

# Recent UIUCnet Changes for Performance, Reliability, and Security

*Charley Kline*

*Manager, Network Engineering  
CITES*

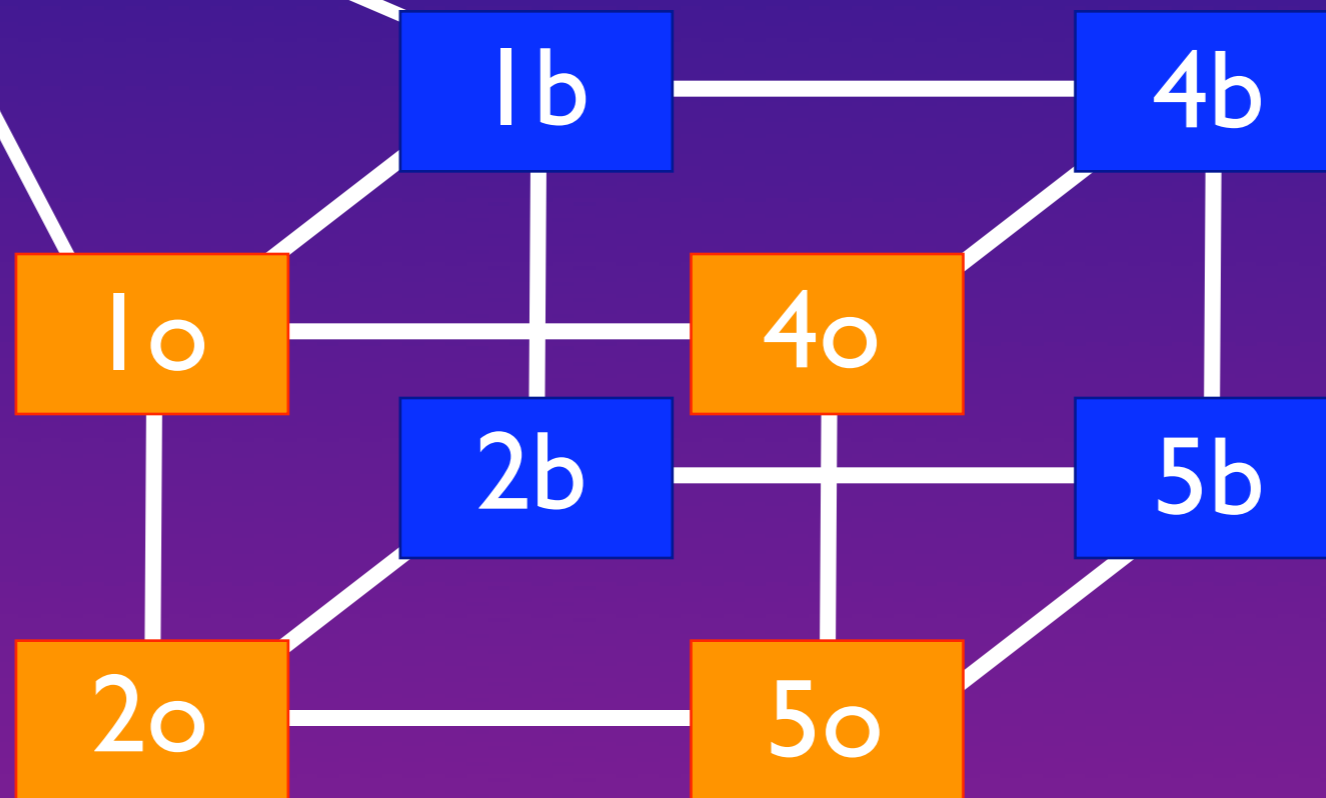
# Hot Topics

- What's going on with the UIUCnet core?
- New exit firewalls and spiffy new redundant exits
- New firewall group?
- Instrumentation, procedures, and tools in pursuit of network security
- Once more with feeling: network design implications for different central models



# UIUCnet Core Status

To exit structure and  
Internet



# UIUCnet Core Status

- Campus exit and existing distribution equipment connected redundantly to both sides of the core
- Buildings connected at 1 Gb/s to one “side” of the core; at slower speeds to older equipment
- Core-Core links fully redundant

# UIUCnet Core Status

- All main core devices are Foundry Jetcore gigabit Ethernet devices
- Provides highest performance Ethernet switching that we have seen
- Switching performance and link speed will last us 4+ years, but...

# UIUCnet Core Status

- Slightly tight on hardware cache space for Ethernet MAC addresses
- Could spend a lot of money to double it
- Can try to repartition slightly to favor one kind of performance over another (switching vs. routing etc.)
- Problem is we're asking these boxes to do both Ethernet switching and IP routing because of our sprawling VLANs

# UIUCnet Core Status

- Core device failures no longer affect traffic except for devices directly plugged into failed equipment
- Redundant connections possible by using *two pair* of gigabit fiber to a building, to both orange and blue sides

# UIUCnet Core Status

- Router redundancy obtained via two virtual router interfaces and VRRP-E protocol
- Physical redundancy obtained via 802.1d Spanning Tree Protocol
- Both work well for this purpose and are well-defined, but...



# New Core Gotchas

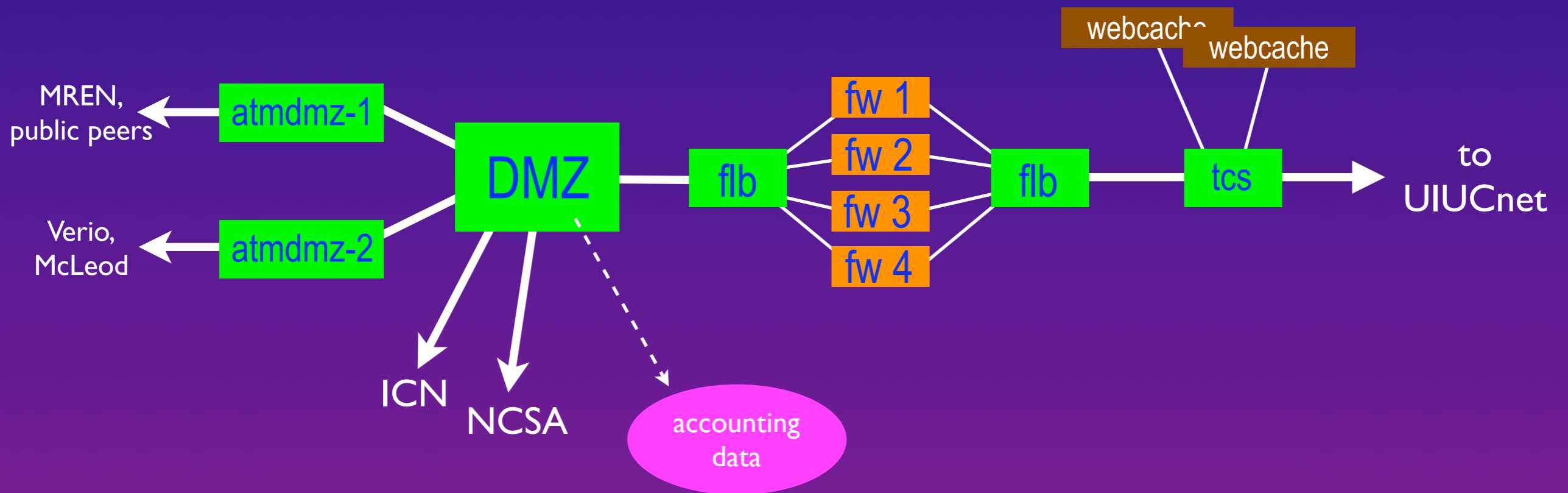
- So these features designed to improve reliability actually work to decrease it
- Which would you rather have?
- We keep planning for the big “node-busting outage” but it never occurs
- Reliability designs plan for catastrophes, not little instabilities

# Internet Access Status

- Last spring we were running on a non-redundant string of devices designed to provide:
  - Path selection and load balancing across multiple Internet Service Providers
  - Transparent web caching for participating customers
  - Multi-level firewall service for participating customers
  - Comprehensive accounting and flow logging for traffic counting and security purposes

# Internet Access Status

Exit Architecture until October 2003



# Internet Access Status

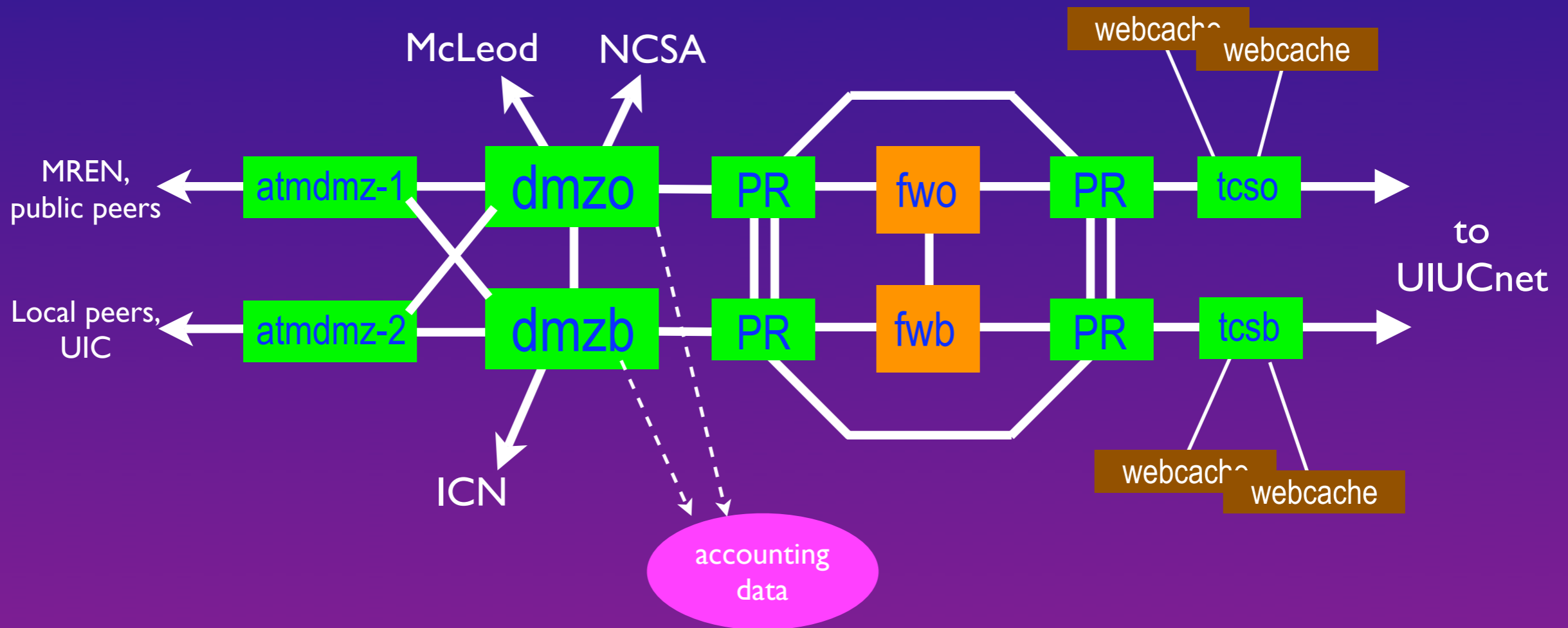
- Many single points of failure
- We had cold spares for everything, but outages were still a major headache and seriously impacted our uptime numbers
- Problem was, application-active devices like web caches and firewalls need to see traffic in both directions to do their job. Imagining redundant architectures was difficult

# Internet Access Status

For a parallel-active structure to function properly, packets would have to be switched in one direction based on *destination* address (easy) but returns would have to be sent back through the same path based on *source* address (hard...not the way IP routing normally works)

# New Exit Structure

As of October 2003





# New Exit Structure

## Features

- Failure of a dmz component causes Internet routing to switch to the other dmz (possible loss of half of our Internet bandwidth)
- Failure of a firewall or PR causes other firewall to take over (via HA feature)
- Failure of any links cause reroutes to the other path

# New Exit Structure

## Features

- “Firewall bypass” can be used to shunt damaging traffic around firewalls (e.g., extremely high-bandwidth or “poorly-behaved” research applications)
- This is done on a source-destination-pair basis

# New Exit Structure

- Now in full production with only a few minor issues left to work out
- TCS and web caches not yet in service
- Session sync of new firewalls has problems
- PR slightly “leaky” (1 out of 3000 packets or so--very rare)





# Fighting the Good Fight

- CITES acts as the custodian for Internet security for UIUC
- UIUCnet is instrumented with various (and growing) tools that allow us to identify and isolate compromised machines that pose a clear threat to the Internet or UIUCnet

# Fighting the Good Fight

- Netflow accounting data from the exit is our most valuable tool (although it cannot detect on-campus activity)
- Flows from all on-campus machines is summarized once per hour, and “odd-looking” patterns are either “eyeballed” or found using filters we have written to detect particular activity



# Netflow Data

## with MSBlaster/Welchia filter

Rank	Hostname	Total: Flows	%Src	%Sink	
1	hijack10001.tn.ttu.edu	5,236	81%	18%	
2	hijack10002.tn.ttu.edu	4,360	83%	16%	
3	cyclops.cso.uiuc.edu	34	0%	100%	
4	argus.cso.uiuc.edu	31	0%	100%	
5	firefly.prairienet.org	14	42%	57%	
6	apache.itg.uiuc.edu	9	55%	44%	
7	par1698.urh.uiuc.edu	8	0%	100%	
8	gutenberg.press.uiuc.edu	7	71%	28%	
9	ups05.ks.uiuc.edu	7	57%	42%	
10	t-node2-1.gw.uiuc.edu	6	100%	0%	
11	relay3.cso.uiuc.edu	6	0%	100%	
12	pc2.reec.uiuc.edu	6	50%	50%	
13	fshn3218.foods.uiuc.edu	6	50%	50%	
14	aa26.aae.uiuc.edu	6	50%	50%	
15	bi-hsrp2-2167.beckman.uiuc.edu	6	100%	0%	
Hosts: ( 818)		GRAND TOTAL:	16,403	54%	45%

# Interdiction

- **Firewall block** prevents machine's IP address from accessing or being accessed from off-campus systems (still works on campus)
- **Router ACL block** prevents machine's IP address from accessing anything off its subnet
- Both of these provide logging of access attempts

# Interdiction

- **Switch MAC address block** prevents machine's hardware address from accessing anything off its subnet (no matter what IP address it is given)
- Most used method now since it (mostly) prevents moving IP addresses to regain functionality
- However there are limited numbers of these available on core equipment, and no logging is performed

# Interdiction

- **Port disabling** completely cuts machine off networks (hopefully we don't get into a chase as the user then moves from jack to jack)
- Only possible on CITES-controlled switches
- Can be the cleanest method where it works

# Interdiction

- **Building disabling** is the most drastic measure at our disposal
- Used only as a last resort to protect UIUCnet from damaging traffic
- Used only when CITES has no access to in-building switching equipment

# Prevention

- **Antispoofing filters** prevent traffic from leaving a subnet which does not contain a source on that subnet
  - Prevents many kinds of DOS attacks
  - Prevents misconfigured machines from getting traffic on the backbone
- Only in limited deployment due to Foundry resource allocation issues, but very close
- Firewalls do this for all of UIUC address space at the exit

# Prevention

- CITES *strongly* recommends you take advantage of the provided firewall service and put desktop machines in the “fully closed” group
- The firewalls provide unilateral filtering of some traffic
  - SNMP
  - Port 1434 (slammer worm)
  - MS Networking ports

# How (We) You Can Help

- We'd like to provide better tools to help departments track down compromised and unauthorized machines
- You need to be able to find such machines by jack number on your network

# How (We) You Can Help

- A database of IP-to-MAC and MAC-to-switchport associations already mostly exists for any switch being managed by IRIS
- Network Engineering continues development of this, and will be integrating the information and database lookups into IRIS itself

# Database Example

Last Seen Data for 130.126.113.4:

FQDN	IP	Last MAC	First Seen	Last Seen	Router
spiffy.cso.uiuc.edu	130.126.113.4	0090.27ea.9274	11/13/2003 15:33	11/20/2003 01:55	core1o

Port Data (experimental!)

Switch	Port	Port Mac Count	Last Seen
sw-dcl3	FastEthernet7/9	1	11/20/2003 01:55

Historical records for 130.126.113.4:

FQDN	IP	Mac	First Seen	Notes
spiffy.cso.uiuc.edu	130.126.113.4	0090.27ea.9274	11/13/2003 15:33	MAC change
spiffy.cso.uiuc.edu	130.126.113.4	0030.654b.a2c4	3/27/2003 20:03	

# Other Latent Features

- Many switch security features are there for the asking, and merely need to get support into IRIS to be available
- One good example: port security, which locks a port to the first learned MAC address and disables the port if a different MAC appears... prevents abuse of ports in public locations

“Not in all,” he murmured with a smile. “Time is forever dividing itself toward innumerable futures and in one of them I am your enemy.”

-- Jorge Luis Borges, *The Garden of Forking Paths*

# Architectural Matters

## The Good, the Bad, and the Ugly

- What else can be done by CITES or by departments to improve IT security from a network perspective?
- What should we *not* do?
- What's possible but not among the best ideas?

# The Good

- CITES Network Engineering continually researches products and technologies that might help
- Intrusion Protection Appliances look really promising, but there are too many places they would need to be placed, and they're expensive
- Better monitoring and detection is not so hard, and in the works, but a little like closing the barn door after the horse is out

# The Good

- Router ACL's perform at wire speed on the core and can be used for more than just antispoofing
  - Optional internal blocks of "bad" ports such as 135
  - Where possible, block known bad patterns such as Welchia
  - Block access to/from "unfriendly" subnets (a little scary)
- Encourage site licensing of "personal firewall" products such as zonealarm and the built-in firewall features of XP and Linux





# Questions + Wrapup