Patching Windows 2000 Clients With Wake ON LAN

Don Payne
GSEC v1.4c
22/09/2004

Index:

1 Abstract:

Business today demands that IT administrators enforce best practice principles to ensure the integrity, availability and confidentiality of corporate information is protected at all times. All operating systems are vulnerable in some way to data leakage or compromise and manufacturers of these systems are constantly required to provide 'Patches' to alleviate these risks as they become known.

Applying these patches of Workstations is one of the most time, labour intensive and difficult processes facing Security Administrators in a Client / Server architecture today. Network resources are at a premium and Core Business systems are given precedence by management, especially in networks where the available bandwidth is not sufficient to enable core systems and administrative tasks to run concurrently. This means that system patching needs to be performed manually or after business hours, which creates a bevy of problems for those responsible for patching clients. This poses the question of how do we ensure that patches can be scheduled for automatic installation overnight and ensure that all network clients are available to receive these updates.

2 Outline:

The answer to this question is Wake on LAN.

Within this paper I will demonstrate a method of ensuring patches automatically submitted to clients are received and installed by as many clients as possible. Many papers have been written on Patch Management so I intend to demonstrate how utilising Wake on LAN can assist Administrators in this task.

Patch Management is one of the most important aspects of Defence in Depth when securing Network clients. It is also a requirement of the ISO17799 standard (Section 10 Compliance with Legal Requirements) and the Health Insurance Portability and Accountability Act (HIPPA) that systems are maintained and updated to ensure the security of data communication.

Other considerations are how do administrators know the current status of systems in relation to their patch level. There are a number of tools such as HFNetcheckPro, GFI Languard and CIS Windows NT/2000 Security Scoring Tool all of which are based on the HFNetcheck.xml file. These tools can be run on individual clients to assess the current patch level of systems and will also provide details of available patches which have not yet been installed. Another requirement is to establish an organisational Standard Operating Environment (SOE) which is imaged onto all current clients and new clients (plus delivered patches) as they are installed so that all clients are at the same patch level before attempting to introduce a patch management system.

Failure to patch client Operating Systems or maintain current Virus Definition files can leave a Network vulnerable regardless of how secure your server environment may be. With the priority for management being Core Business systems the Security

Administrator is left with two options for performing this task, manually which can guarantee all systems are patched or automated, which requires all systems be at a state of readiness to receive patches.

Unfortunately performing multiple system patches manually is nigh on impossible in many distributed networks and even in closed LAN's and Workgroups can be very labour intensive with a high labour cost to the organisation. Manual patching is an almost never ending task in large networks where by the time all clients have been patched with one update another is released by the vendor and the process needs to be repeated.

Automated patching on the other hand gives Security Administrators the opportunity to 'hit' all clients in one go where a scripted update from a product such as Microsoft SUS® is released at a specified time and broadcast across the Network to all clients and the patch/patches installed. While this sounds like an effective and cost efficient way of patching clients, we run into trouble using this method as well.

Automated patching is not an issue for administrators if patches are pushed and installed during business hours. However users become frustrated when they are constantly interrupted by requests to reboot their systems while in the middle of important tasks or even the odd occasion where their systems automatically reboot and they lose important work. This is why the ability to patch systems when they are not being used is such an attractive proposition.

How do we ensure all clients are on line and ready to receive updates? We can have an organisational policy stating that Workstations are to be 'logged off' or 'Shut Down and Restarted' each night but we are now at the mercy of our user community. Of course many clients will be powered down each night and for that reason automated patching may not be an effective medium.

There is a solution to this however, it is called "Wake on LAN'. While many see this as a potential security risk, in a properly configured Network it can be a powerful administrative tool. Wake on LAN is a method of booting clients from an off state by sending specially crafted packets to the Network Interface Card of all clients on the LAN/WAN which will in turn send a signal to the BIOS of the Workstations on which they are installed instructing it to boot.

It must be noted that the theory and practical implementation of Wake on LAN can be introduced over all platforms, however the focus of this document will be Windows 2000.

3 Wake on LAN:

As stated above one method of dealing with this problem especially on distributed networks is Wake on LAN (WOL).

Wake on LAN is a technology created by the unison of IBM and Intel (Advanced Manageability Alliance) although AMD also lay claim to having been responsible for the development through the implementation of their 'Magic Packet™' technology. It is a system where special data packets are broadcast across the network with the sole intention of waking computers that are Advanced Configuration Power Interface (ACPI) compliant from an off or standby state.

4 Magic Packets:

These packets referred to as 'Magic Packets™' (MP) are a technology encompassing a complete system solution created by an alliance of AMD and Hewlett Packard as a method of triggering a system wake up from a suspend state. The packets must be structured to meet the requirements of the relevant network topology (Ethernet or Token Ring), contain a source address, destination address and a cyclic redundancy check (CRC). The payload or data frame contained in the packet consists solely of a synchronisation sequence, which consists of 6bytes of FFh (6*0xFF) and 16 repetitions (96bytes) of the target devices Ethernet Address.

There are no other restrictions that apply to 'Magic Packets™' and as a result the frame can be included in a UDP, TCP/IP or even an IPX packet.

These packets will be received by every node on the source and target subnets but will be discarded by every LAN controller which does not recognise the destination Ethernet address. The target systems LAN Controller will accept the packet extract the data frame and then send a signal to alert the PC's Power Management Circuitry to commence booting the system. This signal is transmitted either through the system bus (PCI2.2) or by a special 2 or 3 pin Control Cable (on older PCI2.1 systems) between the LAN Controller and the Motherboard specifically for the purpose of initiating WOL sequences.

A sample 'Magic Packet™' from a system with the Ethernet Address of 01:AB:23:CD:45:EF to a target system with an Ethernet Address of 98:76:54:32:10:12 (assuming an Ethernet topology) would be structured as follows:

```
  Destination Address          Source Address
9876543210201AB23CD45EFMisc.FFFFFFFFFFFFF87654321012987654321012
98765432101298765432101298765432101298765432101298765432101298765 43
21012987654321012987654321012987654321012987654321012987654321012 98
76543210129876543210129876543210 12 Misc. CRC
```

For Wake on LAN to be employed it is essential that the systems to be implemented contain a motherboard that supports the OnNow power management technology for networked PC's incorporating a standby power supply and BIOS. Also required are Ethernet Controllers that support Wake on Lan and appropriate Network Management Software (Operating Systems).

5 Wake on LAN Hardware Requirements:

5.1 Ethernet Controllers

The basic feature set required to enable 'Magic Packet™' technology is:

- **Magic Packet™ Enable**
- **Magic Packet™ Frame Detection**
- **Magic Packet™ Disable**

Magic Packet™ Enable is the state into which an Ethernet controller must be placed when a PC is shutdown or goes into a Standby state. This can be done in either hardware where the Sleep# pin is driven low or in software where the system BIOS which is constantly aware of the computers state sets a bit on the Ethernet controller. The software solution is the most common where the bit set by the system BIOS stops the controller from performing normal network functions and places it into a Magic Packet™ Frame Detection state. It is this process which makes it critical that PC's are shut down in an orderly manner and not by simply pushing the power button.

Magic Packet™ Frame Detection is the state where the controller passively scans all packets addressed to the node waiting for the specially crafted Magic Packet™ which tells the controller to instigate a system start.

Magic Packet™ Disable is the stage where the Ethernet controller is placed back into normal network mode. This may be as a result of the receipt of a Magic Packet™ or by user intervention such as pressing the power button or if in a standby state by pressing a keyboard key or moving the mouse. This function once again is performed by the system BIOS by removing the bit that was set on the Ethernet controller and allows the PC to now receive all data packets that are presented to the system.

There is a number of Wake on LAN compatible Ethernet cards manufactured by Intel and AMD.
Intel have produced 3 Generations of Wake on LAN card and all except for the PRO/100M Desktop Adapter (A80897-xxx) come with the standard 3pin WOL connector and connecting cable. Of the cards fitted with the onboard WOL port they do not necessarily require the cable to facilitate Wake on LAN if the Motherboard PCI2.2 compliant. The only Wake on LAN compatible card manufactured by Intel where the cable must be used is the:

- Intel® PRO/100+ Management Adapter
  Models:
  - 691334-xxx (not PCI2.2 compliant)
  - 701738-xxx (not PCI2.2 compliant)

Other available cards are the

- Intel® PRO/100+ Management Adapter
  Model:
  - 721383-xxx (PCI2.2 compliant)

- Intel® PRO/100 S Management Adapter
  Models:
  - 748566-xxx (PCI2.2 compliant)

  - 748564-xxx (PCI2.2 compliant)

All of the above mentioned cards are now obsolete and Intel has ceased manufacture of these, however they may be present in existing machines.

The current product specification for Wake on LAN Ethernet Controllers from Intel is:

- Intel® PRO/100 S Desktop Adapter
  Models:
  - 751767-xxx (PCI2.2 compliant)

- Intel® PRO/100 M Desktop Adapter
  Models:
  - A80897-xxx (PCI2.2 compliant)

    *This card is not equipped with a 3pin WOL cable and there fore cannot receive standby power from the bus of older PCI2.1 systems and therefore cannot be used to boot these systems from power off mode.

The PRO/100X series of desktop adapters require power to be supplied to them at all times when the PC is powered down to enable them to receive and process control packets. Wake on LAN enabled computers have standby power supplies which direct current to the Ethernet Controller whenever AC current is available.

The PRO/100 M Desktop adapter is a 3.3volt device which it receives through the system bus on PCI2.2 motherboards but has an inbuilt power regulator which also allows it to operate from a 5volt supply. The standby supply must be capable of supplying 0.2 amps for each installed adapter.

The PRO/100 S desktop adapter, PRO/100 M Management adapter and the PRO/100+ Management adapter are also 3.3volt devices but can receive their power either through the PCI bus (in PCI2.2 systems) or a 5 volt supply through the 3pin adapter cable (PCI2.1 systems) which is regulated by an inbuilt power regulator. The exceptions to this are the PRO/100+ Management adapters (691334-xxx, 707138-xxx) which is not PCI2.2 compliant and therefore can only receive the 5 volt supply through the adapter cable.

A 3 to 2 pin Wake on LAN adapter cable may be required to enable effective connection of WOL Ethernet controllers with some Legacy versions of IBM Wake on LAN systems.

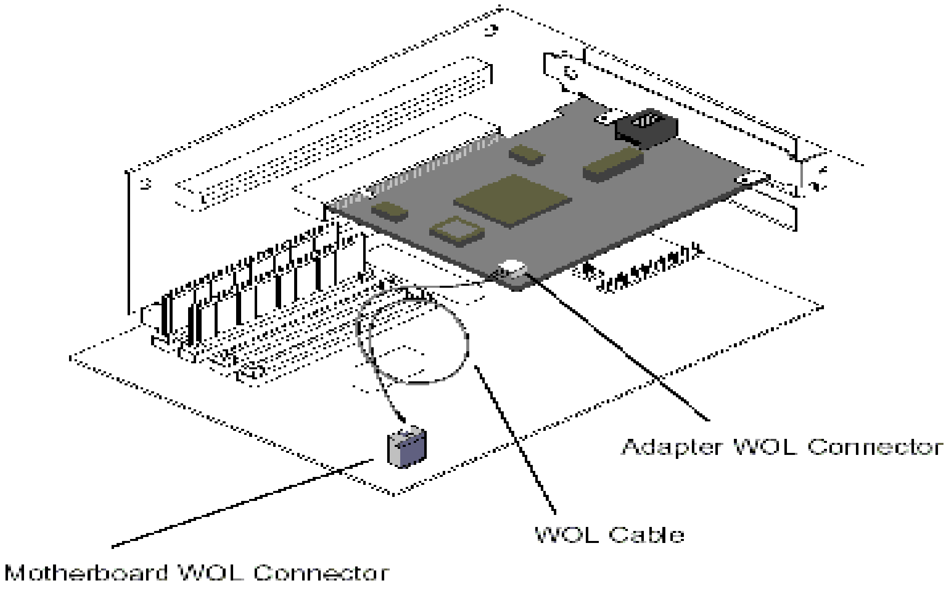


Figure 1. – Connecting the Wake on LAN adapter cable.*

AMD have produced the, PCnet – Fast + and PCnet – Fast III Ethernet controllers which all support ‘Magic Packet™’ technology and this is now a standard that will be built into all future AMD controllers.

- PCnet – Fast +
  Models:
  - Am79C972
- PCnet – Fast III
  Models:
  - Am79C973/Am79C975
  -

Both of these controllers are 3.3volt devices with built in 5volt tolerance.

* AMD.com, Magic Packet™ Technology, 07/04/2004, page 5
http://www.amd.com/us-en/ConnectivitySolutions/TechnicalResources/0,,50_2334_2481,00.html

5.2 Motherboards

All motherboards in production today that support the OnNow power initiative are Wake on LAN compliant. To enable Wake on LAN on these systems, they must be configured through the system BIOS to accept power on commands from the Ethernet controller. An example of how to do this follows:
On a Compaq EN PIII 1.0GHz Desktop system:

- Power on the system
- Before POST (Power on system test) commences press F10
- When prompted select the language required
- Select Security
- Network Service Boot – Enable
- Check Boot Order and ensure Ethernet Controller exists as follows:

- CDRom first
- Floppy second *
- Hard Drive third
- Ethernet Controller fourth **

- Select Save Changes and Exit
- Press F10

*If exists.
**Will always be last in boot order.

5.3 Routers

To enable ‘Magic Packets™’ to be broadcast across remote networks it is necessary to allow Directed Broadcasts to be passed by routers. The reason for this is that as the targeted PC’s should be powered off, the PC will have no IP address and will not respond to ARP requests from routers therefore only local subnet broadcasts packets which are directed to the target Ethernet address will be transmitted on the segment. Also with the continued prevalence of layer two switches on networks between routers and PC’s the switch is not aware of the port to which PC’s are physically connected and only a layer two broadcast packet will be transmitted out all switch ports.

To enable this the routers administrator must ensure the configuration line ‘no ip directed-broadcast’ is not present. This line will force routers to drop ‘Magic Packets’ whenever received and is now a default setting on Cisco routers to assist in defending against ‘Smurf’ attacks. While Defence in Depth dictates that this is best practice, the critical router in this scenario is the border or Internet facing router that controls the type of traffic allowed to enter your network from the Internet. If these routers are configured to not allow IP Directed Broadcast along with a properly configured firewall the likelihood of being victim to this type of attack is drastically reduced.

Alternately if removing the ‘no ip directed-broadcast’ is specified as a required configuration setting or the administrator is reluctant to remove this setting it is possible to configure Cisco routers to accept directed broadcasts from specific hosts. A sample configuration line could be:

```
ip forward-protocol <udp/tcp> <port#>
.......ip helper address x.x.x.x
```

*where x.x.x.x is the IP Address of the trusted host.
This is a very specific command line which is both router and interface specific.

6 Operating System Settings:

6.1 Windows 2000

To enable Wake on LAN on a Windows 2000 based client it is necessary to configure the Ethernet adapter inside the Windows system. To do this the following steps must be followed:

- Right mouse click on My Computer, select 'Properties' from the drop down window.

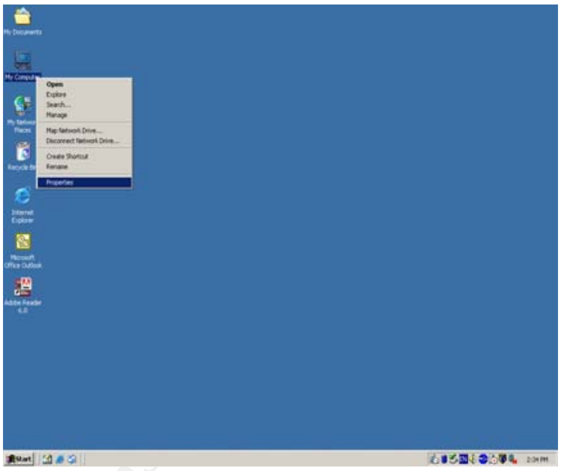
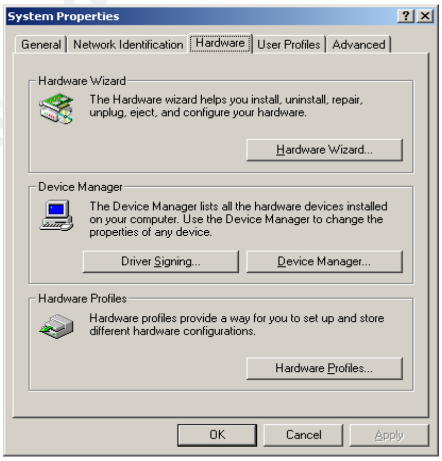


Figure 2 Selecting System Properties

- This will open a new Interface called System Properties
- Select the Hardware tab and then the 'Device Manager' button.



Hardware Wizard

The Hardware wizard helps you install, uninstall, repair, unplug, eject, and configure your hardware.

Device Manager

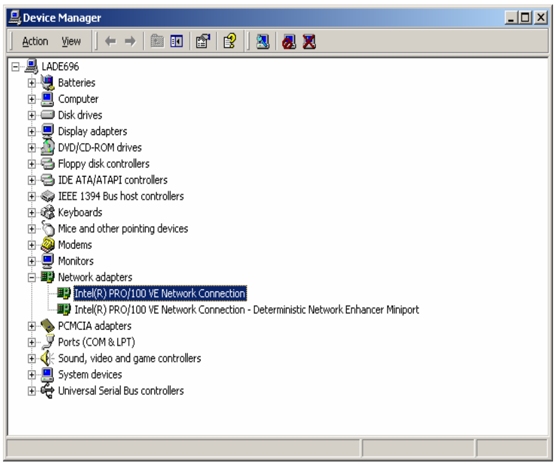
The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.

Hardware Profiles

Hardware profiles provide a way for you to set up and store different hardware configurations.

Figure 3 System Properties Window

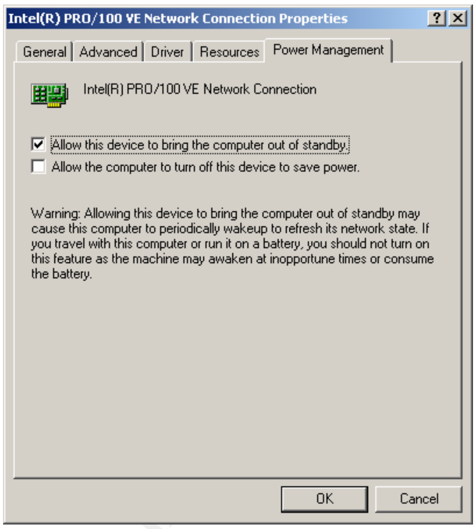
- This will then open a new window listing all of the hardware devices that are installed and are configurable by Windows.
- Select 'Network Adapters' and expand the list to show all available devices.



```
LADE696
  Batteries
  Computer
  Disk drives
  Display adapters
  DVD/CD-ROM drives
  Floppy disk controllers
  IDE ATA/ATAPI controllers
  IEEE 1394 Bus host controllers
  Keyboards
  Mice and other pointing devices
  Modems
  Monitors
  Network adapters
    Intel(R) PRO/100 VE Network Connection
    Intel(R) PRO/100 VE Network Connection - Deterministic Network Enhancer Miniport
  PCMCIA adapters
  Ports (COM & LPT)
  Sound, video and game controllers
  System devices
  Universal Serial Bus controllers
```

Figure 4 Hardware Device list

- Select the ‘Primary Network Adapter’ and right mouse click on it, select Properties from the drop down window, this will generate another screen where the Network adapter can be configured.
- Select the ‘Power Management’ tab and check the box to ‘Allow this device to bring the computer out of standby’.



Intel(R) PRO/100 VE Network Connection

☑ Allow this device to bring the computer out of standby.
□ Allow the computer to turn off this device to save power.

Warning: Allowing this device to bring the computer out of standby may cause this computer to periodically wakeup to refresh its network state. If you travel with this computer or run it on a battery, you should not turn on this feature as the machine may awaken at inopportune times or consume the battery.

Figure 5 Power Management screen

By following these steps and configuring the network adapter appropriately, the clients will respond to Wake on LAN requests from Standby and Hibernation states.

7 Software Management Systems:

7.1 Software Update Service

Software Update Service (SUS) is a component of Microsoft ’Strategic Technology Platform Protection’ which is designed for the management and distribution of Windows system patches and updates.

This system is based on the Windows update service where administrators configure a Virtual Update Server inside their own network to service requests from Windows 2000 servers and clients. SUS is best suited to an Active Directory environment although this is not a necessary requirement.

The use of SUS reduces the number of clients that require direct access to the Internet to receive critical patches and system updates to one and also reduces the risk of users installing patches that have not been thoroughly tested in the local environment. This ‘Virtual’ server which must have a minimum configuration of Windows 2000 Service Pack 2 and IIS 5.0 is configured as an administrator controlled content synchronisation service that downloads and stores updates from the Windows Update site on a schedule defined by local administrators. It is also possible to synchronise this server with the Windows Update site itself in order to download updates as they become available if local administrators do not want to define a schedule. This server then acts as an update server for all other clients on the network.

Once downloaded patches have been thoroughly tested on a group of ‘sacrificial’ machines (an indicative cross section of clients on your local network) to ensure that the patch causes no problems in your local environment the patch can be published to all local clients.

Updates are sent to clients using the Background Intelligent Transfer Service (BITS) which Microsoft claims ‘trickles’ the update using only idle bandwidth to preserve the network for core functions. For BITS to function in native Windows 2000 installations it is necessary to ensure that the Windows 2000 Service Pack 2 Automatic Updates installer has been installed. Once a client has received the update, it by default backs off for a random period of upto 23 hours before installation however it is also possible to schedule the installation time using Group Policy. This is where the ability of Wake on LAN to provide clients outside of core business hours can be utilised to ensure updates are successfully installed. SUS also provides for chained installations where multiple updates may be installed without the necessity to reboot (if required) until the last update is installed.

Although a scheduled install time outside of core business hours may have been set, this will only occur if the computer is left in a powered on state, if not the installation will occur at the first opportunity after the scheduled time. The client does not have to be actively logged on to the network but does need to be in a ready state. If clients are powered down overnight users may be required to reboot their computers minutes after logging in at the start of their day to enable the completion of an updates installation.

In Active Directory Network these update behaviours and schedules can be set in Group Policy. Performing configuration in this way (Administrative Policy) by using the default policy template Wuau.adm, which was provided with the SUS installation package or System.adm provided in Windows 2000 Service Pack 3 also disables the local user interface on all clients rendering these clients safe from 'fiddling' users.

In native Windows 2000 networks that do not run Active Directory it is necessary to update the registry to enable automatic updates. A sample registry key for a client system would resemble:

HKLM\Software\Policies\|Microsoft\Windows\Windows Update\AU
NoAutoUpdate=0 where 0 = enabled
AUOptions=4 where 4 = download updates and schedule installation
ScheduleInstallDay=3 where 3 = Tuesday
ScheduleInstallTime=2 where 2 = 2:00am
UseWUServer=1 where 1 = use the SUS server as specified in WUServer
WUServer=http://mynetworkSUS
WUStatusServer=http://mynetworkSUS

The WUServer and WUStatusServer keys determine the server responsible for providing the updates (WUServer) and the server that records the statistics relating to the status of updates of SUS clients (WUStatusServer). Internet addresses are used for these servers due to the fact that clients use the http protocol to communicate with the SUS server.

The above settings are the same as those that would be set automatically using a Group Policy Object in an Active Directory domain

All local system events related to SUS are written to the local Event Log. The following events are recorded:

- **Unable to connect**
  (cannot download and install updates – system will keep trying).
- **Install ready – No Recurring Schedule**
  (an administrator needs to log on locally to install updates)
- **Install ready – Recurring Schedule**
  (updates downloaded waiting for scheduled time to install)
- **Install Success**
- **Install Failure**
- **Restart Required – No Recurring Schedule**
  (requires restart to complete installation. No new updates can be downloaded or installed)
- **Restart Required –Recurring Schedule**
  (will be restarted within 5 minutes. No new updates can be downloaded or installed)

These events can also be extracted from the local event log and collected and analysed be other monitoring tools to provide detailed reporting on the status of clients.

7.2 Systems Management Server

Microsoft has developed a complete systems management solution to help administrators with maintenance of their Windows based operating systems.

Systems Management Server (SMS) has the scalability to provide change and configuration management regardless of the size of the network to which it is applied, whether it be a small closed workgroup or a WAN spanning the globe.

SMS can be utilised to provide system updates/patches or even complete programs to client machines that have had the SMS client agent installed. It also provides a network discovery agent which can be used to identify all client computers and servers on your network. The data obtained as a result of the discovery scan is then stored in a local database on the Primary Site Server (PSS) on the relevant SMS site or subnet. This data is also used to perform software inventory scans of all identified clients, utilising the built in Software Inventor Tool.

The SMS structure defines a Central Site Server (CSS) which acts as a master for all Primary Site Servers that may be located throughout a network structure. The Central Site Server maintains a complete database recording all the data from the various Primary Site Servers beneath it in the structure and can be used to perform maintenance tasks across the entire network if required. The Primary Site Server will be installed on designated master sites throughout a network to enable management of all network clients. These Primary Site Servers have an administration console to enable the deployment of packages to local clients targeted for system updates and as mentioned above maintain a database of the status and existence of clients. There may also be a number Secondary Site Servers (SSS) configured and located on various sites throughout the network, a Secondary Site Server can only exist as a 'child' of a existing Primary Site Server. These Secondary Site Servers have no administration capability and may be installed on remote subnets or sites where no administrator is present. Essentially the Secondary Site Servers act as a repeater for instructions sent by the Primary Site Server (or parent) directly above it in the SMS hierarchy.

Patches or updates are distributed to clients by creating SMS packages, which are then 'advertised' to clients. The clients then connect to a determined Client Access Point (CAP) that then in turn directs to the appropriate point to access the system package.

The SMS packages are created in the SMS administrator console either on the Primary Site Server for specific subnet targeted broadcasts or they can be created on the Central Site Server for enterprise wide deployment rather than duplicating the package at each site. The packages may contain the source file of the patch and any associated command lines that may be necessary to execute an unattended installation of the file. In cases where the program does not have associated unattended installation option, administrators can utilise the SMS installer to create an unattended installation file. The package may also indicate an alternate point from which the program source file must be accessed for installation, this alternate point is known as a Distribution Point (DP).

Other methods of creating packages are also available such as the Distribute Software Wizard or by the creation of package definition files and using the Create Package from Definition File Wizard. A definition file is a precompiled list of command line switches and program source files created to automatically install the desired program.

Once a package has been created it must be published to a distribution point from which the targeted clients are directed to retrieve them. This task can be completed by using the manage distribution Points Wizard.

Once packages have been published, clients are advised of the available package by 'Advertisements' that are directed to the target clients. These advertisements that can also be scheduled for activation at specific times alert the client to the availability of a package and the address of the CAP that contains the package detail.

The advertisements define whether the package will be installed silently on a predetermined schedule or if user intervention is required. The SMS Client Agent manages packages that are installed in silent mode and the advertisements are referred to as 'Assigned Advertisements'.

If packages which have previously been published require updating or change it is possible to do this during the life of the scheduled advertisement, however clients which have already connected and installed the original package will not receive the updated package.

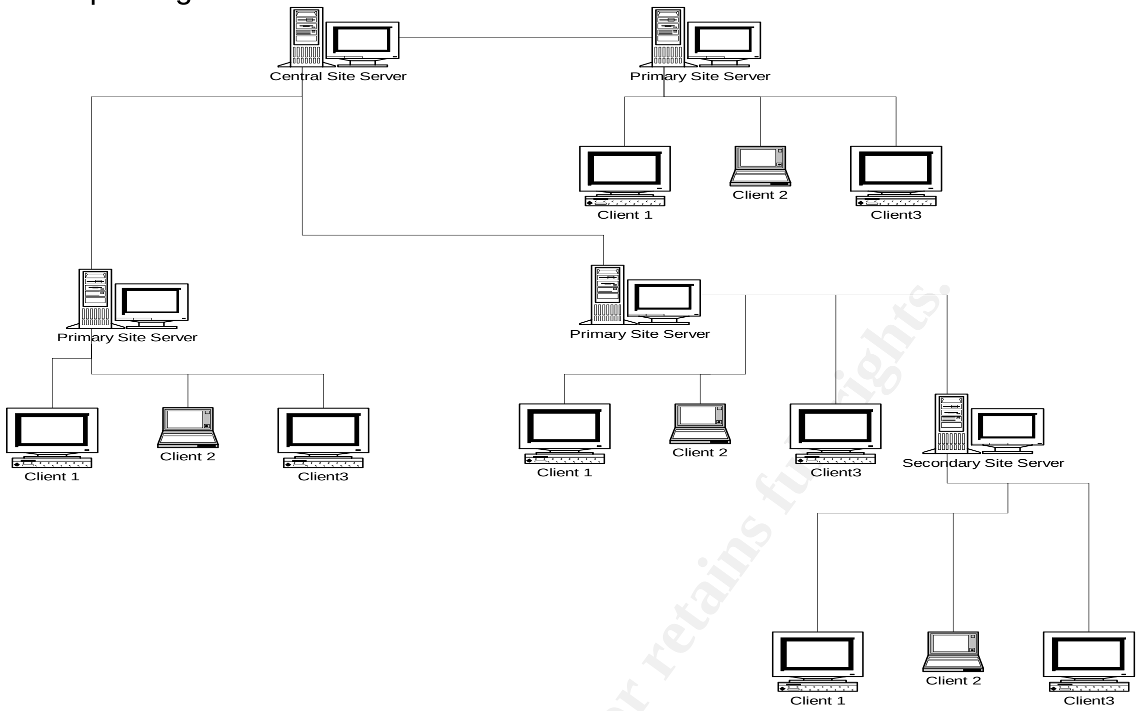


Figure 6: A sample SMS Site Configuration

8 Wake on LAN Solutions:

8.1 Combining WOL and POL with SUS

This is a technical solution developed by Ed Van Balen of the Netherlands. It incorporates the following technologies as quoted by Ed Van Balen:

- **Windows 2000 Active Directory Domain**
- **Software Update Service SP-1**
- **PowerOff**
- **PsShutdown**
- **Kixtart**

This method of remotely waking clients can only be implemented in native Windows 2000 networks utilising Active Directory.

Power Off is a freeware tool created by Jorgen Bosman that can be used to control the power state of all Windows based computers. It is possible to use this system either with a GUI that enables commands to be sent only to one computer at a time, or via a Command Line interface that enables the scripting of commands to multiple computers at one time.

PS Shutdown is another freeware tool that can be used for shutting down clients using PowerOff on LAN. It does not require any additional software or hardware other than that which is already in place to enable Wake on LAN to be installed on clients and was created by SysInternals.

Kixtart is a careware program for use with most operating systems, it provides both a language and scripting engine which is mainly used for Logon scripts with Windows systems. For the purpose of enabling the Wake on LAN with Kixtart there are four individual scripts required.

As detailed earlier in the SUS review, Group Policy can be used to define the download and installation process and schedule for Windows updates. To facilitate this at least one Organisational Unit (OU) must be created containing all the computers that are to retrieve updates via SUS. This Organisational Unit will then have the Group Policy applied to it, which will automatically apply all the settings to the registry mirroring those that we demonstrated earlier in the manual registry configuration.

To enable the Wake on LAN function on clients in the Organisational Unit/s, a number of files need to be appended to the appropriate Netlogon share, as quoted by Ed van Balen they are:

- **Kix32.exe** **-** (the Kixtart Engine**)**
- **PowerOff.exe** **-** (the PowerOff executable)
- **PS Shutdown.exe** **-** (the PS Shutdown executable)
- **Status.kix**** **-** (Kixtart script to check the SUS status of clients and set the Wake on LAN trigger at system shutdown*)
- **NoWol.kix**** **-** (Kixtart script to reset the Wake on LAN trigger on clients at start-up)
- **Wol.kix**** **-** (Kixtart script to start required clients and set the PowerOff on LAN trigger)
- **Pol.kix**** **-** (Kixtart script to power off the required clients using PowerOff on LAN)

* Client computers must be powered down correctly using the Windows Shut Down command. If clients are switched off using the power switch Status.kix will run and no record of the client will be found in the required initialisation file. This will result in clients not receiving Wake on LAN commands and updates installing after user logon.

** Fully functional samples of these files are available online at http://www.xs4all.nl/~equator/suswol/

As well as the above scripts in Netlogon it is necessary to append the Status.kix and Wake on LAN.kix files to the Organisational Unit for SUS clients.

Status.kix is applied as a shutdown script which checks the Active Update status of a client at shutdown and if a scheduled install is pending an initialisation file (WOL.ini) is created in the first instance or updated by subsequent clients with the clients IP Address in a designated share (WOL$). A log file that is located in the shared folder is also appended to maintain a record of all clients that have been successfully updated.

The NoWOL.kix file is applied as a start-up script that will remove any entry in the WOL.ini file for the source computer as soon as it is started. These two files NoWOL.kix and status.kix) work together to ensure that only clients with scheduled installations and in a powered off state are targeted for Wake on LAN.

To trigger the Wake on LAN process a scheduled task must be created on the domain controller. This task which executes the WOL.kix script should be scheduled to run 5 minutes before clients are scheduled to start the installation of updates. The WOL.kix script uses the information in the WOL.ini file created as described above to start the listed computers using the 'PowerOff Wake on LAN function. All clients that are started using this script also are appended to another file (POL.ini) in the WOL share to enable automatic shutdown if this process is required.

The shutdown process is the same as that for start-up where a scheduled task is created which leverages PS Shutdown using POL.kix and the information in the POL.ini file to shutdown clients. This task can be scheduled to run at any time after WOL.kix and will only send shutdown commands to clients which were started using WOL.kix to protect systems which may have been left on deliberately.

8.2 SMSWakeUp

SMSWakeUp is a system designed by 1E Ltd. to fully integrate with Microsoft Systems Management Server (SMS). It provides a method of delivering system updates to 100% of targeted clients twenty-four hours a day, seven days a week. It is fully compatible with SMS v2.0 (Service Pack 4) or Windows 2003 with the Hardware Inventory client and Advertised Programs client agents enabled. All target machines must be registered in the SMS client database and also support Wake on LAN by way of compatible Ethernet Controller, BIOS settings and be APM or ACPI compliant. SMSWakeUp works with bridged networks (where packets are forwarded to all bridge ports) and with routed networks using one of 3 available set up options:

- **Master Mode**
- **Dedicated Slave**
- **Multi Slave**

SMSWakeUp utilises subnet directed broadcasts to send 'Magic Packets to target clients therefore if routers on your network do not allow IP directed broadcasts, SMSWakeUp must be implemented in either dedicated or Multi Slave mode.

SMSWakeUp must be installed on all SMS Primary Site Servers on your network. It uses the information stored in the SMS database on these systems such as the Mandatory Advertisement Schedule and System Inventory to establish when and where to send out wake up frames. This can be controlled either by individual site servers or centrally from the Central Site Server.

In master Mode the SMSWakeUp Master Service should be installed on the SMS host in all subnets containing Wake on LAN enabled clients. These hosts designated as Primary Site Servers will be responsible for sending wake up frames to all clients on their own subnet. Once installed the Master Service will interrogate the local SMS database to determine a list of all clients connected to the host segment so that the only clients targeted with these wake up packets are local clients or those on non-primary sub-sites.

In Master Mode SMSWakeUp will send out a wake up frame to all clients that are scheduled to receive an update 15 minutes before the scheduled advertisement to ensure the client is available and ready to receive the update.

As part of the default Master Service installation process, the SMSWakeUp Slave Service is also installed to enable communication between remote slave clients and the host.

The SMSWakeUp Designated Slave service must be installed on a designated host on remote subnets. This host which must be always on receives instructions from the Master Service on a different subnet. Once an instruction sequence is received the Dedicated Slave then sends Wake-up packets to the required clients on the local subnet as directed by the Master Service. Using this method resolves the issue relating to the forwarding of IP Directed Broadcasts through routers.

The Multi Slave Mode works in much the same way as Designated Slave however there is no need for a dedicated host. In this mode the Slave service must be installed on all clients in the remote subnet and the remote Master Service will attempt to communicate with clients in order of the last successful connection backwards until an available host is found. Once an available host has been found this will then be used to send wake-up frames to all targeted clients on the subnet.

The Master Service collates all statistics in relation to the SMSWakeUp service by collecting data directly from clients or receiving data from the controlling Slave Service on remote subnets. This enables reporting and reconciliation of clients receiving targeted updates.

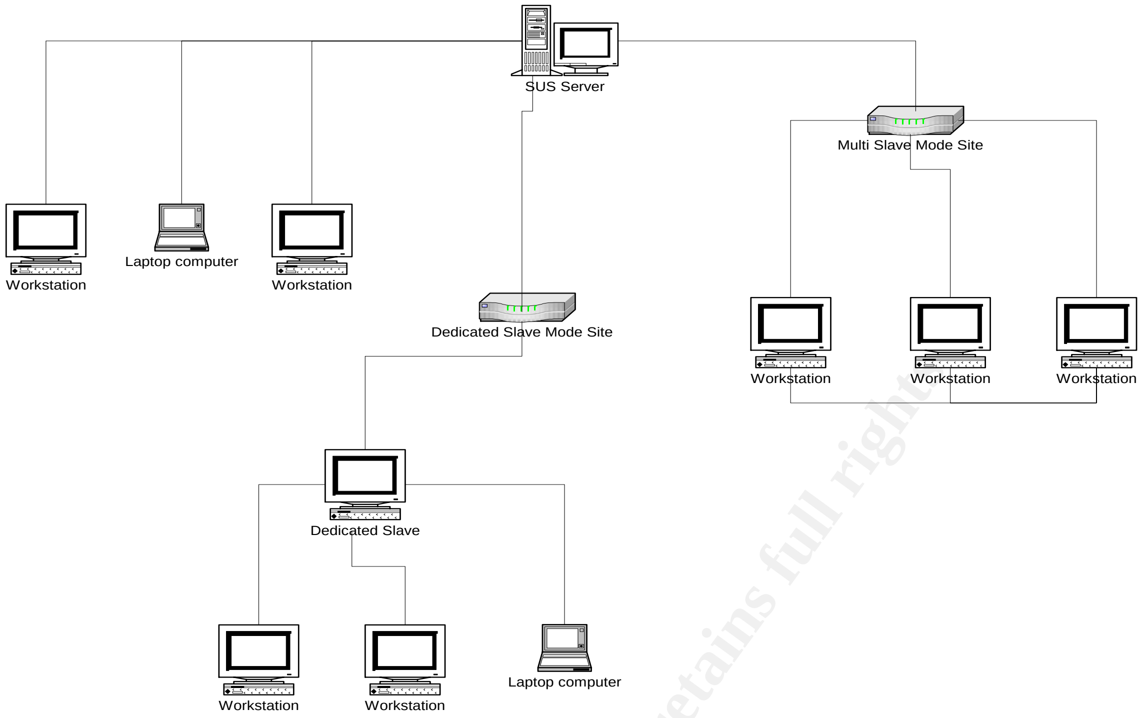


Figure 7: A sample SMSWakeUp configuration

9 Conclusion:

We have investigated and shown that it is possible to implement an effective patch management system that is not reliant on users following Organisational Policy and ensuring that clients are left powered on overnight to ensure availability for system maintenance purposes. We have also proven that these same systems can remove the burden placed on administrators and support officers in the deployment of patches in a timely manner.

With a fully implemented Wake on LAN system, administrators can be assured that patches that have been submitted to clients are received and installed on schedules that are determined by the administrators. By performing these installations during periods of network inactivity there is no conflict with Core business systems, users experience no added aggravation by being forced to reboot systems unexpectedly to finalise the installation of software which they know nothing about and available bandwidth is utilised effectively during periods of 'Slack' time. This also provides a dual monetary benefit to management in that additional bandwidth capacity does not need to be purchased to facilitate administrative tasks and that the available bandwidth is utilised more effectively over a 24 hour period than just over core business hours.

The two systems that have been examined are both fully compatible with the prime Microsoft ® systems management packages and therefore are the ideal solution in a native Windows ® domain. SMSWakeUp is a fully tested and functional system designed to be used with Microsoft Systems Management Server 2.0 and 2003 that can be implemented easily utilising existing hardware. The ability to manage this system centrally also reduces any requirement for domain administrators across the WAN to synchronise system updates manually and duplicate processes at each site.

By implementing Microsofts Systems Update Service and combining this with the Wake on LAN scripts and other freeware packages as described by Ed van Balen, administrators can also perform the patching process outside of normal business hours, however this system is not effective as a centrally managed process on a distributed WAN. As the process requires scripts to be run on each client at both startup and shutdown it is necessary to perform the management of this process at each separate domain within the WAN. This leads to local administrators being responsible for the coordination and updating of all system patches for their site.

Based on all of the factors that need to be considered the solution that is the best fit for the problem of scheduled patch management is SMSWakeUp and SMS which provides the additional abilities of installing complete Microsoft software packages and other system management tools. In addition the reporting and inventory components of SMS enable administrators to be much more secure in the knowledge that they know what state their systems are in.

10

Acknowledgments:

The following web sites were used for research and reference in this paper:

1. Oliveira, Jose, Wake on LAN mini HOWTO, v0.14, 23/04/2002
http://gsd.di.uminho.pt/jpo/software/wakeonlan/mini-howto/ 06/08/2004

2. Solarwinds.net, Wake on LAN Configuration,
http://support.solarwinds.net/Help/Wake-On-Lan/overview.htm 24/07/2004

3. Madge.com, Remote PC Wake-Up, 18/01/2002
http://www.madge.com/_assets/downloads/lsshelp8.0/LSSHelp/AdvFeat/WonLAN/WonLAN2.htm 24/07/2004

4. Bosmen, Jorgen, Poweroff 3.0
http://users.pandora.be/jbosman/poweroff/poweroff.htm 06/08/2004

5. Microsoft ® Corporation, NDIS New Features,
http://www.microsoft.com/windows2000/techinfo/reskit/en-us/cnet/cnad_arc_stvy.asp?frame=true 30/07/2004

6. 1e.com, 1E : Software products : SMSWakeUp : FAQ,
http://www.1e.com/SoftwareProducts/SMSWakeUp/FAQ.aspx 24/07/2004

7. Intel.com, Desktop Adapters - Wake on LAN* and System Compatibility, 12/02/2004
http://www.intel.com/support/network/adapter/pro100/sb/cs-008438.htm 28/07/2004 11/08/2004

8. van Balen, Ed, How to Combine WOL and POL with SUS, v3, 21/06/2004
http://www.xs4all.nl/~equator/suswol/ 30/07/2004

9. Microsoft Corporation, How to Enable WakeOnLAN Only for "Magic" Packet Pattern, v3.7.5.0, 10/08/2004
http://support.microsoft.com/default.aspx?scid=kb;EN-US;257277 11/08/2004

10. SecuriTeam.com, Magic packet™ generating script has been released (WakeUp on Lan, 01/05/2000
http://www.securiteam.com/securitynews/5XP031F0BM.html 11/08/2004

11. AMD.com, PCNet™ - PRO, 11/09/2004
http://www.amd.com/us-en/ConnectivitySolutions/ProductInformation/0,,50_2330_6629_2421,00.html 23/08/2004

12. AMD.com, Magic Packet™ Technology, 07/04/2004
http://www.amd.com/us-en/ConnectivitySolutions/TechnicalResources/0,,50_2334_2481,00.html 28/07/2004

13. AMD.com, AMD Connectivity Solutions - Networking - PCNet™ - FAST III, 11/09/2003
http://www.amd.com/us-en/ConnectivitySolutions/ProductInformation/0,,50_2330_6629_2425,00.html
23/08/2004

14. AMD.com, AMD Connectivity Solutions - Networking - PCNet™ - FAST+, 11/09/2003
http://www.amd.com/us-en/ConnectivitySolutions/ProductInformation/0,,50_2330_6629_2429,00.html
23/08/2004

15. Microsoft Corporation, Systems Management Server 2003 Operations Guide, 13/10/2003
http://www.microsoft.com/downloads/details.aspx?FamilyId=BD2B3619-4704-4C19-A00B-628E65F6F826&displaylang=en 21/08/2004

16. Microsoft Corporation, Software Update Services Overview, June 2002
http://download.microsoft.com/download/b/f/7/bf73ffa1-39ed-4cc1-b9eb-4c99154b31b4/SUSOverview.doc 14/08/2004

17. F, Landers, Wake on LAN, 10/07/2004
http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci214609,00.html
24/07/2004

18. Active Experts Software, Introduction to Wake-On-LAN
http://www.activexperts.com/activsocket/introduction-wake-on-lan 30/07/2004