

Quarantine: Controlling network access using DHCP

National Laboratories Information Technology Summit
June 2007

James Calloway
Information Technology Services Division

DHCP, Briefly ...

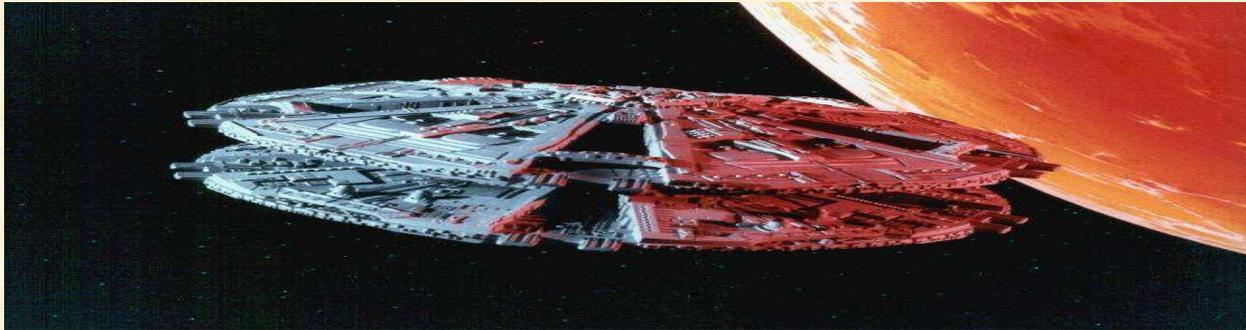
- **DHCP**

- **Facilitates network access**
- **Provides clients with network configuration information**

RFC 2131: The Dynamic Host Configuration Protocol (DHCP) provides configuration parameters to Internet hosts. DHCP consists of two components: a protocol for delivering host-specific configuration parameters from a DHCP server to a host and a mechanism for allocation of network addresses to hosts

DHCP At ORNL

- **ISC DHCP**
- **Registered devices get static address assignments**
- **“Home base” ... can roam**
- **Subnet pools defined to allow registered clients to roam from subnet to subnet**

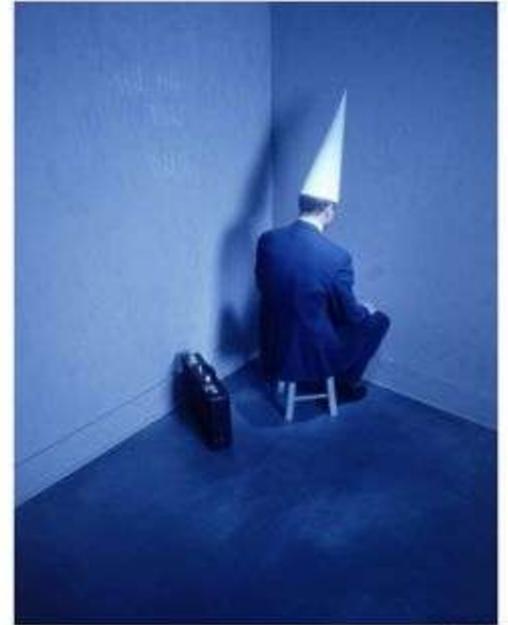


Defense In Depth (DiD) 2006

- **Method to segregate systems that were non-compliant**
- **Examples**
 - **Approved Operating Systems**
 - **Vulnerabilities**
 - **Registration system mismatches**
 - **Invalid property no.**
 - **Configuration**
 - **Are they checking in with patch server**
 - **Does CoreIT have Access**

Isolation

- **Use DHCP to isolate systems**
 - 94-95% of desktop systems using dhcp
 - Percentage will only increase
 - July 1, dhcp becomes requirement
- **Experience with using DHCP to isolate systems**
 - NetJail / Autoreg
 - DHCP hands out phony DNS server to “unknown” hosts



Quarantine ...

- **Quarantine – DHCP is used to isolate a non-compliant system from the rest of the network**
- **The user is given a chance to remediate or “heal” their system from this state**
 - **Self-remedy, doesn’t require IT intervention**
 - **User can fix themselves outside of business hours**

Quarantine Process

- **3 “phases”**
- **Quarantine: Initial phase**
 - Separate subnet pool, heavily filtered network, limited dns
- **Remediation: Healing Phase**
 - Separate subnet pool, filtered network, regular dns
- **Parole: As far as DHCP knows, you’re back to normal**
 - These devices are marked in our database for review by our parole officer

Thrown In The “Pool”

- **DHCP address manipulation**
 - Extra subnet Pools defined for Quarantine and Remediation
- **DHCP Subnet 128.99.212.0**
- **New subnets added to dhcp**
 - 10.8.212.0 Quarantine
 - 10.9.212.0 Remediation



DHCP Configuration

- Quarantine/Remediate clients are identified by their hardware address and placed in a dhcp class
- Protect the rest of us!
 - DHCP Allow, deny rules placed on subnet pools
 - Quarantine : Only interfaces in class “quarantine”
 - Remediate: Only interfaces in class “remediate”
 - Other pools: Deny quarantine, remediate
 - Had some experience with these before: known, unknown



Starting A Quarantine

- **Quarantines initiated through NACmgr application**
- **NACmgr allows you to specify reason for quarantine**
 - **Most likely, the user already knows why**
- **Authorized Users perform the Quarantine**
 - **Division security officer requests, Cyber Security**





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

Search for Network Registration (NetReg) Records -- for Access Control

Only one field is required.
All records are retrieved from NetReg database

Access Control Type

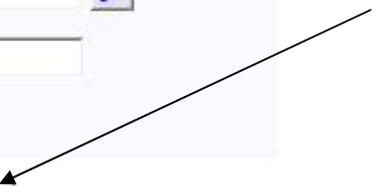
Device Name

MAC Address [get](#)

IP Address

Organization ID (8 char)

[reSet](#) [Back](#) [Search Logs](#) [search](#)



Verify Access Control

Requested Access Control: **QUARANTINE**

Device Name	Network Interface	IP Address	Device Status	IF Status	Owner
DENGAR	00.0D.56.E0.21.F0	160.091.216.043	ACTIVE	ACTIVE	746268

Give Access Control Reasons

Choose from this list and/or enter other reasons/remedies

- not DID Compliant
- Overdue Vulnerabilities
- Contaminated with virus/worm
- Other (detail below)

Other Reason(s) for Access Control

improper registration

Other Remedy(s) for Access Control

no property # is listed in the network registration system

The 'Other' text fields together cannot be more than 1022 characters

reSet Back Continue

Database, DHCP Changes

- **Interface status set to Quarantine**
- **Emails sent to owners, sysadmins, division security officer(s)**
- **DHCP regularly polls database**
 - 3-5 Minutes
 - Checks interface status

Entering Quarantine

- **Once you're in the quarantine grouping, the only place you can go is in the quarantine pool**
 - Forced to 10.8.x.x address
 - Initially, solely dependent on lease
- **Includes all subnets**

“Give Me My Old Address!!”

- May 23 13:46:20 x dhcpd: [ID 702911 local7.info] DHCPREQUEST for x.x.x.x (x.x.x.x) from 00:90:96:fb:83:a8 via x.x.x.x : unknown lease xx.x.x.
- May 23 13:50:33 x dhcpd: [ID 702911 local7.info] DHCPDISCOVER from 00:90:96:fb:83:a8
- May 23 13:50:34 x dhcpd: [ID 702911 local7.info] DHCPPOFFER on 10.8.88.252 to 00:90:96:fb:83:a8 (dengar)
- May 23 13:50:34 x dhcpd: [ID 702911 local7.info] DHCPREQUEST for 10.8.88.252 (160.91.1.30) from 00:90:96:fb:83:a8 (dengar)
- May 23 13:50:34 x dhcpd: [ID 702911 local7.info] DHCPACK on 10.8.88.252 to 00:90:96:fb:83:a8 (dengar) via x.x.x.x



Changes Along The Way



- Previous example was of client whose lease had run out
- Now, client's port is bounced
 - Most do DHCPDISCOVER

Computer and Network Security

Your network access is Quarantined

This device has been quarantined due to one or more cyber security issues.

Proceed to [Remediation](#)

or Contact [HelpLine](#) for assistance

[241-ORNL \(241-6765\)](tel:241-ORNL)

Quarantine DNS

- **DNS Server we push only resolves to quarantine web page**

Yahoo.com
Microsoft.com
Google.com
Aol.com



Quarantine Characteristics

- **Heavily Filtered Network**
 - Quarantine Page Only
- **Every network has these pools defined**
 - Prevents roaming
 - Wireless
- **Network Registration locking**





Oak Ridge National Lab's Network Registration System

Where users control their own network access

Brought to you by Information Technology Services Division

for ORNL Employees on the wired and wireless networks

Search Network Registration Database

1 devices
1 total records
- 1 Pages -

Page: 1: dengar GO PREVIOUS NEXT Sort By: -- sort by -- GO Rows: 10 GO

Select	Device Name	Serial #	OS Type	Division	Sysmgr's Badge	Building	Device Comments	Interface#	MAC Address	Last Active	DHCP Lease	IP Address	DHCP Status	IP Name
1.	DENGAR	4FB1Q51	WINDOWS	50256117	746268	5600		001	00.0D.56.E0.21.F0		2007-05-21	160.91.216.43	Ready	dengar.ornl.gov

First select **what** to do, and then **to what**.

reLoad Return Do What? To What? Continue

Missing a **To What** item? Make sure that the object type is an output field.

Email output to ZCL@ornl.gov send Back

For questions try the [FAQ](#) or call HelpLine at 241-ORNL (241-6765).

- [disclaimers](#)
- [ORNL Home](#)
- [Networking Home](#)
- [Home](#)
- [Search](#)
- [UserSearch](#)
- [MyDevices](#)
- [MyComputers](#)
- [NewDevice](#)

If you should encounter an error or bug, please report it.
NETREG.5.6

Search Network Registration Database
 https://netreg.ornl.gov/sec-cgi-bin/cgiwrap/dns/search.cgi

Network Registration System

Brought to you by
Information Technology Services Division

Where users control their own network access

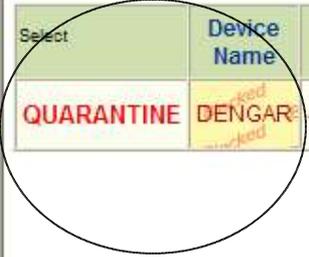
for ORNL Employees
on the wired and wireless networks

Search Network Registration Database

1 devices
1 total records
- 1 Pages -

Page: 1: dengar [GO] [PREVIOUS] [NEXT] Sort By: -- sort by -- [GO] Rows: 10 [GO]

Select	Device Name	Serial #	OS Type	Division	Sysmgr's Badge	Building	Device Comments	Interface#	MAC Address	Last Active	DHCP Lease	IP Address	DHCP Status	IP N
<input type="checkbox"/>	QUARANTINE DENGAR	4FB1Q51	WINDOWS	50256117	746268	5600		001	00:0D:56:E0:21:F0		2007-05-21	160.91.216.43	Not defined	DENGAR



First select **what** to do, and then **to what**.

[reLoad] [Return] [Do What?] [To What?] [Continue]

Missing a **To What** item? Make sure that the object type is an output field.

Email output to [ZCL@ornl.gov] [send] [Back]

For questions try the [FAQ](#) or call HelpLine at 241-ORNL (241-6765).

- [disclaimers](#)
- [ORNL Home](#)
- [Networking Home](#)
- [Home](#)
- [Search](#)
- [UserSearch](#)
- [MyDevices](#)
- [MyComputers](#)
- [NewDevice](#)

If you should encounter an error or bug, please report it.
NETREG.5.6

Decisions, Decisions, Decisions...

- Get very familiar with the Quarantine web page
- Fix yourself: Proceed to remediation button
- Call HelpLine
- Ignore Us
 - After two weeks device is blocked
 - Before quarantine, probably would have been blocked anyway
 - Nicer



Computer and Network Security

Your network access is Quarantined

This device has been quarantined due to one or more cyber security issues.

Proceed to [Remediation](#)

or Contact **HelpLine** for assistance

[241-ORNL \(241-6765\)](tel:241-ORNL)





Computer and Network Security

Remediation

SAVE THIS PAGE TO YOUR DESKTOP FOR FUTURE REFERENCE BEFORE PROCEEDING

Note: It can take up to 5 minutes before you are able to proceed

This device has been placed in **QUARANTINE** status

Reason: improper registration
Remedy: no property # is listed in the network registration system

Once these issues are addressed you may click **Request Removal** and your computer access will return to normal and your case will be reviewed by Cyber Security. *A device in REMEDIATION status longer than 24 hours is subject to being blocked*

More information can be found on VSWEB <http://home.ornl.gov/~vs4/prod>

For assistance or questions, please contact the HelpLine at (865) 241-ORNL.

Note: If you browse away from this page or have to reboot this device to apply fixes, you can return to this page by going to <https://remediation.ornl.gov> from this device.

Request Removal

“Remediation”

- CGI page tells you why you are not compliant
 - IP used to identify device and pull specific reasons on why device was blocked
 - User probably already knows
- Purpose of stage: Fix the issue which is causing the system to be non-compliant
- 10.9 address space
 - 3-5 minutes 10.8(q) --> 10.9(r)
 - Lease times, 30 seconds



“Remediation”

- Allow, deny rules on pools make sure only devices in remediation can get into 10.9.x.x address space
- Emails sent to owner, sysadmin, security officer
- Regular DNS
 - Go where you want to so you can fix yourself
 - Purpose of remediation is to heal
 - Get patches that we may not have available internally



“Remediation”

- **Less restricted, but Still painful**
 - Still filtered
 - No email, SAP
- **Fix problem, one click**
 - User told to save page to desktop if they need to reboot and still want to look at problem list
- **Hurry!**
 - 1 day limit, then block





Computer and Network Security

Remediation

SAVE THIS PAGE TO YOUR DESKTOP FOR FUTURE REFERENCE BEFORE PROCEEDING

Note: It can take up to 5 minutes before you are able to proceed

This device has been placed in **QUARANTINE** status

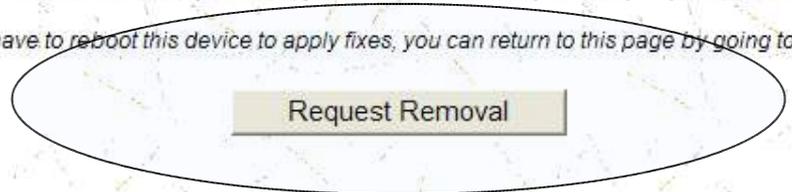
Reason: improper registration
Remedy: no property # is listed in the network registration system

Once these issues are addressed you may click **Request Removal** and your computer access will return to normal and your case will be reviewed by Cyber Security. *A device in REMEDIATION status longer than 24 hours is subject to being blocked*

More information can be found on VSWEB <http://home.ornl.gov/~vs4/prod>

For assistance or questions, please contact the HelpLine at (865) 241-ORNL.

Note: If you browse away from this page or have to reboot this device to apply fixes, you can return to this page by going to <https://remediation.ornl.gov> from this device.



Computer and Network Security

A request to unquarantine your device has been sent.

It can take up to 5 minutes before this device is restored to normal operation

Contact HelpLine for assistance

241-ORNL (241-6765)

“Parole”

- **Email generated to inform user, sysadm, division security officers of new status**
- **DHCP -- Back to normal**
 - Old address restored
 - 3-5 Minutes
- **Queued up for scan**

Parole Email

Date: Mon, 02 Apr 2007 11:16:30 -0400 (EDT)

From: helpline@ornl.gov

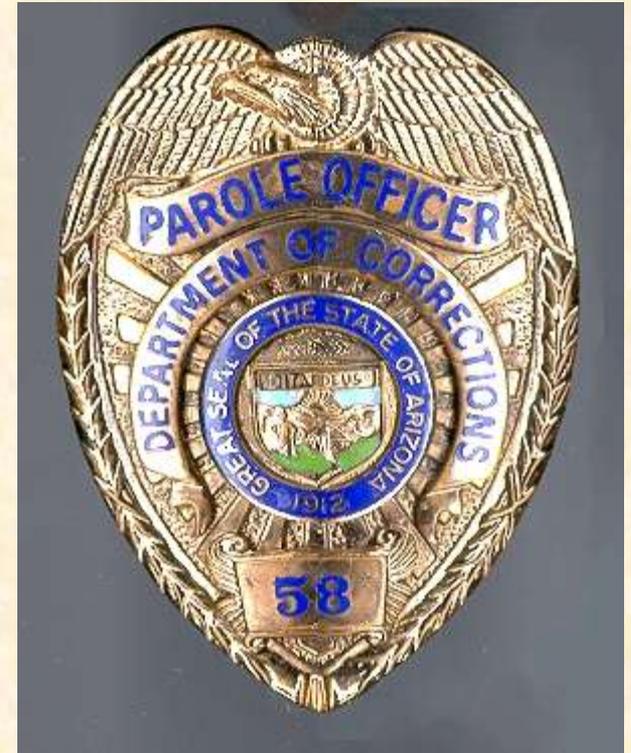
To: callowayj@ornl.gov

Subject: PAROLE for Device OKIMO

Device OKIMO has moved to PAROLE status.

“Parole” Characteristics

- **Not really anything special**
 - Regular address
 - DNS, DHCP back to normal
 - No filters to speak of
- **Parole officer can check out NACMgr to see list of paroled devices**





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

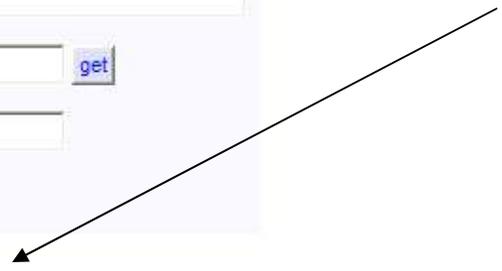
[Network Config](#) | [Polling](#) | [Access Control](#) | [Check Reg](#) | [Help](#)

Network Access Control Manager

Search for Network Registration (NetReg) Records -- for Access Control

Only one field is required.
All records are retrieved from NetReg database

Access Control Type	<input type="text" value="On Parole"/>
Device Name	<input type="text"/>
MAC Address	<input type="text"/> <input type="button" value="get"/>
IP Address	<input type="text"/>
Organization ID (8 char)	<input type="text"/>



Help!

- **At any time, quarantined folks can call the HelpLine**
- **Helpline has access to NACMgr to move to the various states**
- **So far, the user doesn't really seem to need it**



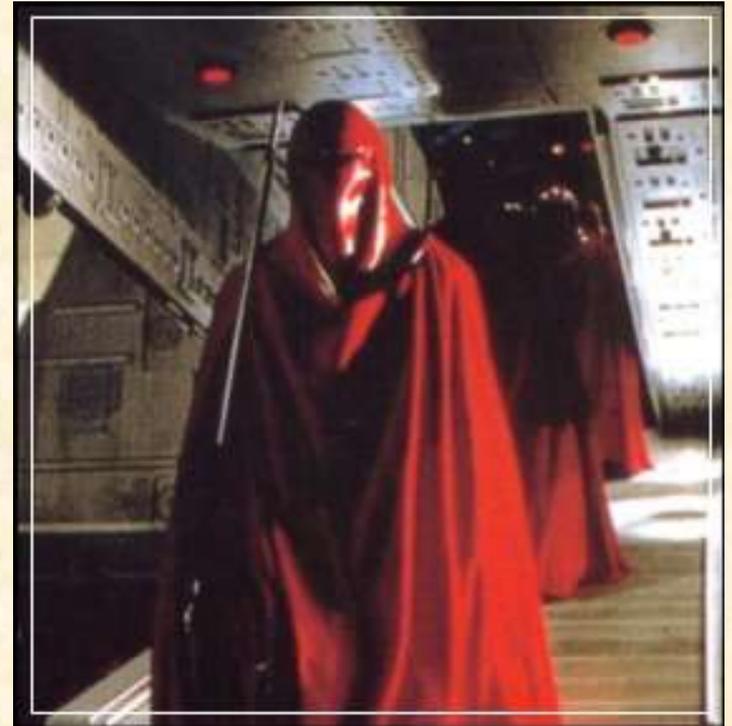
Quarantine --> DHCP-Blocks

- **Starting the process initiates a timer...**
 - Quarantine: 14 days
 - Remediation: 1 day
- **After then, you are dhcp-blocked**
- **Emails sent out**
 - User might not be in a state to read them
- **NACMgr can also directly do dhcp-blocks**



DHCP-Blocks, after the Quarantine

- **DHCP Configuration manipulated**
 - Group noboot {deny booting;}
 - By interface
 - DHCP routinely updated by information in database
- **Client doesn't get an ip address from DHCP server**



DHCP-Blocks

- **Normally, the dhcp client does not appreciate this turn of events**
- **Generate lots of logs, traffic**
- **User sometimes thinks something is wrong with the system**



DHCP Blocks -- Logs

May 23 11:51:36 dns dhcpd: [ID 702911 local7.info] DHCPDISCOVER

from 10:92:96:fb:83:a8 via 160.7.7.7: booting disallowed

May 23 11:51:36 dns dhcpd: [ID 702911 local7.info] DHCPDISCOVER

from 10:92:96:fb:83:a8 via 160.7.7.7: booting disallowed

May 23 11:52:12 dns dhcpd: [ID 702911 local7.info] DHCPDISCOVER

from 10:92:96:fb:83:a8 via 160.7.7.7: booting disallowed

May 23 11:52:12 dns dhcpd: [ID 702911 local7.info] DHCPDISCOVER

from 10:92:96:fb:83:a8 via 160.7.7.7: booting disallowed

May 23 11:52:17 dns dhcpd: [ID 702911 local7.info] DHCPDISCOVER

from 10:92:96:fb:83:a8 via 160.7.7.7: booting disallowed

May 23 11:52:17 dns dhcpd: [ID 702911 local7.info] DHCPDISCOVER

from 10:92:96:fb:83:a8 via 160.7.7.7: booting disallowed

First test..

- Someone had to be first
 - Initially, 12 devices were quarantined
- Within 1 day , all but one of the devices doing DHCP and on the network had entered quarantine



Oops!

- One escaped because a subnet had been overlooked (no quarantine and remediation pools)
 - That one was caught the *next* day



First test ..

- **Eventually, All of the folks doing dhcp were successfully quarantined**
 - Only 1 called HelpLine
- **Quarantined devices made it to parole**
- **A few (3-4) went to block status**
 - Not on network
- **Check NACMgr to see where the devices are at in the quarantine process**

Checking Up

- **NACmgr can be queried to see where the devices are at in the quarantine process**
- **Can query on any of the categories**
 - Quarantine
 - Remediation
 - Parole
 - DHCP-Block





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

Search for Network Registration (NetReg) Records -- for Access Control

Only one field is required.
All records are retrieved from NetReg database

Access Control Type	<input type="text"/>
Device Name	<input type="text"/>
MAC Address	<input type="text"/>
IP Address	<input type="text"/>
Organization ID (8 char)	<input type="text"/>

reSet | Back | [Search Logs](#) | search



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

Search Results -- Access Control

select	Device Name	Network Interface	IP Address	Device Status	Interface Status	NACmgr Block Status	Block Info Entered Modified	Dates DHCP Lease Last Seen	Days not using DHCP (Activity - Lease)
<input checked="" type="checkbox"/>	DENGAR	00.0D.56.E0.21.F0	160.091.216.043	REMEDiate	REMEDiate	-	-		WARNING - Interface is not using DHCP Quarantine and DHCP-Block will NOT work Only Access Control option is <u>Port Block</u>
<input type="checkbox"/>	DENGAR	00.90.96.FB.83.A8	010.003.005.165	REMEDiate	REMEDiate	-	-		WARNING - Interface is not using DHCP Quarantine and DHCP-Block will NOT work Only Access Control option is <u>Port Block</u>

Back | reSet | Select All | -- select Access Type -- | Control Access

Display Access Control | Show Logs | Show Polling



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 Access Control Manager

Search for Network Registration (NetReg) Records -- for Access Control

Only one field is required.
All records are retrieved from NetReg database

Access Control Type	<input type="text"/>
Device Name	<input type="text"/>
MAC Address	<input type="text"/>
IP Address	<input type="text"/>
Organization ID (8 char)	<input type="text"/>

- Quarantine
- Remediate
- On Parole
- Port Blocked
- DHCP Blocked**
- ANY Access Control Type

|
 |
 |



NAC Manager
NETWORK DETECTIVE AND POLICY ENFORCER

Oak Ridge National Laboratory's
Network Access Control Manager

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

Network Access Control Manager

Search Results -- Access Control

select	Device Name	Network Interface	IP Address	Device Status	Interface Status	NACmgr Block Status	Block Info Entered Modified	Dates DHCP Lease Last Seen	Days not using DHCP (Activity - Lease)
<input type="checkbox"/>	CRLIBRARY12	00.01.02.C3.A3.E8	160.091.172.059	DHCP-BLOCK	DHCP-BLOCK	DHCP-BLOCK	2007-04-03 - PIY 2007-04-17 - hlm	03-14-2007 -03-14-2007-	0
<input type="checkbox"/>	LOANER69761	00.18.8B.A8.67.F5	160.091.216.157	DHCP-BLOCK	DHCP-BLOCK	DHCP-BLOCK	2007-03-15 - PST --	03-01-2007 -03-01-2007-	0
<input type="checkbox"/>	NARASIMHANC	00.12.3F.14.E1.C6	Not Registered	-	-	DHCP-BLOCK	2007-04-03 - PIY 2007-04-17 - hlm	-	0
	NARASIMHANC	00.90.4B.FB.B9.D6	Not Registered	-	-	DHCP-BLOCK	2007-04-03 - PIY 2007-04-17 - hlm	-	0
<input type="checkbox"/>	OGLERBHPLT	00.0F.B0.75.01.18	128.219.194.059	DHCP-BLOCK	DHCP-BLOCK	DHCP-BLOCK	2007-04-03 - PIY 2007-04-17 - hlm	03-22-2007 -03-22-2007-	0
	OGLERBHPLT	00.14.A5.10.6A.BC	010.003.007.180	DHCP-BLOCK	DHCP-BLOCK	DHCP-BLOCK	2007-04-03 - PIY 2007-04-17 - hlm	03-20-2007 -02-08-2007-	40
<input type="checkbox"/>	THOMASDK-LAPTOP	00.00.86.5A.0F.9D	128.219.192.044	DHCP-BLOCK	DHCP-BLOCK	DHCP-BLOCK	2007-04-03 - PIY 2007-04-17 - hlm	03-01-2007 -03-01-2007-	0

Back reSet Select All -- select Access Type -- Control Access

Display Access Control Show Logs Show Polling

Quarantine Logging

- NACmgr has table for device status logging
 - Quarantine/Remediate cgi apps update this table
 - quarantine --> remediate, remediate --> parole
 - Even when user goes to remediate page more than one time
- Check to see if someone is consistently getting thrown into Quarantine for same issue
- Keep up with client activity





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

Search for Network Registration (NetReg) Records -- for Access Control

Only one field is required.
All records are retrieved from NetReg database

Access Control Type

Device Name

MAC Address [get](#)

IP Address

Organization ID (8 char)



reSet | Back | [Search Logs](#) | search

					<p>Remedy: Instructional aids for becoming compliant with DID requirements can be found at https://sharepoint.ornl.gov/nctd/cis/DID-2006/docs/default.aspx. You can also contact the Helpline at 241-ORNL for assistance.</p>
JAMESTEST	0C.0C.0C.0C.0C.0C	746268	QUARANTINE	2007-05-03:08:51:06 by ZCL	<p>This device has been placed in QUARANTINE status</p> <p>Reason: The network device named JAMESTEST registered to JAMES C CALLOWAY(746268) has been quarantined due to non-compliance with Defense In Depth (DID) requirements. You can determine the requirement(s) for which the device is not compliant by accessing the Individual Cyber Security Report (ICSR) at https://home.ornl.gov/sec-cgi-bin/cgiwrap/~csp/prod/fcsr.cgi and entering the badge number of the device owner.</p> <p>Remedy: Instructional aids for becoming compliant with DID requirements can be found at https://sharepoint.ornl.gov/nctd/cis/DID-2006/docs/default.aspx. You can also contact the Helpline at 241-ORNL for assistance.</p>
JAMESTEST	0A.0A.0A.0A.0A.0A	746268	REMEDiate	2007-05-03:08:51:29 by zcl	User has clicked the button to proceed to remediation
JAMESTEST	0B.0B.0B.0B.0B.0B	746268	REMEDiate	2007-05-03:08:51:30 by zcl	User has clicked the button to proceed to remediation
JAMESTEST	0C.0C.0C.0C.0C.0C	746268	REMEDiate	2007-05-03:08:51:30 by zcl	User has clicked the button to proceed to remediation
JAMESTEST	0A.0A.0A.0A.0A.0A	746268	PAROLE	2007-05-03:08:51:38 by zcl	User says they are ready to be paroled
JAMESTEST	0A.0A.0A.0A.0A.0A	746268	PAROLE	2007-05-03:08:51:38 by zcl	User says they are ready to be paroled

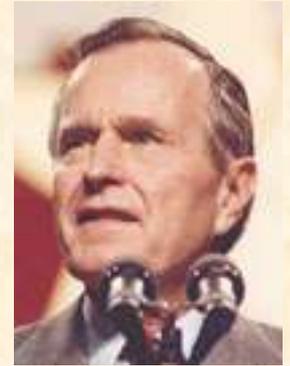
DHCP Requirement

- **Doesn't work for people not doing DHCP**
- **93-95% of our devices do DHCP already**
 - Upcoming requirement
- **If we need to, Port block**

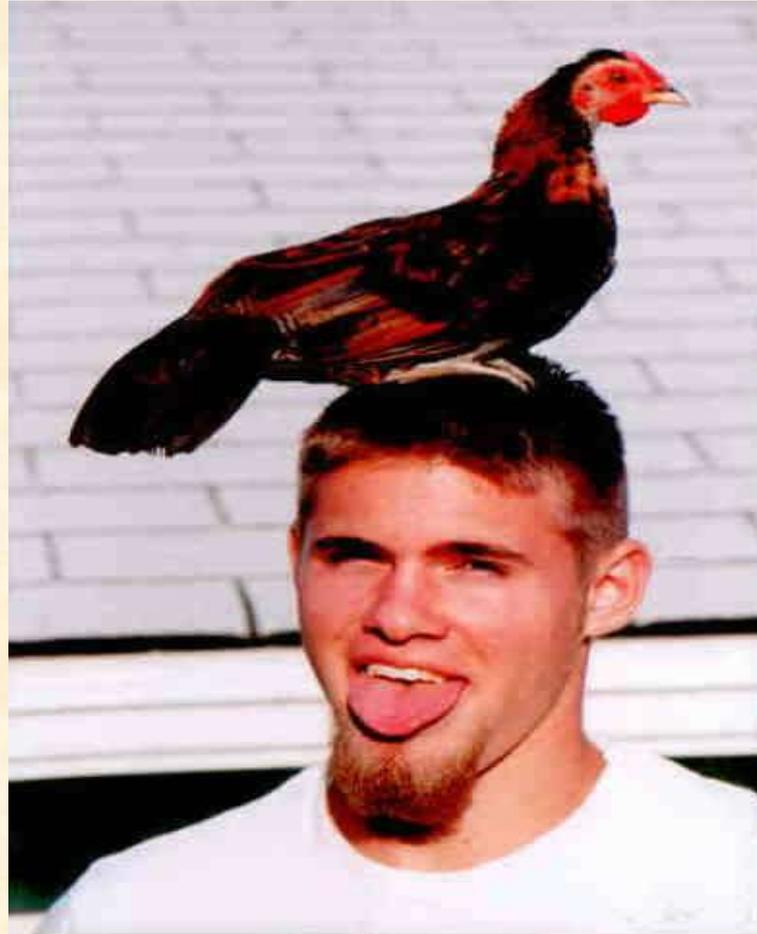


Quarantine, In the end...

- **ORNL's Kinder, gentler block**
 - Ability to self-remedy
 - Fix yourself on weekends, nights
- **More informative to the user**
- **Can usually fix themselves and return to normal in 10-15 minutes**
 - Patches
 - Network registration problems
 - Security requirements
- **Review by parole officer**



Questions ?



Supplemental Slides

ORNL DHCP

```
host randomhost {  
    hardware ethernet aa:aa:aa:aa:aa:aa;  
    fixed-address 128.214.22.11;  
    option host-name "randomhost";  
    option domain-name "ornl.gov";  
}
```

DHCP Classes

```
class "remediate" {  
    match hardware;  
    default-lease-time 30;  
    max-lease-time 30;  
    option domain-name-servers 16.91.130, 16.91.86.16;  
}
```

```
class "quarantine" {  
    match hardware;  
    default-lease-time 30;  
    max-lease-time 30;  
    option domain-name-servers 16.91.1.162,  
16.91.86.17;  
}
```

Shared Network, regular subnet

```
shared-network GE216-219
```

```
subnet 160.91.216.0 netmask 255.255.252.0 {
```

```
    authoritative;
```

```
    option domain-name "ornl.gov";
```

```
    option routers 160.91.216.1;
```

```
    option subnet-mask 255.255.252.0;
```

```
    option broadcast-address 160.91.219.255;
```

```
    pool {
```

```
        allow known clients;
```

```
        deny members of "quarantine";
```

```
        deny members of "remediate";
```

```
        range 160.91.219.2 160.91.219.127;
```

```
        default-lease-time 3600;
```

```
        max-lease-time 10800;
```

```
    }
```

Shared network, Autoreg subnet

```
subnet 10.1.216.0 netmask 255.255.252.0 {  
    authoritative;  
    option domain-name "ornl.gov";  
    option routers 10.1.216.1;  
    option subnet-mask 255.255.252.0;  
    option broadcast-address 10.1.219.255;  
    # AutoReg  
    pool {  
        allow unknown clients;  
        deny members of "quarantine";  
        deny members of "remediate";  
        range 10.1.216.32 10.1.216.47;  
        default-lease-time 900;  
        max-lease-time 900;  
        option domain-name-servers 160.91.86.7, 160.91.1.62;  
        option netbios-name-servers 160.91.86.7, 160.91.1.62;  
    }  
}
```

Shared network, Quarantine

```
subnet 10.8.216.0 netmask 255.255.252.0 {  
    authoritative;  
  
    option routers 10.8.216.1;  
  
    option broadcast-address 10.8.219.255;  
  
    pool {  
        allow members of "quarantine";  
        range 10.8.216.2 10.8.217.252;  
    }  
}
```

Shared network, Remediate

```
subnet 10.9.216.0 netmask 255.255.252.0 {  
  
    authoritative;  
  
    option domain-name "ornl.gov";  
  
    option routers 10.9.216.1;  
  
    option broadcast-address 10.9.219.255;  
  
    option domain-name-servers 160.91.1.62, 160.91.86.7;  
  
    pool {  
        allow members of "remediate";  
  
        range 10.9.216.2 10.9.217.252;  
  
    }  
  
}
```

Quarantine → Remediation

- May 23 13:40:34 netsrv2 dhcpd: [ID 702911 local7.info] DHCPREQUEST for 10.8.88.252 (160.91.1.30) from 00:90:96:fb:83:a8 via 160.91.88.3: unknown lease 10.8.88.252.
- May 23 13:41:11 ns1 dhcpd: [ID 702911 local7.info] DHCPOFFER on 10.9.88.252 to 00:90:96:fb:83:a8 (dengar) via 160.91.88.2
- May 23 13:41:11 ns1 dhcpd: [ID 702911 local7.info] DHCPREQUEST for 10.9.88.252 (160.91.1.30) from 00:90:96:fb:83:a8 (dengar) via 160.91.88.2
- May 23 13:41:11 ns1 dhcpd: [ID 702911 local7.info] DHCPACK on 10.9.88.252 to 00:90:96:fb:83:a8 (dengar) via 160.91.88.2

Remediation → Parole

May 23 13:57:32 ns1 dhcpd: [ID 702911 local7.info] DHCPREQUEST for 10.9.88.252 from 00:90:96:fb:83:a8 via bge0: lease 10.9.88.252 unavailable.

May 23 13:57:32 ns1 dhcpd: [ID 702911 local7.info] DHCPNAK on 10.9.88.252 to 00:90:96:fb:83:a8 via bge0

May 23 13:57:37 ns1 dhcpd: [ID 702911 local7.info] DHCPDISCOVER from 00:90:96:fb:83:a8 via 160.91.88.2

May 23 13:57:38 ns1 dhcpd: [ID 702911 local7.info] DHCPPOFFER on 160.91.89.63 to 00:90:96:fb:83:a8 (dengar) via 160.91.88.2

May 23 13:57:38 ns1 dhcpd: [ID 702911 local7.info] DHCPREQUEST for 160.91.89.63 (160.91.1.30) from 00:90:96:fb:83:a8 (dengar) via 160.91.88.2

May 23 13:57:38 ns1 dhcpd: [ID 702911 local7.info] DHCPACK on 160.91.89.63 to 00:90:96:fb:83:a8 (dengar) via 160.91.88

Quarantine >14 days

Date: Fri, 30 Mar 2007 11:40:39 -0400 (EDT)

From: helpline@ornl.gov

To: callowayj@ornl.gov

Subject: Device JAMESTEST has been DHCP-BLOCKED

Device JAMESTEST has been in QUARANTINE for longer than 14 days.

The status has been changed to DHCP-BLOCK.