Network Installation Troubleshooting

The difference between the stand alone and the network version of Micro-Cap is how the license security is installed and accessed. Rather than connecting a dongle to the local computer, the network version of Micro-Cap lets the dongle be placed on the server. This dongle, in conjunction with the license manager software which is also installed on the server, controls the number of simultaneous users of Micro-Cap. For example, if a 3 seat LAN version was purchased, then a maximum of three users can access Micro-Cap at the same time. While installing the latest HASP device driver will fix nearly every security issue on the stand alone version, the network version has more points at which a security issue can arise. This article will provide a guide on how to troubleshoot possible security issues on a network installation. Since the most common network protocol in use currently is TCP/IP, the focus of this article will be on troubleshooting a network with such a protocol.

When Micro-Cap is launched on the client, the first thing the program will check is to see which protocols are installed on the system. The client will then send out a login request whose format will be dependent upon which protocols are available. Once the license manager on the server receives the login request, it will check to see if the correct dongle is attached to the server. If the correct dongle is present, the license manager will make sure that there is at least one free license available for Micro-Cap. If the login can not be validated, such as when all the licenses are currently in use or the dongle is not available on the server, the license manager will return an error. Otherwise, the license manager will record the user that logged in, and Micro-Cap will be able to start on the client system.

For the network version, the security problem may arise on either the server or the client. While there are no hard rules to determine which computer is causing the problem, there are a couple of ways to indicate where the problem most likely resides. First of all, if any of the clients can run the Micro-Cap software then the problem most likely is occurring on the client system that is unable to run Micro-Cap. If all clients are unable to run the program, it is a good chance that the server is the origin of the problem. The second indication is through the error message that is returned when Micro-Cap is unable to start. One of two error messages are likely to appear. Either, the "Can't find the NetHASP Server" error, shown in Figure 1, or the "Security key missing. Please replace the key" error will be invoked. While not as good of an indicator as the first method, generally the NetHASP error means that the client is unable to find the license manager software, and the security key error means that the HASP license manager is found but there is not a valid dongle associated with it.

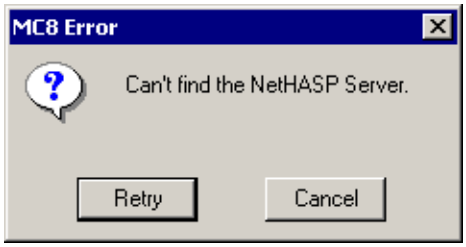

Fig. 1 - Security error message

Server
The security installation on the server is rather simple. The hardware dongle should plug into either the parallel port or the USB port depending on the type of dongle that was purchased. If the server is running an older Windows operating system such as Win9X or WinNT, the HASP device driver should be installed. Finally, the license manager must be installed. If the server is the suspect in the security problem, try the following steps:

1) Make sure that the license manager software (also the HASP device driver if used) is the latest version. The latest version can always be found on Aladdin's website at http://www.aladdin.com. Install the newest version if necessary.

2) It is quite rare for the dongle to fail, but it is a possibility. Try attaching the network dongle directly to one of the client systems that has Micro-Cap installed on it. The client system must have the HASP device driver installed for this test. Try to run Micro-Cap. This will run Micro-Cap as a stand alone version rather than a network version. It is possible that the portion of the key that just controls the network security capability has failed. However, we have never encountered this situation.

3) One other issue that can occur with a Windows server is that the clients have sporadic access to the license manager. At times, Micro-Cap will launch without a problem and at other times, attempts to start the program will return one of the two security login errors. This is usually caused because the license manager has been installed as an application on the server. If the user whose profile the license manager was installed into logs out, the clients will not have access to the license manager as it will no longer be running. The way to solve this problem is to install the license manager as a service instead. The best method to do this is to run the LMSETUP.EXE file which installs the license manager. During the installation process, one of the screens will ask whether the license manager should be installed as an application or as a service. Installing the license manager as a service ensures that the license manager is available to clients even when no one has logged onto the server.

Client
On the client system, the most common configuration is installing the Micro-Cap software on the local drive. The only other component that should be installed on the client is the HASP device driver which will be placed on the system during the course of the normal Micro-Cap installation. The client is typically the failure point for the security problem. There are a number of possible reasons for a failure. Some of them are that the client is unable to see the server that the license manager is located on, the network login request times out before the license manager can be found, or the communication path between the client and server is blocked. If the client is the suspect in the security problem, try the following steps:

1) Try to ping the server. Ping is a network utility that provides a basic test to see if the system being pinged is both operating and accessible from the client. In order to use this utility, the IP address of the server would need to be known. On the client system, open a DOS Command Prompt window. Once the prompt appears, type in the following:

ping <address>

where <address> would be an IP address such as 243.212.54.41. When successful, the ping utility will return a reply from the pinged system which includes the round trip time and packet loss rate. Should the pinged system not be found, the response will say that the request has timed out. If the

system with the license manager can not be pinged from the client, Micro-Cap will be unable to run on that client.

2) Install and run the Monitor program from Aladdin. The installer for the Monitor program can be found on the Micro-Cap CD under the LAN Monitor folder. The Monitor program allows centralized administration of any NetHASP license managers that are installed on the network. A sample screen shot of the Monitor program is displayed in Figure 2. In this figure, a single NetHASP license manager has been found and is displayed underneath the NetHASP LM category. Selecting a license manager item in this category displays the name and address of the computer that the license manager is located on. If no items appear under the NetHASP LM category, then the client is currently unable to see the license manager.

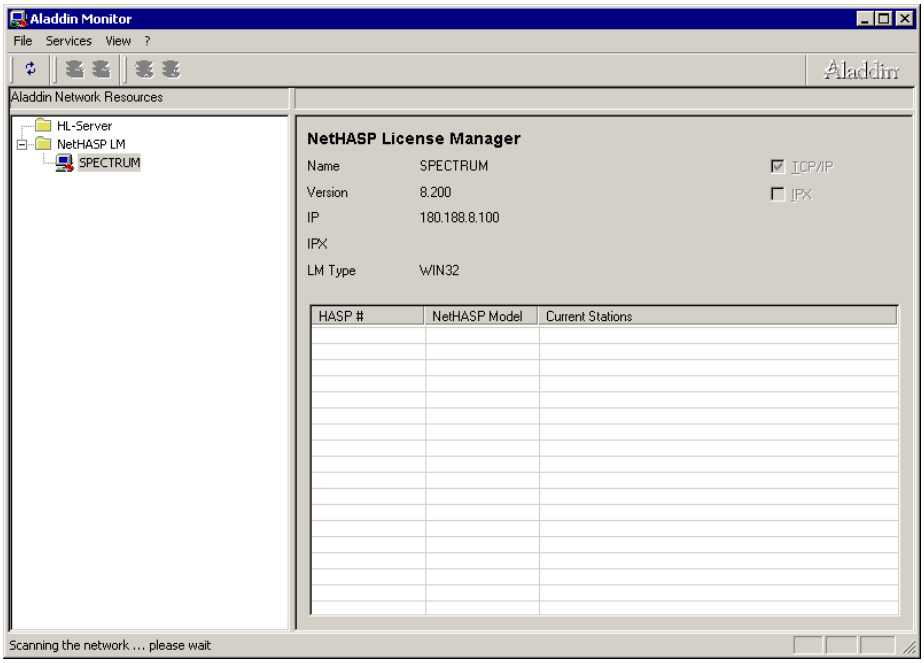

Fig. 2 - Aladdin Monitor program

The Monitor program is also useful if Micro-Cap returns an error about an old license manager being installed on the network. This program would show the location of the other license manager that Micro-Cap is finding. In this case, the older license manager should either be updated or the Nethasp.ini file, which will be described below, should be used with Micro-Cap.

3) Add the Nethasp.ini file to the folder where the Micro-Cap executable is located. This file is a configuration file for the client that specifies how it will communicate with the license manager on the server. Rather than sending the login request throughout the network, this text file lets a specific server address be defined to which the login request will be made. This file is also useful if the load time for Micro-Cap is adversely affected by the search for the license manager. One technique that Aladdin recommends is using the Nethasp.ini file in the same folder as the Monitor program and then make the appropriate edits in the file. As soon as the Monitor program can see the license manager, then just copy the Nethasp.ini file over to the folder that the Micro-Cap executable is located in. The standard Nethasp.ini file for TCP/IP communication is shown as follows. Simply fill in the server address for the NH_SERVER_ADDR entry. Basic templates for the IPX and NetBios protocols can be found on Aladdin's website.

```
[NH_COMMON]
NH_TCPIP = Enabled;                    ; Use the TCP/IP protocol

[NH_TCPIP]
NH_SERVER_ADDR = xx.xx.xx.xx;          ; IP addresses of all the NetHASP
                                       ; License Managers you want to search.
                                       ; Unlimited addresses and multiple
                                       ; lines are possible.
                                       ; Possible address format examples:
                                       ; IP address:       192.114.176.65
                                       ; Local Hostname:   ftp.aladdin.co.il

NH_TCPIP_METHOD = UDP                  ; Send a TCP packet or UDP packet
                                       ; Default:  UDP

NH_USE_BROADCAST = Enabled             ; Use TCP/IP Broadcast mechanism.
                                       ; Default:  Enabled
```

4) In the Nethasp.ini file, set the NH_USE_BROADCAST entry to Disabled. This setting disables the TCP/IP broadcast mechanism. This is most helpful if the client is on a different subnet or domain then the server.

5) Verify that the communication port (475) to the license manager is open and not blocked by a firewall. On the client system, open a DOS Command Prompt window. Once the prompt appears, type in the following:

telnet <ip address> 475

where <ip address> is the IP address of the server where the license manager is located. If working, the DOS window will be cleared. Pressing any key will return the message "Connection to host lost". If port 475 is blocked, the message "Could not open a connection to host on port 475 : Connect failed" will appear. The port would then need to be opened to enable communication between the client and the license manager.

6) Increase the timout value in the Nethasp.ini file. The default initial search period for the NetHASP algorithm is two seconds. This search period can be extended by adding the following text into the [NH_COMMON] section of the Nethasp.ini file:

NH_SESSION=<seconds>

where <seconds> is the new value for the initial search.

7) Reboot the client. We have found in a couple of cases that after making some of the above changes, a reboot of the client system solved the security problem. While it typically should not be necessary to do this, apparently the HASP software may keep some of the communication settings in memory so a reboot will clear those.