Network Testing and Performance Using SeRIF

Charles J. Antonelli
David Richter
Olga Kornievskaia
Nathan Gallaher

Center for Information Technology Integration
University of Michigan

Work supported by U-M ITCom

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

MGRID

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

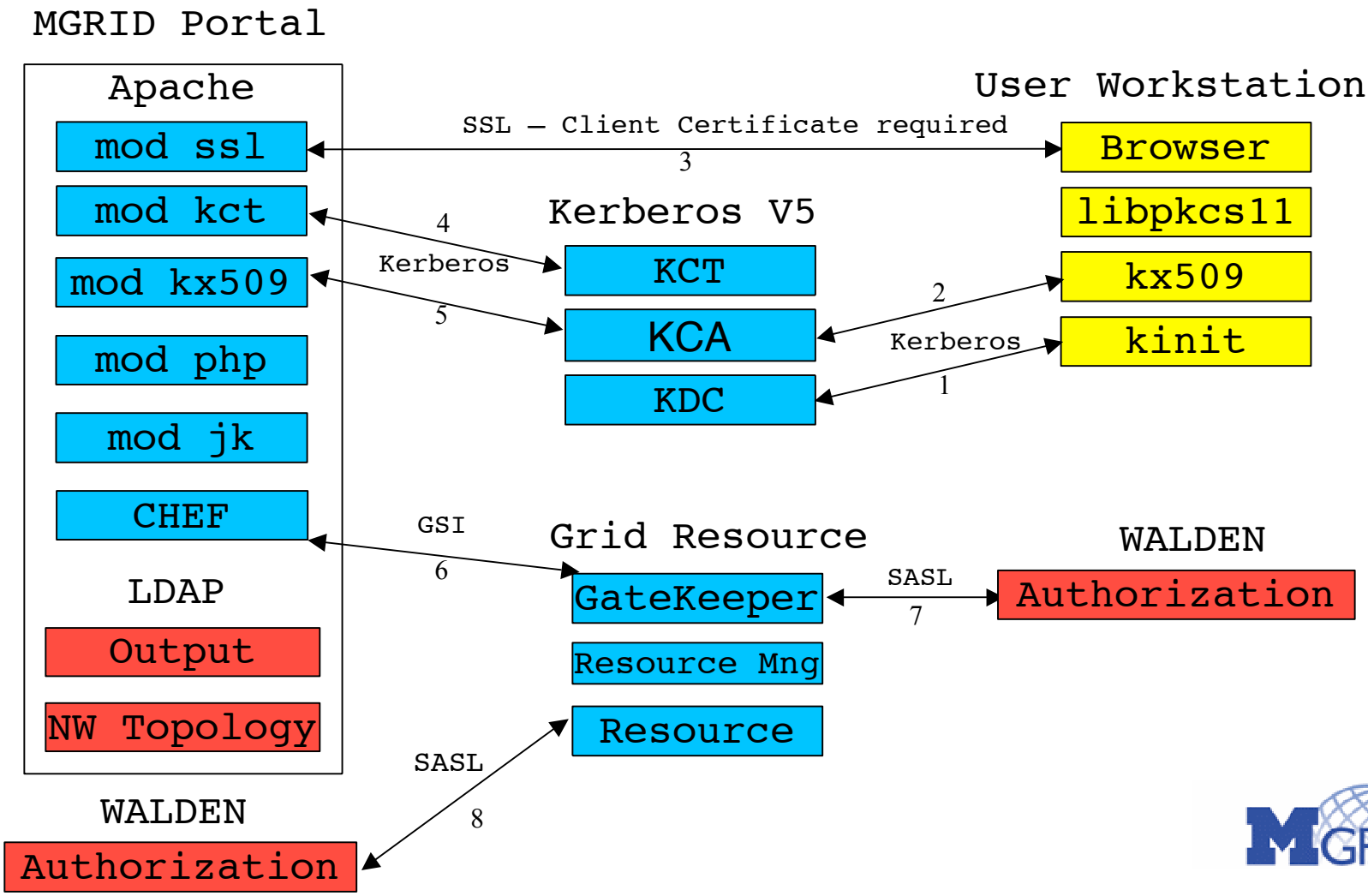
MGRID

NTAP

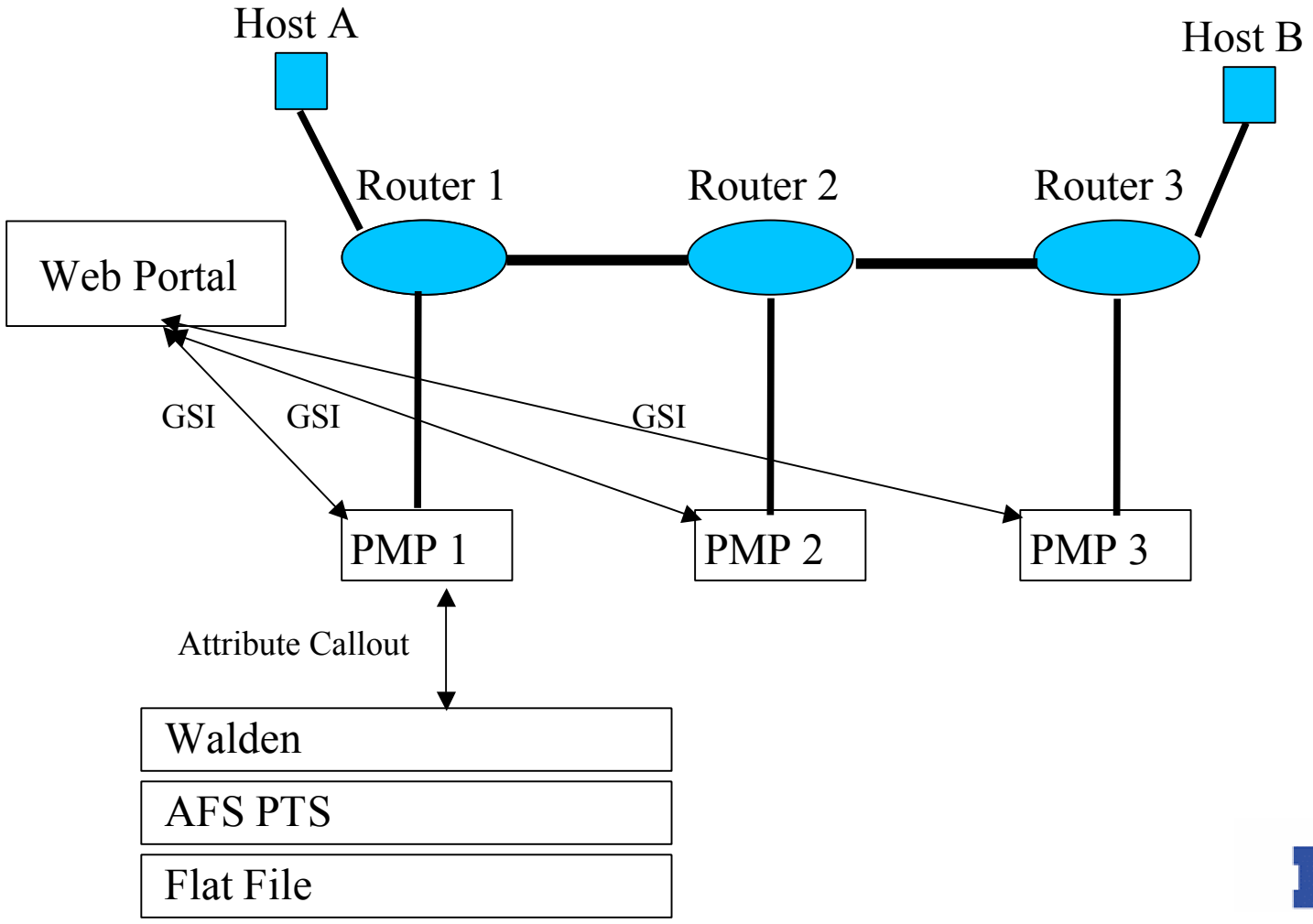
- *NTAP* : Network Testing and Performance

- *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

MGRID Architecture



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

MGRID

NTAP II

- Added authorization plug-in
  - PERMIS policy engine / LDAP group service
- Generalized from bandwidth reservations to the ability to run *securely* arbitrary programs at a Grid service endpoint
  - Designed to add functionality easily
  - Network testing tools supported
    - iperf, traceroute, ping, etc
- Implemented automatic path discovery

MGRID

Segment Mapping

- Strategy
  - Use `traceroute` to obtain packet routing path
  - Use network topology database to map each router to its associated PMP
  - Execute pairwise performance tests along path
- Multi-homed PMP support
  - One routing table per VLAN
  - Routing policy selects routing table based on source address of outgoing packet
  - Emulates a default route per virtual interface

MGRID

Segment Mapping

Search types (Anchors)

- Host
- Router
- Router, no path discovery
- PMP
- PMP, no LDAP search

MGRID

Segment Mapping

Testing Modes

- Simple
  - Uses default VLANs only
  - Fallback mode
- Source
  - One-way QoS modeling, best for asymmetric applications, accurate for multi-hop
- Full
  - Two-way QoS modeling, but not useful for multi-hop

MGRID

Production Hardening

Stable, robust product suitable for continuous operation

- Error handling/recovery
- Cleanup/restart
- Log file management
- Deployment packaging
- Deployment verifier
- Documentation

MGRID

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

MGRID

NTAP III

- Deployment
  - PMPs deployed at ITCom, Merit, Internet2
- Added authorization plug-in
  - PERMIS policy engine / LDAP group service
- 10 Gbps PMPs
- Host Endpoint Testing
- Automated Testing
- Profile-based interface

MGRID

Walden

- Fine-grained authorization at gatekeeper
- Uses XACML policy file
  - Resource, Action, Subject attributes

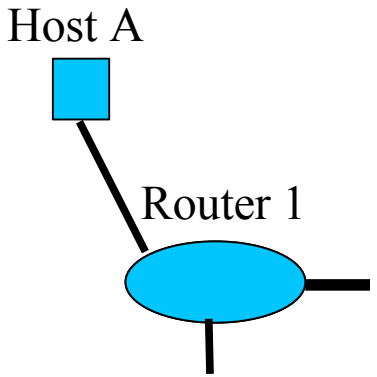
MGRID

Automated Testing

- Want repetitive, automated testing
  - … but with secure authentication and authorization
- Solution: renewable credentials
  - User obtains Globus credentials
  - Portal schedules repetitive testing
  - Prior to test cycle, portal derives single-use credential from user credential
  - Rest of NTAP architecture unchanged

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



Profile-based Interface

- Database of test paths and test requests
  - Segment mapped or user-specified
  - Captures common test configurations
- Available as library of standard configurations
  - Select test profile
  - Attach one or more test profiles
  - Run test and record results
- Leverages test expertise
- Authorized access contemplated

MGRID

MGRID NTAP Project

Demonstration

Future Work

- Post-processed statistics, graphs
- Cross-domain testing
- Alternatives to topology database
- Automated tools
  - Tune TCP stack
  - Detect duplex mismatches
- Graph the topology database

MGRID

Any Questions?

http://www.citi.umich.edu