

# NetSentinel Reference

- Installing Software for Network Versions ..... 2**
  - The Rainbow NetSentinel Software ..... 2
  - Network Version Requirements..... 3
  - Installing the Rainbow Network Software..... 3
  - Security Server Reference ..... 4
    - Choosing the Security Computer ..... 4
    - Running the Security Server on a NetWare File Server ..... 6
    - Running the NetSentinel Service Security Server under Windows NT ..... 9
    - Running the Win32 Windows Security Server ..... 13
    - Running the Security Server on a DOS Computer ..... 16
    - Running the Security Server on an OS/2 Computer..... 19
  - Security Monitor Reference ..... 22
    - The Security Monitor Programs ..... 22
    - Running WINMON, the Windows-Based Security Monitor ..... 23
    - Running DOSMON, the DOS-Based Security Monitor ..... 24
    - Running OS2MON, the OS2-Based Security Monitor ..... 26
  - NetSentinel Configuration Reference..... 28
    - Banyan Vines ..... 28
    - IBM LAN Server/Requester 2.x and 3.x..... 29
    - LANTastic..... 30
    - Microsoft LAN Server/Requester 2.0 and 2.1 ..... 31
    - Novell NetWare 3.x and 4.x ..... 32
    - Windows for Workgroups 3.11 (NetBEUI) ..... 32
    - Windows NT / Windows NT with Novell NetWare ..... 33
    - Windows 95 / Windows 95 with Novell NetWare ..... 34
    - Using TCP/IP with Windows 95 and NT ..... 35

## Installing Software for Network Versions

### The Rainbow NetSentinel Software

The SLOPE/W Network Version makes it possible for you to use SLOPE/W on any computer in your network. It also allows a group of people to use the software simultaneously. For example, if you purchased a 5-user license of the SLOPE/W Network Version, up to 5 people on the network can use SLOPE/W concurrently.

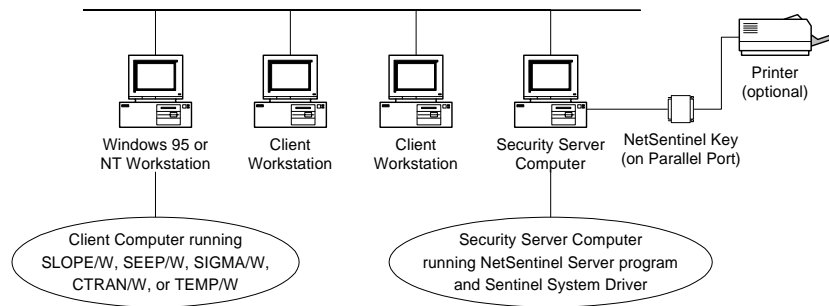
The SLOPE/W NetSentinel network security key is supplied with the SLOPE/W Network Version. The NetSentinel security key monitors the number of users running SLOPE/W concurrently and ascertains that properly licensed software is being used. The NetSentinel key must be attached to a designated computer somewhere on your network; this computer is referred to here as the *security computer*.

The SLOPE/W Network Version requires additional software to manage the NetSentinel security key. This software is supplied to GEO-SLOPE by Rainbow Technologies, the makers of the NetSentinel key. The Rainbow NetSentinel software includes the following three items:

1. A *network security server* program must be run on the security computer; this program communicates with the NetSentinel key and keeps track of how many users are running SLOPE/W concurrently.
2. A Sentinel system driver is installed on the security computer; this driver allows the security server program to communicate with the NetSentinel key on the parallel port.
3. A *network security monitor* program can optionally be run from any computer on the network.

This monitoring program displays information about the security server and security key. This information includes server transport protocols, the number of licenses in use, the number of users who were disconnected after timing out, and the license limit for each key. You do not need to install the security monitor to use the SLOPE/W Network Version; however, the security monitor is useful for administrating the network software.

The following diagram illustrates how the NetSentinel security key and software are connected to your network:



NetSentinel Security Key and Software Configuration

---

## Network Version Requirements

The SLOPE/W Network Version can be run from the network file server or from each user's local hard disk, depending on your preference. The basic requirements for running the SLOPE/W Network Version are:

1. The computer network must support at least one of the following protocols: NetBIOS, IPX/SPX, Named Pipes, or TCP/IP.
  - If TCP/IP is used, the NetSentinel key must be connected to a computer running Windows 95 or Windows NT.
  - If the IPX/SPX protocol is used, *both* IPX *and* SPX must be loaded on the server computer and on each client computer running SLOPE/W.
2. The NetSentinel security key must be attached to the parallel printer port on one computer on the network.
  - This security computer may be the network file server or any one of the client computers.
3. The security computer must be running an appropriate version of the security server program.
  - Security server programs are included for Windows 95, Windows NT, Novell NetWare 3.x and 4.x, OS/2, and DOS.
  - The NetSentinel NLM security server is fully approved and certified by Novell Labs for use on NetWare file servers.

---

NOTE: If you are running the SLOPE/W Network Version using IPX/SPX under Windows 95, you must install Microsoft's NWLINK IPX software patch. This software patch fixes a bug in versions of Windows 95 prior to Service Release 2. You will be prompted to install this patch (if it is necessary) when you are running the SLOPE/W Setup program or the Network Software Setup program.

---

## Installing the Rainbow Network Software

➤ **To install the Rainbow software:**

1. Choose Install Additional Software for Network Versions from the main Setup window.

The Network Software Setup program begins execution.
2. Select the software components that you wish to install: the security servers, the security monitors, and the Sentinel system driver.
  - For the security servers, select the appropriate version for the operating system you are running on the security computer. You can select more than one security server version if you wish.
  - For the monitoring programs, select the appropriate versions for all client computers that you wish to run the security monitors. You can select more than one security monitor version.
  - Install the Sentinel system driver if you are also installing the Windows or OS/2 versions of the security server; for DOS or NetWare versions of the security server, you do not require a Sentinel system driver.

3. Follow the remaining Setup instructions.

The security server and monitoring programs are copied to subdirectories within the specified directory. The subdirectories are named DOS, NW, OS2 and WIN32 (applicable to Windows 95 or NT) corresponding to the name of the operating systems. If you are installing server or monitoring programs for WIN32, Setup will create program folders for them. You can run these program by clicking on their icons.

➤ **To run the SLOPE/W Network Version:**

1. Attach the NetSentinel key to the security computer and run the installed security server.
2. Run the installed security monitoring program on any client computer on the network.
3. Run the installed SLOPE/W Network Version.

The security monitoring program will indicate one SLOPE/W license in use.

## Security Server Reference

### Choosing the Security Computer

The GEO-SLOPE network software includes six versions of the security server program as shown in Table 2.1.

**Table 2.1 Network Security Server Software Versions**

Program	Description
NSRVDI.EXE	DOS IPX/SPX TSR server
NSRVDN.EXE	DOS NetBIOS TSR server
NSRVOM.EXE	Multi-protocol OS/2 server
NSRVNI.NLM	NetWare NLM IPX/SPX server
NSSRVICE.EXE	NetSentinel Service for Windows NT using IPX/SPX, NetBIOS, and TCP/IP
NSRVGX.EXE	Windows 32-bit IPX/SPX, NetBIOS, and TCP/IP server

The different versions of the security server allow you the flexibility of running the program on a Windows 95, Windows NT, DOS or OS/2 workstation or on a Novell NetWare or Windows NT file server. The computer you choose will depend on your specific network environment and available computer resources. Remember that the NetSentinel security key must be connected to a parallel port on the security computer.

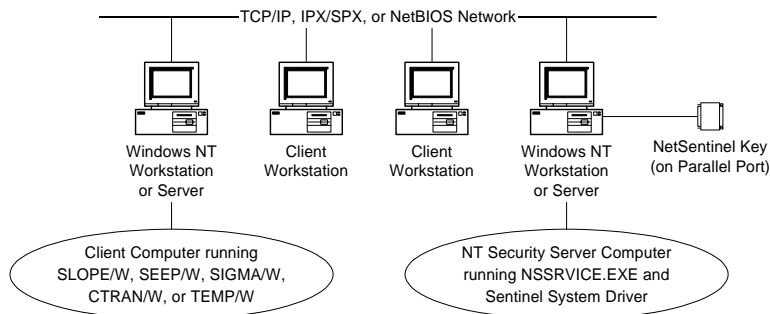
In most circumstances, the best option is to run a version of the security server on a computer that is always running. Your network file server, for example, provides the NetSentinel security server with a robust hardware platform; choosing a security computer that crashes frequently would force all SLOPE/W users to restart the program. The file server also provides a measure of physical security to the NetSentinel key, since the file server is normally locked in a limited-access facility.

### Windows NT

If you are using Windows NT Server or Workstation on your network, the best option may be to run NSSRVICE.EXE, the version of the NetSentinel security server that is implemented as a Windows NT service. Since it is an NT service, this security server is automatically started whenever the Windows NT

operating system is started. There is no need to log on to Windows NT to start the security server, and the server will not be stopped when you log off from Windows NT. The NetSentinel Service supports NetBIOS, IPX/SPX, and TCP/IP.

The following diagram illustrates the NetSentinel security key and software connected to a typical Windows NT network:

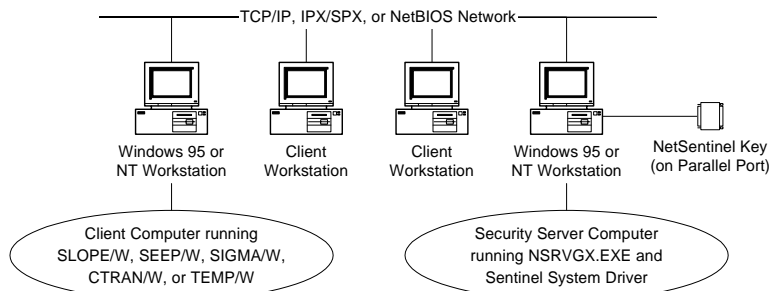


NetSentinel Security Key on a Windows NT network

### Windows 95 or NT

The Win32 security server (NSRVGX.EXE) is a good choice if you are using Windows 95 or if you are using Windows NT and do not wish to use the NT Service security server. The Win32 security server is a native 32-bit Windows program and supports NetBIOS, IPX/SPX, and TCP/IP.

The following diagram illustrates the NetSentinel security key and software connected to a typical Windows 95 or NT network:

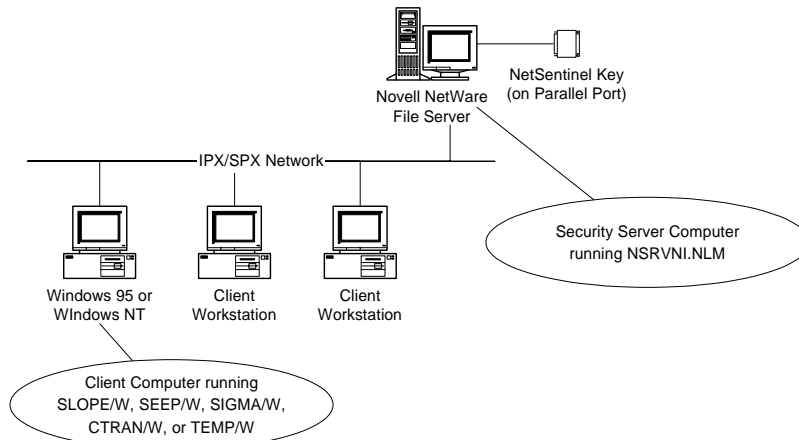


NetSentinel Security Key on a Windows 95 or NT network

### Novell NetWare

If you are using Novell NetWare, the best option may be to run the NLM (NetWare Loadable Module) version of the security server on the Novell file server. This NLM, tested and approved by Novell Labs, can be loaded and unloaded without rebooting the file server.

The following diagram illustrates the NetSentinel security key and software connected to a typical Novell NetWare network:

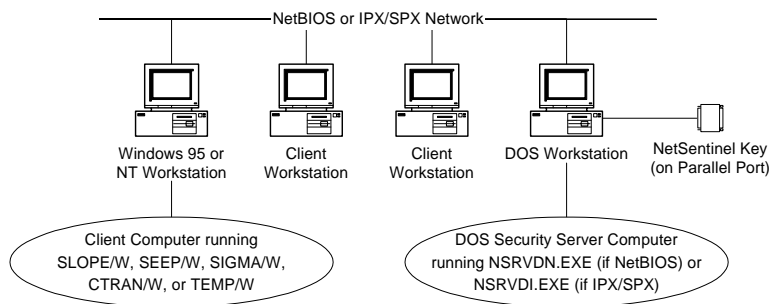


NetSentinel Security Key on a Novell NetWare Network

## DOS

You might choose a DOS computer to be the security server if the computer is used infrequently. However, if you use the computer to run other programs and these programs crash, you may have to reboot your computer. This will restart the security server, forcing everyone using the SLOPE/W Network Version to restart SLOPE/W. It is therefore recommended that you choose one of the other server programs (e.g., the Win32 security server) instead of the DOS-based security servers. If you choose a DOS-based security computer, choose one that will remain up and running as much as possible, even if it is an older computer model.

The following diagram illustrates the NetSentinel security key and software connected to a typical NetBIOS network:



NetSentinel Security Key on a NetBIOS or IPX/SPX network

## Running the Security Server on a NetWare File Server

The NetWare version of the security server runs as an NLM (NetWare Loadable Module) on a Novell NetWare 3.x or 4.x file server. This NLM, tested and approved by Novell Labs, can be loaded and unloaded without rebooting the file server.

### ➤ To run the security server on a Novell NetWare NLM file server:

1. Copy the file NSRVNI.NLM to your network file server. This file is installed by the Network Software Setup program and is located in the SERVER\NW sub-directory.

2. Attach the network security key to the parallel port on the file server.
3. Load the security server program from the command line into memory. For example, type:

```
load nsrvni.nlm
```

Since the NetWare version of the security server is a NetWare Loadable Module (NLM), you can also unload the program from the file server. For example, type:

```
unload nsrvni.nlm
```

The security server NLM will tell you if there are any licenses in use and give you the opportunity to change your mind before unloading.

---

NOTE: If you wish to load the security server automatically when the file server is booted, you can simply add the load command to the file server's AUTOEXEC.NCF file. Also, remember that the NLM version of the security server supports IPX/SPX clients only.

---

Table 2.2 shows the command line options supported by the NLM security server (the command line switches are not case sensitive).

Table 2.2 NLM Security Server Command Line Options

NLM Server Option	Description
/AT:<nnn>	<p>Sets the timing delay in milliseconds between each instruction sent to the NetSentinel key. The default is auto-detection (/AT:0). In the case of a Novell file server running on a fast system, /AT:50 or /AT:100 is recommended.</p> <p>The default value of 0 causes the server to internally compute a value corresponding to a 10 microsecond wait (typically 80 on 486DX2 PC's). By increasing this number, more wait time can be given on computers for which an internally computed wait time is artificially low due to multi-level caches on the computer.</p>
/DN:<name>	<p>Changes the security server's department name from NETINEL to &lt;name&gt;. You do not need to use this option, since the SLOPE/W Network Version can only access a department name of NETINEL.</p>
/DT:<nnn>	<p>Sets the timing delay in milliseconds between establishing SPX connection and sending the handshake message. The default is 0 milliseconds. Specify /DT:50 if the SLOPE/W Network Version occasionally cannot find the NetSentinel key after it has been loaded and running for a while.</p>
/H:<nnn>	<p>Sets the maximum number of licenses that can be in use at any one time on this server to &lt;nnn&gt;. (The default is 150).</p> <p>Your effective license limit is the <i>smaller</i> of (1) the number you set here and (2) the sum of the limits of the keys connected to this server. Specifying a limit higher than what the attached keys support does not increase the license limit. Specifying a limit lower than what the attached keys support effectively disables some licenses.</p>
/MS:<nnn>	<p>Sets the maximum number of servers running on the network to &lt;nnn&gt;. The indicated value ranges from 1 to 10, and is used to determine the range of server names (e.g., NETINEL0, NETINEL1, etc.). If you are only using one security key, you do not need to use this option.</p>
/N:<name>	<p>Sets the name displayed by the security monitor program for this server to &lt;name&gt;. The default is your computer's Ethernet address (NetBIOS) or IPX node number (NetWare).</p>
/P	<p>Overrides the server's use of BIOS parallel port table addresses and uses the standard values 0x278, 0x378, and 0x3BC. This option is needed when the server is run on a machine where other software (such as PowerLAN) has zeroed out the BIOS table located in memory from 40:8 to 40:D.</p>
/P:<port>	<p>Overrides the server's use of BIOS parallel port table addresses and uses the hexadecimal address &lt;port&gt;. Up to three addresses may be specified. This option is needed when the server is run on a machine where other software (such as PowerLAN) has zeroed out the BIOS table located in memory from 40:8 to 40:D, and when a security key is located on a parallel port configured for an I/O location other than 0x278, 0x378, or 0x3BC. For example, <b>/p:278 /p:378</b> identifies parallel ports at I/O addresses 0x278 and 0x378.</p>

---

/Q	Suppresses sign-on messages.
/S:<nnn>	Sets the maximum number of clients that can actively communicate with the server at one time to <nnn>. Note that half of the sessions are used to turn away clients. The default is 4 (two clients at a time).
/SL:<nnnn>	Sets the maximum number of sub-licenses expected to be open at any one time to <nnnn>. This option only applies if you are using multiple GEO-SLOPE products. The default is 256 product sub-licenses.
/ST	Enables strict license time-out enforcement. If this option is set, active licenses are immediately revoked and made available for reuse if the SLOPE/W Network Version has not communicated with the key for 20 minutes (This may happen if SLOPE/W crashes and is unable to free its license before it exits). Setting this option will automatically disconnect timed-out applications from the key. By default, a timed-out license is revoked only if another computer starts a GEO-SLOPE network version and there are no other licenses available (i.e., you've already reached your maximum user limit).
/W:<password>	Sets a password of up to 12 characters. If the server is set with a password option, that password will be required by the security monitoring program whenever licenses are being deleted. If the server is not set to require a password, the server will delete all licenses shown by the security monitor without requiring a password.
/?	Displays the available command line options and then terminates. Output can be redirected to a file using ">".

---

## Running the NetSentinel Service Security Server under Windows NT

The Windows NT service version of the NetSentinel security server (NSSRVIC.EXE) supports IPX/SPX, NWLINK and TCP/IP protocols (For more information about TCP/IP support, see the Using TCP/IP with Windows 95 and NT section in the NetSentinel Configuration Reference in this chapter). Novell IPX/SPX client applications can communicate with the Win32 server if the NWLINK protocol is present on the workstation where the server is running.

NetBIOS and NetBEUI protocols are also supported. The NetSentinel Service supports whatever NetBIOS transports are installed under the NetBIOS interface. More than one NetBIOS may be present at the same time. The server supports Microsoft NetBEUI as well as NWLINK NetBIOS, which is interoperable with Novell NetBIOS clients.

---

**NOTE:** Before you can run the NetSentinel Service security server, you *must* install the NT Sentinel System Driver (Version 5.18 or later) to allow Windows NT to communicate with the NetSentinel key. If you are using an earlier version of the Sentinel driver, please install the latest version from the SLOPE/W CD-ROM; otherwise, Windows NT will generate an event log and the NT service will terminate.

---

The NetSentinel Service security server (NSSRVIC.EXE) can be run on a computer using Windows NT Server or Workstation 3.5 or higher. The Network Software Setup program installs NSSRVIC into the specified folder (e.g., \GSI\_NET\NetServr\Win32).

### ➤ To install the NetSentinel Service security server on a Windows NT computer:

1. Attach the NetSentinel security key to the parallel port on the computer.

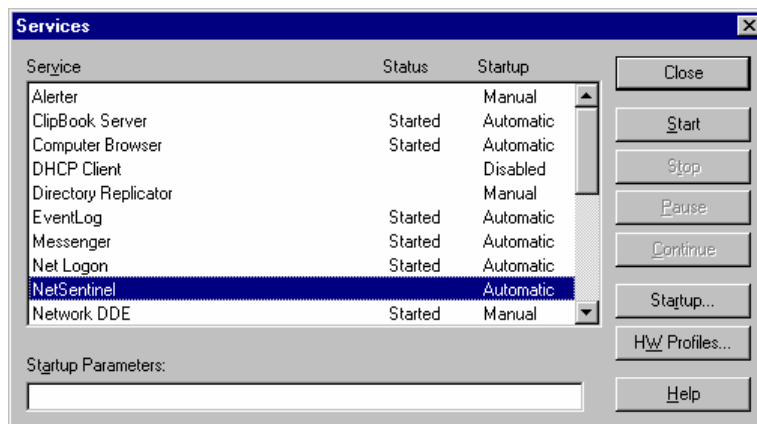
2. Install the NT Sentinel System Driver (Version 5.18 or later) to allow Windows NT to communicate with the NetSentinel key.
3. Copy NSSRVICE.EXE from the installed directory (e.g., \GSI\_NET\NetServr\Win32) to the Windows NT %SystemRoot%\System32 directory (e.g., \WinNT\System32) on the computer.
4. To install the service, choose Run from the Start menu or Program Manager and run **NSSRVICE /I**

The NetSentinel service will run automatically the next time you reboot your Windows NT computer. You do not need to log on to start the service.

A registry entry for the NetSentinel service is created under HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services.

➤ **To run the NetSentinel Service security server:**

- Reboot your computer, or
- At the Windows NT command prompt, type NET START NETSENTINEL, or
- Run Control Panel and double-click on the Services applet. When the dialog box appears (as follows), select the NetSentinel Service and press the Start button.



NOTE: Status information pertaining to the NetSentinel service is reported to the Windows NT application log. Upon successful startup of the service, information such as server version, protocol stacks, and available keys is logged as two separate events in the application log. Please use the NT Event Viewer in the Administrator Tools group to view this information.

➤ **To un-install the NetSentinel Service security server:**

1. Log on to the Windows NT computer.
2. Stop the NetSentinel NT service by typing NET STOP NETSENTINEL at the NT command prompt. Alternatively, you can run Control Panel, double-click on the Services applet, select the NetSentinel Service, and press the Stop button.
3. Choose Run from the Start menu or Program Manager and run **NSSRVICE /U**

The registry entry for the NetSentinel Service is removed from HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services.

➤ **To display the version of the NetSentinel Service security server:**

- Choose Run from the Start menu or Program Manager and run **NSSERVICE /V**

---

NOTE: If you are using the NetBIOS or NETBEUI protocols, you must *only* use Lana Number 0. To view and modify this setting, run the Control Panel Network applet, choose Network Services, and select NetBIOS Interface. Click on the Properties button (or Configure button in NT 3.51) to display the current Lana Number settings.

---

Table 2.4 shows the command line options supported by the NetSentinel Service security server (the command line switches are not case sensitive). The specified options, if any, will take effect the next time the service is started.

**Table 2.3 NetSentinel Service Security Server Command Line Options**

NetSentinel Service Option	Description
/BI:<address>	Overrides the default "Find_Server" UDP broadcast address to direct the search over TCP/IP to a specified subnet. (The default address is set to 255.255.255.255, for a limited broadcast to all connected network segments).
/DN:<name>	Changes the security server's department name from NETINEL to <name>. You do not need to use this option, since GEO-SLOPE's network versions can only access a department name of NETINEL.
/H:<nnn>	Sets the maximum number of licenses that can be in use at any one time on this server to <nnn>. (The default is 150).  Your effective license limit is the <i>smaller</i> of (1) the number you set here and (2) the sum of the limits of the keys connected to this server. Specifying a limit higher than what the attached keys support does not increase the license limit. Specifying a limit lower than what the attached keys support effectively disables some licenses.
/MS:<nnn>	Sets the maximum number of servers running on the network to <nnn>. The indicated value ranges from 1 to 10, and is used to determine the range of server names (e.g., NETINEL0, NETINEL1, etc.). If you are only using one security key, you do not need to use this option.
/N:<name>	Sets the name displayed by the security monitor program for this server to <name>. The default is your computer's Ethernet address (NetBIOS) or IPX node number (NetWare).
/RI:<num>	Defines the number of retry operations when searching for servers running over TCP/IP. The default is 3.
/SI: <nnnn>	Sets the number of threads devoted to handling TCP/IP clients to <nnnn>. Values range from 0 to 4; the default if 4. Specifying <b>/SN:0</b> disables all TCP/IP support.
/SL: <nnnn>	Defines the number of entries in the sub-license table.
/SN:<nnnn>	Sets the number of threads devoted to handling NetBIOS/NetBEUI clients to <nnnn>. Values range from 0 to 4; the default is 4. Specifying <b>/SN:0</b> disables all NetBIOS/NetBEUI support.
/ST	Enables strict license time-out enforcement. If this option is set, active licenses are immediately revoked and made available for reuse if the SLOPE/W Network Version has not communicated with the key for 20 minutes (This may happen if SLOPE/W crashes and is unable to free its license before it exits). Setting this option will automatically disconnect timed-out applications from the key. By default, a timed-out license is revoked only if another computer starts a GEO-SLOPE network version and there are no other licenses available (i.e., you've already reached your maximum user limit).

---

/SW:<nnnn>	Sets the number of threads devoted to handling IPX/SPX (NWLINK) clients to <nnnn>. Values range from 0 to 4; the default is 4. Specifying /SW:0 disables all IPX/SPX (NWLINK) support.
/TI:<num>	Sets the time-out value in seconds for each retry operation when searching for servers running over TCP/IP. The default is 5.
/W:<password>	Sets a password of up to 12 characters. If the server is set with a password option, that password will be required by the security monitoring program whenever licenses are being deleted. If the server is not set to require a password, the server will delete all licenses shown by the security monitor without requiring a password.

---

## Running the Win32 Windows Security Server

The 32-bit Windows version of the NetSentinel security server (NSRVGX.EXE) supports IPX/SPX, NWLINK and TCP/IP protocols (For more information about TCP/IP support, see the Using TCP/IP with Windows 95 and NT section in the NetSentinel Configuration Reference in this chapter). Novell IPX/SPX client applications can communicate with the Win32 server if the NWLINK protocol is present on the workstation where the server is running.

NetBIOS and NetBEUI protocols are also supported. The Win32 server supports whatever NetBIOS transports are installed under the NetBIOS interface. More than one NetBIOS may be present at the same time. The server supports Microsoft NetBEUI as well as NWLINK NetBIOS, which is interoperable with Novell NetBIOS clients.

---

**NOTE:** Before you can run the Win32 security server under Windows NT, you *must* install the NT Sentinel System Driver to allow Windows NT to communicate with the NetSentinel key. If you are running under Windows 95, it is recommended that you install the Windows 95 Sentinel System Driver before running the Win32 security server.

---

The Win32 security server (NSRVGX.EXE) can be run on a Windows NT or Windows 95 computer. The Network Software Setup program installs NSRVGX and creates a folder containing NSRVGX for you:



### ➤ To run the Win32 security server on a Windows NT or Windows 95 computer:

1. Attach the NetSentinel security key to the parallel port on the computer.
2. Run NSRVGX from the folder created by the Network Software Setup program (e.g., \GSI\_NET\NetServr\Win32\NSRVGX.EXE). Alternatively, you can run NSRVGX by choosing Run from the Start menu or Program Manager and specifying its full path.

The server program displays a copyright message as it loads. When loaded, the program appears as an icon on the display screen. If you want to view information about the server as it runs, maximum its icon.

3. To unload the Win32 NetSentinel server, close the program.

---

NOTE: If you are using the NetBIOS or NETBEUI protocols, you must *only* use Lana Number 0. To view and modify this setting, run the Control Panel Network applet, choose Network Services, and select NetBIOS Interface. Click on the Properties button (or Configure button in NT 3.51) to display the current Lana Number settings.

---

Table 2.4 shows the command line options supported by the Win32 security server (the command line switches are not case sensitive).

**Table 2.4 Win32 Security Server Command Line Options**

Win32 Server Option	Description
/BI:<address>	Overrides the default "Find_Server" UDP broadcast address to direct the search over TCP/IP to a specified subnet. (The default address is set to 255.255.255.255, for a limited broadcast to all connected network segments).
/DN:<name>	Changes the security server's department name from NETINEL to <name>. You do not need to use this option, since GEO-SLOPE's network versions can only access a department name of NETINEL.
/H:<nnn>	Sets the maximum number of licenses that can be in use at any one time on this server to <nnn>. (The default is 150).  Your effective license limit is the <i>smaller</i> of (1) the number you set here and (2) the sum of the limits of the keys connected to this server. Specifying a limit higher than what the attached keys support does not increase the license limit. Specifying a limit lower than what the attached keys support effectively disables some licenses.
/MS:<nnn>	Sets the maximum number of servers running on the network to <nnn>. The indicated value ranges from 1 to 10, and is used to determine the range of server names (e.g., NETINEL0, NETINEL1, etc.). If you are only using one security key, you do not need to use this option.
/N:<name>	Sets the name displayed by the security monitor program for this server to <name>. The default is your computer's Ethernet address (NetBIOS) or IPX node number (NetWare).
/Q	Suppresses sign-on messages.
/RI:<num>	Defines the number of retry operations when searching for servers running over TCP/IP. The default is 3.
/SI: <nnnn>	Sets the number of threads devoted to handling TCP/IP clients to <nnnn>. Values range from 0 to 4; the default is 4. Specifying <b>/SN:0</b> disables all TCP/IP support.
/SL: <nnnn>	Defines the number of entries in the sub-license table.
/SN:<nnnn>	Sets the number of threads devoted to handling NetBIOS/NetBEUI clients to <nnnn>. Values range from 0 to 4; the default is 4. Specifying <b>/SN:0</b> disables all NetBIOS/NetBEUI support.
/ST	Enables strict license time-out enforcement. If this option is set, active licenses are immediately revoked and made available for reuse if the SLOPE/W Network Version has not communicated with the key for 20 minutes (This may happen if SLOPE/W crashes and is unable to free its license before it exits). Setting this option will automatically disconnect timed-out applications from the key. By default, a timed-out license is revoked only if another computer starts a GEO-SLOPE network version and there are no other licenses available (i.e., you've already reached your maximum user limit).

<code>/SW:&lt;nnnn&gt;</code>	Sets the number of threads devoted to handling IPX/SPX (NWLINK) clients to <nnnn>. Values range from 0 to 4; the default is 4. Specifying <code>/SW:0</code> disables all IPX/SPX (NWLINK) support.
<code>/TI:&lt;num&gt;</code>	Sets the time-out value in seconds for each retry operation when searching for servers running over TCP/IP. The default is 5.
<code>/W:&lt;password&gt;</code>	Sets a password of up to 12 characters. If the server is set with a password option, that password will be required by the security monitoring program whenever licenses are being deleted. If the server is not set to require a password, the server will delete all licenses shown by the security monitor without requiring a password.

---

## Running the Security Server on a DOS Computer

The DOS versions of the security server are provided in case you wish to run the security server on a rarely-used, DOS-based computer. Since DOS-based computers are frequently unstable and prone to crashing, it is recommended that you run one of the other security server programs (e.g., the Win32 security server) instead of the DOS-based security servers.

The DOS versions of the security server run as TSR (Terminate and Stay Resident) programs. One version uses the NetBIOS protocol, and the other version uses the IPX/SPX protocol.

### ➤ To run the security server on a DOS computer:

1. Determine whether your network uses the NetBIOS or IPX/SPX protocols.

NetBIOS is a popular protocol supported by many networks, while IPX/SPX is the native Novell NetWare protocol.

2. If you are using NetBIOS, copy the files NSRVND.EXE and NSRVND.PIF to the local hard drive on the DOS server computer. These files are installed by the Network Software Setup program; their default location is in the `\GSI_NET\NetServr\DOS` directory.
3. Otherwise, if you are using IPX/SPX, copy the file NSRVDI.EXE to the local hard drive on the DOS server computer. This file is installed by the Network Software Setup program; its default location is in the `\GSI_NET\NetServr\DOS` directory.
4. Add a line to your AUTOEXEC.BAT file to run the security server each time the computer is turned on. For example, if you installed the NetBIOS security server, add the following line to AUTOEXEC.BAT:

```
c:\nsrvdn
```

If you installed the IPX/SPX security server, add the following line to AUTOEXEC.BAT:

```
c:\nsrvdi
```

5. Attach the network security key to the parallel port of your computer and reboot the computer.

The security server program is loaded into memory when the computer is restarted. This computer should always be running whenever anyone on the network is using the GEO-SLOPE network software.

---

If you are running Windows on the security computer, use the following guidelines :

- Always start the network transport protocol (IPX/SPX or NetBIOS) *and* the DOS-based security server *before* starting Windows.
- If you are using Windows for Workgroups on the security computer, add the following line to AUTOEXEC.BAT just before the security server is loaded:

```
net start netbeui
```

This statement will start the NetBIOS protocol in real mode, which is required by the DOS version of the security server. Otherwise, Windows for Workgroups will load NetBIOS in 386 enhanced mode, and the security server will be unable to communicate properly with the security key

This statement should be added to AUTOEXEC.BAT for *all* computers running Windows for Workgroups and the GEO-SLOPE software, since the software must communicate with the security server in real mode when using NetBIOS.

- Never run an application in exclusive mode under Windows on the security computer. This will prevent the security server from communicating with the security key.
- If you are running DOS applications under Windows in 386 enhanced mode, make sure background processing is enabled. (This can be done by editing the application's PIF file and checking the **Background** option). Also, lock all memory used by the DOS application. (Edit the application's PIF file, select **Advanced**, and check **Lock Application Memory**). Not doing so may prevent the security server from communicating with the security key.
- Configure the parallel port to never warn about conflicts. (From the Windows Control Panel, select **386 Enhanced** and then select **Never Warn** for the appropriate port under **Device Contention**).

---

NOTE: Do not run one of the DOS-based security servers from a DOS box under Windows.

---

Table 2.5 shows the command line options supported by the DOS security server (the command line switches are not case sensitive).

**Table 2.5 DOS Security Server Command Line Options**

<b>DOS Server Option</b>	<b>Description</b>
/DN:<name>	Changes the security server's department name from NETINEL to <name>. You do not need to use this option, since GEO-SLOPE's network versions can only access a department name of NETINEL.
/DT:<nnn>	Sets the timing delay in milliseconds between establishing SPX connection and sending the handshake message. The default is 0 milliseconds. Specify /DT:50 if the SLOPE/W Network Version occasionally cannot find the NetSentinel key after it has been loaded and running for a while. This option applies to NSRVDI.EXE but not to NSRVDN.EXE.
/H:<nnn>	Sets the maximum number of licenses that can be in use at any one time on this server to <nnn>. (The default is 150).  Your effective license limit is the <i>smaller</i> of (1) the number you set here and (2) the sum of the limits of the keys connected to this server. Specifying a limit higher than what the attached keys support does not increase the license limit. Specifying a limit lower than what the attached keys support effectively disables some licenses.
/MS:<nnn>	Sets the maximum number of servers running on the network to <nnn>. The indicated value ranges from 1 to 10, and is used to determine the range of server names (e.g., NETINEL0, NETINEL1, etc.). If you are only using one security key, you do not need to use this option.
/N:<name>	Sets the name displayed by the security monitor program for this server to <name>. The default is your computer's Ethernet address (NetBIOS) or IPX node number (NetWare).
/P	Overrides the server's use of BIOS parallel port table addresses and uses the standard values 0x278, 0x378, and 0x3BC. This option is needed when the server is run on a machine where other software (such as PowerLAN) has zeroed out the BIOS table located in memory from 40:8 to 40:D.
/P:<port>	Overrides the server's use of BIOS parallel port table addresses and uses the hexadecimal address <port>. Up to three addresses may be specified. This option is needed when the server is run on a machine where other software (such as PowerLAN) has zeroed out the BIOS table located in memory from 40:8 to 40:D, and when a security key is located on a parallel port configured for an I/O location other than 0x278, 0x378, or 0x3BC. For example, <b>/p:278 /p:378</b> identifies parallel ports at I/O addresses 0x278 and 0x378.
/Q	Suppresses sign-on messages.
/R	Conditionally unloads a previous instance of the server from memory, if and only if there are no open security sessions.
/S:<nnn>	Sets the maximum number of clients that can actively communicate with the server at one time. Note that half of the sessions are used to turn away clients. The default is 4 (two clients at a time).

---

/SL:<nnnn>	Defines the number of entries in the sub-license table.
/ST	Enables strict license time-out enforcement. If this option is set, active licenses are immediately revoked and made available for reuse if the SLOPE/W Network Version has not communicated with the key for 20 minutes (This may happen if SLOPE/W crashes and is unable to free its license before it exits). Setting this option will automatically disconnect timed-out applications from the key. By default, a timed-out license is revoked only if another computer starts a GEO-SLOPE network version and there are no other licenses available (i.e., you've already reached your maximum user limit).
/U	Unconditionally unloads a previous instance of the server from memory, whether or not there are open security sessions.
/W:<password>	Sets a password of up to 12 characters. If the server is set with a password option, that password will be required by the security monitoring program whenever licenses are being deleted. If the server is not set to require a password, the server will delete all licenses shown by the security monitor without requiring a password.
/?	Displays help information on the console and then terminates. Output can be redirected to a file using ">".

---

## Running the Security Server on an OS/2 Computer

The OS/2 version of the security server runs as an OS/2 application. You can unload it by simply terminating the program, just as with any other OS/2 application.

---

NOTE: Before you can run the OS/2 security server, you *must* install the OS/2 Sentinel System Driver (SENTINEL.SYS) to allow OS/2 to communicate with the NetSentinel key. The location of this device driver must be specified in the CONFIG.SYS file. See the README.TXT file in the \SENTINEL\OS2 directory on the GEO-SLOPE distribution CD-ROM for information on installing the OS/2 Sentinel system driver.

---

### ➤ To run the OS/2 security server:

1. Install the OS/2 Sentinel System Driver to allow OS/2 to communicate with the NetSentinel key.
2. Add a line to your CONFIG.SYS file to load the OS/2 Sentinel device driver. For example, add the following line to CONFIG.SYS:
 

```
DEVICE=C:\SENTINEL.SYS
```
3. Attach the NetSentinel security key to the parallel port on the computer.
4. Reboot the security computer.
5. Copy the file NSRVOM.EXE to the OS/2 security computer. This file is installed by the Network Software Setup program (run under Windows); its default location is in the C:\GSI\_NET\NetServr\OS2 directory.
6. **For IBM or Microsoft Named Pipes:**

Use the ACCESS CONTROL function in NET to share the pipe named \PIPE\deptname, where deptname is your security server's department name. The default deptname is NETINEL.

**For Novell Named Pipes:**

Install the OS/2 Requester. Make the security server a Named Pipes server, and make every computer that is running the SLOPE/W Network Version a Named Pipes client.

7. Execute the security server program (NSRVOM) from the OS/2 command line, adding any options you desire.
8. Wait (about a minute) for the "Server Initialization completed" message to appear.

Once started, the server program appears as an icon on the screen. To stop running the server program, close the window in which the server program is running. To restart the server program, type **NSRVOM** followed by any desired options.

If desired, you can also run the program with no visible indication on the screen and no keyboard input/output. From the OS/2 command line or in the STARTUP.CMD file, type **DETACH NSRVOM** followed by any desired options. If you use this option, however, you will need to restart your computer if you wish to stop running the server program.

Table 2.6 shows the command line options supported by the OS/2 security server (the command line switches are not case sensitive).

**Table 2.6 OS/2 Security Server Command Line Options**

OS/2 Server Option	Description
/DN:<name>	Changes the security server's department name from NETINEL to <name>. You do not need to use this option, since GEO-SLOPE's network versions can only access a department name of NETINEL.
/H:<nnn>	Sets the maximum number of licenses that can be in use at any one time on this server to <nnn>. (The default is 150).  Your effective license limit is the <i>smaller</i> of (1) the number you set here and (2) the sum of the limits of the keys connected to this server. Specifying a limit higher than what the attached keys support does not increase the license limit. Specifying a limit lower than what the attached keys support effectively disables some licenses.
/L:<type>:<dll>	Configures the server for a specific network operating system. By default, the server program looks for certain DLLs to determine which system is installed. Use the /L option if you have a network with multiple network operating systems installed and wish to control which is selected.  Enter /L:1 for IBM LAN Server (ACSNETB.DLL), or /L:2 for Microsoft LAN Manager or Novell NetWare OS/2 Requester (NETAPI.DLL).  If you want to specify the DLL to be used, enter the name after the number. For example, /L:1:ACSNEW.DLL loads the ACSNEW.DLL file and uses it as an IBM-type NetBIOS DLL.
/MS:<nnn>	Sets the maximum number of servers running on the network to <nnn>. The indicated value ranges from 1 to 10, and is used to determine the range of server names (e.g., NETINEL0, NETINEL1, etc.). If you are only using one security key, you do not need to use this option.
/N:<name>	Sets the name displayed by the security monitor program for this server to <name>. The default is your computer's Ethernet address (NetBIOS) or IPX node number (NetWare).
/Q	Suppresses sign-on messages.
/SL: <nnnn>	Defines the number of entries in the sub-license table.
/SN:<nnn>	Sets the number of threads allocated for NetBIOS to <nnn>. In general, more threads provide better performance but require more memory. If you do not support NetBIOS, enter /SN:0. The default is 6.
/SP:<nnn>	Sets the number of threads allocated for Named Pipes to <nnn>. In general, more threads provide better performance but require more memory. If you do not support Named Pipes, enter /SP:0. The default is 6.

<code>/ST</code>	Enables strict license time-out enforcement. If this option is set, active licenses are immediately revoked and made available for reuse if the SLOPE/W Network Version has not communicated with the key for 20 minutes (This may happen if SLOPE/W crashes and is unable to free its license before it exits). Setting this option will automatically disconnect timed-out applications from the key. By default, a timed-out license is revoked only if another computer starts a GEO-SLOPE network version and there are no other licenses available (i.e., you've already reached your maximum user limit).
<code>/W:&lt;password&gt;</code>	Sets a password of up to 12 characters. If the server is set with a password option, that password will be required by the security monitoring program whenever licenses are being deleted. If the server is not set to require a password, the server will delete all licenses shown by the security monitor without requiring a password.
<code>/?</code>	Displays help information on the console and then terminates. Output can be redirected to a file using ">".

---

## Security Monitor Reference

### The Security Monitor Programs

The NetSentinel security monitoring program displays information about the security server and security key. This information includes server transport protocols, the number of licenses in use, the number of users who were disconnected after timing out, and the license limit for each key. You do not need to install the security monitor to use the SLOPE/W Network Version; however, the security monitor is useful for administrating the network software.

The security monitor can be run from any computer on the network. Before running the program, make sure you have started the appropriate network transport protocol (IPX/SPX, NetBIOS, Named Pipes, or TCP/IP).

The following versions of the security monitor programs are provided:

- **WINMON** A Windows-based tool that displays NetSentinel servers, keys, products, and users in the field. Unused licenses may be released and re-assigned from a single screen. The monitor may be customized by the system administrator to identify servers, users and products by name.
- **DOSMON** A DOS-based tool that displays all security servers, NetSentinel keys, and users on the network (except servers that use Named Pipes).
- **OS2MON** An OS/2-based tool that displays all security servers, NetSentinel keys, and users on the network.

## Running WINMON, the Windows-Based Security Monitor

WINMON is the most flexible of the security monitoring programs. It is a 32-bit Windows program that can be run from any Windows 95 or Windows NT computer on the network. The Network Software Setup program installs WINMON and creates a folder containing WINMON for you:



### ➤ To run WINMON on a Windows NT or Windows 95 computer:

1. Run WINMON from the folder created by the Network Software Setup program. Alternatively, you can run WINMON from another network computer by choosing Run from the Start menu and specifying WINMON.EXE in the MONITORS\WIN32 sub-directory created by the Network Software Setup program.

WINMON searches the network for NetSentinel security servers and NetSentinel keys and displays the names in the Server and Key drop-down edit boxes.

For all NetSentinel keys found on the network, the following information is displayed in the WINMON Keys list box:

- **Name** The name of the NetSentinel key (e.g., GEO-SLOPE)
- **Type** The type of the NetSentinel key (e.g., NS-C)
- **AlgoID** A hexadecimal number unique to each key name (e.g., 0000e3fd)
- **Subs** The number of sub-licenses (GEO-SLOPE products) controlled by the key. The GEO-SLOPE NetSentinel key controls five GEO-SLOPE software products, including SLOPE/W.
- **Max** The maximum number of licenses available (i.e., the maximum number of users that can run any GEO-SLOPE software simultaneously)
- **Users** The current number licenses in use (i.e., the current number of users running any GEO-SLOPE software)
- **Peak** The peak number of licenses used (i.e., the maximum number of users that have been running GEO-SLOPE software simultaneously)
- **Locked** **Yes** if the NetSentinel key is locked, **No** if it is unlocked and available for queries

If anyone is currently using any GEO-SLOPE software, the user names and last access time are displayed in the WINMON Users list box. The user name begins with **B:** or **S:** followed by the user's network address. **B:** refers to a base license and **S:** refers to a sub-license. A base license is granted the first time the user runs any of GEO-SLOPE's software products. The user is granted a sub-license for each GEO-SLOPE product running. For example, if a user starts running SLOPE/W DEFINE, a GEO-SLOPE base license and a SLOPE/W sub-license is granted. If the user then runs SLOPE/W DEFINE, a SLOPE/W sub-license is granted; a base license is not granted, since it was already given when SLOPE/W was started. If the user then runs SLOPE/W CONTOUR, no sub-licenses are granted, since the user already has a SLOPE/W sub-license.

2. In the Key drop-down list box, select GEO-SLOPE.

Only GEO-SLOPE key information is displayed in the WINMON Key list box. The five GEO-SLOPE products are listed in the Product drop-down list box.

3. In the Product drop-down list box, select SLOPE/W.

All SLOPE/W sub-licenses currently in use are displayed in the User list box.

4. Press the Edit Mapping File button if you wish to modify the names displayed by WINMON. The Edit Monitor Map dialog box appears.

5. To display actual user names in WINMON instead of network addresses, click the Add User button and enter the user information in the edit boxes.

The WINMON names are stored in a file called MAPFILE.TXT in the same directory as WINMON.EXE. GEO-SLOPE has created names in this file for each GEO-SLOPE software product.

6. Choose Done in the Edit Monitor Map dialog box.
7. Choose Help Contents for more information on running WINMON.
8. To exit WINMON, press the Quit button.

WINMON can also be used to remove user licenses; this will disconnect the user from the NetSentinel key and cause the GEO-SLOPE application to terminate. Since you may not want everyone to delete licenses, you should start the security server with the password command line option. This will require the user to enter the password before the licenses can be deleted.

➤ **To remove licenses using WINMON:**

1. In the WINMON Users list box, select the licenses that you wish to delete.

You can select a GEO-SLOPE license or a product sub-license. Deleting a GEO-SLOPE license will terminate all GEO-SLOPE applications currently running on the user's computer. Deleting a product sub-license (e.g., SLOPE/W) will only terminate SLOPE/W on the user's computer.

2. Press the Delete User License button.

If the security server program was run with the /W password option, a password dialog box is displayed. Enter the password used to run the security server.

## **Running DOSMON, the DOS-Based Security Monitor**

DOSMON can monitor NetSentinel keys attached to security computers running any NetBIOS or IPX/SPX based security server programs. DOSMON was the first security monitoring program available; it is not as full-featured or as easy to use as WINMON.

You can run DOSMON from DOS or from a DOS box under Windows. It is installed in the TOOLS\DOS sub-directory created by the Network Software Setup program.

When it is first started, DOSMON searches the network for all security keys; a bar graph is displayed, showing the progress of the search. Once the search is complete, a menu is displayed. Select **View by server** or **View by algorithm** to display information about the security key.

The following general rules should help you use DOSMON:

- To select an item from a list (and see more detailed data on it), move the highlight bar to it using the arrow keys and press ENTER.
- To return to the previous screen, press ESC. Pressing ESC from the first screen exits the program. The exit must be verified before the program will terminate.
- To update the date on your screen, press TAB. The message **Working - Please Wait** is displayed while new data is collected. If it is necessary to search the entire network, a bar graph is displayed, showing the progress of the update.
- For help on any screen, press the F1 key.
- The monitor will recognize a mouse. On menus, a single click moves the highlight bar, and a single click on the highlight bar or a double click on a non-highlighted selection selects the menu option. In lists, clicking on an item selects the item. Clicking on any bar at the bottom of the screen is the same as pressing the key highlighted in the bar.

In most cases, the monitor program will automatically detect the monitor type you are using. However, when a monochrome monitor is used with a color card, the monitor program will detect a color monitor. There may also be situations where a monochrome monitor is detected instead of a color monitor. To override automatic monitor type detection, set the environment variable PNLMONO to 1 for a monochrome monitor (i.e., type SET PNLMONO=1) or set PNLCOLOR to 1 for a color monitor (i.e., type SET PNLCOLOR=1). The environment variable must be set prior to starting the monitor program.

Table 2.7 shows the command line options supported by DOSMON (the command line switches are not case sensitive).

**Table 2.7 DOSMON Command Line Options**

DOSMON Option	Description
/DN:<name>	Changes the security server's department name from NETINEL to <name>. You do not need to use this option, since GEO-SLOPE's network versions can only access a department name of NETINEL.
/H, /?	Displays help information on the console and then terminates. Output can be redirected to a file using ">".
/I	Searches for security servers using the IPX/SPX protocol.
/MS:<nnn>	Sets the maximum number of servers running on the network to <nnn>. The indicated value ranges from 1 to 10, and is used to determine the range of server names (e.g., NETINEL0, NETINEL1, etc.). If you are only using one security key, you do not need to use this option.
/N	Searches for security servers using the NetBIOS protocol.
/S	Displays software security information (network license configuration and status) on the console, and then terminates. Output can be redirected to a file using ">". The information displayed is the same as that printed by <b>Print network data base</b> .

DOSMON will search only for those security servers that use the protocols specified on the command line. If no protocol is specified, the default is to use all protocols (e.g., **/I/P**).

### **Running OS2MON, the OS2-Based Security Monitor**

OS2MON can monitor NetSentinel keys attached to security computers running any NetBIOS or IPX/SPX based security server programs. OS2MON is an OS/2-based version of DOSMON; it is not as full-featured or as easy to use as WINMON.

You can run OS2MON from the TOOLS\OS2 sub-directory created by the Network Software Setup program.

Table 2.8 shows the command line options supported by OS2MON (the command line switches are not case sensitive, and each option must be preceded by at least one space).

**Table 2.8 OS2MON Command Line Options**

OS2MON Option	Description
/A	Searches for security servers using the NetBIOS ACSNETB protocol.
/DN:<name>	Changes the security server's department name from NETINEL to <name>. You do not need to use this option, since GEO-SLOPE's network versions can only access a department name of NETINEL.
/H, /?	Displays help information on the console and then terminates. Output can be redirected to a file using ">".
/I	Searches for security servers using the IPX/SPX protocol.
/L:<type>:<dll>	Configures the monitor for a specific network operating system. By default, the monitor program looks for certain DLLs to determine which system is installed. Use the /L option if you have a network with multiple network operating systems installed and wish to control which is selected.  Enter /L:1 for IBM LAN Server (ACSNETB.DLL), or /L:2 for Microsoft LAN Manager or Novell NetWare OS/2 Requester (NETAPI.DLL).  If you want to specify the DLL to be used, enter the name after the number. For example, /L:1:ACSNEW.DLL loads the ACSNEW.DLL file and uses it as an IBM-type NetBIOS DLL.
/MS:<nnn>	Sets the maximum number of servers running on the network to <nnn>. The indicated value ranges from 1 to 10, and is used to determine the range of server names (e.g., NETINEL0, NETINEL1, etc.). If you are only using one security key, you do not need to use this option.
/N	Searches for security servers using the NetBIOS NETAPI protocol.
/O:<file>	Specifies the NETOEM (Network Named Pipes) DLL file name.
/P	Searches for security servers using the Named Pipes protocol.
/S	Displays software security information (network license configuration and status) on the console, and then terminates. Output can be redirected to a file using ">". The information displayed is the same as that printed by <b>Print network data base</b> .

OS2MON will search only for those security servers that use the protocols specified on the command line. If no protocol is specified, the default is to use all protocols (e.g., /I /P /N /A).

The default DLL file names are ACSNETB.DLL, NETAPI.DLL, and NETOEM.DLL. Your LIBPATH is used to locate these DLLs. If you specify a DLL file name without a path and extension (for example, NEWDLL) the monitor uses your LIBPATH to locate the file. If the specified DLL cannot be located, the associated protocol will not be supported. An error message is displayed only if no transport protocols are available.

The following are examples of running OS2MON:

- **OS2MON** Searches for security servers using IPX/SPX, Named Pipes, NetBIOS NETAPI, and NetBIOS ACSNETB. This is the default.
- **OS2MON /I/P** Searches for security servers using IPX/SPX and Named Pipes.
- **OS2MON /L:1:NEWDLL** The ACSNETB DLL will be NEWDLL.DLL and must be located in a LIBPATH directory.
- **OS2MON /O:C:\NETWARE\NETWARENEWDLL.DLL** The NETOEM DLL will be C:\NETWARE\NETWARENEWDLL.DLL.

## NetSentinel Configuration Reference

### Banyan Vines

#### Environments Supported

NetSentinel Server OS	Protocol	Server Module
DOS	NetBIOS	NSRVDN.EXE
Windows NT, Windows 95	NetBIOS	NSRVGX.EXE

#### Configuration Issues

If the key is not seen by a particular Banyan VINES client, you may need to increase the number of NetBIOS sessions and commands that are being allocated for that client station (minimum 8 sessions and 12 commands). Also, a NetBIOS name may need to be created on the Banyan server and the NetBIOS software support must be installed.

The following are the minimum requirements for configuring your Banyan network to allow successful execution of NetBIOS application:

- Log into a Banyan VINES server from any station sharing or accessing a NetSentinel key. The server must have previously created a NetBIOS name, using the MSERVICE utility.
- On each client using the NetBIOS name, the *AUTOEXEC.BAT* must be modified. Add a line after the BAN statement stating:  
  

```
SETNETB <NetBIOS service name>
```
- NetBIOS software support must be enabled on every client sharing or accessing the NetSentinel key. Run PCCONFIG.EXE, and select **3 - Special Software Settings**. Choose **1 - Load Resident NetBIOS Emulation software**, and set it to **Y (Yes)**.
- If you are running NSRVGX.EXE on Windows NT, you must install the Sentinel System Driver for Windows NT before starting the server.
- To increase the number of NetBIOS sessions and commands, run the PCCONFIG.EXE program. Choose **2 - Login Environment Options**. Choose **5 - Set Maximum NetBIOS Sessions** and set the value. On the system acting as the NetSentinel server, the minimum session value is 8. Press F10 to save and ESC to return to the Login Environment Options menu. Choose **6 - Set Maximum NetBIOS Commands** and set the value.

On the system acting as the NetSentinel server, the minimum command value is 12.

### Known Problems

NetSentinel has been designed to work on any standard NetBIOS implementation. However, it has been discovered that Banyan VINES' implementation of NetBIOS has problems that, under some circumstances, will cause the workstation where the security server is running to fail.

In addition, Banyan VINES versions 4.10 and later contain a problem that causes the VINES NetBIOS emulator to fail, displaying the message: "Fatal NetBIOS Emulation Error", or causing the workstation running the NetSentinel client or server to hang.

The Banyan error message is, according to Banyan, an indication that the workstation's memory has been corrupted.

Banyan VINES has officially notified Rainbow Technologies that they have resolved this NetBIOS problem. The fix for this problem is included in v5.53.6 of Banyan VINES, and is available to v5.52.5 users as user-installable patch DD-1.

If you wish to obtain the v5.53.6 update or DD-1 patch, you should contact your Banyan VINES reseller for assistance.

## IBM LAN Server/Requester 2.x and 3.x

### Environments Supported

NetSentinel Server OS	Protocol	Server Module
DOS	NetBIOS	NSRVDN.EXE
OS/2	NetBIOS, Named Pipes	NSRVOM.EXE

### Configuration Issues

On all systems acting as NetSentinel servers and clients, you should determine whether NetBIOS components of more than one network operating system are present. It is possible for components of two network operating systems to be present on the same computer.

For example, the IBM Communication Manager may be installed to provide asynchronous communications support, while LAN Manager is installed for LAN services. In this case, both ACSNETB.DLL (IBM NetBIOS) and NETAPI.DLL (IBM, Microsoft, and Novell) may be resident. This could cause a failure to properly initialize NetBIOS during server startup if the NetBIOS interface DLL used is not the correct DLL for the installed NetBIOS protocol stack.

To avoid possible problems, the OS/2 security server (NSRVOM.EXE) should be started with one of the following command-line parameters:

**/L:1** ACSNETB.DLL support for IBM LAN Server

**/L:2** NETAPI.DLL support for Microsoft LAN Manager and Novell NetWare

In the case where the system has two different vendor's versions of NETAPI.DLL installed, such as IBM LAN Manager and Novell NetWare, the OS/2 security server should be started with the appropriate switch and the path to the specific DLL to be used. For example,

```
NSRVOM /L:2 C:\NETWARE\NETAPI.DLL
```

To ensure that there will be an adequate supply of NetBIOS resources to support the NetSentinel Server(s) and Client(s), perform the following with the IBM LAN Server/Requester software:

- Configure your NetBIOS resources by selecting the Install/Config folder and then pressing the Advanced button.
- Select the Configure a Component option from the pop-up menu.
- Choose Adapter from the next menu, and you will be able to edit the fields that control the number of sessions, commands (NCBS), and NetBIOS names. Increase these as needed.

Under IBM LAN Server, a lack of resources can cause the NetSentinel server to fail to start NetBIOS. In some cases, the NetSentinel server runs; however, there are no resources remaining for the OS/2 Monitor (OS2MON.EXE). The workstation executes the program, but does not find the NetSentinel. Performing the following could help:

- Start the NetSentinel server using a small number of threads allocated for NetBIOS, such as:

```
NSRVOM /SN:1
```

- Increase the Sessions, Commands, and/or NetBIOS names as described above. The changes can also be made manually by modifying the PROTOCOL.INI file as follows:

```
Sessions=100
NCBS=100
```

The resources available for this workstation is the difference between the values in PROTOCOL.INI and IBMLAN.INI. For example, if PROTOCOL.INI is set for Sessions=100, and IBMLAN.INI is set for Sessions=40; then there are 60 sessions left for NetSentinel and other NetBIOS applications.

If you are using the OS/2 security server (NSRVOM.EXE), verify it loads completely. The message "NetSentinel Start-Up Complete" will appear.

In addition, do not Close or CTRL-C this process or the server will be stopped. However, minimizing does not stop the server.

## LANTastic

### Environments Supported

NetSentinel Server OS	Protocol	Server Module
DOS	NetBIOS	NSRVDN.EXE

### Configuration Issues

In a LANTastic network, access to the NetSentinel server can require up to two minutes when the NetBIOS client application is loaded on the same node as the NetSentinel security server.

Artisoft has released a new version of their NetBIOS driver for LANTastic that eliminates this problem. A copy of this new driver is available on the Artisoft bulletin board system.

Artisoft BBS telephone number: (602) 884-8646

Communication parameters: 96, N, 8, 1

NetBIOS driver file: contact Artisoft for the file name

## Microsoft LAN Server/Requester 2.0 and 2.1

### Environments Supported

NetSentinel Server OS	Protocol	Server Module
DOS	NetBIOS	NSRVDN.EXE
Windows NT, Windows 95	NetBIOS	NSRVGX.EXE
OS/2	NetBIOS, Named Pipes	NSRVOM.EXE

### Configuration Issues

On all systems acting as NetSentinel servers and clients, you should determine whether NetBIOS components of more than one network operating system are present. It is possible for components of two network operating systems to be present on the same computer.

For example, the IBM Communication Manager may be installed to provide asynchronous communications support, while LAN Manager is installed for LAN services. In this case, both ACSNETB.DLL (IBM NetBIOS) and NETAPI.DLL (IBM, Microsoft, and Novell) may be resident. This could cause a failure to properly initialize NetBIOS during server startup if the NetBIOS interface DLL used is not the correct DLL for the installed NetBIOS protocol stack.

To avoid possible problems, the OS/2 security server (NSRVOM.EXE) should be started with one of the following command-line parameters:

**/L:1** ACSNETB.DLL support for IBM LAN Server

**/L:2** NETAPI.DLL support for Microsoft LAN Manager and Novell NetWare

In the case where the system has two different vendor's versions of NETAPI.DLL installed, such as IBM LAN Manager and Novell NetWare, the OS/2 security server should be started with the appropriate switch and the path to the specific DLL to be used. For example,

```
NSRVOM /L:2 C:\NETWARE\NETAPI.DLL
```

To ensure that there will be an adequate supply of NetBIOS resources to support the NetSentinel Server(s) and Client(s), perform one of the following:

- Manually edit the PROTOCOL.INI file. You will find the NetBIOS parameters under the heading:

```
[NetBEUI_XIF]
```

The LAN Manager installation software does not place entries in the PROTOCOL.INI file for any NetBIOS parameters that are at default. You will need a copy of the LAN Manager documentation while editing this file.

Then, increase the NetBIOS sessions, commands, and/or maximum names.

- Or, run the LAPS utility to increase the maximum allowable value for any of the NetBIOS parameters mentioned above.

Verify that each client wishing to execute the application has started LAN Manager workstation services. To do so, run NET START WORKSTATION.

If you are running NSRVGX.EXE on Windows NT, you must install the Sentinel System Driver for Windows NT before starting the server.

If you are using the OS/2 security server (NSRVOM.EXE), verify it loads completely. The message “NetSentinel Start-Up Complete” will appear.

In addition, do not Close or CTRL-C this process or the server will be stopped. However, minimizing does not stop the server.

## Novell NetWare 3.x and 4.x

### Environments Supported

NetSentinel Server OS	Protocol	Server Module
DOS	IPX/SPX	NSRVDI.EXE
DOS	NetBIOS	NSRVDN.EXE
NetWare	IPX/SPX	NSRVNI.NLM
Windows NT	IPX/SPX, NetBIOS	NSRVGX.EXE
Windows 95	IPX/SPX, NetBIOS	NSRVGX.EXE
OS/2	NetBIOS, Named Pipes	NSVROM.EXE

NOTE: If you are using the IPX/SPX protocol under Windows 95, you must install Microsoft’s NWLINK IPX software patch. You will be prompted to install this patch when you are running the SLOPE/W Setup program or the Network Software Setup program.

### Configuration Issues

Current versions of the NetWare DOS and Windows drivers should be used. The DOS drivers are available from Novell, CompuServe (in the files VLMUP3.EXE and NET33X.EXE); or your network card manufacturer. The minimum version required for IPX.COM is at least 3.10, IPXODI.COM is at least 1.20, and NETX.EXE is at least 3.26.

If the GEO-SLOPE software cannot find the NetSentinel key and returns an error message of –19, then you should update each NetSentinel server and client workstation with the above mentioned drivers.

If ODI drivers are utilized, verify IPXODI.COM is not being started with any arguments. Specifically, issuing the command, IPXODI /A, disables SPX services and will prevent the GEO-SLOPE software from successfully accessing the NetSentinel.

You may use PSERVER to share a printer that is connected to a port with a shared NetSentinel key, but PSERVER must not use interrupts. To not use interrupts, run PSERVER <printserver>, and in the configuration stating Use Interrupts? (Y/N), select N for “No”, then save the configuration.

## Windows for Workgroups 3.11 (NetBEUI)

### Environments Supported

NetSentinel Server OS	Protocol	Server Module
DOS	NetBIOS	NSRVDN.EXE

### Configuration Issues

Attaching the NetSentinel security key to a computer running Windows for Workgroups requires you to run the NSRVDN.EXE security server in DOS before starting Windows. To do so, you must add one of the following statements to your AUTOEXEC.BAT file:

- **NET START NETBEUI** Workstation can share its files and printers, but cannot connect to other shared files and printers.
- **NET START FULL** or **NET START WORKSTATION** Workstation cannot share its files and printer, but can connect to other shared files and printers.
- **NET START BASIC** Workstation cannot share its files and printers. It can connect to shared files and directories using the NET USE command at the DOS prompt outside Windows for Workgroups.

Due to the above limitations, it is highly recommended that you run the NetSentinel security server on a computer other than the Windows for Workgroups server.

The “IPX/SPX Compatible Transport with NetBIOS” or “IPX/SPX Compatible Transport” protocol must NOT be loaded. The system will hang when the NetSentinel application checks the IPX/SPX for a NetSentinel key.

To eliminate these limitations, an alternative approach is to execute the NetSentinel server (NSRVDN.EXE) in a Windows for Workgroups DOS box.

#### ➤ To run NSRVDN.EXE in a Windows for Workgroups DOS box:

1. Start Windows for Workgroups.
2. Run NSRVDN.PIF to create a DOS box.

NSRVDN.PIF is located in the same directory as NSRVDN.EXE. It contains the appropriate settings for running NSRVDN.EXE under Windows for Workgroups.

3. Run NSRVDN.EXE inside the DOS box.

---

NOTE: SLOPE/W Version 4 (or higher) *cannot* be run under Windows for Workgroups; SLOPE/W can only be run under Windows 95 or Windows NT. Only the security server and security monitor programs can be run under Windows for Workgroups.

---

## Windows NT / Windows NT with Novell NetWare

### Environments Supported

NetSentinel Server OS	Protocol	Server Module
Windows NT	NWLink/IPX, NetBIOS, TCP/IP	NSRVGX.EXE
Windows NT	NWLink/IPX, NetBIOS, TCP/IP	NSSERVICE.EXE

### Configuration Issues

The Windows NT 32-bit server can be run as an Application (NSRVGX.EXE) or as an NT Service (NSSERVICE.EXE). The advantage of running the NT Service is that NSSERVICE.EXE is automatically started whenever the Windows NT operating system is started. There is no need to log on to Windows NT to start the security server, and the server will not be stopped when you log off from Windows NT. For information on installing NSSERVICE.EXE, see the Running the NetSentinel Service Security Server under Windows NT section in this chapter.

If you wish to run NSRVGX.EXE, however, and have it automatically load during booting, you can configure your system in the following way:

1. Add the value AutoAdminLogon: DWORD:1 to the following key in the Registry Editor by using REGEDT32.EXE:

HKEY\_LOCAL\_MACHINE - SOFTWARE - Microsoft - Windows NT - Current Version - Winlogon

To add the value from the Settings/Control Panel/Network Icon, select Edit, New, DWORD value.

2. Verify the value for DefaultUserName and DefaultPassword. To verify from the Settings/Control Panel/Network Icon, select Edit, New, String Value. If there are no values, add them.

This will automatically log the user in. Place the NSRVGX.EXE in the STARTUP folder and the system should automatically load the server on every re-boot.

If the GEO-SLOPE application and the Win32 NetSentinel server are running on the same workstation, then the TASKING option of CONTROL PANEL's SYSTEM applet must be configured as "Foreground and Background Applications Equally Responsive" to avoid task scheduling problems.

The Windows NT Sentinel System Driver must be installed on the computer running the Win32 security server program. This driver is installed from the GEO-SLOPE distribution CD-ROM.

---

NOTE: For information about TCP/IP support, see the Using TCP/IP with Windows 95 and NT section in this chapter.

---

### Known Problems

Due to an incompatibility between NWLink/IPX's router packet definition and Novell's routing software, it is impossible at this time to access a NetSentinel server across a Novell router. Novell and Microsoft are currently investigating this issue.

## Windows 95 / Windows 95 with Novell NetWare

### Environments Supported

NetSentinel Server OS	Protocol	Server Module
Windows 95	NWLink/IPX, NetBIOS, TCP/IP	NSRVGX.EXE

### Configuration Issues

Currently, the Windows 95 server only *officially* supports the NetBIOS/NetBEUI and TCP/IP protocols.

Rainbow Technologies has implemented IPX/SPX support in the Windows 95 server, and is actively working with Microsoft to overcome issues with Windows 95, multi-threaded applications, and IPX/SPX. Recently, Microsoft released a Windows 95 Beta patch, NWLNKUPD.EXE, that seems to correct these issues. You are prompted to install this patch when you install the GEO-SLOPE application software from the distribution CD-ROM. This patch also seems to resolve issues with multi-threaded applications (like the NetSentinel client) running on Windows 95 utilizing the IPX/SPX protocol.

Installation of Novell's Windows 95 drivers seems to help as well, but does not completely resolve all the issues. We recommend installation of the NWLNKUPD.EXE patch instead.

---

NOTE: Unlike Windows NT, the Sentinel System Driver does *not* have to be loaded to run the Windows 95 server (NSRVGX.EXE).

---

To use the Windows 95 security server with the TCP/IP protocol, the TCP/IP protocol must be installed on the workstation acting as the NetSentinel server. From the Settings/Control Panel/Network Icon, verify that TCP/IP is listed as a protocol. If not, select Add, highlight Microsoft, add TCP/IP and click OK. A Standard Windows 95 installation does not install the TCP/IP Protocol stack by default. You must install this service.

---

NOTE: For information about TCP/IP support, see the Using TCP/IP with Windows 95 and NT section in this chapter.

---

## Using TCP/IP with Windows 95 and NT

SLOPE/W Version 4 can use the TCP/IP protocol to connect to one of the Win32 NetSentinel security servers (i.e., NSRVGX.EXE or NSSERVICE.EXE). You will need to install TCP/IP on both the client computer and the security server computer. If you are using a non-Win32 security server, such as NSRVDN.EXE or NSRVDI.EXE, you cannot use TCP/IP to find the security server; instead, you will need to install additional protocols, such as NetBIOS or IPX/SPX.

By default, when SLOPE/W uses TCP/IP, it will only search for the NetSentinel security server on its local subnet. Your *local subnet* is defined by masking your computer's IP address with its subnet mask. For example, if your computer has an IP address of 192.9.100.1 and a subnet mask of 255.255.255.0, the local subnet will consist of all addresses starting with 192.9.100. If you designate your computer as the NetSentinel security server, SLOPE/W can be run from any other computer on this local subnet (e.g., from a computer with an IP address of 192.9.100.7 and a subnet mask of 255.255.255.0).

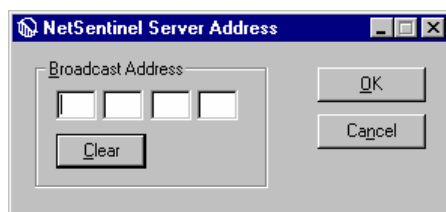
This default configuration is appropriate for most networks, which typically have the security server and the client computers on the same network segment. However, if one of your client computers is on a different subnet, you will not be able to run SLOPE/W using the default TCP/IP settings. For example, if your client computer has an IP address of 192.9.101.7 and a subnet mask of 255.255.255.0, its subnet is 192.9.101; it will not be able to find the NetSentinel security server, since it is on a different subnet.

In this case, you must override the default TCP/IP settings and specify either a *unicast address* or a *directed broadcast* on the client computer. A *unicast address* is simply the IP address of the NetSentinel security server. If you specify a unicast address, SLOPE/W will only check this IP address when it looks for the security server. You should use this option if you know that the IP address of the security server will not change.

If you specify a *directed broadcast* on the client computer, SLOPE/W will search for the NetSentinel security server on a particular subnet. A directed broadcast consists of the subnet address followed by all 1's (in binary). For example, if you wish to search for the security server on the 192.9.100 subnet, you should specify a directed broadcast address of 192.9.100.255. The advantage of using a directed broadcast is that you can move the security server to any computer on the specified subnet; it will still be found by SLOPE/W, because you are specifying the subnet to search, not the exact IP address. In this example, the security server could be any computer on the 192.9.100 subnet, such as 192.9.100.7 or 192.9.100.145.

### ➤ To specify a unicast address on the client computer:

1. On the client computer, run `\OfficeV4\Network\Tcpip\ServAddr.exe` from the GEO-SLOPE Office CD-ROM. The following window appears:

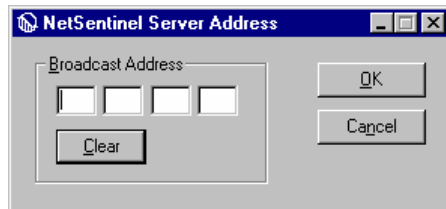


2. In the Broadcast Address edit boxes, type the IP address of the NetSentinel security server computer.
3. Select OK. The broadcast address is stored in the Windows Registry under the keyword \HKEY\_LOCAL\_MACHINE\SOFTWARE\GEO-SLOPE\MRUSystem\NetSentinel-TCPIP-BroadcastAddr.

When you run SLOPE/W, it will look for the security server at this IP address.

➤ **To specify a directed broadcast on the client computer:**

1. On the client computer, run \OfficeV4\Network\Tcpip\ServAddr.exe from the GEO-SLOPE Office CD-ROM. The following window appears:

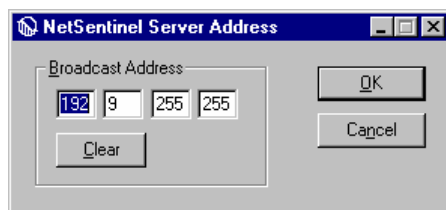


2. Type the broadcast address that you want SLOPE/W to use when it searches for the NetSentinel security server. For example, to search on the 192.18 subnet, type 192.18.255.255 as the broadcast address.
3. Select OK. The broadcast address is stored in the Windows Registry under the keyword \HKEY\_LOCAL\_MACHINE\SOFTWARE\GEO-SLOPE\MRUSystem\NetSentinel-TCPIP-BroadcastAddr.

When you run SLOPE/W, it will perform a directed broadcast to this subnet in order to find the security server.

➤ **To return to the default TCP/IP settings (i.e., to broadcast to the local subnet):**

1. On the client computer, run \OfficeV4\Network\Tcpip\ServAddr.exe from the GEO-SLOPE Office CD-ROM. The following window appears, containing the current broadcast address:



2. Select the Clear button to remove the broadcast address.
3. Select OK to return to the default TCP/IP settings. The broadcast address keyword \HKEY\_LOCAL\_MACHINE\SOFTWARE\GEO-SLOPE\MRUSystem\NetSentinel-TCPIP-BroadcastAddr is deleted from the Windows Registry.

When you run SLOPE/W, it will perform a broadcast to its local subnet in order to find the security server.