

Network Access Control at ORNL

National Laboratories Information Technology Summit
June 2007

Paige Stafford

Information Technologies Services Division

Outline

- **Introduction and Background**
- **Definition of NAC**
 - NAC Elements
- **Define ORNL's Objectives**
- **How ORNL Meets Objectives**
- **Implementation**
 - Strategy and NACmgr Implementation
- **NACmgr System**
 - NACmgr Web Interface Examples
- **Conclusion**

Introduction

- Over the years, ORNL's control over its network has steadily increased, especially after the implementation of DHCP in 2002
- **DHCP provides basic access control**
 - Is the means by which systems obtain network access
 - Traps unregistered systems in NetJail
 - All IP names resolve to NetReg.ornl.gov
 - Simplifies registration process
 - Controls host's Network Configuration

Background

Last year at this time...

- 95% desktops using DHCP
- 90% all systems using DHCP Policy based
- No way to control network access for non-DHCP systems

Background

Last year at this time... (cont'd)

- **Because not all systems use DHCP**
 - it could not be depended upon to completely control all access to the network
- **ORNL had a significant **toolset** beyond DHCP**
 - for enforcing and monitoring network compliance
 - Network registration
 - authentication to AD
 - acceptable OS patch level
 - No vulnerabilities

Background

ORNL Toolset

(Beyond DHCP and not limited to)

- **Network Registration**
- **Cyber Security Scanning**
 - Registration-based minimal scan with NetJail
 - After registration, and quarterly full scans
- **Filters between Visitor and Employee Networks**



Background

ORNL Toolset (cont'd)

- **Polling - ARP cache harvesting**
 - Map IP to mac
- **Systems Management Server (SMS)**
 - Provides software updates and passive operating system fingerprinting
- **Active Directory (AD)**
 - Only Windows OS types can authenticate to AD



Background

ORNL Toolset (cont'd)

- **CSR: Cyper Security Reporting System**
 - Tracks non-compliance on registered systems
 - Makes system owners accountable
 - Takes data from (not limited to)
 - AD
 - SMS
 - Vulnerability scan results
 - Polling



Background

Last year at this time... (cont'd)

- ORNL was looking for a better solution for enforcing network compliance
- “NAC” in the spotlight as the answer to all access control needs and perhaps our missing piece of our puzzle?



But what is NAC?

Definition of NAC

From Ofir Arkin: Bypassing NAC v2.0 -- <http://www.insightix.com>

- **A hot topic**
 - Used and Misused by Venders for advantage
 - Great demand by customers
- **No standardization or common definition**
- **First introduced by Cisco in 2003**
 - To combat viruses and worms as a lesson from Blaster

Definition of NAC (cont'd)

From Ofir Arkin: Bypassing NAC v2.0 -- <http://www.insightix.com>

A definition

Network Access Control (NAC) is a set of technologies and defined processes that aim to control access to the network, allowing only authorized and compliant devices to access and operate on a network

Definition of NAC (cont'd)

Elements of NAC

1. Detection
2. Authentication
3. Compliance
4. Quarantine and Remediation
5. Enforcement
6. Authorization
7. Post-Admission Protection

<http://www.insightix.com>

<http://www.eweek.com/article2/0,1895,1860588,00.asp>

<http://www.infoexpress.com>

ORNL's NAC Objectives

per ORNL's CIO, Scott Studham



- **All Computers Validate to Network:**
 1. All network addresses are allocated using DHCP;
 2. Quarantine non-compliant systems considering approved operating system, approved software, configuration, vulnerabilities, and behavior
 3. Develop network trolling tools to characterize systems
 4. Automate quarantine process for first time connections, re-connections, and on regular basis

ORNL's NAC Objectives (cont'd)

- **ORNL's NAC design features will work together to keep:**
 - 1. "bad" devices off the network**
 - 2. and thus affectively authenticate "good" devices onto the network**

Meeting ORNL's NAC Objectives

Meeting ORNL's NAC Objectives

- Looked at available COTS packages
- Deployment Requirements
 - Must satisfy ORNL's NAC objectives
 - Easy integration with existing infrastructure
 - Affordable
 - Non-intrusive to user or network

Meeting ORNL's NAC Objectives (cont'd)

- **Three different types of NAC:**
 - **Hardware based**
 - Hardware on the network monitor and control traffic
 - Cisco and Lockdown
 - **Software (client side) based**
 - Software installed on client that connects to NAC server
 - Microsoft, Trusted Networks
 - **Open Source**
 - viability issues

Meeting ORNL's NAC Objectives (cont'd)

- Cisco's NAC
 - Network Hardware and OS restrictive
 - Good product and good support
 - Very Expensive
- Lockdown (first choice)
 - Accommodates mixed network
 - Good product with good support
 - Not as expensive but question viability

Meeting ORNL's NAC Objectives (cont'd)

- COTS packages did not meet ORNL deployment objectives
 - Bottom line: too expensive
- Decided to enhance ORNL's Tool Set
- And incorporate the Elements of NAC to build our own version of NAC



ORNL's Implementation Strategy

ORNL's Implementation Strategy

(Incorporating the Elements of NAC)

- **Detection**

- The ability to detect (new or otherwise) systems on the network
- SNMP polling down to L2 port on all ORNL networks
- Ability to poll all switch/router types on network
- Optimal periodicity based on ARP/Bridge TTL
- All new hosts must be found within 5 minutes
- Data accessible via CGI and database



ORNL's Implementation Strategy (cont'd)

(Incorporating the Elements of NAC)

- **Authentication**
 - The ability to authenticate each user accessing the network regardless of source or destination
 - Active Directory (AD)
 - for Windows, and MACs
 - LDAP for UNIX types



ORNL's Implementation Strategy (cont'd)

(Incorporating the Elements of NAC)

- **Compliance**

- The ability to assess whether any host on the ORNL network complies with ORNL network security policy
- Systems must meet current published requirements for
 - Authentication (AD, LDAP)
 - patching (SMS, Red Hat Patch Server)
 - configuration (mobile system encryption, CoreIT access, Virus protection)
 - The requirements are published by OS, but all have the same underlying goals



Compliance (cont'd)

- **No system vulnerabilities are permitted**
 - Scan for cyber security vulnerabilities
 - Cursory scan at registration (NetJail)
 - Medium scan if off network more than 4 hours
 - Full scan for all newly registered and quarterly



ORNL's Implementation Strategy (cont'd)

(Incorporating the Elements of NAC)

- **Quarantine**

- The process of isolating an host from the rest of the network Triggered when a new host is detected and/or when an host is non-compliant with ORNL security policy and the host should be able to remediate from this state
- **Non-compliant systems must be quarantined**



- systems defined by CSR
- Any mac address with extended visit in NetJail
- “Sensitive” systems not on assigned network

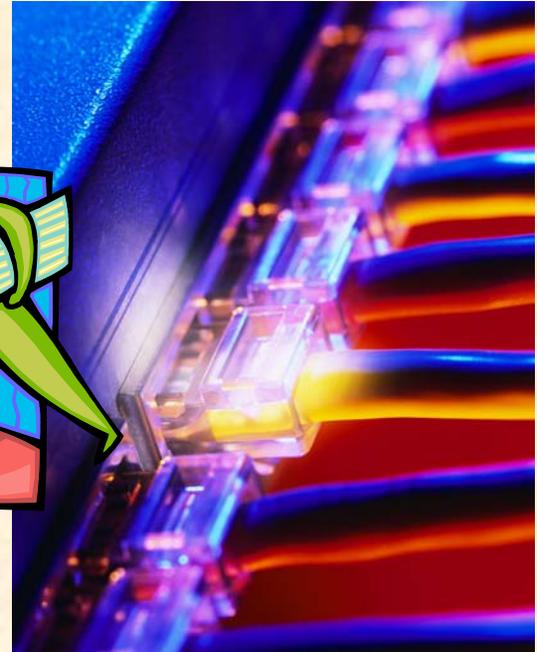
Quarantine (cont'd)

- Quarantined systems must reside in a separate, heavily filtered network
 - Cannot go anywhere except splash page, DHCP, and dummy DNS
- Quarantined systems must move into quarantine state immediately
 - Upon quarantine, the client's port is bounced
 - Bouncing the port makes most clients do a DHCP-DISCOVERY



Quarantine (cont'd)

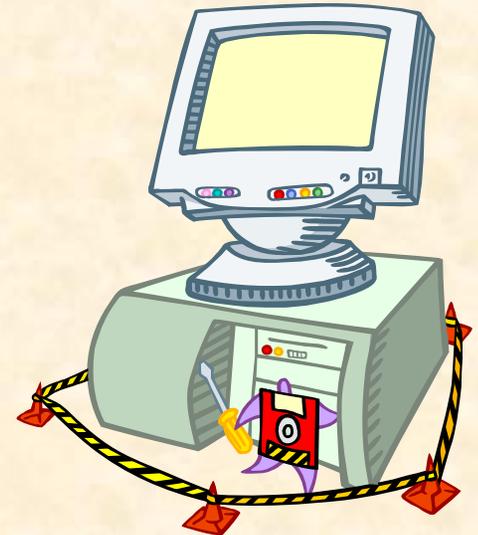
- User must have the ability to remediate
 - get patches, etc
- If the System not using DHCP then Disable Port



ORNL's Implementation Strategy (cont'd)

(Incorporating the Elements of NAC)

- **Remediate**
 - The process of fixing an issue causing a host to be non-compliant
 - Filtered network
 - No ORNL services (e.g. mail, SAP)
 - Allow 24-hour to remediate
 - then Block
 - System is monitored and re-tested for compliance



ORNL's Implementation Strategy (cont'd)

(Incorporating the Elements of NAC)

- **Enforcement**

- The ability to restrict a non-compliant host's access to the network
- Automated block if
 - Not registered and not using DHCP
- Remove the non-compliant from network
 - DHCP quarantine/remediation/block
 - Port Blocking or assigning mac to uplink port

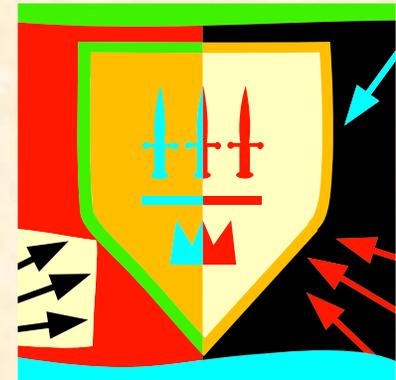


ORNL's Implementation Strategy (cont'd)

(Incorporating the Elements of NAC)

- **Post-Admission Protection**

- The ability to continuously monitor hosts on the network for vulnerabilities and non-compliance
- Re-scanning devices that have not been seen on network in 4 hours
- Quarterly scans
- SMS updates
- Sensitive systems are placed in isolated VLANs



ORNL's Implementation Strategy (Obvious Weaknesses)

- The host is already on the network
 - Before non-compliance is detected
- It is possible to spoof the MAC address
- Unable to detect masquerading hosts
 - NAT (network address translation)
 - Virtualization software
 - e.g. Virtual PC, Vmware



ORNL's Implementation

ORNL's NAC Implementation

NACmgr

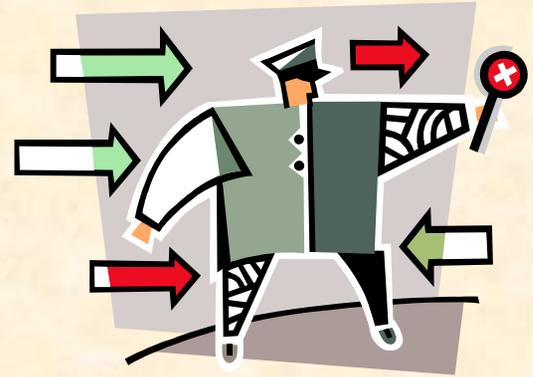
- Next phase of ORNL NAC begins with the implementation of [NACmgr](#)
 - Network Access Control Manager
- Primary role
 - Detection and Enforcement



ORNL's NAC Implementation (cont'd)

NACmgr

- NACmgr uses Detection with overlying logic
 - to trigger compliance and enforcement of ORNL's network policies
- Integrates ORNL's Tool Set
 - CSR, Network Registration, Cyber Scanning, etc.



ORNL's NAC Implementation (cont'd)

NACmgr

- Detects and monitoring all MAC addresses on the network (Detection)
- Updates network registration database for each systems activity on the network
- Detects non-compliant (Compliance)
 - Unregistered
 - Interfaces in wrong protection VLAN
 - Monitoring CSR block-list

ORNL's NAC Implementation (cont'd)

NACmgr

- Detects systems that have been off network for more than 4 hours and submits scan requests (Post-admission protection)
 - Nessus scanner
 - The scanning policy is based on the ISS X-Force's Catastrophic Risk Index
 - which is an up-to-date list of the most serious, high-risk vulnerabilities and attacks
 - includes major exploits, pervasive worms, and critical patches covering serious software weaknesses.
 - The SANS Top 20 vulnerabilities is also consulted.



ORNL's NAC Implementation (cont'd)

NACmgr

- Places systems in Quarantine
 - via web interface
 - or automatically according to the policy for the specific non-compliance
- Places systems in Remediation
 - User-based cgi
 - Or via IT helpline web interface for non-web capable systems in quarantine
- **Non-DHCP systems must be “blocked”**
(Enforcement)

ORNL's NAC Implementation (cont'd)

NACmgr

- **Perform L2 Blocks**
 - Port disabling
 - Assign mac to uplink port*
 - Drop mac address*
- **Enforcement is monitored***
 - To ensure system hasn't "resisted arrest"
 - Moving to different jack/network
 - From DHCP to static



* Still in development

NACmgr System Specifications

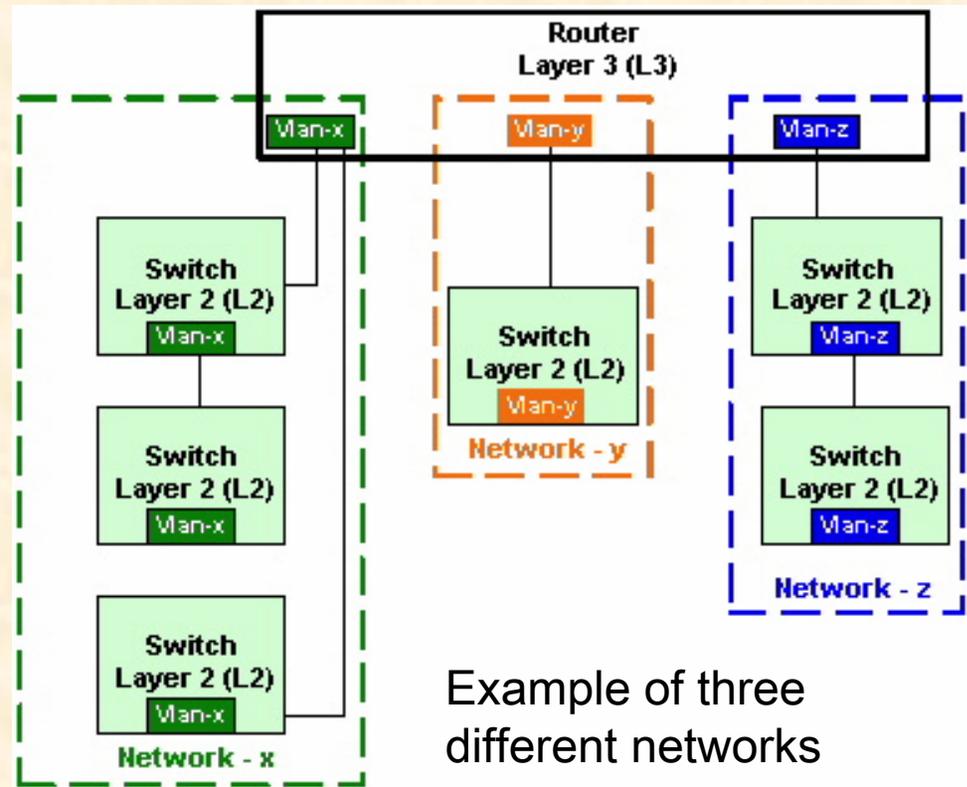
- **Large server system**
 - Linux, 4-cpu, Large memory and storage
 - 8-interfaces
- **PostgreSQL database**
- **Three separate servers to distribution load**

NACmgr Code Specifications

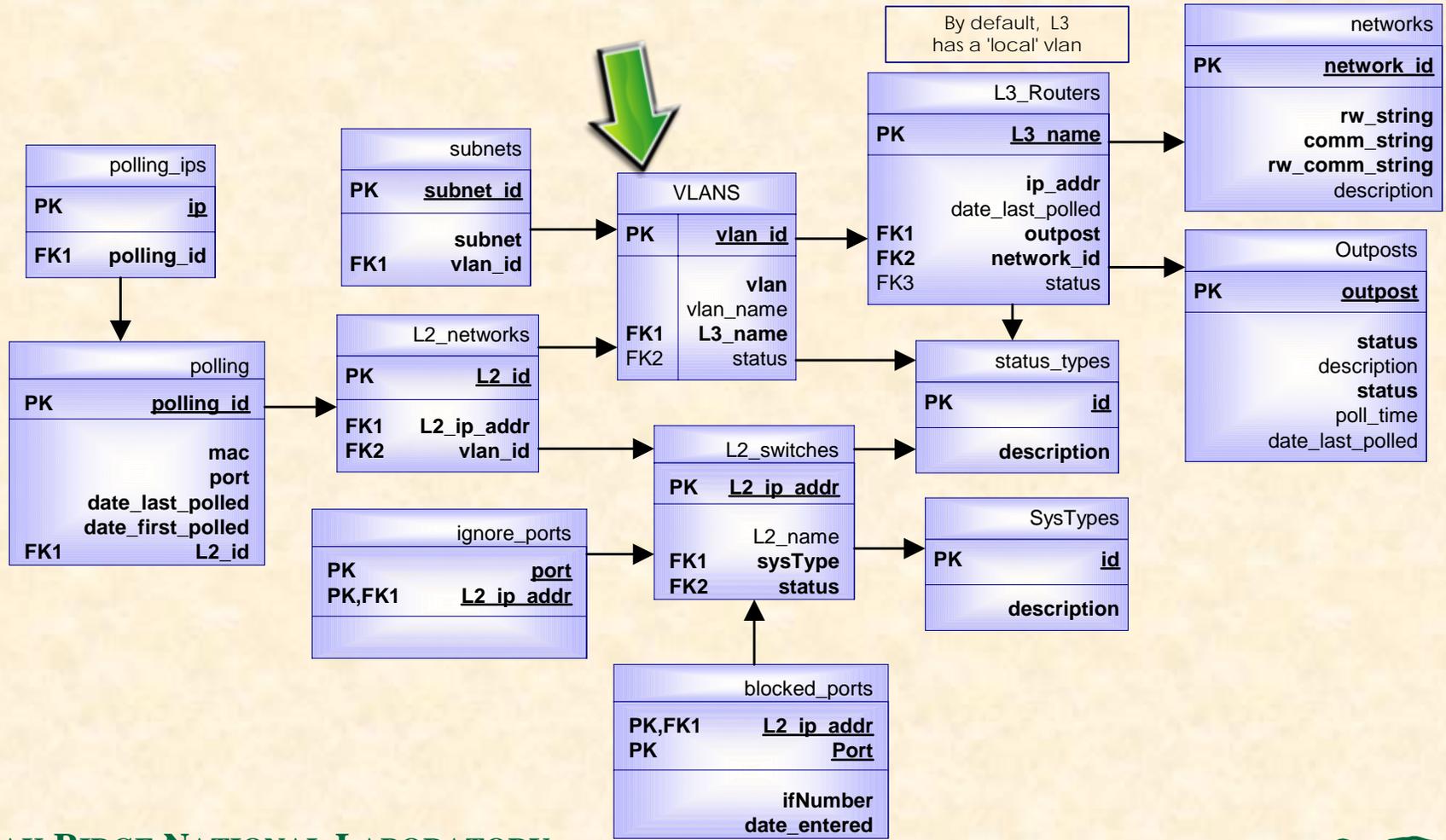
- **NACmgr Code Specifications**
 - Programming language: Researched benchmarks of execution time of hash algorithms of C, C++, Java
 - C++ seemed best suited
 - http://bruscy.multicon.pl/pages/przemek/java_not_really_faster_than_cpp.html
 - <http://members.lycos.co.uk/wjgoh/JavavsC.html>
 - <http://www.kano.net/javabench/data>
 - **Libraries:**
 - Net-SNMP: SNMP library for C
 - pqxx: PostgreSQL library for C++
 - RudeCGI: C++ CGI library
 - pThreads: POSIX threaded library

NACmgr Design

- A NACmgr network is composed of three parts
 - L3 router
 - Arp Caches
 - One or many Vlans
 - Vlan
 - Ties L3 to L2
 - Unique subnet
 - L2 switch(es)
 - Bridge Table



NACmgr Design (cont'd)



NACmgr Design (cont'd)

- **NACmgr uses SNMP**
 - Uses -v1 to accommodate 3com, Foundry
 - L2 bridge data mapped to L3 routing table
 - or as Local Only VLAN
 - Used to disable/enable (or bounce) L2 ports
 - Used to (semi-autoDiscover) NACmgr Network
- **EXPECT script used to assign MAC address to uplink port**

NACmgr Design (cont'd)

- **Load monitored**
 - On network devices and NAC devices
- **Distributed task among three outposts**
- **Two minute delta T**

NACmgr – Web Interface

- Web based NACmgr
 - “Network Detective”
 - Still in development
 - Role-based access
 - Failover to outpost1
 - DB and CGI
 - Polling data retrieval
 - Interface to Manual Enforcement
 - Blocks, quarantine, etc.
 - NAC Network Management
 - NACmgr systems monitoring



NACmgr – Web Interface (cont'd)

- Start page for NACmgr “Network Configuration”
- Monitor page for
 - outpost polling duration
 - Outpost Router assignments

NAC Manager
NETWORK DETECTIVE AND POLICY ENFORCER
Oak Ridge National Laboratory's
Network Access Control Manager

Monitor and I
Monitor and I
Monitor DHCP
Security Sca

Network Config Polling Access Control Check Reg

Network Access Control Manager

NAC Network Configuration

Outpost	status	Date/Time Last Polled	Duration (seconds)	L3 Networks Defined	Blocked Ports
<input type="radio"/> NAC1	ACTIVE	2007-05-24 15:37:39	571	SWGE4500N SWGE6010 SWGEC5B-1	3
<input type="radio"/> NAC2	ACTIVE	2007-05-24 15:37:17	76	SWGE1060 SWGE1505 SWGE2525 SWGEC3025 SWGE4500S SWGE7603	2
<input type="radio"/> NACmgr	ACTIVE	2007-05-24 15:39:03	62	NTRCGWY ORGWY RALPH SWGECNMS SWGEC5B-2 SWGEC5NS WIRELESS3750	5

Back reSet L3 Outpost Configuration

Search: networks vlans L2

NACmgr – Web Interface (cont'd)

- NACmgr web interface must be used to define the networks
- Semi-Auto-discovers networks using SNMP
 - User must define the L3 and how to connect
 - Vlans and L2 switches can then be auto-discovered via SNMP

Example – Adding a VLAN

The screenshot displays the NAC Manager web interface. At the top, there is a header with the NAC Manager logo and a list of features: Monitor and Manage Poled Devices, Monitor and Manage Blocked Devices, Monitor DHCP activity of clients, and Security Scans. Below the header is a navigation bar with links for Network Config, Polling, Access Control, Check Reg, and Help. The main content area is titled "Network Access Control Manager" and shows "Results of L3 Router Search". A table lists several L3 routers with columns for select, L3 Router Name, L3 Router IP Address, OutPost, Network Type, Time Poll Start, Time Poll End, Delta_t Poll Time, and Status. Below the table are buttons for Back, Modify, Delete, Add New, L3 Vlans, (re)Construct Network, and L2 Network. At the bottom, there is a footer with links for ORNL Home, NetTools, Nagios, NMC, NetReg, and Home.

select	L3 Router Name	L3 Router IP Address	OutPost	Network Type	Time Poll Start	Time Poll End	Delta_t Poll Time	Status
<input type="checkbox"/>	SWGE1060	160.091.096.005	NAC1	ORNL	2007-05-31:11:44:01	2007-05-31:11:45:11	00:01:09.926556	ACTIVE
<input type="checkbox"/>	SWGE1505	160.091.000.018	NAC1	ORNL	2007-05-31:11:44:01	2007-05-31:11:44:53	00:00:51.923968	ACTIVE
<input type="checkbox"/>	SWGE2525	160.091.000.025	NAC1	ORNL	2007-05-31:11:44:01	2007-05-31:11:45:07	00:01:06.124113	ACTIVE
<input type="checkbox"/>	SWGE4500N	160.091.000.050	NAC1	ORNL	2007-05-31:11:44:01	2007-05-31:11:45:31	00:01:29.982049	ACTIVE
<input type="checkbox"/>	SWGE6010	160.091.000.010	NAC1	ORNL	2007-05-31:11:44:01	2007-05-31:11:45:00	00:00:59.114478	ACTIVE
<input type="checkbox"/>	SWGE7603	160.091.000.034	NAC1	ORNL	2007-05-31:11:46:02	2007-05-31:11:46:13	00:00:11.321279	ACTIVE
<input type="checkbox"/>	SWGECSB-1	160.091.216.001	NAC1	ORNL	2007-05-31:11:44:01	2007-05-31:11:45:36	00:01:34.628381	ACTIVE

- Listing of L3s for outpost
- To semi-autoDiscover the VLANS associated with a L3:
 - Select the L3 Router
 - Click on “(re)Construct Network”

Example – Adding a VLAN (cont'd)

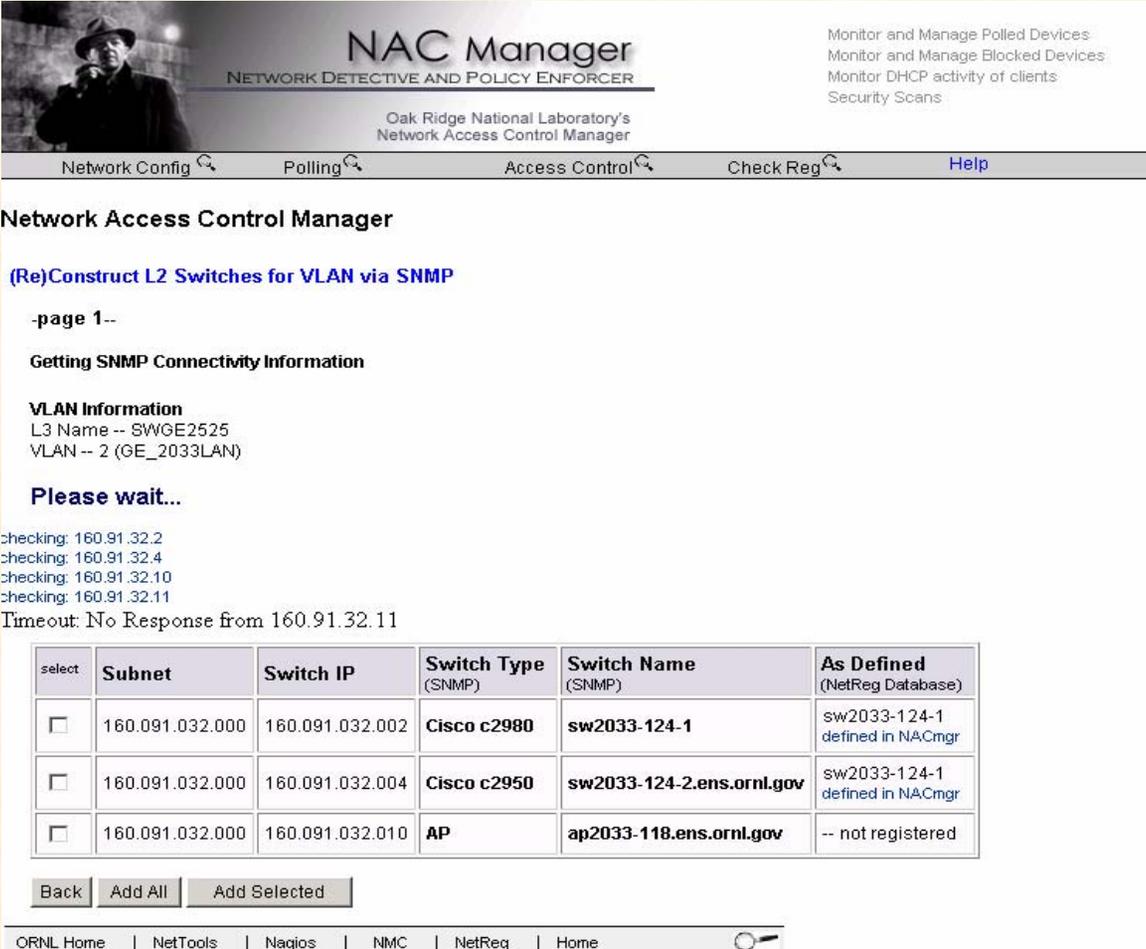
- **SNMP retrieval of L3 VLAN info**
 - Vlan Number
 - Subnet
 - Mask
 - Gateway

The screenshot displays the NAC Manager web interface. At the top, it identifies the system as 'NAC Manager NETWORK DETECTIVE AND POLICY ENFORCER' for 'Oak Ridge National Laboratory's Network Access Control Manager'. A navigation bar includes 'Network Config', 'Polling', 'Access Control', 'Check Reg', and 'Help'. The main content area is titled 'Network Access Control Manager' and shows configuration for 'L3 Router Network' on 'L3 Router SWGE1060'. It features a table comparing 'Subnet Information from the Router' (retrieved via SNMP) with 'As defined' (from the PostgreSQL database). The table lists three VLANs: Vlan 3, Vlan 4, and Vlan 24, each with its corresponding gateway, subnet, and mask. At the bottom, there are buttons for 'Back', 'reSet', 'Update Selected', and 'Update All'.

VLAN	Subnet Information from the Router			As defined	
-- SNMP --	-- SNMP --			-- postgresQL database --	
	Gateway	Subnet	Mask	VLAN Name	Subnet
<input type="checkbox"/> Vlan 3	010.009.100.001	010.009.100.000	255.255.254.000 /23	TECH_VILAN	010.009.100.000
	010.008.100.001	010.008.100.000	255.255.254.000 /23		010.008.100.000
	160.091.100.001	160.091.100.000	255.255.254.000 /23		160.091.100.000
	010.001.100.001	010.001.100.000	255.255.254.000 /23		010.001.100.000
<input type="checkbox"/> Vlan 4	010.009.103.001	010.009.103.000	255.255.254.000 /23	GE_1009COM-2LAN	010.009.103.000
	010.008.103.001	010.008.103.000	255.255.254.000 /23		010.008.103.000
	160.091.103.001	160.091.103.000	255.255.255.000 /24		160.091.103.000
	010.001.103.001	010.001.103.000	255.255.255.000 /24		010.001.103.000
<input type="checkbox"/> Vlan 24	160.091.096.005	160.091.096.000	255.255.255.240 /28	TOWNSITE_GE <small>from subnet name</small>	

Example – Defining L2s for Network

- Tests each IP address in the network pool for SNMP connectivity
- Uses Network Registration to define network pool



NAC Manager
NETWORK DETECTIVE AND POLICY ENFORCER
Oak Ridge National Laboratory's
Network Access Control Manager

Monitor and Manage Polled Devices
Monitor and Manage Blocked Devices
Monitor DHCP activity of clients
Security Scans

Network Config | Polling | Access Control | Check Reg | Help

Network Access Control Manager

[\(Re\)Construct L2 Switches for VLAN via SNMP](#)

-page 1--

Getting SNMP Connectivity Information

VLAN Information
L3 Name -- SWGE2525
VLAN -- 2 (GE_2033LAN)

Please wait...

checking: 160.91.32.2
checking: 160.91.32.4
checking: 160.91.32.10
checking: 160.91.32.11
Timeout: No Response from 160.91.32.11

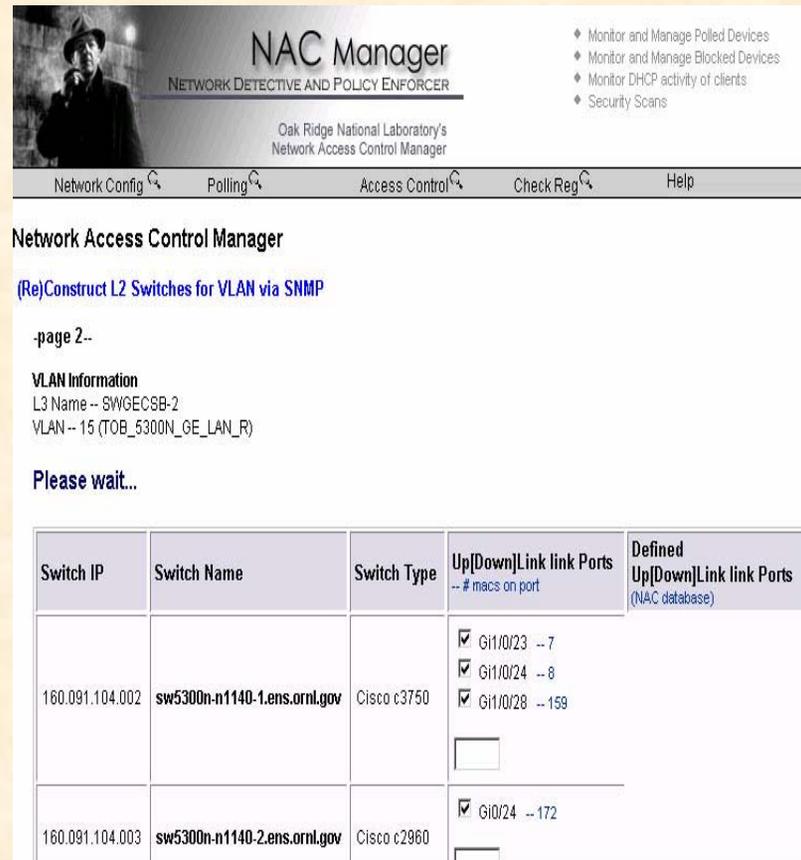
select	Subnet	Switch IP	Switch Type (SNMP)	Switch Name (SNMP)	As Defined (NetReg Database)
<input type="checkbox"/>	160.091.032.000	160.091.032.002	Cisco c2980	sw2033-124-1	sw2033-124-1 defined in NACmgr
<input type="checkbox"/>	160.091.032.000	160.091.032.004	Cisco c2950	sw2033-124-2.ens.ornl.gov	sw2033-124-1 defined in NACmgr
<input type="checkbox"/>	160.091.032.000	160.091.032.010	AP	ap2033-118.ens.ornl.gov	-- not registered

Back | Add All | Add Selected

ORNL Home | NetTools | Nagios | NMC | NetReg | Home

Example – Defining L2s for Network (cont'd)

- **Must define Ignore Ports**
 - Uplink/Downlink Ports
 - Not “resident” traffic
 - e.g. other switches or APs
 - An SNMP best guess
 - Ports with multiple macs
- **Upon committing, new L2 network will begin to get polled**



The screenshot shows the NAC Manager web interface. The header includes the title "NAC Manager" and the subtitle "NETWORK DETECTIVE AND POLICY ENFORCER". Below the header, there is a navigation menu with options: "Network Config", "Polling", "Access Control", "Check Reg", and "Help". The main content area displays "Network Access Control Manager" and a link "(Re)Construct L2 Switches for VLAN via SNMP". Below this, it shows "page 2--" and "VLAN Information" with details: "L3 Name -- SWGECSB-2" and "VLAN -- 15 (TOB_5300N_GE_LAN_R)". A "Please wait.." message is displayed above a table.

Switch IP	Switch Name	Switch Type	Up[Down]Link link Ports -- # macs on port	Defined Up[Down]Link link Ports (NAC database)
160.091.104.002	sw5300n-n1140-1.ens.ornl.gov	Cisco c3750	<input checked="" type="checkbox"/> Gi1/0/23 -- 7 <input checked="" type="checkbox"/> Gi1/0/24 -- 8 <input checked="" type="checkbox"/> Gi1/0/28 -- 159 <input type="checkbox"/>	
160.091.104.003	sw5300n-n1140-2.ens.ornl.gov	Cisco c2960	<input checked="" type="checkbox"/> Gi0/24 -- 172 <input type="checkbox"/>	

Example - Access Control

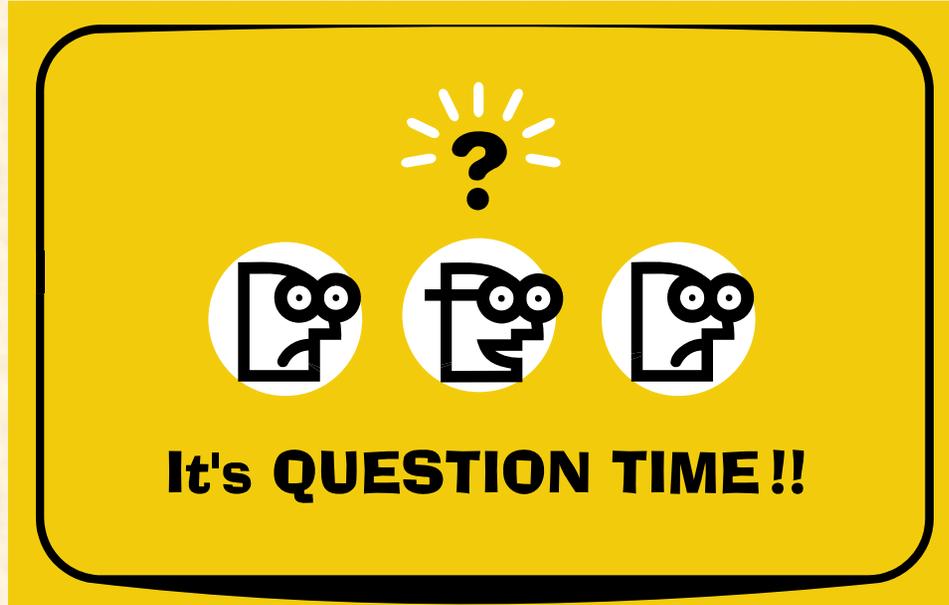
- Enforcement interface
 - Retrieves registered devices for controlling access
 - View access history
 - “Rap sheets”
 - Access flow
 1. Quarantine or block
 2. Remediation
 3. Parole



The screenshot displays the NAC Manager web interface. At the top, there is a header with a logo of a man in a hat and the text "NAC Manager NETWORK DETECTIVE AND POLICY ENFORCER". Below the header, there is a navigation bar with links for "Network Config", "Polling", and "Access Control". The main content area is titled "Network Access Control Manager" and contains a search form for "Search for Network Registration (NetReg) Records -- for Access Control". The form includes a dropdown menu for "Access Control Type", input fields for "Device Name", "MAC Address", "IP Address", and "Organization ID (8 char)", and a "get" button. Below the form are buttons for "reSet", "Back", "Search Logs", and "search". At the bottom, there is a footer with navigation links: "ORNL Home", "NetTools", "Nagios", "NMC", "NetReg", and "Home".

Conclusion

- ORNL has come up with an interim solution for NAC
- Still in development stages
 - Need further testing and refinement
- More work to be done to better automate NACmgr network discovery
- Still looking for a COTS solution that will solve ORNL's NAC objectives



More In-Depth Presentations related to ORNL's Defense in Depth Project

- Network Enhancements for Defense in Depth at ORNL
Clark Piercy
- Managing Unix/Linux at ORNL
Brett Ellis
- Defense in Depth Reporting at ORNL
Steve Parham
- Managing Macs in an Enterprise
Brian Wallace
- Quarantine: Controlling Network Access Using DHCP
James Calloway

