Introduction to Internet Measurement: What, Where, Why and How

Nina Taft

Technicolor Research Palo Alto

Outline

Motivation & Ecosystem

Quick examples of where and why

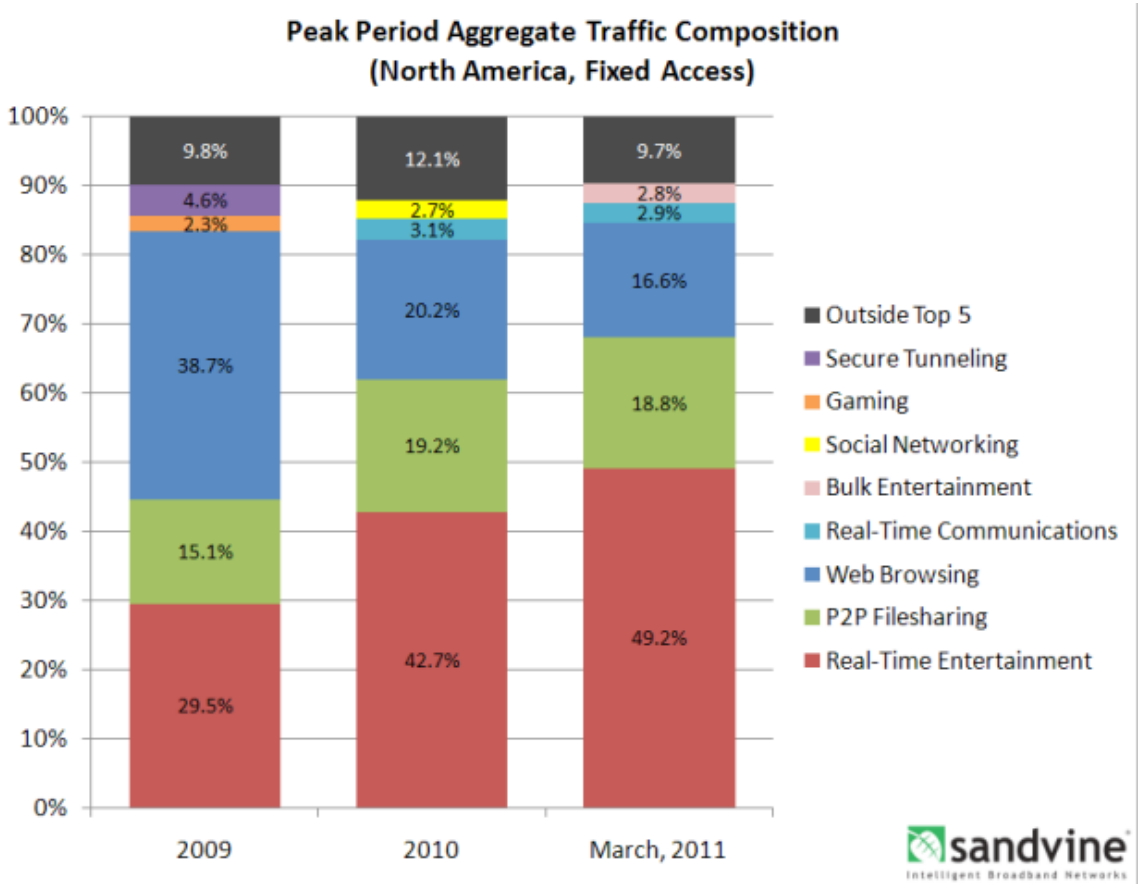
Areas

- traffic
- performance
- topology
- security
- traffic matrices

Summary

Why measure the internet? (1/3)

Cool things to learn



Who wants to know?
- business
- commercial

Slide source: http://techcrunch.com/2011/05/17/netflix-largest-internet-traffic/

technicolor

Why measure the internet (2/3)

Just to understand

Why won't the web page download ?

Why is my netflix movie so slow ?

Who wants to know?
- users !!

Why measure the internet ? (3/3)

Planning for the future

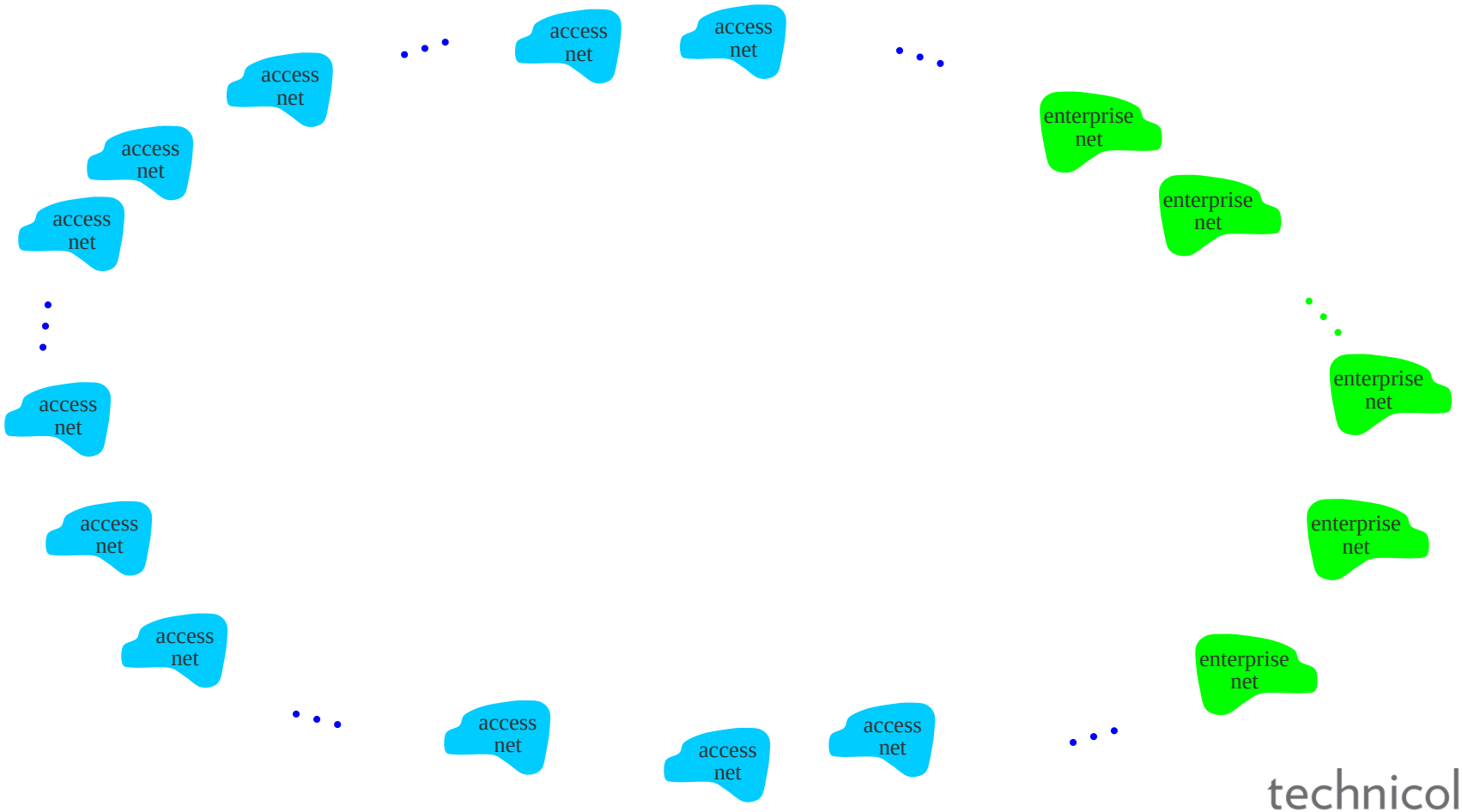
Cisco predictions for 2016:

- **Global IP traffic will reach 1.3 zettabytes per year**
- **The gigabyte equivalent of all movies ever made will cross global IP networks every 3 minutes.**
- **Number of devices connected to IP networks will be nearly three times as high as the global population**

Who wants to know?
- service providers

How is the Internet structured?

How to connect thousands of access service providers, and enterprises?

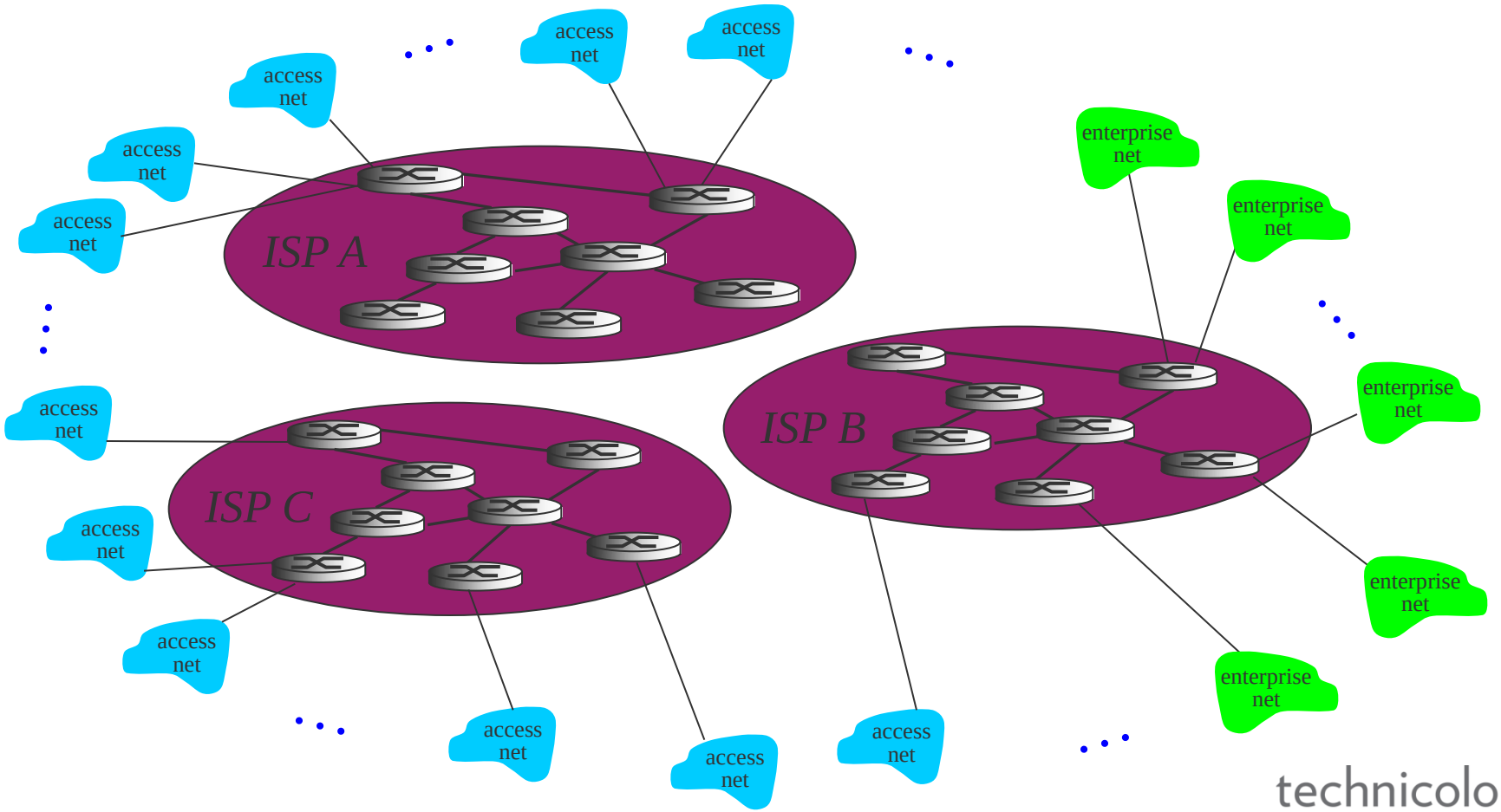


Slide source: http://www-net.cs.umass.edu/kurose-ross-ppt-6e/

technicolor

Internet structure

Access Internet Service Providers (ISP) connect to a global transit ISP.
Customer and provider ISPs have economic agreement.

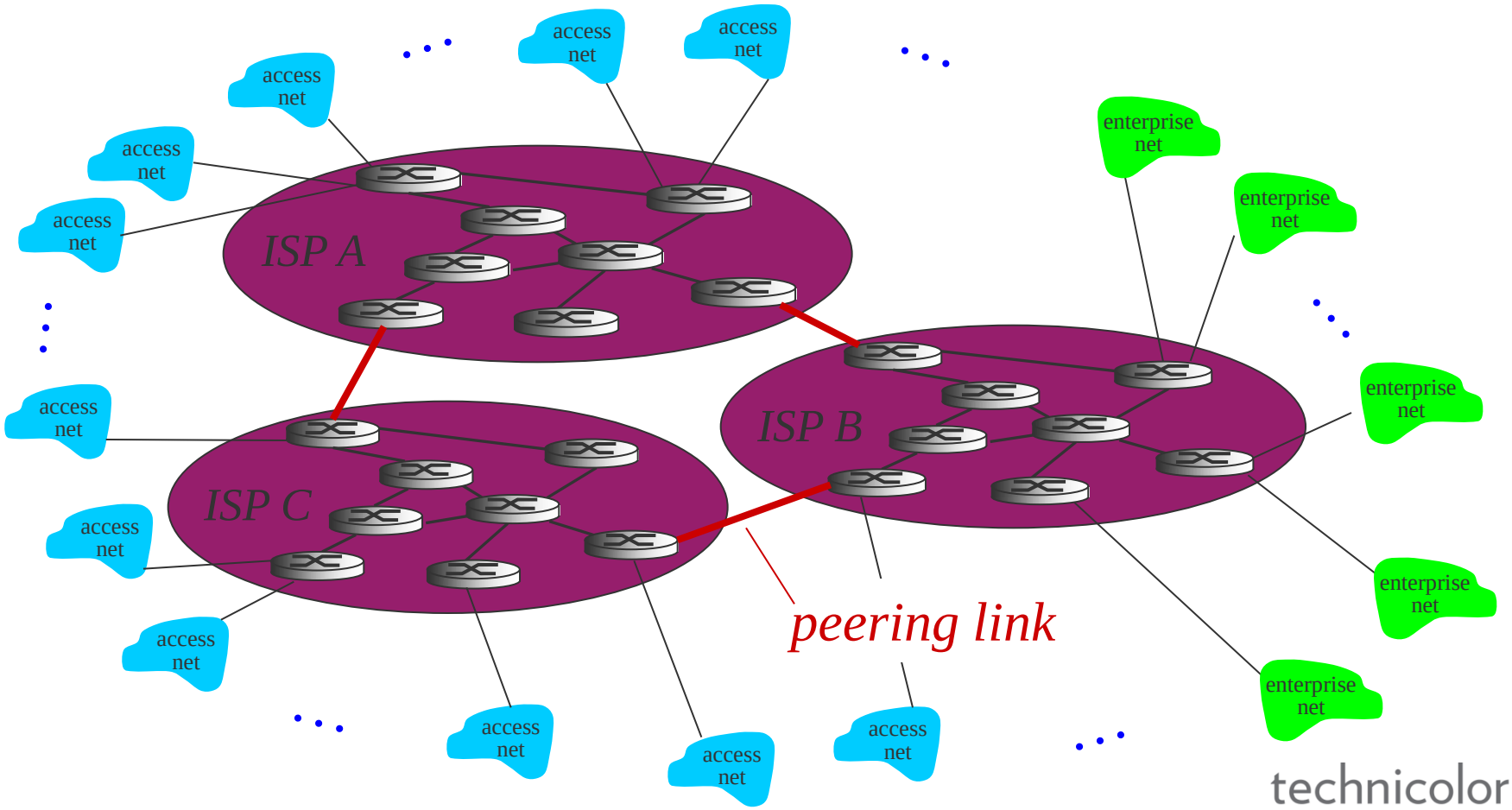


Slide source: http://www-net.cs.umass.edu/kurose-ross-ppt-6e/

technicolor

Internet structure

Global ISPs must be interconnected

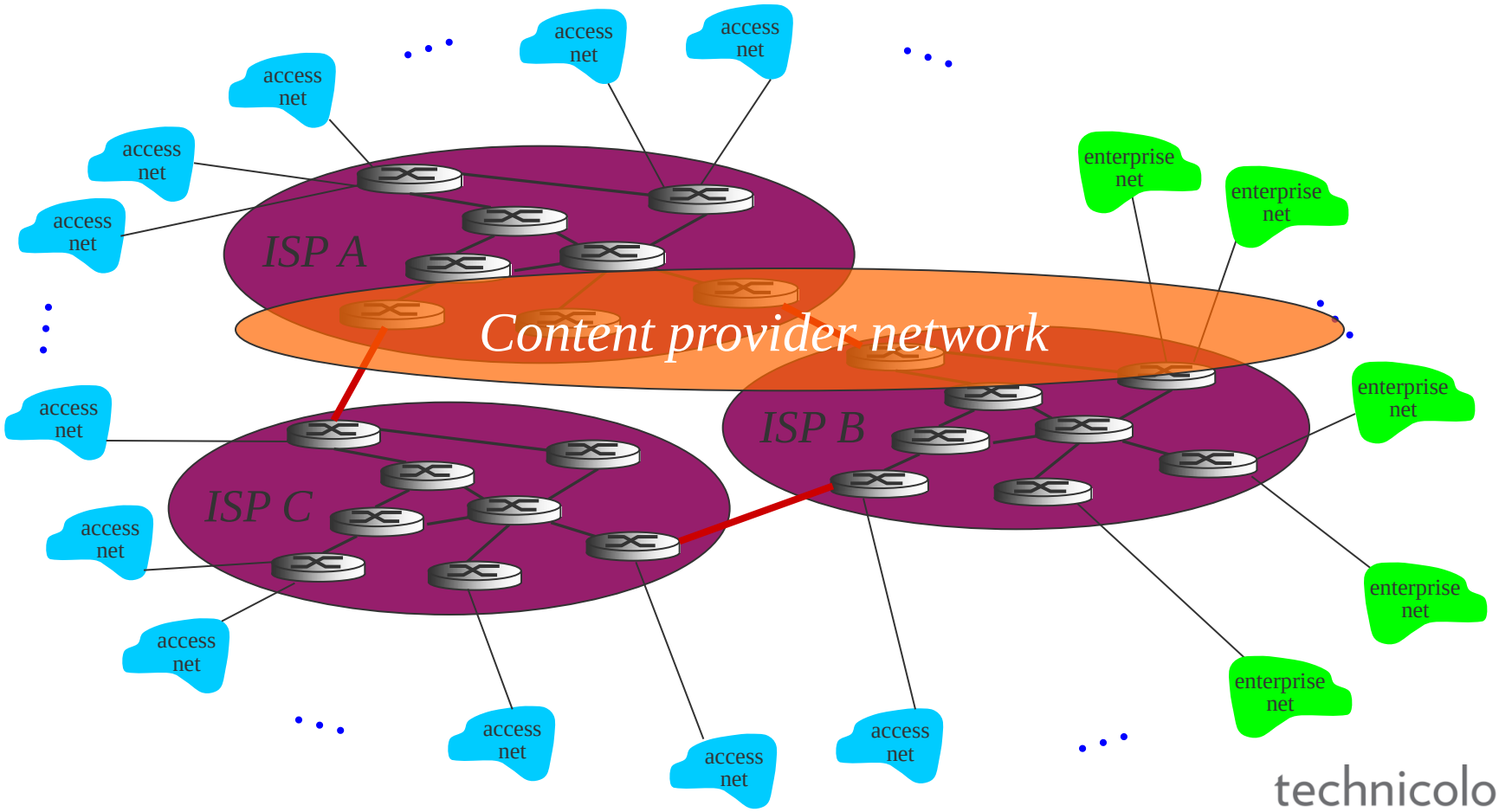


Slide source: http://www-net.cs.umass.edu/kurose-ross-ppt-6e/

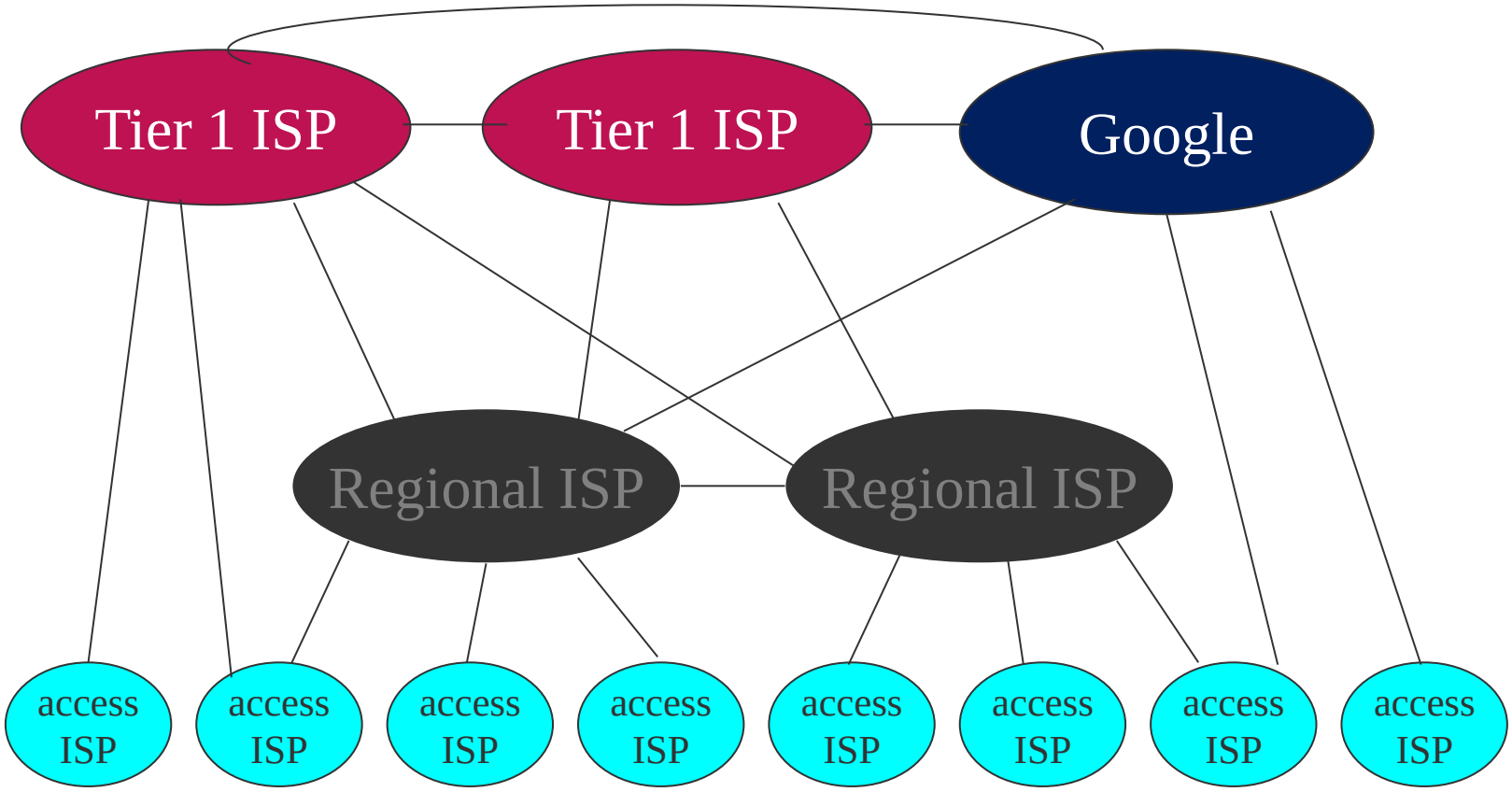
technicolor

Internet structure

Content provider networks (e.g., Google, Microsoft, Akamai) may run their own network,

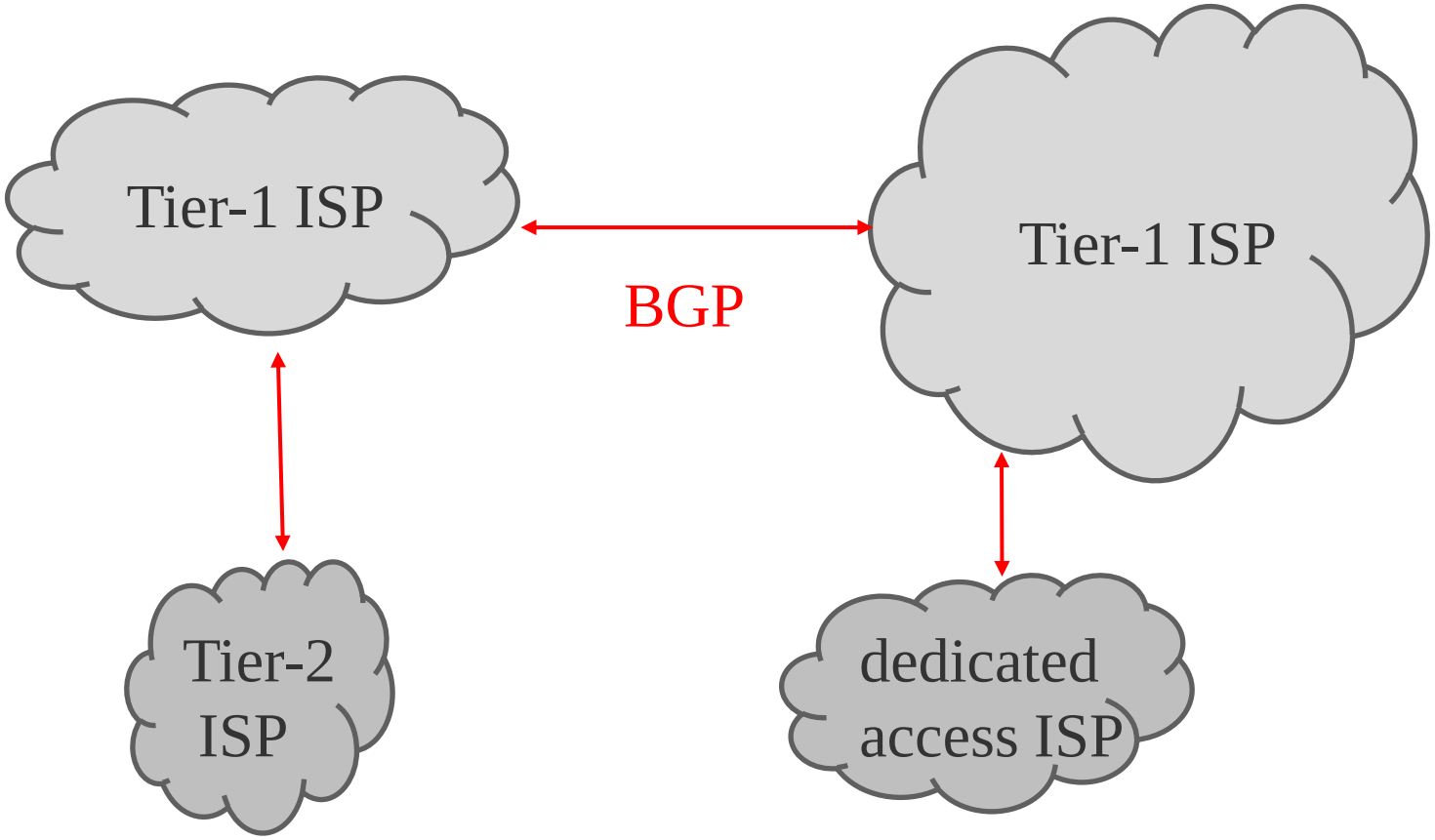


Internet structure: network of networks



Slide source: http://www-net.cs.umass.edu/kurose-ross-ppt-6e/

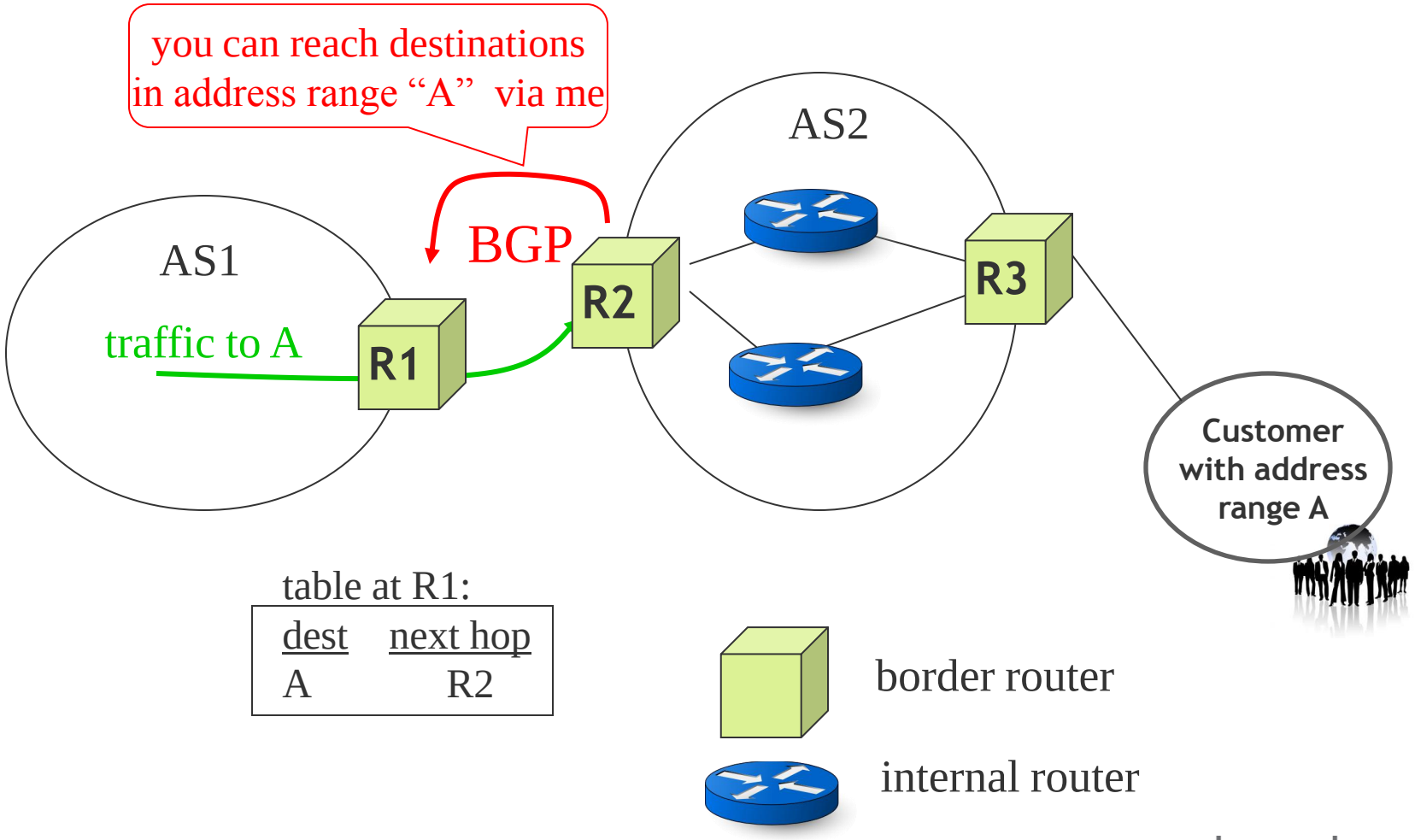
Communication between service providers



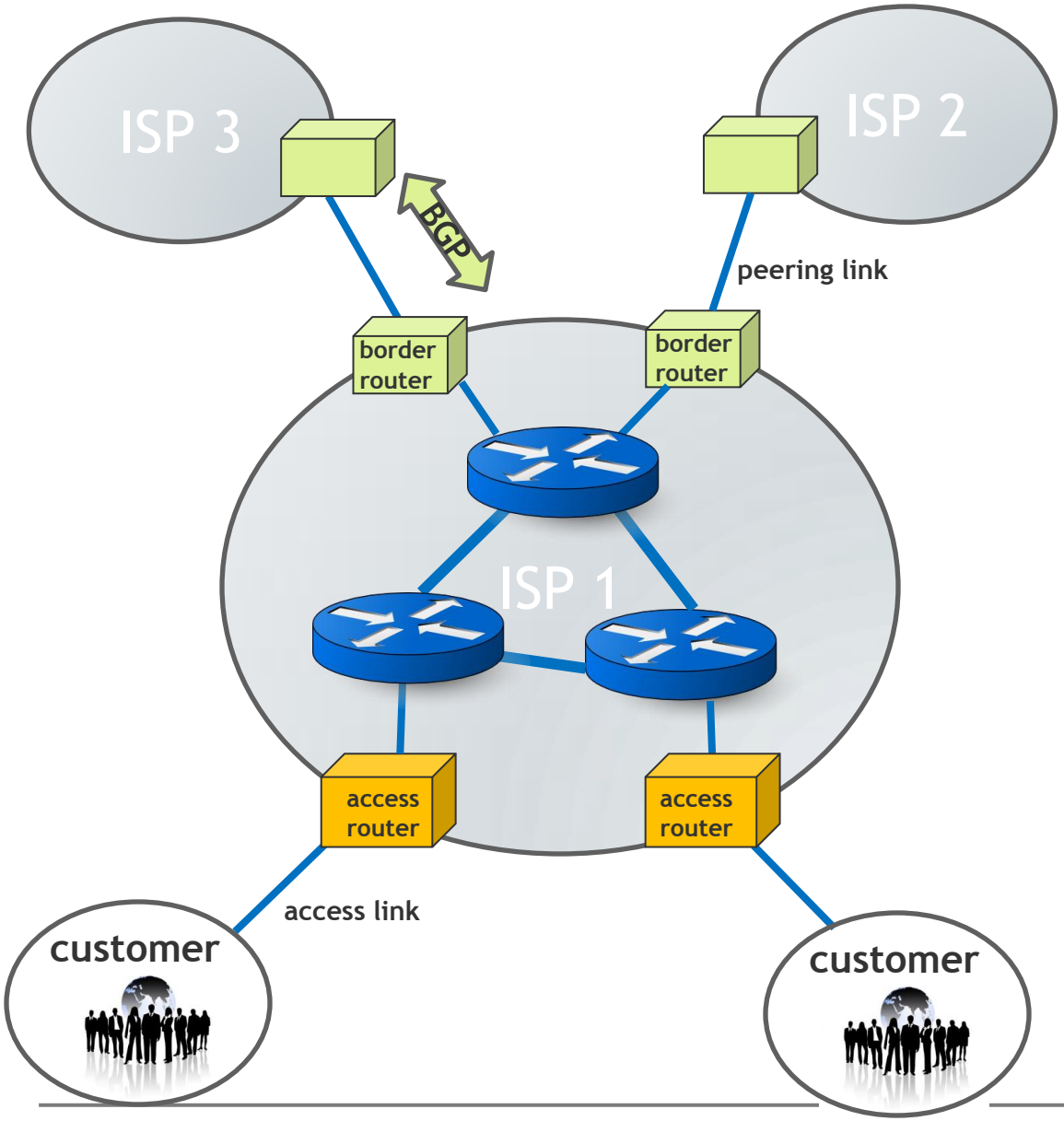
- AS (Autonomous System) - a collection of routers under the same technical and administrative domain.
- BGP (Border Gateway Protocol) - used between two AS's to allow them to exchange routing information so that traffic can be forwarded across AS borders.

A word about BGP

Purpose: to share connectivity information



Network structure within one ISP



technicolor

So the internet structure is super complicated!

What should we measure?

Where should we measure?

How do we capture data?

It all depends upon what you want to do with the data !

Outline

Motivation & Ecosystem

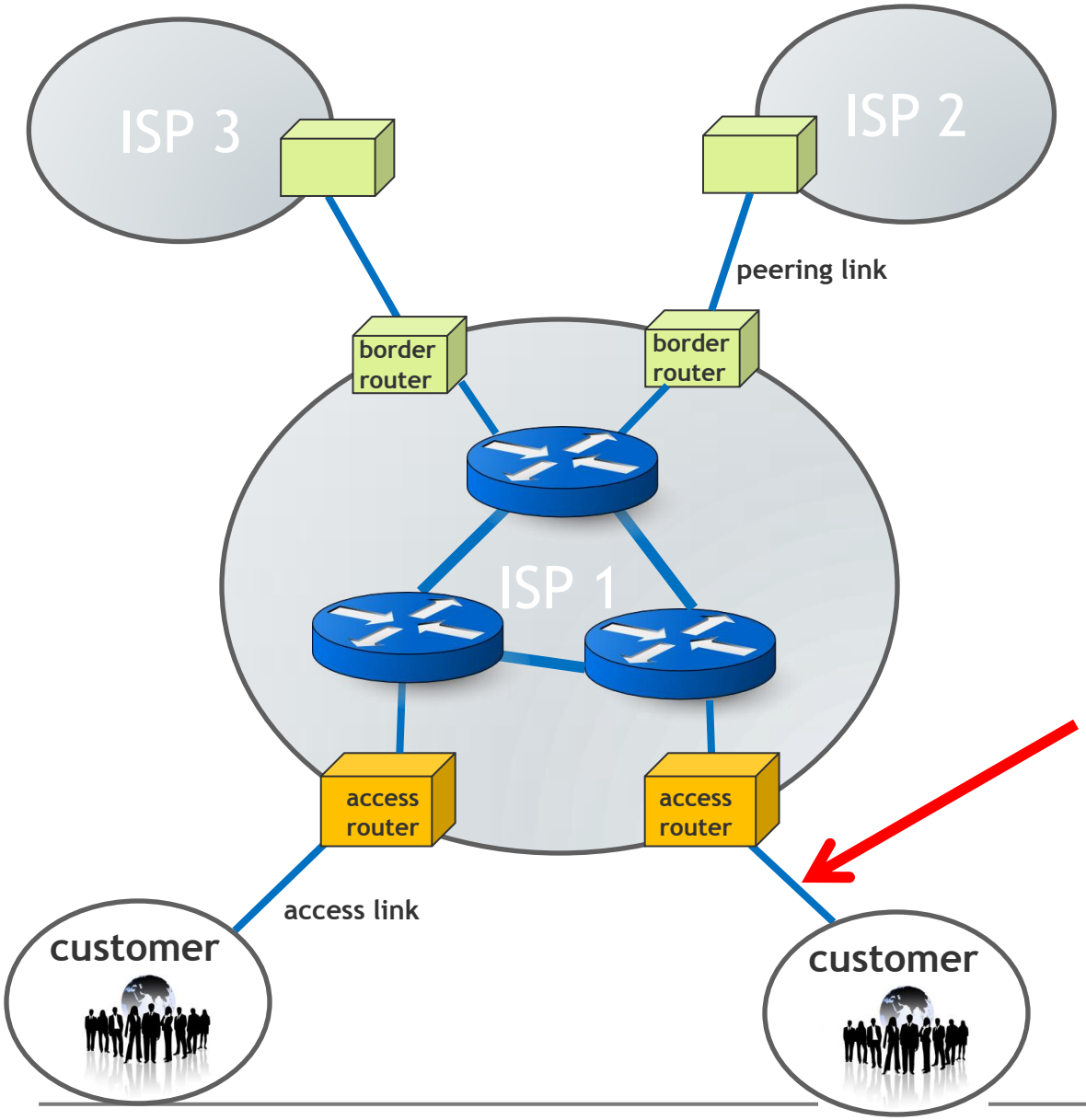
Quick examples of where and why

Areas

- traffic
- performance
- topology
- security
- traffic matrices

Summary

Where measure ? And why ? (1/5)

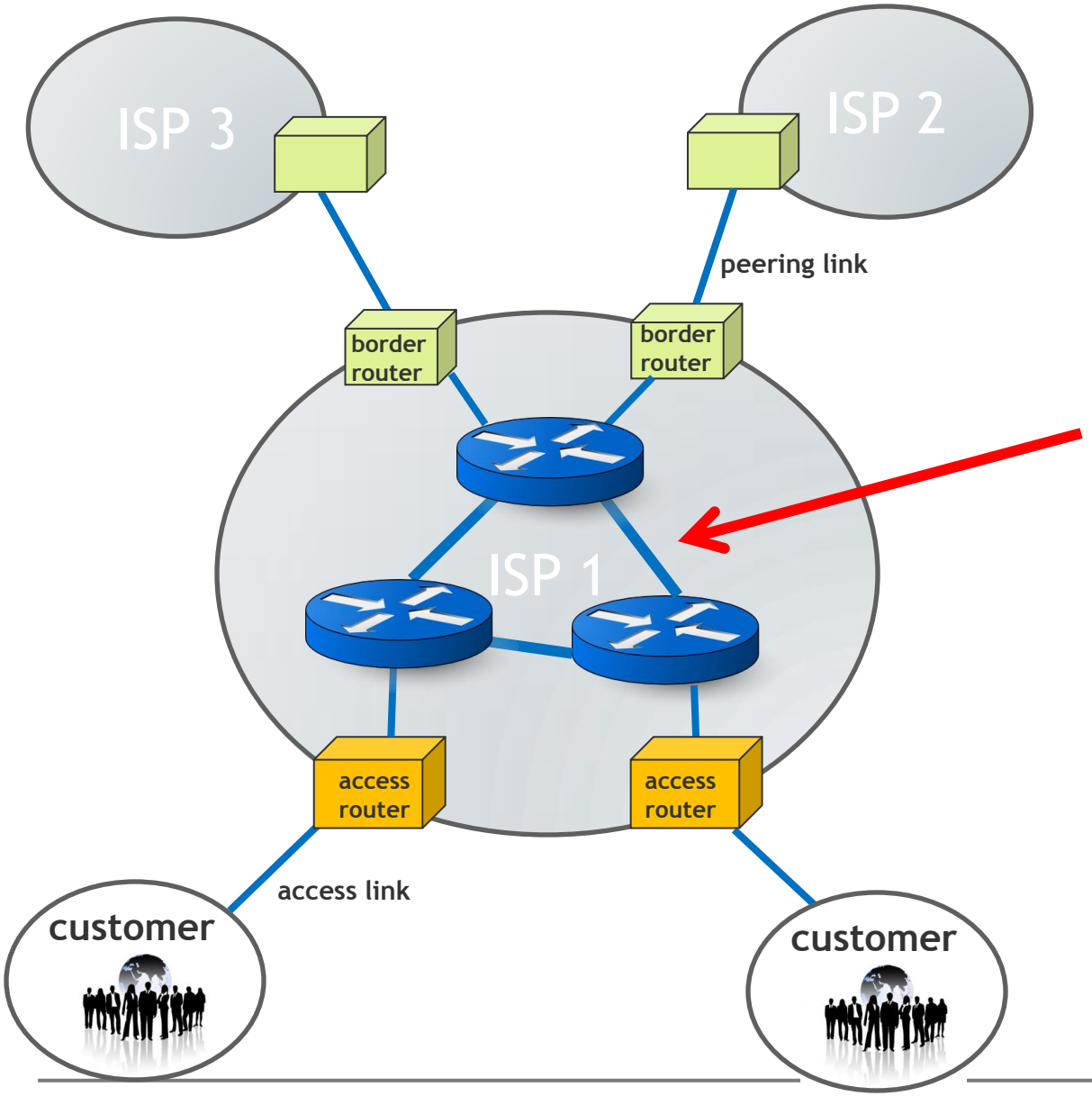


Example 1:

What? Ingress traffic at access router.

Why? ISPs can see if their customer traffic is growing, or if there is unwanted traffic

Where measure ? And why ? (2/5)



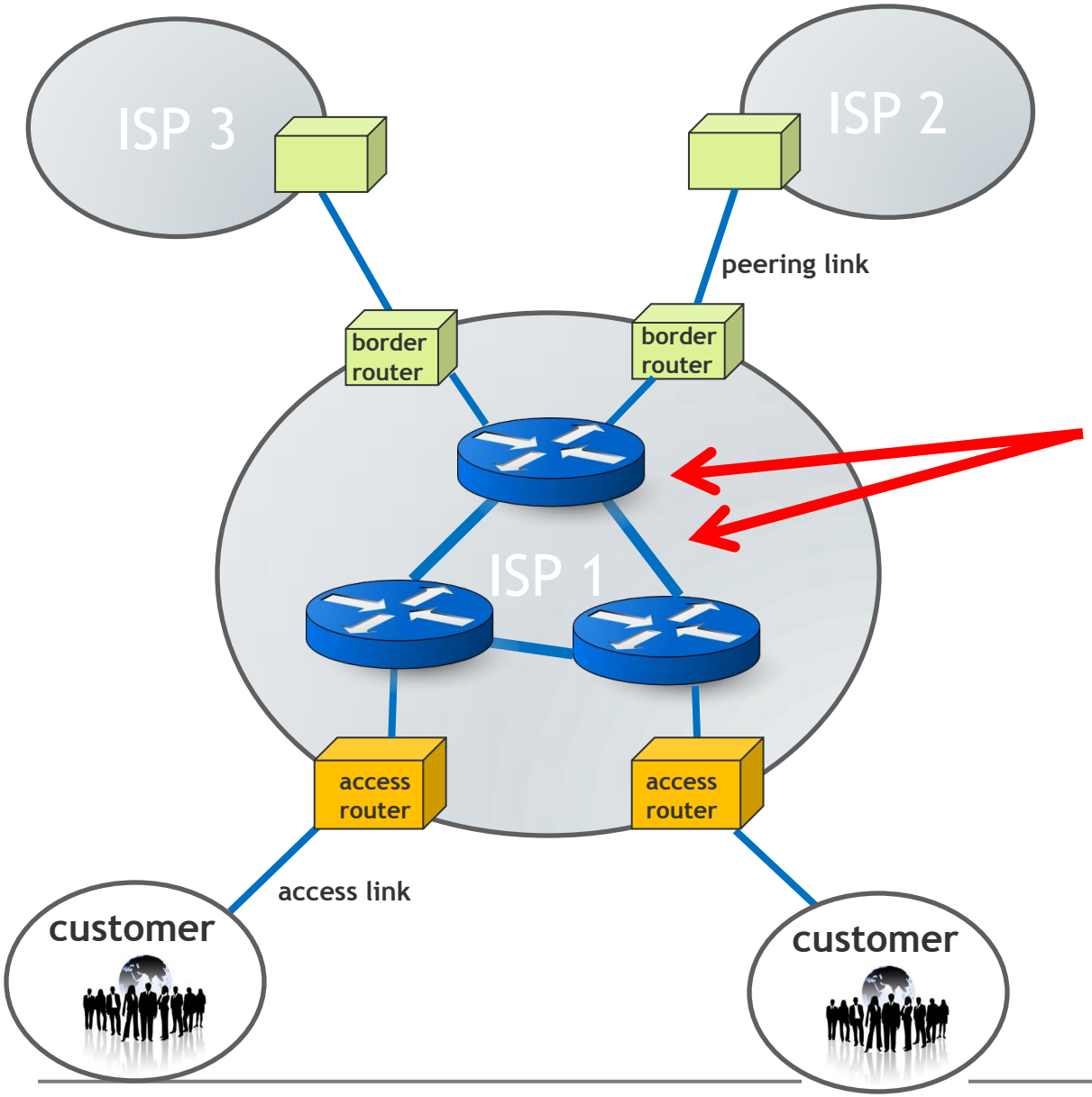
Example 2:

What? Aggregate traffic inside backbone traffic.

Why? ISPs need to know when to upgrade a router, or add a new one; when to upgrade link capacity.

technicolor

Where measure ? And why ? (3/5)

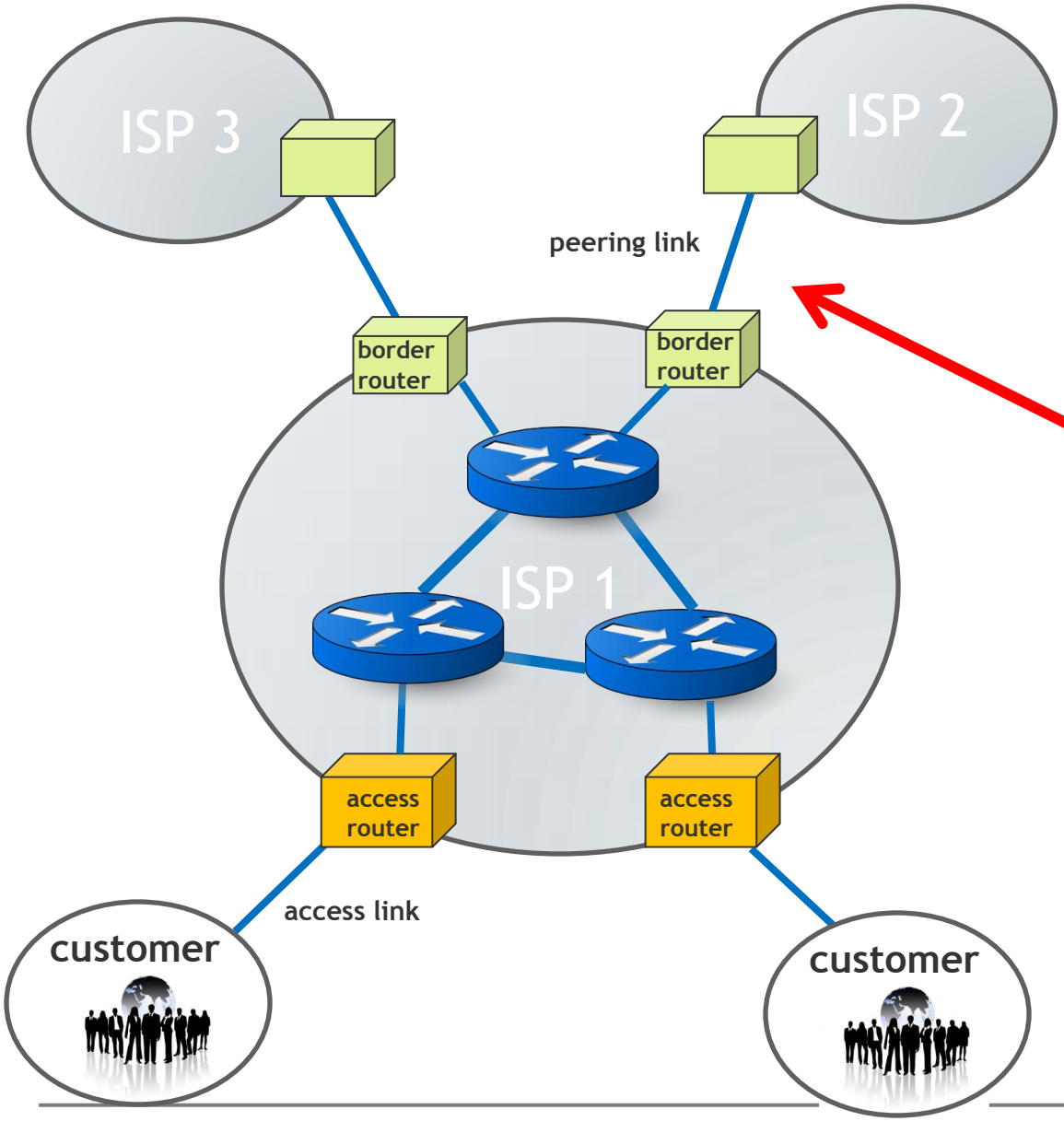


Example 3:
What ? Failures

Why? To know if recover well from outages, and how often they occur

technicolor

Where measure ? And why ? (4/5)



Example 4:
Where ? Peering links

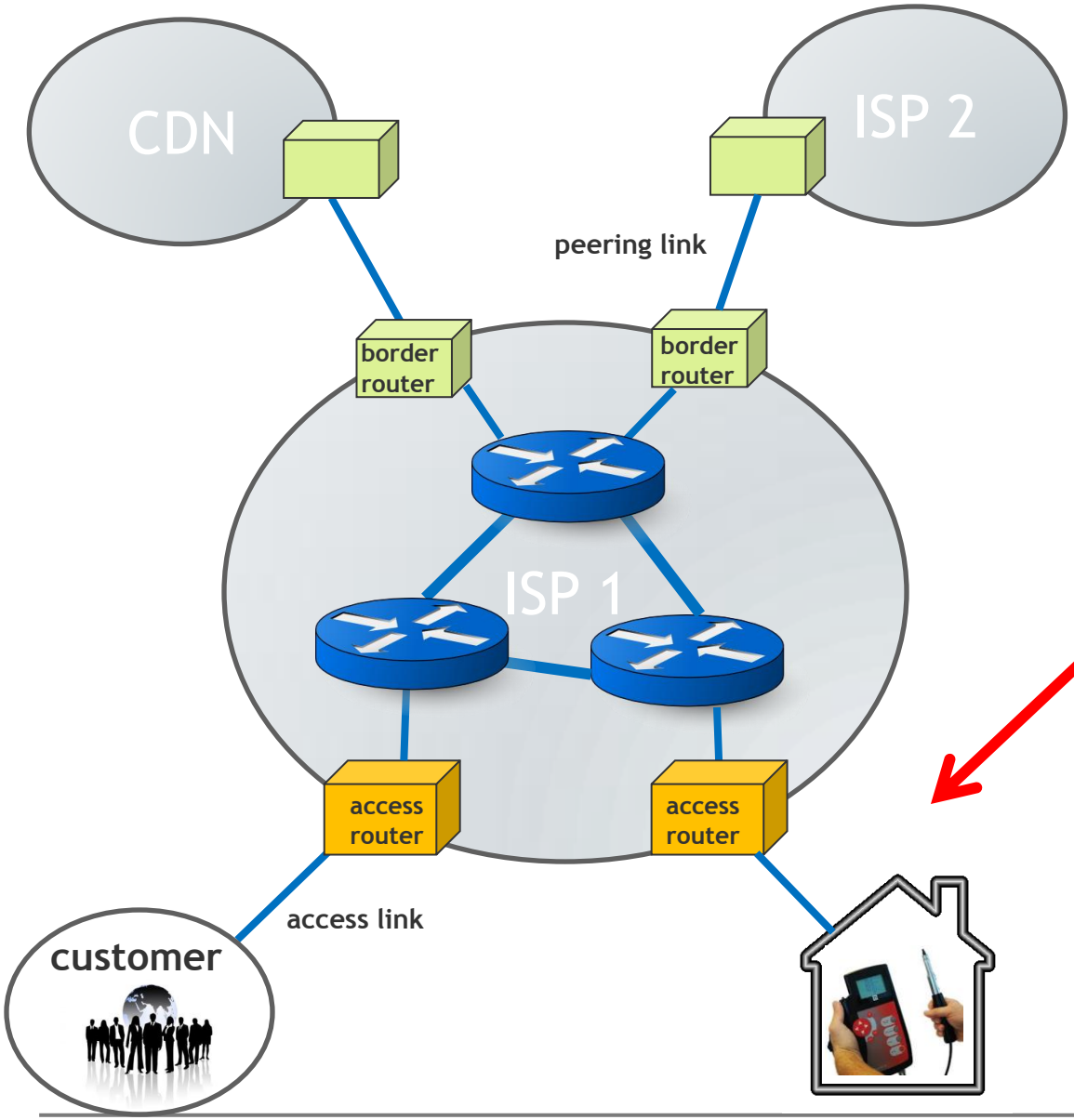
What ? BGP routing announcements

Why ? Learn who is connected to whom

Why ? Make sure no routing loops

technicolor

Where measure ? And why ? (5/5)



Example 5:
Where ? In the home

Why ? Understand performance of a video streaming

technicolor

Measurement is hard! (1/2)

Ecosystem of distributed semi-autonomous systems – no one sees it all !

Even those who regulate it are confused:

> "The Internet .. is not a big truck,
> it is a series of tubes" (former-US senator)

Data ownership and privacy

Measurement is hard! (2/2)

Representativeness:

- Did you get enough samples of – routers? clients? servers? paths? to make general claim about internet ?
- Many things hard to do without access to a large infrastructure. Researchers have created distributed measurement platforms.

Uncertainty principle “observer effect”

- measurements of certain systems cannot be made without affecting the systems

Getting accurate timestamps can be challenging

Two broad categories of measurement techniques

Examples of some well known tools (there are many others)

What \ How	**Passive Methods**	**Active Methods**
Traffic	pcap: packet capture Netflow: flow capture SNMP: per-link data	
Performance		packet-pair probes ping
Topology	routeviews: capture BGP routing table views	traceroute, ping
Security	netflow telescope	

Outline

Motivation & Ecosystem

Quick examples of where and why

Areas

- **traffic**
- performance
- topology
- security
- traffic matrices

Summary

Why do we want to understand traffic?

Link Provisioning

- Diurnal traffic patterns
  - can my network accommodate bursts and peaks?
  - provisioning depends upon aggregate traffic mix
- Compliance with Service-Level-Agreements SLAs
  - delay & loss performance (for example)

Long Term Traffic Trends

- Application mix constantly evolving

Identify abnormalities

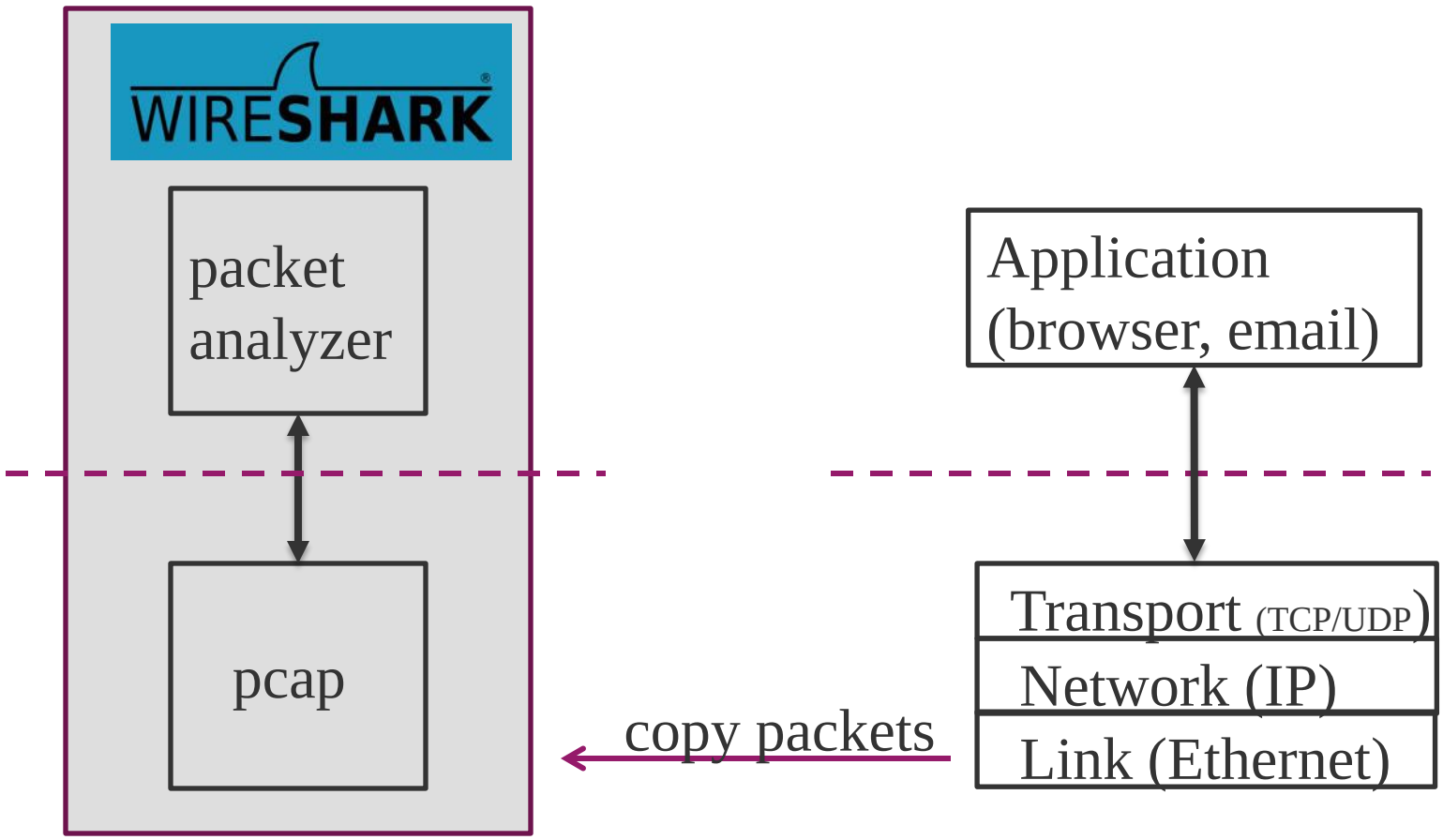
- Failures
- Security

Passive Measurement Tools

For Traffic Measurement

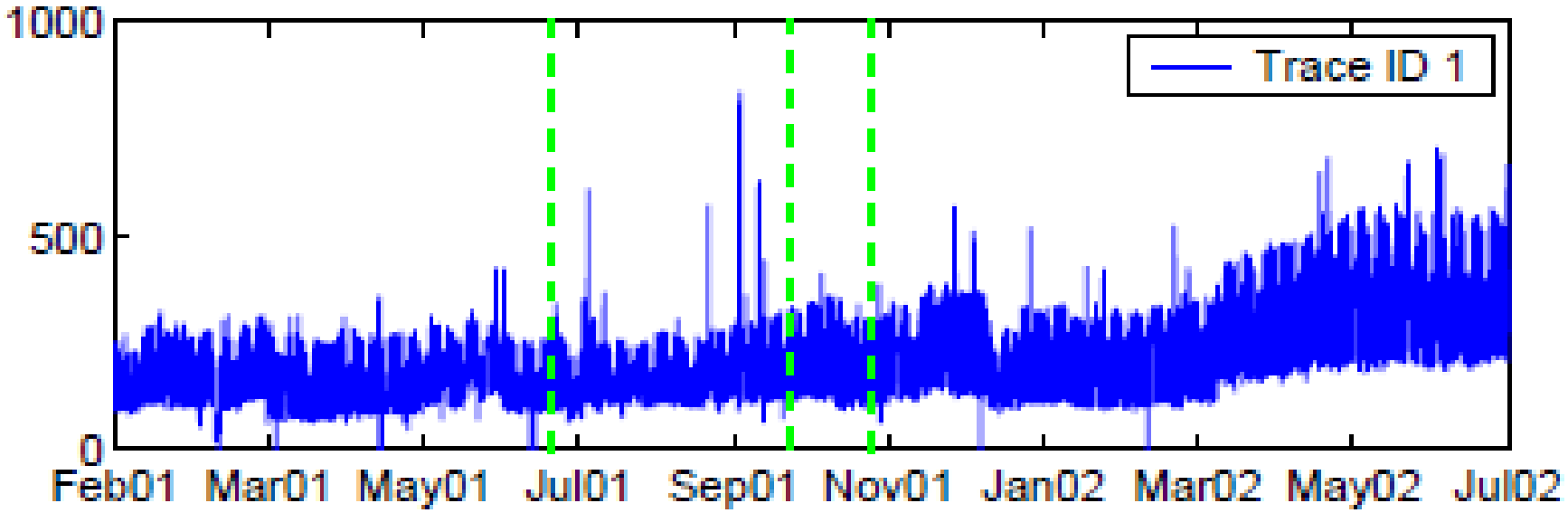
- Approach 1: capture packets
- Example Tools:
  - Libpcap: for general purpose systems
  - OC192MON: specialized hardware for backbone links (~10Gbps)
- Analysis tools: tcpdump & Wireshark
- Approach 2: capture flows
  - Flow commonly defined as “5-tuple”:
    (srcIPaddr, srcPort, dstIPaddr, dstPort, protocol-id)
  - Example Tools: Cisco’s Netflow, Juniper’s cflowd
  - Typical data recorded: start-time, end-time, number of bytes, number of packets
  - Reduced trace size compared to packet capture

Wireshark


WIRESHARK
packet analyzer
pcap
copy packets
Application (browser, email)
Transport (TCP/UDP)
Network (IP)
Link (Ethernet)

WIRESHARK DEMO

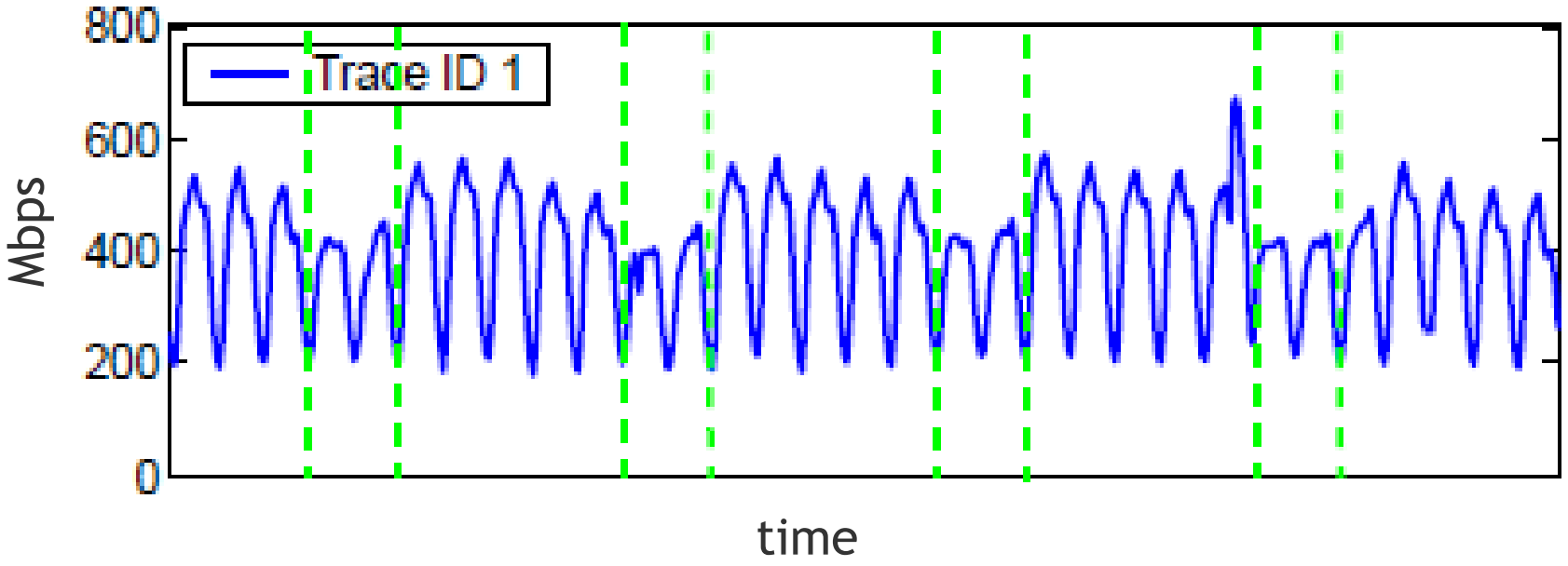
Traffic Trends



Example of backbone traffic in Tier1 ISP

- Average growing over time
- Variability is growing over time
- Spikes present throughout

Traffic Patterns



Timescale: zoom in to one month of previous trace

- We see strong diurnal trends
- Clear periodicities at 24 and 12 hour periods
- Weekdays vs. weekends

Recap on Traffic

Who and Why?

- ISPs collect packets and flows inside their ISPs to better manage their network, and to be ready for the future.
- “pcap” can be put anywhere – an end user can do it from their home; how’s my traffic composition changing?
- Enterprise networks also need to understand corporate traffic

Outline

Motivation & Ecosystem

Quick examples of where and why

Areas

- traffic
- **performance**
- topology
- security
- traffic matrices

Summary

Performance Measurement

What are bandwidth measurements useful for?

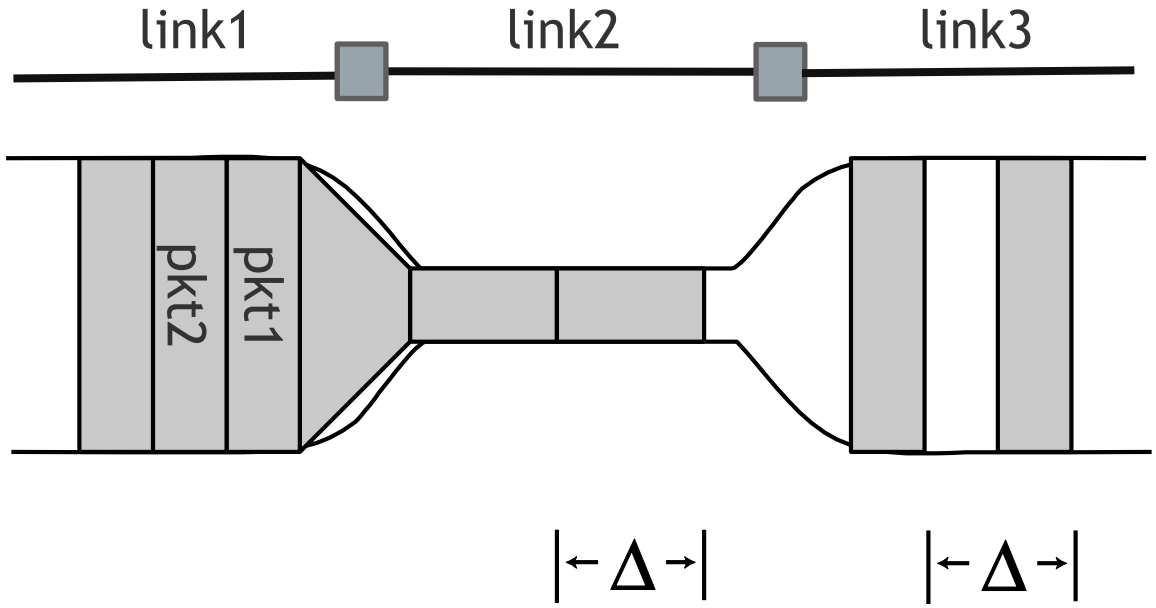
- Applications that adapt their rate accordingly (video streaming)
- Verifying SLA (service level agreements)
- and more

What are latency measurements useful for?

- Usually measures the latency of a path
- Any app that involves choosing among different paths to deliver data: CDNs, P2P, multiuser games, …

Measuring such things often involves a measurement process at multiple places in the network

Example: measure the bottleneck bandwidth of a path



Packets of equal size transmitted back-to-back onto a path

Slowest link creates fixed delay between start of pkt1 and pkt2

When packets leave narrow link, fixed delay Δ is preserved

$$\Delta = \frac{pkt\ len}{capacity} \Rightarrow capacity = \frac{pkt\ len}{\Delta}$$

Image source: courtesy of Mark Crovella @ Boston University

Outline

Motivation & Ecosystem

Quick examples of where and why

Areas

- traffic
- performance
- **topology**
- security
- traffic matrices

Summary

Topology

A way to visualize the interconnection patterns of Internet components

AS graph

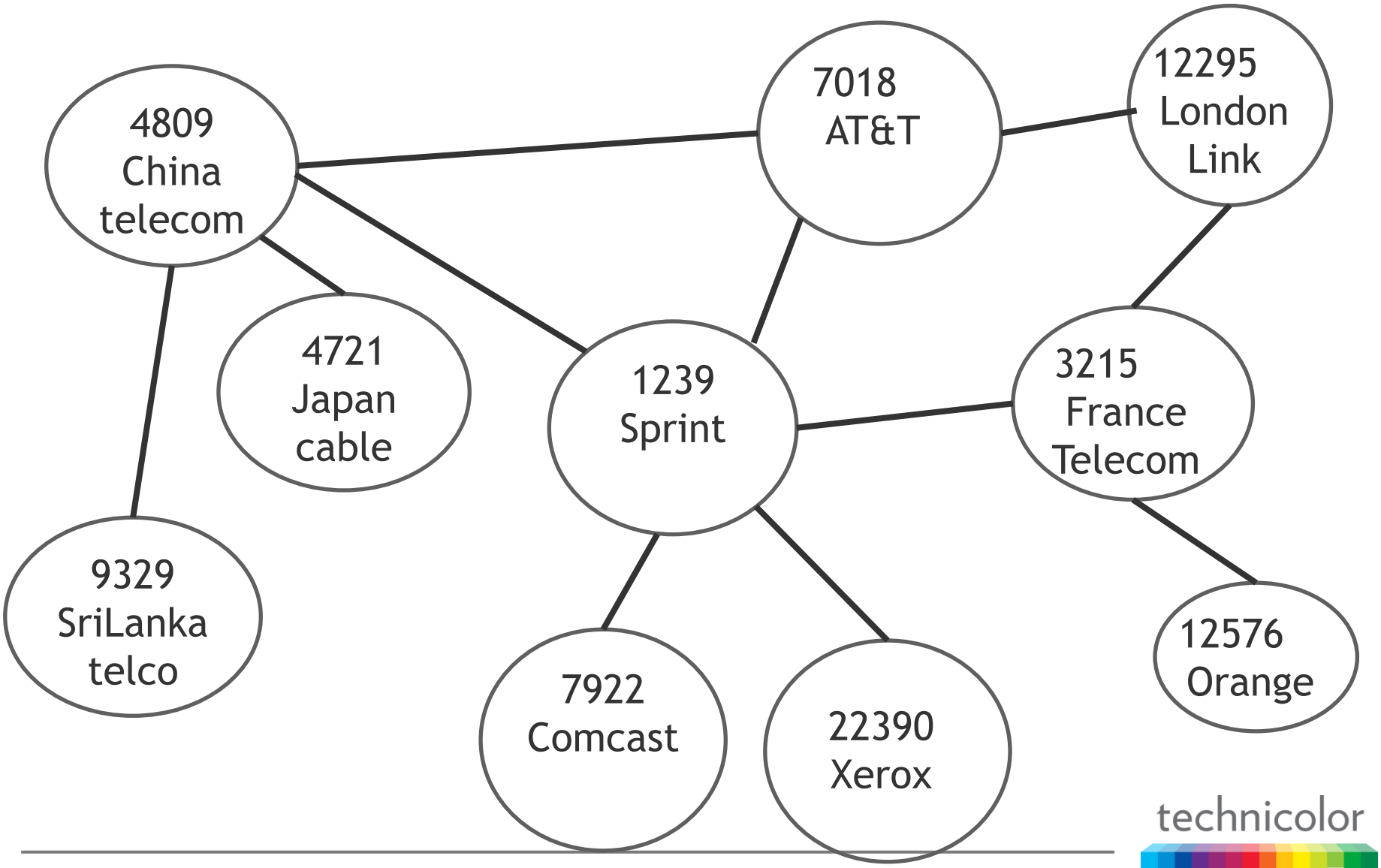
- Interconnection pattern of ASes : each node is an AS, and each edge are peering links (or AS exchange points).

Router-level graph

- Each node is a router, and each edge is a one-hop link between 2 routers. Can annotate edges with link capacity.

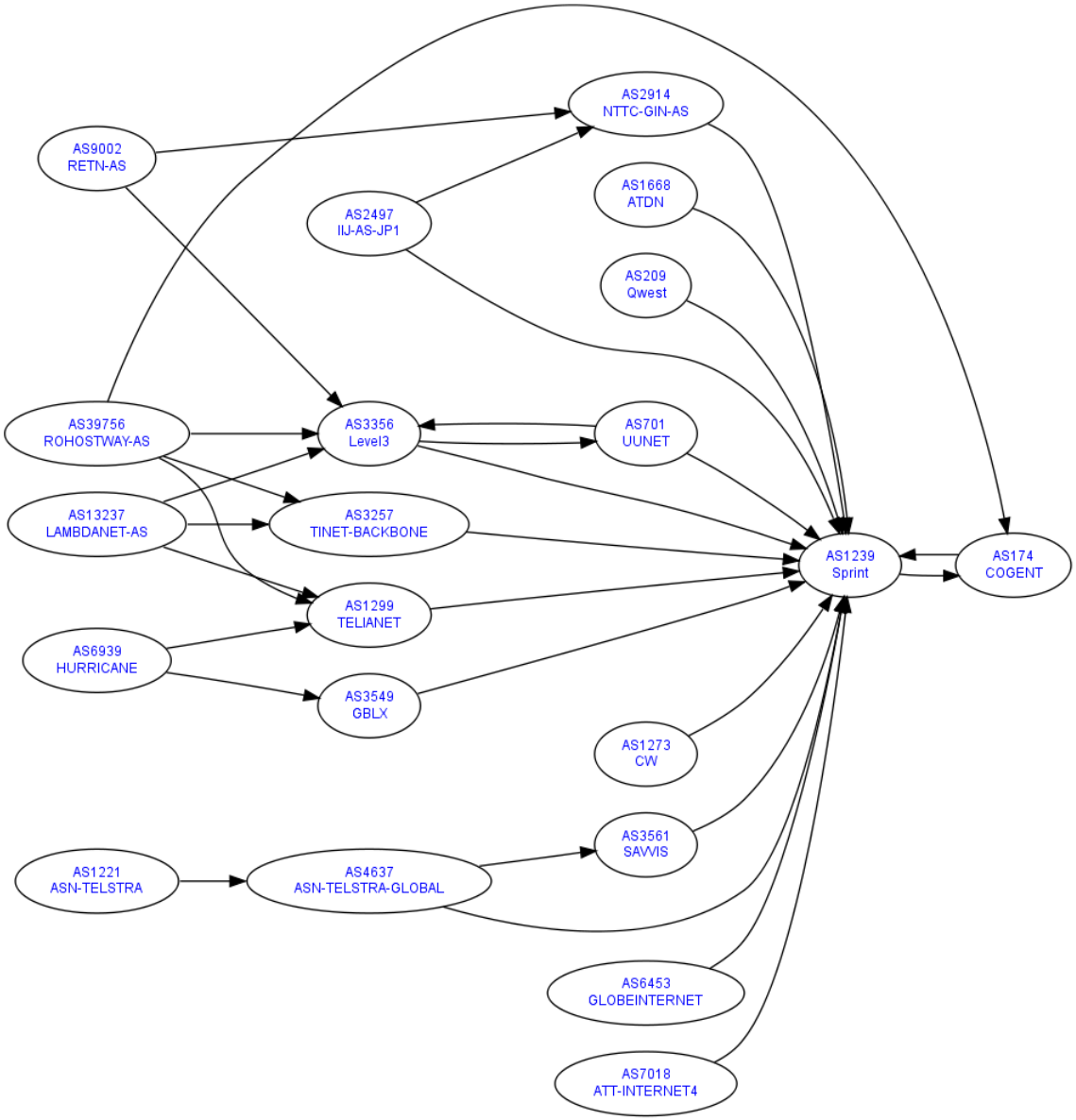
(there are others too, but these 2 are common)

Toy Example of an AS graph



technicolor

What does a “slice” of the AS graph look like?



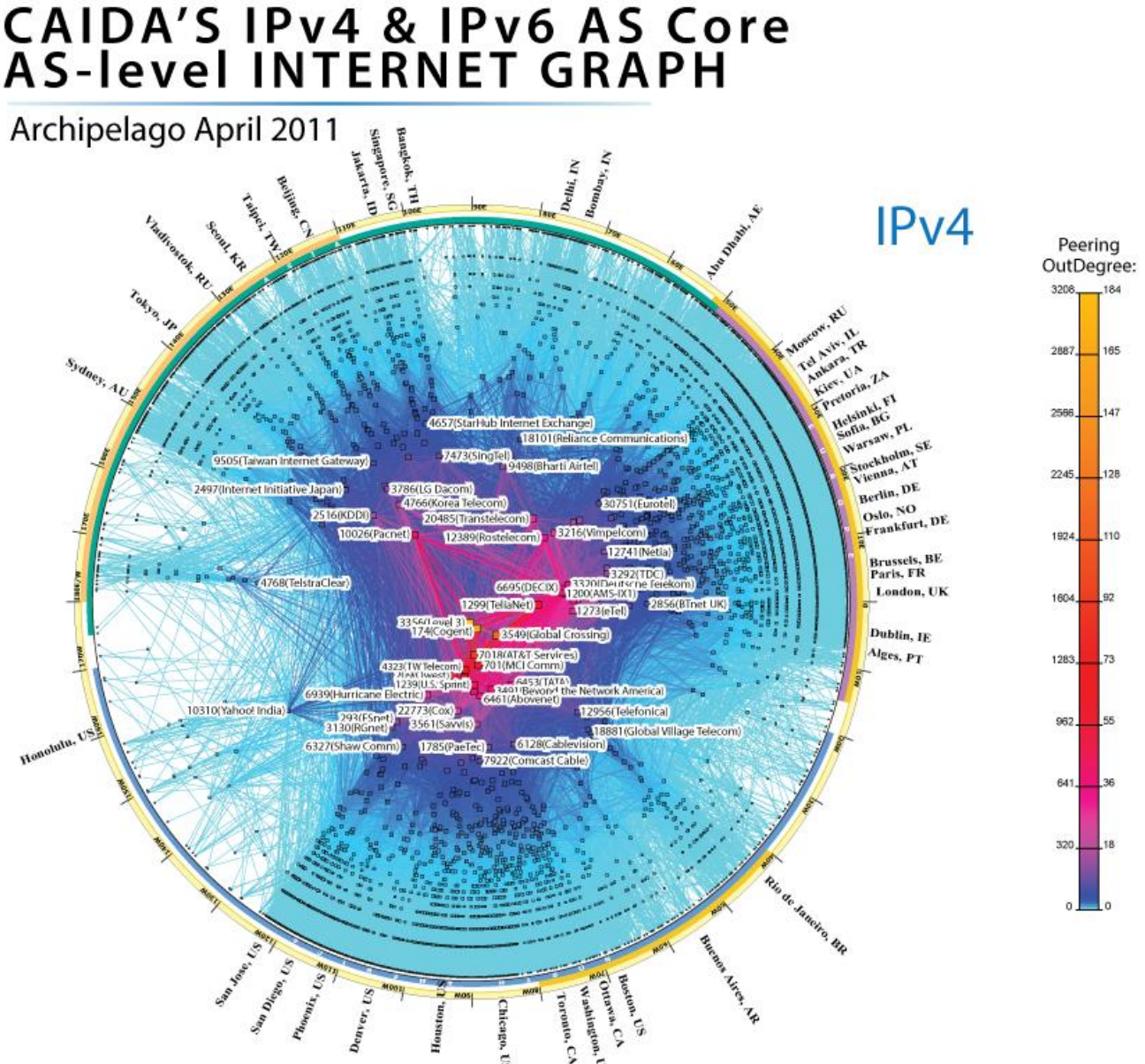
These are various incoming paths to reach Sprint

Graph source: http://as.robtex.com/

technicolor

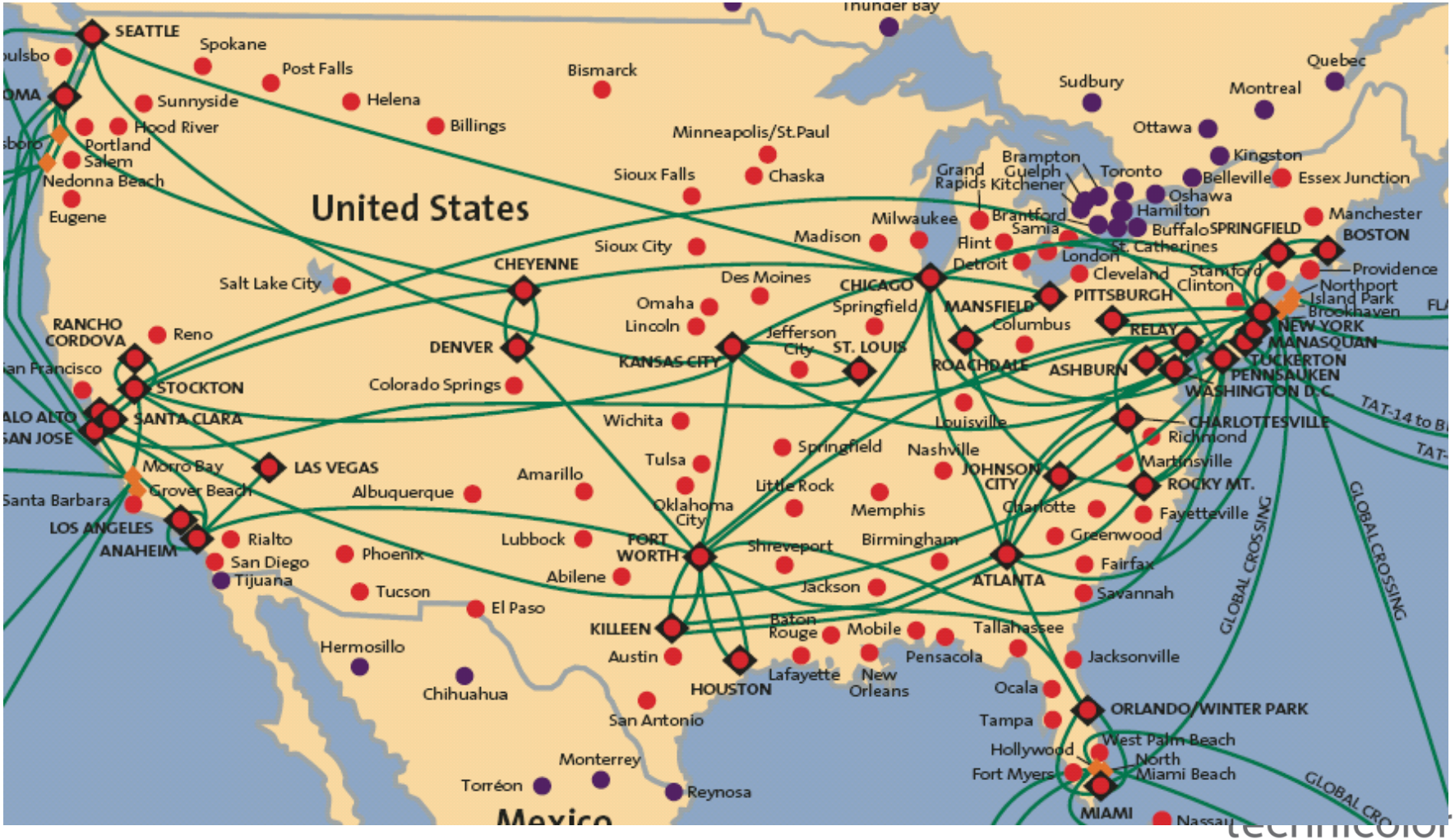
What does the whole AS graph look like?

We can't really be sure, but here's a large chunk of it:



What does a router level topology look like?

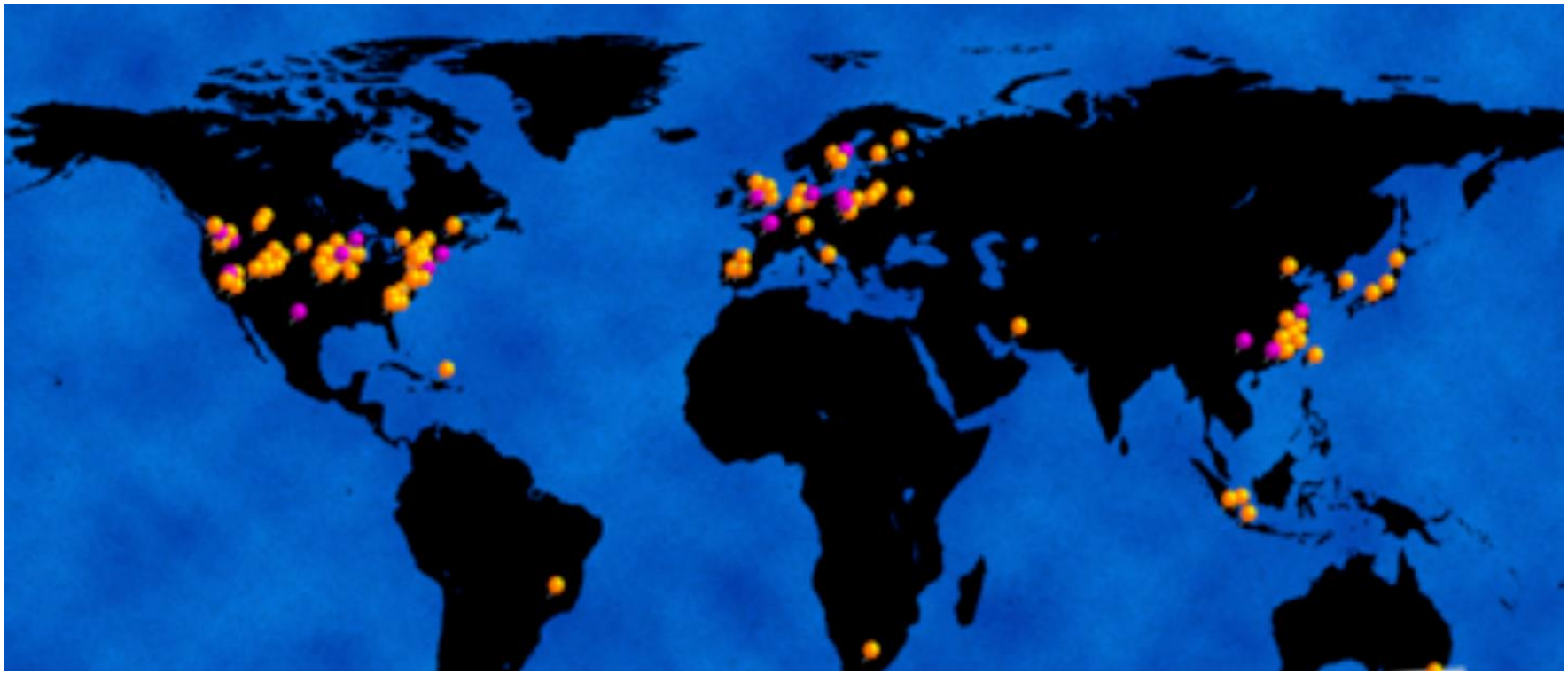
For one ISP (simple version):



How to build a these topologies

Need large-scale infrastructures, with monitors all over the world, to obtain needed data

Each location with monitoring equipment called “vantage point”



Slide source: http://www.monkey.org/~labovit/

How to build a these topologies

Two examples of large-scale infrastructures to obtain needed data

Approach #1: Archipeligo

- Combines 2 different data types: traceroute data and BGP routing tables
- Have ~70 monitors worldwide

Approach #2: Dimes

- Built a worldwide community of thousands of users who installed host software (*Dimes agent*) to run traceroutes and pings (at low rates) from their hosts. Data collected centrally for analysis.

Traceroute data has ambiguities in it. There was much debate over a number of years on the best way to produce these topologies. After settling on a model many researchers liked, the Internet changed again…

Outline

Motivation & Ecosystem

Quick examples of where and why

Areas

- traffic
- performance
- topology
- **security**
- traffic matrices

Summary

Network telescopes (1/2)

Refers to a set of the IPv4 address space that is not used for standard network connectivity; it contains no legitimate hosts.

Idea: all inbound traffic to such addresses must be anomalous, so collect it!

- Route packets with those addresses to a collection point.

Useful for security:

- To detect scanning behavior by worms, and DoS attacks on web servers.

Started using them in 2001. In 2003 Slammer worm released.

Network Telescope (2/2)

First ones appears in 2001.

In 2003 Slammer worm released.

- Reached very high scanning rate in 3 minutes.
- Overwhelmed many servers, some disabled, slowed down links

Slammer studied using telescope data, and predictions made: 1) could target small populations; 2) spreading speed could increase.

- Both of these predictions were realized by the Witty worm in 2004.

Outline

Motivation & Ecosystem

Quick examples of where and why

Areas

- traffic
- performance
- topology
- security
- **traffic matrices**

Summary

What's a traffic matrix?

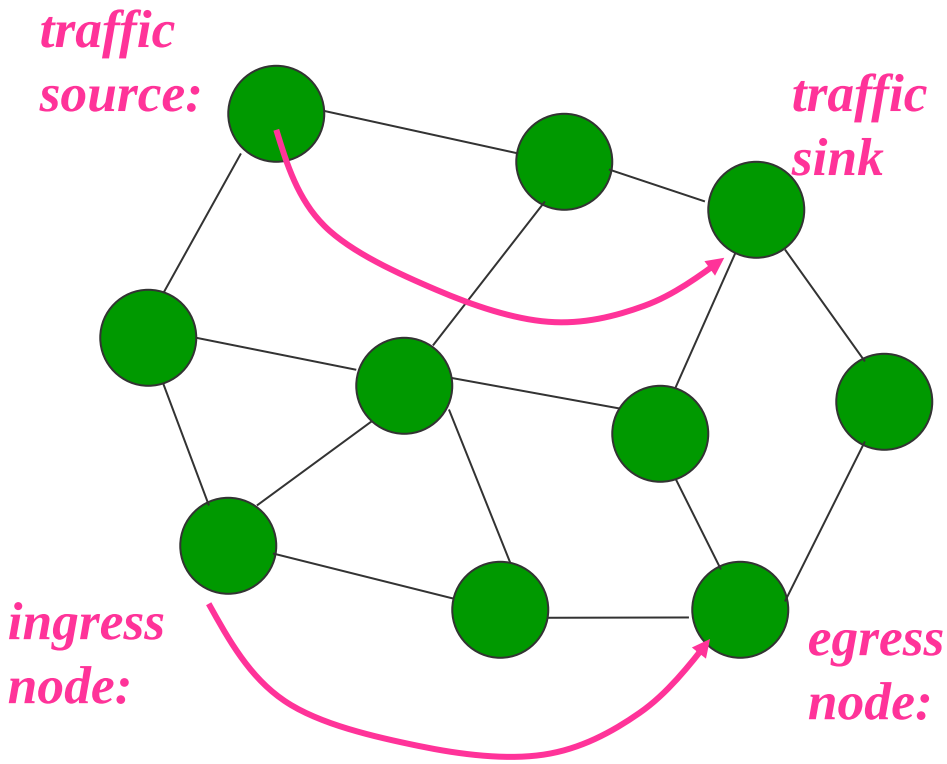
destination / origin	City A	City B	City C
City A			
City B	250 Mbps		
City C			

- Usually contains average values
- Can define variety of matrices
  - Select timescale
  - City-to-city, or router-to-router

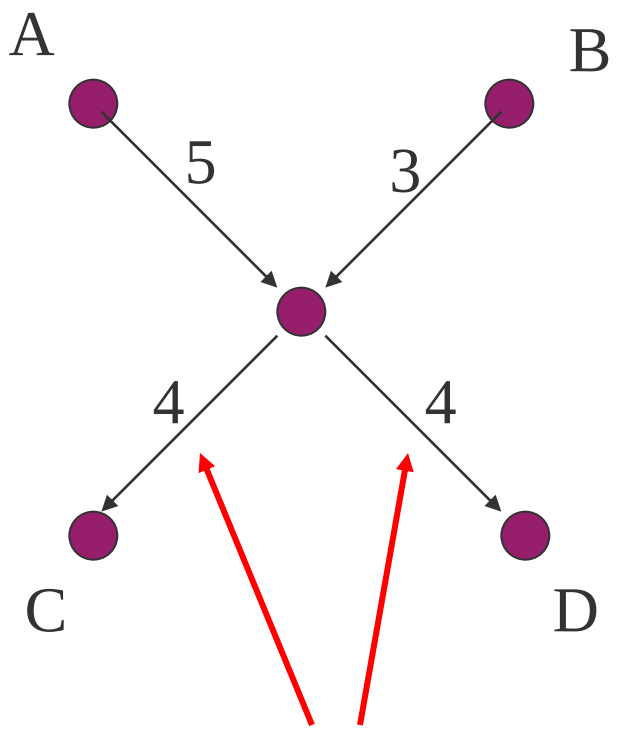
Traditional Traffic Matrix

Describes traffic demands for all node-pairs: end-to-end flows within a single network
(e.g., AS domain)

router-to-router topology:



Example Problem



How much traffic flows between origin-destination pairs?

A->D

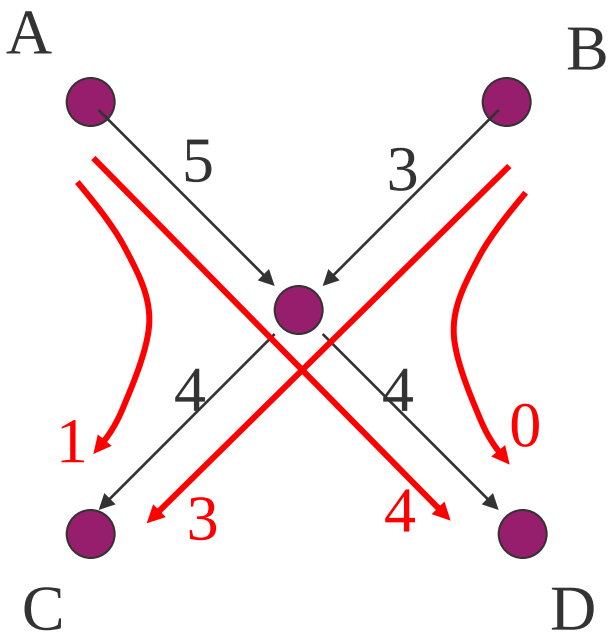
A->C

B->C

B->D

SNMP byte counts per link

Example: One Solution



How much traffic flows between?

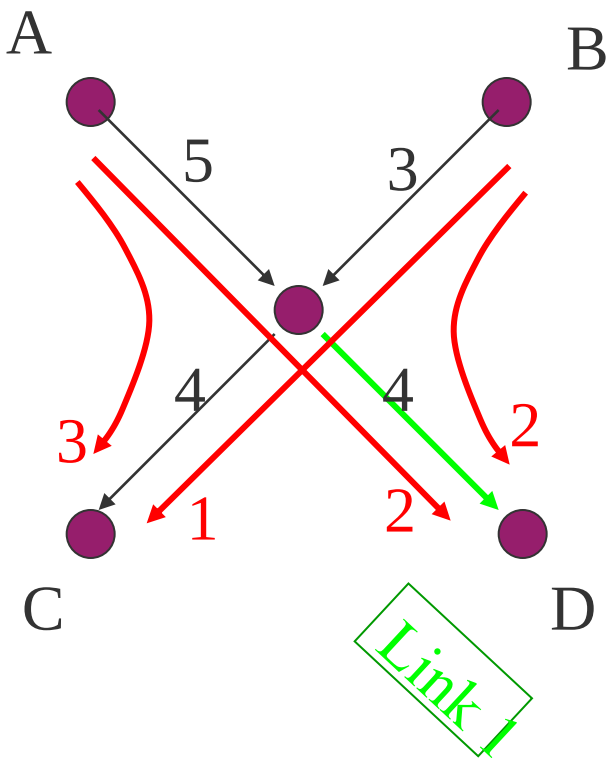
A->D: 4

A->C: 1

B->C: 3

B->D: 0

Example: Another Solution



How much traffic flows between?

A->D: 2

A->C: 3

B->C: 1

B->D: 2

type of equations: $Link1 = X_{AD} + X_{BD}$

Notation: Problem Formulation

routing matrix

$$\begin{pmatrix} \text{Link1} \\ \text{Link2} \\ \text{Link3} \\ . \\ \text{Link L} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & . & . & \\ & & & & & & \\ & & & & & & \\ & & & & & & \end{pmatrix} \begin{pmatrix} X_{AB} \\ X_{AC} \\ X_{AD} \\ . \\ . \\ . \end{pmatrix}$$

Have linear system: $Y = A X$

technicolor

Problem Statement

System: Y = AX

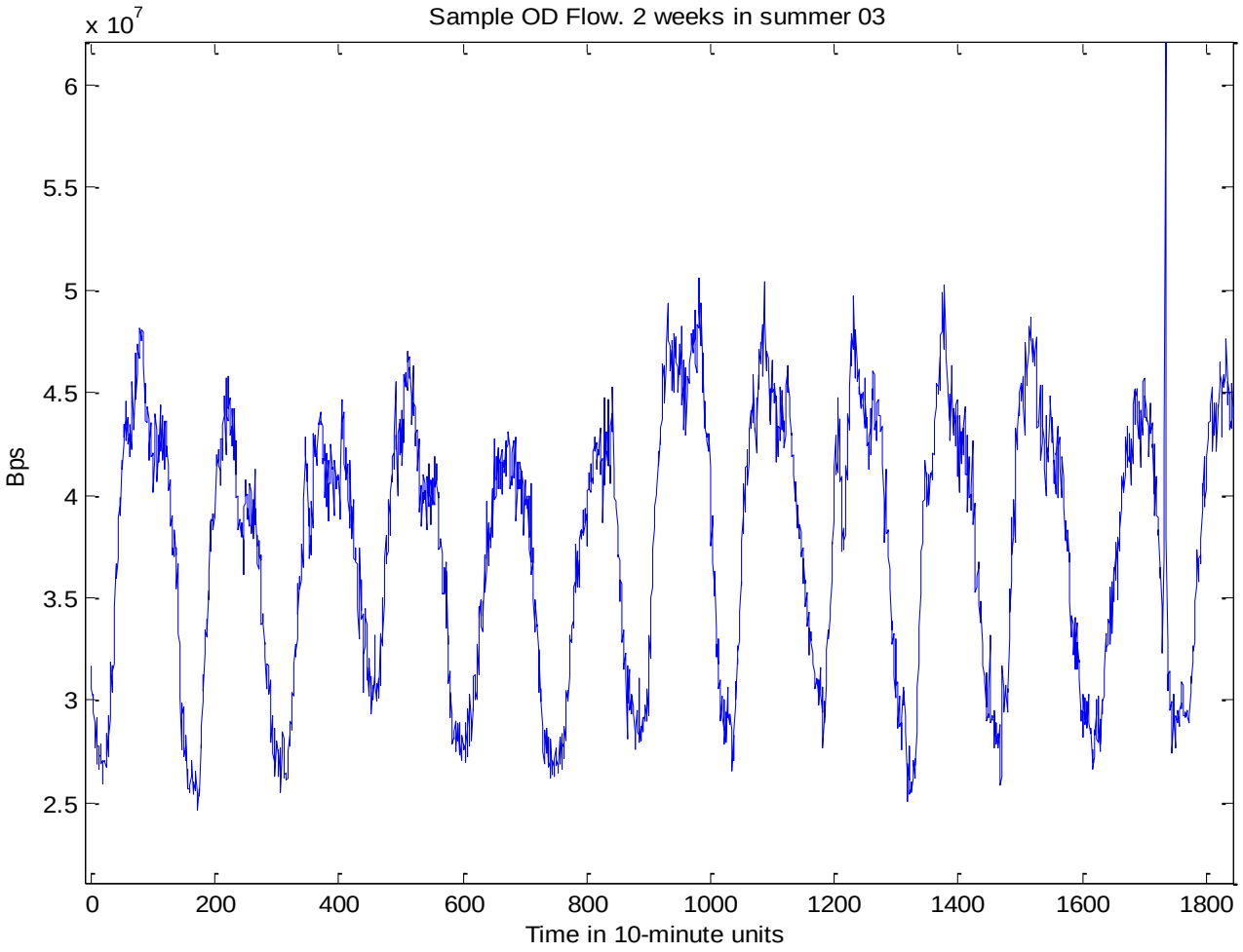
We have Y from SNMP link measurements

We know A from OSPF link weights
(so we can compute shortest paths)

problem: find X

issue:
links < < # OD pairs
=> underconstrained system
=> infinite # of solutions

What does city-to-city traffic look like?



technicolor

Summary

What	How	Who	Why
Traffic	packet or flow capture	ISPs	network planning
		everyone	traffic evolution
Performance	active probes	CDNs	web download performance
		users	Fairness
		ISPs	delivering promised performance
Topology	many vantage points	service providers	vulnerabilities
		everyone	connectedness
Security	network telescopes, deep packet inspection	everyone	(isn't that obvious!)

What's Next: "The only constant is change"

New devices

Web-enabled toaster + weather forecaster

Tweet-a-watt: monitor energy use

Internet refrigerator

Internet is flattening

Google

Akamai

Comcast

Content & search providers building their own infrastructure

New apps, new OSN uses

technicolor

Acknowledgements

Book “Internet Measurement” by Prof. Mark Crovella (Boston University) and Bala Krishnamurthy (AT&T Research)

Some slideware thanks to Prof. Jim Kurose (University of Massachusetts at Amherst)

online course material from book
“Computer Networking: Top-Down Approach”
by Kurose and Ross


Thank You
Questions ?