The NESTOR Project

Alexander V. Konstantinou

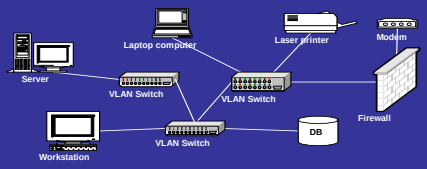
Columbia University

Overview

- Background
- Architecture
- Operations
- Application to Active Networks

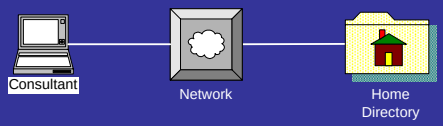
Configuration Mgmt is Difficult

- Knowledge intensive
  - Making changes without violating integrity rules
  - Manual recovery from failures
- Transact with distributed heterogeneous config data
  - Single task involves multiple transactions
  - Duplication & dependencies



Config Mgmt By Example

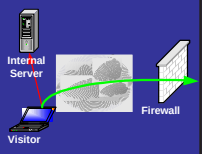
- Collaboration with DARPA project at Telcordia
- Consultant visiting client needs to access home directory
- Goal: Plug laptop + double-click on home folder



Security Policies

Client

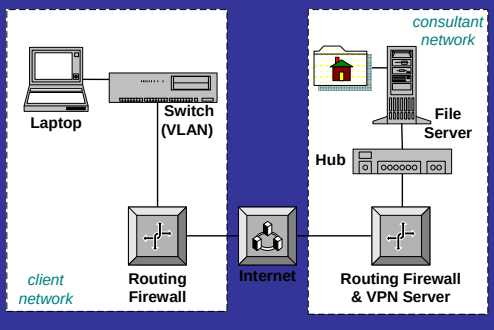
- No visitor access to internal hosts
  - Switch, router, physical configuration
- Restricted visitor Internet access
  - Firewall configuration



Consultant

- VPN clients obtain restricted file access
  - File, http, ftp server configuration

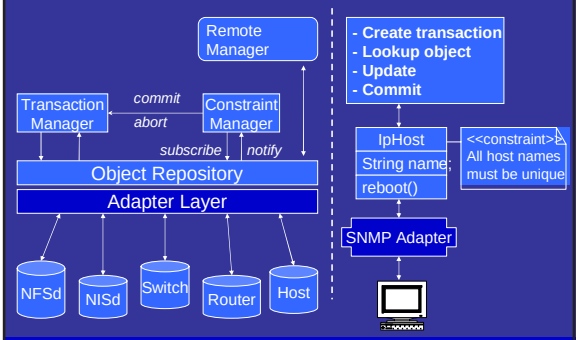
Example Network Topology



NESTOR Functions

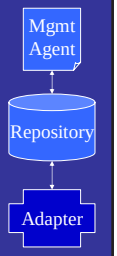
- NESTOR provides means to:
  - Program configuration and change propagation
  - Enforce configuration integrity constraints
  - Enable configuration rollback and recovery
  - Protect against configuration attacks

NESTOR Architecture



Repository Operations

- Transactional access:
  - Read-only, update, or cache (leased)
- Object creation/removal
- Object lookup & event notification
  - By object ID (distributed), class, attribute
  - Returns shallow proxies
- Commit invokes constraint manager
- Pushing changes to world at commit



Configuration Modeling

- Model expressed in Resource Definition Lang
  - Extends CORBA IDL with relationships

```
interface nestor::IpHost : nestor::ManagedObject {
    attribute String hostname "Name of host";
    relationshipset interfacedThrough,
                    IpNetworkInterface, partOf;  }
```

Integrity Constraint Example

- Constraints expressed in OCL (Object Constraint Language -- part of UML)
- Example : "All nodes connected to an internal VLAN port should be *trusted* "

```
EthernetVlanSwitchPort->allInstances
->select(port | port.isEnabled)
->forAll(port |
 if (port.securityMgr.isTrusted(port.vlanID))
   port.forwardsNodes->forAll
     (node | node.securityMgr.isTrusted(node))
```

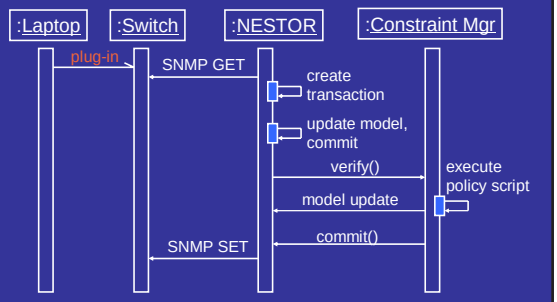

Policy Script Example

- Constraint violations handled by policy scripts (Java methods)
- Example (cont.): policy script changes the VLAN id of the violating port

```
EthernetVlanSwitchPort->allInstances
->select(port | port.isEnabled)
->forAll(port |
 if (port.securityMgr.isTrusted(port.vlanID))
   port.forwardsNodes->forAll
     (node | node.securityMgr.isTrusted(node))
```

```
{
  port.vlanID = port.securityMgr.getPublicVlanID();
}
```

Laptop Plug-In Interaction



Second Prototype Status

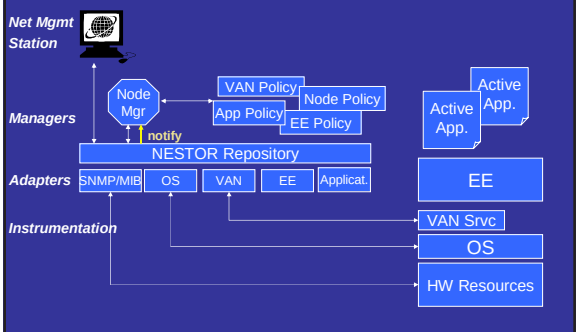
- Java + Jini based (~ 30K lines)
- NESTOR core API (100% interfaces)
- Prototype distributed object repository (Gaia)
  - Mobile objects, Transaction support, Persistence
- RDL and CPL compilers
- Sample models and adapters
- Simple GUI repository browser

Future Work

- Short term: prototype release
- Security config mgmt
  - Attacks often use misconfigured elements
  - Use NESTOR to program security constraints
- Active net config mgmt
  - Active app must be configured to avoid failures
  - Use NESTOR to program config of active apps
  - Feature interaction

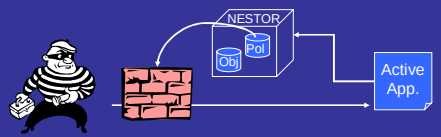
Application of NESTOR to Active Network Mgmt

Node Manager Architecture



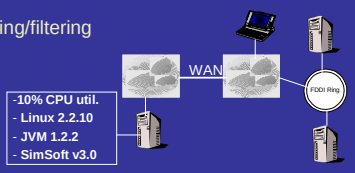
Active Intrusion Detection

- Application registers with NESTOR:
  - Configuration objects
  - Constraints on object state
  - Policies for resolving constraint violations
    - If number of bad packets > X, add rule to firewall
    - If password changed locally, disable account
- NESTOR monitors application



Active Simulation Support

- Management of object distribution:
  - Physical topology configuration
  - Modeling link and node characteristics
- Monitoring of simulation objects:
  - Performance behavior
  - Fault detection
  - Remote monitoring/filtering

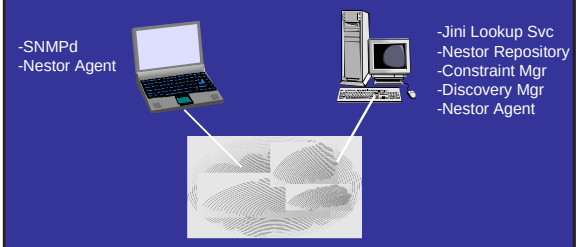


NESTOR Demonstration

Overview

- Example: Model IP network with DNS and firewall constraints
- DNS client network configuration propagates to nodes
- Telnet service disabled

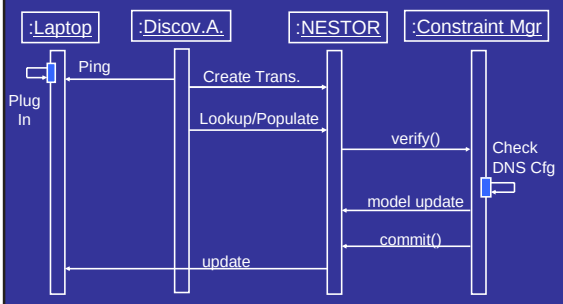
Demo Topology



Bootstrapping

- Jini lookup service
- NESTOR repository
  - Discovers lookup service; registers
- Constraint manager
- Model network (DNS client config).
- Discover nodes
- Add DNS client constraint
- Add Telnet disabled constraint

Automated Laptop Config. Demo



Network Model