swisscom

Training Seminar: how to use [Free]NAC

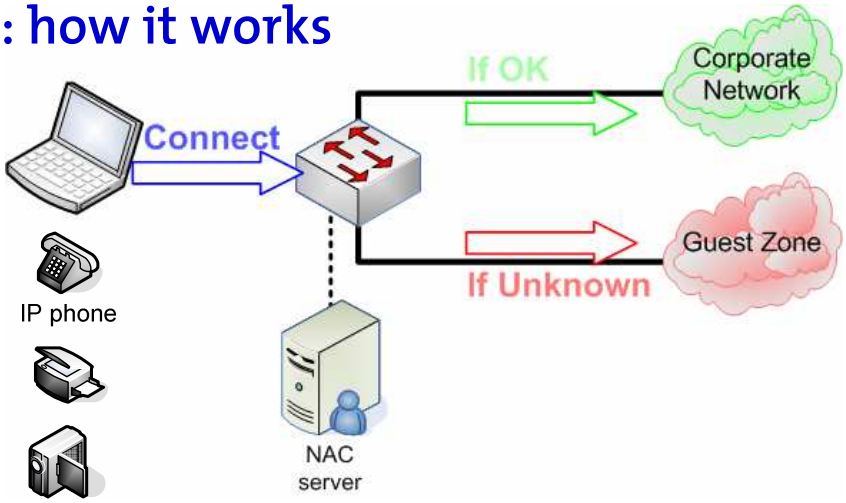
Date: 27.03.2007

Training course for FreeNAC and the NAC Enterprise Version
By Sean Boran, Swisscom.
Last Update: 27. March 2007

Presentation structure

1. NAC Overview
2. Windows GUI: Overview & Edit Tabs
3. Windows GUI: Server Log, Change Log, Switch, Ports
4. Windows GUI: Lookups, reporting
5. Advanced topics
6. Questions

NAC: how it works



- Access is granted based on the MAC address (VMPS mode)
- Or, 802.1x authentication (Windows Domain)

3

NOTES:

HOW IT WORKS:

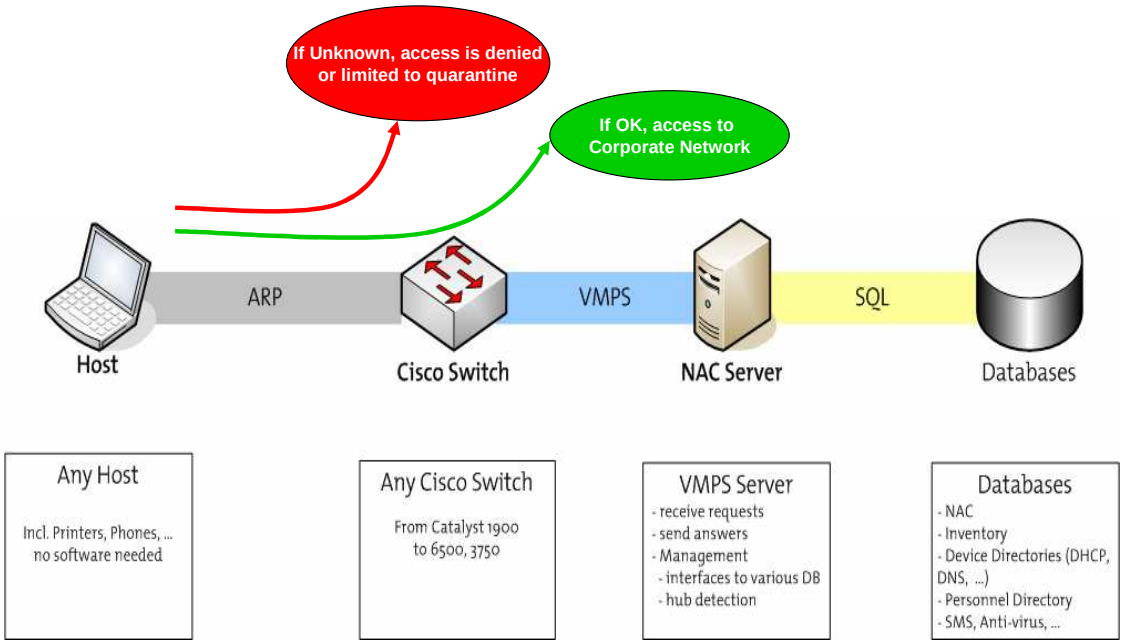
•The Switch detects a new PC and requests authorisation from NAC via the VMPS protocol, which checks its Database and refuses or grants access based on the MAC address

•802.1x is supported with User Authentication in the Windows Domain, and Vlan assignment based on MAC address

•only for **Cisco Switches** (at the moment) and **any kind of network device** (PC, Printers, IP phones, Webcams, etc)

NAC can directly replace other VMPS solutions, or manual "port based MAC lists" with **major improvements in ease of use.**

How NAC works in “vmps mode”



Any Host

Incl. Printers, Phones, ...
no software needed

Any Cisco Switch

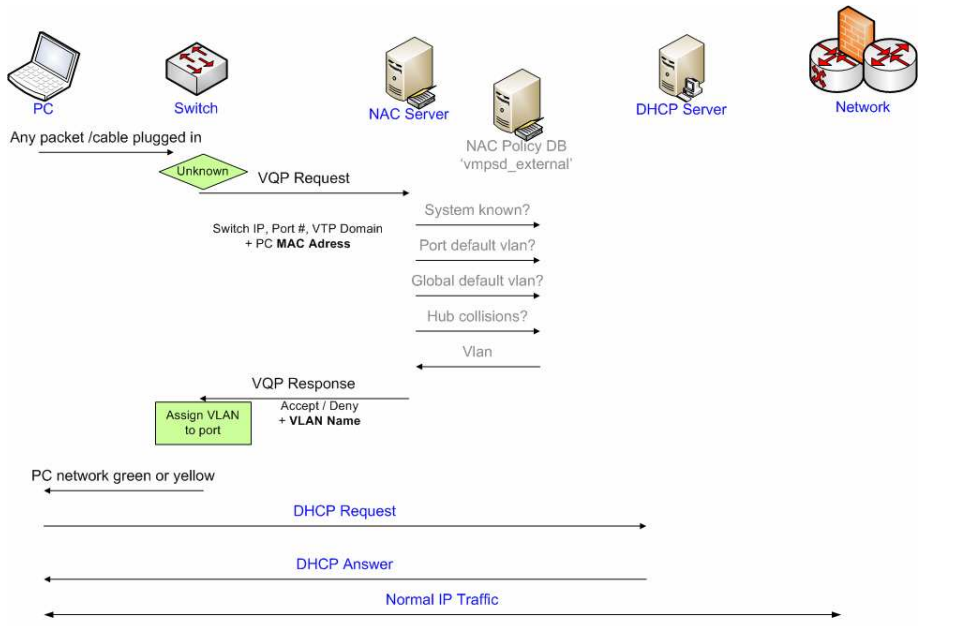
From Catalyst 1900
to 6500, 3750

VMPS Server

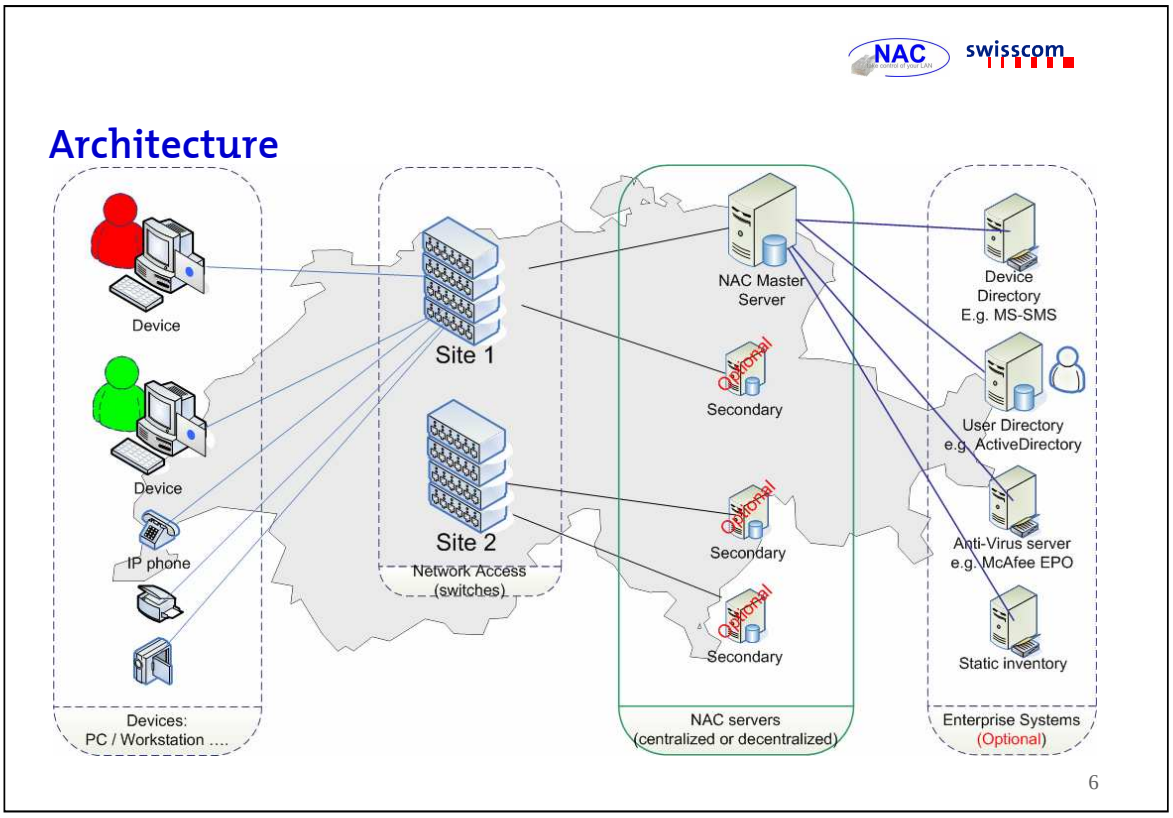
- receive requests
- send answers
- Management
  - interfaces to various DB
  - hub detection

Databases

- NAC
- Inventory
- Device Directories (DHCP, DNS, ...)
- Personnel Directory
- SMS, Anti-virus, ...



End-device authentication: Sequence of events in 'vmps mode'



NOTES:

NAC consists of

- One Master server with Database and Control programs
- Optionally: one or more slave servers for redundancy and load distribution

In a fully integrated environment, NAC requires:

Access to an email server for delivery of alerts

- Access to DNS for discovering names associated IP addresses
- Recommended : SNMP read/write access to switches (to restart ports and scan for unmanaged end devices)
- Recommended : SNMP read access to routers (to query MAC/IP tables)
- Recommended : Syslog messages from switches
- Optionally: Interface to Enterprise Static Inventory, User, Device, Inventory, MS-SMS, MS-Wsus, McAfee EPO, or other database

NAC is remotely configured via a Windows-based GUI, that may be installed on one or more a Windows PC or via a Web-based interface.

NAC tasks

Once NAC has been installed, configured, tuned and is running smoothly, what are the tasks to be done?

1. Add new PCs:

   This is usually done by the person who install new PCs. Before delivery to Users, the PC is connected to a NAC network port, NAC detects the system as 'unknown', the NAC Gui then is used to set the vlan, enable the device.

2. 'Unknowns' appear on the network:
   An email alert is received by the administrator, indicating either an intrusion, a Visitor who needs access, or a User with an unknown PC.
   Read the email alert to see where it is and then either pro-actively check/configure NAC for that device, or wait for the user to call.

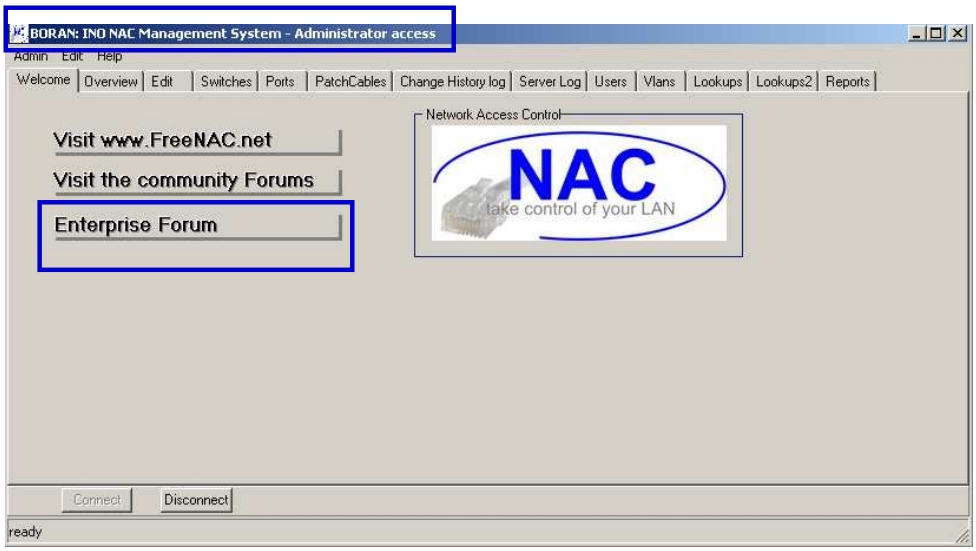
3. Periodically you may wish to run reports, or check the status of systems or switches.

This presentation explains the Windows Gui, so you can see how NAC is configured.

Presentation structure

1. NAC Overview
2. Windows GUI: Overview & Edit Tabs
3. Windows GUI: Server Log, Change Log, Switch, Ports
4. Windows GUI:
5. Advanced topics
6. Questions

Starting the Windows GUI



9

The Enterprise forum is where you can look for help /support. Please subscribe!

The community forms may provide additional help.

The main website, www.FreeNAC.net provides lots of documentation and provides a search function.

What happens when an “unknown” connects to the network?

- Devices which are not in the NAC database, are ‘unknown’
- These will be denied access, or switched to a specific lan, depending on your policy

- How do you notice an ‘unknown’?
- What needs to be done to grant access?

What do automated Email Alerts look like?

```
From: root vmps1
Sent: Thursday, February 09, 2006 6:06 PM
To:
Subject: VMPS alert 2/40 in office 3.16,

New unknown 000a.e476.1b38 (Wistron), switch sw0303(Patch:
Schenker,Wyler,Berger  -x 03.013 3.16 TGDSCED1 )
```

11

NOTES:

A new device has been connected to the network (port 2/40 switch sw0303), but not authorised.

-it was in room 3.16

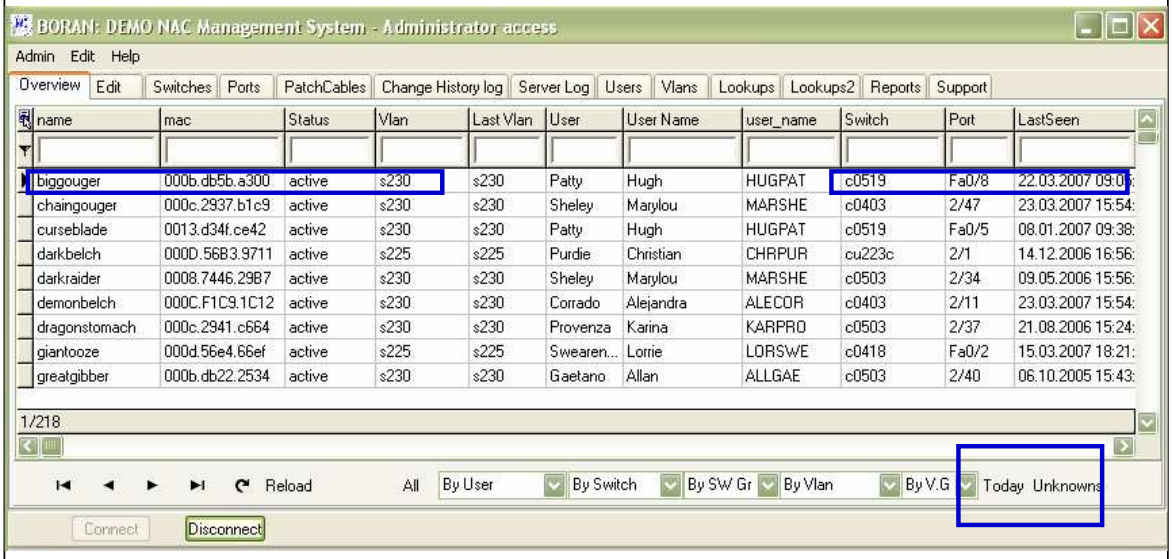
-on Cable socket X 03.013 (this is the name written on the socket in the wall)

-in this room the users Schenker, Wyler and Berger have their offices

-The user TGDSCED1 has been documented as using this cable

The 'super-users' defined for this switch are Schädler and Rappo, so they receive the Alert, along with the NAC Administrators.

Overview Tab



12

Key fields are noted in blue.

The 'today' and 'unknowns' toggle buttons are in the "down" start when you start the GUI, meaning that only unknown systems

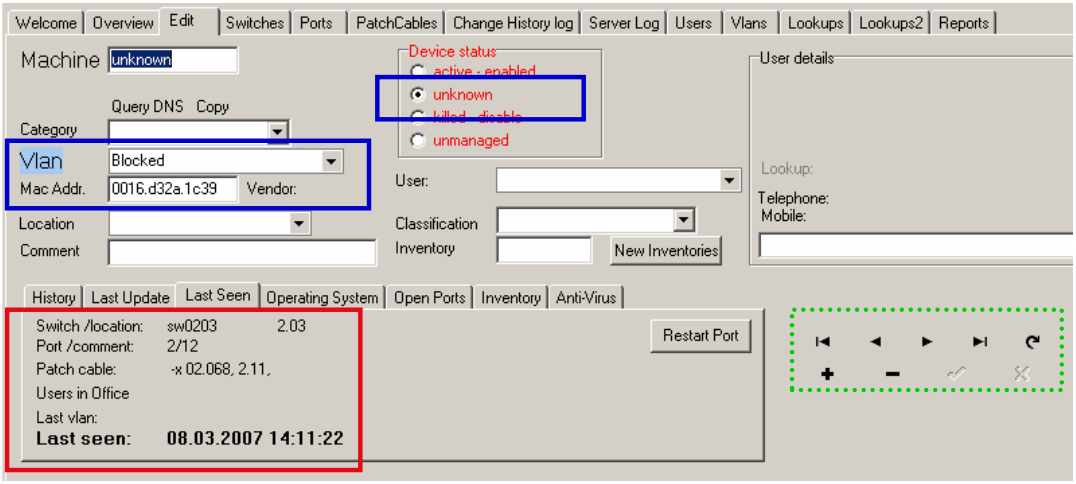
seen in the last 24 hours are displayed.

Press each button again to put them in the "up" status, or press the "all" button to see every systems in the overview.

There are also several drop-down lists for showing the systems per user, per switch, per group of switches, per vlan, and vlan group.

Each of these filters inserts an appropriate text into the filter row in the grid. In fact you can add your own manual filters there too!

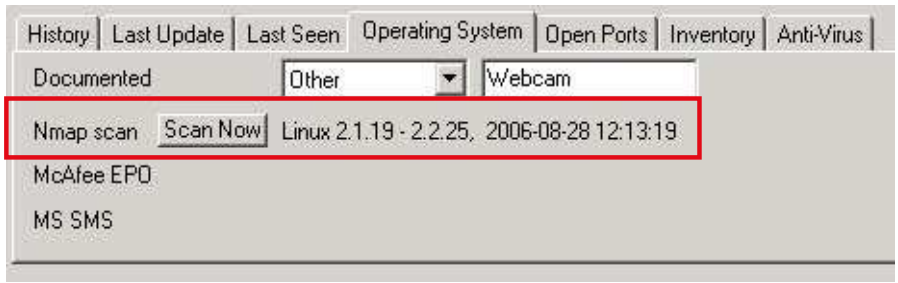
Edit Tab

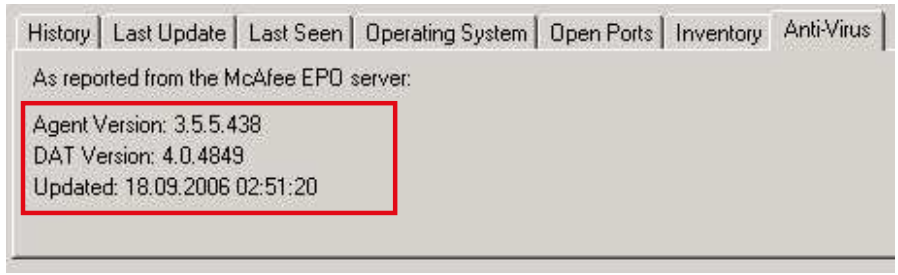


13

1. In blue is the crucial MAC information: mac address, the status (which must be active if a device is allowed access) and the vlan we assign.
2. In red is information about where the end-device was last seen, and where.
3. All other fields are informational, and thus an option. You need to decide what is best for your environment. We come back to the Edit Tab in more detail later
4. There are several optional modules (nmap, static inventory, patch cables, McAfee Anti-virus), if these are not enabled in your environment, they will be disabled on invisible.

Edit Tab: nmap and Anti-Virus





14

•The Nmap scanning module can detection operating system version and open ports. It can scan one device immediately, or the list of IPs in the NAC database on a scheduled basis.

•If the McAfee EPO module is enabled, the operating system of end devices, as reported by McAfee, and the current Anti-Virus status, can be displayed.

•Beside the Anti-Virus tab, we also se an "inventory", which is where we link to you in-house static Inventory Database, if required.

Presentation structure

1. NAC Overview
2. Windows GUI: Overview & Edit Tabs
3. Windows GUI: Logs, Switch/Ports, Patches, Users
4. Windows GUI:
5. Advanced topics
6. Questions

Server Log: what is the server doing?

Welcome | Overview | Edit | Switches | Ports | PatchCables | Change History log | Server Log | Users | Vlans | Lookups | Lookups2 | Reports

Click here to define a filter

Time	priority	Message
22.02.2007 08:13:10	info	New INFNET 000b.5d46.383d (FUJITSU) u128116, TZHDERO3, , switch sw
22.02.2007 08:13:08	info	New user added for Direx: TZHDERO3
22.02.2007 08:13:08	info	Port successfully restarted 2\/43 on switch 192.168.245.175
22.02.2007 06:33:52	info	Manual Users synced from Direx
22.02.2007 06:00:04	info	User table synced from Direx 1 new entries, 180 updates
22.02.2007 06:00:04	info	Insert Direx user: Daniel,Boos,TGDBODA7,Ber-Omu93,7.23,,INO-UAL
21.02.2007 18:01:18	info	New port Fa0/8 on sw 192.168.245.97, location=Ber-Omu93.
21.02.2007 16:17:49	info	New port Fa0/1 on sw 192.168.245.97, location=Ber-Omu93.
21.02.2007 16:17:49	info	New switch entry 192.168.245.97, please update the description.
21.02.2007 06:33:52	info	Manual Users synced from Direx
21.02.2007 06:00:04	info	User table synced from Direx 0 new entries, 0 updates
20.02.2007 19:17:16	info	New INFNET 0015.c547.fee8 (unknown) u152028, TGDZUSI2, , switch sw
20.02.2007 19:17:13	info	New user added for Direx: TGDZUSI2

Get 500 older entries: Previous Next offset=0

GUI Change Log: who is logged on, what have they done?

Overview | Edit | Switches | Ports | PatchCables | Change History log | Server Log | Users | Vlans | Lookups | Lookups2 | Reports | Support

Click here to define a filter

datetime	Host	Priority	User Name	Message
27.03.2007 09:42:44	INOTGDBOSE1	info		Logon successful: () BORAN, INO
27.03.2007 09:41:26	INOTGDBOSE1	info		Pre-Post system: unknown, 0000.0000.0001, uid:, comment: , office: , Port: , , vlan1
27.03.2007 09:41:26	INOTGDBOSE1	info		Updated system: unknown, 0000.0000.0001, Id: , , , Port: , , vlan1
27.03.2007 09:37:28	INOTGDBOSE1	info		Pre-Post system: unknown, 000c.2937.b1c9, uid:195, comment: , office: 0, Port: 2/4
27.03.2007 09:37:28	INOTGDBOSE1	info		Updated system: unknown, 000c.2937.b1c9, Id: 195, , 0, Port: 2/47, c0403, vlan1
27.03.2007 09:27:37	INOTGDBOSE1	info		Logon successful: () BORAN, INO

Switch & Ports

Overview | Edit | Switches | Ports | PatchCables | Change History log | Server Log | Users | Vlans | Lookups | Lookups2 | Reports | Support

name	Location	GUI Group	comment	notify	ip	Enabl	Firmware	hw
c0503	Floss Street 5.03	5		notify1@freenac.net,notify2@freenac.net	192.168.245.71	☑	8.4(1)GLX	WS-C2948G
c0603	Floss Street 6.03	6		notify1@freenac.net,notify2@freenac.net	192.168.245.72	☑	8.4(1)GLX	WS-C2948G
clablab	Floss Street GRL	GR		notify1@freenac.net,notify2@freenac.net	192.168.245.79	☑	8.4(1)GLX	WS-C2948G
csrvback	Floss Street U140	GR		notify1@freenac.net,notify2@freenac.net	192.168.245.159	☑	8.4(1)GLX	WS-C2948G
c0703	Floss Street 7.03	7		notify1@freenac.net,notify2@freenac.net	192.168.245.73	☑	8.4(1)GLX	WS-C2948G
csrvita	Floss Street U140	GR		notify1@freenac.net,notify2@freenac.net	192.168.245.81	☐	8.4(1)GLX	WS-X2948G

Overview | Edit | Switches | Ports | PatchCables | Change History log | Server Log | Users | Vlans | Lookups | Lookups2 | Reports | Sup

switch	Port	Default Vlan	Comment	Patch details	Last Vlar	Last Used	Index
				Click here to define a filter			
cdemo	Fa0/15				s230	23.03.2007 09:00:42	587
ceg03	2/47				s230	26.03.2007 05:27:06	433
ceg03	2/48	iads	Bonvin	-x 0.025 unknown	s230	22.02.2007 14:25:10	434
cgrllab	2/48			-x U1.602 U139	s230	26.02.2007 11:38:33	690
cu305	2/48			-x U3.017 U310	s230	26.03.2007 05:26:27	464
czg03	2/10			-x ZG.007 unknown	s230	23.02.2007 16:18:39	334

18

Switches:

- location
- group field, used in the overview tab for grouping
- comment
- Emails list for notifications of new unknown devices
- Enable SNMP scanning?
- Documentation: Firmware, hardware

Ports:

- switch name, port name
- default vlan, for that port (i.e. ignore global default)
- Patch cable details (if the PatchCable option is enabled, and the tables filled)
- The last vlan used on that port, and when that port was last used

Patch Cables

Overview | Edit | Switches | Ports | PatchCables | Change History log | Server Log | Users | Vlans | Lookups | Lookups2 | Reports | Support

Rack	Rack socket	Office Soc	Office	Users in that office	Cable type	Switch port	Destination	Comment
Click here to define a filter								
01-03.1	09/07	-x 01.022	Floss Street 4.19	Christian	telco		01-03.2	
01-03.1	09/06	-x 01.021	Floss Street 4.18		phone		01-03.2	
01-03.1	09/05	-x 01.020	Floss Street 1.20		phone		01-03.2	
01-03.1	09/04	-x 01.019	Floss Street 1.20		phone		01-03.2	
01-03.1	09/03	-x 01.018	Floss Street 419		grouplan		01-03.221/01	
01-03.1	09/02	-x 01.017	Floss Street 1.20		phone		01-03.2	
01-03.1	09/01	-x 01.016	Floss Street 5.12	Tyrone	dynamic	c0103 2/36	01-03.226/36	

19

The Cabling screen is design to allow complete documentation of cabling rooms, not just LAN cables, but telephone, point to point etc.

In the blue box is a switch a port references by a specific cable.

•Rack: consists of floor number, room number, and rack number

•Rack socket: which unit number, counted from the ground up, and which sockets, counted from the left

•Office socket: the name written on the final Socket (at the user's desk)

•Office: the location of the final socket.

•Users in that office: this information is automatically looked up from a central user directory

•Cable type: **dynamic (i.e. computer LAN with NAC), static (static LAN port**), telco, phone, pointtopoint, adsl

•**Switch port**: lookup into switches and ports documented in NAC

•Destination: floor number - room number, rack number (1 digit), switch port (e.g. 6/36)

Users

Overview | Edit | Switches | Ports | PatchCables | Change History log | Server Log | Users | Vlans | Lookups | Lookups2 | Reports | Support

User details

NT Account: ALLGAE [Search]
GivenName: Gaetano
Surname: Allan [Search]
Email: Allan.Gaetano@freenac.net
Department: Marketing
Floss Street 4.16
Telephone: +41-88-1877625
Mobile: +41-49-5054382

Last time updated from Directory
26.03.2007

NAC Gui Rights
- no access
- Read-only
- Edit - changes allowed
- Administartor

Manual Directory Sync

Queries
Administrators | Edit allowed | ReadOnly Users | Expired Users

Patty Hugh, HUGPAT
Pinzon Allan, ALLPIN
Corrado Alejandra, ALECOR
Gaetano Allan, ALLGAE

Comment

20

Users can be created locally with NAC, but are usually synchronised via an external Enterprise data source such as Active Directory.

Key fields:

•Username

•NAC GUI rights: Administrator, Edit mode, Readonly, Otherwise, no access

Also:

•Comment: This text field is not synchronised with Directories, so its just an information on the user stored in NAC.

•Manual Directory Sync: used for forcing a single user synchronisation, for advanced administration only.

•The queries on the right provide a list of NAC configured administrators, those who can make changes, and the list of users with read-only access.

Edit Tab: in detail

- Status: Is this system enabled, not yet authorised, not actively managed by NAC, or to be explicitly denied?
- Expiry: A date after which a device is to be denied access
- DNS forward/reverse lookups and copy
- Comment
- Bottom box:
  - History
  - Last Update
  - Operating System. Open Ports
  - Static Inventory
  - Anti-Virus

21

Device expiry: With v2.2, one can now set an expiry date for devices in NAC. This may be useful in limiting how long external visitors have access.

When an expired device is detected, its is set to the "killed" state, and an email alert is sent. In the killed state the device is blocked, but no alerts are sent.

Example email alert:

> Subject: NAC alert: expired device
>
> Device inossmhaur1(0008.7446.2aa5) with expiration date 2007-02-25 12:00:00 has been refused network access and its status has been set to killed.

Edit Tab: in detail

Overview | Edit | Switches | Ports | PatchCables | Change History log | Server Log | Users | Vlans | Lookups | Lookups2 | Reports | Support

Machine giantooze

Query DNS Copy 10.0.225.123

Category unknown

Vlan Slab225 Floors:2,3,4,7,8,9 DHC

Mac Addr. 000d.56e4.66ef Vendor: Dell

Location

Comment

Device status
- active - enabled
- killed - disable
- unknown
- unmanaged

Expiry

User: Lorrie

Classification

Inventory 0 New Inventories

User details 26.03.2007

Swearengin Lorrie
LORSWE HR

44 Nac Street 4.12
Floss Street 4.12

Telephone: +41-88-806913
Mobile: +41-49-1291093

Lorrie.Swearengin@freenac.net

History | Last Update | Last Seen | Operating System | Open Ports | Inventory | Anti-Virus

Documented Windows XP

Nmap scan Scan Now Microsoft Windows 2003 Server or XP SP2 2006-10-30 12:09:04

McAfee EPO

Presentation structure

1. NAC Overview
2. Windows GUI: Overview & Edit Tabs
3. Windows GUI: Server Log, Change Log, Switch, Ports
4. Windows GUI: Lookups, reporting
5. Advanced topics
6. Questions

Lookup tables: vlans

Overview | Edit | Switches | Ports | PatchCables | Change History log | Server Log | Users | Vlans | Lookups | Lookups2 | Reports | Support

Name on Swi...	Group	GUI Description	Numb...	D...
iPhones	551	Voip Phones	551	
iVoIP	550	Voip Server	550	
Lab5	965	Lab5 Context	965	
OneComm	560	Project X5Comm	560	
s225	2	Slab225 Floors:2,3,4,7,8,9 D...	10	
s226	2	Slab226 DHCP	11	
s227	2	Slab227 Servers	9	
s230	2	Slab230 DHCP	13	
s237	3	Slab237	31	
sadsl0	500	ITAadsl0	500	
sadsl1	500	ITAadsl1	501	
sadsl2	500	ITAadsl02	502	
TV-Demo	511	TV-Demo	511	

20/20

Standard Vlan names

Switch	Default Vlan	Vlan on this switch - exac

<No data to display>

Vlan name exceptions per switch

24

- The vlan table must contain the exact vlan name as configured on the switch.
- The Group is used is collect vlans of the same security level and physical location: if intelligent hub detection is enabled, NAC with switch a users vlan within a vlan group, to avoid conflicts on hubs.
- The 'Gui Description' is the name shown in the Edit tab, and should be easy to understand for first level support staff.
- The Number corresponds to the vlan number on the switch. This number is only used for documentation

The "vlan exception" table is not yet used, planned for a later feature allowing location dependant vlans.

Lookups: Operating System

Welcome | Overview | Edit | Switches | Ports | PatchCables | Change History log | Server Log | Users | Vlans | Lookups | Lookups2 | Reports

Operating System

id	value
1	unknown
2	Windows
3	Linux
5	BSD
6	MacOS
7	Unix
8	Other

OS #1

id	value
1	unknown
2	98
3	ME
4	NT
5	2000
6	XP
7	2003
8	Vista
9	RedHat
10	Fedora
11	Gentoo
12	Suse
13	macos
14	FreeBSD

OS #2

id	value
1	unknown
2	RTM
3	SP1
4	SP2
5	SP3
6	SP4
7	SP5
8	SP6

OS #3

id	value
1	unknown
2	x86
3	x64
4	sparc
5	sparc64
6	ppc
7	ppc64
8	hppa
9	alpha

25

These 4 tables define the list of operating system options presented in the ‘Edit Tab’

Lookups: locations, device types

Overview | Edit | Switches | Ports | PatchCables | Change History log | Server Log | Users | Vlans | Lookups | Lookups2 | Reports | Support

Buildings

id	name
1	unknown
2	Floss Street

Locations

Location	Building	id
316	Floss Street	327
316	Floss Street	172
320	Floss Street	93
320	Floss Street	313
4	Floss Street	229
4. Stock	Floss Street	91
4.03	Floss Street	276
4.1	Floss Street	260
4.11	Floss Street	9
4.12	Floss Street	7
4.14	Floss Street	14
4.15	Floss Street	11
4.16	Floss Street	23

Device Type #1

id	value
1	unknown
3	Workstation
5	Server
10	Appliance
11	Web Cam
20	VM
40	Printer
50	IP phone
70	Externals: Consultar
90	Network Componen

Device Type#2

id	value

<No data to display>

26

The documentation of where Users and Devices depending on buildings being defined (the left table), and then a list of locations or offices defined within that building. When locations have been defined, they are available in drop down lists on the Edit, Switch, Users and PatchCable tabs.

On some sites the Buildings and Locations are automatically synchronised from Enterprise sources.

The device type tables are just categories that you would find useful in for organisation for the end devices. They are used in the Edit Tab.

Reporting

Overview | Edit | Switches | Ports | PatchCables | Change History log | Server Log | Users | Vlans | Lookups | Lookups2 | Reports | Support

Drag a column header here to group by that column

Click here to define a filter

name	Surname	GivenName	Department	LastSeenDir	mac	comment	value	LastSeen
labnaclaol02	Bonvin	Oliver	UNIT3XARC	26.03.2007	000e.a6b6.b4f1		active	22.02.2007 14:27:29
ogrebasher	Emilia	Morein	HR	26.03.2007	0011.4343.c0b4		active	22.02.2007 14:25:58
rottooth	Allan	Gaetano	Marketing	26.03.2007	0002.b3f0.9c2e		active	22.02.2007 14:17:21
slimekill	Allan	Gaetano	Marketing	26.03.2007	0002.b3f0.9b72		active	22.02.2007 14:17:21
evilrot	Allan	Gaetano	Marketing	26.03.2007	0001.03cd.8622		active	22.02.2007 14:17:21
filthscum	Allan	Gaetano	Marketing	26.03.2007	0001.03cd.8653		active	22.02.2007 14:17:19
sun5	Christian	Purdie	Finance	26.03.2007	0800.2083.8fdd		unmanaged	21.02.2007 11:53:54
mossgloom	Hugh	Patty	HR	26.03.2007	0013.d4c9.d365		active	21.02.2007 11:14:49
labnacbafl11	Scafe	Bourquin	Development	26.03.2007	0018.8ba6.bd4f		active	16.02.2007 12:14:08
greatstealer	Jessie	Morini	Development	26.03.2007	0008.74e6.1357		active	15.02.2007 16:18:21
cursetracker	Ericka	Hallberg	Development	26.03.2007	0015.c509.abd9		active	12.02.2007 11:12:52
vm	Allan	Jenner	HR	26.03.2007	000c.2927.2051		active	07.02.2007 11:58:39

Expired Users | Expired Users: Systems | Unused Systems | Systems with old AV | All Systems | Export to Excel

27

The reporting tab allows some standard reports to be generated, and these can option be exported to excel.

In the above example, the “Unused Systems” report was run.

Note that if you let the mouse hover over the button of each report it tells you want the report does, e.g. “Devices not seen in over 30 days”.

Presentation structure

1. NAC Overview
2. Windows GUI: Overview & Edit Tabs
3. Windows GUI: Server Log, Change Log, Switch, Ports
4. Windows GUI:
5. Advanced topics
6. Questions

Advanced Topics: Cisco IOS Switch configuration example

1. Configure the switch for VMPS

```
conf t
vmps server 192.168.245.40
vmps server 192.168.245.41
vmps reconfirm 120
vmps retry 5
```

2. Verify configuration

```
vmps reconfirm
show vmps
show vmps stat
show vlan
```

3. Enable VMPS on port fa0/2:

```
conf t
int fa0/2
switchport access vlan dynamic
```

IP address or primary/secondary NAC servers

Re-authorise all MAC every 2hrs

Attempt to contact NAC server 5 times, before switching to a secondary

Ask switch to re-authorise all macs

Advanced Topics: Cisco IOS Switch configuration example

- Tuning

```
conf t
arp mac-address-table aging-time XXX
```

- more commands:

```
no vmps server  192.168.245.18
clear mac-address-table dynamic
vmps reconfirm
clear vmps statistics
```

Keep MAC in memory for XXX seconds. Should be 12hrs if you don't have 7x24 support

Remove NAC server

To be sure the switch forgets all MACs is now has

Advanced Topics: 'emergency off' scripts

The aim is to configures switches such that all ports which were 'dynamic' i.e. NAC controlled, are re-configured with static vlan, so that NAC no longer has any influence.

procedure:

```
cd /opt/nac/enterprise
# Enter the switch user/passwords
vi swconf.inc
# Generate a recovery script per switch:
swconfig_static.php
```

Generated scripts are stored in 'swtmp'. In an emergency, execute the script for a particular switch, e.g. the switch called 'bav205s1'

```
cd /opt/nac/enterprise/swtmp
./static_bav205s1
```

31

Planning for disaster

If Nac is installed into your core network, and can affect the availability of critical workstation and server, you may wish to have a way of deactivating NAC, in case of severe network problems. We've never had to use these scripts so far, but planning for disaster is important.

- After executing the emergency stop script, the switch no longer has any dynamic ports
- If you wish to re-enable switch ports to dynamic, this will have to be done manually, or via a tool such as ciscoworks, or the free tool 'ciscocmd'
http://cosi-nms.sourceforge.net/
- If you cannot remember which ports were dynamic, just look at those that have a lastvlan or defaultvlan in the switches tab of the Windows GUI.

Advanced Topics: Importing external data

- You may need to be able to import list of systems with mac address, vlan, etc.. into NAC
- Such scripts tend to be site specific

- One example is ' import_systems_csv1' in /opt/nac/contrib,
  examine it and sample_csv1.txt and adapt for your needs

Advanced Topics: UNIX commands

```
tail -f /var/log/messages
log
logv

tcpdump -X -n port 1589
tcpdump -X -n host 192.168.2.1

ps -ef | egrep 'mysql|vmps'

crontab -l
ls -altr /opt/nac
ls -altr /etc/init.d/vmps*

mysql opennac
mysql> show tables;

cat /etc/mods
```

- Monitoring logs
- Monitoring vmps essential logs
- sniffing vmps traffic, or to/from a specific host
- are essential programs running?
- List automatically scheduled programs
- Show DB tables
- Show system changelog

Advanced Topics: further reading

On the FreeNAC.net website, documentation may be of use:
http://www.freenac.net/pages/documentation.php as well as the repository, http://svn.sourceforge.net/viewvc/opennac/branches/2.2/doc/ and In the /opt/nac/doc, /opt/nac/enterprise/doc directory on the NAC server.

- Master server installation notes:
  master_enterprise_install.txt, unix_install.txt, master_server_install.txt, master_server_config.txt, db_install.txt
- Slave server installation: unix_install.txt, slave_server.txt, slave_mysql_sync.txt
- Description of components: website,
  README.vmpsd, nac_components.txt, vmpsd_external_flow1.png, README.ad_user_sync, README.port_scan, README.rdiff, README.web2, direx_user_management.txt, mssql.txt, mssql_epo.txt, mssql_wsus.txt, README.snmp
- troubleshooting tips: troubleshooting.txt, troubleshooting_freeradius.txt
- Switch tips: cisco_switch.txt, sw_config_catos.txt, sw_config_ios.txt, sw_802.1x_tests.txt

Presentation structure

1. NAC Overview
2. Windows GUI: Overview & Edit Tabs
3. Windows GUI: Server Log, Change Log, Switch, Ports
4. Windows GUI:
5. Email Alerts
6. Questions

Thank you for your attention, questions?

Appendix: Optional slides - Web interfaces

- The web interface is not yet as rich as the primary windows interface, and hence it is not the focus of this training.
- Some screen shots are provided however.

Web interface

Web: edit mode

FreeNAC @MyCompany

List Unknowns | Search

Name	MAC	Status	Vlan	Last Vlan	Username	Port	Last Seen	Switch	Last IP
arselaugh	0050.8b75.a625	Active	iadsl	iadsl	HUGPAT	2/10	2006-04-12 09:50:48	c0103	
battlechain	0008.744c.025f	Active	s230	s230	MARSHE	2/28	2006-09-04 15:03:10	c0503	10.0.230.145
battlecraze	0014.22f8.a5b5	Active	s225		CLIPER	2/36	2007-03-15 12:04:04	c0203	10.0.225.113
battlelurker	0011.432a.7d3b	Active			BENBOU	Fa0/29	2006-12-02 13:11:06	c0103	10.0.225.160
bigfilth	0015.c541							c0503	10.0.230.168

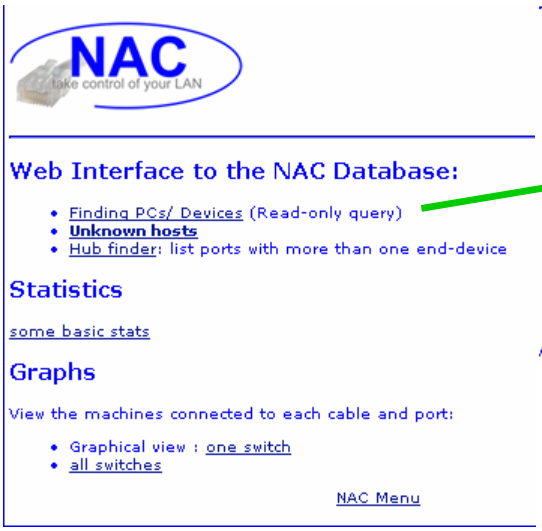
Submit Clear

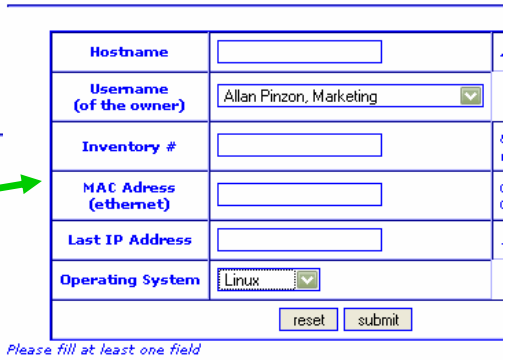
List Unknowns | Search

Name:	bonefire
MAC:	000d.60b0.0cb6 (IBM)
Status:	active
VLAN:	s230
LastVLAN:	s230
User:	Louisa Keown
Office:	Floss Street - 5.20
Switch:	c0503 -- 2/25 -- 5.03
LastIP:	-- 0000-00-00 00:00:00
LastSeen:	2005-12-21 15:02:31
Comment:	

Submit

Web: read-only interface





Web: hub finder

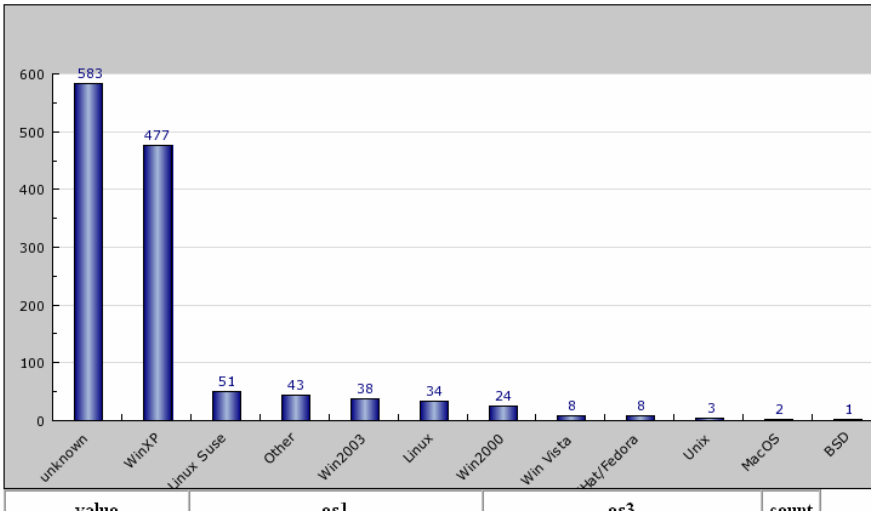
The following ports may have a hub, i.e. with more than one end-device see in the last days:

Switch IP ---- Port -- Location -- PC Name (User name)

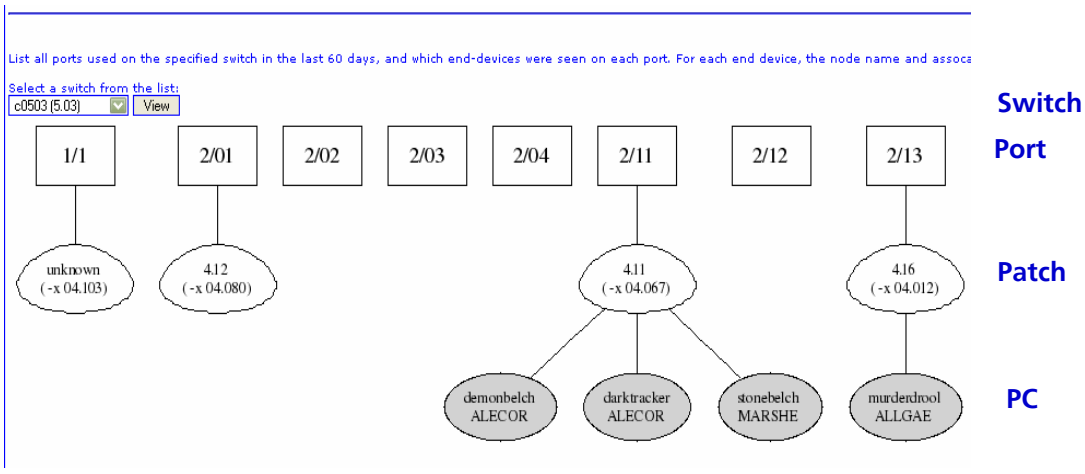
	2/47	Floss Street 5.03	metalhacker (Tyrone Beutler, Finance) filthscream (Tyrone Beutler, Finance) labwowgojo2 (Alejandra Corrado, Marketing)
	2/46	Floss Street 9.03	rotshred (Max Bise, Finance) labforbian4 (Max Bise, Finance)
	2/47	Floss Street 4.03	unknown (Marylou Sheley, Finance) ironburner (Marylou Sheley, Finance)
	2/40	Floss Street 4.03	holestomach (Allan Jenner, HR) labwow-winxpsp2 (Karina Provenza, Development)

Web: statistics

Group by : class - os - switch - vlan - dat -
Graph : pie - bar -



Web: Graphic view of one switch



NOTES:

A Web GUI that maps switch port usage in the last 24 hours.

We see one device on port 2/21, it is connected via cable X05.007 to room 5.15, where the PC inossmkima9 is attached and this PC is assigned to the Use 'TGDKIMA9'

We also see a printer on port 2/24