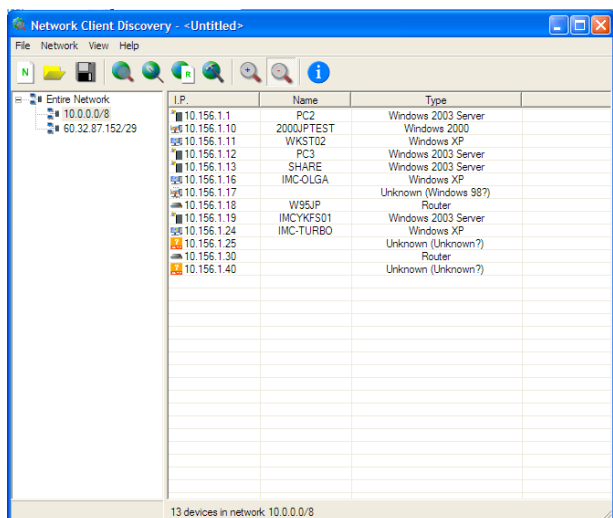


Nippon Security: Security Software suites

NCD V1.0

Main Window



The main window is made up of a menu, toolbar, network tree, network view and status bar.

Menu & Toolbar

Menu	Toolbar	Description
File		Clears all discovered networks and resets discovery options back to the default.
- New		
File		Presents a File Open dialog to the user and opens the previously discovered network selected including any customized options.
- Open		
File		Saves the current discovered network to a previously saved location or presents a File Save dialog to the user if the discovered network has not been previously saved.
- Save		
File		Always presents a File Save dialog to the user regardless of whether the discovered network has been previously saved or not.
- Save As		
Network		Presents the Discover dialog to the user (see Discover)
- Discover		
Network		Presents the Discover dialog to the user and starts discovering the local computer followed by neighboring devices and networks (See "Discover in neighboring networks" under Options)
- Auto-discover		
Network		Presents the Reports dialog to the user (see Reports)
- Reports		
Network		Presents the Options dialog to the user (see Options)
- Options		
		Changes the Network View to Large Icon view with large icons and text below.
		Changes the Network View to List view with small icons and text to the right.
Help		Presents the initial splash screen showing credits and copyright information. Clicking on the image returns control to the main window.
- About		

Network Tree

The Network Tree has two node levels. The top node, the only node in the first level, is called “Entire Network” and represents all devices and networks that have been discovered. The second level of nodes is a list of networks that is created from a combination of IP address and network mask for each device. Where there are conflicts between the network masks detected on devices, the ‘outer’ network is split to accommodate the ‘inner’ so that there are no overlaps. For example, if one device reports an address of 192.168.1.1/24 and another device reports an address of 192.168.1.152/25 the network tree will list 192.168.1.0/25 and 192.168.1.128/25.

Right-clicking a network will present a context menu with options to “Refresh” the selected network or “Delete” the selected network. If “Entire Network” is selected, only “Refresh” is presented. Selecting “Refresh” will present the Discover dialog and will start searching for devices at all possible IPs within the selected network. If “Entire Network” is selected, all possible IPs within all detected networks will be searched. Selecting “Delete” will remove all devices in the selected network and then recreate the list of networks. If a device has multiple IP addresses that are in different networks the device is not removed and must be deleted manually.

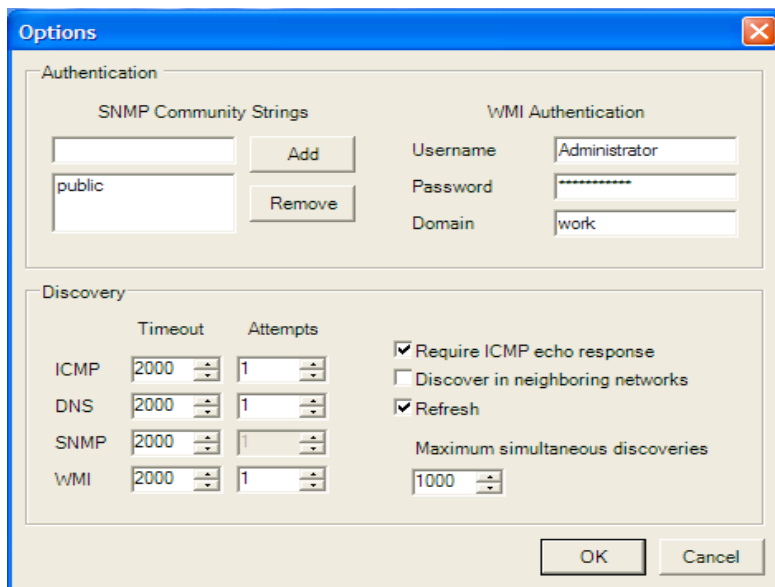
Network View

The content of the Network View depends on which node is selected in the Network Tree. If “Entire Network” is selected, the set of second level nodes from the Network Tree, the detected networks, are presented in icon form. Right-clicking an icon will present a context menu with the same options as the Network Tree. However, several networks can be operated on at the same time from the Network View by using multiple selections. Double-clicking a network has the same effect as selecting a network from the Network Tree.

If a network is selected in the Network Tree, the Network View shows all devices with IPs in that network. Each device has an icon based on its type (see Appendix A) and is listed by IP address (in the selected network) followed by the type of device. If the device type is unknown, the device’s ‘fingerprint’ is listed in brackets followed by a question mark. Right-clicking multiple devices will present a context menu with the options “Refresh” and “Delete” with the same effect as defined earlier. When removing a device, it will be removed from all networks. Right-clicking a single device will present a context menu with an additional option “Properties”. Selecting this will open the Properties dialog for the selected device (see Properties). Double-clicking a device will also open the Properties dialog.

Status Bar

The status bar has a progress bar at the left and text and the right. If “Entire Network” is selected in the Network Tree, the text displays the total number of discovered devices and networks. If a network is selected, the text shows the number of devices discovered in that network. During open and save operations, the progress bar and text display progress information graphically and numerically.



Options dialog
Allows configurations of the parameters of discovery

Authentication

“SNMP Community Strings” are used when attempting to identify each device during discovery. To add a community string, type it in to the text box to the left of the “Add” button and then click “Add”. To remove one or more community strings, make a selection in the list to the left of the “Remove” button and then click “Remove”. Either read-only strings or read-write strings are usable. No write access is attempted using the community strings provided. Any number of strings may be added.

“WMI Authentication” information is also used when attempting to identify each device during discovery. For authentication to be successful the user details entered must have either Domain Admin rights or Administrator rights on any computer identified. If the “WMI Authentication” fields are left blank, the rights of the current user will be used.

Timeout & Attempts

The “Timeout” fields are all in milliseconds. For ICMP and DNS, the minimum value is 100ms and the maximum value is 10000ms. For SNMP and WMI, the minimum value is 1000ms but the maximum values differ; SNMP’s maximum timeout is 30000ms and WMI’s maximum timeout is 40000ms. WMI’s timeout value applies only to the initial connection and not to subsequent reads of data.

The “Attempts” fields all have a minimum of 0 and maximum of 10. Setting a field to 0 will disable that protocol from being attempted. The number of attempts applies to each use of the protocol. However, if the first use fails after the specified number of attempts, the protocol will no longer be attempted. For SNMP, the number of attempts applies to each community string provided.

Other Options

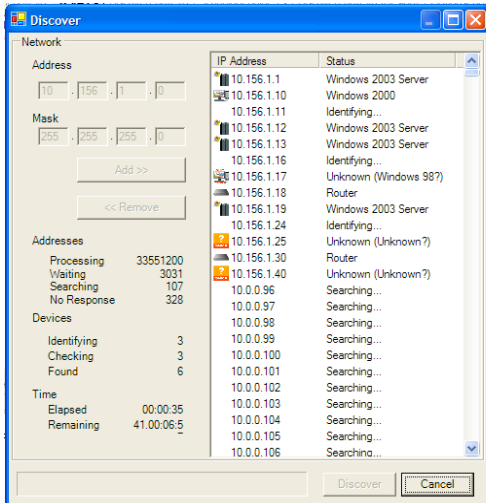
“Require ICMP echo response” indicates that no further identification should be attempted if no reply is received to an ICMP echo request. This is useful where ICMP is firewalled on part or the entire network. However, total discovery time significantly increases with this option.

“Discover in neighboring networks” is the heart of “Auto-discover” although it is enabled by default for regular discoveries as well. If this option is disabled, an “Auto-discover” will still run as if this option was enabled. With this option, each network that a device is attached to will also be scanned. If the device reports an incorrect network mask or a network mask can not be identified, a class A, B or C mask based on the IP address and Internet standards will be used. With this option, a trace route will also be performed and all devices and networks in between will be scanned according to the same rules.

“Refresh devices during discovery” will cause any devices that have been previously discovered to be fully discovered again. This is useful when devices that couldn’t be identified before have been reconfigured to allow access or new authentication information has been entered. Without this option, devices that have been previously identified will be skipped during discovery or refreshing of a network. This option is off by default because it causes devices with multiple IP addresses to be discovered once for each IP address in the networks to be discovered.

“Maximum simultaneous discoveries” specifies the combined maximum number of devices that can be simultaneously in the “Searching...” and “Identifying...” states. The minimum value is 1 and the maximum value is 1000. This option should be set to lower values on machines with low memory or on networks with low bandwidth. Note that the maximum set here may never be reached as device searches are only begun when there are free CPU resources.

Discover Dialog



The Discover Dialog is made up of network entry fields, control buttons, a device listing and status information.

Network Entry Fields

Networks are entered by specifying the network address in the four text fields below “Address” and entering the network mask in the four text fields below “Mask”. In any of the eight text fields, only numbers less than 256 can be entered and entering a “.” or pressing the TAB key will move to the next field. While entering the network address, the network mask will automatically adjust to the largest possible mask that is valid for the entered network address.

Pressing the “Add” button will add all IPs in the network entered to the Device Listing. The IPs are checked to ensure there are no duplicates within the device listing. The “Remove” will remove any IPs selected in the Device Listing. During both the add operation and the remove operation, the progress bar at the bottom of the dialog will show the progress. This is necessary when adding large network ranges such as a class B network.

Control Buttons

The “Discover” button will disable all text fields and buttons except the “Cancel” button and then begin to discover all the IPs in the Device Listing. If the Device Listing is empty and there is a valid network entered into the Network Entry fields, that network will first be added to the device listing. Otherwise the user will be notified that there are no devices to discover.

The “Cancel” button will stop all searches in progress and exit the dialog. Any devices already identified when the cancel button is pressed will be added to the discovered network. Cancellation may take a short time to complete on computers with low resources.

Device Listing

When a network is added, all IPs in that network are added to the Device Listing. When discovery is started, each device will go through several phases that can be seen from the change in the status field. The first status is “Searching...” which signifies that contact is being attempted with the device. If no contact can be made per the user’s selected options, the IP is removed from the device listing.

The status changes to “Identifying...” once contact has been made. During this stage, each management protocol is attempted and as much information is extracted as possible. If no information can be extracted and the device responds to ICMP, a ‘fingerprint’ will be taken to determine the characteristics of the device’s IP implementation, which is then matched against an operating system. Once a device has been fully identified, its status will change to “Checking connections...” and neighboring networks will be added to the device list if the option has been enabled. Finally, a device’s status will change to the type of device detected and a corresponding icon will be shown using the same format as is described in the Network View of the Main Window.

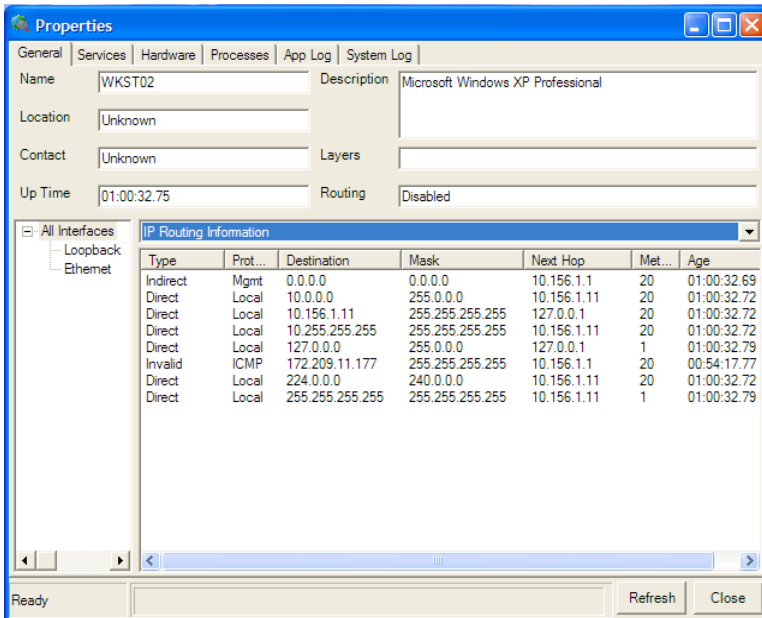
Status Information

The Status Information is divided into three sections. The “Addresses” section shows statistics on the number of IPs at which devices have not been found. “Remaining” shows the number of IPs for which discovery has not yet been started. “Searching” shows the number of IPs that are currently being checked for contactability. “Not Found” shows the number of IPs that have not responded within the specified timeouts.

The “Devices” section shows statistics on the number of IPs at which devices have been found. “Identifying” shows the number of devices from which information is currently being gathered. “Found” shows the number of devices for which

identification has been completed.

The “Time” section shows the time elapsed since discovery started and an estimation on the amount of time required for all devices to be discovered. The estimated time remaining is inevitably wrong toward the very end of a discovery as the time required for the last devices to be identified cannot be ascertained.



Properties Dialog

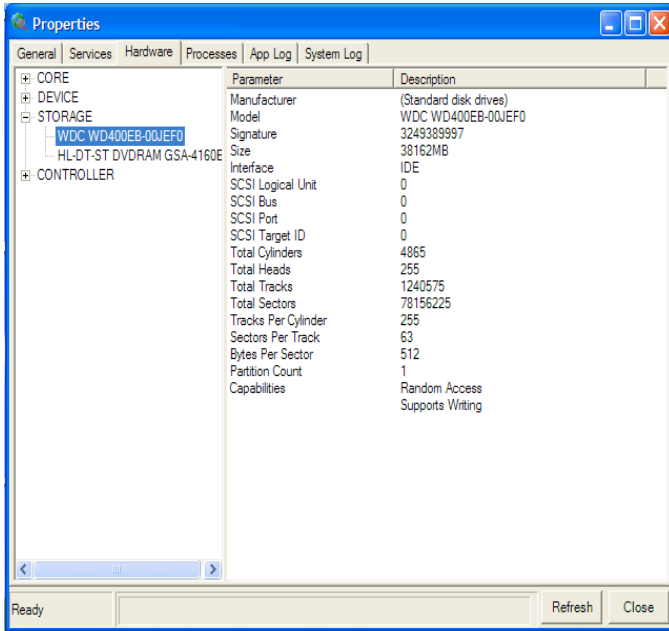
The properties dialog contains category selection tabs across the top, a refresh toggle button and a close push button. When the refresh button is enabled, the current page will be updated continuously with a minimum half-second pause between each update. The close button will stop any current refresh and exit the dialog.

General Tab

The General Tab presents several fields in the top half of the dialog. The Name field is what the computer reports as its hostname. This does not necessarily match the host component of the associated DNS host entries and is usually either the NBT name or internally defined host name. The Location and Contact fields are only reported if set by the administrator of the device. The Up Time field shows the amount of time since the devices networking subsystem was last reset – usually the time since the device was restarted. The Description field is as is reported by the device and usually contains the OS version and a basic description of the hardware. The Layers field lists the layers in the OSI model that the device reports as implementing. The Routing field shows whether the device will forward traffic between its interfaces.

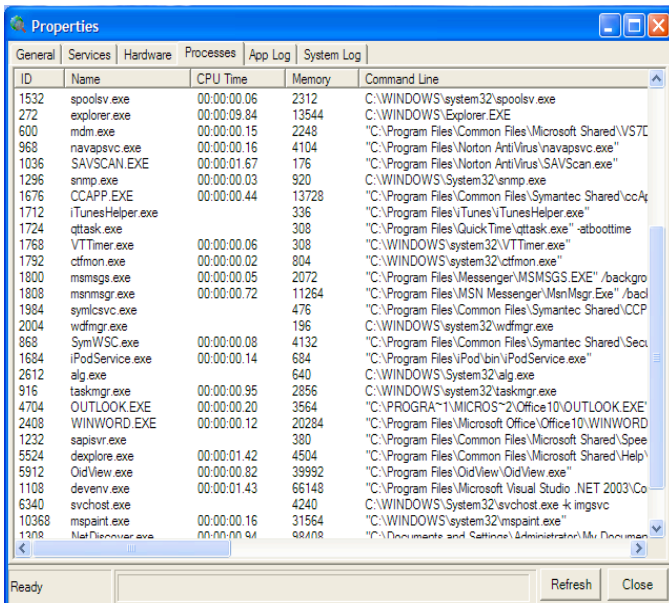
In the bottom half of the dialog is information on the network configuration of the device. The left contains a list of detected network interface cards (NIC) and a special entry titled “All Interfaces”. At the top right is a list box that lets the user choose which information to view in the bottom right. The information shown is in relation to the selection in the list of NICs. If “All Interfaces” is selected, information from each interface is combined in to the view.

Hardware Tab



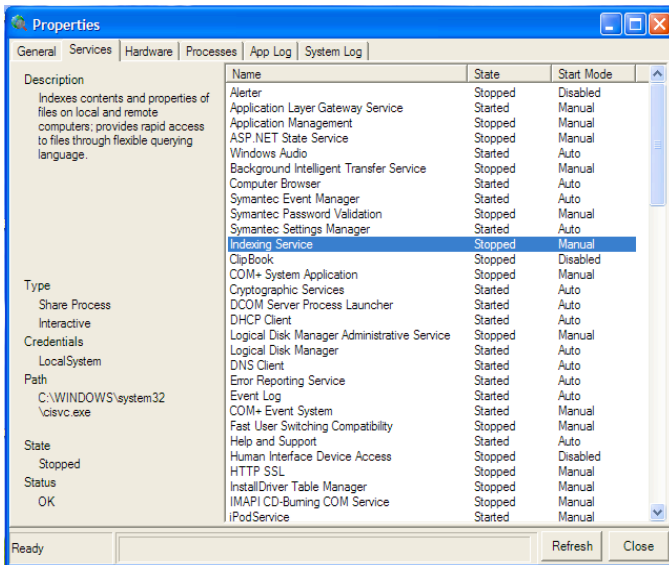
The Hardware Tab presents a list of detected hardware in the left pane and details of an individual hardware component in the right pane. Hardware on the left is categorized into hardware sub-systems.

Processes Tab



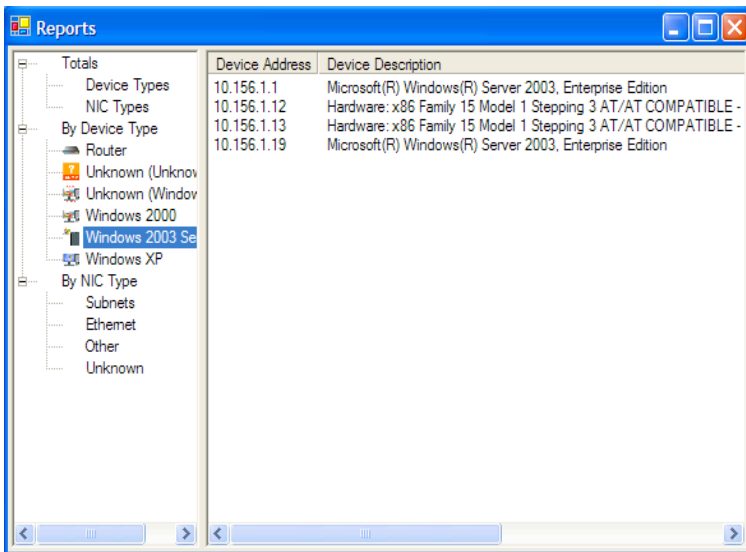
The Processes Tab presents a table of information showing each process running on the device. The ID field is OS-specific but is always unique. The Name field is usually the process's executable's name. The CPU Time field is cumulative processor usage. The Memory field is the amount of memory mapped to the process in kilobytes. The Command Line field shows the full set of arguments used to start the process.

Services Tab



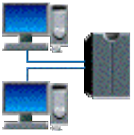
The Services Tab shows a list of installed services in the right pane and details about each service in the left pane. In the right pane, each service is listed by Name and shows its State, either started or stopped, and how it is set to Start Up, either Automatic, Manual or Disabled. Selecting a service in the right pane will update the left pane with details of that service. The Description field is reported by the service in the same language as the device's software. The Type shows the class of service and whether it has been assigned the right to interact with the desktop. The Credentials field shows which user the service is running as. The Path field lists the full execution parameters of the service. The State is equivalent to the listing in the right pane. The Status is reported by the service and shows if any problems have occurred.

Reports



The Reports window provides various views of the data collected during network discovery. Its purpose is to allow for finding of specific information quickly and easily.

Device Types (Appendix A)



Network



Router



Switch



Windows 2003 Server



Windows 2000 Server
Windows NT Server



Unix



MacOS



Thin Client



IP Telephone



Unknown SNMP Compatible



Bridge



Hub



Windows XP Client



Windows 2000 Client



Windows NT Client



Windows 98



Windows 95



Windows CE



Printer



Unknown