Internet Infrastructure Security

Simon Fraser University

Scott Wakelin

Road Map

- Project Goals and Overview
- Project Status
- Network Infrastructure
  - ISP Topology
  - ISP Interconnection
- Routing Protocols
- Routing Protocol Security Issues
- Example Case: OSPF
- Future Work
- References

Project Goals

- **Understand Internet Infrastructure and typical topology**
- **Understand routing protocols**
- **Understand attacks against Internet Infrastructure**
- **Demonstrate weaknesses of routing protocols using OPNET and NS-2.**

Is it important?

“Our very way of life depends on the secure and safe operations of critical systems that depend on cyberspace”

- **Richard Clarke, Former US Homeland Security Advisor on Cyberterrorism**

Current Status

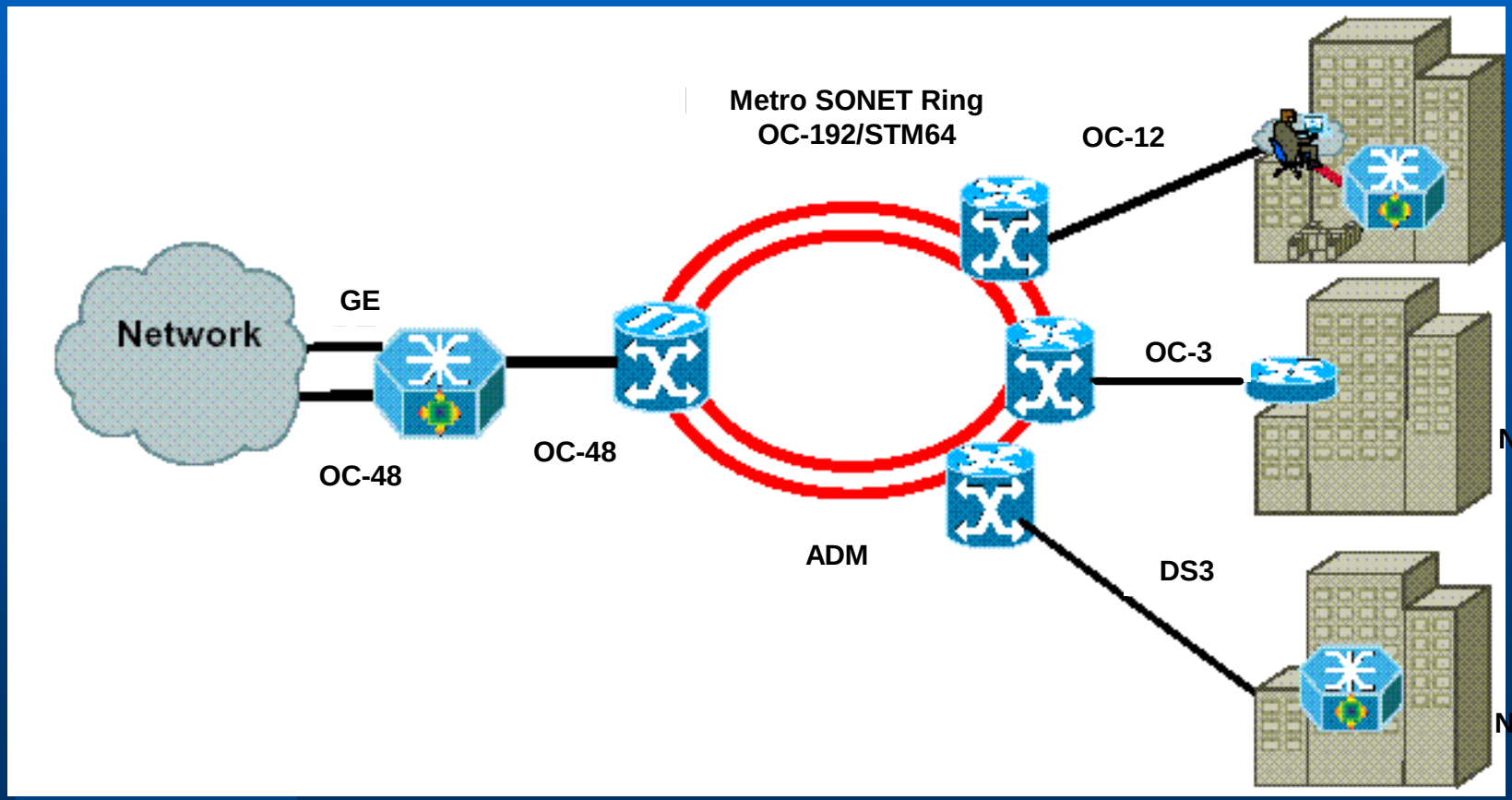
- **Completed:**
  - **Implemented OSPF network using OPNET**
  - **Created “misbehaving” router scenario in OPNET**
  - **Used FlowAnalysis to analyze routing tables, in addition to link and host statistics**
  - **Examined internal implementation of OSPF process module, function blocks, identified potential code changes**
  - **Built NS model to simulate link cutting attacks**
- **Work Remaining:**
  - **Determine feasibility of modifying OPNET to support “faulty” router operation (eg. I know what to do, but can it be done?)**
  - **Gather additional traffic statistics**
  - **Code link selection/cutting algorithm in Tcl for NS-2**
  - **Demo, and Final Report**

Internet Infrastructure

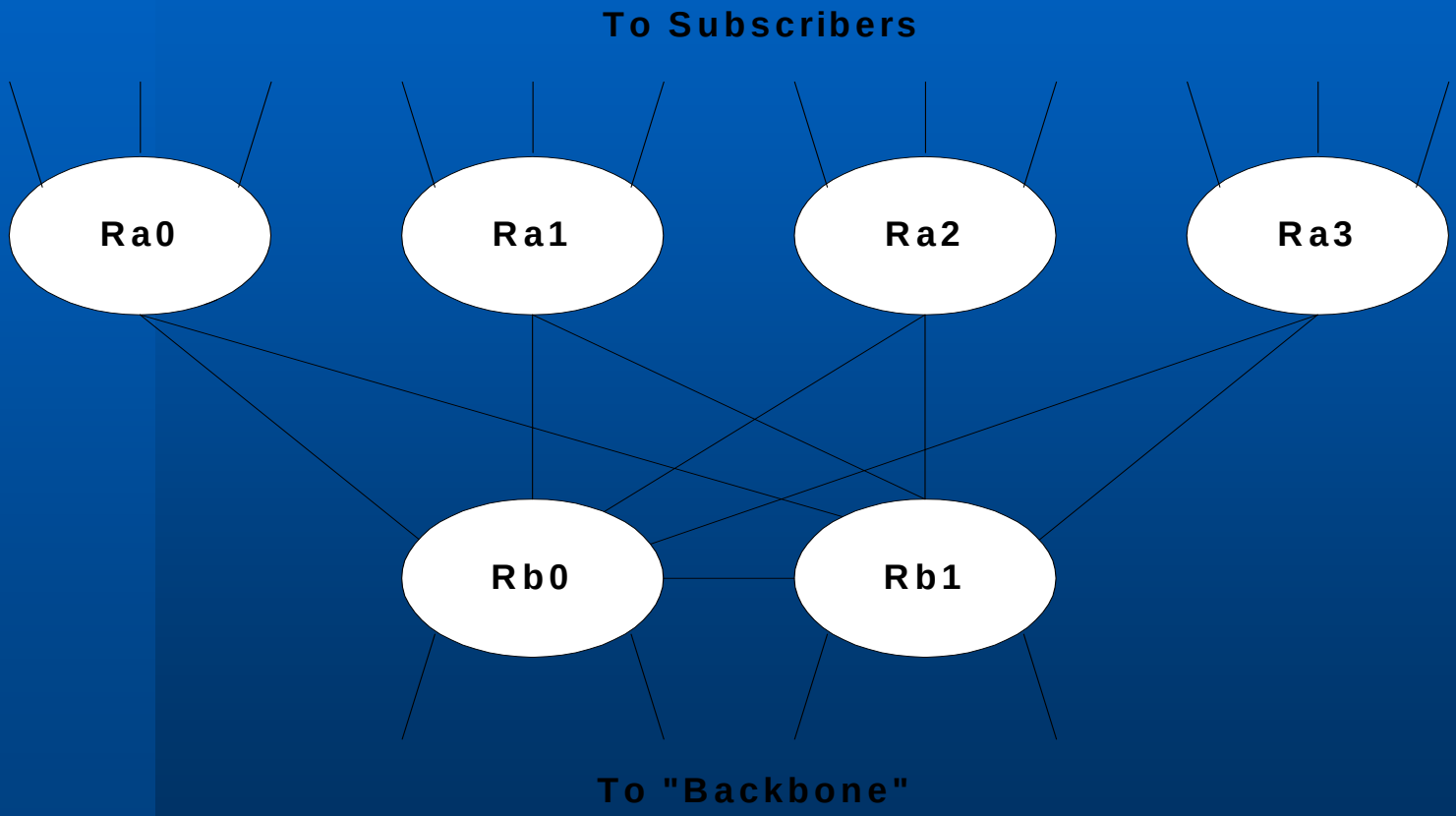
- **“Network of Networks”**
- **Subscriber networks connect to ISP POP’s**
- **ISP POP’s interconnected via IP backbone routers**
- **ISP’s interconnected IXP (eg. MAE-WEST)**

ISP = Internet Service Provider
POP = Point of Presence
IXP = Internet Exchange Point

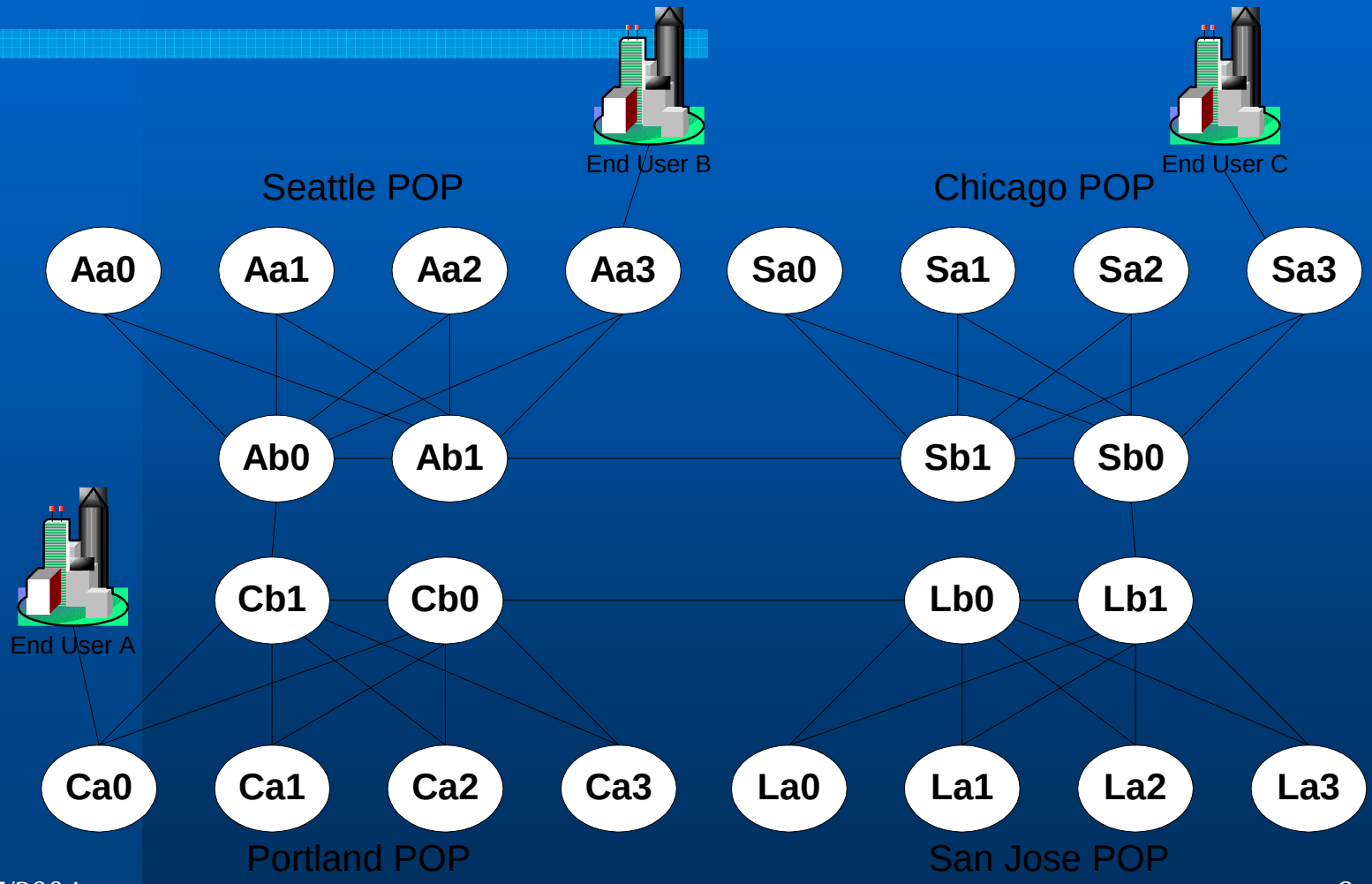
Subscriber to ISP Network



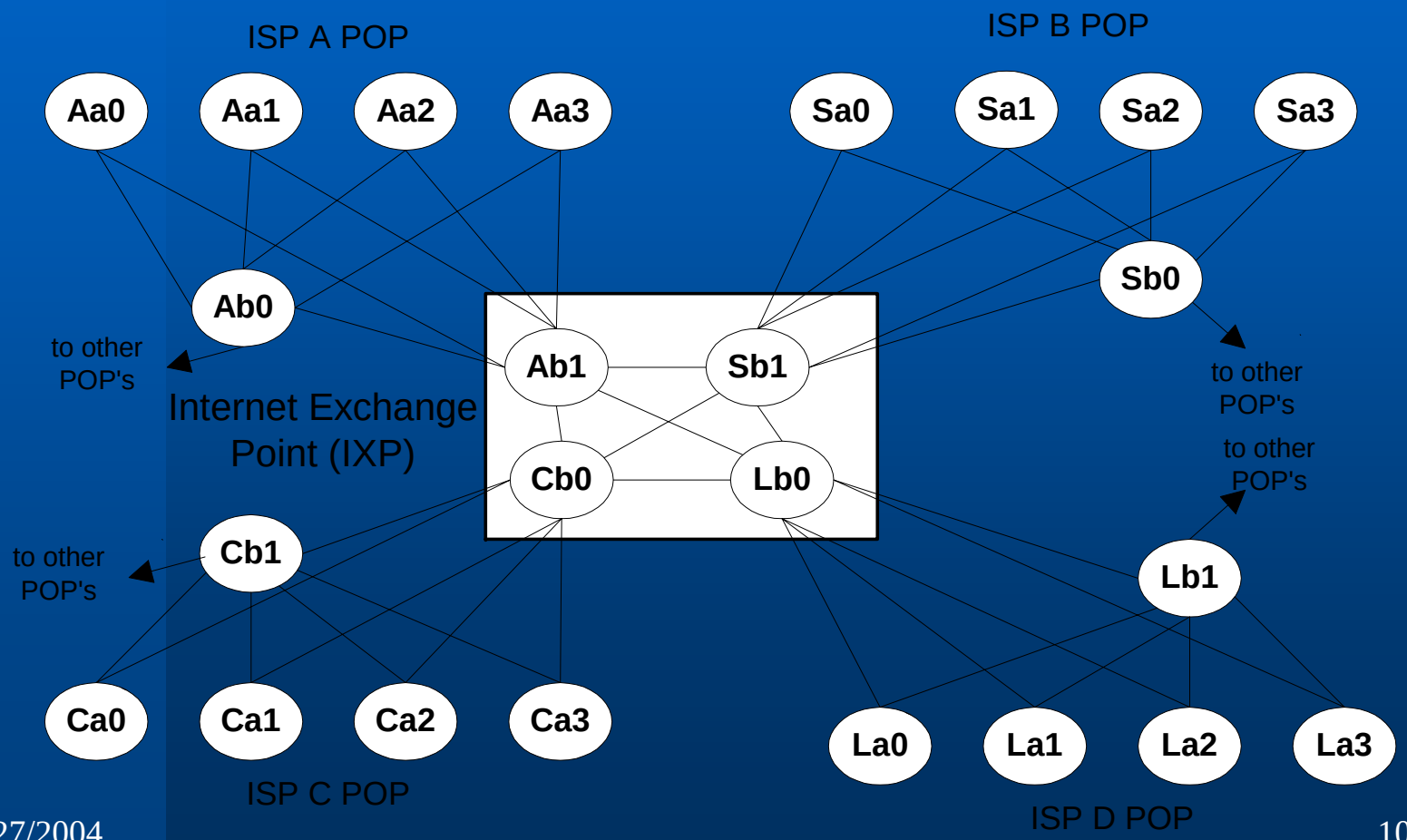
Typical POP Architecture



ISP POP Interconnect



Interconnecting ISP's



Routing Protocols: OSPF

- OSPF is defined in RCF 2328
- Link State Routing protocol
- Intra-domain protocol
- OSPF Phases:
  - Neighbor Discovery
  - LSA Generation
  - LSA Propagation
  - Shortest Path Calculation
- OSPF runs over IP

OSPF: Open Shorted Path First
LSA: Link State Advertisement

OSPF Packet Header

Octets	
1	Version
1	Packet Type
2	Packet Length
4	Router ID
4	Area ID
2	Checksum
2	Authentication Type
8	Authentication Data

Routing Protocols: BGP-4

- BGP-4 is defined in RFC 1771
- Path-Vector algorithm
- Inter-domain protocol
- BGP Phases:
  - Opening a BGP Connection
  - Exchange of routing tables
  - Maintenance of the connection
- BGP Runs over TCP

BGP: Border Gateway Protocol

OSPF/BGP Interworking

- **OSPF and BGP work alongside each other in a router**
- **Router maintain two route tables, one internal, one external**
- **Router uses BGP next-hop to index into OSPF table**

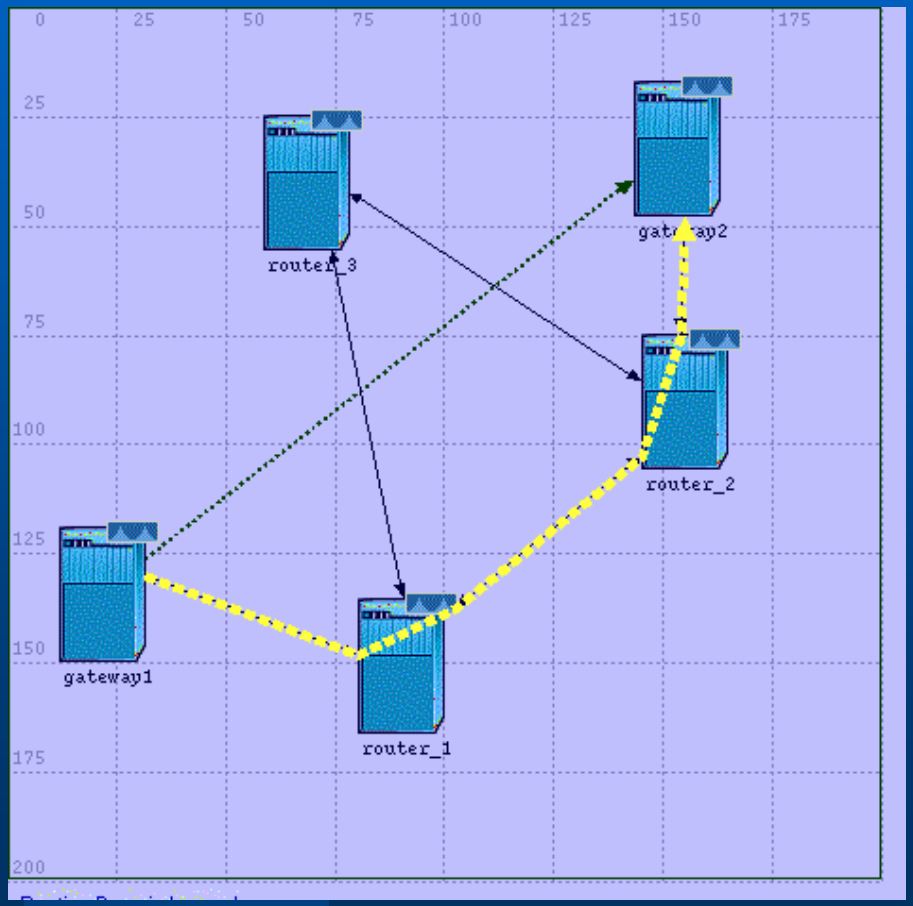
Routing Protocol Security

- ….or lack thereof…
- Implicit trust relationship amongst routers
- Attacks can be devastating:
  - Service disruption
  - Loss of confidentiality
- And difficult to detect
  - How does one router know another is lying?

OSPF Example

- One router can lie and advertise incorrect costs
- The lying router then becomes the part of the preferred route to some other router (perhaps gateway)
- The lying router can then do just about anything it wants with the traffic

Example Topology using OPNET

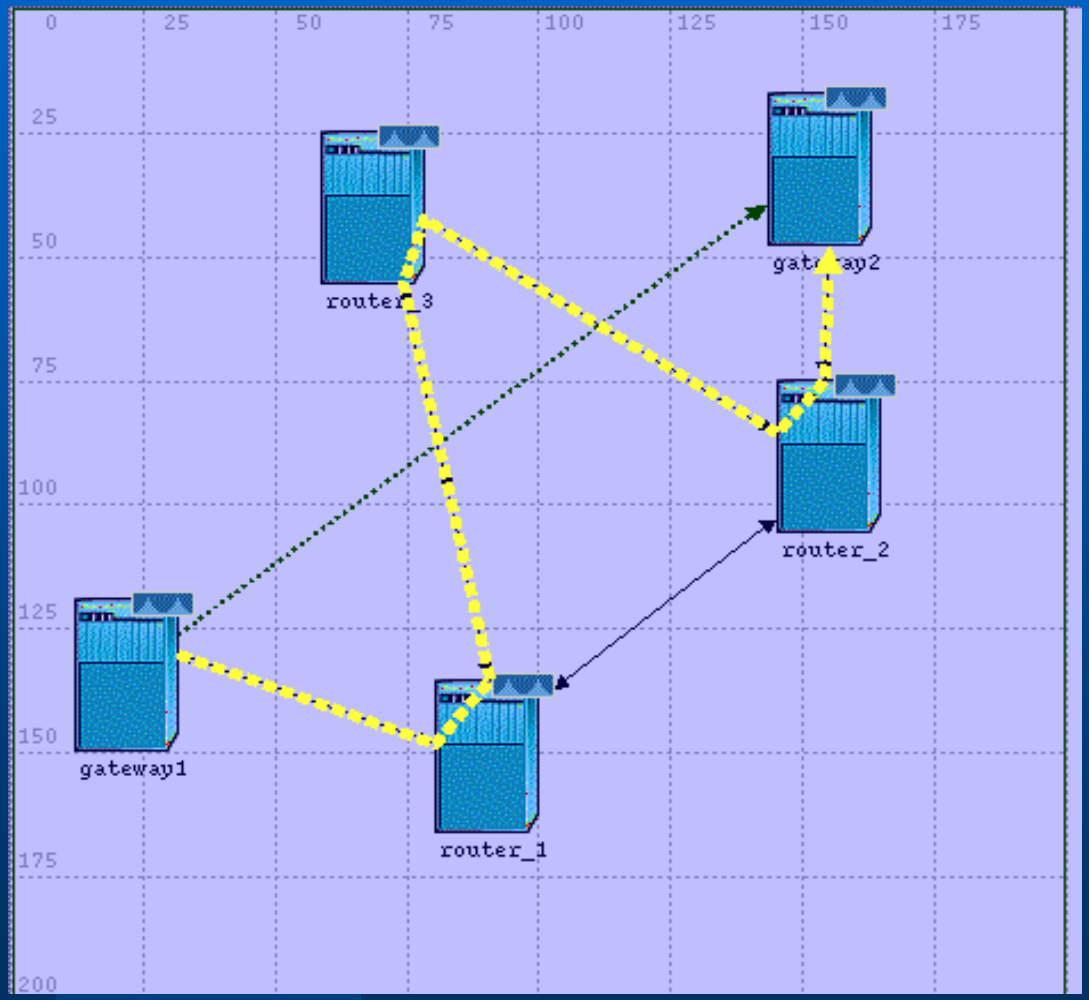


- Assume gateway1 has sensitive data to send to gateway2
- Assume all link costs equal
- Normal route:
  - G1 -> R1 -> R2 -> G2

But what if…

- **Router 3 lies?**
- **Routers 1, 2 and the gateway routers don’t know that Router 3 is lying.**
- **They assume that what Router 3 advertises is correct**

OSPF Failure Case



- Now all traffic from G1 -> G2 goes through Router 3
- New Route:
  - G1 -> R1 -> R3 -> R2 -> G2
- Possible results:
  - Snooping
  - Packet mistreatment
  - Congestion
  - ???

But what about OSPF Auth?

- **Authentication field in OSPF only provides assurance that Router 3 sent the message**
- **Authentication field DOES NOT mean that the information is correct**

S-OSPF: A Solution?

- One solution is to have each router digitally sign/authenticate each LSA
- Problems:
  - Computationally expensive
  - Requires PKI for certification
  - Others
- Still not a complete solution
  - Link Cutting

Link Cutting

- Targetting specific hosts/links and bringing them down
- How?
  - Fibre cuts (for the serious attacker)
  - DDoS attacks
  - Others…
- Idea: Force traffic to go through a node/link controlled by an attacker
- Requires some knowledge of the network topology:
  - Not so hard to obtain…See Rocketfuel research.
- Bellovin et al. developed algorithm to select which links to cut.

Link Cutting…cont.

- **Traceroute can provide a lot of information:**

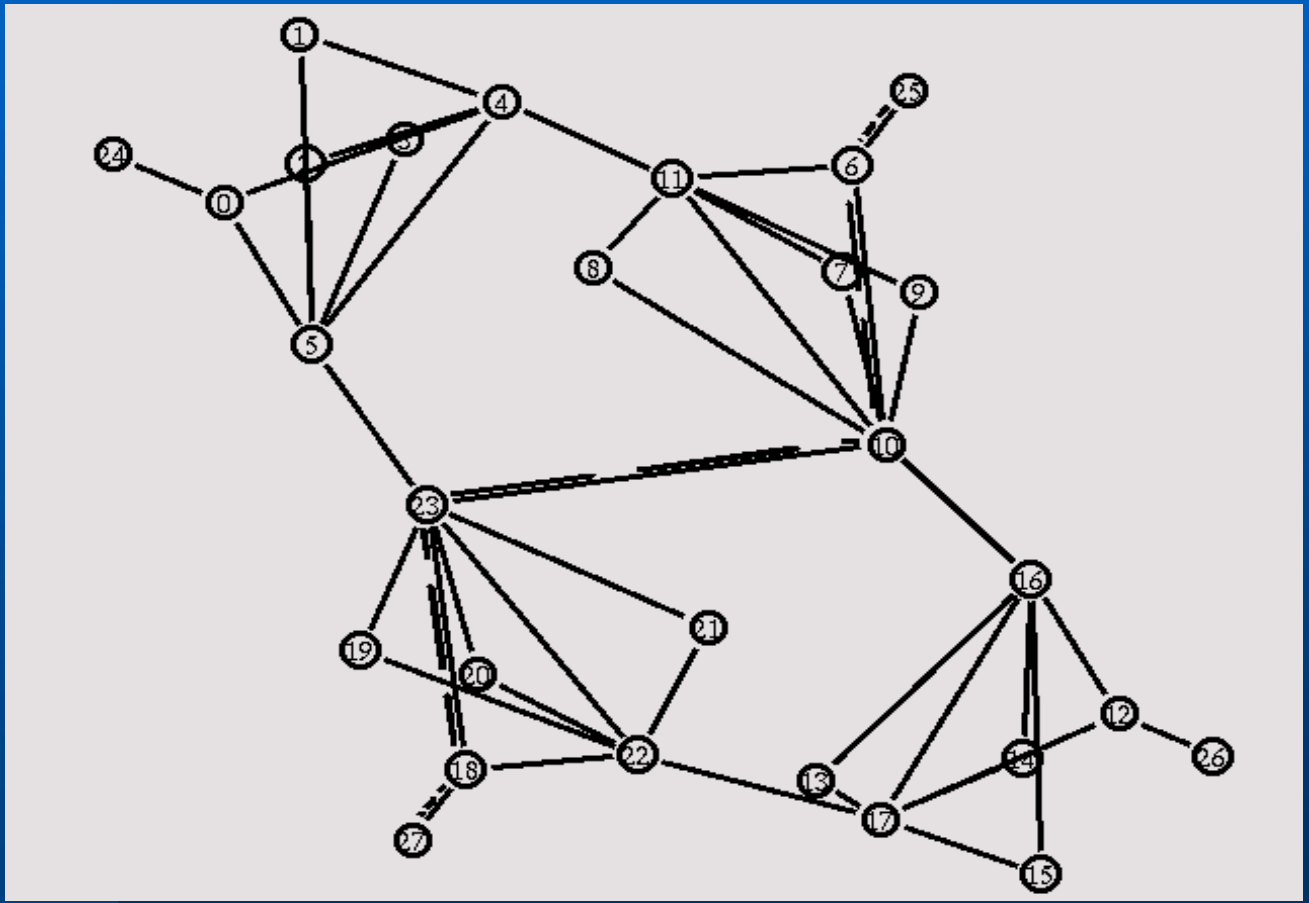
Tracing route to www.sprint.net [199.0.233.22]
over a maximum of 30 hops:

1	20 ms	30 ms	20 ms	209.53.1.226
2	20 ms	30 ms	20 ms	208.181.229.118
3	20 ms	30 ms	20 ms	vancbc01gr01.bb.telus.com [154.11.4.97]
4	30 ms	30 ms	30 ms	vancbc01br01.bb.telus.com [154.11.10.49]
5	20 ms	30 ms	30 ms	sttlwa01gr01.bb.telus.com [209.53.75.166]
6	20 ms	30 ms	30 ms	**sl-gw14-sea-10-0.sprintlink.net [144.224.23.33]**
7	20 ms	30 ms	30 ms	sl-bb21-sea-9-1.sprintlink.net [144.232.6.133]
8	70 ms	70 ms	70 ms	sl-bb25-chi-2-0.sprintlink.net [144.232.20.157]
9	70 ms	71 ms	70 ms	sl-bb23-chi-15-0.sprintlink.net [144.232.26.93]
10	90 ms	90 ms	90 ms	sl-bb27-rly-11-0.sprintlink.net [144.232.20.185]
11	90 ms	90 ms	*	sl-bb22-rly-10-0.sprintlink.net [144.232.14.177]

Link Cutting Example: NS-2

- **Network built using ISP topology shown on pg. 7.**
- **Attacker wants to see traffic flowing between Node 27 and 25**
- **Assume attacker has control of backbone router 4**
- **Normal path:**
  - **Nodes 27 -> *18* -> 23 -> 10 -> *6* -> 25**

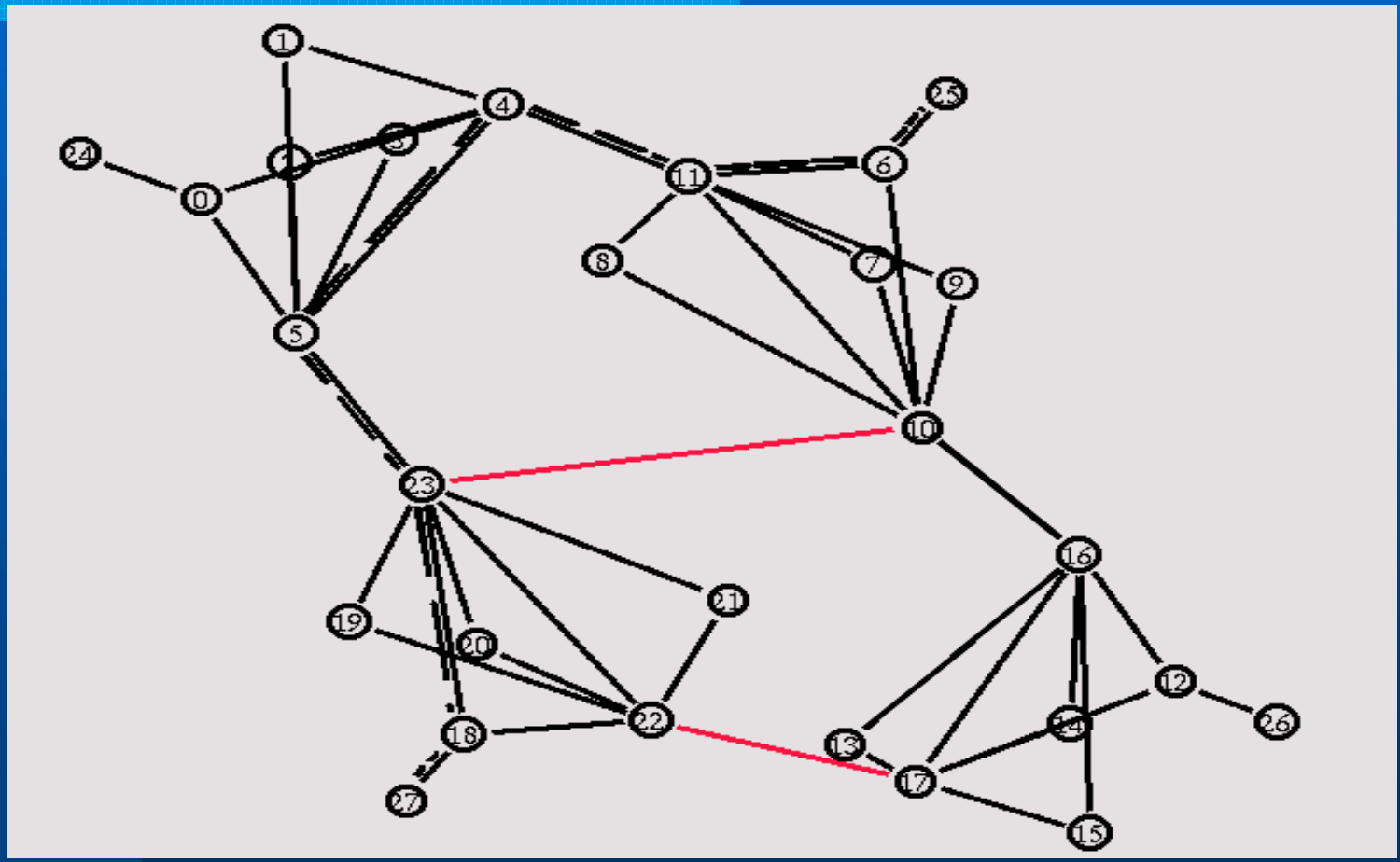
Normal Case: NS-2



Link Cutting Attack

- **Attack Links 23-10, 22-17**
- **Causes traffic to flow through backbone router 4**
- **New route:**
  - **27, *18*, 23, 5, 4, 11, *6*, 25**

Link Cutting Attack, cont.



Future Work

- **Implement S-BGP**
  - **IBGP, EBGP peers communicate using IPSec**
  - **Each router cryptographically signs its advertisements**
- **Implement S-OSPF**
- **Are the solutions scalable?**
- **What other pitfalls exist?**

References

- [1] J. Moy, “OSPF Version 2”, RFC 2328, April 1998.
- [2] Y. Rekhter and P. Gross, “Application of the Border Gateway Protocol in the Internet”, RFC 1772, March 1995.
- [3] C. Metz, “Interconnecting ISP Networks”, *IEEE Internet Computing*, vol. 5, no. 2, March-April 2001, pp 74-80.
- [4] S. Kent, C. Lynn, and K. Seo, “Secure Border Gateway Protocol (S-BGP)”, *IEEE Journal on Selected Areas in Communications*, vol. 18, no. 4, April 2000. pp. 582-592.
- [5] S. Kent, C. Lynn, and K. Seo, “Public-key infrastructure for the Secure Border Gateway Protocol (S-BGP)”, *Proc. Darpa Information Survivability Conference and Exposition II*, vol. 1, June 2001, pp. 239-252.
- [6] S. Kent, C. Lynn, and K. Seo, “Design and analysis of the Secure Border Gateway Protocol (S-BGP)”, *Proc. Darpa Information Survivability Conference and Exposition II*, vol. 1, Jan. 2000, pp 18-33.
- [7] H. Papadimitratos, “Securing the Routing Infrastructure”, *IEEE Communications Magazine,* vol. 40, no. 10, Oct. 2002, pp. 60-68.
- [8] A. Chakrabarti, and G. Manimaran, “Internet Infrastructure Security: A Taxonomy”, *IEEE Network*, vol. 16, no. 6, Nov.-Dec. 2002, pp. 13-21.
- [9] S. M. Bellovin, and E. R. Gansner, “Using Link Cuts to Attack Internet Routing”, DRAFT, May 2003.
- [10] Rocketfuel, http://www.cs.washington.edu/research/networking/rocketfuel/
- [11] Marc Greis’ Tutorial for the UCB/LBNL/VINT Network Simulator “ns”, http://www.isi.edu/nsnam/ns/tutorial/index.html

Questions?