Understanding the Host Integration Server Client

**Abstract**: This white paper discusses the Microsoft® Host Integration Server (HIS) Client. Topics include the installation and configuration of the HIS Client as well as details around some of the underlying HIS client/server architecture and how HIS resources are located by the HIS Client. In addition, some guidance is given around best practices for the HIS Client.

**Author**: Stephen Jackson, Principal Escalation Engineer, Microsoft Host Integration Server Support

**Technical Reviewer**: Chris Houser, Senior Program Manager, Microsoft Host Integration Server

Contents

[Introduction 3](#_Toc232944877)

[Host Integration Server Client 3](#_Toc232944878)

[Installation 3](#_Toc232944879)

[Configuration 7](#_Toc232944880)

[Common Settings 7](#_Toc232944881)

[Data Integration 11](#_Toc232944882)

[Best Practices 12](#_Toc232944883)

[Client/Server Interface 13](#_Toc232944884)

[Sponsor Clients 13](#_Toc232944885)

[Active Directory Clients 16](#_Toc232944886)

[Service Table 20](#_Toc232944887)

[HIS Client Logon 22](#_Toc232944888)

[NTLM 23](#_Toc232944889)

[Kerberos 23](#_Toc232944890)

[Load Balancing/Fault Tolerance (Client Side) 25](#_Toc232944891)

[Load Balancing 3270/LUA LUs Across HIS Servers 26](#_Toc232944892)

[Load Balancing APPC (LU 6.2) Sessions Across HIS Servers 27](#_Toc232944893)

[Fault Tolerance 29](#_Toc232944894)

[Resource Location 30](#_Toc232944895)

[3270/LUA Resource Location 30](#_Toc232944896)

[APPC/CPI-C Resource Location 33](#_Toc232944897)

[APPC Application Uses a Specific Local APPC LU Alias 34](#_Toc232944898)

[APPC Application Specifies a “Blank” Local APPC LU Alias 35](#_Toc232944899)

[Encryption 37](#_Toc232944900)

[Conclusion 39](#_Toc232944901)

[Copyright 40](#_Toc232944902)

# Introduction

The Microsoft® Host Integration Server (HIS) Client software provides the basis that allows SNA applications to communicate with HIS Server-side services for IBM host system integration. The following are the key components that make up the HIS Client:

* **SNADMOD.DLL and transport DLLs** – Provide the network communication facilities between the HIS Clients and HIS Servers.
* **SnaBase** – Used to communicate with the SnaBase services on HIS Servers to allow HIS Clients to locate resources available to the client and its SNA applications.
* **HIS API DLLs** – The API DLLs provide the HIS clients and servers the ability to support various SNA application types that include APPC, CPI-C, LUA (SLI & RUI), and 3270 EIS (or FMI) applications.

The purpose of this white paper is to provide details regarding the installation, configuration, and functionality of the HIS Client. The goal is to provide HIS administrators with details about how the HIS Client interacts with the resources (3270 LUs, APPC LUs, etc.) defined on HIS Servers. Topics that are covered include installation, configuration, resource location, load balancing, fault tolerance, data encryption, and client authentication as well as some best practices.

The information included is generally specific to Host Integration Server 2006 and Host Integration Server 2009. However, the majority of the information also applies to Host Integration Server 2004. In fact, much of the core functionality has been in the product since the product line began as SNA Server.

 Any information that does not apply to a specific version of Host Integration Server will be explicitly identified.

**Intended Audience**

This information is intended for HIS administrators or other users that have some knowledge of Microsoft Host Integration Server.

# Host Integration Server Client

## Installation

**Software Requirements for the HIS 2006 Client**

* Microsoft Windows® 2000 Service Pack 4 or later, together with Update for Microsoft Windows 2000 KB821887 hotfix
* Microsoft Windows XP Professional with Service Pack 1 or later
* Microsoft Windows Server® 2003 (x86 or x64), Windows Server 2003 R2 (x86 or x64)

**Software Requirements for the HIS 2009 Client**

* Microsoft Windows Vista® SP1 (x86 or x64)
* Windows XP Professional SP2 (x86 or x64)
* Windows Server 2008 (x86 or x64)
* Windows Server 2003 R2 SP2 (x86 or x64)
* Windows Server 2003 SP2 (x86 or x64)
* Virtualization with Hyper-V

**Note:** An actual check for the installed operating system has been removed from the installation process; however, the general guidelines for supportability and usage are the HIS Client on a Client OS and the HIS Server on a Server OS.

HIS 2006 and HIS 2009 include a single Setup.exe process that detects the underlying processor architecture (x86 or x64) in order to install the correct version of the HIS Client.

The HIS 2006 and HIS 2009 Client is installed based on selecting the **Client** component on the **Component Installation** page.

**HIS 2006**



**HIS 2009**



The HIS Client components that are needed will depend on your specific needs. The base Client component will install everything that is needed for an HIS Client to communicate with an HIS Server. This includes the HIS client/server interface (SnaBase, SnaDMOD) and the SNA APIs (EIS, APPC, CPI-C, LUA). The other components are explained here and can be installed as needed:

* **Administration** (**Administration Tools** in HIS 2009) – Tools used for remote administration of the SNA Gateway components on HIS Servers. This includes the SNA Manager MMC snap-in used to create, secure, and manage a set of SNA services, including connections to IBM mainframes and iSeries (AS/400) computers supporting terminal and printer sessions.
* **Data Providers** - Data access providers for integrating vital data stored in DB2 databases and host file systems with new solutions running on Windows computers. This includes the OLE DB Provider for DB2, the OLE DB Provider for AS/400 and VSAM, the Managed Provider for DB2, and the ODBC Driver for DB2.
* **Emulators** - Windows 3270 and 5250 terminal emulation clients for accessing IBM mainframe and AS/400 applications.
* **Enterprise Single Sign-On Administration** (**Single Sign-On Tools** in HIS 2009) - Administration and client tools for managing and connecting to Enterprise Single Sign-On Services.

## Configuration

After setup finishes the installation of the HIS Client components, an option is enabled by default to run the HIS configuration tool. The configuration tool (Configuration.exe) is used to configure the HIS Client so that it can locate and connect to the HIS Servers in the HIS subdomain.

There are two main sections in the configuration tool for HIS Clients: **Common Settings** and **Data Integration**. The options are the same for the HIS 2006 and HIS 2009 Clients.

### Common Settings

Under **Common Settings**, you will configure the following configuration options:



* **Security Group** – These are the two groups used by Host Integration Server to secure access to HIS objects, such as the HIS installation files/folders, HIS registry keys, and HIS services. The HIS Runtime Users group will contain the HIS service account by default. The HIS Administrators group will contain the user account of the user that launched the configuration tool and the Network Service account. The group names are populated with default names (HIS Runtime Users and HIS Administrators), but they can be changed. These groups can be either local or domain groups. If local groups are specified, they will be created by the configuration tool if they do not exist. Domain groups must be pre-existing.
* **Enable Support for 3270, APPC, and LUA Applications –** This option is used to indicate if the HIS Client will support 3270, APPC, and LUA applications. If this option is enabled, the resource location options are made available to allow the client to be configured to communicate with HIS Servers.
* **Resource Location** – The resource location options determine how the HIS Client will locate available HIS Servers in the HIS subdomain.
	+ **Sponsor Server Support**: If this option is chosen, you will enter the server name or TCP/IP address of one or more HIS Servers that you want the client to use as sponsor servers. Multiple servers should be separated by a comma. Please refer to the Sponsor Client section under Client/Server Interface for details on how sponsor clients locate HIS Servers.

**Note**: If you enter a server name here, the name will have to be resolved to a TCP/IP address. If you have problems connecting to a sponsor server, you might try entering the server’s TCP/IP address to rule out a name resolution issue.

* + **Active** **Directory Support**: If this option is chosen, you will enter one or more Organizational Units (OUs) that the HIS Client will use to locate HIS resources. A maximum of five OUs can be entered for the client. Please refer to the Active Directory section under Client/Server Interface for details on how Active Directory clients locate HIS resources.
* **Windows Service** – This is where you specify the user account that the SnaBase process will run under if it is configured to run as a Windows service. This user account has to be manually created as a regular user account. It does not require administrative privileges. The HIS configuration process will add the **Generate Security Audits** and **Log on as a service** user rights to the account. The service account will be added to the HIS Runtime Users group that is configured during the HIS configuration process.
* **Resource Location Advanced Settings --** The following advanced configuration options are available by clicking the **Advanced** button:



* **Terminate Sponsor** – If this option is selected, SnaBase will terminate the sponsor connection after the specified number of seconds after all of the SNA applications are closed. If this option is not selected, the sponsor connection will be kept open until SnaBase is terminated. This option only takes effect when SnaBase is started by an SNA application (e.g. 3270 emulator). It doesn’t apply if SnaBase is started manually.
* **Update list dynamically** - When the client opens a sponsor connection to the server, it receives a list of all the sponsor servers running in the subdomain. If this configuration option is chosen, the client SnaBase will automatically save the names of these other servers whenever the sponsor connection is opened. This option, along with **Select Random Sponsor**, allows HIS Clients to randomly distribute the sponsor connection traffic to all HIS Servers in the subdomain, even if the clients are originally configured with a single HIS Server during initial client configuration.
* **Select Random Sponsor** - If there is more than one sponsor server name listed and this option is chosen, the HIS Client will randomly select a server from this list, instead of trying the servers in the order that they're configured. Assuming that all clients may enumerate the same list of sponsor servers, this feature allows clients to "randomize" the server choice in order to evenly distribute client sponsor connection load across more than one HIS Server.
* **Accept Backup Sponsors** - SNA Manager allows the administrator to centrally define the backup sponsor servers for the subdomain. When an HIS Client establishes a sponsor connection to the server with this option selected, the client automatically saves this backup information into its local registry in the following key under:

**HKEY\_LOCAL\_MACHINE \Software\Microsoft\SnaBase\Parameters:**

**BackupSponsors : REG\_MULTI\_SZ:**

**Note**: If SnaBase is configured to run as a Windows service, the registry entry will be under **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnaBase\Parameters**

If SnaBase is unable to connect to any of the sponsor servers in its configuration, then the BackupSponsors are tried.

* **Run resource location component as an application** – If this option is selected, the SnaBase process will run as an application instead of as a Windows service.
* **Allow per user settings** – This option allows users to specify configuration options that will only apply to their account. This option is only available when the **Run resource location component as an application** option is enabled. If this option is enabled, the HIS Client configuration options will be written to and read from the registry keys under **HKEY\_CURRENT\_USER\Software\Microsoft\SnaBase**. If this option is not enabled, the HIS Client configuration options will be written to and read from **HKEY\_LOCAL\_MACHINE\SOFTWARE\ Microsoft\SnaBase** when SnaBase is running as an application or **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnaBase** when SnaBase is running as a Windows service.
* **Use the credentials of** – This option is used to determine the user credentials that will be passed from the HIS Client to the HIS Server for authentication. If **Logged On User** is selected, the Windows credentials of the logged on user are passed to the HIS Servers for authentication. If **This Account** is selected, you can specify a specific set of credentials that will be passed to the HIS Servers for authentication.

If you choose the **This Account** option and you enter a user name and password in the User Credentials dialog box, the values entered will be written to the registry in the following location:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SnaBase\Parameters**

The registry entry locations are as follows:

* + **Password, REG\_Binary**
	+ **UserName, REG\_SZ**
	+ **LogonDomain, REG\_SZ**

**Note**: If the specified credentials are for a user account defined in the local Windows Domain or a Trusted Domain, the password will be encrypted and written to the Password registry parameter. If the specified user account is for a non-trusted domain, the password will not be stored in the registry. The result will be that the user will be prompted to enter the password for the specified user account each time the SnaBase process starts. This occurs because the HIS configuration process attempts to verify whether the specified user account has administrative privileges. If this check fails, the password is not stored in the registry. It is not recommended to use an account that has administrative privileges for security purposes.

### Data Integration

Under **Data Integration Settings**, you will configure the following configuration options:



* The **Enable Data Integration Feature** and **Enable Host Files component (DDM) as a service** options need to be enabled if you plan on using the OLE DB Provider for AS/400 and VSAM. When the **Enable Host Files component (DDM) as a service** option is enabled, you will need to specify the user account that the SNA DDM service will log on as. This can be the same user account that is used for SnaBase if you configured SnaBase to run as a Windows service.

## Best Practices

* Use **Sponsor Server Support** resource location unless you have a need to use one of the features that **Active Directory Support** resource location provides, such as LU accumulation across OUs. The sponsor server resource location functionality has been designed to provide an efficient mechanism for locating available HIS resources in the subdomain. Sponsor server resource location has been implemented by the vast majority of customers that use Host Integration Server.
* When using **Sponsor Server Support** resource location, configure multiple sponsor servers on each HIS Client. This allows the clients to connect to a sponsor server even if one (or more) of the HIS Servers are unavailable. In addition, it allows the sponsor connections to be distributed across multiple HIS Servers to prevent any one HIS Server from having to process the entire sponsor connection work. You can achieve the same result in a dynamic fashion by enabling the **Update list dynamically** option in the HIS Client configuration. If this option is enabled, the HIS Client will be automatically updated with the names of all the HIS Servers in the subdomain dynamically. This also allows the HIS Clients to use new HIS Servers added to the HIS subdomain as sponsor servers without any configuration changes on the HIS Client systems.
* If the HIS Clients are configured with multiple sponsor servers or with **the Update list dynamically** option enabled, you should also enable the **Select Random Sponsor** option. The random sponsor option allows each HIS Client to randomly choose which sponsor server to use when the SnaBase process starts, which results in a load balancing of sponsor connections. If each HIS Client randomly chooses a sponsor server, the odds are that the sponsor connections will be distributed among the HIS Servers more evenly than they would be if the random sponsor option is disabled.
* Run the SnaBase process as an application by enabling the **Run resource location component as an application** option unless you have a requirement to run SnaBase as a Windows service. One reason to run SnaBase as a Windows service is if the SNA applications that you will be using on HIS Client systems are also running as Windows services. The following are benefits of running SnaBase as an application:
	+ Users can stop and start applications as needed, but many users don’t have the necessary privileges to start Windows services. If SnaBase is running as a service and it terminates for some reason, the user may need to restart their system to have the service started.
	+ You can use the **Terminate Sponsor** option to have SnaBase terminate when the running SNA applications are terminated in order to save system resources when SnaBase is not needed.
* Make sure that the **Use client/server encryption** option is enabled for all users and groups configured in SNA Manager. This option is automatically enabled by default for each user or group added to SNA Manager. The use of encryption hasn’t impacted performance to any extent that has been noticeable by HIS customers.
* Use Kerberos authentication where possible to maximize security.

## Client/Server Interface

### Sponsor Clients



HIS Clients configured to use sponsor servers for resource location utilize two LAN sessions. The first LAN session is used for the sponsor connection and the second is used for the application session. The sponsor connection is the first TCP/IP connection an HIS Client makes to an HIS Server. The sponsor connection uses TCP port 1478 by default. The application connection is used for connections to the SNA Server service and it uses TCP port 1477 by default.

HIS Clients can be a member of only a single HIS subdomain at a time. If you want to have the HIS Client connect to a different HIS subdomain, you need to reconfigure the client to specify a sponsor server(s) from that other subdomain.

**Note**: HIS Servers include HIS Client functionality so that you can run SNA applications on HIS Server systems. However, SNA applications running on HIS Servers will only be able to access resources (LUs) that exist in the HIS subdomain that the HIS Server is a member of. In other words, SNA applications running on HIS Servers will not be able to access LUs that exist in other HIS subdomains that might exist in the environment.

#### Sponsor (SnaBase) Connection

* A connection between the client SnaBase and the server SnaBase. SNA Server clients prior to Host Integration Server 2000 used a persistent sponsor connection. Since Host Integration Server 2000, HIS Clients have been updated to utilize an On Demand (dynamic) sponsor connection.

**Note**: The On Demand sponsor connection did not work with the initial release of HIS 2006. A hotfix was released to correct the problem. The hotfix was included in HIS 2006 Service Pack 1.

The On Demand sponsor connection works just like persistent sponsor connections, but the network connection is closed after five minutes of inactivity. HIS Clients will disable the use of On Demand sponsor connections under the following circumstances:

* + An invokable APPC/CPI-C TP (Transaction Program) is running on the client.
	+ SNA Manager is running on the client.
	+ The SNA LU 6.2 Resync TP service is running on the HIS 2000 Administrator client.

Under these conditions, the client will use a persistent sponsor connection. Once the On Demand sponsor connection is closed, it will only be reopened by SnaBase if it needs to send a request (i.e., to locate which HIS Servers support the requested SNA resource). It will update its service table whenever the connection is reopened. The sponsor connection will be closed again after the five-minute time-out expires.

**Notes:**

1. An HIS Client will use an On Demand sponsor connection until it detects one of the conditions listed previously. Therefore, it will automatically switch to a persistent sponsor connection once an invokable TP or SNA Manager is started.
2. There is no way to disable the use of the On Demand sponsor connection.
* The initial client connection to a Host Integration Server in a subdomain. The sponsor connection must occur before any SNA application can access an HIS Server.
* When established, the server SnaBase sends "service table" information to the HIS Client, which is used for server resource location and other functions. The service table information sent from the server to the client includes:
	+ SnaBase and SNA Server services residing on other HIS Servers in the subdomain. (HIS Clients running SNA Manager also receive information about the Manage Agent services running in the subdomain.)
	+ Information about how to establish a LAN session to these services (i.e., IP addresses and port numbers, and named pipe names).
	+ The state of the SNA Server service(s) (i.e., whether the SNA Server services are running or not).
	+ The HIS event logging level.
	+ The location of the primary configuration file.
* The HIS server also routes invokable TP requests (FMH-5 Attaches, also referred to as "dynamic load requests" or DLOADs) to the client over the sponsor connection.
* The client uses the sponsor connection to send information to the server, including:
	+ SNA "RPC" requests that perform specific functions
	+ The names of invokable APPC/CPI-C TPs registered on the client computer
	+ Client-side events to be logged in the server's Windows application event log
* All HIS Servers, whether primary or backup, provide sponsor connections.

**Note:** The term “pipe” is commonly used when discussing the client/server interface to indicate a LAN session, whether over sockets or named pipes.

#### Application Connection

* Connection between the SNA application's "DMOD" (HIS dynamic access module) and an SNA Server service (node).
* The LAN session over which the SNA session traffic flows between the SNA Server service and an HIS Client.
* The client SnaBase must first have established a sponsor connection to a server-side SnaBase before the application connection can be made.
* Multiple application connections to one or more HIS Servers can exist from a single HIS Client.

Both connections can use either TCP/IP sockets or Named Pipes over TCP/IP as the transport. The transport used by the sponsor connection will be the transport to be used by all the application connections. There is nothing in the DMOD that prevents the application connection from using a different transport than the sponsor connection. This case would only arise if the initial transport failed and the DMOD reverted to using named pipes.

The sponsor and application connections operate independently of one another, although the application connection requires information obtained by the sponsor connection to find an HIS Server.

The sponsor connection can be lost and re-established without affecting the application connection and vice versa. The use of the On Demand sponsor connections prove that the application session is not dependent on the sponsor connection as long as the sponsor connection was established prior to the attempt to establish the application session.

### Active Directory Clients

Active Directory Client

**HIS 2006 Client**

**App**

**SnaBase**

**Active**

**Directory**

**Windows Server 2003**

**App**

**SnaBase**

**HIS 2006 Server**

**Application Connection**

**Port 1477**

#### SnaBase

* Active Directory support was added in Host Integration Server 2000.
* There is no connection between the HIS Client SnaBase and the HIS Server SnaBase unless the HIS Client has an invokable TP defined in its registry or has an APPC/CPI-C application running that has posted a RECEIVE\_ALLOCATE verb.
* SnaBase is started when an SNA application (3270/5250 Emulator, APPC/CPI-C TP, etc.) is started. It can also be started manually before any SNA applications are started.
* SnaBase is still used to maintain the client service table (ST).
* The service table is created at the first client activation and refreshed every seven minutes. The ST refresh interval is configurable through the **ServiceTableRefreshTime** registry entry.

If SnaBase is running as a Windows service, the **ServiceTableRefreshTime** is defined as follows:

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Snabase\Parameters\ServiceTableRefreshTime**: **REG\_DWORD: (time in minutes)**

If SnaBase is running as an application, the **ServiceTableRefreshTime** is defined as follows:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Snabase\Parameters\ServiceTableRefreshTime: REG\_DWORD: (time in minutes)**

The following Knowledge Base article describes a scenario that can occur due to how the HIS Client’s service table is refreshed when using Active Directory resource location:

**265225 Host Integration Server AD client is slow to find restarted server in Host Integration Server** ([http://support.microsoft.com/default.aspx?scid=kb;EN-US;265225](http://support.microsoft.com/default.aspx?scid=kb;EN-US;265225%20) )

* SnaBase goes through the following process when it is initially started:

	+ It checks to see if Active Directory is enabled for the HIS Client by checking the **UseActiveDirectory** registry entry located under the following key:

	**HKEY\_CURRENT\_USER\Software\Microsoft\SNA Server\CurrentVersion\Setup**
	+ If **UseActiveDirectory** is set to **YES**, SnaBase will initialize the active directory DLL (snaadsi.dll) and retrieve the Host Integration Server OU name(s) that were entered during the client configuration from the following registry key:

	**HKEY\_CURRENT\_USER (or HKEY\_LOCAL\_MACHINE)\Software\Microsoft\SNA Server\CurrentVersion\Setup\AssignedOUList**
	+ SnaBase then connects to the Active Directory on a Windows domain controller to validate the returned list of OUs.
	+ After the OUs are validated, an LDAP query is used to locate the WMI servers that are available for each OU. The WMI servers are used for WMI queries that obtain information such as User Records and Server Lists for resource location.
	+ An LDAP query is sent to query the **SnaGlobalParameters** object. At this point, **SnaGlobalParameters** is only used to store the Host Integration Server subdomain name.
	+ An LDAP query is used to get the list of SnaBase services that are running in each OU so that they can be added to the client’s service table.
	+ An LDAP query is used to get the list of SnaNodes (SNA Server services) that are running in each OU so that they can be added to the client’s service table.
	+ If the HIS Client is running SNA Manager, an additional LDAP query is performed to get the list of MngAgent services that are running in each OU.

#### Application Connection

The application connection for Active Directory clients serves the same purpose as the application connection for sponsor clients. The following is done when an application starts after SnaBase is running:

* It checks to see if Active Directory is enabled for the HIS Client by checking the **UseActiveDirectory** registry entry.
* If **UseActiveDirectory** is being used, the configured Host Integration Server OU name(s) are retrieved from the registry.
* After the OUs are validated, an LDAP query is used to locate the WMI servers that are available for each OU. The WMI servers are used to for WMI queries that obtain information such as User Records and Server Lists for resource location. Active Directory clients use WMI queries instead of the SNA “RPC” requests that sponsor clients use. You will need to make sure that DCOM is enabled to access WMI remotely.

**Note**: The application sessions also query for the WMI servers since this information is not cached on the client. Network traces will show that the WMI server queries occur each time SnaBase and SNA applications start.

* An LDAP query is sent to query the **SnaGlobalParameters** object.
* WMI queries are then used to obtain the necessary information for the application. For example, WMI queries for the user records are done for 3270 applications.
* At this point, the application connection will function just like it does on sponsor clients.

### Service Table



Host Integration Server implements its own internal dynamic "directory" of services referred to as the service table (ST). The service table information is advertised between SnaBase services running on each server, and is sent to each client SnaBase over its sponsor connection for clients configured to use a sponsor connection. Clients that are configured for Active Directory obtain the service table information from the Active Directory when SnaBase starts initially. The ST is then updated whenever the **ServiceTableRefreshTime** expires, which is seven minutes by default.

The client uses the service table information to connect to Host Integration Server services when required by SNA applications. The service table size for the HIS Client is 4094 entries.

#### Server-to-Server “Broadcasts”

The SnaBase service dynamically maintains a list of services running on all of the HIS Servers in its subdomain. This list of services is called the service table (ST). The SnaBase service on each HIS Server periodically communicates with other HIS Servers in the subdomain, notifying other servers about the SNA services supported by the server, and whether the services are running. This keeps all HIS Servers abreast of any configuration change that is made or any action that is being taken in the Host Integration Server subdomain. For example, stopping an SNA Server service (snaservr.exe) on an HIS Server system is a change that the other HIS Servers need to know about. The HIS Servers also send these updates at regular intervals even if no changes have occurred. This interval is configurable via the “Mean Time between Server Broadcasts” option in SNA Manager under the subdomain properties. The default “Mean Time between Server Broadcasts” is 70 seconds. If an HIS Server does not receive periodic updates from the other HIS Servers in the subdomain, it will age out the service table entries for the HIS Servers it is not receiving updates from.

#### Advertised Service Table Entries

Each Host Integration Server computer in the domain advertises the following service table entries when the SnaBase service starts:

* The location of the primary COM.CFG file (CFGLOC/<machine\_name>).

**Tip:** This is found from the registry value: **Role:REG\_SZ: Primary** in the subkey:
**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnaBase\Parameters**

* All SNA Server services that have been registered in the following subkey:
**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\**

|  |  |
| --- | --- |
| SNABASE/<machine\_name>  | SNABASE service |
| SNASERVR/<machine\_name> | SNA Server service |
| SNASRV02/<machine\_name> | Additional SNA Server service |
| SNASRV03/<machine\_name> | Additional SNA Server service |
| SNASRV04/<machine\_name> | Additional SNA Server service |
| NVRUNCMD/<machine\_name> | NetView Run Command service |
| NVALERT/<machine\_name> | NetView Alert service |
| SNANETMN/<machine\_name> | NetView Alert Routing Manager |
| TN3SERVR/<machine\_name> | TN3270 Server service |
| TN5250/<machine\_name> | TN5250 Server service |
| MNGCLI/<machine\_name> | SNA Manage Client  |
| MNGAGENT/<machine\_name> | SNA Manage Agent service |
| SNAPRINT/<machine\_name> | SNA Host Print service |
| PO005/<machine\_name> | AS/400 5250 passthrough demo TP |
| DDM6DB/<machine\_name> | DB2 Offline Demo TP |
| PO009/<machine\_name> | AS/400 5250 Print demo TP |
| UN2/<machine\_name> | SNA LU 6.2 Resync TP |
| DB2SERV/<machine\_name> | SNA DB2 Provider Demo service |
| DDM001/<machine\_name> | SNA DDM Demo service |
| DDM999/<machine\_name> | SNA DRDA Demo service |
| SISERVER/<machine\_name> |  Session Integrator Server service |
| TPTABLE/<machine\_name> | Dynamic table that contains all registered invokable TPs in the subdomain |

**Note:** This list is meant to include all of the possible HIS services that might be running on an HIS Server system. A specific HIS Server might not be running all of these services.

* All installed Host Integration Server link services (SNADLC1/<machine\_name>, for example).

The SNASHMEM.EXE command-line utility can be used to display the domain-wide service table entries for the entire Host Integration Server subdomain. To tell where each service table entry was received from, the machine name is included with each entry.

## HIS Client Logon

Host Integration Server uses a client/server interface to provide secure connections for client-to-server and server-to-server communication. The user authentication is done through SSPI (Security Support Provider Interface). For more information about SSPI, see the MSDN® documentation [SSPI](http://go.microsoft.com/fwlink/?LinkId=154891) (http://go.microsoft.com/fwlink/?LinkId=154891).

Enforcing authentication on the client/server interface provides the following benefits:

* Access to resources (e.g., 3270 LUs) is granted based on user account or group membership.
* Message encryption, detection of replayed packets, detection of messages received out of sequence, mutual authentication, and signed messages and verified signatures
* Integration with Windows security
* Support for SSO (Single Sign-On)

The overall security of the product can be increased by allowing the client and server to negotiate the strongest security provider, while guarding against downgrade attacks. This is accomplished in HIS 2006 by using the Negotiate SSP (Security Support Provider) package instead of NTLM. This will retain the benefits listed above and provide the following additional benefits:

* Allows the system to use the strongest (most secure) available protocol (which currently is Kerberos).
* Ensures forward compatibility with new security packages.
* Supports clients from previous versions of the product.
* When using Kerberos, allows impersonation across multiple computer boundaries.
* When using Kerberos, supports mutual authentication.

Using Kerberos eliminates the authentication delays seen with NTLM, especially in cross-forest domains.

**Microsoft Negotiate**

Microsoft Negotiate is an SSP that acts as an application layer between Security Support Provider Interface (SSPI) and the other SSPs. When an application calls into SSPI to log on to a network, it can specify an SSP to process the request. If the application specifies Negotiate, Negotiate analyzes the request and picks the best SSP to handle the request based on customer-configured security policy.

Currently, the Negotiate security package selects between Kerberos and NTLM. Negotiate selects Kerberos unless it cannot be used by one of the systems involved in the authentication or the calling application did not provide sufficient information to use Kerberos.

To allow Negotiate to select the Kerberos security provider, the client application must provide a service principal name (SPN), a user principal name (UPN), or a NetBIOS account name as the target name. Otherwise, Negotiate always selects the NTLM security provider.

A server that uses the Negotiate package is able to respond to client applications that specifically select either the Kerberos or NTLM security provider. However, a client application must know that a server supports the Negotiate package to request authentication using Negotiate. A server that does not support Negotiate cannot always respond to requests from clients that specify Negotiate as the SSP.

Since HIS 2006 and HIS 2009 use the Negotiate SSP, the following authentication (logon) methods are supported:

* Kerberos
* NTLM

See the following MSDN documentation for more details about Kerberos and NTLM SSP packages:

* [Microsoft Kerberos](http://go.microsoft.com/fwlink/?LinkId=154896) (http://go.microsoft.com/fwlink/?LinkId=154896)
* [Microsoft NTLM](http://go.microsoft.com/fwlink/?LinkId=154897) (http://go.microsoft.com/fwlink/?LinkId=154897)

### NTLM

The HIS Client will use NTLM if Kerberos is not set up on the HIS 2006 or HIS 2009 Servers. No additional configuration is needed to use NTLM authentication.

The following is a general overview of the message flow that occurs during an HIS Client logon using NTLM:

|  |  |
| --- | --- |
| **HIS 2006 Client** | **HIS 2006 Server** |
| NEW(MAN)PIPE + Logon Token 🡪 |  |
| OPEN REQUEST 🡪 | (Open queued internally) |
|  | 🡨 NTLM\_SERVER\_MSG (Challenge) |
| NTLM\_CLIENT\_MSG (Response) 🡪 |  |
|  | 🡨 LOGON\_STATUS |
|  | 🡨 OPEN RESPONSE (if logon OK) |

### Kerberos

Kerberos authentication was added in HIS 2006. The HIS 2006 and HIS 2009 Clients will always try to use Kerberos if the target server is set up to use Kerberos.

In order to configure the HIS 2006 and HIS 2009 Servers for Kerberos authentication, you have to set a Server Principal Name (SPN) for each HIS 2006 Server.

The SETSPN utility can be used to create the SPN. For more information about the SETSPN utility, see [Setspn Overview](http://go.microsoft.com/fwlink/?LinkId=154899) (http://go.microsoft.com/fwlink/?LinkId=154899).

The following is the correct syntax to use when creating the SPN for HIS 2006 and HIS 2009 Servers:

**setspn –A HISSERVICE/<HIS Server name> <domain>\<HIS service account>**

**HISSERVICE** is the Service Class that has been chosen for Host Integration Server.

If you want to create an SPN for an HIS Server named HISSERVER1 that was configured to use DOMAIN1\HIS\_Service as the service account for the HIS services, the correct SETSPN syntax is as follows:

**Setspn –A HISSERVICE/HISSERVER1 DOMAIN1\HIS\_Service**

**Note**: Because SPNs are security-sensitive, you can only set SPNs for user objects if you have domain administrator privileges.

The HIS Client takes the Service Class (HISSERVICE) and the name of the target HIS Server (sponsor server or application server) and forms the SPN that it will try to validate. A request is then sent to a domain controller to find out if the SPN name is registered. If the SPN name is registered, it is returned to the HIS Client and Kerberos authentication will be used.

The following is a basic sequence of events that occurs during an HIS Client logon using Kerberos:

1. The HIS Client DMOD calls **AcquireCredentialsHandle()** with “Negotiate” for the security package name.
2. **InitializeSecurityContext()** provides the Server Principal Name (SPN) for the target server.
3. The client then sends a Ticket Granting Ticket (TGT) and a session ticket request to the Key Distribution Center (KDC).
4. The HIS Client then presents the session ticket to the target server during connection setup.
5. The HIS Server DMOD calls **AcquireCredentialsHandle()** with “Negotiate” for the security package name.
6. The HIS Server DMOD calls **AcceptSecurityContext()**.
7. The session ticket is then verified.

## Load Balancing/Fault Tolerance (Client Side)



One of SnaBase's first tasks on startup is to create the service table. This table contains a list of all the HIS services/resources available in the HIS subdomain. Service tables are created on both servers and clients. On the client computer, the entries are added to the table in a random order. Later during resource location the servers will be contacted in the order they appear in the service table.

It is important to note that on a given client, once SnaBase is started the servers will be contacted in the same order every time an application is started. The list will only be randomized when SnaBase is stopped and restarted.

It is the randomization of entries in the client-side service table that provides the basis for load balancing of SNA session requests to the HIS Servers in the subdomain.

Load balancing encompasses both client-side and server-side features. We’ll discuss the client side load balancing capabilities that exist in addition to the service table randomization in this section. The server-side load balancing features are not discussed in this white paper.

You will need to understand both the server and client-side load balancing features in order to take full advantage of the HIS load balancing capabilities. The server-side load balancing features will be discussed in a subsequent white paper that discusses the SNA Gateway features of Host Integration Server.

### Load Balancing 3270/LUA LUs Across HIS Servers

The client “load balancing” feature added for TN3270 in SNA Server 4.0 SP2 and later added for LU6.2 in Host Integration Server 2000 can also be used for 3270 and LUA applications. The following KB article describes this feature:

**893267** How to distribute pooled 3270 application resources and LUA application resources across multiple computers that are running SNA Server or Host Integration Server

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;893267>

When an SNA application requests a session, the session may be granted from any HIS Server in the subdomain that supports the request 3270 or LUA LU. Subsequent session requests will automatically go to the same HIS Server that provided the original session. This is the default behavior and it can result in a client getting sessions from only one HIS Server as long as that HIS Server can fulfill the request.

You may see that a session request will be sent to an HIS Server that the client has an active connection to even though the HIS Server does not support the requested resource. This session request will fail and then the HIS Client will go through its normal resource location process to locate the requested session.

This behavior is used in order to maximize the efficiency of activating a session on behalf of the SNA application. By sending the session request to the HIS Server that previously provided a session, the HIS Client does not have to go through the resource location overhead and it may not have to establish a new LAN connection to another HIS Server.

For those environments that want to evenly distribute session requests among multiple HIS Servers that support the resources (3270 and LUA LUs/Pools), the **ResLocFlags** parameter provides this capability.

**Note**: The **ResLocFlags** registry entry affects all 3270 or LUA applications running on the HIS Client or HIS Server that it is enabled on.

The feature is enabled by adding a registry entry as described here.

If the HIS Client is configured to run SnaBase as a Windows service, the registry key needs to be added at the following location. This location would also be used if enabling the feature on an HIS Server.

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnaBase\Parameters\Client\**

If the HIS Client is configured to run SnaBase as an application, the registry key needs to be added at the following location:

 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SnaBase\Parameters\Client\**

**ResLocFlags**: **REG\_DWORD**: (default value is 0)

* 0x0 = try local server first or send request to the HIS Server that provided previous session (default behavior if not defined)
* 0x1 = "load balance" across HIS Server computers

If the “default” behavior is used, the SNA application running on an HIS Server will always attempt to obtain sessions from the local SNA Server service. If the SNA application is running on an HIS Client (where there isn’t a local SNA Server service), the HIS Client will attempt to send session requests to the HIS Server that previously provided a session. In this case, the session request is sent to the HIS Server without verifying if the server supports the requested session. If the session request fails, the HIS Client goes through the normal resource location process to determine the best HIS Server to send the session request to.

If the “load balance” behavior is enabled, the HIS Client will balance the session requests across all of the HIS Servers that support the requested resource (LU/Pool). The HIS Client keeps track of the last HIS Server it sent a session request to and it will start from that point in its local service table to find the next HIS Server that supports the requested resource. This allows for a “round-robin” effect to load balance the requests.

### Load Balancing APPC (LU 6.2) Sessions Across HIS Servers

The client “load balancing” feature added for TN3270 in SNA Server 4.0 SP2 was extended to provide APPC (LU6.2) session load balancing as well in Host Integration Server 2000. The following KB article describes this feature:

266275 HIS 2000 Client LU6.2 load balancing across SNA Server services

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;266275>

**Note**: The **ResLocFlags** registry entry affects all APPC or CPI-C applications running on the HIS Client or HIS Server that it is enabled on.

The feature is enabled by adding a registry entry as described below.

If the HIS Client is configured to run SnaBase as a Windows service, the registry key needs to be added at the following location. This location would also be used if enabling the feature on an HIS Server.

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SnaBase\Parameters\Client\**

If the HIS Client is configured to run SnaBase as an application, the registry key needs to be added at the following location:

 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SnaBase\Parameters\Client\**

**ResLocFlags**: **REG\_DWORD**: (default is 0)

* 0x8000 = Local Only
* 0x8001 = Local Only and Random Order

If Local Only is set, the APPC (or CPI-C) application’s DMOD will always try a local SNA Server service even if it has an existing session through an SNA Server service running on another HIS Server system. Customers requested the ability for APPC resource location to favor connections through a locally restarted HIS Server (i.e., where the APPC or CPI-C application is running on the server itself). Before this change was implemented, APPC applications (such as Transaction Integrator) would continue to try “remote” HIS Servers instead of a locally restarted SNA Server service.

If Random Order is set, the APPC (or CPI-C) application’s DMOD will try to load balance LU6.2 session requests across HIS Servers that support the Local APPC LU/Remote APPC LU/APPC Mode triplet being requested by the application. For load balancing to work correctly in this configuration, LU6.2 sessions should be auto-activated on the various servers, since the APPC DLL tends to force conversations through the “best” HIS Server. In other words, HIS Servers that have active LU/LU sessions are favored over servers that don’t, or whose connections are not active.

In the case of HIS Clients, there are no local SNA Server services (snaservr.exe). Therefore, the Random Order setting will cause the HIS Client to evenly balance APPC sessions across multiple HIS Servers assuming that the APPC resources are set up properly and that all the HIS Servers are available.

### Fault Tolerance



Fault tolerance is accomplished in conjunction with load balancing. By having several HIS Servers able to satisfy a request for an SNA resource, if one is unavailable, the client will try the next HIS Server on the list.

**Connection loss**

* SnaBase will silently attempt to reconnect the sponsor connection for sponsor-enabled clients. Losing the sponsor connection does not affect any active application connections that may exist. Active Directory-enabled HIS Clients do not have a sponsor connection.

**Note:** This assumes that the sponsor connection was active at the time the sponsor server became unavailable. As explained previously, HIS 2006 implements an On Demand sponsor connection that is automatically terminated five minutes after it is established. If SnaBase is unable to connect to the original sponsor server when it tries to re-establish the sponsor connection, it will attempt to connect to one of the other configured sponsor servers (if multiple servers are configured).
* If an application connection fails, a "lost locality" error is returned to the application (i.e., to the APPC DLL, 3270 application, etc). An APPC, CPI-C, or LUA application will then receive an error to any API calls that are outstanding or new calls that are made. The application typically reports the session loss to the user, who may then wish to reconnect their session. This requires user involvement, unless the application is designed to automatically attempt to reconnect the session.

For example, the 3270 Client (win3270.exe) included with Host Integration Server supports an automatic reconnection option when configuring the "RetryConns" variable in WIN.INI. The variable is set in the WIN.INI file by adding a section called [SnaServerWin3270] to the file and adding a line with the following syntax to that section:

RetryConns={ Yes | No } Default: No

If set to Yes, RetryConns causes the 3270 Client to retry unsuccessful connection attempts in certain circumstances where the condition causing the problem is probably temporary. Otherwise, the 3270 Client does not retry unsuccessful connection attempts. Instead, the user can retry manually by disconnecting and connecting again.

Conditions that are considered temporary are:

* + All LUs in the requested pool are in use at that moment.
	+ The requested LU pool is not found in the configuration, which may indicate that the server through which the client is attempting to connect is inactive.
	+ The requested connection is inactive at that moment.
	+ The host has not yet responded with an ACTPU (Activate Physical Unit) command.
	+ The host has not yet responded with an ACTLU (Activate Logical Unit) command.

The HIS Client DMOD is notified of LAN session outages when it receives an error code from the underlying transport (i.e., Windows sockets or named pipes).

## Resource Location

Resource location is the process used by HIS to locate the SNA resources (LUs or Pools) that an SNA application (3270, LUA, APPC, CPI-C) wants to use to communicate with an IBM host system.

### 3270/LUA Resource Location

[](http://cid-8ae4e1d7a44ec11a.skydrive.live.com/self.aspx/Host%20Integration%20Server%20Files/Resource%20Location%20%E2%80%93%203270.pptx)

At startup, an SNA application (e.g. a 3270 Emulator) can call into the DMOD (Dynamic Access Module) to obtain 3270 configuration information by calling [SEPDCREC](http://go.microsoft.com/fwlink/?LinkId=154928) (http://go.microsoft.com/fwlink/?LinkId=154928). This will cause a Get User Record message to be sent to the SnaBase service on an HIS Server. The Get User Record response returns the 3270 LUs and/or Pools assigned in the User record in the HIS configuration.

**Note**: The Get User Record request does not use the sponsor connection for this request. The HIS Client will establish a new network connection to the SnaBase service on the HIS Client’s sponsor server for this request. This is done so that the request can be made by using the user context of the application, which may be different than the user context that the local SnaBase process is running under.

The application can use the list of LUs and/or Pool names returned to choose a resource to request in the session request (known as an OPEN SSCP Request) to the SNA Server service. It is not necessary for an application to follow these steps. There are some applications that will allow any LU name to be requested in the OPEN SSCP Request.

Once the OPEN SSCP Request has been issued, the SNA application’s DMOD will send a Get Server List request to SnaBase on the sponsor server to find out which HIS Server(s) support the requested LU or Pool name.

The SNA application’s DMOD will then establish a LAN session to one of the HIS Servers returned in the Get Server List response. LAN sessions will be attempted to the HIS Servers in the order in which they appear in the service table. The service table entries are added randomly by SnaBase when it first creates the service table. This randomization provides load balancing.

Once a LAN session is established, the DMOD will proceed with sending a Newpipe message, the Open SSCP Request containing the LU or Pool name, and the logon response. The HIS Server will queue the Open SSCP Request until the logon is successful, at which point it will return an Open SSCP Response to the SNA application. If the Open SSCP request contained a Pool name, the response will return the name of the specific LU that was selected from the pool.

When the SNA Server service (node) receives the Open SSCP Request, it sends a request to its local SnaBase service to verify that the user has permission to access the LU when 3270 LU security is being used (which is the default setting).

If the Open SSCP Response returns an error, the next action will depend on whether a specific LU name or a pool name was requested. If a pool name was requested, then the next HIS Server that supports the requested pool will be contacted. If a specific LU name was requested, the application will fail for the following conditions: the LU is already in use, the LU does not exist, or the user does not have rights to the LU. If the LU or host connection is inactive, the Open SSCP Response returns with a return code of OK, but a status error will be sent to the application indicating this status.

The following flow chart gives a high-level overview of the process used to locate a 3270 LU when the application uses a 3270 LU Pool called 3270POOL that includes LUs defined on HIS Servers SERVER1 and SERVER2:

| **3270 Application** | **SnaBase/SnaDmod** | **HIS 2006 Server** |
| --- | --- | --- |
| **Session request ->** |  |  |
|  | **Get User Record ->** |  |
|  |  | <- **Get User Record response (3270POOL)** |
| **OPEN SSCP REQUEST (3270POOL) ->** |  |  |
|  | **Get Server List request (3270POOL) ->** |  |
|  |  | **<- Get Server List response (SERVER1, SERVER2)** |
| **OPEN SSCP REQUEST (3270POOL) sent to SERVER2 ->** |  |  |
|  |  | **<- OPEN SSCP RSP OK (3270LU2)** |
|  |  | **3270/LUA Session Established with LU 3270LU2** |
|  |  | **<- Sign-On Screen**  |
| **Session Established** |  |  |

### APPC/CPI-C Resource Location

[](http://cid-8ae4e1d7a44ec11a.skydrive.live.com/self.aspx/Host%20Integration%20Server%20Files/Resource%20Location%20%E2%80%93%20APPC.pptx)

When an invoking APPC program calls TP\_STARTED and [MC\_]ALLOCATE (or when a CPI-C program calls CMINIT and CMALLC) to allocate an LU6.2 conversation, the Host Integration Server APPC interface automatically attempts to locate a suitable HIS Server that supports the APPC local LU alias, remote LU alias, and mode name requested by the program.

The following are two different scenarios to be aware of related to APPC/CPI-C resource location:

### APPC Application Uses a Specific Local APPC LU Alias

A specific Local APPC LU alias is used by the APPC application. This scenario applies if one of the following occurs:

* If the APPC application explicitly specifies the Local LU alias (lu\_alias) in the TP\_STARTED call.

**Note**: A CPI-C application cannot explicitly specify the Local APPC LU alias.

* If the invoking transaction program is defined in the registry and the LocalLU parameter is specified as described in the APPC Programmer's Guide.
* If a default Local LU alias is defined in SNA Manager for the user or group who is running the APPC or CPI-C application.

The following flow chart describes the process used to locate a suitable APPC triplet (Local APPC LU/Remote APPC LU/APPC Mode) in Host Integration Server when an APPC application specifies a Local APPC LU alias.

| **APPC Application** | **WAPPC32.DLL** | **HIS 2006 Server** |
| --- | --- | --- |
| **TP\_STARTED (Local APPC LU alias=LOCAL) ->** |  |  |
|  | **<- TP\_STARTED OK** |  |
| **MC\_ALLOCATE(Remote APPC LU=REMOTE, Mode, Partner TP Name, rtn\_ctl=AP\_WHENSESSION\_ALLOCATED)**  **->** |  |  |
|  | **Get Server List request: REMOTE ->** |  |
|  |  | **<- Get Server List response: SERVER1** |
|  | **OPEN LU62 REQUEST (LOCAL, REMOTE, Mode, Non-Forced) ->** |  |
|  |  | **<- OPEN LU62 RSP ERROR (Err2:xxxx)** |
|  | **OPEN LU62 REQUEST (LOCAL, REMOTE, Mode, Forced) ->** |  |
|  |  | **BIND sent to IBM host to establish APPC session** |
|  |  | **<- OPEN LU62 RSP OK** |
|  | **<- MC\_ALLOCATE OK** |  |

**Notes:**

* The Get Server List message specifies the Remote APPC LU alias used by the application and is sent to the SnaBase service on an HIS Server to find out which HIS Servers (and which SNA Server services on those HIS Servers) support the Remote APPC LU.
* The WAPPC32.DLL (APPC library) issues a "non-forced" OPEN LU6.2 REQUEST message to each HIS Server that supports the local and remote APPC LU specified. If an HIS Server has an active available LU6.2 session over this LU/LU/mode, the "non-forced" open request will succeed and the conversation will be established over the LU6.2 session.

If no suitable APPC session is immediately available (meaning that a successful APPC BIND exchange has been completed), the SNA Server service responds with an OPEN LU6.2 Response Error, indicating an error code (Err2). The error code indicates the state of the SNA Server service or the LU/LU/mode session, and is used by WAPPC32.DLL to determine the most suitable SNA Server service it should try for a "forced" OPEN LU6.2 REQUEST.

HIS internally implements "non-forced" and "forced" open requests to properly handle on-demand connection activation, and to implement client load balancing across HIS 2006 Servers. If all HIS Servers return an error to the non-forced open request, WINAPPC32 will select the "best" server and send it a "forced" open. This forces the server to try to activate the LU/LU/mode session for use by the conversation.

The Err2 error code is used to determine the “best” HIS Server to send a “forced” OPEN LU62 REQUEST to. The various Err2 error codes are defined to indicate SNA Server service or LU/LU/mode session states that are used to determine which one has the best opportunity to fulfill the requested APPC session request.

### APPC Application Specifies a “Blank” Local APPC LU Alias

A specific Local APPC LU alias is not used by the APPC application. This applies if one of the following occurs:

* If the APPC application calls TP\_STARTED and supplies a NULL value for the Local LU alias.

**Note**: CPIC applications do this by default.

* The Local APPC LU alias is not defined in a user or group record in SNA Manager, or in the LocalLU registry parameter for the invoking TP.
* The Local APPC LU is defined to be a "Member of default outgoing Local APPC LU pool" within SNA Manager.

The following flow chart describes the process used to locate a suitable APPC triplet (Local APPC LU/Remote APPC LU/APPC Mode) in Host Integration Server when an APPC application specifies a “Blank” Local APPC LU alias.

| **APPC Application** | **WAPPC32.DLL** | **HIS 2006 Server** |
| --- | --- | --- |
| **TP\_STARTED (Local APPC LU alias=*blank*) ->** |  |  |
|  | **Get Default LUs request ->** |  |
|  |  | **<- Get Default LUs response** |
|  | **<- TP\_STARTED OK** |  |
| **MC\_ALLOCATE(Remote APPC LU=REMOTE, Mode, Partner TP Name, rtn\_ctl=AP\_WHENSESSION\_ALLOCATED)**  **->** |  |  |
|  | **Get Server List request: REMOTE ->** |  |
|  |  | **<- Get Server List response: SERVER1** |
|  | **OPEN LU62 REQUEST (*blank*, REMOTE, Mode, Non-Forced) ->** |  |
|  |  | **<- OPEN LU62 RSP ERROR (Err2:xxxx)** |
|  | **OPEN LU62 REQUEST (*blank*, REMOTE, Mode, Forced) ->** |  |
|  |  | **BIND sent to IBM host to establish APPC session** |
|  |  | **<- OPEN LU62 RSP OK (LOCAL, REMOTE, …)** |
|  | **<- MC\_ALLOCATE OK** |  |

**Notes:**

* The Get Default LUs request is sent to the SnaBase service on an HIS Server to find out if there are any Local or Remote APPC LUs assigned to the user record in SNA Manager for the user that is running the APPC application.
* In this case, you can see that the Local APPC LU alias is blank (or Null) until the SNA Server service fills in the Local APPC LU alias with a Local APPC LU that is in the default outgoing Local APPC LU pool. The APPC application doesn’t get the name of the Local APPC LU alias that it will be using until an APPC session has been established with the IBM host system.

Prior to Host Integration Server 2000, the resource location process for APPC LUs was somewhat different depending on whether a Local APPC LU alias was specified or not. Changes that were included in HIS 2000 have made the resource location process for each scenario very similar as shown in the process flows included here. This was done to allow APPC load balancing and fault tolerance to work better in situations where APPC applications specify the Local APPC LU alias (Transaction Integrator, for example).

In the case where an APPC application specifies a Local APPC LU alias, you may find that the APPC session request fails because HIS does not verify the Local APPC LU prior to issuing the MC\_ALLOCATE verb. This scenario is described in the following Knowledge Base article:

**259205 APPC TP\_STARTED does not verify local LU alias by default in Host Integration Server**

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;259205>

If you need to disable the default behavior and enforce Local APPC LU alias verification when the application issues a TP\_STARTED verb, you can add the **GenerateLUWIDonTPSTARTED** registry entry as described in the KB article.

## Encryption

The traffic that flows between an HIS Client and HIS Servers is encrypted by default in Host Integration Server 2004 and later. This applies to the sponsor connection as well as to any application connection established by the HIS Client. The HIS client/server encryption is implemented by using the Security Support Provider Interface (SSPI) provided by the Windows operating system.

Encryption support is configurable for each of the users or groups added to the Configured Users folder in SNA Manager. The **Use client/server encryption** option is enabled by default whenever a new user or group is added in SNA Manager. If you want to disable the encryption this option needs to be disabled (unchecked). The following is the properties dialog box for the Everyone group that has encryption enabled:



For security purposes, it is recommended that encryption is enabled for all users/groups configured within SNA Manager.

The use of encryption does cause some additional overhead within HIS since the client/server messages have to be encrypted and decrypted on the HIS systems. However, there have been no reports to indicate that this has caused any noticeable performance degradation in customer environments.

If SnaBase is running as an application, you can put the mouse cursor over the SnaBase Systray icon to determine if encryption is enabled. In addition, you can see if Kerberos or NTLM authentication is being used. If the mouse cursor is moved over the SnaBase icon, you may see something similar to the following:

Host Integration Server - *HIS Server Name* (NTLM) (Secure)

*HIS Server Name* would actually contain the name of the HIS Server that the client has connected to as its sponsor server. The authentication method is then shown next in parentheses and will be either NTLM or Kerberos. Finally, the (Secure) value indicates that HIS client/server encryption is enabled.

The following is a screenshot showing that the HIS Client is connected to an HIS Server named SUNDEVILS and that NTLM authentication was used and encryption is enabled:



# Conclusion

This white paper covered details regarding the installation, configuration, and functionality of the Microsoft Host Integration Server (HIS) Client. In addition, several best practices related to the HIS Client were discussed.

For more information about the HIS Client and Host Integration Server, see the [Host Integration Server 2009 online documentation](http://go.microsoft.com/fwlink/?LinkId=154941) (http://go.microsoft.com/fwlink/?LinkId=154941) and the [Host Integration Server 2006 online documentation](http://go.microsoft.com/fwlink/?LinkId=154943) (<http://go.microsoft.com/fwlink/?LinkId=154943>).

Additional HIS information can be found at the following MSDN Blogs:

* [Stephen's Host Integration Server Blog](http://go.microsoft.com/fwlink/?LinkId=154945) (http://go.microsoft.com/fwlink/?LinkId=154945)
* [Charles's Host Integration Server Ramblings](http://go.microsoft.com/fwlink/?LinkId=154946) (http://go.microsoft.com/fwlink/?LinkId=154946)
* [Host Integration Server Blog](http://go.microsoft.com/fwlink/?LinkId=154950) (<http://go.microsoft.com/fwlink/?LinkId=154950>)

# Copyright

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

 2009 Microsoft Corporation. All rights reserved.

Microsoft, MSDN, Windows, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.