Routing Security

Steven M. Bellovin

`smb@research.att.com`

`http://www.research.att.com/~smb`

973-360-8656

AT&T Labs Research

Florham Park, NJ 07932

What is Routing Security?

- Bad guys play games with routing protocols.
- Traffic is diverted.
  - Enemy can see the traffic.
  - Enemy can easily modify the traffic.
  - Enemy can drop the traffic.
- Cryptography can mitigate the effects, but not stop them.

History of Routing Security

- Radia Perlman's dissertation: *Network Layer Protocols with Byzantine Robustness*, 1988.
- Bellovin's "Security Problems in the TCP/IP Protocol Suite".
- More work starting around 1996.
- Kent et al., 2000 (two papers).

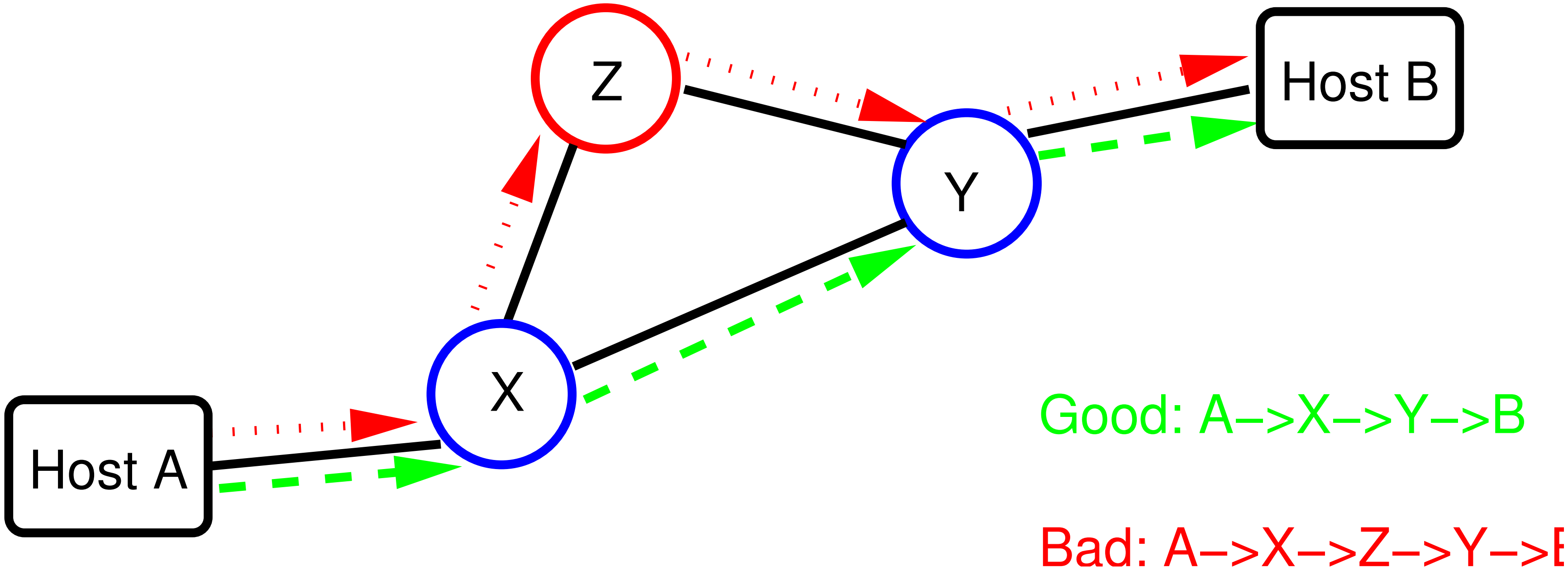
Why So Little Work?

- It's a really hard problem.
- Actually, getting routing to work well is hard enough.
- It's outside the scope of traditional communications security.

How is it Different?

- Most communications security failures happen because of buggy code or broken protocols.
- Routing security failures happen despite good code and functioning protocols. The problem is a dishonest participant.
- Hop-by-hop authentication isn't sufficient.

The Enemy's Goal?

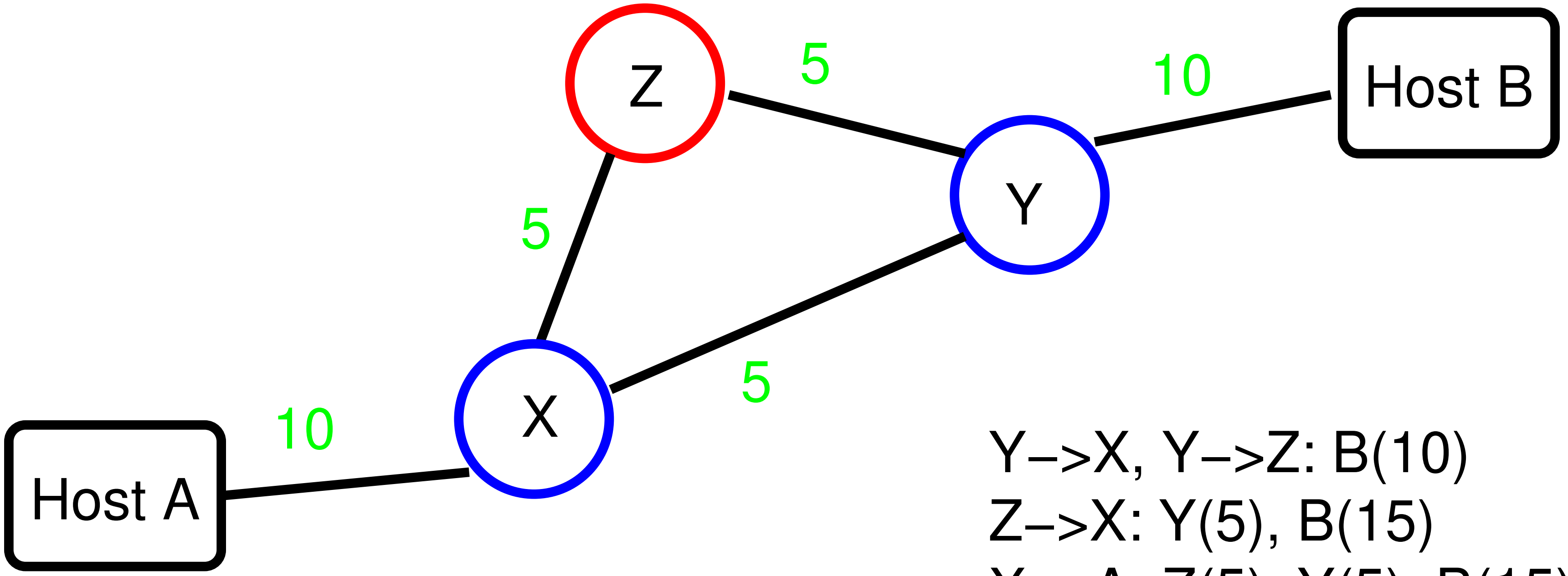


But how can this happen?

Routing Protocols

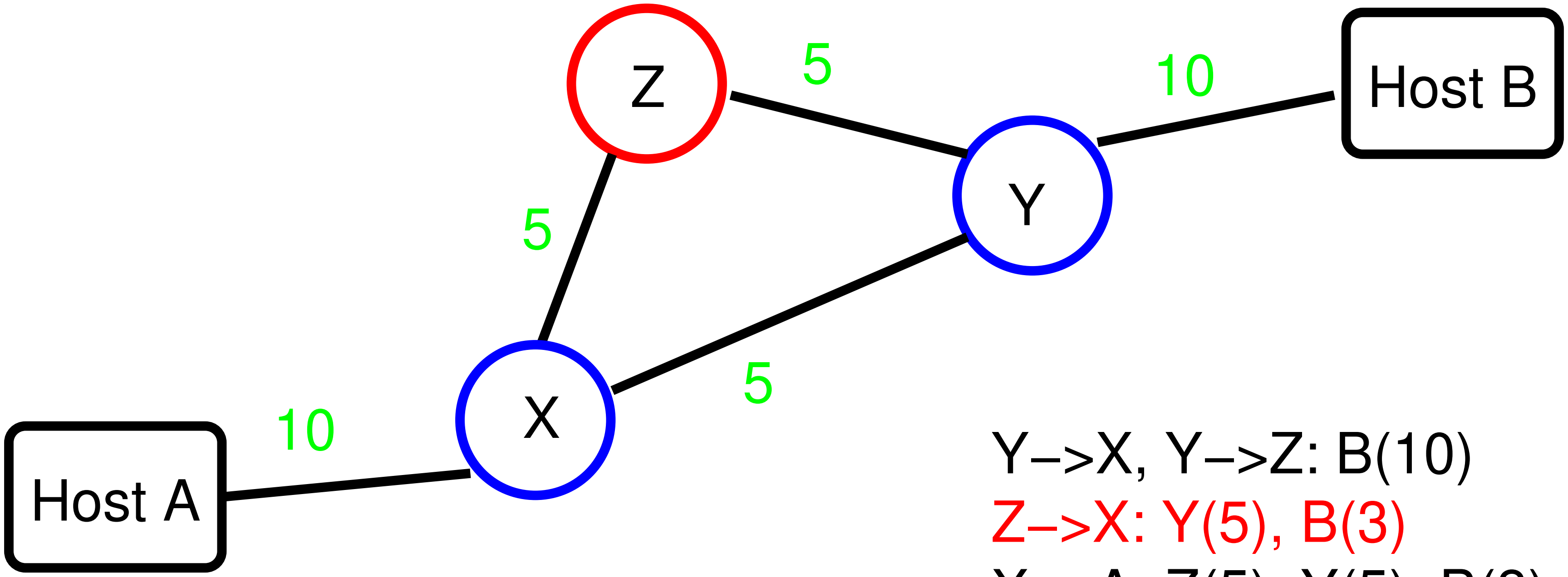
- Routers speak to each other.
- They exchange topology information and cost information.
- Each router calculates the shortest path to each destination.
- Routers forward packets along locally shortest path.
- Attacker can lie to other routers.

Normal Behavior



Y−>X, Y−>Z: B(10)
Z−>X: Y(5), B(15)
X−>A: Z(5), Y(5), B(15)

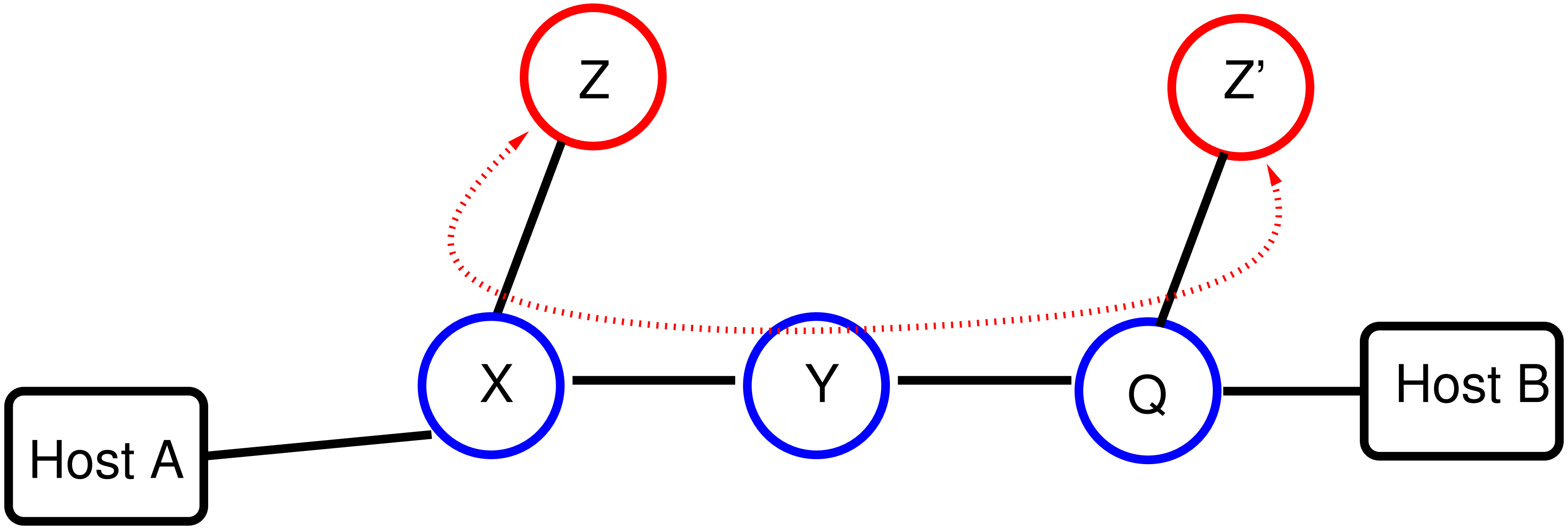
But Z Can Lie



Y–>X, Y–>Z: B(10)
Z–>X: Y(5), B(3)
X–>A: Z(5), Y(5), B(8)

Note that X is telling the truth as it knows it.

Using a Tunnel for Packet Reinjection



Why is the Problem Hard?

- X has no knowledge of Z's real connectivity.
- Even Y has no such knowledge.
- The problem isn't the link from X to Z; the problem is the information being sent. (Note that Z might be deceived by some other neighbor Q.)

Routing in the Internet

- Two types, internal and external routing.
- Internal (within ISP, company): primarily OSPF.
- External (between ISPs, and some customers): BGP.
- Topology matters.

OSPF (Open Shortest Path First)

- Each node announces its own connectivity. Announcement includes link cost.
- Each node reannounces all information received from peers.
- Every node learns the full map of the network.
- Each node calculates the shortest path to all destinations.
- Note: limited to a few thousand nodes at most.

Characteristics of Internal Networks

- Common management.
- Common agreement on cost metrics.
- Companies have less rich topologies, but less controlled networks.
- ISPs have very rich—but very specialized—topologies, but well-controlled networks.
- Often based on Ethernet and its descendants.

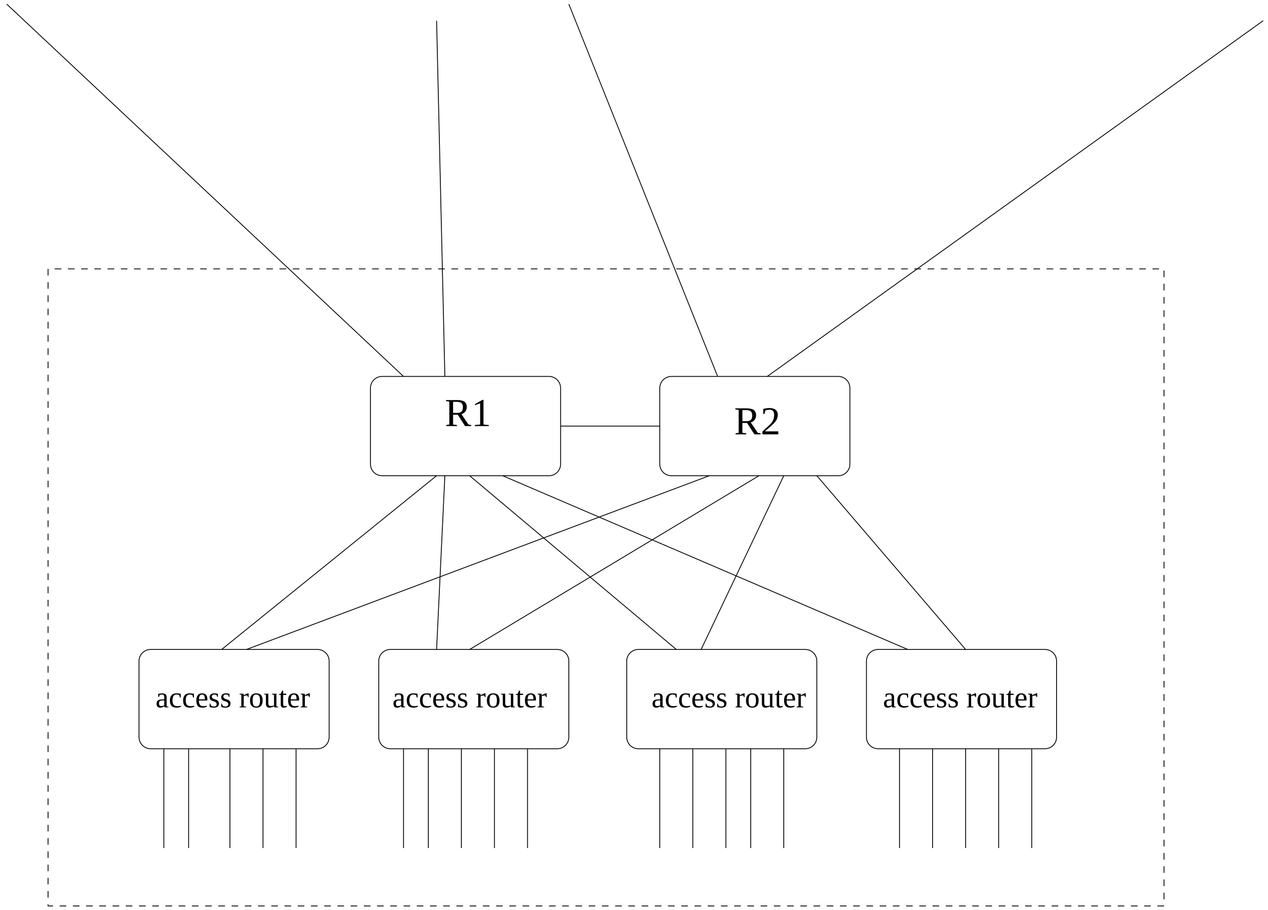
How Do You Secure OSPF?

- Simple link security is hard: multiple-access net.
- Shared secrets guard against new machines being plugged in, but not against an authorized party being dishonest.
- Solution: digitally sign each routing update (expensive!). List authorizations in certificate.
- Experimental RFC by Murphy et al., 1997.
- Note: everyone sees the whole map; monitoring station can note discrepancies from reality. (But bad guys can send out different announcements in different directions.)

External Routing via BGP

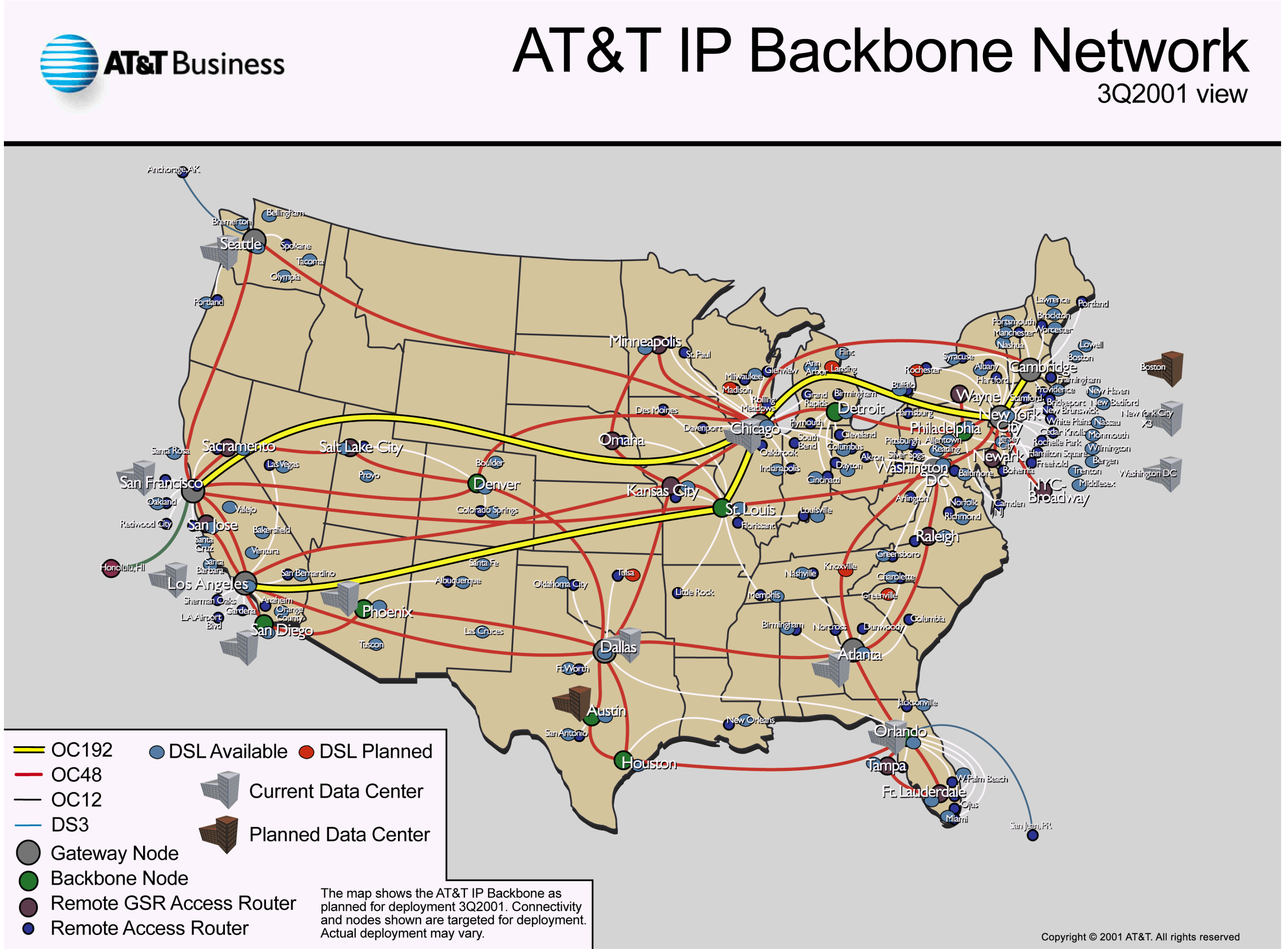
- No common management (hence no metrics beyond hop count).
- No shared trust.
- Policy considerations: by intent, not all paths are actually usable.

POP Topology

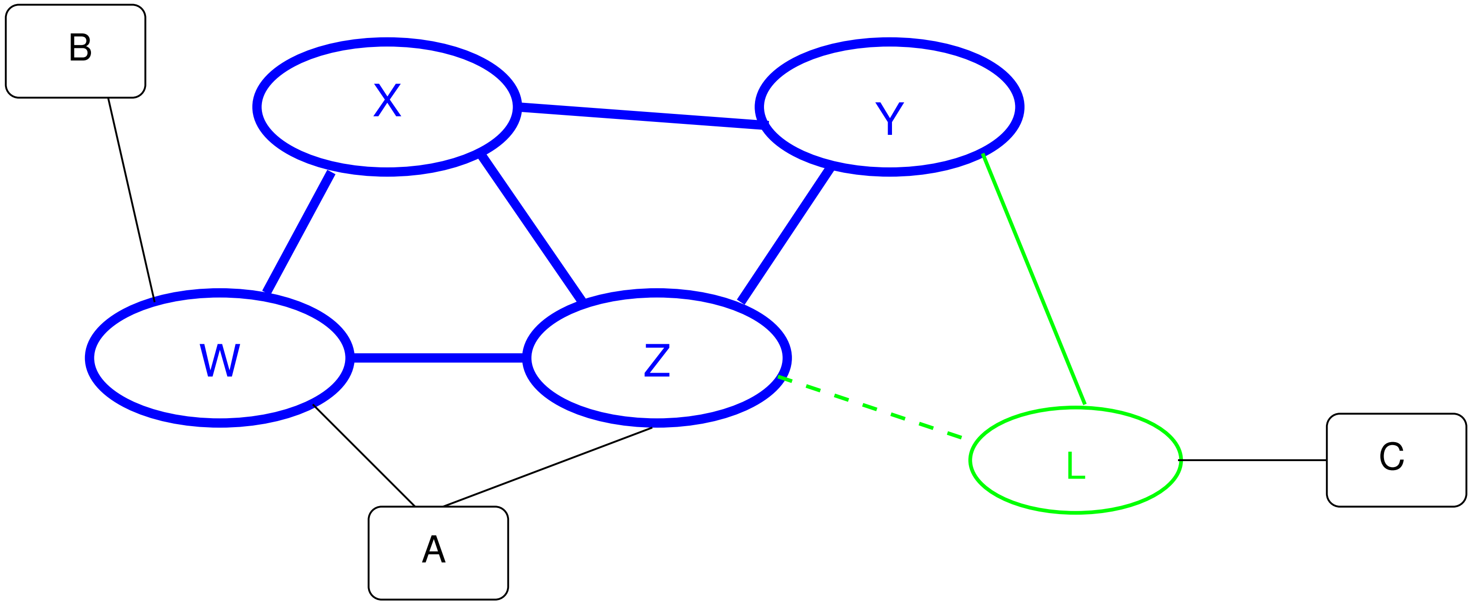


Noteworthy Points

- A lot of attention to redundancy.
- Rarely-used links (i.e., R1$\rightarrow$R2)
  Link cost must be carefully chosen to avoid external hops.
- May have intermediate level of routers to handle fan-out.


AT&T Business
AT&T IP Backbone Network
3Q2001 view
OC192
OC48
OC12
DS3
DSL Available
DSL Planned
Current Data Center
Planned Data Center
Gateway Node
Backbone Node
Remote GSR Access Router
Remote Access Router
The map shows the AT&T IP Backbone as planned for deployment 3Q2001. Connectivity and nodes shown are targeted for deployment. Actual deployment may vary.
Copyright © 2001 AT&T. All rights reserved
Seattle
San Francisco
Sacramento
San Jose
Los Angeles
San Diego
Phoenix
Salt Lake City
Denver
Dallas
Austin
Houston
Kansas City
St. Louis
Omaha
Minneapolis
Chicago
Detroit
Atlanta
Orlando
Tampa
Ft. Lauderdale
Raleigh
Washington DC
Philadelphia
New York City
Newark
Wayne
Cambridge
NYC-Broadway

InterISP Routing



InterISP Routing

- “Tier 1” ISPs are peers, and freely exchange traffic.
- Small ISPs buy service from big ISPs.
- Different grades of service: link L-Z is for customer access, not transit. C→B goes via L-Y-X-W, not L-Z-W.
- A is multi-homed, but W-A-Z is not a legal path, even for backup.
- BGP is distance vector, based on ISP hops. Announcement is full path to origin, not just metric.

Filtering

- ISPs can filter route advertisements from their customers.
- Doesn’t always happen: AS7007 incident, spammers, etc.
- Not feasible at peering links.

Secure BGP (Kent et al.)

- Each node signs its announcements.
- That is, X will send $\{W\}_X, \{Y\}_X, \{Z\}_X$.
- W will send $\{B\}_W, \{A\}_W, \{X\}_W, \{X : \{Z\}_X\}_W$.
- Chain of accountability.

Problems with SBGP

- Lots of digital signatures to calculate and verify.
  - Can use cache
  - Verification can be delayed
- Calculation expense is greatest when topology is changing—i.e., just when you want rapid recovery. (About 120K routes. . .)
- How to deal with route aggregation?
- What about secure route withdrawals when link or node fails?
- Dirty data on address ownership.

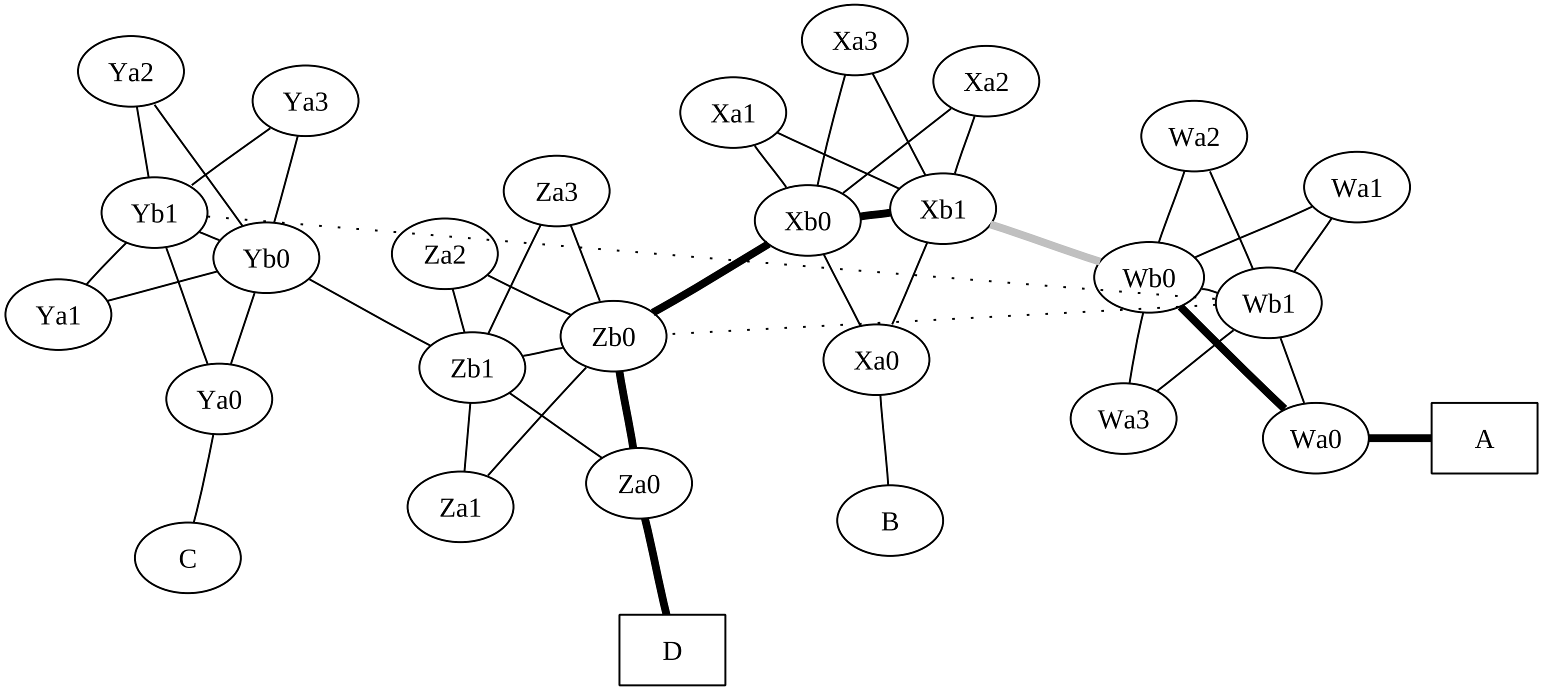
Link-Cutting Attack (Bellovin and Gansner)

- Suppose that we have SBGP and SOSPF.
- Suppose the enemy controls a few links or nodes. Can he or she force traffic to traverse those paths?
- Yes. . .

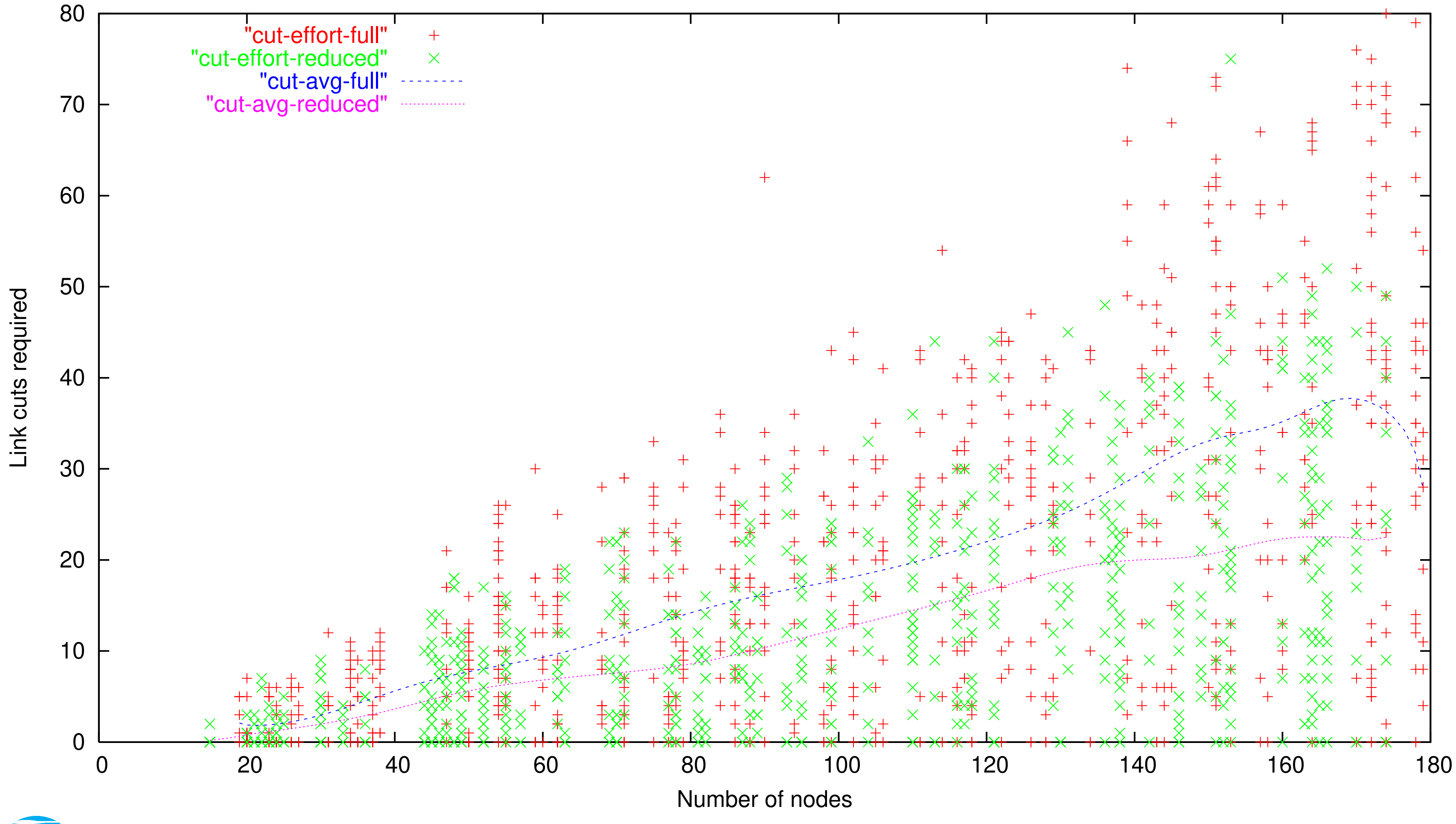
Is Link-Cutting Feasible?

- Attacker must have network map.
  Easy for OSPF; probably doable for BGP—see “Rocketfuel” paper.
- Can attacker determine peering policy? Unclear.
- How can links be cut?
  Backhoes? “Ping of death”? DDoS attack on link bandwidth?

Sample Link-Cutting Attack



Cost of Link-Cutting Attacks on the Backbone



Defenses

- Hard to defend against—routing protocols are doing what they're supposed to!
- Keeping attacker from learning the map is probably infeasible.
- Feed routing data into IDS?
- Link-level restoration is a good choice, but can be expensive.
- Others?

Conclusions

- Routing security is a major challenge.
- Mentioned specifically in White House Cybersecurity document.
- Lots of room for new ideas.