SECURE NETWORK PERFORMANCE TESTING USING NTAP

Dr. Charles J Antonelli
The University of Michigan
10 April 10

Contributors

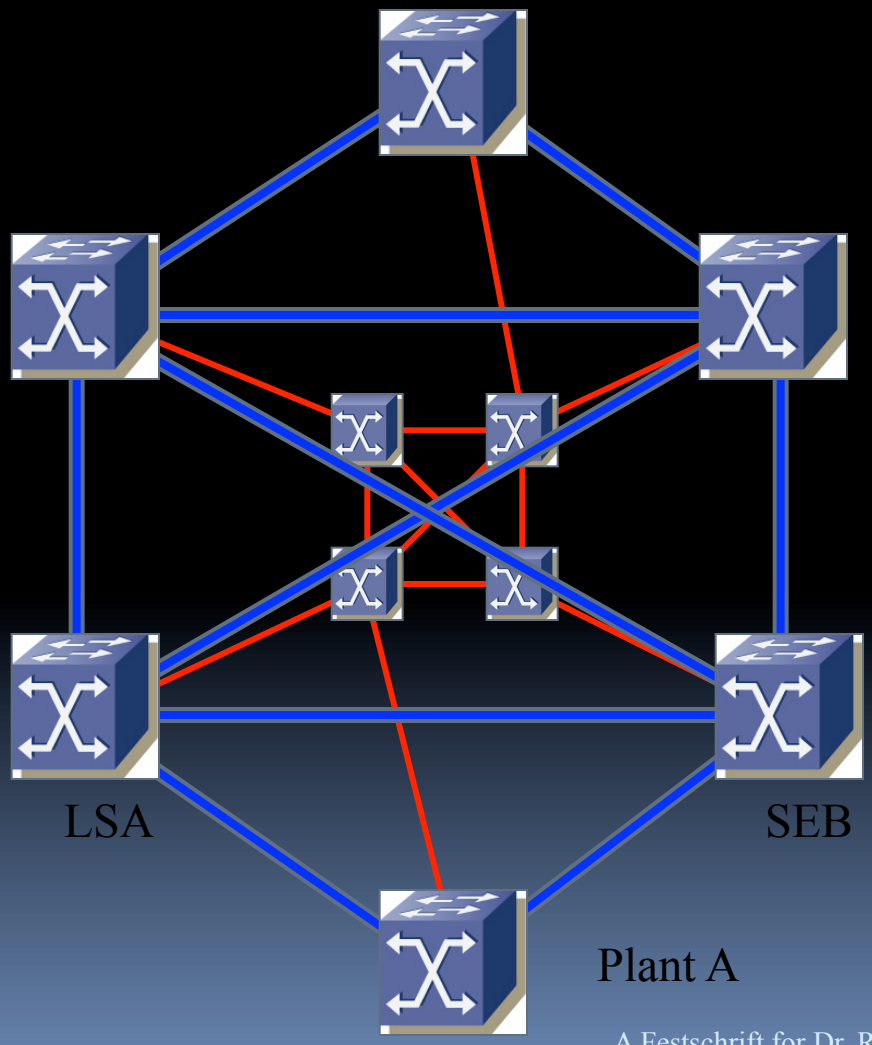
- U-M Center for Information Technology Integration
  - Andy Adamson, Charles Antonelli, Olga Kornievskaia, Peter Honeyman, Nathan Gallaher, David Richter
- U-M MGRID
  - Jim Irrer, Beth Kirschner, Shawn McKee
- U-M ITS Comm
  - Roy Hockett, Walt Reynolds

Work supported by U-M OVPR and ITS Comm

Roadmap

- Motivation
- SeRIF Framework
- NTAP Instance
- Future Work

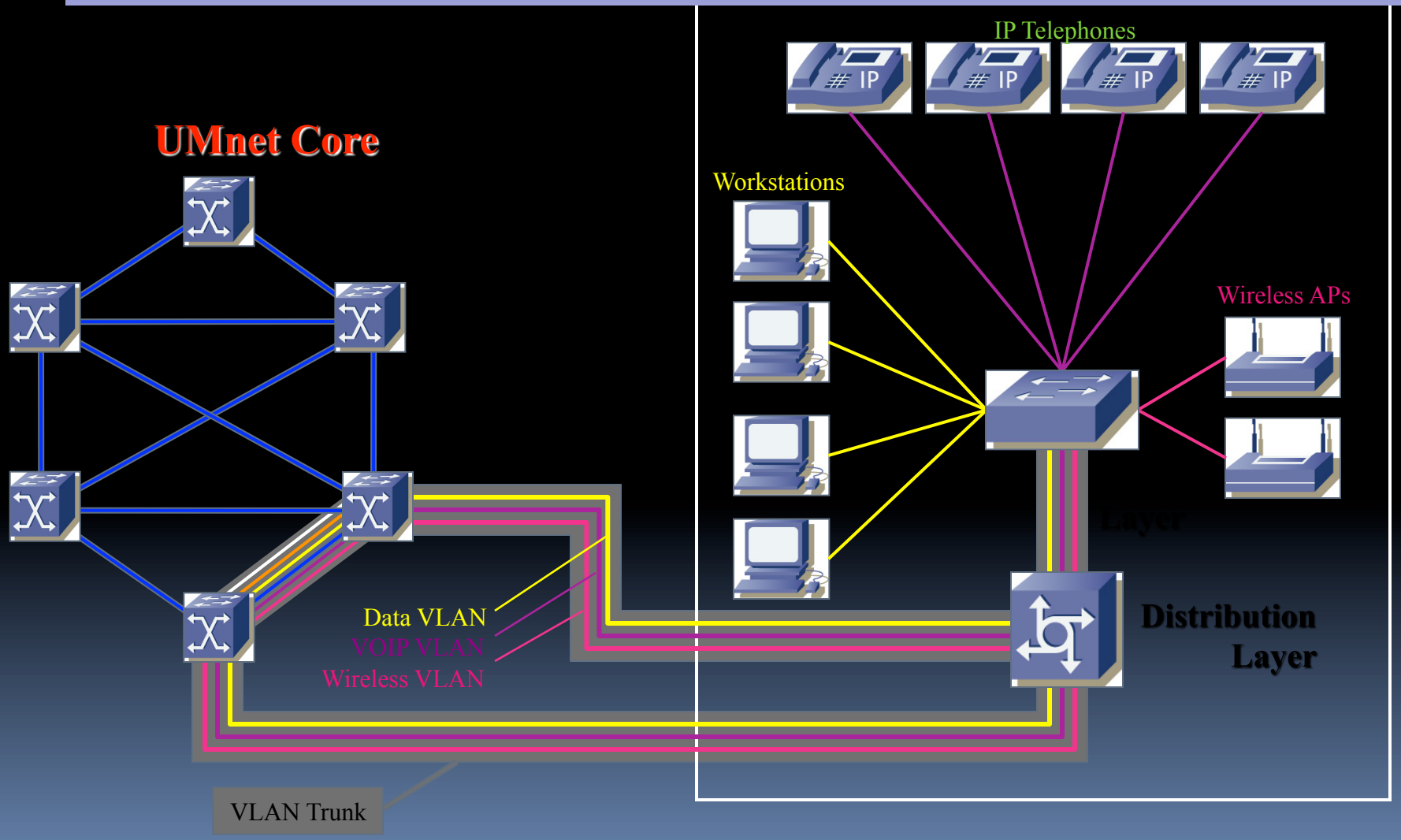
U-M Core Campus Network 2007



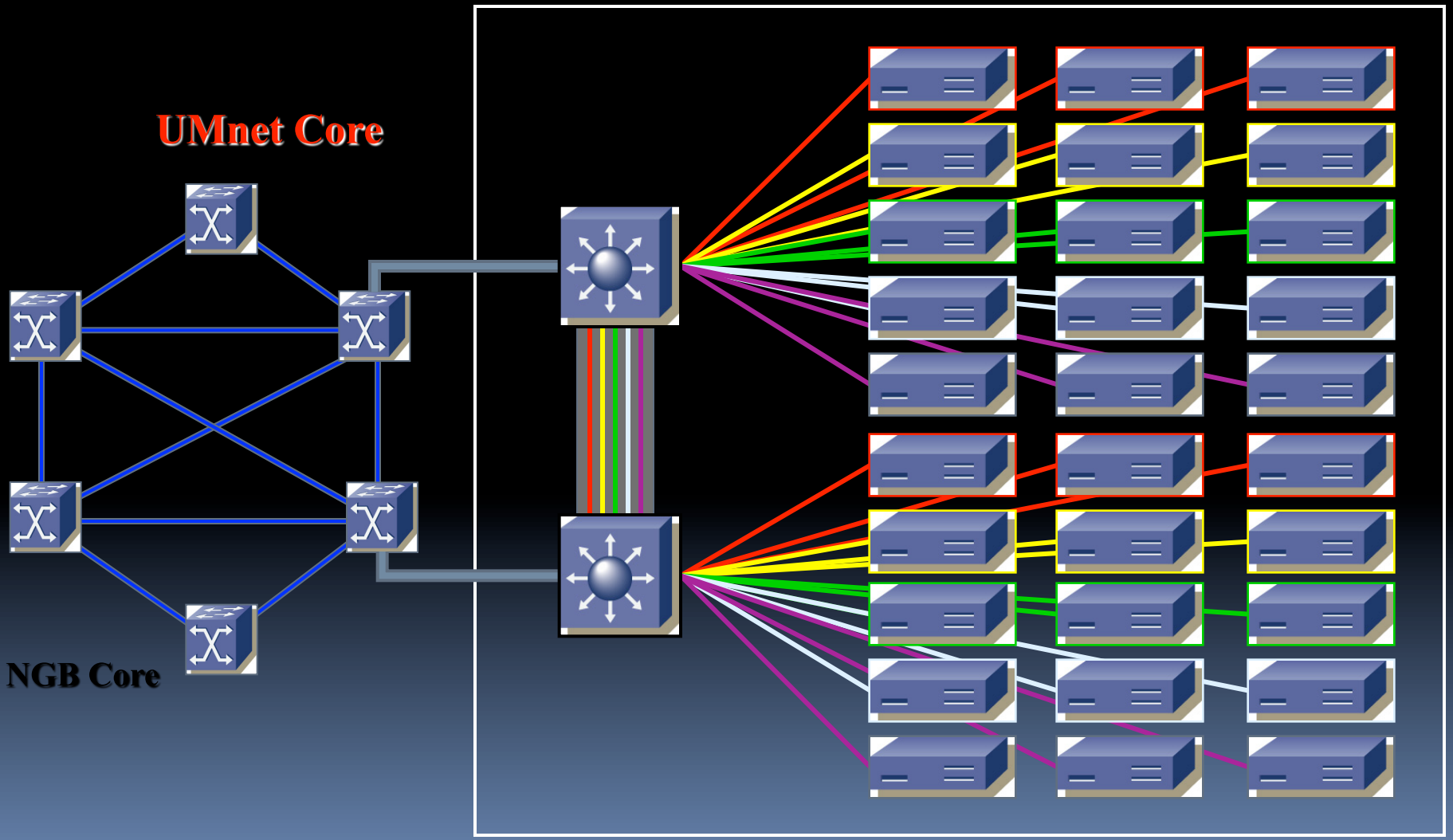
10 Gigabit Ethernet

ATM OC3c/OC12c
(Previous Gen)

U-M Campus Network 2007



U-M Campus Network 2007



Motivation

- End-to-end functionality & performance
- Where is the problem?
  - Few existing tools
  - Manual procedures
  - Little sharing of techniques & results
  - No end-to-end capabilities
  - Poor security

Requirements

- Secure operation
  - Authentication, communication, authorization, execution
- Authentication
  - Strong, time-limited credentials
- Authorization
  - Fine-grained, by actor and activity
- Information storage
  - Secure, scalable, visualization
- Extensible
  - Add arbitrary operations
- Leverage existing campus systems

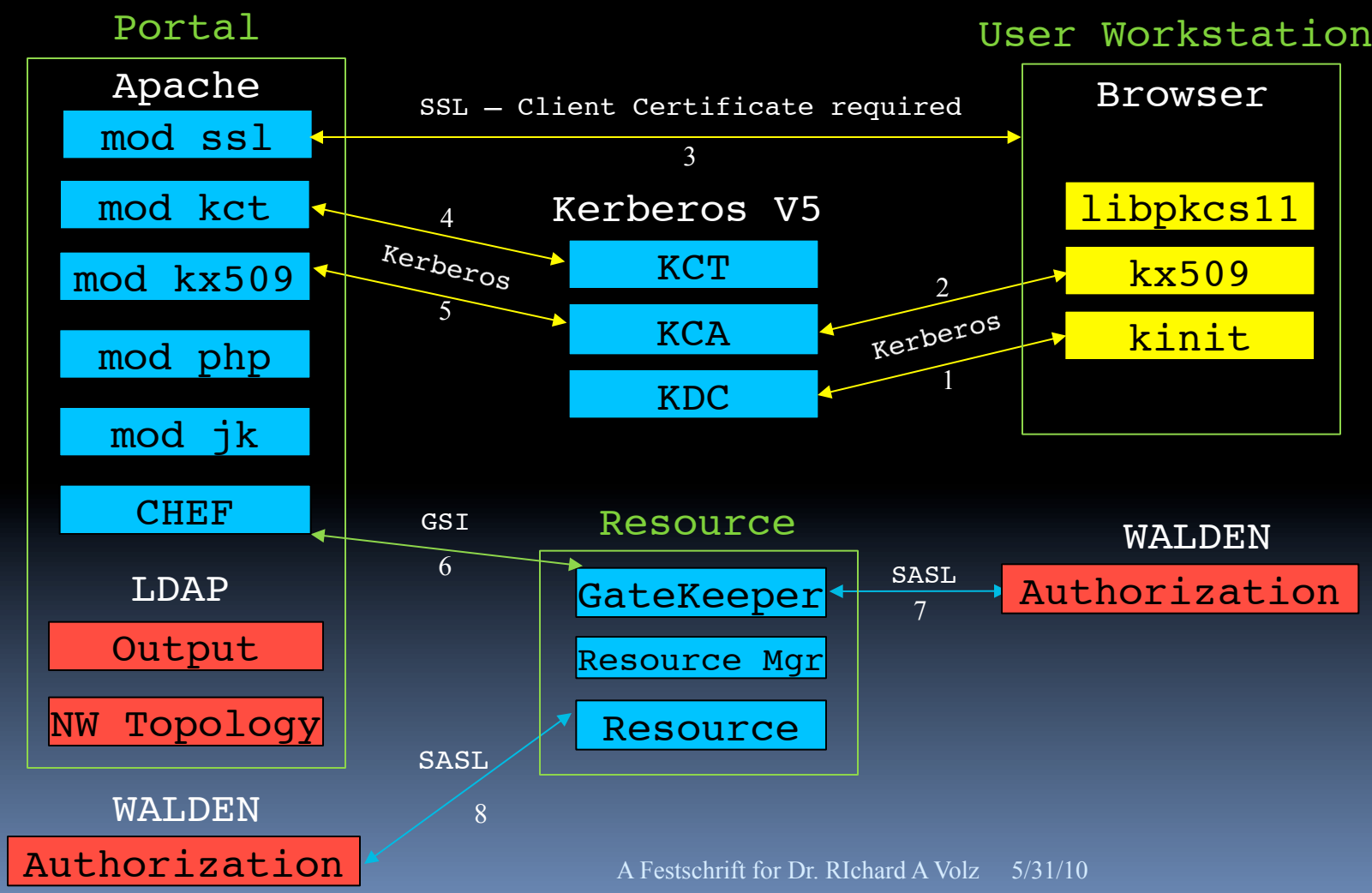
SeRIF

- *SeRIF* : Secure Remote Invocation Framework
- *Purpose* : provide a secure and extensible remote process invocation service, with strong authentication and flexible authorization

SeRIF Architecture

- Central portal host
  - Authentication
  - Control (invocation, parameters, results)
  - Databases (LDAP)
- Dedicated remote nodes
  - Gatekeeper
  - Local scheduler for execution and cleanup
  - Provides status and output redirection
  - Fine grained authorization at resource
- Based on Globus, GARA
- Adds fine-grained authorization
  - Walden

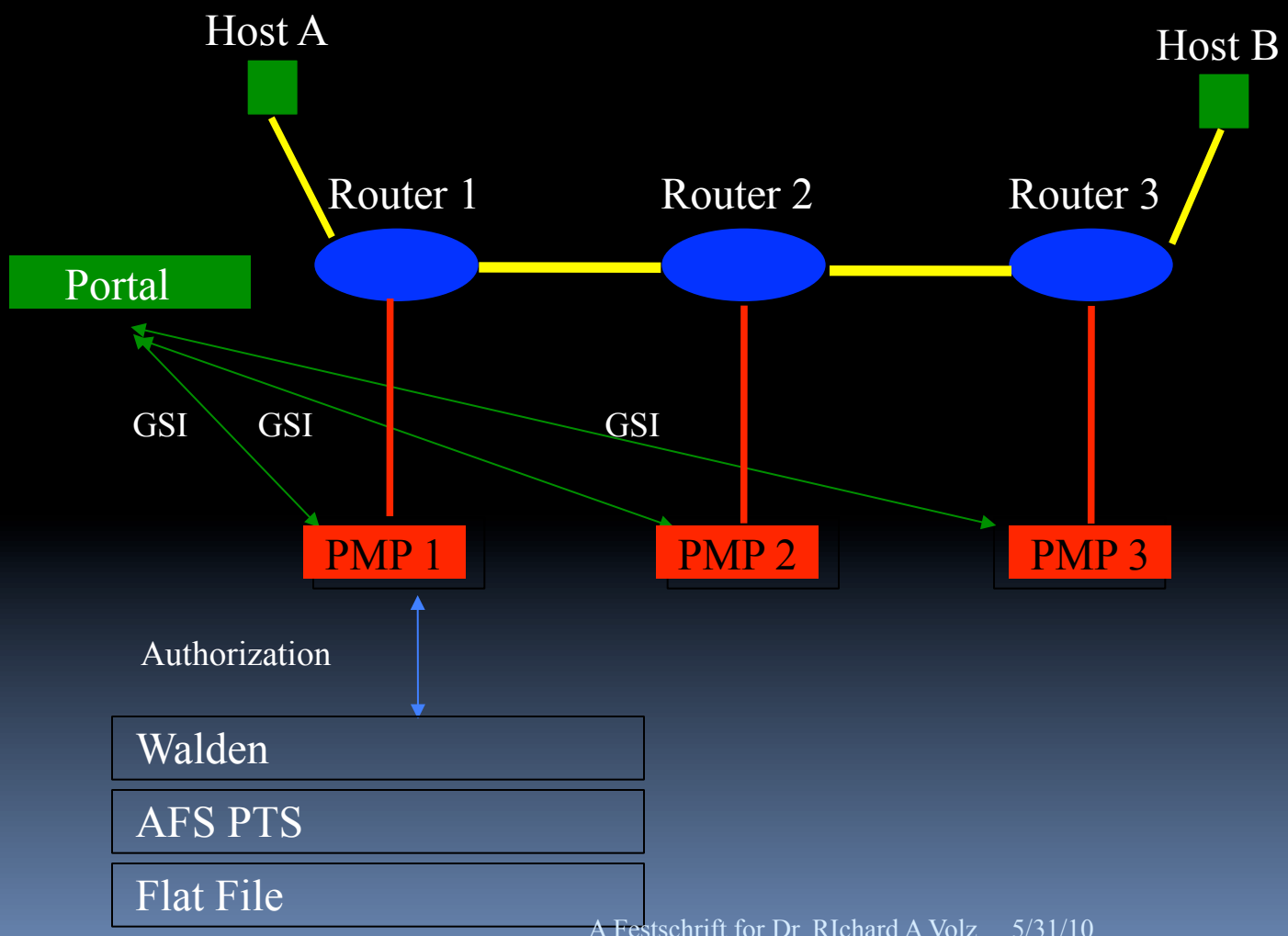
SeRIF Architecture



NTAP

- *NTAP* : Network Testing and Performance
- *Purpose* : provide a secure and extensible network testing and performance tool invocation service at U-M
- Uses SeRIF framework
- Runs on portal host and Performance Measurement Platforms (PMPs) attached to routers in a VLAN environment

NTAP Architecture



NTAP I

- Bandwidth reservation tool:
  - Securely modifies network switch configurations to provide differentiated services
  - Based on GARA extension
    - "General-purpose Architecture for Reservation and Allocation"
    - Layered on Globus
    - Includes scheduler for future reservations
  - Implements modular, fine-grained, role-based authorization
    - Added signed group membership(s) to reservation data
    - Keynote policy engine / AFS PTS group service

NTAP II

- Added PERMIS authorization plug-in
- Generalized to run *securely* arbitrary programs at a Grid service endpoint
- Automatic path discovery
  - traceroute & topology database
- Multihomed PMP support
  - source address selects per-VLAN route
- Production hardening
  - recovery, packaging & installation

Output Database

- Test program outputs captured
- Stored in LDAP database
- Database display tool
  - Output hop-by-hop matrix display
  - Color-coded test history
  - Click through cells for detailed views
    - Links to most recent tests
  - Config file for rapid prototyping

NTAP III

- Deployment
  - PMPs deployed at CITI, ITCom, Merit
- 10 Gbps PMPs
  - PCI-X vs. PCI-X V2.0 vs. PCIe
- Walden authorization plug-in
- Additional Path Testing
- Host Endpoint Testing
- Automated Testing
- Profile-based Interface

Walden

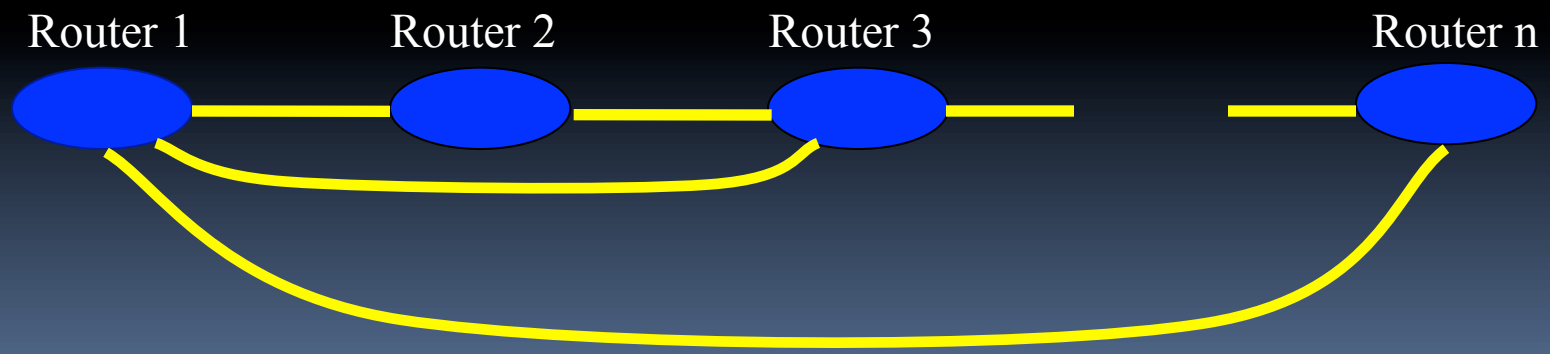
- Fine-grained authorization at gatekeeper
- Walden policy engine / XACML policy file
  - Resource, Action, Subject attributes
- Demo policy
  - Any authenticated principal may run a test on designated PMPs
  - Specific principals may run a test on any PMP

Walden

```
*** Resource (e.g., host machine)

<Resource>
 <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">

  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
  ldemo9.citi.umich.edu</AttributeValue>
  <ResourceAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
      AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"/>


*** Action (e.g., run gara-service, or run pbs job mgr)

<Action>
 <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">

  <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
  gara-service</AttributeValue>
  <ActionAttributeDesignator DataType="http://www.w3.org/2001/XMLSchema#string"
      AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"/>
```

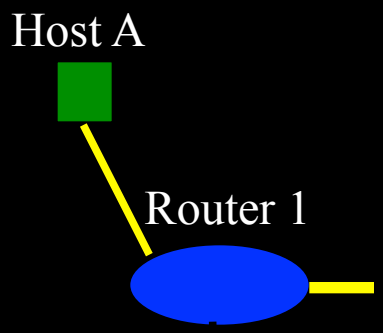
Additional Path Testing

- Adds customer-specified tests to schedule
  - endpoint - add R1-Rn
  - cascade - add R1-R2, R1-R3, …, R1-Rn



Host Endpoint Testing

- First mile problem
  - Leverages Network Diagnostic Tester
- Uses JavaWebStart to run signed apps on client
  - Client downloads NDT app
    - Multi-step process
    - User clicks two links
  - Client identifies first-hop router and attached PMP running NDT server
  - Client runs NDT test and displays results as usual
  - NDT server sends results to NTAP database



Automated Testing

- Need repetitive, automated testing
  - … but with secure authentication and authorization
- Solution: renewable credentials
  - User obtains long-term credentials
  - Portal schedules repetitive testing
  - Prior to a test cycle, portal validates long-term credential and derives from it a short-term credential
  - Rest of SeRIF architecture unchanged

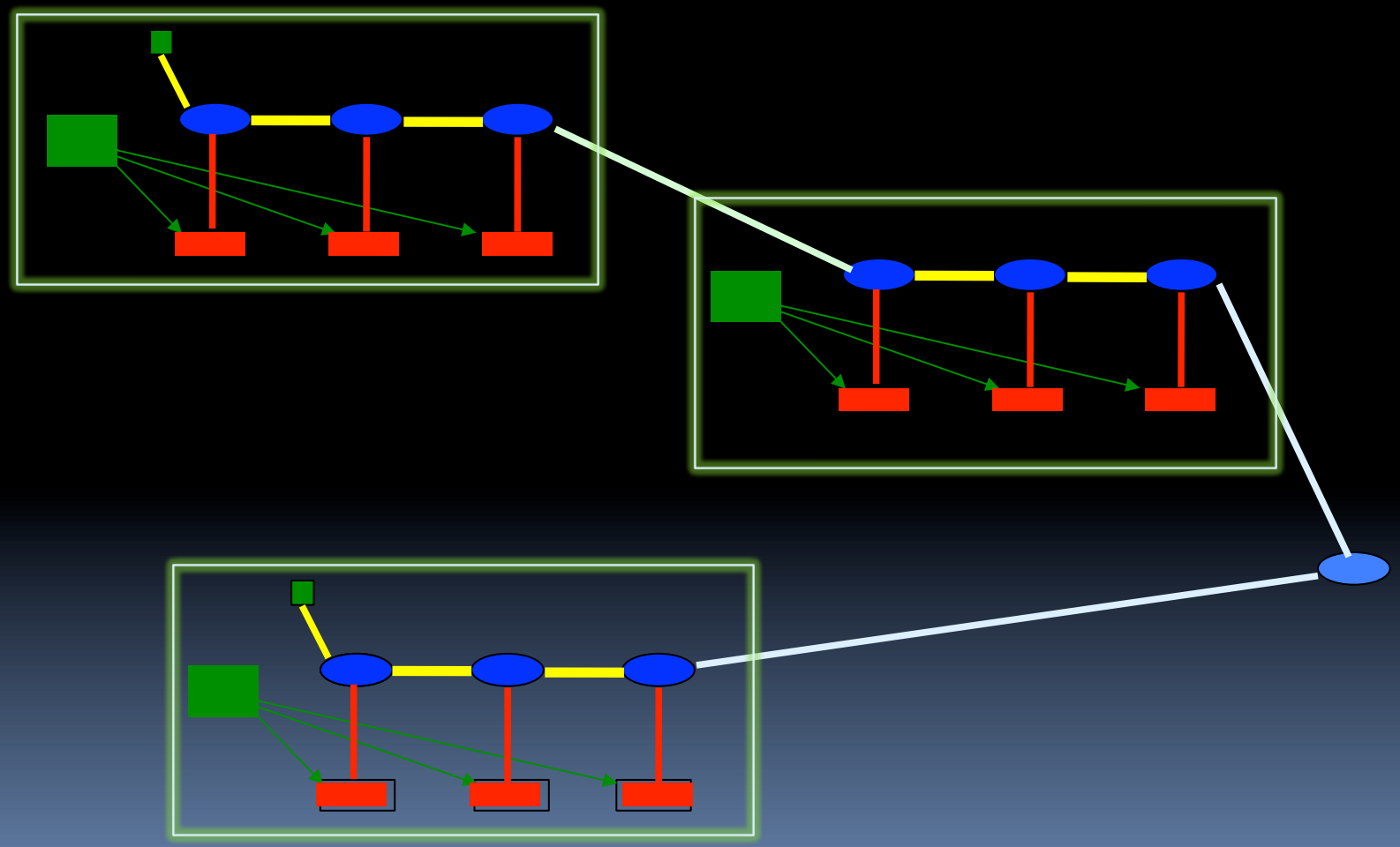
Profile-based Interface

- Tests specified via *test profile*, composed of
  - A *path map*
  - One or more *application profiles*
  - An *output profile*
- Database of path maps and profiles
  - Segment mapped or user-specified
  - Captures common test configurations
  - Leverages testing expertise
- Maps and profiles stored in LDAP database

Future Work

- Statistical, longitudinal summaries
- Graph the topology database
- Alternatives to topology database
  - Active infrastructure probing
- Automated tools
  - Tune TCP stack (NDT)
- Cross-domain measurements

Cross-Domain SeRIF



Cross-Domain SeRIF

- Cross-domain authentication
  - Globus, Shibboleth, …
  - Local authentication (CoSign, …)
- Cross-domain authorization
  - Who can inject packets into my network core?
  - With whom will I share results?
- Replicated portals
  - Inter-portal protocol

SeRIF Resources

- SeRIF & NTAP
  - http://www.citi.umich.edu/projects/ntap
- Frameworks
  - Globus http://www.globus.org/
  - GARA http://qos.internet2.edu/houston2000/proceedings/Roy/20000209-QoS2000-Roy.pdf
  - Walden http://www.mgrid.umich.edu/projects/walden.html
- Tools
  - iperf http://sourceforge.net/projects/iperf/
  - ndt http://e2epi.internet2.edu/ndt/
  - owamp http://e2epi.internet2.edu/owamp/
- References
  - Andy Adamson and Olga Kornievskaia, "A Practical Distributed Authorization System for GARA," CITI Tech Report #01-14, Center for Information Technology Integration, The University of Michigan, 2001.

Any Questions?