Secure Network Performance Testing using SeRIF

Charles J. Antonelli
Center for Information Technology Integration
University of Michigan

Laurence Kirchmeier
MERIT, Inc.

21 June 2005

Contributors

- CITI
  - Andy Adamson
  - Olga Kornievskaia
  - David Richter
  - Nathan Gallaher
- MGRID
- ITCom

Work supported by OVPR and U-M ITCom

center for information technology integration

MGRID

merit NETWORK INC

SeRIF

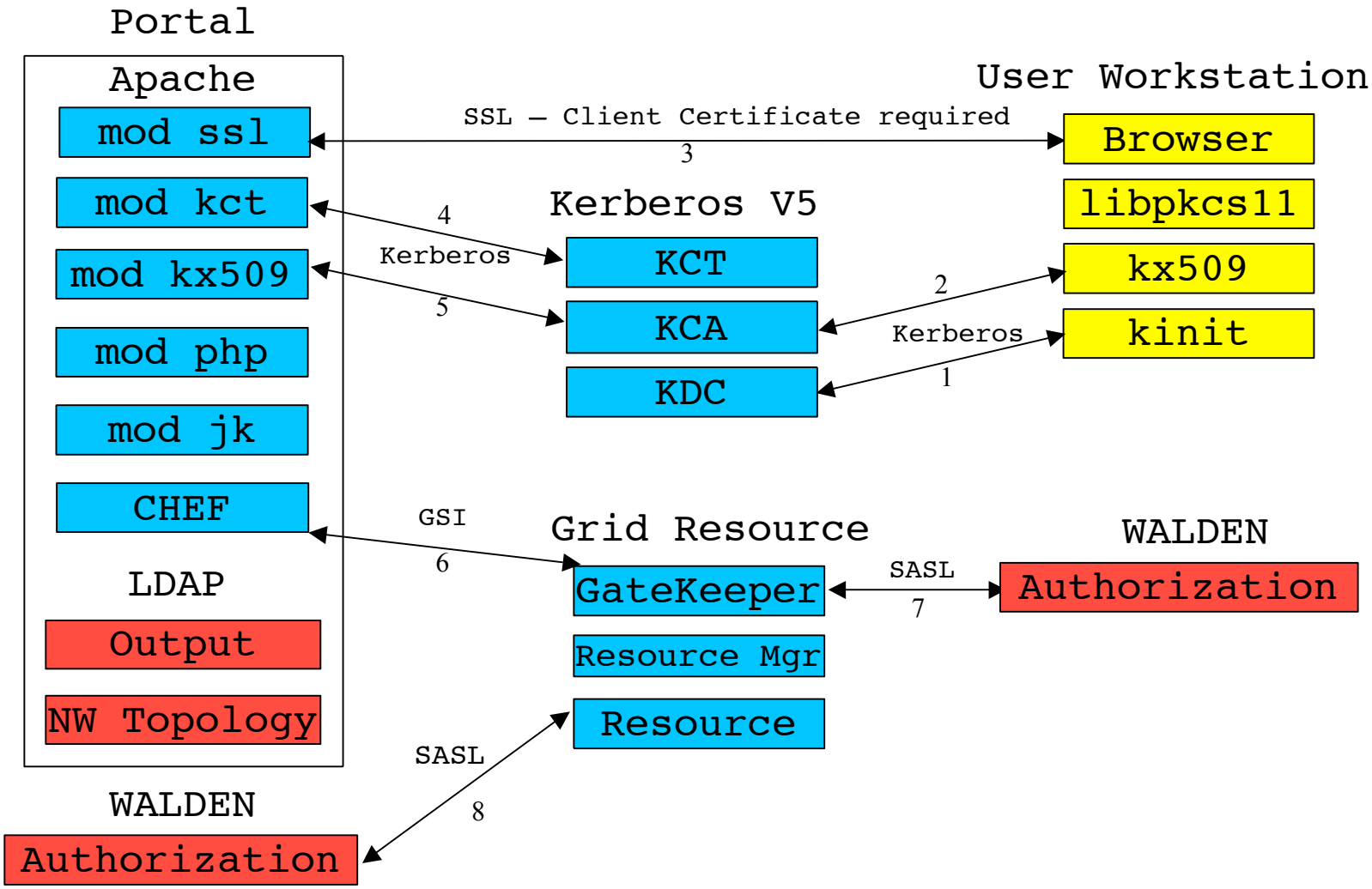
- *SeRIF* : Secure Remote Invocation Framework
- *Purpose* : provide a secure and extensible remote process invocation service, with strong authentication and flexible authorization
- Based on Globus, GARA
- Adds fine-grained authorization
  - Walden

SeRIF

- 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

SeRIF Architecture

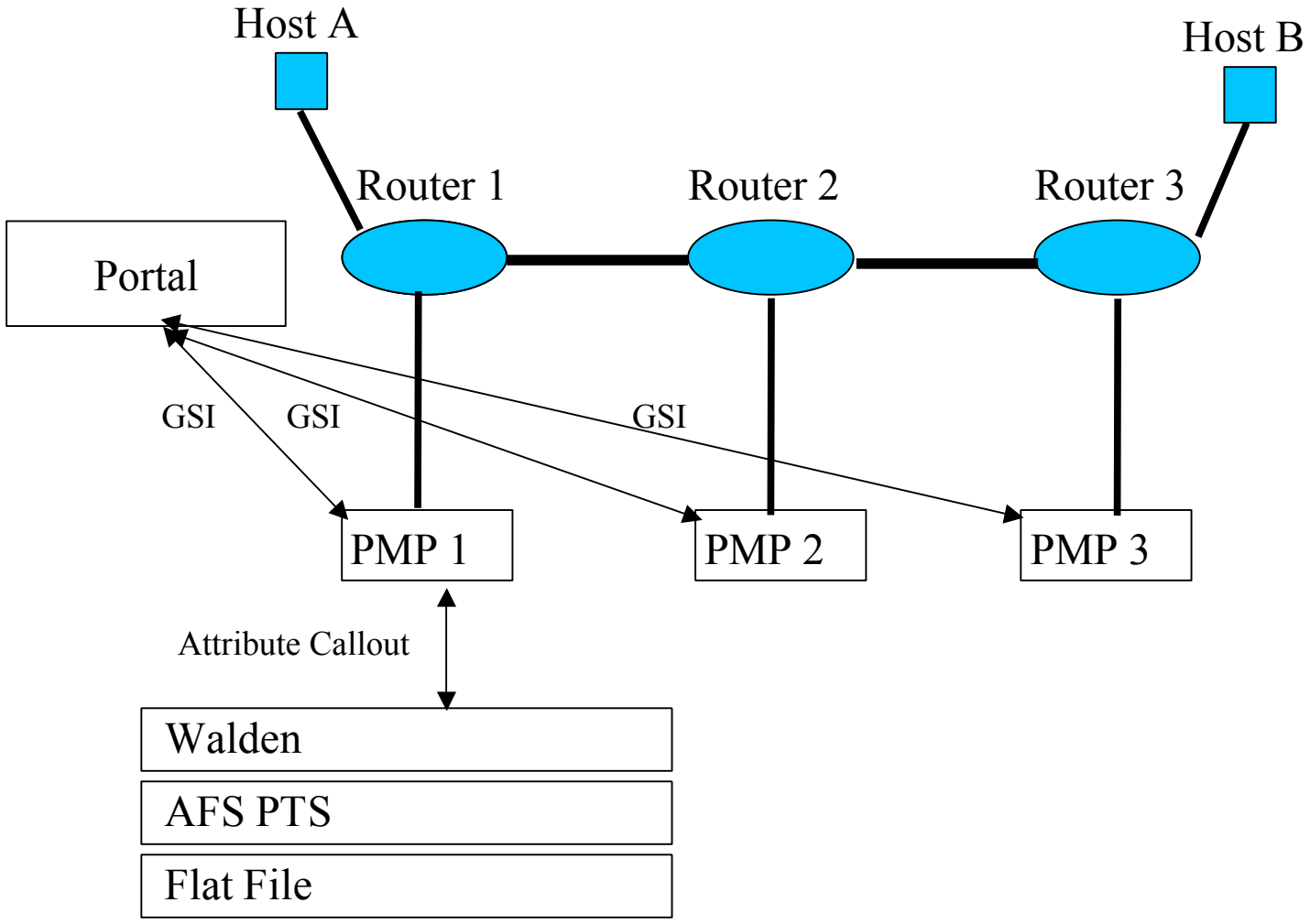


NTAP

- *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

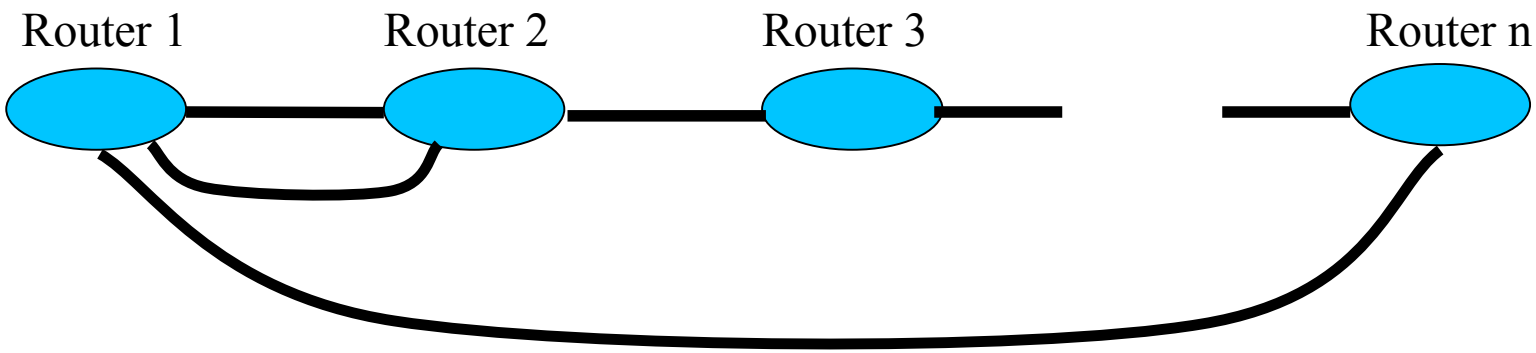
- Fine-grained authorization at gatekeeper
- Walden policy engine / XACML policy file
  - Resource, Action, Subject attributes
- Demo policy
  - Any authenticated principal may run a test on designated PMPs
  - Specific principals may run a test on any PMP

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"/>
```

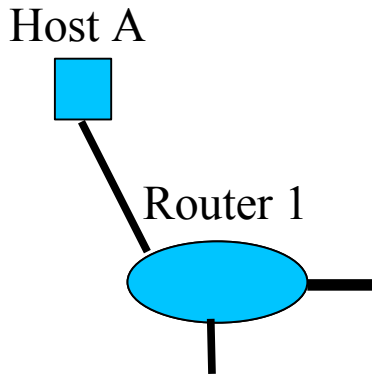
Additional Path Testing

- 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

- Post-processed statistics, graphs
- Cross-domain testing
- Alternatives to topology database
  - Active infrastructure probing
- Automated tools
  - Tune TCP stack
  - Detect conditions, e.g. duplex mismatches
- Graph the topology database

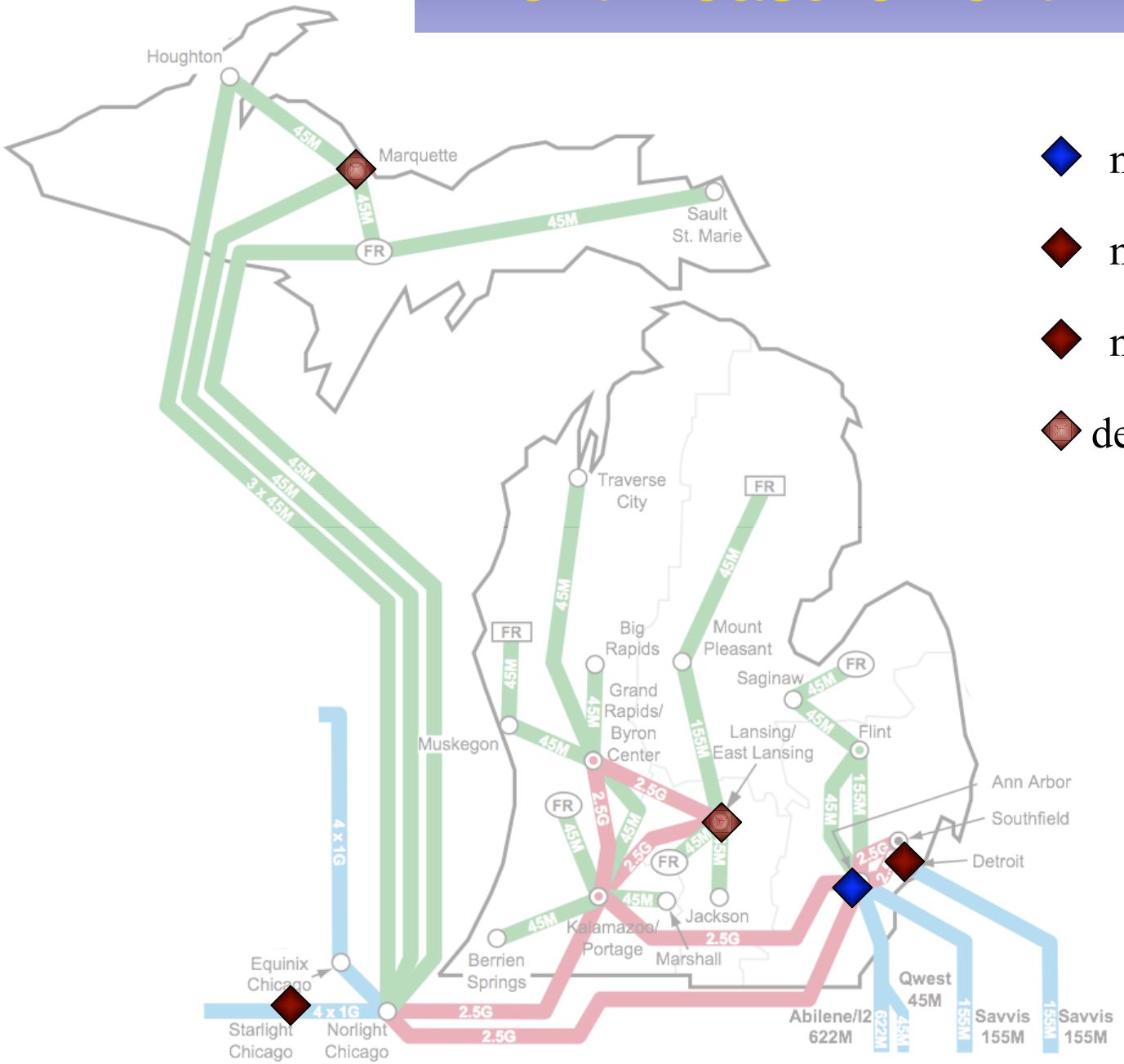
SeRIF Resources

- SeRIF & NTAP home page
  - http://www.citi.umich.edu/projects/ntap
  - FAQ & documentation
  - Download NTAP code & installation instructions
- Tools
  - iperf http://dast.nlanr.net/Projects/Iperf/
  - ndt http://e2epi.internet2.edu/ndt/
  - owamp http://e2epi.internet2.edu/owamp/

Merit's Measurement Infrastructure

- Goals
  - Provide measurement servers located across MichNet
  - Permit ad-hoc measurements to these servers for members and affiliates
  - Perform regular measurements between the servers to track the health of MichNet
  - Tie in MichNet servers with UM's ntap servers & Internet2 measurement infrastructure

Merit Measurement Infrastructure

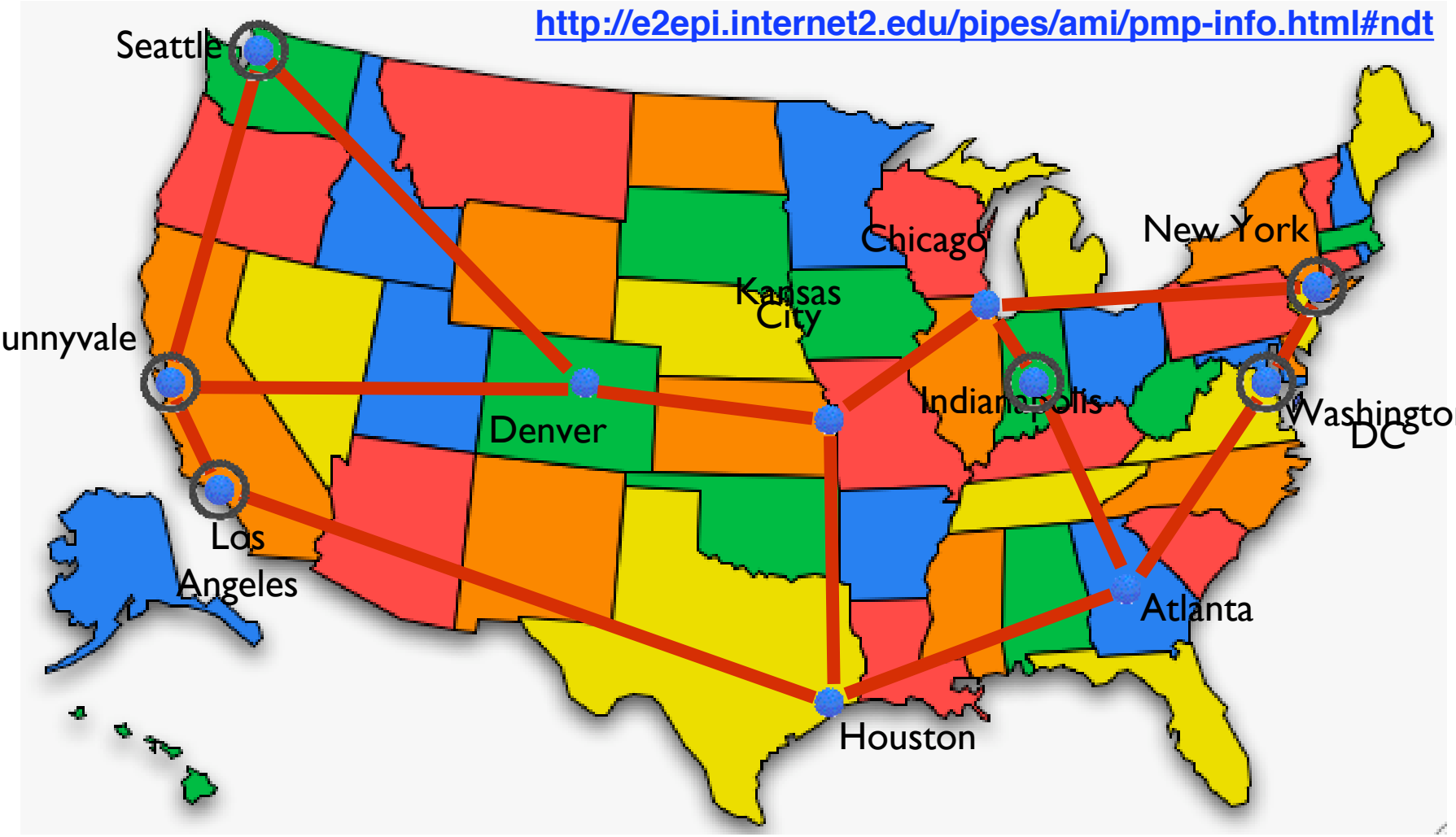


- ntap1.merit.edu
- ntap2.merit.edu
- ntap3.merit.edu
- deployment later summer

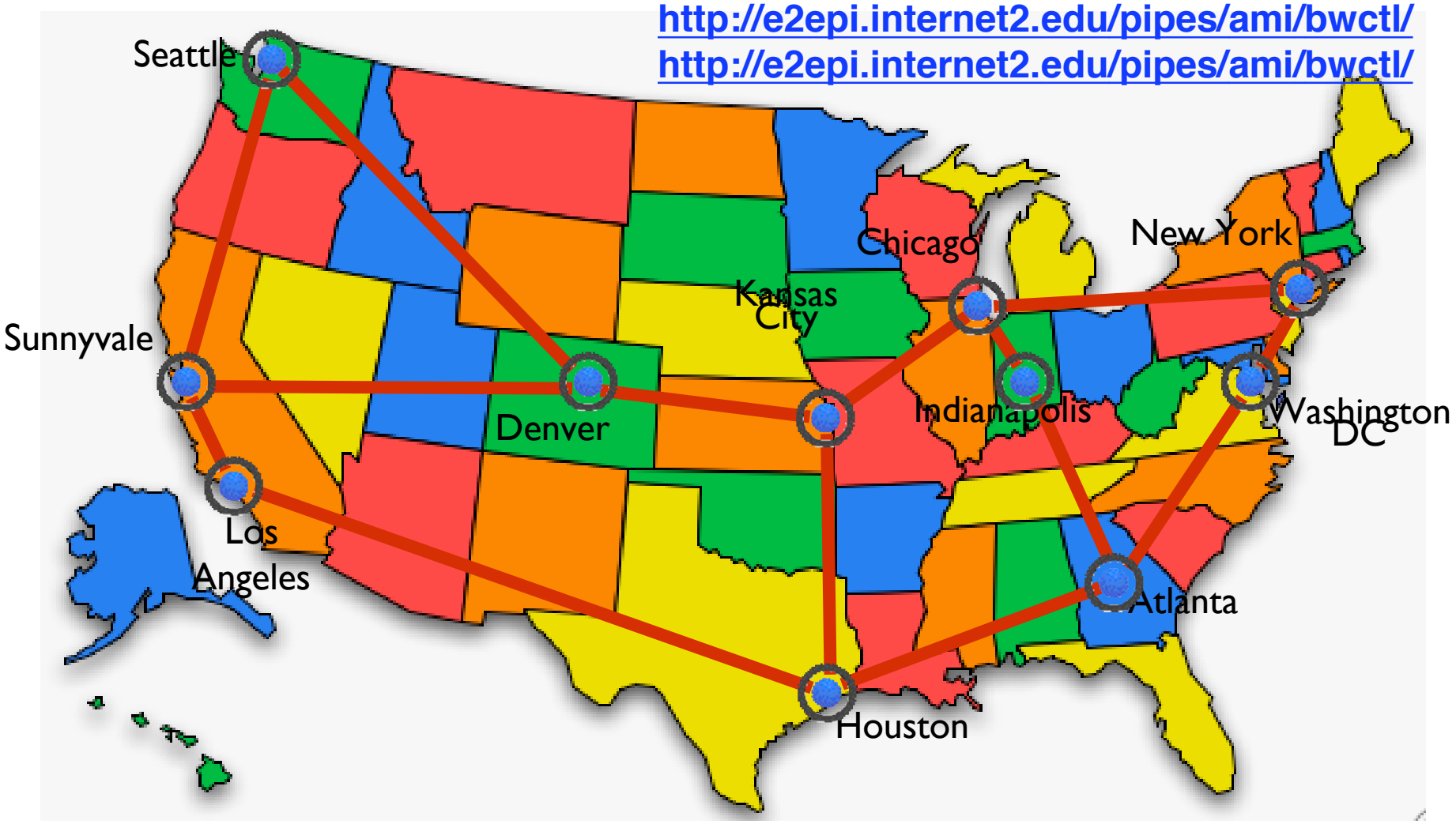
Merit's Measurement Infrastructure

- Measurement tools available
  - ndt
    - Last mile network diagnostic tool
  - owamp
    - One-way ping tool
  - bwctl
    - Bandwidth test controller
- ntap provides strong authentication and authorization to these tools
- See http://e2epi.internet2.edu for more information on these tools

Internet2 ndt servers



Internet2 bwctl & owamp servers



Merit's Measurement Infrastructure

- Next steps
  - Deploy measurement servers
  - Develop report web pages and front-ends to the tools
  - Work with members and affiliates -Internet2 measurement workshop?
  - Review other measurement tools such as Mona Lisa
- Lunchtime BOF on E2E performance and measurement

Merit's Measurement Info

- resources
  - Merit Measurement web pages
    - http://www.merit.edu/nrd/projects/e2e.html
  - Internet2 Measurement Performance workshop
    - http://e2epi.internet2.edu/network-perf-wk/index.html
  - Email:
    - e2einfo@merit.edu

MGRID NTAP Project

Demonstration

Any Questions?

http://www.citi.umich.edu