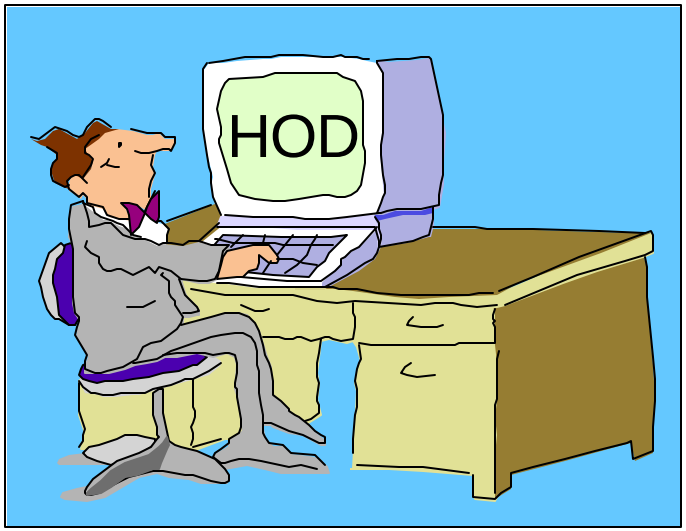
IBM ®

IBM WebSphere Host On-Demand V5 for OS/390



Linda Harrison
lharriso@us.ibm.com
06/26/01

Agenda

- IBM Host On-Demand V5 for OS/390
  - Overview
  - Server
  - Product Packaging
  - Installation
  - CS/390 IP Customization and 3270 Host Print
  - Administration
  - Client
  - New Functions
  - Current Functions
  - TN3270E SSL
  - SSL Client Authentication
  - OS/390 Lightweight Directory Access Protocol HOD Support
  - OS/390 Screen Customizer Support
  - OS/390 Host Publisher Support

Agenda (cont.)

- Appendices
  - Appendix A: TCP/IP Profile Customization
  - Appendix B: Deployment Wizard
  - Appendix C: Edit HTML
  - Appendix D: Configuration Servlet
  - Appendix E: MKKF
  - Appendix F: Migrate MKKF certificate to IKEYMAN
  - Appendix G: GSKKYMAN
  - Appendix H: Make Server certificate available to HOD clients
  - Appendix I: Client SSL
- Bibliography
- Web Sites

Abstract

Title: IBM Host On-Demand V5 for OS/390

Presenter: Linda Harrison supports OS/390 Host On-Demand in IBM Advanced Technical Support.

Audience: OS/390 Host On-Demand Installers

Abstract: Host On-Demand's browser-based access is the simplest way ever for users to reach critical host data because the user is not required to load or configure any software. Host On-Demand is a Java enabled Web based terminal emulation software supporting TN3270(E), TN5250, VT420, and IBM CICS Java Gateway. For users, Host On-Demand helps eliminate the confusing host and port names as all of the configuration is easily provided by the Administrator. From a web browser, users just click on a hyperlink that launches a session with the host. In addition to the usual web access, any number of sessions can be launched with multiple hosts at the same time. Since Host On-Demand installs on a server, maintenance, distribution, and upgrades are simplified. In the case of OS/390 Host On-Demand, the server that Host On-Demand installs onto is the OS/390 system, where most of today's enterprise mission-critical information still resides.

IBM ®

OS/390 Host On-Demand V5: Overview

Host On-Demand Overview

- IBM Host On-Demand V5 is part of the IBM Host Access Client Package, Announcement Letter 201-053.
  - TN3270E, TN5250, VT420 and IBM CICS Java Gateway
  - Secure Sockets Layer (SSL) V3.0 (X.509)
    - ie. Telnet Server of IBM Communications Server for NT V6+
    - ie. Telnet Server of IBM Communications Server for OS/390 V2.6+
    - IBM Vault Registry - standard public key infrastructure (PKI)
  - Screen Customizer/LE (default graphical user interface (GUI))
  - Database On-Demand
    - Java applet uses Java Database Connectivity (JDBC) driver
    - Access to DB2 information on AS/400
    - Structured Query Language (SQL) requests to AS/400 databases
  - Multilingual - 22 languages supported

HOD Overview (cont.)

- Steps to Logon to TSO via a Host On-Demand TN3270 Session:
  1. Start the Web Browser; double click on the browser icon.
  2. Connect the Web Browser to the HTTP Web Server (TCP/IP port 80); enter the Host On-Demand HTML URL or if the URL is bookmarked then click on Favorites and select the Host On-Demand HTML URL.
  3. Logon to the HTTP Web Server with a RACF userid and password. HTTP Server httpd.conf pass rule defines Host On-Demand Server.
  4. Logon to the Host On-Demand Server with a Host On-Demand userid and password. (TCP/IP port 8999). The password is hashed but the userid and preferences are sent in clear text. The Host On-Demand Client Applet (terminal emulator client) is downloaded (TCP/IP port 80) or previously cached on the workstation.
  5. Launch a TN3270 Session; double click on a TN3270 session icon. Host On-Demand session icons look like PComm session icons. Session is established to a TN3270E Server (TCP/IP port 23) and the "green" screen is displayed.
  6. Logon to TSO with a RACF userid and password.

HOD Overview (cont.)

Steps 1 and 2 - Launch the Browser and Enter URL - May be combined by bookmarking URL and dragging and dropping the bookmark to the desktop.

Step 3 - Connect to the HTTP Server - The HTTP Server can prompt for a valid RACF userid/password to authenticate the client. This is optional. HTTP SSL with server authentication may be enabled. HTTP SSL client authentication may be enabled to authenticate the client with a digital certificate.

Step 4 - Logon to the HOD Server - The HOD userid is required to be able to save session setting changes. The password is only required to prevent someone entering some else's userid and changing their session settings. A group userid could be used if the session setting are saved to the workstation instead of the server. The userid/password could be saved in the HTML page but it would require a different page for each user. If the session settings do not need to be saved at all then no userid/password is required. When using the Configuration Servlet the HOD userid/password will be passed as HTTP data so if HTTP Server SSL is enabled this will be encrypted. Native Authentication can be used to make the HOD password the RACF password.

HOD Overview (cont.)

Step 5 - Launch a TN3270 Session - Any session that has "Start Automatically" selected on the Advanced Tab will launch automatically after step 4. TN3270 SSL server authentication may be used to encrypt the session. Optional TN3270 SSL client authentication can be used as well to authenticate the client.

Step 6 - Logon to TSO - This can be eliminated with Express Logon.

Note: The TN3270E Server does not have to be on the same OS/390 as the Host On-Demand and Web Server; it can be on any TN3270E Server on the TCP/IP Network.

Note: HTTP session on port 80, Host On-Demand session on port 8999, and/or telnet session on port 23 may be on other customized ports.

IBM ®

OS/390 Host On-Demand V5: Server

Host On-Demand Server

- HOD Server is supported on the following platforms:
  - Windows NT 4.0 with SP5
  - Windows 2000 (Professional, Server, and Advanced Server)
  - AIX 4.2.x, 4.3.3, and 4.3.4
  - OS/2 Warp Server 4 and OS/2 Warp Server for e-Business 4.5
  - Novell Netware 4 and 5
  - Sun Solaris 2.6 and 2.7
  - OS/400 V4R3, V4R4, and V4R5
  - HP-UX 10.20
  - Redhat Linux 6.2 and 7.0
  - SUSE Linux 6.4
  - **OS/390 2.5, 2.6, 2.7, 2.8, 2.9, and 2.10**
  - Caldera OpenLinux 2.3
  - TurboLinux 6.0
  - SCO Unixware 7
  - Windows Terminal Server 4
  - Linux on S/390

IBM ®

OS/390 Host On-Demand V5: Product Packaging

Host On-Demand Packaging

- Host Access Client Package for Multiplatform Version 1.1 is Program Identification Number PID# 5648-E09.
  - Please see Announcement Letter or Web page for order information.
  - Host On-Demand for OS/390 Media types:
    - 6250 tape
    - 3480 cartridge
    - 4 millimeter cartridge
- Host On-Demand Toolkit CD and Host On-Demand Windows CD are delivered with the 390 media order.

Host On-Demand Software Requirements

- OS/390 Software Requirements

Program Number	Product Name and VRM/Service Level	Install Requirement
5647-A01	OS/390 SMP/E Version 2 Release 5+ with PTF UR51068	Yes
5655-A46	Java for OS/390 V1.1.8 or V1.3	No
5697-D43	Domino Go Webserver for OS/390 V5R0M0+	No

- The OS/390 Communications Server TCP/IP Services and Unix Systems Services, both included with OS/390, are required by IBM Host On-Demand V5 for OS/390 at run time.
- OS/390 V2R10 required APARs (for OS/390 V2R10 only):
  - OW45791 - for LDAP support
  - OW45575 - for Java

HOD Software Requirements (cont.)

- Program Temporary Fix (PTF) = Corrective Service Diskette (CSD)

CSD 1	CSD 2	CSD 3	CSD 4
APAR OW46997 PTF UW75286	APAR OW48084 PTF UW77442	part 1 APAR OW48152 PTF UW77693 part 2 APAR OW48154 PTF UW77707	part 1 APAR OW49332 PTF UW79709 part 2 APAR OW49333 PTF UW79728

- PTFs are cumulative:

  HOD V5 Base tape + CSD 1 = HOD V5.0.1

  HOD V5 Base tape + CSD 2 = HOD V5.0.2

  HOD V5 Base tape + CSD 3 = HOD V5.0.3

  HOD V5 Base tape + CSD 4 = HOD V5.0.4

- After SMP/E install the shell scripts must be executed to create the paths and expand the tar files. In /usr/lpp/HOD:

  hod50mvs.sh - to install base product

  hod50ptf.sh - to install the ptf

IBM ®

OS/390 Host On-Demand V5: Installation

Host On-Demand Installation

- SMP/E install with mainframe media provides Reliability, Availability, and Serviceability support.
- Follow directions in Program Directory, GI10-3175-00.
- 1000 MB HFS space is required.
- hod50mvs.sh may take a longer than expected time to complete (depending on system resources). TSO time-out and other timers should be customized accordingly to prevent interruption of execution before completion.

HOD Install (cont.)

- As per the Program Directory, the following lines should be added to the HTTP Webserver's configuration file (ie. /etc/httpd.conf):

```
pass /hod/*.html /usr/lpp/HOD/hostondemand/HOD/*.html.ascii
pass /hod/*.HTML /usr/lpp/HOD/hostondemand/HOD/*.HTML.ascii
pass /hod/* /usr/lpp/HOD/hostondemand/HOD/*
AddType  .cab  application/octet-steam     binary 1.0
AddType  .jar  multipart/x-zip             binary 1.0
```

  - Note: The HTTP Server must be recycled to pick up the above changes.

- Uncomment the classpath in the ServiceManager.sh as appropriate. I needed both of the following:

```
export CLASSPATH=/usr/lpp/java/J1.1/lib/classes.zip
export PATH=$PATH:/usr/lpp/java/J1.1/bin
```

HOD Install (cont.)

- A sample PROC is provided as file "HOMSERVR" in the directory "/usr/lpp/HOD/hostondemand/lib/". This may be copied to your system PROCLIB and used to start the Host On-Demand Server. This requires a userid with **UID 0**. You must use the RACF STARTED class to enable this.

- If the userid with **UID 0** is HODSERV in group OMVSGRP and the proc name used to start the Host On-Demand server is HODSRV, enter the following RACF commands:

```
RDEFINE STARTED HODSRV.* STDATA(USER(HODSERV) GROUP(OMVSGRP))
SETROPTS RACLIST(STARTED) REFRESH
```

HOD Install (cont.)

- The Host On-Demand Directories After Installation

  /usr/lpp/HOD - default distribution libraries

  /usr/lpp/HOD/hostondemand/HOD - the "publish" directory

  /usr/lpp/HOD/hostondemand/private - the private directory

  /usr/lpp/HOD/hostondemand/lib - ServiceManager.sh directory

  /usr/lpp/HOD/hostondemand/HOD/en/doc/samples/html - session1&2 directory

HOD Install (cont.)

- Optional Steps
  - Make Host On-Demand server bind to only one TCP/IP stack. Add the following to the ServiceManager.sh:

    `export _BPXK_SETIBMOPT_TRANSPORT=`*`stname`

    (where *stname* is the TCP/IP stack name)
  - Change the Service Manager's Configuration port. See the Online Help Index item "changing the Service Manager's configuration port".
    - Remember to change the port number reserved in the PROFILE.TCPIP file if you change the Service Manager's Configuration port.

HOD Install (cont.)

Note: The "/" may be missing from the "STDOUT DD" and "STDERR DD" "PATH" statements in the sample PROC. If the bottom of the PROC looks like this:

```
//STDOUT   DD PATH='tmp/homservr-stdout',
//         PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//         PATHMODE=SIRWXU
//STDERR   DD PATH='tmp/homservr-stderr',
//         PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//         PATHMODE=SIRWXU
//SYSOUT   DD SYSOUT=*
```

It should be changed to this:

```
//STDOUT   DD PATH='/tmp/homservr-stdout',
//         PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//         PATHMODE=SIRWXU
//STDERR   DD PATH='/tmp/homservr-stderr',
//         PATHOPTS=(OWRONLY,OCREAT,OTRUNC),
//         PATHMODE=SIRWXU
//SYSOUT   DD SYSOUT=*
```

IBM ®

OS/390 Communications Server
IP Customization
and 3270 Host Print

IP Customization for Host On-Demand

- Defining HOD in the PROFILE TCPIP
  - Host On-Demand can be autologged by TCP/IP and a port can be reserved for the Host On-Demand Server. Add the following to the PROFILE TCPIP:

```
AUTOLOG 5
    HOMSERVR
PORT
    8999  TCP  HOMSERVR
```

(where HOMSERVR is the name of the proc to start the HOD Service Manager)

IP Customization for HOD (cont.)

- You may want to rename the HOMSERVR sample job to a started PROC name of less than 8 characters (ie. HOMSRVR). This will help when displaying subprocesses and stopping the Host On-Demand Server. You can add the following to the PROFILE TCPIP:

  AUTOLOG 5

  HODSRVR

  PORT

  8999 TCP OMVS

- After HOD comes up display the ports and take note of what job is using 8999 with the following command:

  D TCPIP,procname,NETSTAT,SOCKETS

  (where procname is the name of the proc to start the TCP/IP stack)

  - Then optionally you may replace OMVS on the PORT statement with the job name using the port.

  Note: If you do this you may need to check to make sure the job name does not change when you migrate to new releases.

IP Telnet Customization for HOD

➢ PROFILE TCPIP BEGINVTAM STATEMENT

PORT xxxx -define which telnet port the BEGINVTAM effects

HNGROUP -define group of host names (available in OS/390 V2R7 and above)

IPGROUP -define group of ipaddrs

LUGROUP -define group of LUs

LUMAP -map LU or LUGROUP to host name, HNGROUP, ipaddr, or IPGROUP and optionally associate a printer LU or PRTGROUP

PRTGROUP -define group of printer LUs

PRTMAP -map printer LU or PRTGROUP to host name, HNGROUP, ipaddr, or IPGROUP

➢ HOD Session Customization

Destination Port

TN3270E -required for LU or LU Pool specification

LU or LU Pool

Associated Printer Session

3270 Printing with HOD

- Host On-Demand 3270 Printer Session
  - Emulates an IBM 3287 printer in either LU Type 1 (SCS) or LU Type 3 mode.
    - The printer LU must be defined in VTAM and TCP/IP.
    - The mainframe application that the user is printing from must be setup to print to the VTAM LU.
    - Please see the Host On-Demand V5 Host Printing Reference.
    - In some applications a printer is associated with a userid. For this type of application TCP/IP has the capability to "associate" or "map" printer LUs "generically" or "specifically" with user terminal LUs.
- PROFILE TCPIP BEGINVTAM Statement Example
  - Please see Appendix A in this presentation for an example.

IBM ®

OS/390 Host On-Demand: Administration

Host On-Demand Administration

- Essentially the same as for all the other Host On-Demand server platforms:
  - Connect to HOD server:

    http://hod_server_name/hod/HODMain.html
  - Select Administration and logon as **admin/password**.
  - The password may be changed but the userid cannot be changed.
  - Once logged on:

    Create groups

    Create sessions (ie. TN3270E, TN5250, VT, etc.) for groups

    Create users and assign them to groups

    Create specific sessions for individual users as necessary

HOD Admin (cont.)

- A session defines the Emulator Options (Destination Address, Destination Port, TN3270E Support, Enable Host Graphics, etc.)
- Sessions can be created for a group or an individual user.
- Users will inherit all sessions associated with all of the groups to which they belong, in addition to any specific sessions created for that individual user.
- Every user must be a member of at least one group.
  - When NOT using LDAP, a user may be a member of multiple groups.
  - When using LDAP, a user may only be a member of ONE group.
- Before creating groups, users, and sessions, the administrator needs to list what users need Host On-Demand access and what sessions they need. Can they be separated into groups? Do they need to be able to modify session options? If they don't need to modify session options they can even share a userid.
- The first time HOD Administrator might be interested in looking at the Online Help "Basic Configuration Steps" document, and the Online Help Contents item "Administration Tasks".

HOD Admin (cont.)

- When a user or group session is modified by a user, the changed session is saved as a user session. After a user logs on they are presented with an icon for each session defined for the group they are in and each individual session defined for the user.
- One potential issue exists if users are allowed to define their own sessions or modify inherited sessions.
  - A user who modifies a session inherited from a group level definition now has a local "instance" of that session. This may present a help desk problem since neither the help desk nor the user can differentiate the two sessions should the user subsequently have reason to call in for assistance.

IBM ®

OS/390 Host On-Demand: Client

Host On-Demand Client

- Host On-Demand Client is supported on the following platforms:
  - Windows 95, 98, ME, NT (4.0 with SP5), 2000 (Professional, Server, and Advanced Server) (HOD Local Client only supported on Windows)
  - AIX 4.2.x, 4.3.3, and 4.3.4
  - OS/2 Warp Server 4
  - Sun Solaris 2.6 and 7
  - HP-UX 10.20
  - Redhat Linux 6.2
  - SUSE Linux 6.4
  - Caldera OpenLinux 2.3
  - TurboLinux 6.0
  - IBM Netstation 2.1.0

HOD Client (cont.)

- Host On-Demand Client is supported on the following browsers:
  - Netscape Navigator 4.6, and 4.7 (Netscape 6.0 is not supported)
    - Supported on Windows and Unix
  - Netscape Navigator 4.61
    - Supported on OS/2
  - Microsoft Internet Explorer 4.01 with SP1, 5.0 or 5.1 (with JVM level 3165+)
- See the Host On-Demand README file for "Checking and upgrading the JVM level for Microsoft Internet Explorer.
- Security warning windows may appear when accessing the Host On-Demand server. The purpose of the windows is to indicate that HOD was created by International Business Machines and ask whether you trust it.
- The first time HOD end user should be told that taking down their browser will take down their HOD sessions.
- The first time HOD end user might be interested in looking at the Online Help Contents item "User Tasks".

HOD Client (cont.)

- HTML page that end user enters or selects in browser determines what Host On-Demand Client is downloaded.
- Sessions defined for the Host On-Demand userid (as group or individual sessions) are presented as icons, or optionally buttons, or automatically launched after the Client code is downloaded.
- Sessions defined in the HTML, with no Host On-Demand userid, are automatically launched after the Client code is downloaded.
- If there is no Host On-Demand userid, password, and logon to the HOD server, there is no need for the Service Manager to be started.
  - Without HOD userid, password, and logon to the HOD server, no session preferences may be saved for future use.
  - Logon as the HOD Administrator does require the Service Manager to be started.

HOD Client (cont.)

➢ Types of Host On-Demand Clients

To access a HOD client use a browser to open http://*hod_server*/hod/*htmlpage*, where *hod_server* is the IP address or host name of the HOD server and *htmlpage* is HODMain.html (which lists all the clients) or one of the following to access one of the clients directly:

Function	Client	HTML Page
Administrator	Administrator	HODAdmin.html
	Administrator cached	HODAdminCached.html
	Administrator cached w/ problem determination	HODAdminCachedDebug.html
Emulator Client	Cached	HODCached.html
	Cached w/ problem determination	HODCachedDebug.html
	Download	HOD.html
	Download w/ problem determination	HODDebug.html
	Download w/ Screen Customizer/LE Interface	HODCustom.html
	Function On-Demand	HODThin.html
Database Client	Database	HODDatabase.html
	Database cached	HODDatabaseCached.html
	Database cached w/ problem determination	HODDatabaseCachedDebug.html
Utilities	Remove Cached Client	HODRemove.html
	New user	NewUser.html
	New user cached	NewUserCached.html
	New user cached w/ problem determination	NewUserCachedDebug.html

HOD Client (cont.)

- The cached client loads faster than the others, and is therefore the recommended client.
- The download client will not run on a workstation with the cached client installed. If the cached client is installed it must be removed before the download client can be used. Remove the cached client with the HODRemove.html page.
- Locally-installed client can be installed from the CD on Windows 95, 98, 2000, NT 4.0 with SP3 or later.
  - To start locally-installed client:

    Click Start, Programs, IBM Host On-Demand, Host On-Demand
- For more information about Host On-Demand clients see the Host On-Demand "Planning and Installation Guide" also known as "Getting Started".

HOD Client (cont.)

- AutoHODxxx.html
  - There are some AutoHODxxx.html files, that correspond to some of the HODxxx.html files, that launch the session automatically instead of having to double click the icon. They are located in the "publish" directory (default is /usr/lpp/HOD/hostondemand/HOD).
- Session 1 and Session 2
  - HTML sample files that can be copied to the "publish" directory and customized:
  - Session 1 is like AutoHOD.html with these added capabilities:
    - Save the userid and password in the HTML page.
    - Launch the session automatically instead of having to double click the icon.
    - Run the session embedded in the browser window or in a separate window.
    - Change session icons into buttons.
    - /usr/lpp/HOD/hostondemand/HOD/en/doc/samples/html/session1.html.ascii
  - Session 2 is also like AutoHOD.html with these added capabilities:
    - No userid and password required, which means that settings cannot be saved.
    - /usr/lpp/HOD/hostondemand/HOD/en/doc/samples/html/session2.html.ascii

HOD Client (cont.)

- The Deployment Wizard on the Host On-Demand for Windows V5 CD may be used to create HTML pages or the HTML may be edited manually.
- Deployment Wizard
  - A wizard-driven administration tool that provides easy planning and configuration of sessions, administration options, and deployment methods.
  - See Appendix B in this presentation and Online Help Contents item "Administration Tasks, Sessions, Creating an HTML file for starting sessions".
- Edit HTML pages
  - After HTML pages are edited on non-OS/390 platform, they must be binary FTPed to the OS/390 Host On-Demand Publish Directory.
  - When HTML files are FTPed to the OS/390 Host On-Demand server for the first time the permission bits setting on the file created in OMVS may not allow the use of the HTML page. You may need to change the permission bits to something usable, like 644.
  - HTML pages are in ASCII (even on OS/390). Please see Appendix C in this presentation for editing options.

IBM ®

OS/390 Host On-Demand
New Functions

Host On-Demand New Functions

- Functional Enhancements Added to Host On-Demand V5.0.0:
  - Componentization
  - Smart Cache
  - Configuration Servlet
  - Deployment Wizard
  - Policy Management and Feature/Function Disable
  - Express Logon
  - Printer Definition File Support in Windows
  - Improved Color Remap
  - Improved Key Remap
  - Multiple Session Launch Support
  - Paste Improvements
  - Improved Error and Status Indicators
  - Improved Menu Usability
  - Toolkit CD Package
  - Code Page Enhancements

HOD New Functions (cont.)

- Blink Attribute
- Telnet-negotiated Transport Layer Security (TLS)
- Native Authentication
- Java 2 Platform Support

(Announcement Letter 200-324 and the Host On-Demand "Planning and Installation Guide" also known as "Getting Started")

- Functional Enhancements Added to Host On-Demand V5.0.3:
  - Directory Utility
  - FTP Client
  - Security Enhancements (Including Smart Card Support)
  - Database On-Demand File Upload
  - Launch Emulator Session Macro

(Announcement Letter 201-053 and the Host On-Demand "Planning and Installation Guide" also known as "Getting Started")

IBM ®

OS/390 Host On-Demand Current Functions

Host On-Demand Current Functions

- Online Help
  - In addition to the documentation provided with the product, listed in Bibliography, there is extensive online help available when using HTML pages.
  - If you click on the ? that appears in the top right corner of the window, after clicking on a Help button or when viewing some of the Help documents, the Online Help documents will then be accessible under a Contents tab and/or Index tab. Throughout this presentation the items listed under the Contents and Index tabs are mentioned for further information.
- User Filter
  - There is a "Disable User Filter" check box on the Users/Groups page of the Administrator Client. When selected all userids will be displayed. When unselected a filter may be used to only display a subset of userids. The userids are case sensitive so filter a* will display userid "admin" but filter A* will not.
- Multiple Session Icon/Launch
  - After defining sessions they may be defined in a Multiple Session Icon on the Users/Groups page of the Administrator Client.
  - See Online Help Index item "multiple session icon overview".

HOD Current Functions (cont.)

- Policy Management and Feature/Function Disable
  - Allows administrators to control, via policies, which features are available to which users, as well as completely disable, through the menus, toolbar and other areas, any feature.
  - Deployment Wizard
    - Create HTML files with features/functions disabled. You must select "Use the Configuration Server" = "No", for use without the Configuration Server (Service Manager), to be able to disable features/functions. Without the Service Manager no session preference changes may be saved to the Service Manager (the Host On-Demand server), only to the local PC.
  - Edit HTML Files with a Text Editor
    - Use the Disable parameter in the HTML. See Online Help Index item "disabling functions through HTML files".

HOD Current Functions (cont.)

- Lock Session Properties
  - Session properties may be individually "locked" when the session is created.
  - If session properties are not locked (or disabled) they can be modified by the user.
    - Session colors can be remapped.
    - Light Pen Mode can be enabled.
    - An Applet can be run.
    - A Macro can be saved or run.
  - See Online Help Contents item "User Tasks, Sessions".
- Saving Preferences
  - User modifications to session properties will be saved unless "Do not save preferences" is selected on the userid.
  - A shared HOD userid can be created with "Do not save preferences" and "User cannot change password" selected. The password may even be blank.

HOD Current Functions (cont.)

- Save Session Properties on Local PC
  - Session customization changes done by the user may be saved to the local PC rather than back on the server. In this way, one standard session can be created with one shared userid defined. Every user that uses that session may customize it and the changes will be saved locally and only effect them.
  - Save Cached Client Session Properties on Local PC

Use the Deployment Wizard to create a definition with "Use the Configuration Server"="No" and "Allow users to save session changes?"="Yes".

Note: The file permissions must be 666.

- Save Download or Locally Installed Client Session Properties on Local PC

Use the Session 2 HTML file. On Locally Installed Client copy C:\hostondemand\lib\doc\samples\html\session2.html to C:\hostondemand\lib\test1.html (where test1.html is the name you want to use).

See the Online Help Index item "applet tag parameters".

HOD Current Functions (cont.)

Set the following parameters in the HTML:

```
<PARAM NAME="SessionName"     VALUE="">
<PARAM NAME="Host"            VALUE="">
<PARAM NAME="SessionType"     VALUE="">
<PARAM NAME="SessionID"       VALUE="">
<PARAM NAME="Save"            VALUE="">
<PARAM NAME="Config"          VALUE="">
<PARAM NAME="ConfigDefault"   VALUE="">
<PARAM NAME="ConfigOverwrite" VALUE="">
```

ie.:

```
<PARAM NAME="SessionName"     VALUE="mvsnm2">
<PARAM NAME="Host"            VALUE="9.82.1.100">
<PARAM NAME="SessionType"     VALUE="1">
<PARAM NAME="SessionID"       VALUE="A">
<PARAM NAME="Save"            VALUE="text2.txt">
<PARAM NAME="Config"     VALUE="http://127.0.0.1/hod/text2.txt">
<PARAM NAME="ConfigDefault"   VALUE="true">
<PARAM NAME="ConfigOverwrite" VALUE="true">
```

HOD Current Functions (cont.)

- Change Password
  - Host On-Demand password may be changed when logging onto the HOD server unless "User cannot change password" has been selected for the userid.
- Redirector
  - Configure HOD Server to "redirect" session to a TN3270 server.
  - Hides TN3270 real IP address and port from end users.
  - SSL is not supported by the Host On-Demand/390 Server Redirector. The only way to enable SSL to the HOD/390 Server is to use the Configuration Servlet and the HTTP Server SSL support. A TN3270 session between a HOD client and a TN3270 server will use SSL if the TN3270 session has SSL defined and the TN3270 server supports it, whether or not the session is redirected.
  - See Online Help Contents items "Administration Tasks, Redirector", and "User Tasks, Sessions, Configuring to connect to the Redirector".

HOD Current Functions (cont.)

- Lightweight Directory Access Protocol (LDAP) Support
  - LDAP can be defined instead of Host On-Demand's User Preferences Private Data Store by selecting "Use Directory Service" on the Directory Service page of the Administrator Client.
  - Already defined Users/Groups/Sessions can be migrated to the LDAP by selecting "Migrate Configuration to Directory Service" on the Directory Service page of the Administrator Client.
  - There is no service to migrate LDAP definitions to Host On-Demand's User Preferences Private Data Store.
  - See the Program Directory, the LDAP section of this presentation, and the Host On-Demand "Planning and Installation Guide" also known as "Getting Started".
- Directory Utility
  - Add, update and delete users, groups and sessions by a command line Java application.
  - Uses ASCII file in XML format to manage configuration information.
  - Supports Host On-Demand's User Preferences Private Data Store or LDAP.
  - See Online Help Index item "Directory Utility, using the".

HOD Current Functions (cont.)

- OS/400 Proxy Server
  - So that only one port is opened through the firewall when transferring files to an AS/400 system.
  - Not supported on the HOD/390 server.
- Host On-Demand Licenses
  - License-Use Statistics may be enabled or displayed on the Licenses page of the Administrator Client.
  - See the Online Help Contents item "Administration Tasks, License usage".
- Service Location Protocol (SLP)
  - Enables client to dynamically locate TN3270 and TN5250 server, and connect to the least-loaded server.
  - Not supported on HOD/390 server.

HOD Current Functions (cont.)

- Bookmark Session
  - See Online Help Contents item "User Tasks, Sessions, Bookmarking".
- Allow Users to Create Accounts
  - Customize NewUser.html provided in the "publish" directory to allow end users to create Host On-Demand userids.
  - See the Online Help Index item "account, creating your own user".

HOD Current Functions (cont.)

- Optionally provide multiple copies of the file with different file names and customize different group names in the HTML. Use the httpd.conf PROTECTION and PROTECT to allow only group coordinators to create Host On-Demand userids in a particular group:

```
Protection Acct_Co {
        ServerId        Accounting_Coordinator
        AuthType        Basic
        PasswdFile      %%SAF%%
        Mask            CSMITH,csmith
}
Protect /NewAcctUser.* Acct_Co
Protection Admin_Co {
        ServerId        Administration_Coordinator
        AuthType        Basic
        PasswdFile      %%SAF%%
        Mask            EJONES,ejones
}
Protect /NewAdminUser.* Admin_Co
```

HOD Current Functions (cont.)

- Error Messages
  - See Online Help Contents item "User Tasks, Message help".
- Tracing
  - Service Trace
    - Start and stop a trace from the Services page of the Administrator Client.
    - View Trace and Log data by clicking on "Server Log".
  - User Trace
    - Start a trace from the Debug Client. Select save location of "Local" or "Server".
    - If the save location is "Local", view the Trace data in the "console" on the Debug Client.
    - If the save location is "Server", view the Trace data by right mouse clicking the user and selecting "Trace Facility" on the Users/Groups page of the Administrator Client.

HOD Current Functions (cont.)

- Check Version
  - ASCII file with the Host On-Demand installed version listed is:

    /usr/lpp/HOD/hostondemand/lib/.version
  - ASCII file with the Screen Customizer installed version listed is:

    /usr/lpp/customizer/customizer/.version-sed
- Troubleshooting
  - For additional troubleshooting ideas see the Online Help index items "troubleshooting" and "aids, problem determination".
- Applet/Macro Support
  - See the Online Help Contents item "User Tasks, Macro Manager".
- Launch Emulator Session Macro
  - Use a macro to launch an emulator session while using Host On-Demand with Screen Customizer/LE (default GUI) or Screen Customizer product.

HOD Current Functions (cont.)

- Secure Sockets Layer (SSL)
  - If "Enable Security (SSL)" is selected on the session Security tab the session will use SSL encryption with Server Authentication.
  - If "Server Authentication (SSL)" is selected on the session Security tab a DNS Server hostname verification is done. The hostname defined in the server certificate must match the hostname defined in the DNS.
  - If "Send a Certificate" is selected on the session Security tab the session will use Client Authentication.
- Telnet-negotiated Transport Layer Security (TLS)
  - Communications Server for OS/390 V2R10 only.
  - Supported on 3270 display and printer sessions.
  - For more information about TN3270 SSL and TLS see the SSL section of this presentation, the "IP Configuration Guide, SC31-8725" Chapter 6 "Accessing Remote Hosts Using Telnet" section "Connection Security", the "IP Configuration Reference, SC31-8726" Chapter 11 "Telnet", the "System Secure Sockets Layer Programming Guide and Reference, SC24-5877-03" Chapter 6 "Certificate/Key Management", and the Host On-Demand "Planning and Installation Guide" also known as "Getting Started".

HOD Current Functions (cont.)

- Screen Customizer
  - See the Screen Customizer section of this presentation.
- Keyboard Remap
  - Provides a panel to see which keys are mapped and what options are available for remap.
  - See Online Help Contents items "User Tasks, Sessions, Remapping the keyboard" and "User Tasks, Sessions, Specifying keys to not repeat".
- File Transfer
  - Host File Transfer Function
    - Does not use FTP.
  - FTP Client
    - Standard FTP Client to upload files, download files and navigate directories on remote FTP server and the local file system.
  - See Online Help Contents item "User Tasks, Printing".

HOD Current Functions (cont.)

- Componentization
  - Cached Client reduced download size possible. Download only the features desired.
  - Deployment Wizard
    - Select the desired download features on the "Preload Configuration" page.
    - If the client tries to use a feature that has not been downloaded then the feature will be downloaded at that time.
  - Edit HTML Files with a Text Editor
    - Use the PreloadCodeModules parameter in the HTML. See Online Help Index item "cached client parameters, setting".
    - If the client tries to use a feature that has not been downloaded then the error "Results in class not found exception" will occur.

HOD Current Functions (cont.)

- Cached Client Load from CD/Network Drive
  - Deployment Wizard
    - To the question "Where will the components be installed from?", select "CD/Network Drive" instead of "Web server".
  - See the Host On-Demand "Planning and Installation Guide" also known as "Getting Started" Chapter 8 "Loading the Host On-Demand clients" section "Cached clients" subsection "Installing the Cached client".
- Smart Cache
  - Cache client updates take place in the background, while the older cached code is used for the current session.
  - Deployment Wizard
    - Select "Upgrade in background" or "Prompt user" instead of "Upgrade in foreground".
  - Edit HTML Files with a Text Editor
    - There will be a prompt unless the UpgradePromptResponse parameter is coded in the HTML. See the Online Help Index item "cached client parameters, setting".

HOD Current Functions (cont.)

- Smart Card Support
  - Store client certificate in the client's browser or in a dedicated security device such as a smart card.
    - Select "Certificate in browser or security device" on Security tab of session definition.
  - Store client certificate in a local or network-accessed file, in PKCS12 or PFX format, or in a URL, protected by a password.
    - Select "Certificate in URL or local file" on Security tab of session definition.
  - Add the browser's keyring to Host On-Demand client so that client will accept Certificate Authorities (CAs) trusted by the Microsoft Internet Explorer browser.
    - Select "Add MSIE browser's keyring" on Security tab of session definition.
- Copy/Paste
  - See Online Help Contents item "User Tasks, Sessions, Cut, copy and pasting text in a session".

HOD Current Functions (cont.)

- Blink Attribute
  - 3270 and 5250 Blink Attribute. Similar VT Blink Attribute.
  - See the Online Help Index item "attributes, setting the display".
- Code Page Enhancements
  - Code page table support includes all the code pages currently supported by Personal Communications.
    - Code pages added include: 1153 (Latin 2 Euro); 1154 (Cyrillic Euro); 1155 (Turkey Euro); 1156 (Estonia Euro); 1158 (Cyrillic Ukraine Euro); 1160 (Thai Euro); 1364 (Korean Euro); 1371 (Taiwan Euro); 1390 (Japan Katakana Euro); and 1399 (Japan Latin Euro).
    - Code pages modified to enable the Euro Currency Symbol include: 420 (Arabic); 424 (Israel); 803 (Israel); and 875 (Greece).
  - For more information see the Host On-Demand "Planning and Installation Guide" also known as "Getting Started" and Online Help Contents item "National language support".

HOD Current Functions (cont.)

- Printer Support
  - You can print host application files on a printer that is directly attached to your workstation or to a network printer.
    - See the "Host Print Reference" and the IP Customization and 3270 Host Print section of this presentation.
  - You can print a screen.
    - See Online Help Contents item "User Tasks, Printing, Printing the screen".
- Printer Definition File Support in Windows
  - Allows a user to access a printer from a Host On-Demand Windows client with a host print session PDT (3270) or Model (5250).
  - See Online Help Contents item "Administration Tasks, Printing, Using a Windows printer".

HOD Current Functions (cont.)

- Configuration Servlet
  - Optional servlet to eliminate configuring specific ports (ie. 8999) to a firewall. When used with WebSphere Application Server, it allows Host On-Demand to use the HTTP or HTTPS ports exclusively for Host On-Demand server configuration traffic (TN3270 port is still required for TN3270 session host connectivity). This allows Host On-Demand to be easily deployed across the Extranet, with no firewall restrictions. Please see Appendix D of this presentation.
  - It must be installed on a Web Application Server that supports the Java Servlet 2.0 API. The OS/390 WebSphere Application Servers V1R1, V1R2, V3R02, and V3R5 are supported (V4 will be supported by HOD V6).
  - The Host On-Demand clients connect to the Configuration Servlet using port 80 (or configured port) and the Configuration Servlet connects to the Host On-Demand server using port 8999 (or the configured port).
  - See the Online Help Index item "configuring the Configuration Servlet".
  - See the Online Help Index item "Configuring Host On-Demand with an IBM firewall" for directions about using Host On-Demand through a firewall without the Configuration Servlet.

HOD Current Functions (cont.)

- Native Authentication
  - Native Authentication enables users to logon to the Host On-Demand server using the same password they use when logging onto OS/390.
  - This requires LDAP.
  - "Use Native Authentication" may be selected per userid.
  - See the Program Directory and the Online Help Index item "authentication, using native".
- Express Logon Feature
  - Enables a user, running a 3270 client session, to logon to an SNA host application (ie. TSO) using an SSL Client Digital Certificate defined to RACF instead of user ID and password.
  - Requires Communications Server for AIX, Communications Server for NT, or Communications Server for OS/2 TN3270 server between client and OS/390 V2R10 application host.
  - zOS/390 V1R2 and OS/390 V2R10 will support Express Logon without a middle tier Communications Server TN3270 between client and 390.

HOD Current Functions (cont.)

- A session configured to use SSL client authentication with an express logon macro associated with it. When the session is launched the user is prompted to enter a PIN for the SSL client certificate.
- The TSO password change has no effect since the password is never known to the client but the client certificate change is a manual process. Wherever the certificate is created, on the server or client, it must be updated to RACF at the same time that it is updated on the client workstation.
- See the White Paper "Setting up and Using the Express Logon Feature" that is available on the Library section of the Host On-Demand Home Page, and the Online Help Index items "express logon feature" and "express logon macro, recording".

HOD Current Functions (cont.)

- Database On-Demand
  - Java applet to perform SQL requests to AS/400 databases through a JDBC driver.
  - See the Online Help Contents item "Administration Tasks, Database On-Demand".
- Database On-Demand File Upload
  - Graphical Interface for uploading entire files from client to host database.
  - Manipulates database data specifically.
  - Provides for different File Upload statement types.
  - Uploads numerous file formats.
  - Connects to any database using a Java Database Connectivity (JDBC) driver.
  - Different than AS/400 File Upload feature and SQL Wizard.

HOD Current Functions (cont.)

- IBM Host Access Toolkit
  - Provided on CD for Windows 95, 98, NT 4.0 with SP3 or higher, and 2000.
  - Includes the following support:
    - Host Access Class Libraries (HACL) for Java
      - Allows the development of platform-independent applications that can access host information without the need for a graphical display.
    - Host Access Beans for Java
      - Beans that use HACL libraries.
    - ActiveX support the same as PComm

HOD Current Functions (cont.)

- Bean Builders (HACL and Host Access Beans for Java) are supported on:
  - Sun's Bean Development Kit V1.0
  - VisualAge for Java V3.0 and 3.5 Beta
  - Sunsoft Java Workshop V2.0
  - Lotus Development's BeanMachine V1.1.4
  - WebGain's Visual Cafe Professional Development Edition V4.0
  - Borland/Inprise's JBuilder V2 and 3.5
- The following documentation is available from the "IBM Host Access Toolkit" directory after Toolkit installation:
  - Getting Started (also available from first CD panel)
  - Host Access Class Library Reference
  - Host Access Beans for Java Reference
  - Open Host Interface Objects Reference

HOD Current Functions (cont.)

- EHLLAPI Enablement Tool
  - Allows users to run existing EHLLAPI applications using a variety of interfaces on HOD emulator sessions.
  - Available from the Download section of the Host On-Demand Home Page.

IBM ®

OS/390 TN3270E
Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL)

- Secure Sockets Layer (SSL) Certificate consists of a Key Pair:
  - Public Key - The key that is given to other hosts. The only key that can decrypt data that has been encrypted by the Private Key.
  - Private Key - The key that must never be given to other hosts. The only key that can decrypt data that has been encrypted by the Public Key.

Secure Sockets Layer (cont.)

- Server Authentication SSL:
  1. Client sends connection request to Server.
  2. Server sends Server public key encrypted with Signer's private key. The Signer is the Well-Known Certificate Authority (CA) or the Server of the Self Sign Certificate.
  3. Client has all Well-Known CA public keys (all browsers have preloaded Well-Known CA public keys). Client can also have Self Sign Certificate public keys defined as well.
  4. If appropriate Signer public key decrypts Server public key then session is approved for SSL encryption.
  5. Client encrypts a new randomly generated key pair with Server public key (remember only Server private key can decrypt data encrypted with Server public key) and sends.
  6. Server and client use this new randomly generated key pair for SSL session encryption.

Secure Sockets Layer (cont.)

- Additional Optional Client Authentication SSL:
  1. Server Authentication is done.
  2. Client sends Client public key encrypted with Signer's private key.
  3. Server must have Well-Known CA public key or Self Sign Certificate public key defined.
  4. If appropriate Signer's public key decrypts Client public key then session is approved.

Host On-Demand and SSL

- There are multiple ways of using SSL with Host On-Demand.
  - SSL can be used on the HTTP session to port 80. Between Client Browser and HTTP Web Server. Please refer to HTTP Web Server documentation.
  - SSL can be used on the TN3270 session to port 23. Between the HOD Client and the TN3270 Server.
  - Not supported on OS/390 Host On-Demand Redirector, but supported on other HOD servers is the SSL encrypted Redirected HOD session.

SSL Requirements

OS 390	Product	Optional Feature Name	Function Provided
R5	Domino Go Webserv	DGW Export Security	HTTP SSL 56-bit
R5	Domino Go Webserv	DGW France Secure	HTTP SSL 40-bit
R5	Domino Go Webserv	DGW N America Secure	HTTP SSL 128-bit
R5	Comm Server	IP Security CDMF	IP Sec CDMF
R5	Comm Server	IP Security DES/CDMF	IP Sec DES/CDMF
R5	Comm Server	IP Kerberos DES	Kerberos DES 56-bit
R5	Comm Server	IP Kerberos non-DES	Kerberos non-DES
R6	Domino Go Webserv	DGW Export Security	HTTP SSL 56-bit
R6	Domino Go Webserv	DGW France Secure	HTTP SSL 40-bit
R6	Domino Go Webserv	DGW N America Secure	HTTP SSL 128-bit
R6	Comm Server	IP Security CDMF	IP Sec CDMF, and
			Telnet SSL RC2/RC4 40bit
R6	Comm Server	IP Security DES/CDMF	IP Sec DES/CDMF, and
			Telnet SSL DES 56bit
R6	Comm Server	IP Security TDES	IP Sec TDES, and
			Telnet SSL TDES
R6	Comm Server	IP Kerberos DES	Kerberos DES 56-bit
R6	Comm Server	IP Kerberos non-DES	Kerberos non-DES

SSL Requirements (cont.)

OS 390	Product	Optional Feature Name	Function Provided
R7	IBM HTTP Server	IBM HTTP Export Sec	HTTP SSL 56-bit
R7	IBM HTTP Server	IBM HTTP France Sec	HTTP SSL 40-bit
R7	IBM HTTP Server	IBM HTTP NA Secure	HTTP SSL 128-bit
R7	Comm Server	eNetwork CS Sec Lev 1	IP Sec CDMF, and
			Telnet SSL RC2/RC4 40bit,
			Kerberos non-DES
R7	Comm Server	eNetwork CS Sec Lev 2	IP Sec DES/CDMF,
			Telnet SSL DES 56bit,
			Kerberos DES 56-bit, and
			SNMPV3 CBC DES 56-bit
R7	Comm Server	eNetwork CS Sec Lev 3	IP Sec TDES,
			Telnet SSL TDES,
			Kerberos DES 56-bit, and
			SNMPV3 CBC DES 56-bit

SSL Requirements (cont.)

OS 390	Product	Optional Feature Name	Function Provided
R8&9	IBM HTTP Server	IBM HTTP Export Sec	HTTP SSL 56-bit
R8&9	IBM HTTP Server	IBM HTTP France Sec	HTTP SSL 40-bit
R8&9	IBM HTTP Server	IBM HTTP NA Secure	HTTP SSL 128-bit
R8&9	Comm Server	SecureWay CS Sec Lev 1	IP Sec CDMF, and
			Telnet SSL RC2/RC4 40bit,
			Kerberos non-DES
R8&9	Comm Server	SecureWay CS Sec Lev 2	IP Sec DES/CDMF,
			Telnet SSL DES 56bit,
			Kerberos DES 56-bit, and
			SNMPV3 CBC DES 56-bit
R8&9	Comm Server	SecureWay CS Sec Lev 3	IP Sec TDES,
			Telnet SSL TDES,
			Kerberos DES 56-bit, and
			SNMPV3 CBC DES 56-bit

SSL Requirements (cont.)

OS 390	Product	Optional Feature Name	Function Provided
R10	IBM HTTP Server	IBM HTTP NA Secure	HTTP SSL 128-bit
R10	Comm Server	IBM CS base	IP Sec CDMF,
			IP Sec DES/CDMF, and
			SNMPV3 CBC DES 56-bit
R10	Comm Server	SecureWay CS Sec Lev 1	Kerberos non-DES
R10	Comm Server	SecureWay CS Sec Lev 2	Kerberos DES 56-bit
R10	Comm Server	SecureWay CS Sec Lev 3	IP Sec TDES
R10	Crypto Services	Crypto Services base	HTTP SSL 56-bit,
			HTTP SSL 40-bit, and
			Telnet SSL RC2/RC4 40bit,
			Telnet SSL DES 56-bit
R10	System SSL Sec	Sys SSL Security Lev 3	Telnet SSL TDES

(System SSL Sec does not need to be enabled unless Firewall is used)

SSL Requirements (cont.)

- To use TN3270 SSL create a Certificate Request and/or Server Public/Private Keys.
- There have been four Certificate Tools on OS/390. From the oldest to the newest: MKKF, IKEYMAN, GSKKYMAN, and RACF.

SSL Server Authentication

- The OS/390 V2R6 and V2R7 TCP/IP telnet servers require an MKKF format certificate.
  - The MKKF utility that ships as part of the OS/390 V2R6 and V2R7 LDAP server supports a 512-bit key size.
  - For OS/390 V2R6 and R7, how to create a private key and server certificate in the server's key ring file and a password stash file using MKKF is documented in "OS/390 Communications Server, IP Configuration, SC31-8513", Appendix D. Please see Appendix E in this presentation.
  - To use MKKF with certificate authority (CA) VeriSign, APAR OW39793 is required and a password for the keyringfile has to be 6 to 8 characters.

SSL Server Auth (cont.)

- The OS/390 V2R8 telnet server requires a certificate in the format of the GSKKYMAN utility.
  - GSKKYMAN utility is part of OS/390 V2R8+ System Secure Sockets Layer.
  - How to create the server key database using GSKKYMAN is documented in "OS/390 Communications Server, IP Configuration, SC31-8513", Appendix C, and the Redbook "IBM Host On-Demand 4.0: Enterprise Communications in the Era of Network Computing, SG24-2149-01". Please see Appendix G in this presentation.
- The OS/390 V2R10 telnet server requires a certificate in the format of the GSKKYMAN utility or RACF's Certificate Management Support.
  - The RACF RACDCERT command is detailed in the "OS/390 Security Server (RACF), Command Language Reference, SC28-1919".

SSL Server Auth (cont.)

- Some releases of the HTTP Web Server require an IKEYMAN format certificate.
  - A certificate created with MKKF can be migrated to an IKEYMAN format. Please see Appendix F in this presentation.
- An MKKF certificate can be migrated to GSKKYMAN and a GSKKYMAN database can be migrated to RACF.
  - Please see "OS/390 System SSL Programming Guide and Reference, SC24-5877".
- A certificate created with IKEYMAN can be exported using IKEYMAN and then a GSKKYMAN key database file can be created and the certificate can be imported into it.

OS/390 TN3270 SSL

- To start a TN3270 SSL port on an OS/390 telnet server the Cryptography library must be defined to LINKLST.
  - I added the line

    `LNKLST ADD NAME(WSC.LINKLST) DSNAME(SYS1.CRYPTO.SGSKLOAD)`

    to my **`SYS1.PARMLIB(PROGF2)`** member. Without this I received an **`IEA995I SYMPTOM DUMP`** with CODE=0C4. The dataset must also be program controlled. In RACF I changed the **`CLASS=PROGRAM`** with **`PROFILE=*`**. I added '**`SYS1.CRYPTO.SGSKLOAD`**' to the member list.

OS/390 TN3270 SSL

- TELNETPARMS SECUREPORT
  - On OS/390 V2R6+ TCP/IP uses the TELNETPARMS SECUREPORT statement to enable SSL Server Authentication.
- TELNETGLOBALS SECUREPORT
  - On OS/390 V2R10 TCP/IP you can specify SECUREPORT in the TELNETGLOBALS block instead of the TELNETPARMS block.
- TELNETPARMS KEYRING SAF
  - On OS/390 V2R10 TCP/IP uses the TELNETPARMS KEYRING SAF statement to define a RACF keyring to the telnet server.

OS/390 TN3270 SSL (cont.)

- TELNETPARMS ENCRYPTION
  - On OS/390 V2R7+ the TELNETPARMS ENCRYPTION statement specifies a subset of the supported encryption algorithms to use for a port.
- TELNETPARMS CONNTYPE
  - On OS/390 V2R10+ the TELNETPARMS CONNTYPE can define TLS-based Telnet SLL for TN3270 negotiation of SSL.
- Distribute Self Signed Certificate
  - The Server Self Signed Certificate public key can be defined to the HOD Server. If it is defined to the HOD Server it will be passed to each HOD Client. So even Self Signed Certificates or ones created by non-Well-Known CA's can be used without distributing the CA's public key to each client manually. Please see Appendix H of this presentation.

Optional SSL Client Authentication

- TELNETPARMS CLIENTAUTH
  - On OS/390 V2R8+ use the TELNETPARMS CLIENTAUTH statement to enable SSL Client Authentication.
  - SSLCERT enables SSL Client Authentication only
  - SAFCERT enables SSL Client Authentication and checks that the user has a valid RACF userid assigned. The certificate must be defined to RACF with the RACDCERT command.
- SERVAUTH
  - RACF class SERVAUTH may be used to limit access on a port basis.

IBM ®

HOD SSL Client Authentication

SSL Client Authentication

- Create Client Certificate
  - Host On-Demand Locally Installed Client has a key-management utility that can be used to create a Client Certificate. This is detailed in the Redbook
    "SecureWay Communications Server for OS/390 V2R8 TCP/IP: Guide to Enhancements, SG24-5631-00", section "3.2.3.6 Working with the client certificate".
    http://www.redbooks.ibm.com
  - A Client Certificate can be obtained from a Well Known CA and exported in pkcs12 format from the browser thru which it was received. The certificate can be stored on the local disk, network drive, or web server, from which the client can get it.
  - A Self Signed Client Certificate created on OS/390 using GSKKYMAN is only a V1 P12 file. HOD needs a V3 PKCS12 file so a browser can be used to convert the file. See Appendix I in this presentation for converting the file using a browser.

IBM ®

OS/390 Lightweight Directory Access Protocol (LDAP) Server HOD Support

OS/390 LDAP

- Host On-Demand V5 supports LDAP Directory Servers:
  - Netscape Directory Server V3.1 and V4.0 on NT or AIX
  - OS/390 LDAP Server on OS/390 V2R5 through R10
  - IBM SecureWay LDAP Server V2.1
  - IBM LDAP Directory Server V3.1.1
    - IBM schema pre-installed

IBM ®

OS/390 Screen Customizer Support

Screen Customizer Overview

- Screen Customizer is a thin Java client that automatically converts host screens into a graphical presentation.
- A Limited Edition version of Screen Customizer (Screen Customizer/LE), also referred to as the default GUI, is included in all the Host On-Demand clients and can be turned on in the session configuration panels but cannot be customized. The separate Screen Customizer product is required for customization.

Screen Customizer

- There are three components of Screen Customizer:
  - Administrator
    - Capture host screens for customization.
    - Identify screens and save as maps.
    - Set global defaults and save in profile.
  - Customization Studio
    - Customize screens captured by Administrator.
  - Client
    - Default or customized graphical interface for host sessions.
- Only the Screen Customizer "Client" is supported on OS/390.

Screen Customizer (cont.)

- Screen Customizer Administrator is supported on:
  - Host On-Demand Client
  - Personal Communications
- Screen Customizer Client is supported on:
  - Host On-Demand Server
  - Host On-Demand Client
  - Personal Communications
- Screen Customizer Studio is supported on:
  - Windows 95, 98, 98SE, ME, NT (4.0 with SP5), and 2000 (Professional, Server, and Advanced Server)
- Note: Review Software Announcement Letter 200-152, for Personal Communication's limitations.

Screen Customizer (cont.)

- ResQ!Net was renamed to IBM Screen Customizer.
- Screen Customizer V2 is part of the IBM Host Access Client Package.
  - Announcement Letter 201-053
- HOD V5.0 supports IBM Screen Customizer (CS) 2.0.

Program Temporary Fix (PTF) = Corrective Service Diskette (CSD)

CSD 1	CSD 2	CSD 3	CSD 4
APAR OW47000 PTF UW75551	APAR OW48085 PTF UW77452	APAR OW48153 PTF UW77685	APAR OW49335 PTF UW79761

- After a CSD has been installed mvscli.sh must be run.

Screen Cust V2.0 Base + CSD 1 = SC V2.0.1 (supported by HOD V5.01)

Screen Cust V2.0 Base + CSD 2 = SC V2.0.2 (supported by HOD V5.02)

Screen Cust V2.0 Base + CSD 3 = SC V2.0.3 (supported by HOD V5.03)

Screen Cust V2.0 Base + CSD 4 = SC V2.0.4 (supported by HOD V5.04)

Screen Customizer (cont.)

- The mvscli.sh shell script requires the CLASSPATH defined for java. I needed to add the following to the mvscli.sh file:

  export CLASSPATH=$CLASSPATH:/usr/lpp/java/J1.1/lib/classes.zip

  export PATH=$PATH:/usr/lpp/java/J1.1/bin

- After the mvscli.sh finishes look at the bottom of file /usr/lpp/customizer/HODLink-UNIX-errors. The last two lines must be the following or there were errors encountered:

  Linking HOD files.
  Done.

Copy Custom Files

- Copy Custom Files
  - After installing Screen Customizer Client, copy customized files from a Windows Screen Customizer Administrator to OS/390.
  - FTP the files of each subdirectory in C:\hostondemand\HOD\custom on the Windows Administrator to the OS/390 host in the /usr/lpp/customizer/customizer/custom directory. Files must be transferred in BINARY for all directories except "/lst" which must be transferred in ASCII.
  - The .scm and .psd files in screen.db are expected to be lower case on OS/390.

Copy Custom Files (cont.)

- In order to FTP the files you will need to create the subdirectories on OS/390 in the /usr/lpp/customizer/customizer/custom directory, ie.:

  /usr/lpp/customizer/customizer/custom/lst

  /usr/lpp/customizer/customizer/custom/map

  /usr/lpp/customizer/customizer/custom/ps

  /usr/lpp/customizer/customizer/custom/ref

  /usr/lpp/customizer/customizer/custom/wsp

  /usr/lpp/customizer/customizer/custom/img

  /usr/lpp/customizer/customizer/custom/(lang)/help

  Set the permission bits to (7,5,5) for the subdirectories.

- If separate sets of customizations for different users/groups have been stored in replicas of the custom directory, these directories must also be copied to OS/390.

Screen Customizer Functions

- Functional Enhancements Added to Screen Customizer V2.0.0, as per Announcement Letter 200-324:
  - Global customization enhancements — Control the look and function of many different emulator screens at once by creating templates that can be automatically combined with both mapped screens and non-mapped screens at runtime.
  - Simplified screen capture process — Toolbar buttons to capture a screen, start the Studio, and work with screens IDs.
  - Web link button improvements — Additional options have been added for Web link buttons. Text for links changes color when the mouse pointer is held over it, displaying a standard Web link. Settings can be saved for individual Web links.
  - Light pen support — Use your mouse as a light pen when accessing host applications that require a light pen. Light pen fields can be displayed as check boxes or buttons, depending on the type of field.
  - AS/400 subfiles — AS/400 subfile screens are automatically converted into multicolumn tables with button hotspots that send the appropriate commands for manipulating objects in the subfile list.

Screen Customizer Functions (cont.)

- Screen Customizer API — You can programmatically set properties for graphical interface objects and the data represented by the object (for example, buttons, valid values, button captions or choice options). This provides the ability to dynamically modify graphical components and data at runtime. The Screen Customizer API is documented in the SCCI Reference included with the Host On-Demand Host Access Toolkit.
- Screen Customizer bean — Use Screen Customizer within your own application or embedded directly into a Web page. The bean allows rapid application development with full capabilities to display customized screens. It is documented in the Host Access Beans for Java Reference included with the Host On-Demand Host Access Toolkit.
- Host On-Demand integration — Screen Customizer now reuses the function-rich Host On-Demand toolbar and keyboard remap facilities. Screen Customizer is also adding the ability to launch macros created in Host On-Demand.
- Auto install for AIX — Provides a GUI for installing Screen Customizer on AIX.
- Additional language support — Enablement for Hindi and Thai languages have been added. This product, however, does not translate Hindi and Thai languages.

Screen Customizer Functions (cont.)

- Functional Enhancements Added to Screen Customizer V2.0.3, as per Announcement Letter 201-053:
  - Page Up/Page Down — Enables the page up and page down keys, along with the mouse, to scroll an application window effectively.
  - Right Mouse Click — The addition of "What Is It" choice provides a direct link to information from the Help menu.
  - Screen ID Sorting — Provides sorting and search capabilities to a list of Screen IDs. Customers with large lists can easily find the ID they are looking for.

IBM ®

OS/390 Host Publisher Support

Host Publisher Overview

- Host Publisher takes 3270, 5250, VT, JDBC, and Java host applications, and turns them into HTML Web pages for web access from even non-Java browsers.

Host Publisher

- There are two components of Host Publisher:
  - Studio - Development Environment
    - Generates Integration Object (JavaBean).
    - Contains JavaBean Factories.
    - Creates Applications.
    - Generates Java Server Pages (JSP).
  - Server - Run Time Environment
    - Integrates multi-platform Web servers.
    - Provides JSP parsing.
    - Provides Servlet API support.
    - Contains Java classes for connection management.
    - Provides an administration capability.
- Only the Host Publisher "Server" is supported on OS/390.

Host Publisher (cont.)

- Host Publisher Studio is only supported on:
  - Windows 95, 98, and NT
- Host Publisher Server is supported on:
  - AIX
  - Windows NT
  - Solaris
  - OS/390
- OS/390 Host Publisher V2.2:

  Announcement Letter 200-262

Host Publisher (cont.)

- There are three parts of Host Publisher Studio:
  - Host Publisher Studio
    - Creates Applications using JSP's to invoke Integration Objects.
  - Host Access Wizard
    - Create 3270, 5250, and VT Integration Objects.
  - Database Access Wizard
    - Create JDBC Integration Objects.

IBM ®

Appendix A:
OS/390 TCPIP PROFILE Customization

IP PROFILE

➢ PROFILE TCPIP BEGINVTAM Statement Example

```
PORT 223
HNGROUP HNAMES1 andyh.washington.ibm.com patb.washington.ibm.com ENDHNGROUP
HNGROUP HNAMES2 **.bet.ibm.com ENDHNGROUP
IPGROUP IPNAMES1 255.255.240.0:9.82.0.0 ENDIPGROUP
IPGROUP IPNAMES2 9.82.130.4 9.82.1.161 ENDIPGROUP
IPGROUP IPNAMES3 255.255.224.0:9.82.128.0 ENDIPGROUP
IPGROUP IPNAMES4 9.82.1.2 9.82.1.10 ENDIPGROUP
LUGROUP NONHOD1 TCP20001..TCP20010 ENDLUGROUP
LUGROUP NONHOD2 TCP20011..TCP20020 ENDLUGROUP
LUGROUP HODLUG2 TCP20H01..TCP20H02 ENDLUGROUP
LUGROUP HODLUG3 TCP20H11..TCP20H20 ENDLUGROUP
LUGROUP HODLUG4 TCP20H21..TCP20H22 ENDLUGROUP
PRTGROUP PRTLUS1 TCP20P01..TCP20P10 ENDPRTGROUP
PRTGROUP PRTLUS2 TCP20P11..TCP20P12 ENDPRTGROUP
PRTGROUP PRTLUS4 TCP20P21..TCP20P22 ENDPRTGROUP
```

IP PROFILE (cont.)

PRTMAP PRTLUS1 IPNAMES1 ===> see section 1 below

LUMAP NONHOD1 HNAMES1 ===> see section 2 below

LUMAP NONHOD2 HNAMES2 ===> see section 3 below

LUMAP HODLUG2 IPNAMES2 SPECIFIC PRTLUS2 ===> see section 4 below

LUMAP HODLUG3 IPNAMES3 ===> see section 5 below

LUMAP HODLUG4 IPNAMES4 GENERIC PRTLUS4 ===> see section 6 below

1. If a printer session is initiated to port 223 from any IP address in the 9.82.0.0 subnet (mask 255.255.240.0), the first available LU will be assigned between TCP20P01 and TCP20P10.
2. If andyh or patb from domain washington.ibm.com telnets into port 223, the first available LU will be assigned between TCP20H01 and TCP20H10.
3. If any host from domain bet.ibm.com or any sub-domain (including tomv.bet.ibm.com and suej.rustbuck.bet.ibm.com) telnets into port 223, the first available LU will be assigned between TCP20H11 and TCP20H20.

IP PROFILE (cont.)

4. If 9.82.130.4 telnets to port 223 and requests LU TCP20H01, it will be assigned and a printer session with LU TCP20P11 will be initiated and associated with the host session. Likewise if 9.82.1.161 telnets to port 223 and requests LU TCP20H02, it will be assigned and a printer session with LU TCP20P12 will be initiated and associated with the host session.
5. If any IP address in the 9.82.128.0 subnet (mask 255.255.224.0) telnets into port 223, the first available LU will be assigned between TCP20H11 and TCP20H20.
6. If 9.82.1.2 telnets to port 223, the first available LU will be assigned between TCP20H21 and TCP20H22, and a printer session will be initiated and associated with the host session. Likewise if 9.82.1.10 telnets to port 223, the first available LU will be assigned between TCP20H21 and TCP20H22, and a printer session will be initiated and associated with the host session. Where TCP20P21 is the printer LU if the host LU is TCP20H21, and TCP20P22 is the printer LU if the host LU is TCP20H22.

IBM ®

Appendix B: Deployment Wizard

Deployment Wizard

- If the Deployment Wizard is used to create an HTML page, two HTML files and a subdirectory structure with multiple files in it are created in one zip file. This zip file must be binary FTPed to the Host On-Demand Server and unzipped, or all the files, preserving the subdirectory structure, must be binary FTPed to the Host On-Demand Server. The files must be put in the publish directory (the default is /usr/lpp/HOD/hostondemand/HOD) on the Host On-Demand Server and the HTML files and (if there are any) .txt files must have the .ascii extension added. There is no .ascii extension required on .cf and .obj files. As an example, if the Deployment Wizard created file HODTest1.html, you might end up with the following files on OS/390:
  - /usr/lpp/HOD/hostondemand/HOD/HODTest1.html.ascii
  - /usr/lpp/HOD/hostondemand/HOD/AutoHODTest1.html.ascii
  - /usr/lpp/HOD/hostondemand/HOD/HODData/HODTest1/params.txt.ascii
  - /usr/lpp/HOD/hostondemand/HOD/HODData/HODTest1/wInfo.txt.ascii
  - /usr/lpp/HOD/hostondemand/HOD/HODData/HODTest1/cfg0.cf
  - /usr/lpp/HOD/hostondemand/HOD/HODData/HODTest1/policy.obj
  - /usr/lpp/HOD/hostondemand/HOD/HODData/HODTest1/preloads.obj

Deployment Wizard (cont.)

- Deployment Wizard Pages:
  1. "Welcome to Host On-Demand Deployment Wizard"
     - "Do you want to create or edit an HTML file?"
       Select "Create a new HTML file" or "Edit an existing HTML file"
     - And then Click "Next"
  2. "Connection Options"
     - "Use the Configuration Server"
       Select "Yes" or "No"
       - If "Yes" then "Do you want to use the Configuration Servlet?"
         Select "Yes" or "No"
         - If "Yes" then enter "Configuration Servlet URL"
           For example /iphost/servlet/hodconfig/hod (where "iphost" is either the IP address or hostname of the Configuration Server)
         - If "No" then enter "Configuration Server Port"
           For example 8999
     - And then Click "Next"
     - If "Use the Configuration Server" = "No" then skip to 4

Deployment Wizard (cont.)

- Deployment Wizard Pages (cont.):
  3. "Logon Options"
     - "Require users to logon?"

       Select "Yes" or "No"
       - If "No" then enter "User ID to automatically logon as" and "Password for this user ID"
     - And then Click "Next"
  4. "Additional Options"
     - "Allow users to save session changes?"

       Select "Yes" or "No"
     - "Cache Host On-Demand applet?"

       Select "Yes" or "No"
     - "Include problem determination components?"

       Select "Yes" or "No"
     - And then Click "Next"
     - If "Cache Host On-Demand applet" = "No" then skip to 9

Deployment Wizard (cont.)

- Deployment Wizard Pages (cont.):
  5. "Cache Client Options"
     - "Debug cached client installation process?"
       Select "Yes" or "No"
     - "Where will the components be installed from?"
       Select "Web server" or "CD/Network Drive"
     - "Enter the size of the progress indicator frame"
       Enter "Width" (default 550) (options 300, 350, 400, 450...800)
       Enter "Height (default 250) (options 150, 200, 250, 300, 350, 400)
     - And then Click "Next"

Deployment Wizard (cont.)

- Deployment Wizard Pages (cont.):
  6. "Cache Client Upgrade Options"
     - "When an upgrade version of cached client is available"

       Select "Allow all users to upgrade", "Don't allow any users to upgrade", or "Control user upgrades"
       - If "Control user upgrades" then select "Percent of users who can upgrade at a time" or "Only allow upgrade if specified file contains the word upgrade"
         - If "Percent of users who can upgrade at a time" then enter the percentage (default 100) (options 10, 20, 30...100)
         - If "Only allow upgrade if specified file contains the word upgrade" then enter "URL to file"
     - Select "Upgrade in foreground", "Upgrade in background", or "Prompt user"
     - And then Click "Next"
     - If "Use the Configuration Server" = "Yes" then skip to 9

Deployment Wizard (cont.)

- Deployment Wizard Pages (cont.):
  7. "Host Sessions"
     - Define Sessions
     - And then Click "Next"
  8. "HTML Level Policy Configuration"
     - Enable or disable functions
     - And then Click "Next"
  9. "Display Options"
     - Select "Standard Host On-Demand Client" or "Grid of Buttons"
     - Enter "Applet size" (default Large) (options Autosize, Small, Medium, Large)
     - Enter "Maximum number of concurrent sessions per user" (default 26) (options 1 to 26)
     - And then Click "Next"
  10. "Preload Configuration"
     - Select the components to include in the initial download
     - And then Click "Next"

Deployment Wizard (cont.)

- Deployment Wizard Pages (cont.):
  11. "Page Title and Summary"
      - Enter Bookmark page title
      - And then Click "Next"
  12. "Create HTML"
      - Select Path for file to be saved
      - Enter "File Name"
      - And then Click "Create"
  13. "Congratulations!"
      - Click "Restart Wizard" to create or edit more HTML files, or click "Close" to exit the Deployment Wizard

IBM ®

Appendix C:
Edit HTML Files

Edit HTML

- To be able to edit the OS/390 file it must be converted to EBCDIC or sent to another platform like Windows 95:
  - To edit on OS/390:
    1. In OMVS issue the following command, all on one line:

       ```
       iconv -f IBM-932 -t IBM-1047
       /usr/lpp/HOD/hostondemand/HOD/en/doc/samples/html/session1.html.ascii >
       /u/user1/session1.html
       ```

    2. Edit /u/user1/session1.html from the OS/390 ISHELL.
    3. In OMVS use the iconv command again to "publish" the html page, all on one line:

       ```
       iconv -f IBM-1047 -t IBM-932 /u/user1/session1.html >
       /usr/lpp/HOD/hostondemand/HOD/session1.html.ascii
       ```

  - To edit on Windows 95:
    1. FTP the file in binary to a Windows 95 workstation.
    2. Edit the file with Windows Notepad or WordPad.
    3. FTP the file in binary to the "publish" directory (default is /usr/lpp/HOD/hostondemand/HOD).

Edit HTML (cont.)

- The following parameter must be changed:

  <PARAM NAME="Host" VALUE="">

  to add the IP Address or Hostname of the TN3270 Server, ie.:

  <PARAM NAME="Host" VALUE="9.82.1.100">

  to be able to use the following HTML files properly:

  AutoHOD.html.ascii

  AutoHODCached.html.ascii

  AutoHODCachedDebug.html.ascii

  AutoHODCustom.html.ascii

  AutoHODDebug.html.ascii

  AutoHODThin.html.ascii

  session2.html.ascii

Edit HTML (cont.)

- The following parameters must be changed:

  <PARAM NAME="User" VALUE="">

  <PARAM NAME="Password" VALUE="">

  to add the userid and password of the Host On-Demand user, ie.:

  <PARAM NAME="User" VALUE="huser1">

  <PARAM NAME="Password" VALUE="u1pass">

  to be able to use the following HTML file properly:

  session1.html.ascii

Edit HTML (cont.)

- The following parameters may be changed:

  <PARAM NAME="User" VALUE="">

  <PARAM NAME="Password" VALUE="">

  to add the userid and password of the Host On-Demand user, ie.:

  <PARAM NAME="User" VALUE="huser1">

  <PARAM NAME="Password" VALUE="u1pass">

  to skip the logon prompt when using the following HTML files:

  HOD.html.ascii

  HODCached.html.ascii (without quote marks)

  HODDebug.html.ascii

  HODThin.html.ascii

Edit HTML (cont.)

- The following parameters may be added:

  <PARAM NAME="CachedClient" VALUE="true">

  to add change the client to a cached client when using the following HTML files:

  session1

  session2

- Please see Online Help Contents item "Administration Tasks, Sessions, Session parameters" and Online Help Index item "cached client parameters, setting" for HTML parameters.

IBM ®

Appendix D: Configuration Servlet

Configuration Servlet

- I did the following on my system which has WebSphere Application Server V1.2:
  1. I added the following to my was.config file "ncf.jvm.classpath=" statement:

     /usr/lpp/HOD/hostondemand/lib/cfgsrvlt.jar
  2. I also added the following statement to my was.config file:
     servlet.hodconfig.code=com.ibm.eNetwork.HODUtil.services.remote.HODCfgServlet
  3. I did not add the following to my httpd.conf file because it was already there:

     Service /servlet/* /usr/lpp/WebSphere/AppServer/lib/libadpter.so:AdapterService
  4. I copied HOD.html.ascii to HODCServ.html.ascii.
  5. I added the following to HODCServ.html.ascii:

     <PARAM NAME=ConfigServerURL VALUE=9.82.1.100/servlet/hodconfig/hod>

     Where 9.82.1.100 is the IP address or hostname of the Configuration Server.

Configuration Servlet

- I did the following on my system which has WebSphere Application Server V3.02:
  1. I added the following to my was.config file:

```
deployedwebapp.HOD.host=default_host
# rooturi must match pathname on Service statement in httpd.conf:
deployedwebapp.HOD.rooturi=/servlet
# The following two lines are all on one line with no spaces:
deployedwebapp.HOD.classpath=/usr/lpp/servlets:/usr/HOD/hostondemand/lib/cfgsrvl
   t.jar:/usr/lpp/HOD/hostondemand/HOD:/usr/lpp/java/J1.1/lib/classes.zip
deployedwebapp.HOD.documentroot=/usr/lpp/HOD/hostondemand/lib
webapp.HOD.jspmapping=*.jsp
webapp.HOD.jspmapping=*.jhtml
webapp.HOD.jsplevel=1.0
webapp.HOD.filemapping=/
# URL to servlet by code name or servletmapping alias listed below:
# The following two lines are all on one line with no spaces:
webapp.HOD.servlet.HODConfigServlet.code=com.ibm.eNetwork.HODUtil.services.remot
   e.HODCfgServlet
webapp.HOD.servlet.HODConfigServlet.servletmapping=/hodconfig
# The following two lines are all on one line with no spaces:
webapp.HOD.servlet.HODConfigServlet.initargs=ConfigServer=127.0.0.1,ConfigPort=8
   999,ShowStats=true,Trace=true
webapp.HOD.servlet.HODConfigServlet.autostart=true
```

  2. I added the following to my httpd.conf file:

```
Service /servlet/* /usr/lpp/WebSphere/AppServer/bin/was302plugin.so:service_exit
Service /*.jsp /usr/lpp/WebSphere/AppServer/bin/was302plugin.so:service_exit
EnableFRCA off
```

Configuration Servlet (cont.)

3. I copied HOD.html.ascii to HODCServ.html.ascii.
4. I added the following to HODCServ.html.ascii:

```
<PARAM NAME=ConfigServerURL VALUE=servlet/hodconfig/hod>
```

Where 9.82.1.100 is the IP address or hostname of the Configuration Server.

IBM ®

Appendix E:
OS/390 V2R6 and R7
MKKF Server Certificate

MKKF Server Certificate

➢ Create Certificate with MKKF

1. Go to OMVS on OS/390, change the directory to the directory that you want the key ring to be in, and start MKKF:

   mkkf

2. Create and name the Server Keyring file (n for new):

   n

3. Input the key ring filename or press Enter for the default keyfile.kyr filename.

   This is the key ring filename to be used in the TCPIP PROFILE.

4. 'Work with keys and certificates':

   w

5. 'Create a key pair and request a certificate':

   c

6. Input the key ring password.
7. Input the password again for verification.

MKKF Server Certificate (cont.)

8. Select if the password will expire.

   To have the password expire, enter y and the number of days until it expires.

   To have the password not expire, enter n.

9. Request a server certificate or a CA certificate:

   s

10. Modify the key and certificate fields:

    m

11. Enter the Key Name label.
12. Select the Key Size.
13. Enter the Server Name; fully-qualified host name of the TN3270E server.

    If you select "Server Authentication" on your HOD session this Server Name must match the host name in the DNS for the IP address of the TN3270E server.

14. Enter the Organization Name.
15. Enter the Organization Unit Name.
16. Enter the Locality/City.
17. Enter the State/Province.

MKKF Server Certificate (cont.)

18. Enter the Postal Code.
19. Enter the two digit Country Code:

    US
20. Create the key pair and certificate request:

    r
21. Enter the certificate request filename.
22. Exit the Key menu:

    x
23. Create a stash file:

    c
24. Exit the Key Ring menu

    x
25. Save the key ring file and exit MKKF:

    y
26. If you are going to purchase a signed certificate from a Well Known Certificate Authority (CA), like VeriSign or Thawte, e-mail the certificate request to the CA and they will return it signed.

MKKF Server Certificate (cont.)

27. Start MKKF:

    mkkf

28. Open the key ring file:

    o

29. Enter the key ring filename from step 3.
30. Enter the password from step 6.
31. Receive the certificate into the key ring:

    r

32. Enter the certificate filename from step 21.
33. If you are receiving a self-signed certificate, confirm that you want to add the certificate to the key ring:

    y

34. If prompted, enter the certificate label for the signed certificate.
35. Exit the Key Ring Menu:

    x

36. Save the key ring file and exit MKKF:

    y

MKKF Server Certificate (cont.)

37. Start MKKF:

    mkkf

38. Open the key ring file:

    o

39. Enter the key ring filename from step 3.

40. Enter the password from step 6.

41. Work with keys and certificates:

    w

42. List the keys:

    l

43. Either select the key you want to make the default key:

    s

    Or display the next key:

    n

44. Make the key the default key in the key ring:

    f

MKKF Server Certificate (cont.)

45. Confirm the default key:

    y

46. Exit the Key Menu:

    x

47. Exit the Key Ring Menu:

    x

48. Save the key ring file and exit MKKF:

    y

IBM ®

Appendix F:
Migrate MKKF Certificate to IKEYMAN

Migrate MKKF Certificate to IKEYMAN

➢ Migrate the certificate from MKKF to IKEYMAN

1. Go to OMVS on OS/390, change the directory to the directory that has the certificate in it.
2. Set up the environment for IKEYMAN:

```
export PATH=/usr/lpp/internet/bin:$PATH
export LIBPATH=/usr/lpp/internet/bin:$LIBPATH
export NLSPATH=/usr/lpp/internet/%L/%N:$NLSPATH
```

3. Convert kyr file to kdb format:

```
ikeyman -m -r keyfile.kyr
```

   where keyfile is the name of the mkkf key ring file.

4. Enter password.

   File keyfile.kdb is created.

5. Start IKEYMAN:

```
ikeyman
```

6. 'Open key database':

```
2
```

Migrate MKKF Certificate (cont.)

7. Enter the key database name:

   keyfile.kdb

8. Enter password.

9. 'List/Manage keys and certificates':

   1

10. Select the number of the certificate you want to make available to HOD clients.

11. 'Copy the certificate of this key to a file':

    5

12. Select binary file type:

    2

13. Input filename:

    cert.der

    This is the certificate to be made available to the HOD clients.

14. Exit IKEYMAN:

    1

IBM ®

Appendix G:
OS/390 V2R8
GSKKYMAN Server Certificate

GSKKYMAN Server Certificate

➢ Create Certificate with GSKKYMAN

1. Go to OMVS on OS/390, change the directory to the directory that you want the key ring to be in.

   My directory on my system is /u/harrisl.

2. You can display your environment settings, including STEPLIB:

   env

   I needed to add the C and Crypto library to my STEPLIB:

   export STEPLIB=$STEPLIB:SYS1.CRYPTO.SGSKLOAD:SYS1.CPP.SCLBDLL

3. Start GSKKYMAN:

   gskkyman

4. 'Create new key database':

   1

5. Input a database filename or press Enter for the default key.kdb filename.

   I input nm512.kdb and file ***/u/harrisl/nm512.kdb*** was created.

6. Input a password.

   I input *one0ssl* on my system.

GSKKYMAN Server Certificate (cont.)

7. Input password again for verification.
8. Select if the password will expire.

   I selected *1* so that the password would expire.

   Then I pressed *Enter* to default to a 60 day expiration.
9. Select to work with the database now:

   1
10. If you are going to purchase a signed certificate from a Well Known Certificate Authority (CA), like VeriSign or Thawte, select 3 'Create new key pair and certificate request'. If you are going to create a self-signed certificate, select 5 'Create a self-signed certificate'.

    I created a self-signed certificate:

    5
11. Select a version 3 Certificate:

    3
12. Input a certificate label name:

    I input *nmlow* for a certificate label name on my system.

GSKKYMAN Server Certificate (cont.)

13. Select key size.

    I selected *1* for 512 key size.

14. Input 'Common Name'; the fully-qualified host name of the TN3270E server.

    I input *mvsnm2*.

    If you select "Server Authentication" on your HOD session this 'Common Name' must match the hostname in the DNS for the IP address of the TN3270E server.

15. Input the 'Organization'.

    I input *IBM*.

16. Input the 'Organization Unit'.

    I input *nsc*.

17. Input the 'City'.

    I input *GBURG*.

18. Input 'State'.

    I input *MD*.

GSKKYMAN Server Certificate (cont.)

19. Input two digit 'Country'.

    I input *US*.

    Note: If you use USA then you get the following error when you try to save:

    Error: An asn.1 encoding/decoding error occurred.

20. Input number of days for certificate.

    I pressed *ENTER* to default to 365 days.

21. If you are purchasing a signed certificate, send the request to CA and after the request is returned select 4 'Receive a certificate issued for your request'.

22. Set key as the default key in the database:

    1

23. Save the certificate to a file:

    1

24. Save as a binary file:

    2

25. Input a filename or press Enter for the default name of cert.crt.

    I input *nmlow.crt* and file ***/u/harrisl/nmlow.crt*** was created.

GSKKYMAN Server Certificate (cont.)

26. Do not exit yet:

    0

27. 'Store encrypted database password':

    11

    I received a message back that password had been stored in

    /u/harrisl/nm512.sth.

28. Exit GSKKYMAN:

    1

IBM ®

Appendix H:
Make SSL Server Certificate Available to HOD Clients

HOD SSL Server Certificate

➢ Make the Certificate Available to the HOD Clients

1. Change to the root directory:

   cd /

2. Locate the HOD web-published directory:

   find . -name WellKnown TrustedCAs.class*

   The published directory on my system is the default /usr/lpp/HOD/hostondemand/HOD.

3. Copy the binary certificate into the published directory:

   cp /u/harrisl/nmlow.crt /usr/lpp/HOD/hostondemand/HOD/nmlow.crt

   Note: Copy as a binary file and no character conversion.

4. Locate the Host On-Demand server directory:

   find . -name sm.zip*

   The server directory contains the file archives used to run the Service Manager.

   The server directory on my system is /usr/lpp/HOD/hostondemand/lib.

5. Change to the HOD published directory:

   cd /usr/lpp/HOD/hostondemand/HOD

HOD SSL Server Certificate (cont.)

6. Add the certificate to the CustomizedCAs.class file, using the keyrng Java Utility.

   For HOD V3 type the following, all on one line:

   `java -classpath .:HOD_SERVER_DIR/sm.zip:$CLASSPATH com.ibm.sslight.tools.keyrng CustomizedCAs add --certificatetype cert.der`

   For HOD V4 or V5 type the following, all on one line:

   `java -classpath .:HOD_SERVER_DIR/sm.zip:$CLASSPATH com.ibm.hodsslight.tools.keyrng CustomizedCAs add --certificatetype cert.der`

   where **`HOD_SERVER_DIR`** is the HOD server directory,

   `certificatetype` is **`ca`** if you are adding a CA root certificate

   or **`site`** if you are adding a site or self-signed certificate,

   and **`cert.der`** is the name of the file containing the binary certificate.

(continued on next page)

HOD SSL Server Certificate (cont.)

6. (cont.)

Note: **CustomizedCAs** must be capitalized exactly as shown, there is a single hyphen before the classpath parameter, and a double hyphen before the certificate parameter. If the java command is typed in with incorrect syntax you will get the following error:

Unable to initialize Threads: Cannot find class /java/lang/Thread

If no CustomizedCAs.class file exists, keyrng prompts you for a password with which to encrypt the new class-file. However, CustomizedCAs.class must NOT be encrypted, so just ENTER at the password prompt.

I found I needed the following path to the java code:

```
export PATH=$PATH:/usr/lpp/java/J1.1/bin
```

I found this in the ServiceManager.sh script in /usr/lpp/HOD/hostondemand/lib.

I issued the following on my system:

```
java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip:\
/usr/lpp/java/J1.1/lib/classes.zip \
com.ibm.hodsslight.tools.keyrng CustomizedCAs add --site nmlow.crt
```

HOD SSL Server Certificate (cont.)

7. Check to see if the certificate was added.

   For HOD V3 type the following, all on one line:

   java -classpath .:HOD_SERVER_DIR/sm.zip:$CLASSPATH

   com.ibm.sslight.tools.keyrng CustomizedCAs verify

   For HOD V4 or V5 type the following, all on one line:

   java -classpath .:HOD_SERVER_DIR/sm.zip:$CLASSPATH

   com.ibm.hodsslight.tools.keyrng CustomizedCAs verify

   This should be followed by something similar to the following:

   ```
   --------Key ring entry:  1 -------------------
   Entry type:  Site Certificate
   Key:  RSA/512 bits
   Subject:  aix-f26.raleigh.ibm.com,ibm,US
   Issuer:  aix-f26.raleigh.ibm.com,ibm,US
   Valid from:  Fri Aug 13 2:21:29 EDT 1999
   Valid to:  Sun Aug 13 12:21:29 EDT 2000
   Finger print:  D7:2D:E9:6B:66:00:54:04:44:DE:02:E4:4E:1C:80:85
   ```

   The last certificate shown should be the one just added.

(continued on the next page)

HOD SSL Server Certificate (cont.)

7. (cont.)

   I issued the following on my system:

   ```
   java -classpath .:/usr/lpp/HOD/hostondemand/lib/sm.zip:\
   /usr/lpp/java/J1.1/lib/classes.zip \
   com.ibm.hodsslight.tools.keyrng CustomizedCAs verify
   ```

   Note: The CustomizedCAs.class file does not remove any previous information but instead adds the new certificate information so the file may be corrupted if an error occurs when trying to use SSL like the following:

   ```
   keyrng: Cannot retrieve key ring data: com.ibm.hodsslight.SSLException
   ```

   or

   ```
   EZZ6021I TELNET PROFILE UPDATE FAILURE FOR PORT  723 on the system log,
   EZZ6029I PROFILE ERROR ON PORT   723, SSL NOT AVAILABLE
   ```

   If this happens try deleting the CustomizedCAs.class file from the publish directory and issuing the above java command again.

8. Exit OMVS.

HOD SSL Server Certificate (cont.)

9. Create HOD session with "Enable Security (SSL)" selected.

   Note: If you select "Server Authentication (SSL)" on your HOD session the 'Common Name' input when creating the certificate must match the host name in the DNS for the IP address of the TN3270E server.

10. On OS/390 TN3270E server create TELNET SECUREPORT statement and BEGINVTAM PORT statement in TCPIP PROFILE:

```
TELNETPARMS
   SECUREPORT 723 KEYRING HFS /u/harrisl/nm412.kdb
   ...
ENDTELNETPARMS
BEGINVTAM
   PORT 723
   ...
ENDVTAM
```

11. Recycle HOD and TCP/IP servers and you're done!

IBM ®

Appendix I:
Client Certificate and Browser

Client Certificate

➢ Create Client Certificate with GSKKYMAN

1. Create a new key database and self-signed certificate with GSKKYMAN, just like the server certificate. This is the client key database and public key.
2. Add this client certificate (public key) to the Server key database.
3. Use GSKKYMAN to export the key by using option "9 Export keys" to create a p12 file.
4. FTP p12 file (in binary) to the client workstation.
5. Use the workstation browser to upgrade the p12 certificate.

Client Certificate

- Create Client Certificate with GSKKYMAN
- Add Client Public key to Server Key Database:
  1. Start GSKKYMAN:

     gskkyman
  2. Open Server key database:

     nm512.kdb
  3. Enter password:

     one0ssl
  4. Store a CA certificate:

     6
  5. Enter certificate file name:

     lin512.crt
  6. Enter label:

     lin512
  7. Exit GSKKYMAN:

     1

Client Certificate

- Client Certificate and Netscape Browser
- Netscape Communicator 4.72 - On the Netscape Communicator window:
  1. Select Communicator, Tools, Security Info
  2. Select Yours under Certificates
  3. Select Import a Certificate
  4. Enter the password of the file to import it
  5. Select file that you FTPed from OS/390
  6. Enter password
  7. Select the P12 file that just appeared under "These are your certificates"
  8. Select Export
  9. Enter new password for the new file
  10. Enter the location to save the new file (to be used by HOD)

Client Certificate (cont.)

- Client Certificate and Internet Explorer Browser
- Internet Explorer V5 - On the Internet Explorer window:
  1. Select Tools, Internet Options
  2. Select the Content tab
  3. Select Certificates
  4. Select Import
  5. Enter filename to import it
  6. Enter the password of the file
  7. Select the P12 file that just appeared under "Issued To"
  8. Select Export
  9. Enter new password for the new file
  10. Enter the location to save the new file (to be used by HOD)

IBM ®

Bibliography

Bibliography

- Announcement Letters:
  - 200-324 IBM Host Access Client Package V1R0
  - 201-053 IBM Host Access Client Package V1R1
  - 200-262 IBM Host Publisher V2R2
- Program Directories:
  - GI10-3175-00 IBM Host On-Demand Version 5 for System/390
  - GI10-3176-00 IBM Screen Customizer Version 2 for System/390
- The following three documents are available after installation (where 9.82.1.100 is the IP address of the OS/390 system where HOD is installed) and they are also available on the HOD Library page off of the Host On-Demand Home page:
  - Host On-Demand Readme

    http://9.82.1.100/hod/en/doc/readme/readme.html
  - Planning and Installation Guide (also available in pdf as install.pdf)

    http://9.82.1.100/hod/en/doc/install/install.html
  - Host Printing Reference

    http://9.82.1.100/hod/en/doc/hostprint/hostprintref.html

Bibliography

- The following four documents are available from the "IBM Host Access Toolkit" directory after Toolkit installation:
  - Getting Started (also available from the Toolkit CD panel)
  - Host Access Class Library Reference
  - Host Access Beans for Java Reference
  - Open Host Interface Objects Reference
- The following Redbooks are available at http://www.redbooks.ibm.com:
  - IBM SecureWay Host On-Demand 4.0: Enterprise Communications in the Era of Network Computing, SG24-2149-01
  - IBM WebSphere Host On-Demand: Version 5 Enhancements, SG24-5989
  - IBM SecureWay Communications Server for OS/390 V2R8 TCP/IP: Guide to Enhancements, SG24-5631
  - IBM Web-to-Host Integration Solutions, SG24-5237-01

Bibliography

- IBM OS/390 manuals:
  - Communications Server for OS/390, IP Configuration, SC31-8513
  - Communications Server for OS/390, IP Configuration Guide, SC31-8725
  - Communications Server for OS/390, IP Configuration Reference, SC31-8726
  - System Secure Sockets Layer (SSL) Programming Guide and Reference, SC24-5877
  - OS/390 Security Server (RACF) Command Language Reference, SC28-1919

IBM ®

Web Sites

Web Sites

- Host On-Demand Product Information site:

  http://www-4.ibm.com/software/webservers/hostondemand

  Select Support from the above Home Page to get to the Support Page.

  Select Library from the above Home Page to get to the Library page.
- This presentation is available as presentation PRS162 on web site:

  http://www.ibm.com/support/techdocs