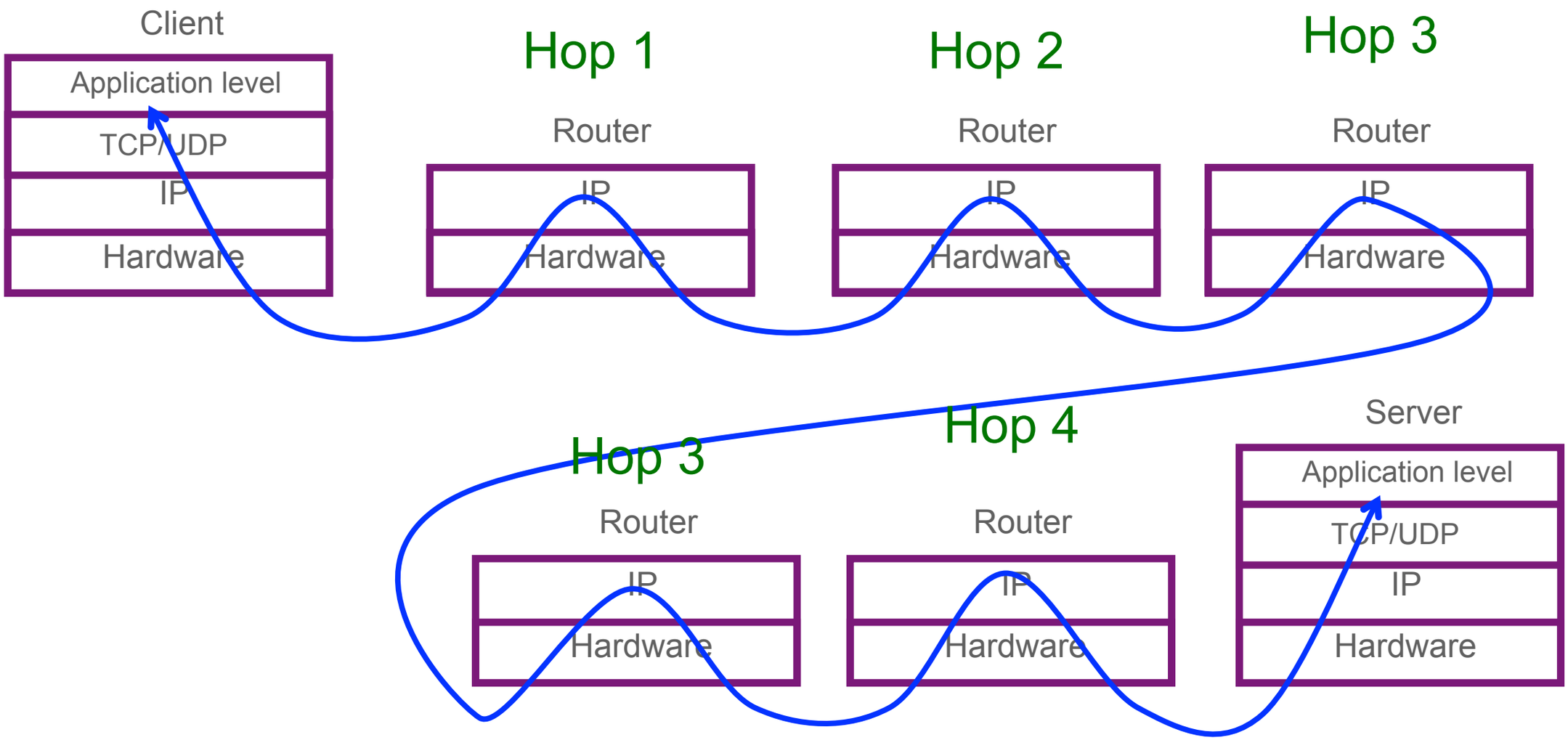
Methods - network discovery (ND)

- **Obtain master network list**
  - **network lists from Merit, RIPE, APNIC, etc.**
  - **BGP data or routing data from customers**
  - **hand-assembled list of Yugoslavia/Bosnia**
- **Run a TTL-type (traceroute) scan towards each network**
- **Stop on error, completion, no data**
  - **Keep the natives happy**

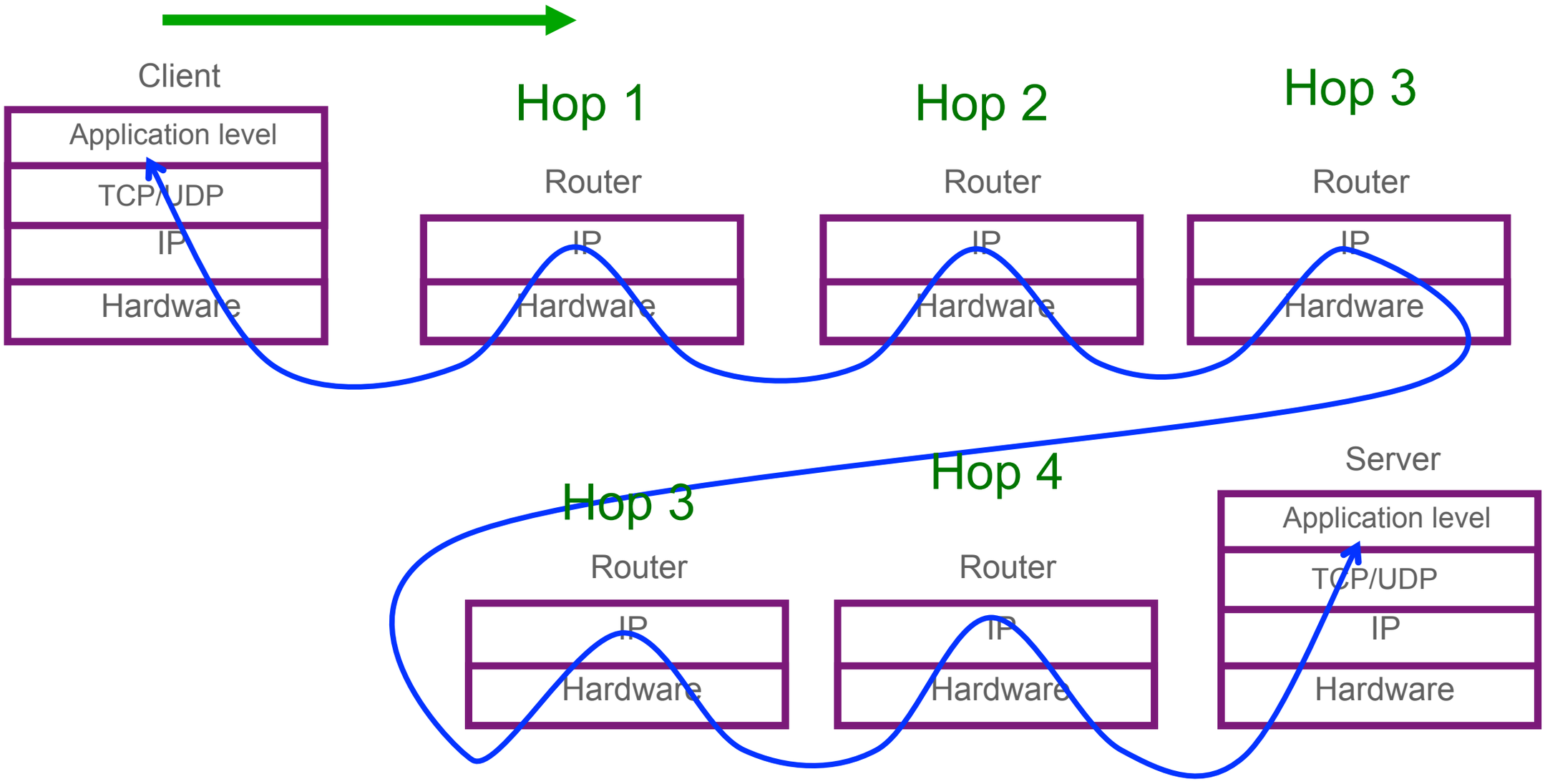
Traceroute

- **Probes toward each target network with increasing TTL**
- **Probes are ICMP, UDP, TCP to port 80, 25, 139, etc.**
- **Some people block UDP, others ICMP**

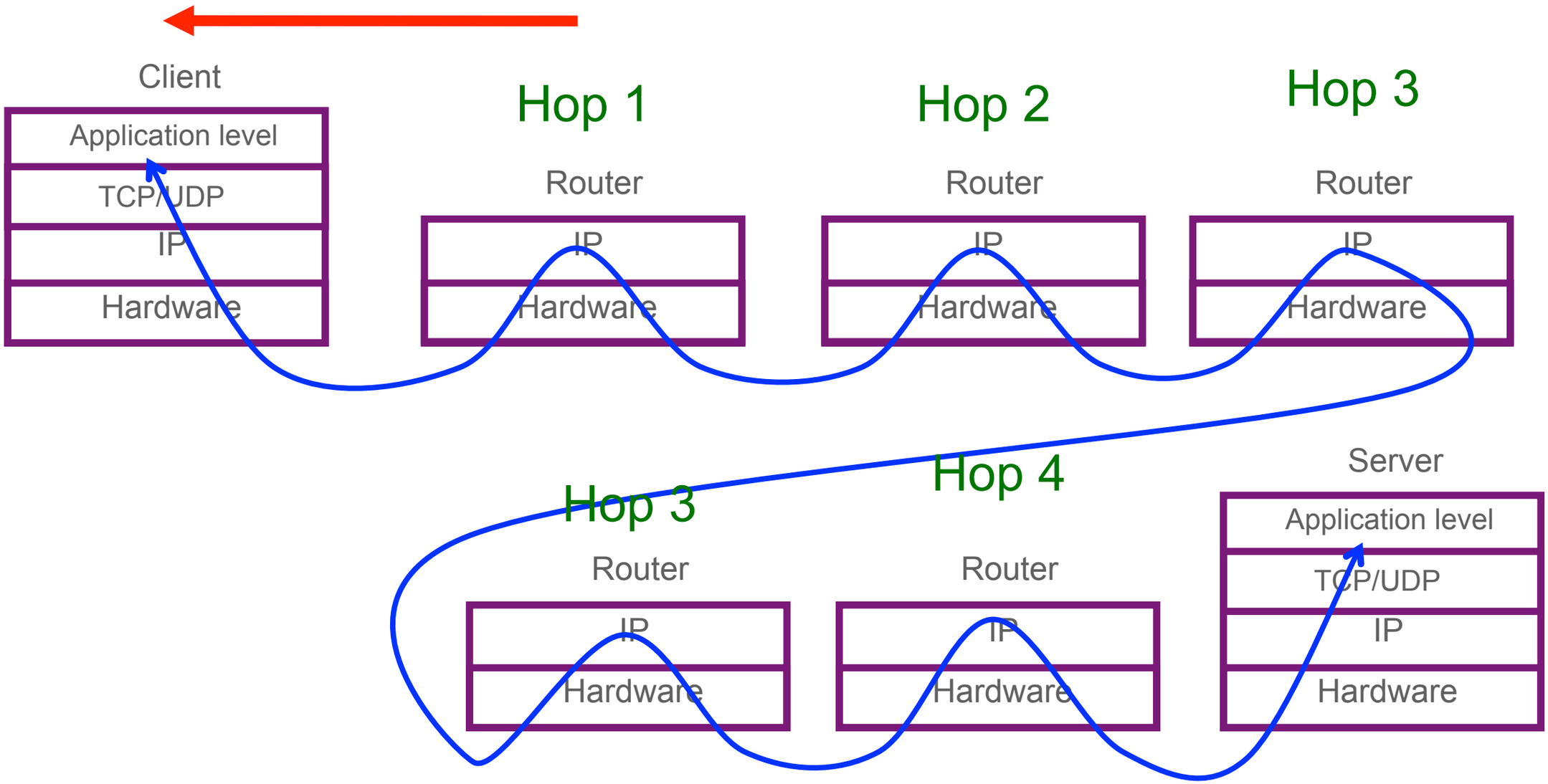
Traceroute


Client
Application level
TCP/UDP
IP
Hardware
Hop 1
Router
IP
Hardware
Hop 2
Router
IP
Hardware
Hop 3
Router
IP
Hardware
Hop 3
Router
IP
Hardware
Hop 4
Router
IP
Hardware
Server
Application level
TCP/UDP
IP
Hardware

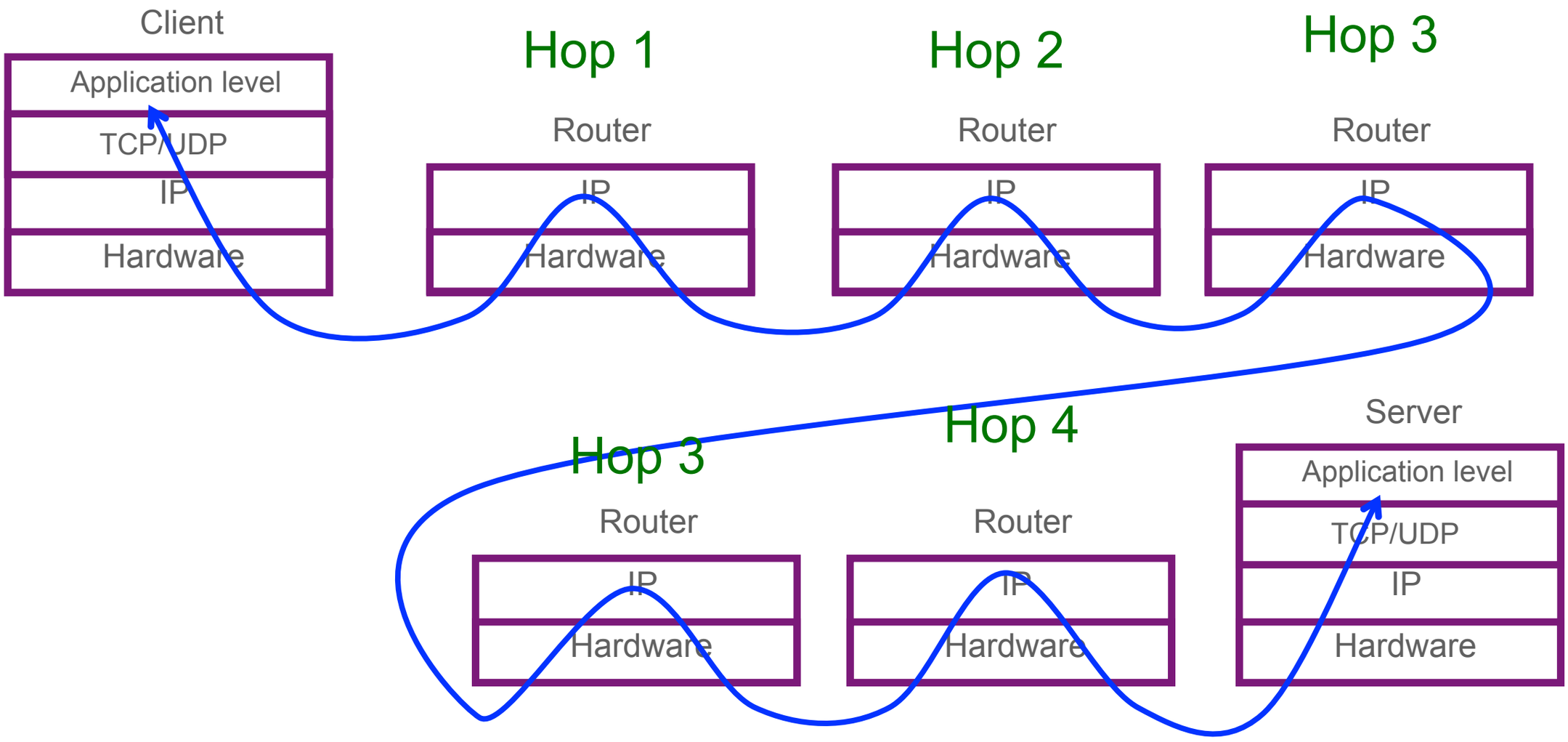
Send a packet with a TTL of 1…



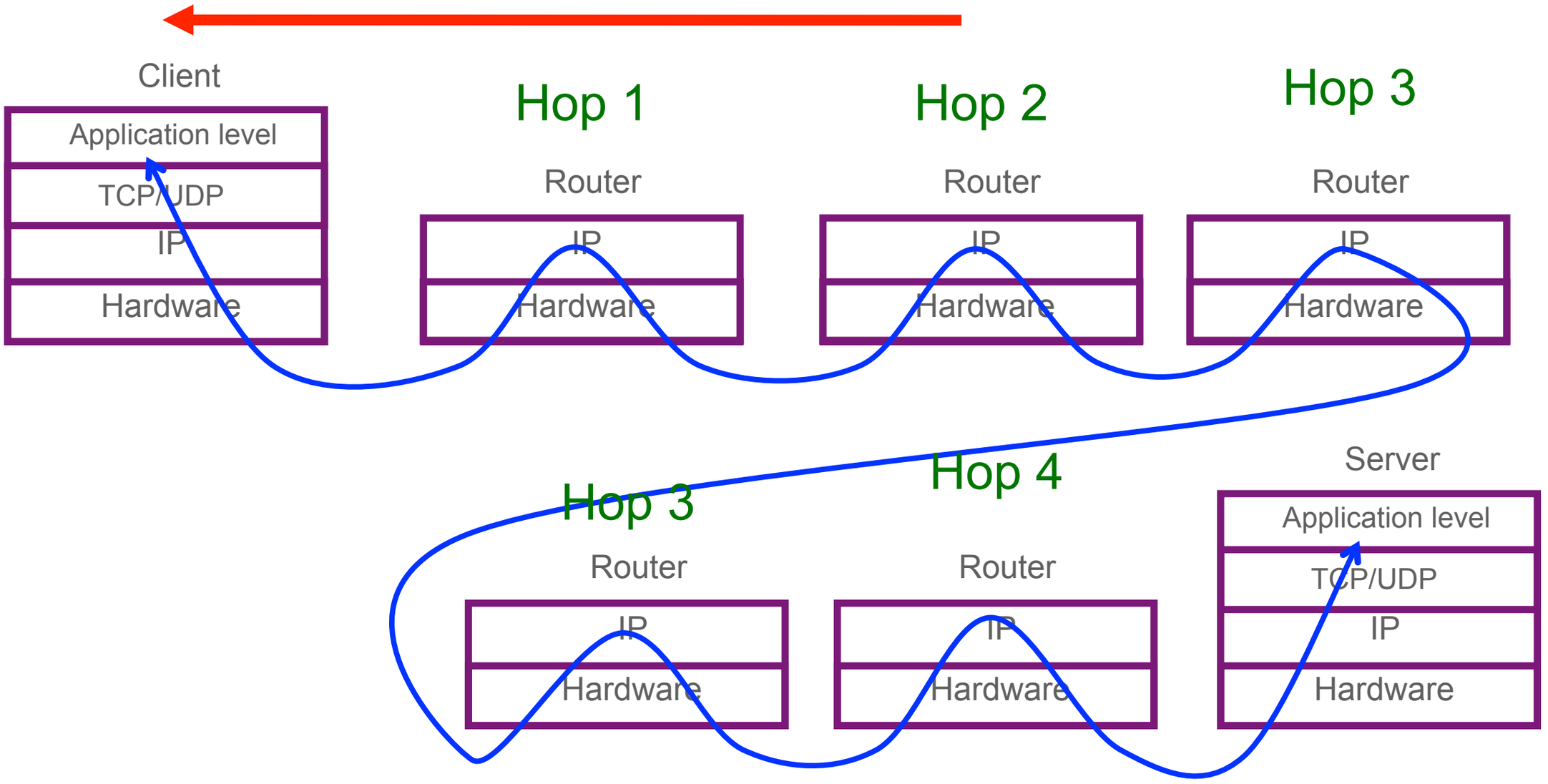
...and we get the death notice from the first hop

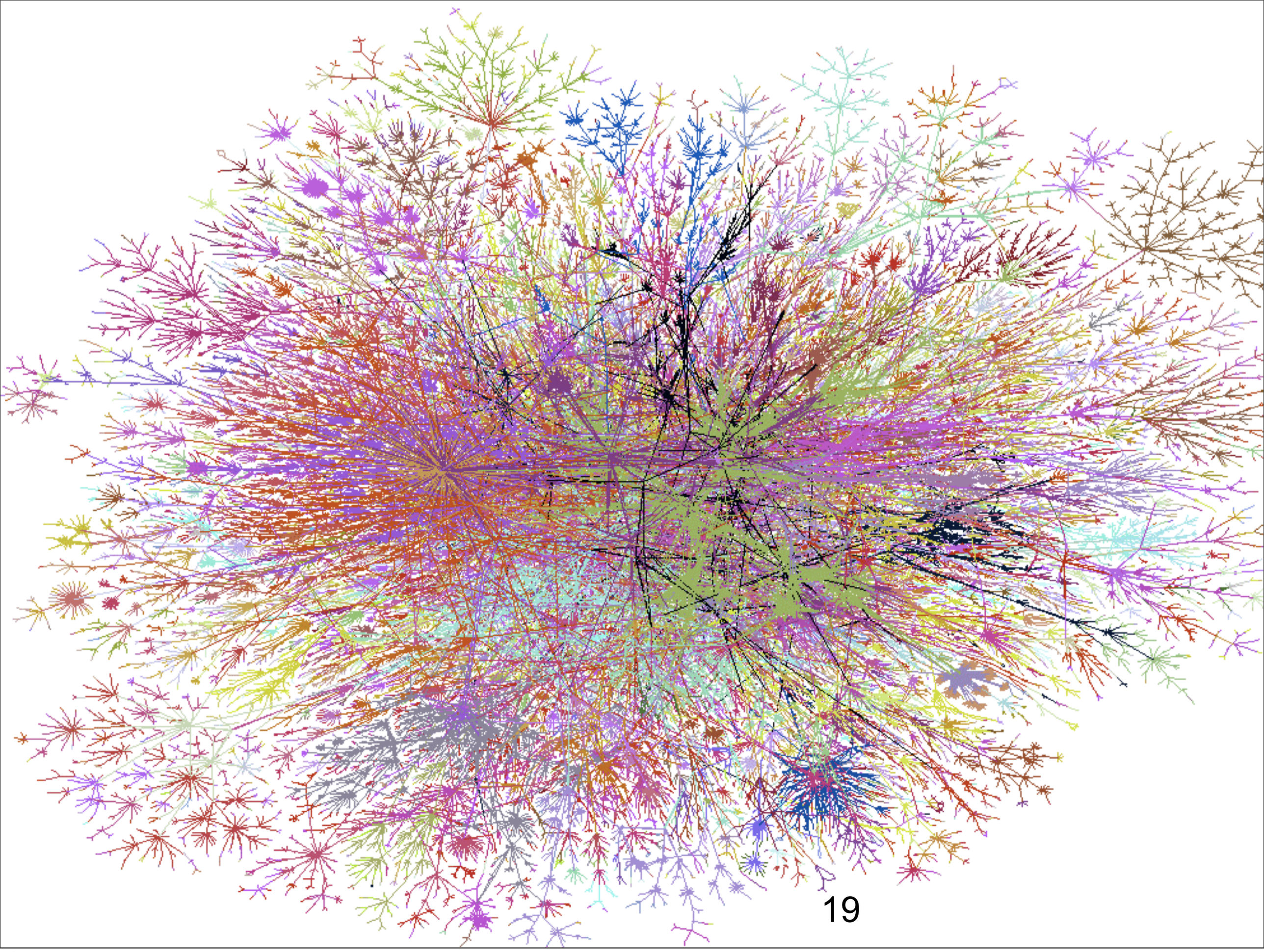


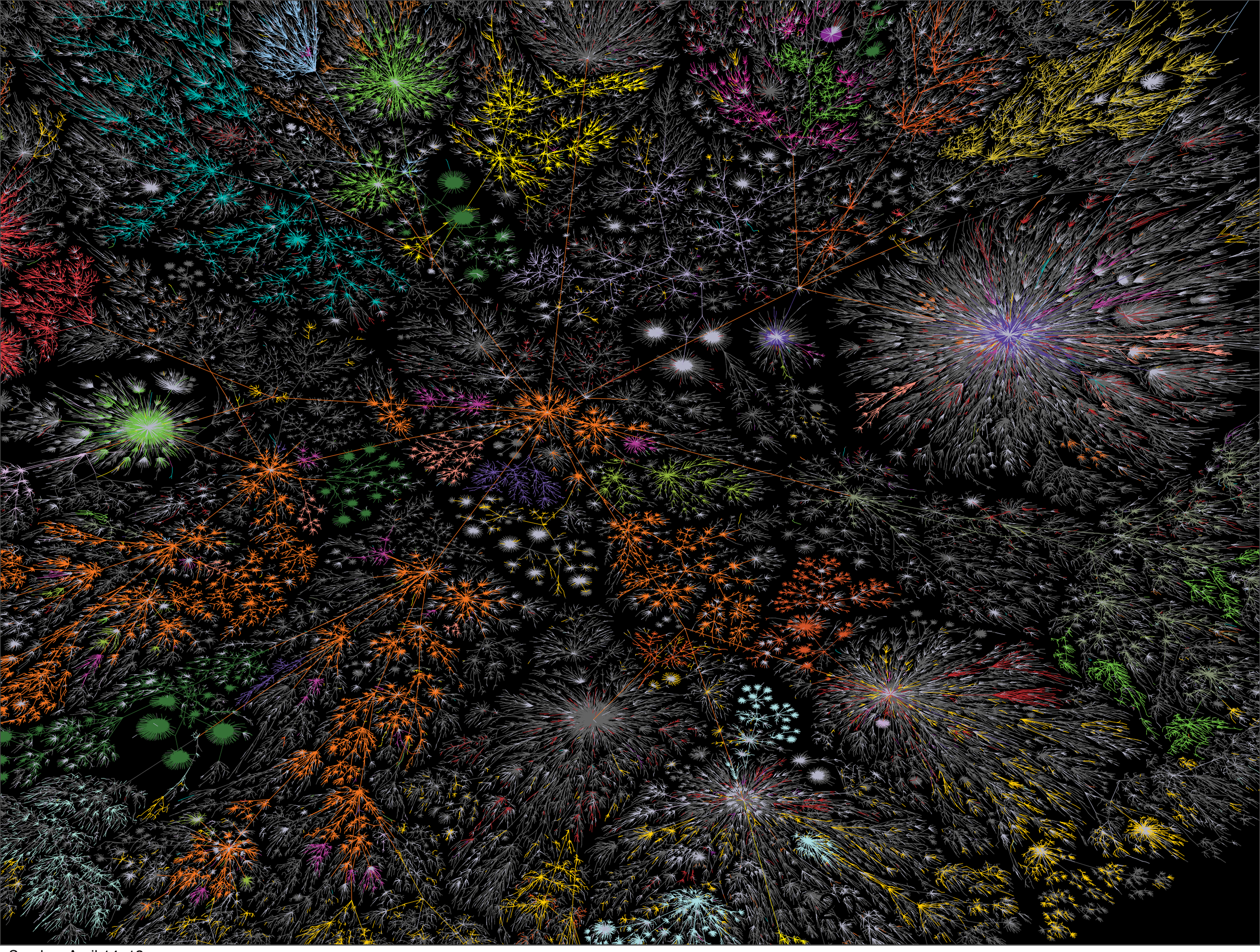
Send a packet with a TTL of 2...

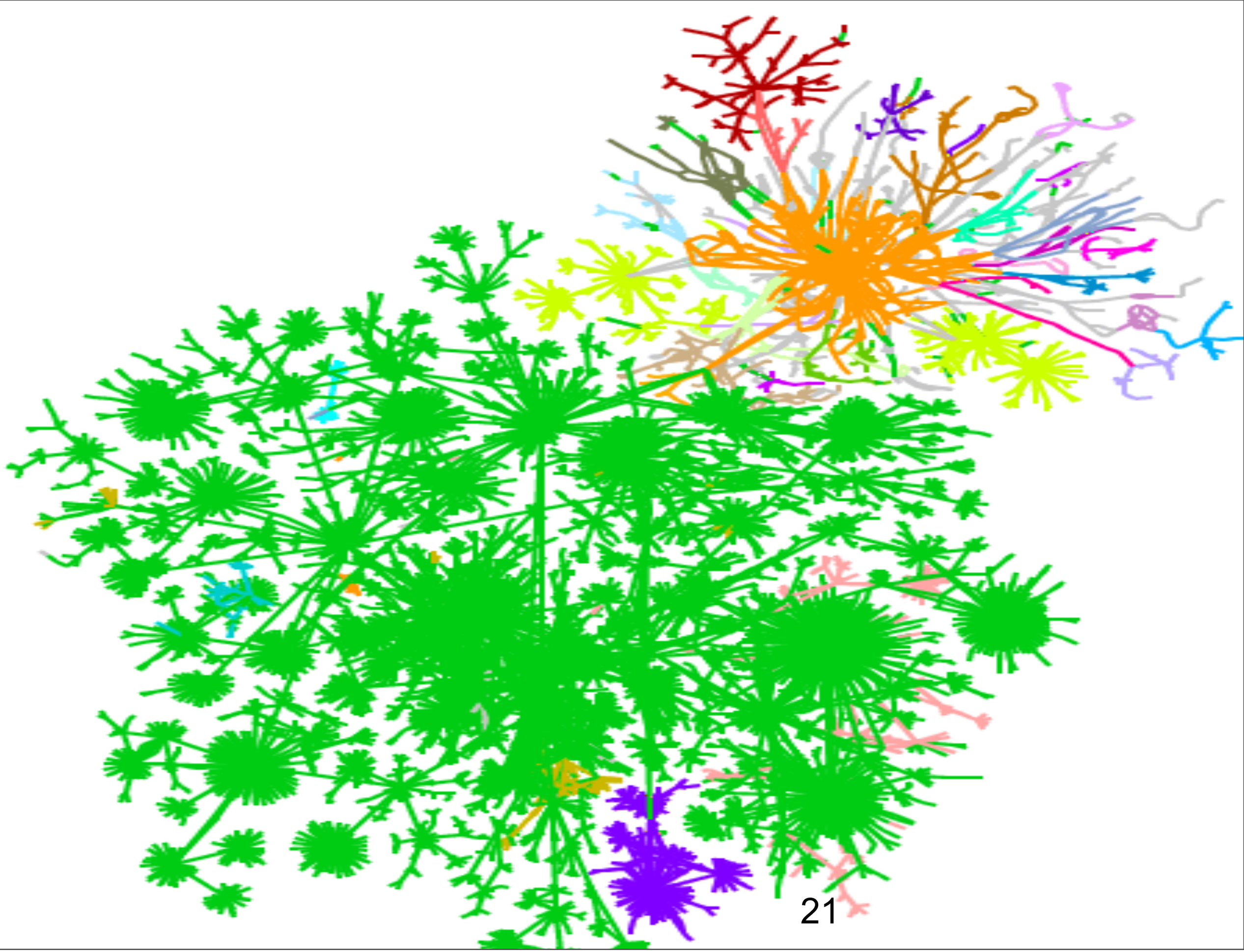


… and so on …


Client
Application level
TCP/UDP
IP
Hardware
Hop 1
Router
IP
Hardware
Hop 2
Router
IP
Hardware
Hop 3
Router
IP
Hardware
Hop 4
Router
IP
Hardware
Hop 3
Router
IP
Hardware
Server
Application level
TCP/UDP
IP
Hardware

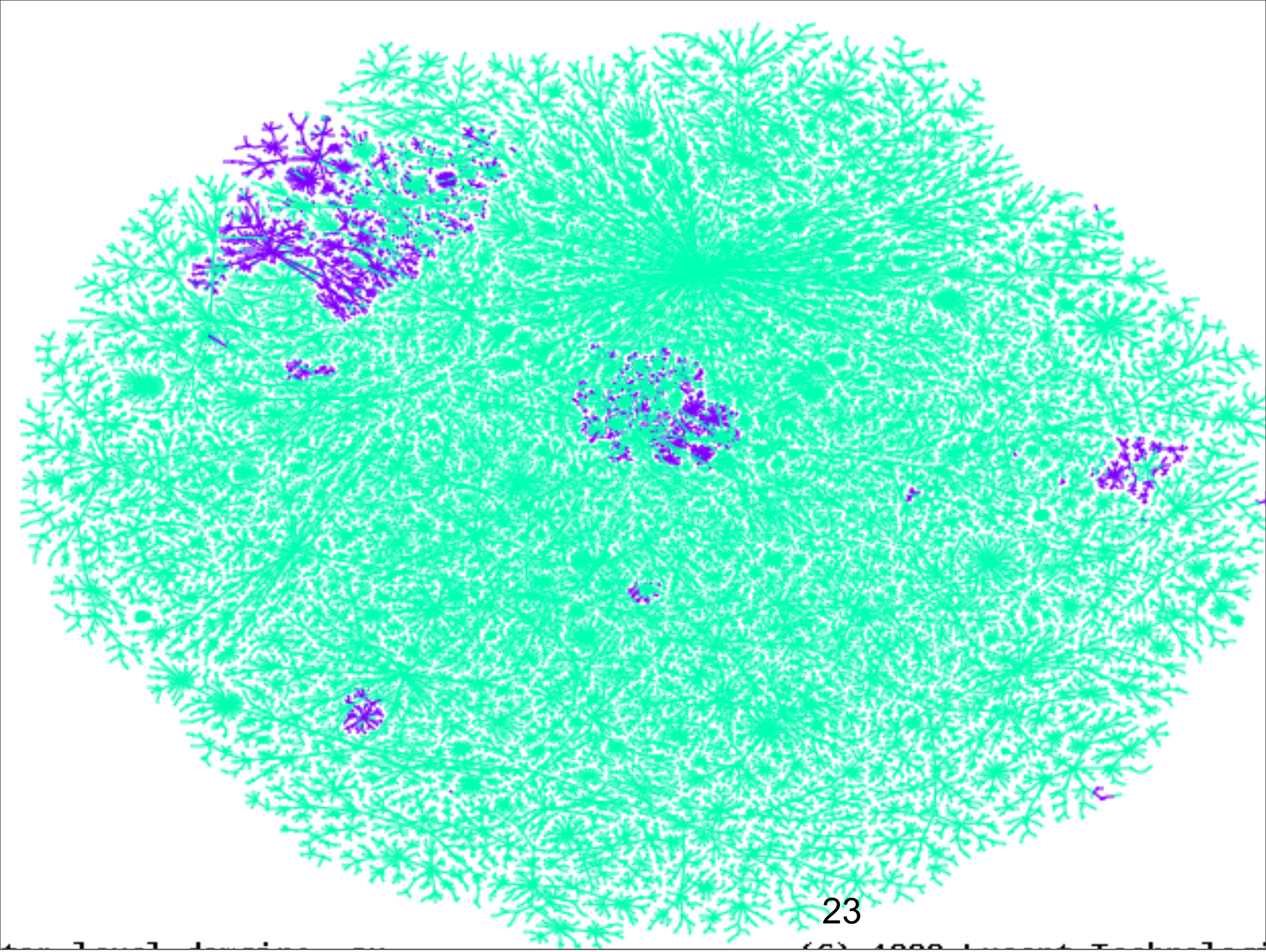

19

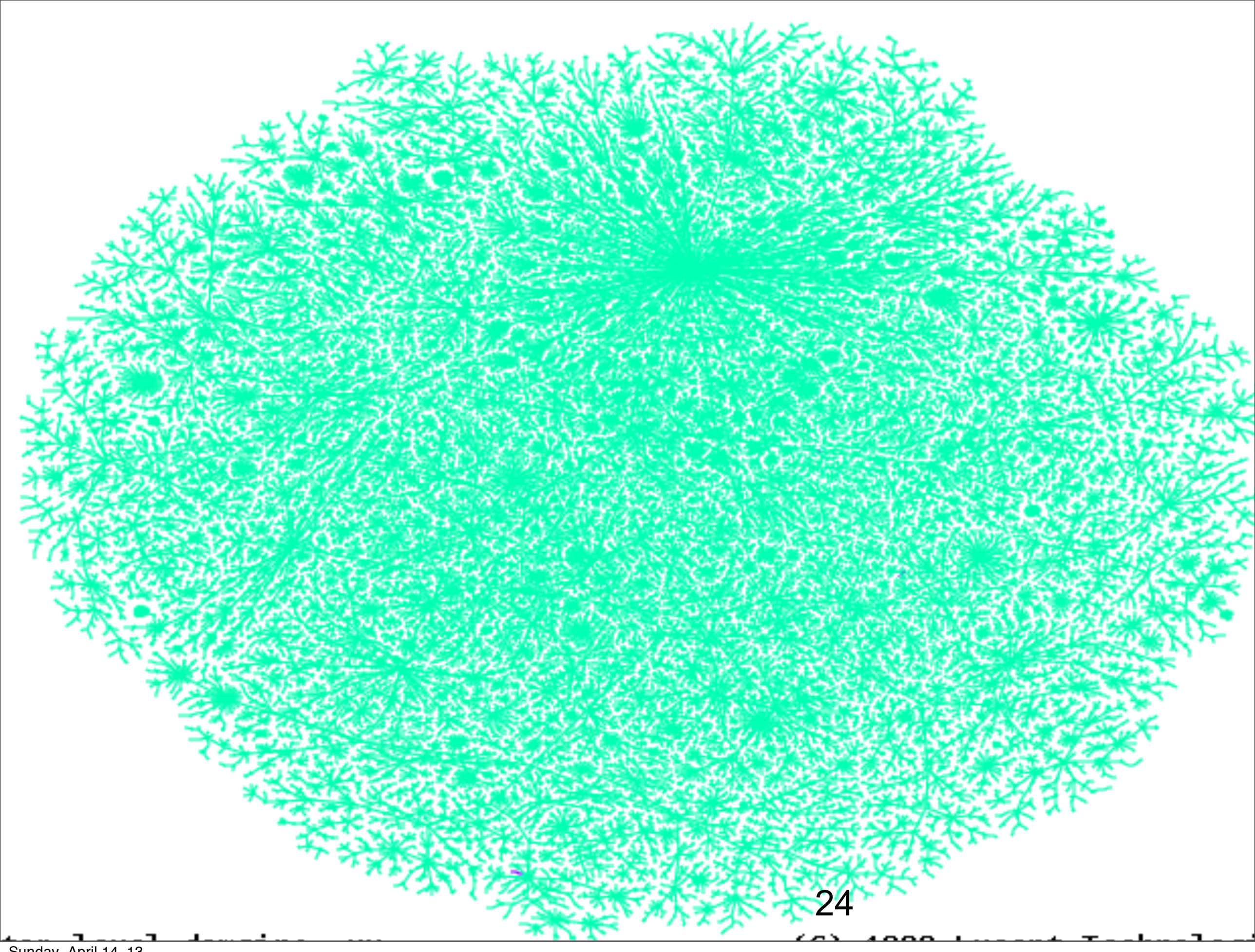




Lesson: The best attackers are patient

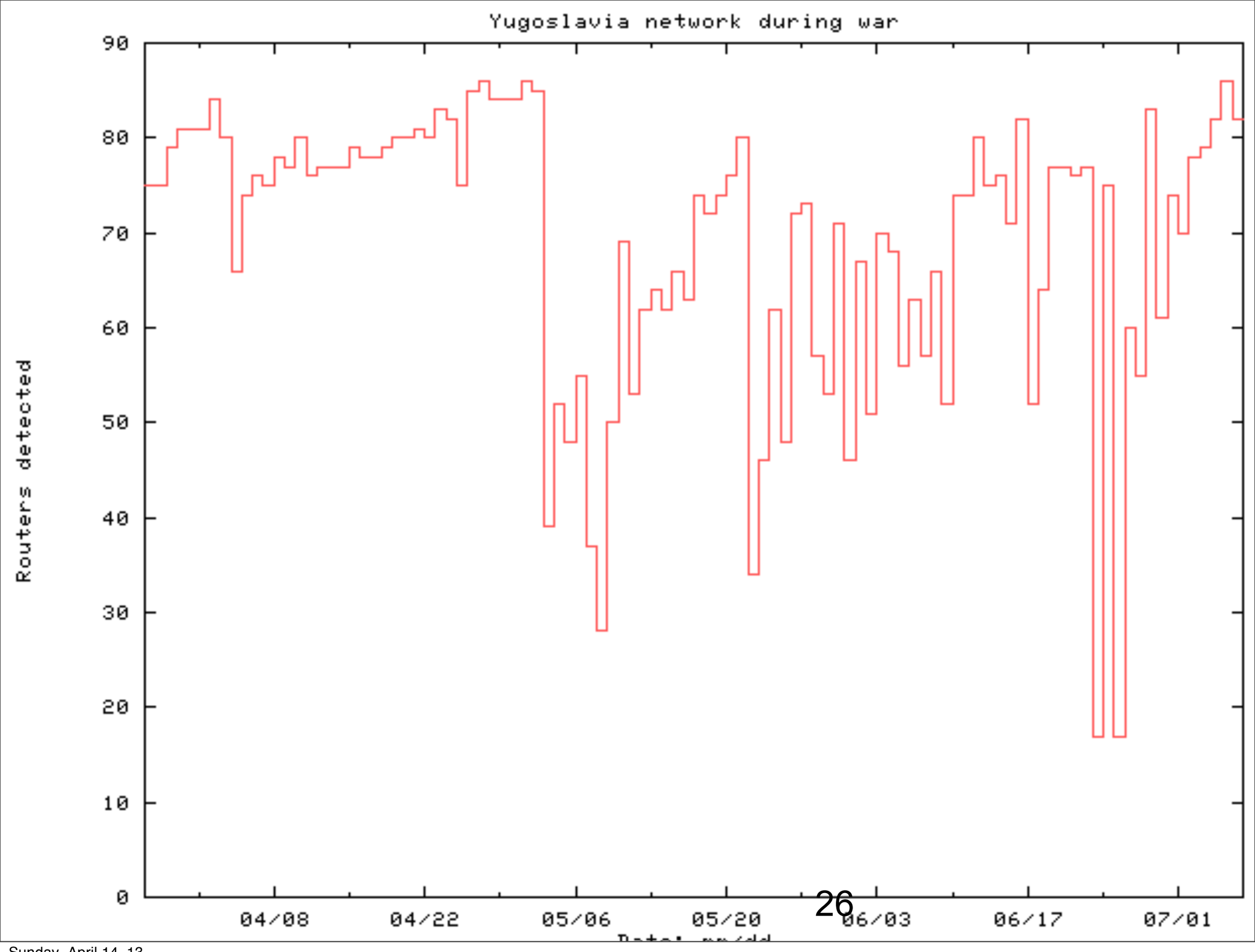
- **IMP:**
  - **pinged the SSN Hawaii (before commissioning)**
  - **Iranian network access: rare connections**
  - **Serbian bombing**

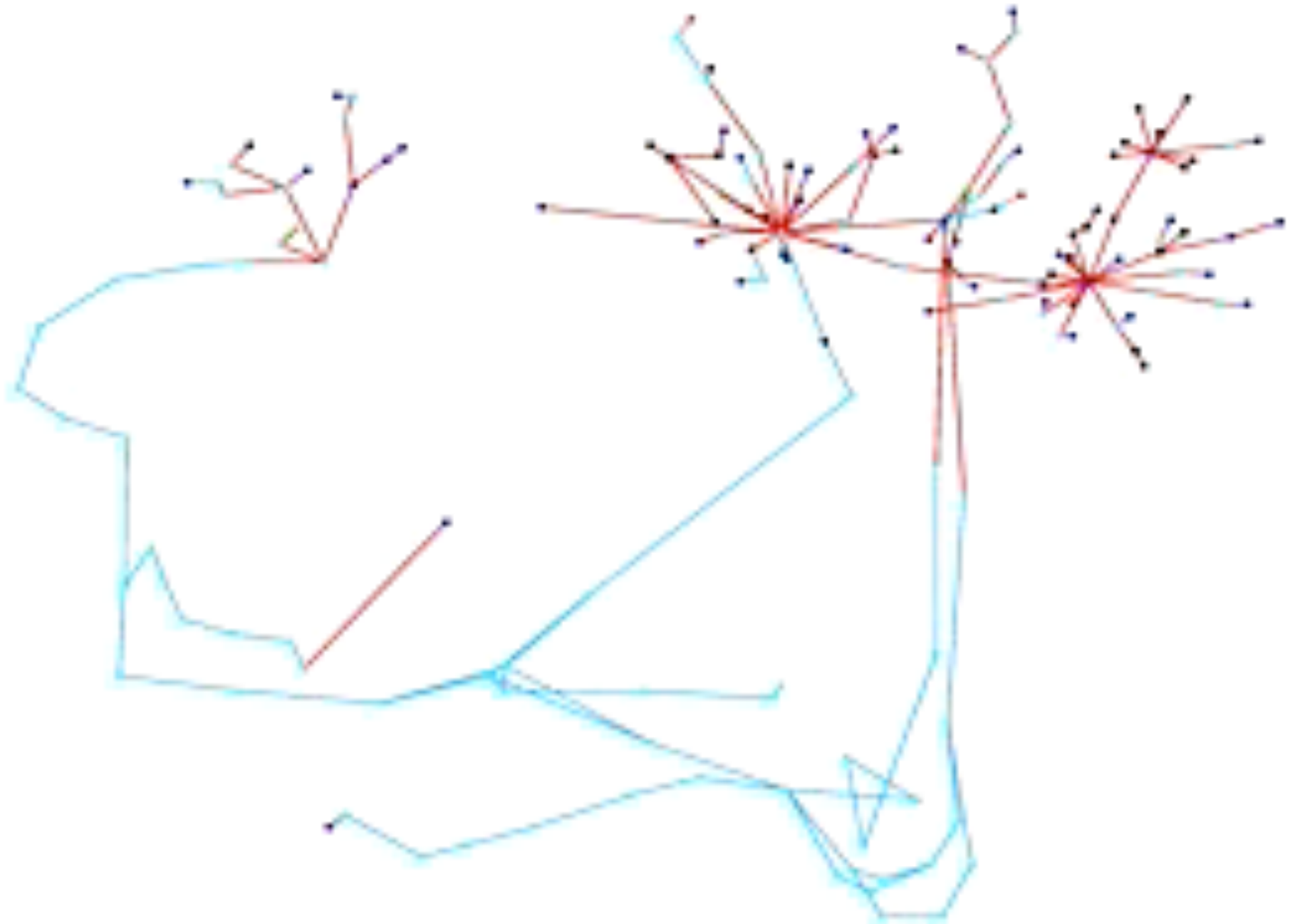




Yugoslavia

An unclassified peek at a new battlefield


Yugoslavia network during war
Routers detected
90
80
70
60
50
40
30
20
10
0
04/08
04/22
05/06
05/20
06/03
06/17
07/01



05/01/1998

Policy issues

- **Is it an act of war to ping Finland?**
- **How about running traceroutes to its networks?**
- **I needed a personal foreign policy**
- **The public now participates in cyber attacks**

Lesson: traceroutes are informative

- **Lesson: low TTL packets can be very dangerous**
- **They are easily detected, and have few causes:**
  - **routing loop (rare)**
  - **administrator tests (common)**
  - **attack mapping (?)**

Goals

- **Espionage**
- **Damage**
- **Loss of confidence**
- **False flag operations**

Damage

- **Soft damage**
  - **Can be very subtle, and disrupt operations for years.**
- **Hard damage**
  - **best if replacement equipment is scarce**
  - **massive attack can overwhelm supply chains**
  - **It is also much harder to do**

Soft Damage

- **Erasing or changing data**
  - **Subverting or destroying backups.**
- **Make operators take the wrong action**
- **Perhaps convince management that the project is not worthwhile**

Hard Damage

- **Destroying hardware**
  - **disk crashes?**
  - **Flash has a limited number of writes**
- **Damage or destroy equipment**
- **Take out a dam, blow transformers, etc.**

Loss of confidence: "Gremlin attack"

- **Reduce confidence in the venture**
- **Make them reject certain approaches**
- **"Cursing" a technique, certain equipment, or people**
  - **two PC virus payloads from the 1980s**
- **the beach house TV story**

False flag operations

- **Attribution is the major problem in information warfare**
- **Make it look like someone else is doing something bad**

Assets

Tools

- **Day 0 exploits are rare, expensive, and have a shelf life**
- **Crypto**
- **BBB**
- **"social engineering" i.e. spy techniques**
- **Standard attacks still work**
- **Supply chain attacks**
  - **defective equipment for Russia, Iran**
- **Botnets**

Market for Day 0 exploits (via Forbes)

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

People

- network administrators
- key engineers/scientists
- BBB
- money, traitors, moral objectors

Gain access

- **software hacks**
  - **day 0 exploits**
    - expensive, single use, has a shelf life
  - **well-known exploits on old software**
    - (which is common)
- **email/web injection**
- **USB sticks**
- **crypto: digital hash collision**

Mapping

- people
- network
- devices
- software

Network

- **the Official Map**
- **ping/traceroute**
- **SNMP dumps**
- **reverse DNS**
- **passive packet monitoring**
- **activity of people (see above)**

Devices

- **industrial controllers**
- **network gear**
- **client hosts**
- **misc. devices**
  - **often not updated**
  - **printers are especially bad**

Exfiltrating Data

- **Operational progress, *i.e.* debugging**
- **To the Internet**
  - **VPNs**
  - **stego: TCP headers, web requests, email, etc.**
  - **Depends on the volume, which can be huge**
- **Over the cell network**
- **USB sticks/laptops/cell phones?**
  - **strip search on your way out?**

Lesson: these backchannels may be the best way to detect an attack

- **Generally, a highly-secure site should generate little to no outgoing traffic**
- **Monitor flows**
  - **the openvpn story after a PCI audit**
- **Instrument nearby cell towers**
- **Look for any radio emissions**
- **Look for laser beams?**

Lesson: air gap defense didn’t work

- **USB sticks, laptops, spies**

Lesson: one attacking goal is to blind the operators

- **Include alternative backup instrumentation and reporting**
- **This is a common movie trope**

Lesson: there are unknown weaknesses in MD5

- **a state actor was willing to risk revealing some of this**
- **and maybe most/all digital signature technologies**

Lesson: The standard SSL cert. chain is unreliable

- **But you knew that, right?**

Lesson: tools will be enhanced and repurposed

- **Flame, Duqu, Gauss, …**
- **This is nothing new**

Attackers' concerns

- **Getting noticed**
- **Getting caught**
- **Expending exploits**
- **Misleading information**
  - **the double agent problem**
- **Wasting time and money**
- **Controlling exponential growth**
  - **Morris worm**
  - **Stuxnet got away, after a while**

There are weak points in these attacks

- **Discovery phase can create brief signatures on the network and in hosts.**
- **Secret honeypots and sentinels can force attackers to show their hand**
- **Exfiltration can be discovered**
- **Feedback from other sources**
  - **The Russians told the Germans that Purple had been broken**
- **Deception toolkits: Fred Cohen**

Defense that is good enough

- **Requires deep monitoring of your own people**
- **Data exfiltration could be detectable**
- **Bulkheads to limit damage**
- **Logging to learn about what they did - "no sparrow shall fall..."**

Lesson: watch for mapping activity

- **Detect all SNMP activity**
- **Low TTL packets are highly suspect (traceroute of any kind)**
- **Any unusual net activity**
- **High-entropy packets and flows**
- **Day 0 backups for comparisons**

Lesson: watch for mapping activity

- **xprobe packets**
  - **(weird option settings, etc.)**
- **access to Official Network Maps**
- **unexpected traffic on any device**
- **seek machines with promiscuous mode turned on**

Stuxnet *et al.*

- **I never thought the operations behind the Stuxnet group of attacks would be revealed**
- **Precedent is important**
  - **explain the boldness of Chinese attacks analyzed by Mendiant?**
- **Treaty of Westphalia**

Obama's Secret Wars and Surprising Use of American Power

David E. Sanger

2012

Rings true to me

- **The story is feasible, and matches what I know of the spooks**
  - **The testing described was right on**
- **It is about how I would try to do it**
- **"Olympic games" does not sound right**
  - **"Lathe Gambit"**
  - **probably several efforts with different names were combined**

Lesson: Attacks will continue, even after discovery

- **Motivated attackers switch to alternate access and targets**
- **1,000 centrifuges went down weeks after discovery**
- **The defenders are usually slow to catch on**
- **Do they find every leak?**

Policy issues

- **Question: where to spooks get their botnets from?**
  - **they certainly have them**
  - **seems like a clear ECPA violation to me**
- **“Ahead of the law”**
  - **unindicted oc-conspirator**

Lesson: suspect enemy action

- **Even if it usually incompetence.**

Lesson

We know these attacks are real, and you don’t have to be separating uranium isotopes to be worth all this effort.

You may well be a target

- **You have to be worth the ammo (exposing expendables)**
  - **but cyber bullets can often be used more than once**
- **If so, they will come in low, slow, quietly, and suck you dry of your vital information**

Defense is expensive, and part of the overhead

- **hard to justify**
- **ehg and Google**

Results

- **These attacks set precedent**
  - **Review Eisenhower and satellite overflight rules**
- **The tools are re-tasked and reused by others**
- **Vast review of software by manufacturers of controllers**
  - **I sure know that Seimens is working on it**

Lessons From Stuxnet

Bill Cheswick

http://www.cheswick.com/ches/talks/