How Do I Manage All of This?!

Eliot Lear
Cisco Systems

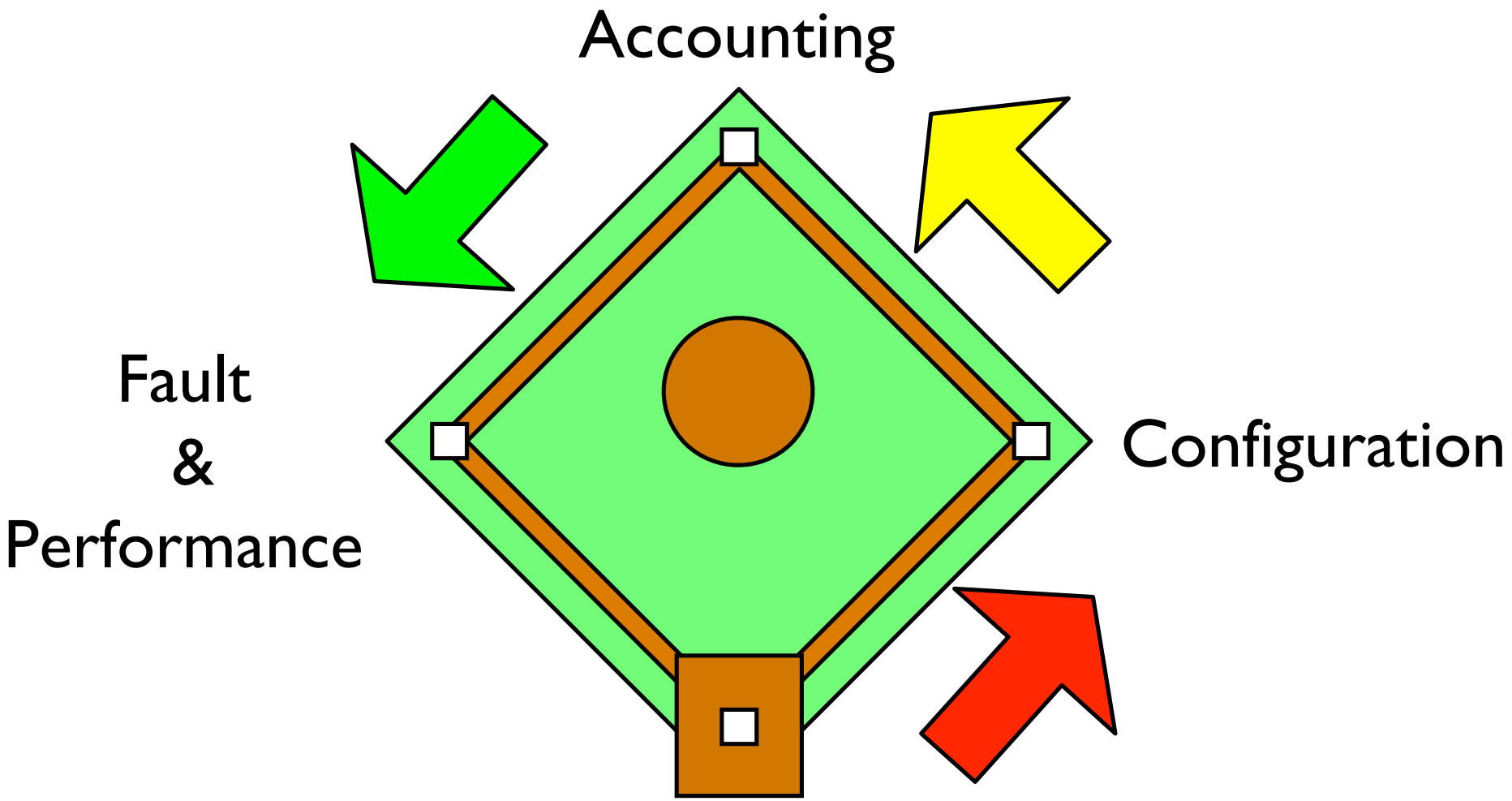
Why is all this management stuff important?

$?

Internet Management Goals

- 1987: Collect statistics and measure performance for non-critical systems
- Today:
  - Full customer facing provisioning, accounting, and performance management
  - Report and control predictable key functions, including front and back office services (this includes voice)

State Of Network Management



What's Changed Lately?

- Larger focus on security demands more focus on network management
- There are more network elements that can/should be managed
- Networks are getting more complex (voice, VPNs)
- We rely on them for more services

To Manage…

To know and control.

Knowing

- What you've got
  - Discovery
  - Inventory
- What state it's in
  - Fault & Performance

Discover what?

YesterYear	Today
Routers	Routers, Switches, Cable modems
Hubs	Phones, SIP servers, NATs, firewalls
Printers	Wireless Access Points
Hosts	Content switches, hosts
	Printers, Faxes, Scanners
	VPN concentrators

Discovery: Threat or Menace?

- Mechanisms:
  - Ping, ARP/ IP routing, CDP, SNMP, netstat, DNS, DHCP server, DOCSIS/Call Home

    Active Hello vs. Passive Response

    Layer 2 vs. Layer 3

DNS-SEC

Both network managers AND hackers LOVE discovery!

Discovery

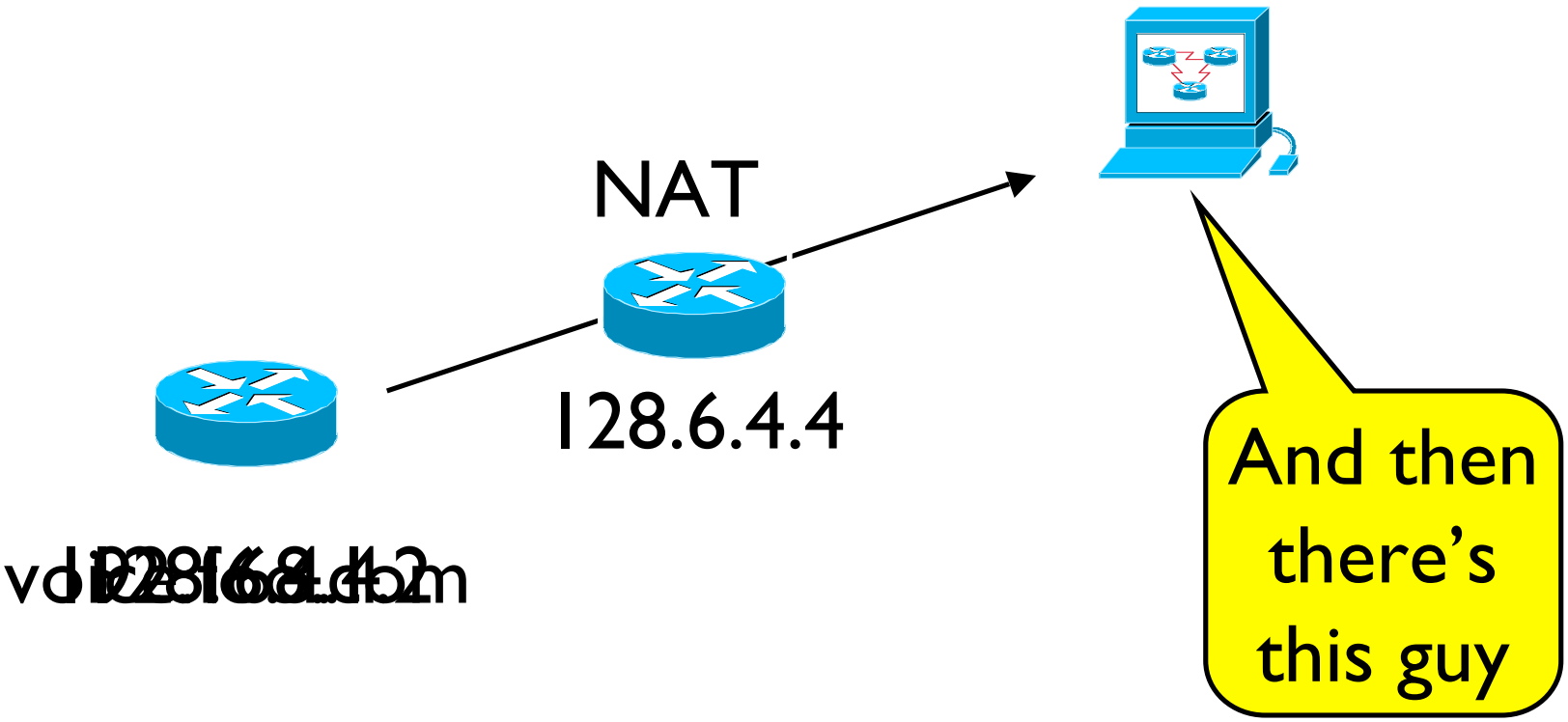
- Hackers love it more when network managers don't discover and they do!

Your network is discoverable. Don't make it hard for your NMS to discover it.

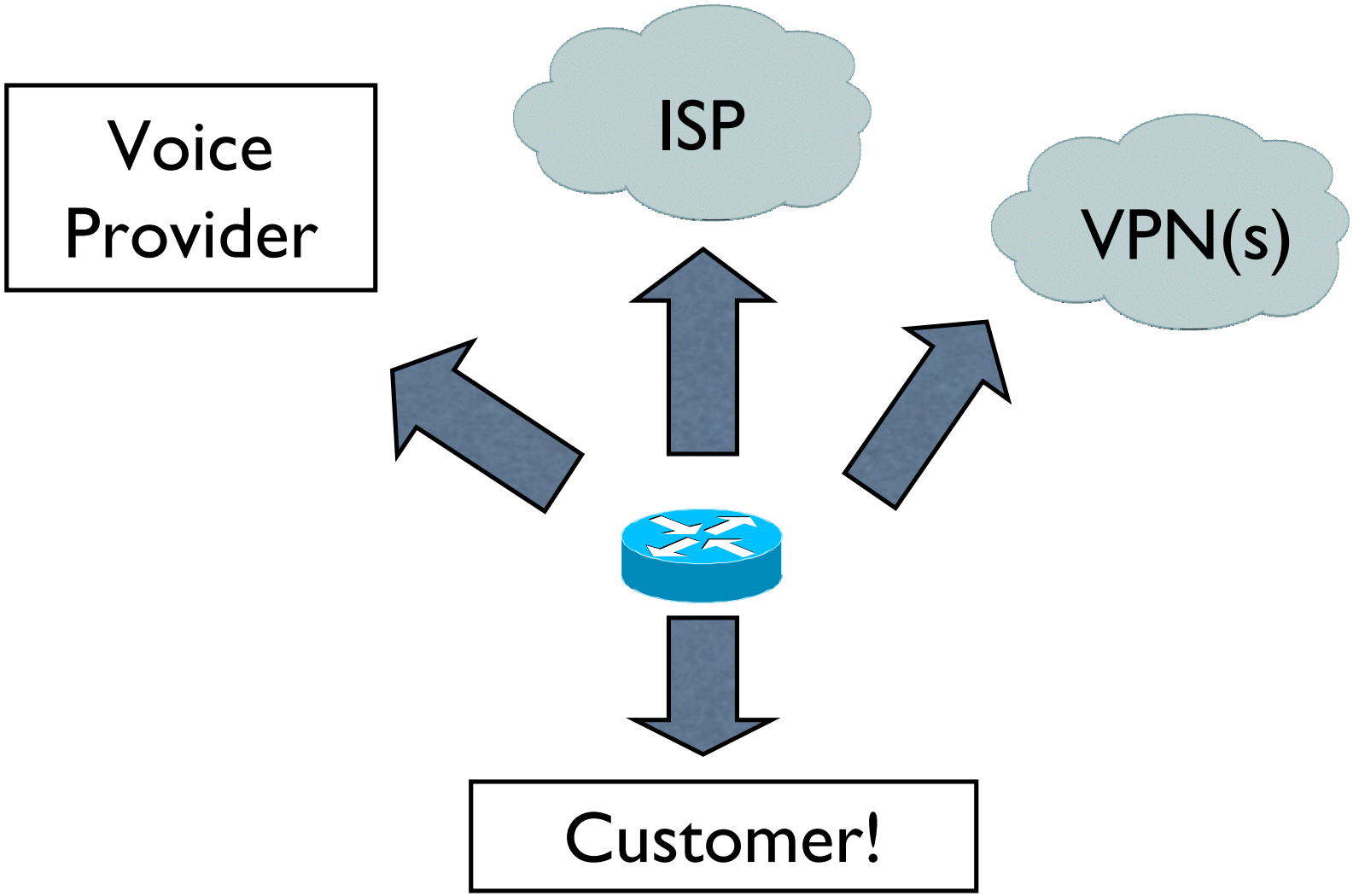
Call Home Mechanisms

- There are multiple standards today (PPPoX, DOCSIS, proprietary). More coming.
- Service providers can only query their own infrastructure O(2000 elements).
- They need a way to manage part of the CPE configuration. PPPoX doesn't cut it.
- Big service providers have $O(10^6)$ customers

Who IS It?



Nirvana or Nightmare?



Knowing - Fault, Performance, and…

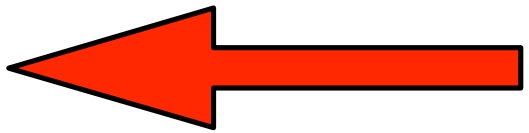
Steady Improvement

- Most devices and many functions are instrumented (perhaps too much so)
- The standards for state retrieval and report have matured (SNMP v3, SYSLOG)
- Lots of tools out there (MRTG, Cricket, HPOV, Tivoli, CA, …)
- Basic fault correlation is getting there...

Or at least so I thought...

```
Reporting-MTA: dns;xbe-ams-312.XXXXXXXX.com
Received-From-MTA: dns;sj-iport-4.XXXXXXXX.com
Arrival-Date: Wed, 2 Jun 2004 13:25:11 +0200

Final-Recipient: rfc822;croot@exch.EXAMPLE.com
Action: failed
Status: 5.1.1
```



??????

End User Left Out of the Equation

UNIX Fault Management

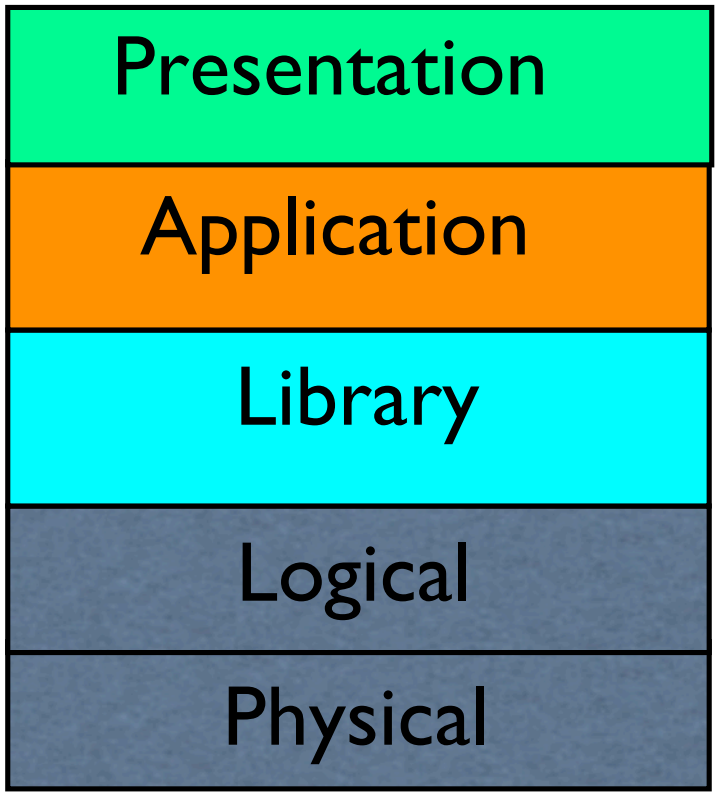
"A fault in your disk strikes- more"
"You die."

fprintf(f,"%s",*s)=EPHYS

_write(fp,data,size)=EPHYS

fswr(fs,sect,data)=EPHYS

phwr(D,sect,data)=EPHYS

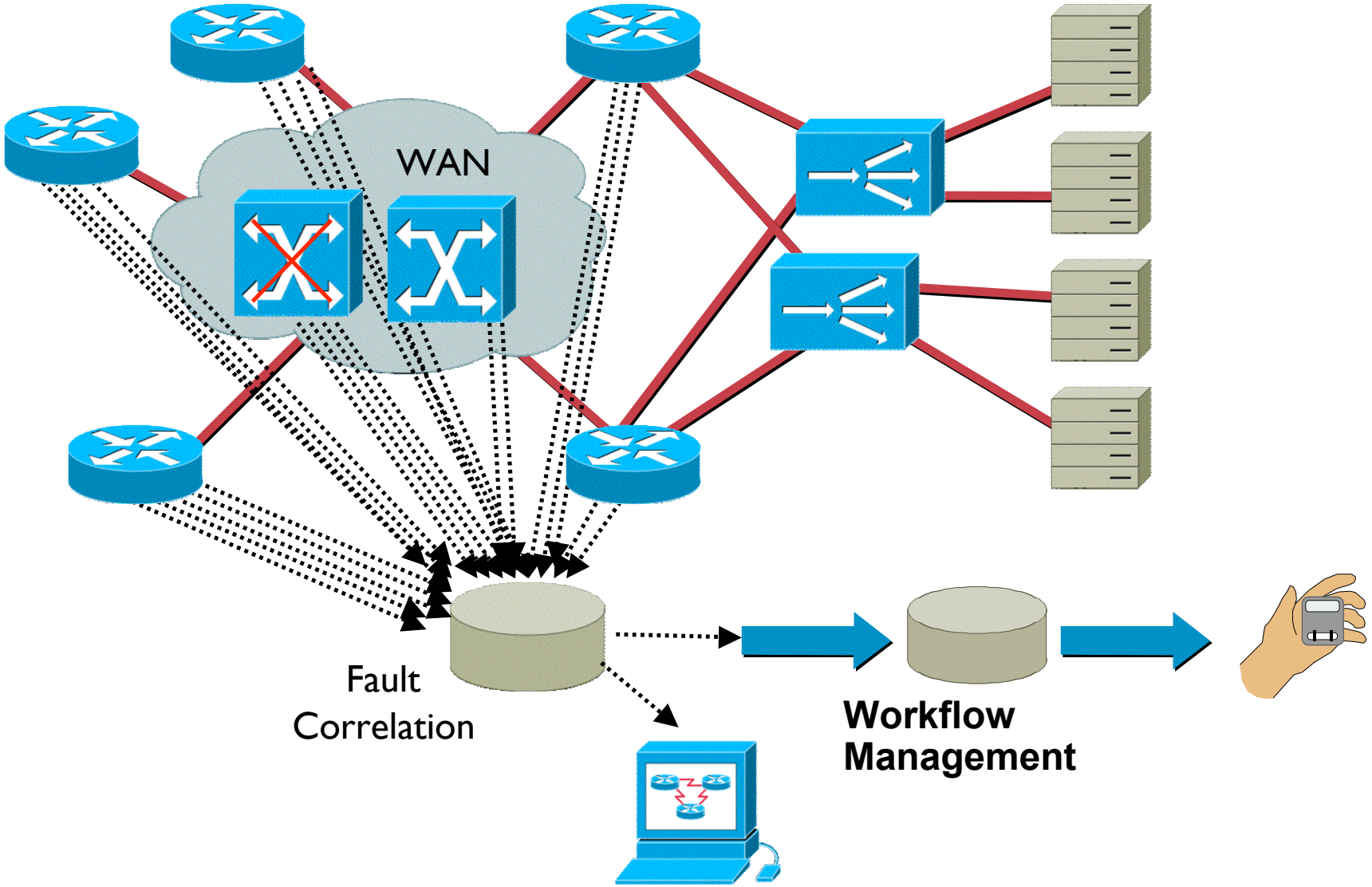


nethack

libc

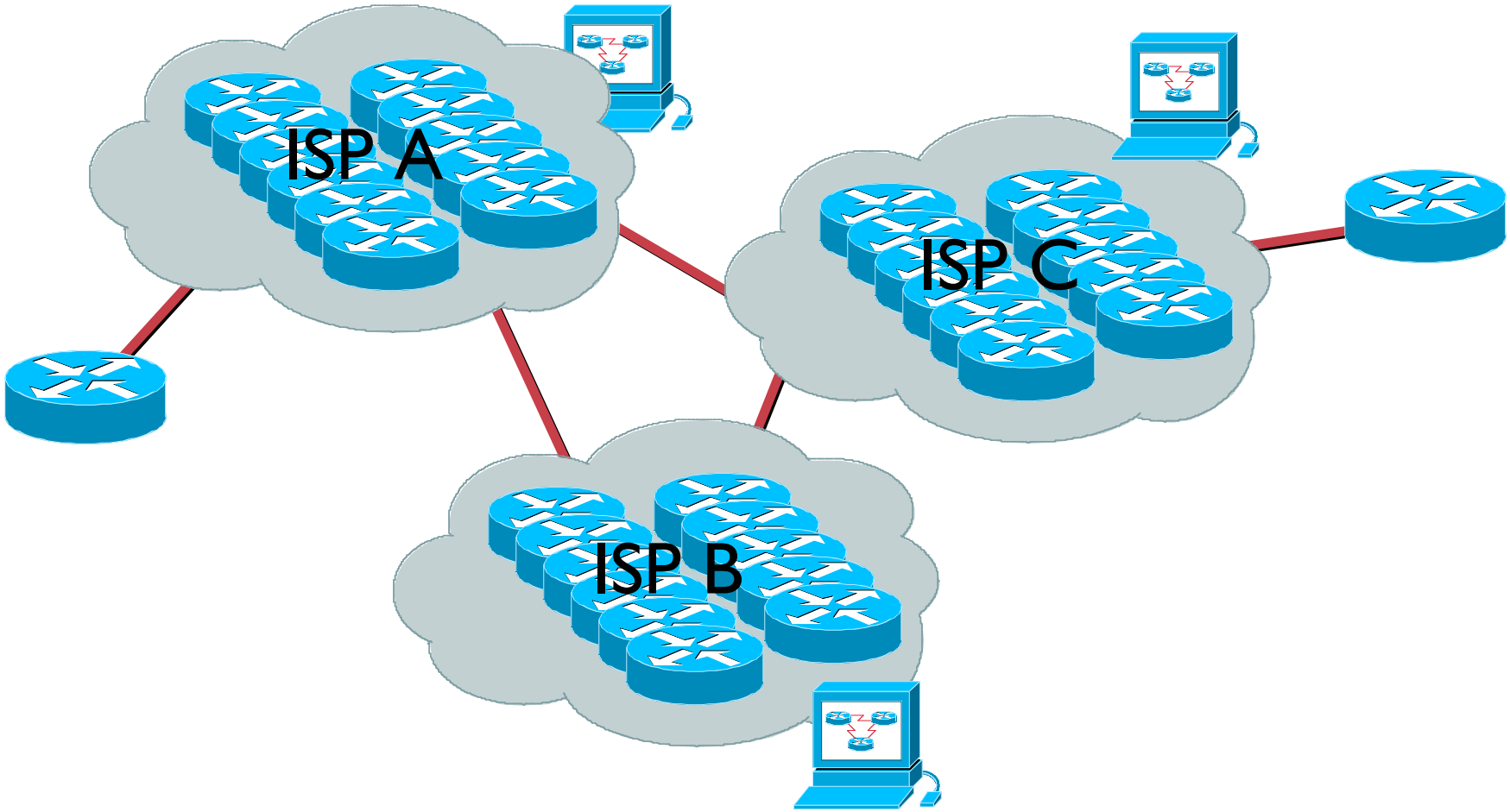
kernel

Layering and multiplexing makes IP different



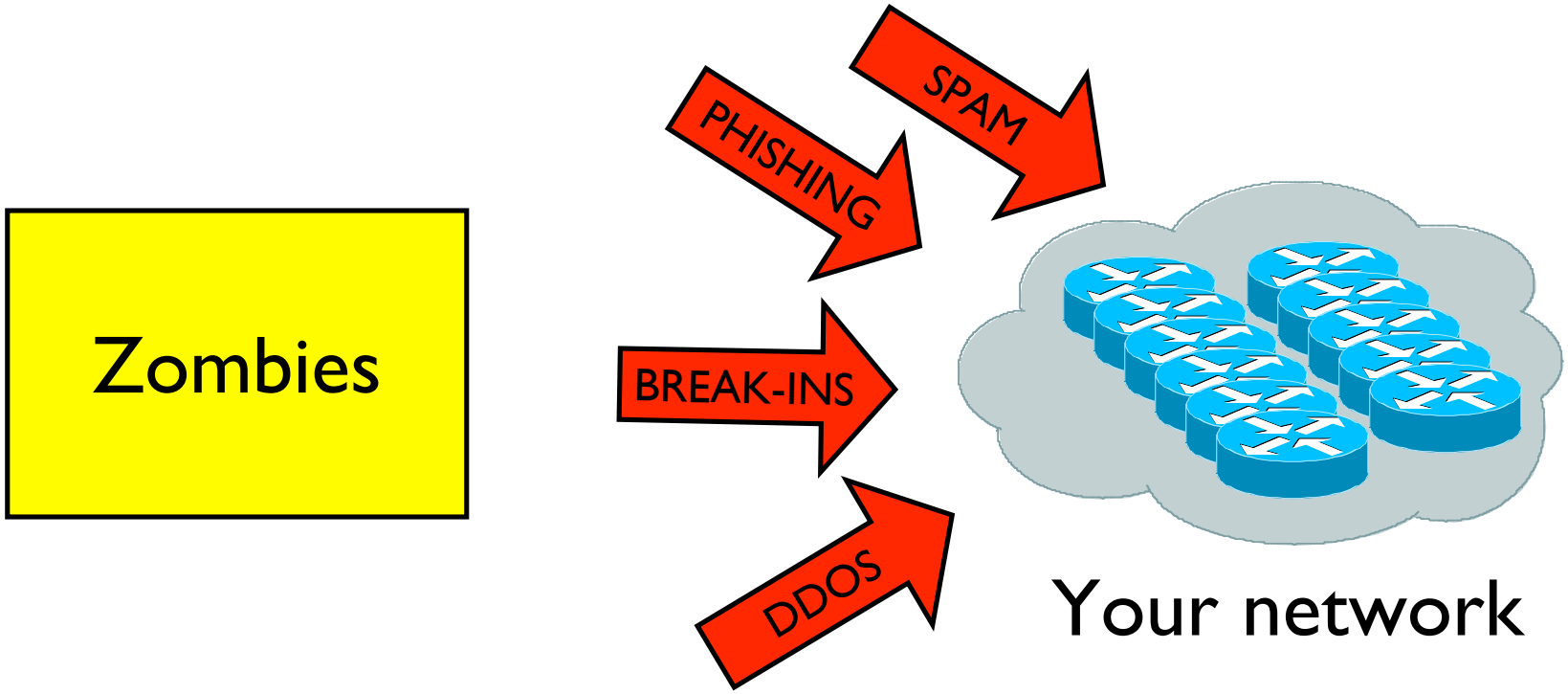
Avoiding this…

Who's fault is it, anyway?

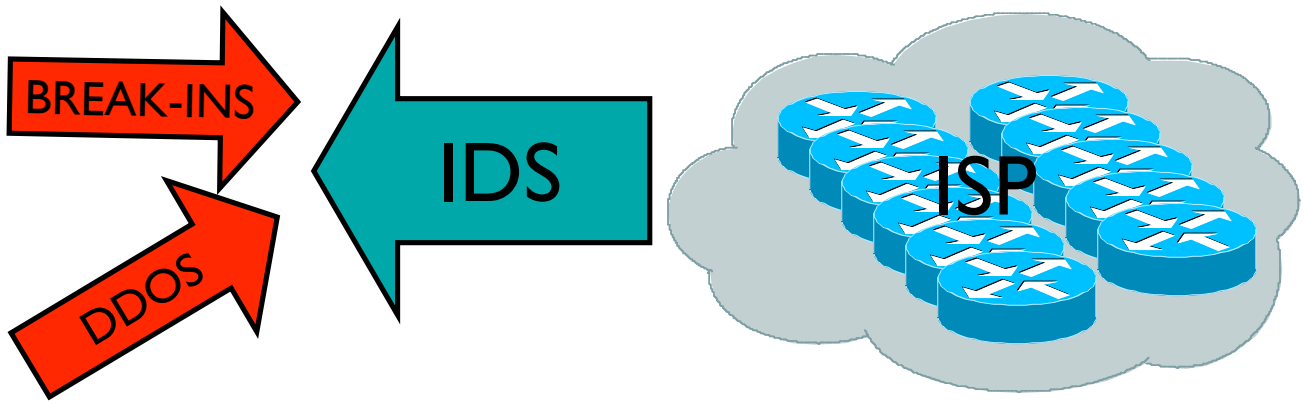


And that's just "fault"

- It doesn't include security management



IDS takes on a new role

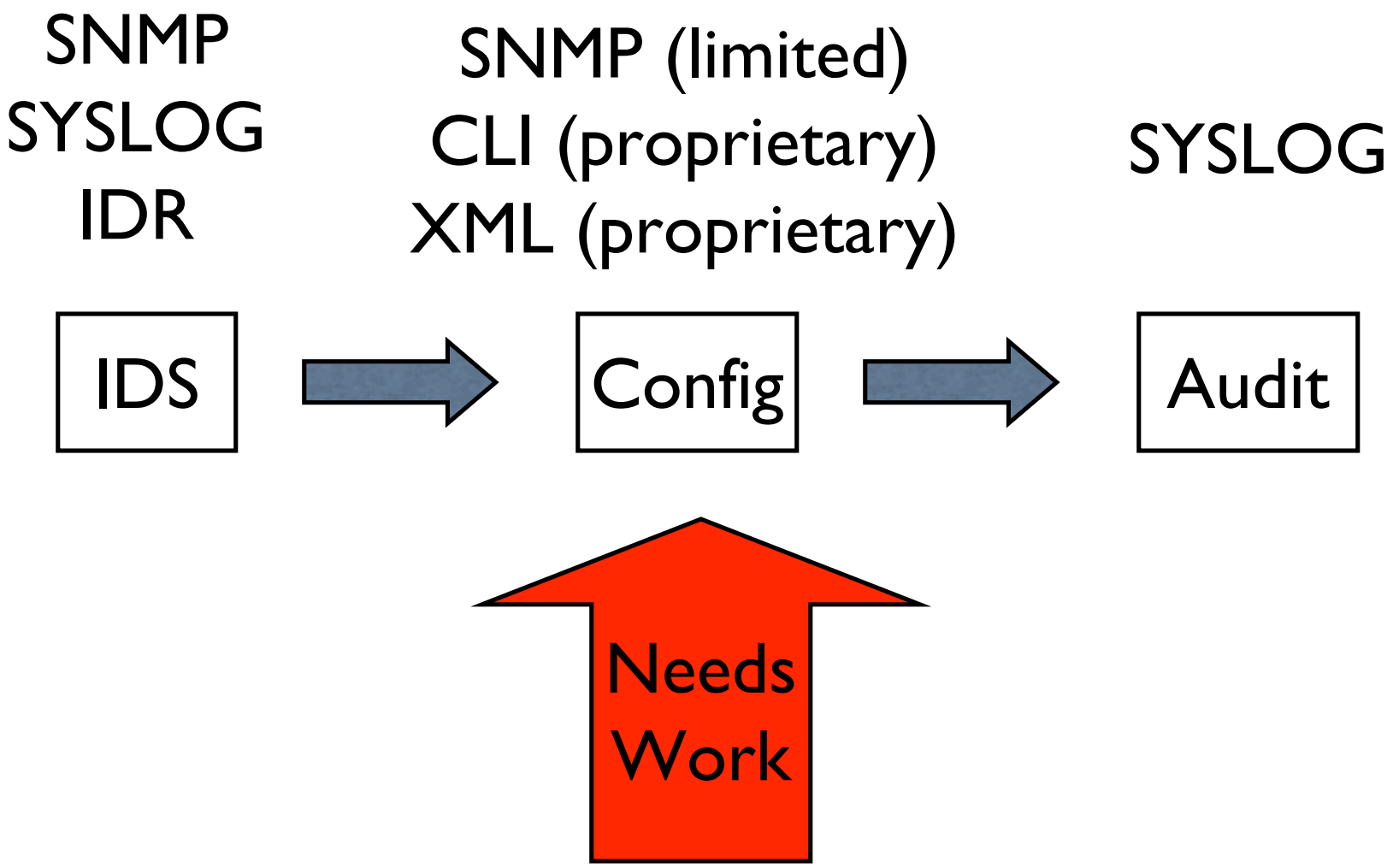


The more it touches your network, the more
You pay for it

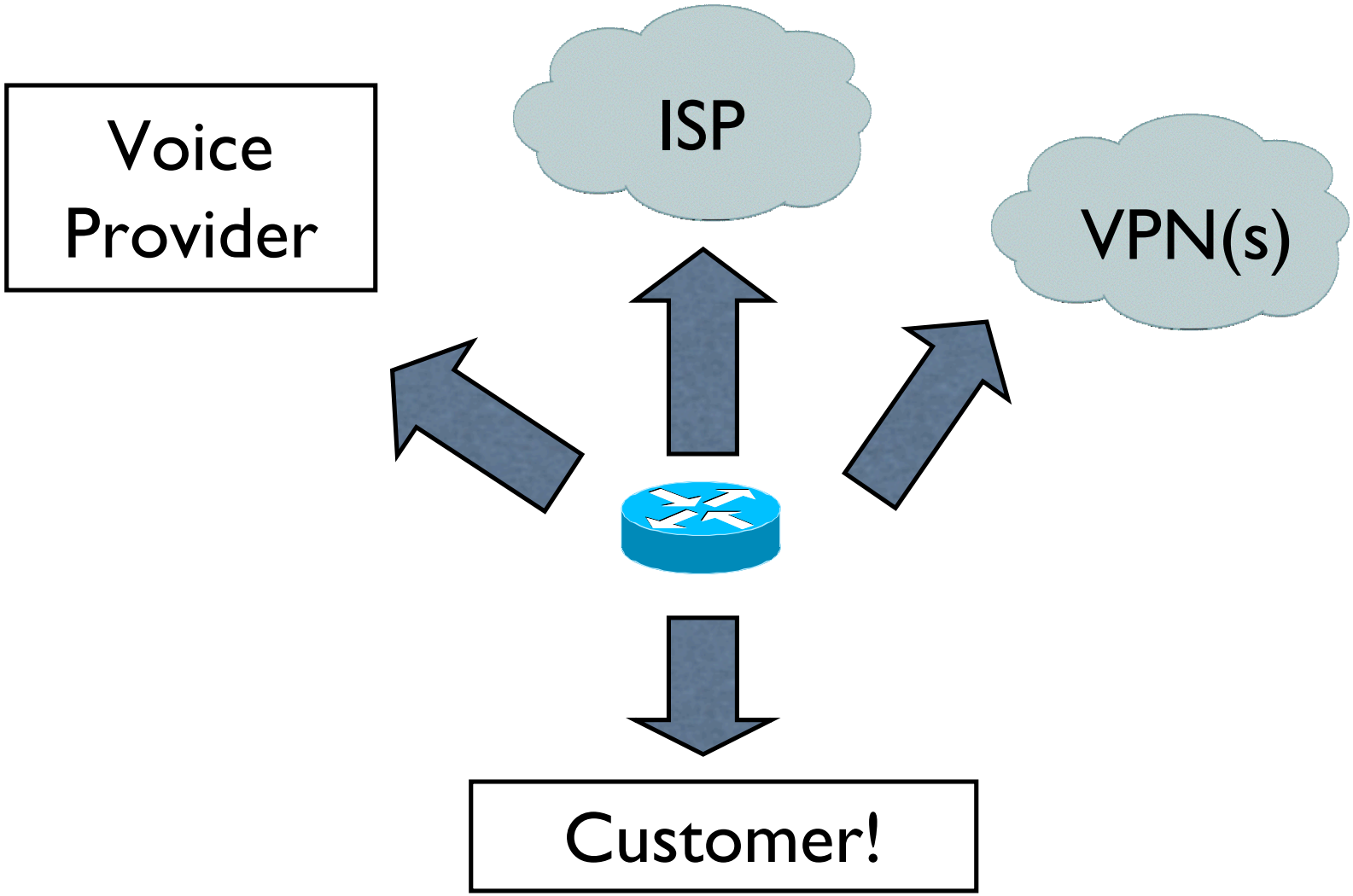
But What's Needed to support that?

How does this system behave with a virus?

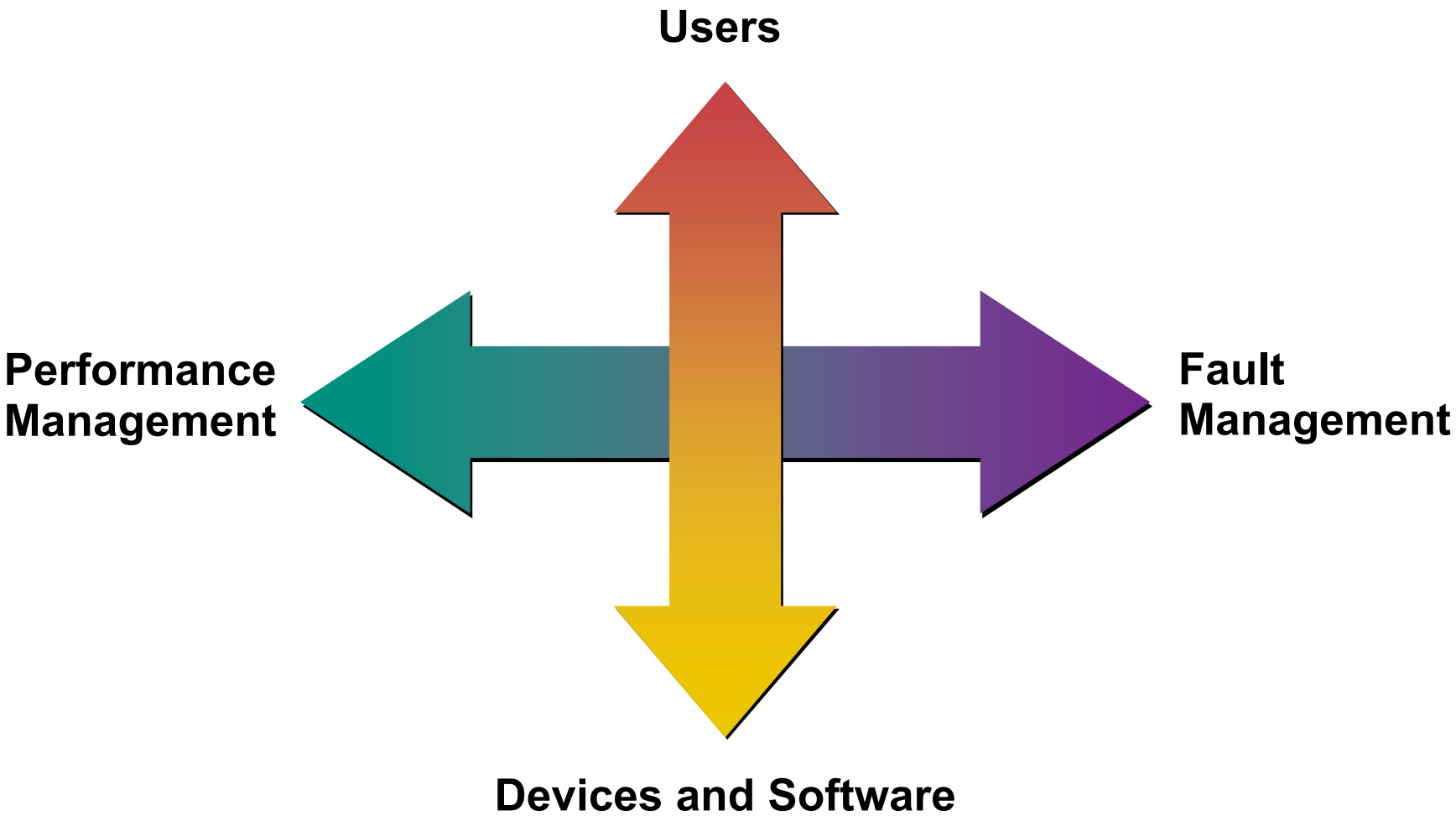
What's the interface?



Remember This?



Performance v. Fault Management

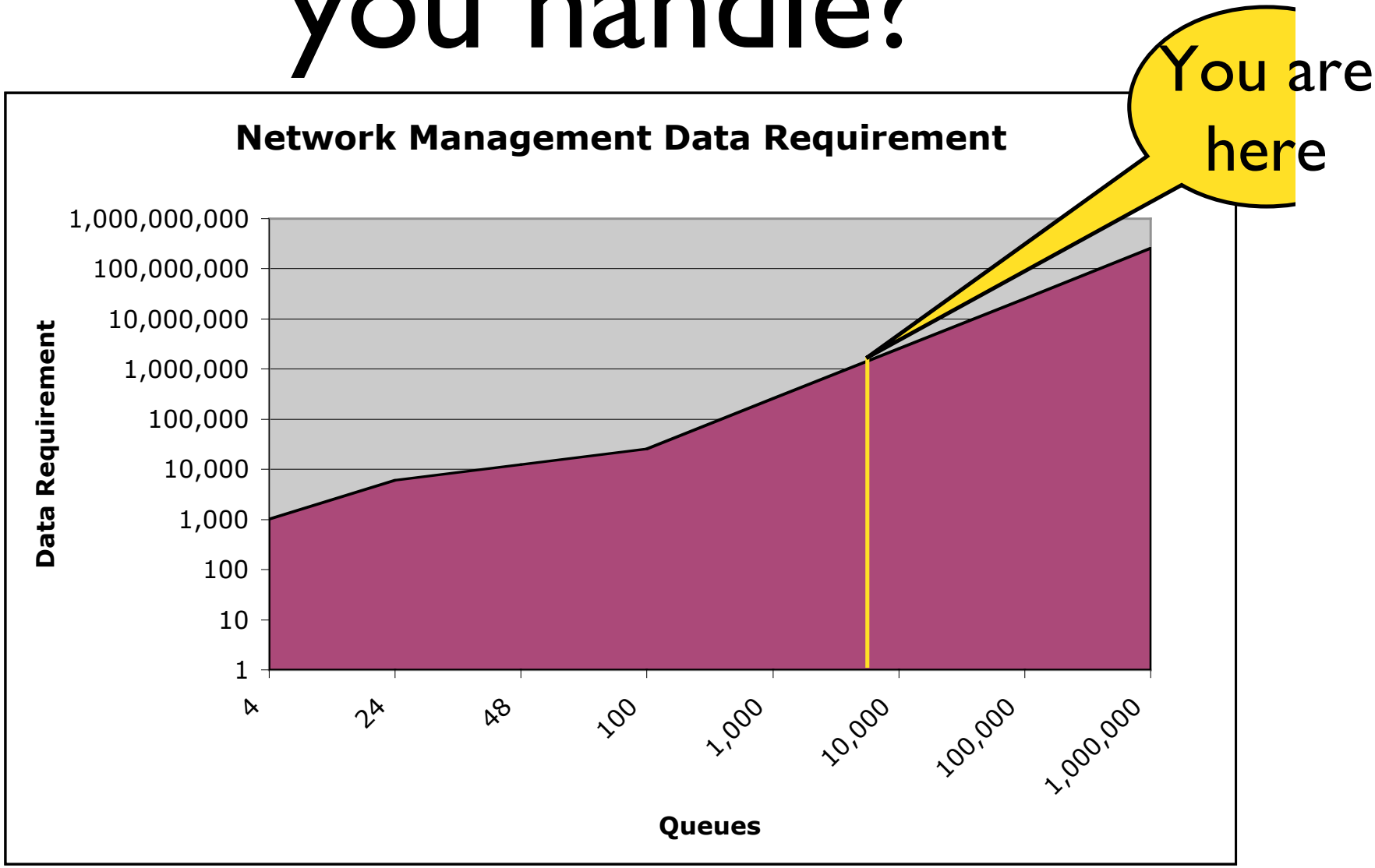


Latency as a detective's tool?

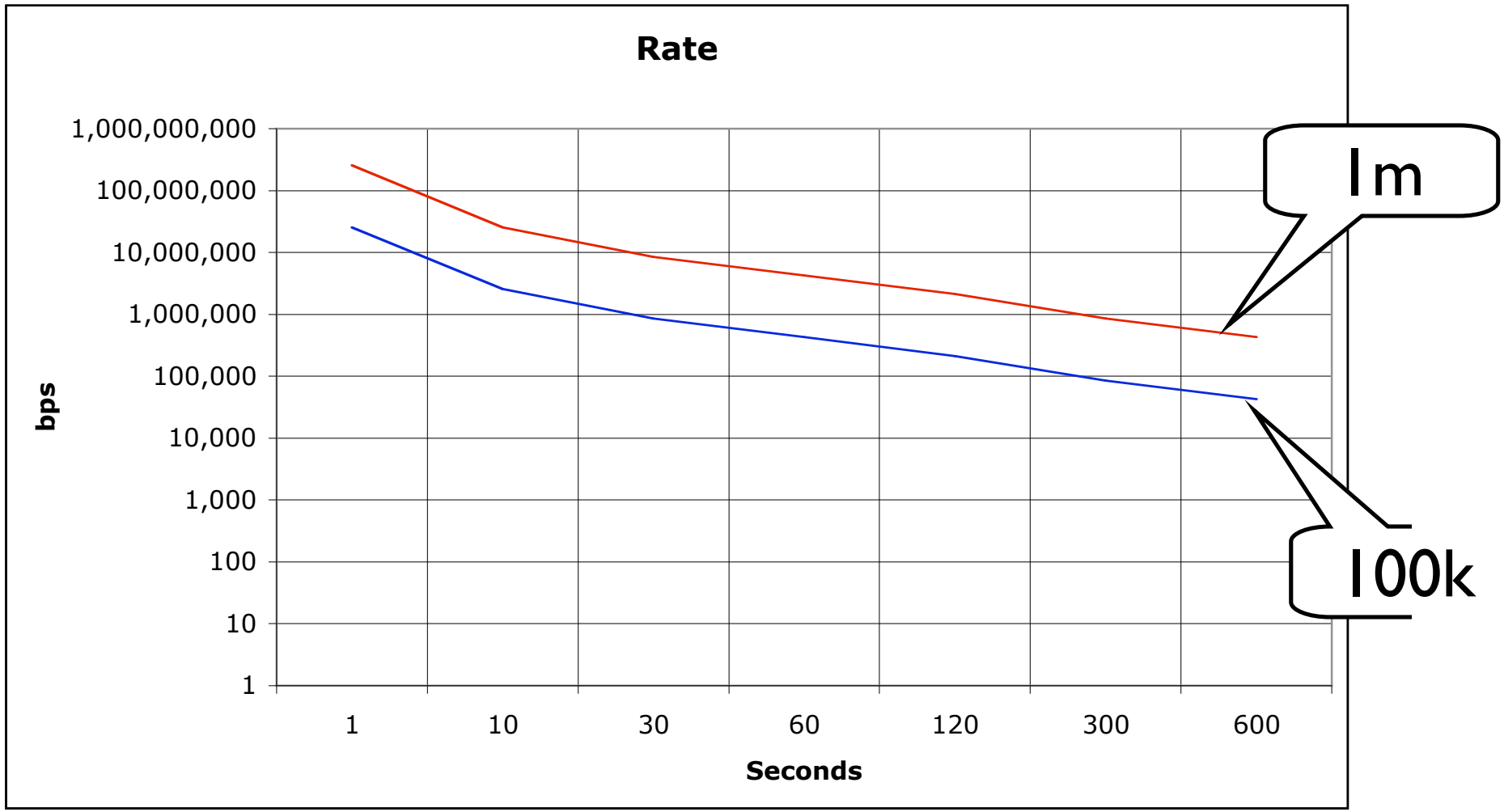
- Latency from New York to London on a clear link should be (round trip) 70ms.
- What happens when it's less than that?!
- A violation of the law of physics is a clear sign of an anomaly.

Latency between two points has an expected value. But is it worth checking?

How much data can you handle?



Data Processing Rate



Configuration Management

And then there's my car

Common Features

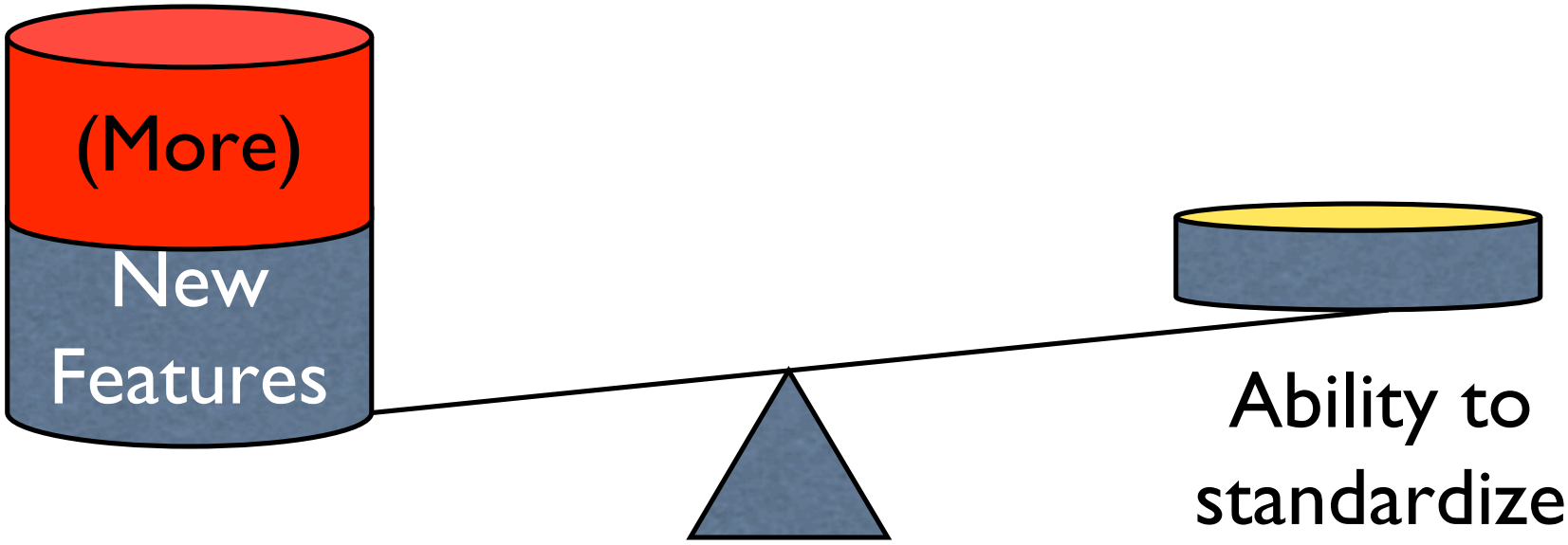
- Steering wheel
- Clutch, as & brake pedals
- Four doors
- Mirrors
- Ignition Key

If you can drive one, you can drive the other

“Differentiators”

- Automatic windshield wipers on right stalk
- Cruise control on lower left stalk.
- “Improved” turn-signal control
- Six speed
- Traction control system
- Information management system

Why we're not there?



Technologies Mature

- UNIX has had over 30 years to mature.
  - POSIX works great away from h/w
- IP management is a bit behind.
- This is not entirely bad.

*NIX

Configuration Components	How?
Passwd/group information	Shadow / Kerberos / LDAP
Standard Tasks	Cron / AT
Application Components (sendmail, http)	Small number of well known configuration languages
User Configuration	~/.{files}
Device configuration	??? -- maybe /etc/sysconfig or /proc ???

And with Network Elements?

- IP addresses, subnet masks of interfaces
- Basic routing parameters for routers
  - BGP neighbors, IGP configuration
- Basic SNMP configuration

Far more is still proprietary!

Config. Standards Progression

Date	What	Purpose
CLI	1970s	Everything
SNMPv1	1988	Monitoring
TL.1	1980s	Config & Monitoring
SOAP/XML/ WSDL	1999-now	RPC

XML What?!

- Just <>s without common schema
- Common schema is hard

  -- getting this right will take years
- And we need aSTANDARD way to transport XML for network management
- We think we have one just about cooked

NETCONF

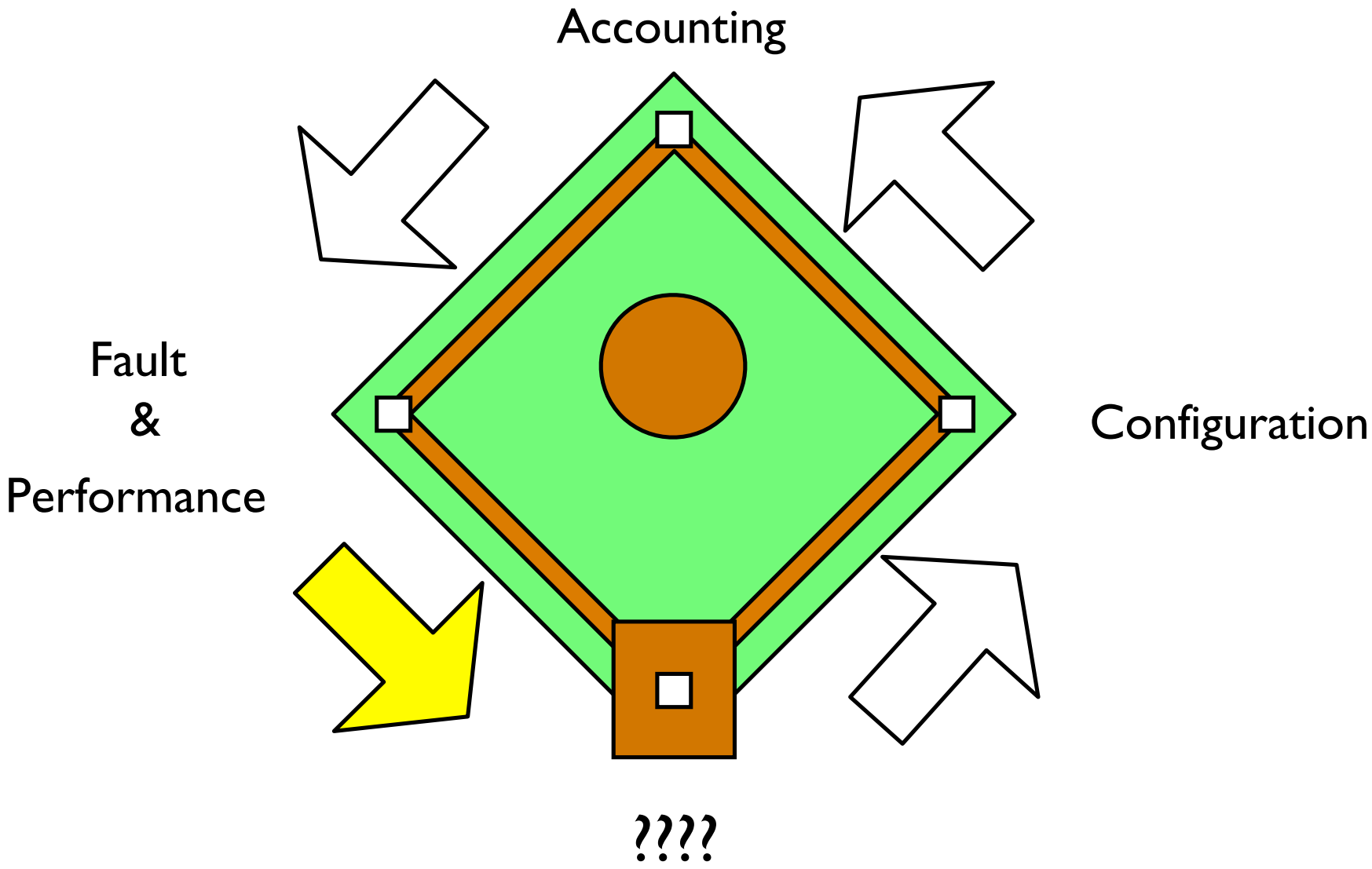
- Uses BEEP for protocol reversability
- Also mapped to SSH for those who prefer it
- Data-model agnostic
- Provides for numerous device operating models (big and small)
- It's not quite done -- we could use help

What to do?

Use the Force.

The Internet Engineering Task Force

What's a home run??



Identity Management

- Inside the company we do well
- Consumers are feeling the pain
  - Multiple passwords for numerous services
  - Identity theft
  - Loss of privacy

Getting In to My Bank

+

+ 8 digit user name
+ challenge / response
+ PIN

This might be okay if it were **just** my bank.

Unified Identities: Many Have Tried!

- Major PC OS vendors
- Large Phone manufacturers
- Small Password Protection Programs
- International credit card companies

Each wants to be king of the mountain

Start Small, Grasshopper

- Standard username/password interface?
- Let the users control access to their identities
- Maybe work with smart card folk to standardize secure interface
- Maybe listen to Bruce Schneier talk more

If we solve this one, maybe we solve spam.

What I'm saying…

- Too much of anything (data) is a BAD thing
  - We need to figure better ways to aggregate and reduce
- Some linkage is still missing for automation
  - Provisioning is hard (still) but not impossible
- Security Management and Network Management are very tightly related
- Expect more from your local router
- We're awash in keys!

Thanks for your time and help.