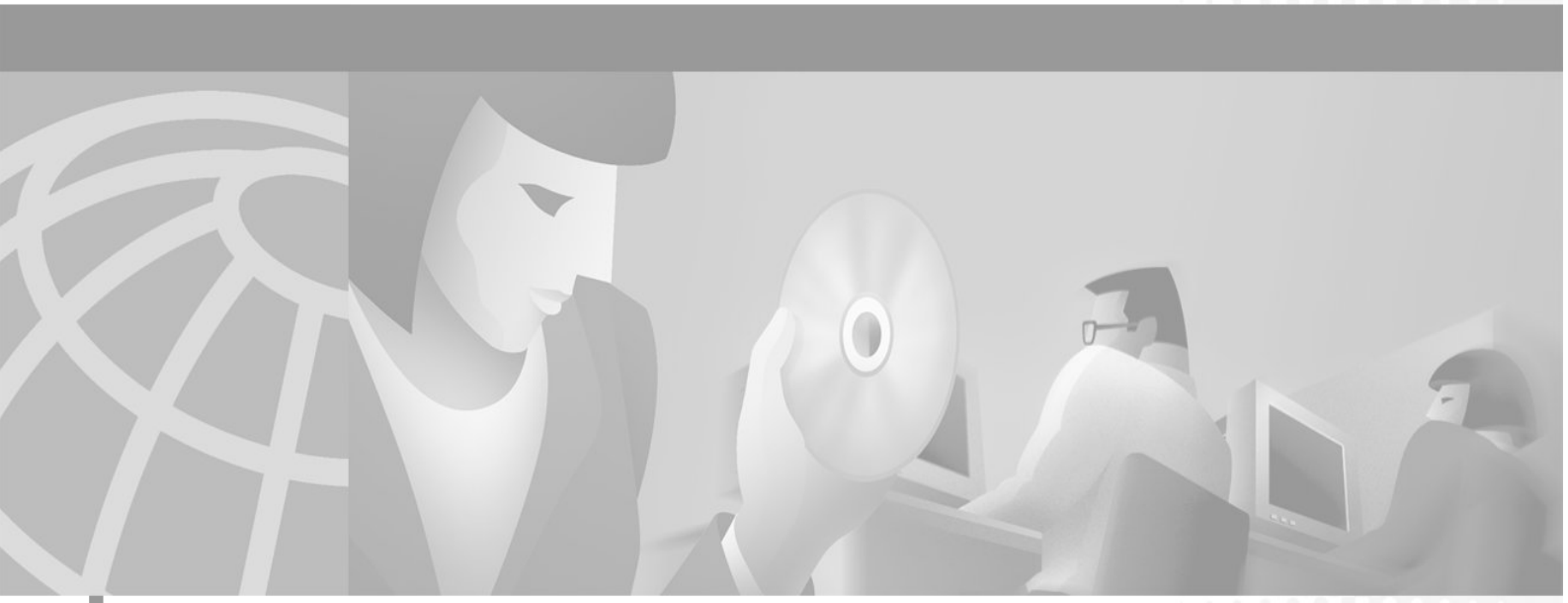


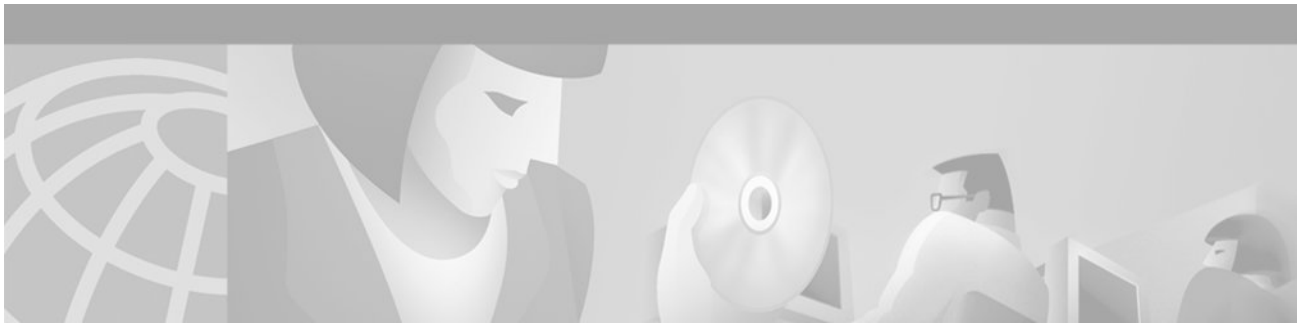
Cisco ICM

Release 6.0(0) Staging

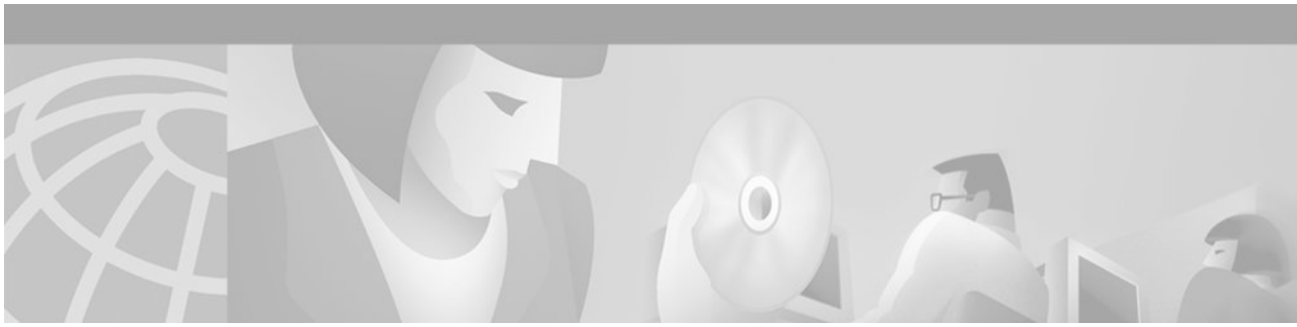
On Windows 2000

May 2004

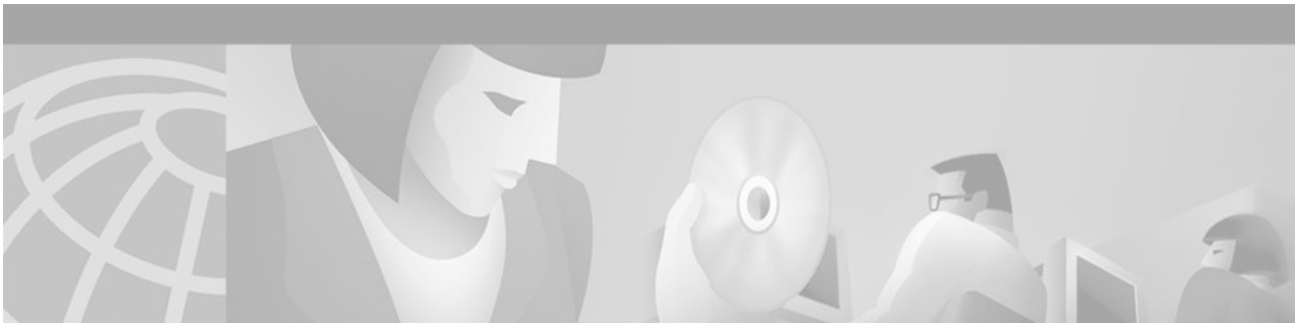
Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com



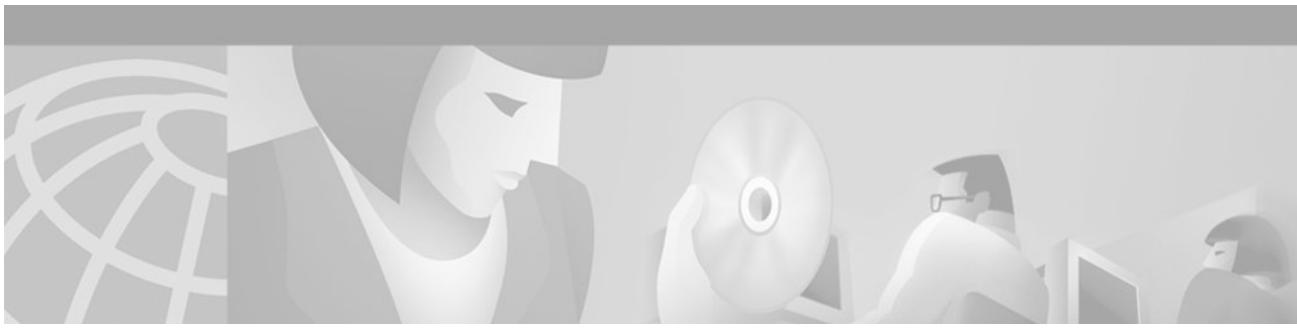
Contents



Tables



Figures



About This Guide

Purpose and Audience

This document is intended for the individuals responsible for staging new deployments of Cisco Enterprise ICM or Hosted NAM/CICM on Windows® 2000. Individuals should be trained on the use and functions of ICM as well as Windows 2000, Active Directory and DNS. This document does not provide detailed Enterprise ICM, Hosted NAM/CICM or Windows 2000 specific information. This information can be found elsewhere in specific documentation from Cisco and/or Microsoft.

This document contains system diagrams, staging steps and sample test cases for supported Models of Enterprise and Hosted ICM. Those Models are:

- Enterprise ICM Dedicated Forest/Domain Model
- Enterprise ICM Child Domain Model
- Hosted NAM/CICM Model

Individuals utilizing this document should have knowledge and experience with the following tools/software/hardware to stage the ICM software as described in this document:

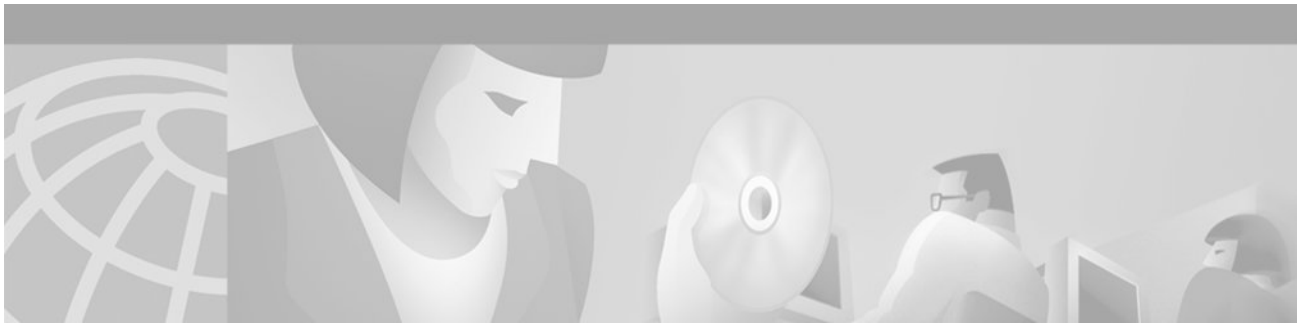
- Cisco ICM components and their functions
- Cisco ICM Scripting and Configuration Tools
- Cisco ICM WebView and third party software (if installed)
- Windows 2000 system administration
- Microsoft SQL Server administration.

Other Publications

If you are planning ICM or NAM/CICM deployments, you should have familiarity with the Cisco Intelligent Call Management Documentation relative to ICM, IPCC, NAM, and Remote Monitoring Suite. You can find the various guides for these products at Cisco.com

Use the companion guide, *Cisco ICM Windows 2000 Planning for Release 6.0(0)*, during the planning phase of an ICM/NAM deployment project to define the required Active Directory and DNS Plans and select a supported Windows 2000 Model.

Important: You should also read and follow the guidelines set forth in the document "*Security Best Practices for Cisco Intelligent Contact Management Software Release 6.0(0)*" before staging your Windows 2000 environment. The Security Best Practices document contains important guidelines for creating a secure Windows Server environment.



Staging Prerequisites

ICM System Design Specification

An ICM/NAM System Design Specification should be documented and accepted prior to every staging event. A System Design Specification consists of diagrams and records required to execute the Staging phase. An ICM 6.0(0) System Design Specification Template can be found at http://www.cisco.com/partner/WWChannels/technologies/IPCC/design2.html

These diagrams and records contain settings and values that are required inputs during the setup of all 3rd Party and ICM Software.

A System Design Specification should consist of:

- Description of ICM Sites and Nodes
- Data Communications Infrastructure
- Event Notification and Remote Access Points
- ICM Naming Convention for Domain, Instance, DNS Suffix, Sites, Networks, Hostnames
- IP Addressing Scheme
- Windows 2000 Model
  - Active Directory Plan
    - Domain Controllers
    - Trust Relationships
    - Domain Members
    - Standalone Servers
    - Active Directory Sites
    - Time Source
  - DNS Plan
    - DNS Servers and Clients
    - DNS Forward and Reverse Lookup Zones and Records
- System Diagrams
- Configuration Settings (Physical Controller ID's, Logical Controller ID's and Peripheral Controller ID's)
- 3rd Party Host Forms – entries/values for fields which are blank or different from defaults utilized during Setup of 3rd Party Software

- ICM Node Charts – entries/values for fields which are blank or different from defaults utilized during Setup of ICM Software

Platform Hardware and Software

During the System Design phase of an ICM deployment project, the Hardware specifications and 3rd Party Software requirements are defined. Cisco's guide for Hardware and 3rd Party software is the Bill of Materials for Contact Center Software Applications contains Cisco's recommendations for hardware and third party software. You can find this guide on http://www.cisco.com/.

Staging Environment

Perform the following tasks prior to ICM or NAM Staging:

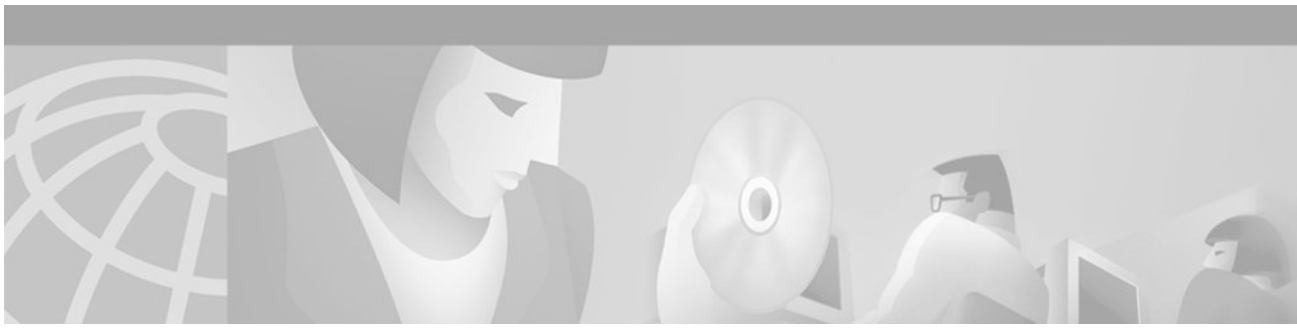
- Stage all machines in racks, or on a work surface, with the following:
  - RAM installed
  - Hard Drives installed
  - RAID arrays configured
  - Video and Ethernet Cards installed
  - All multiple rack mount systems occupying the same rack are attached to keyboard, mouse and monitor sharing unit
  - All machines are labelled with HOSTNAME per System Diagram. All ethernet connections are labelled "visible" or "private"
  - There are sufficient power outlets for all machines to be simultaneously connected and turned on
- Ensure there are at least 2 phone lines for testing of dialup modem access
- Ensure all CDs (software), driver software on diskette or CD and Vendor documentation for all platforms are in the work area
- Ensure all Software License Numbers are available
- Ensure the simulated ICM Network is in place and successfully tested
  - All LAN Switches are configured for required subnets per ICM System Diagram.
  - All IP CallRouters are configured as required
  - IP connectivity between all subnets has been successfully tested
  - Required ethernet connections are in place between ICM platforms and LAN switches.
  - Required Packet prioritisation has been configured on IP CallRouters
- Ensure the assigned engineers can follow the Staging Plan, and are available on site for the duration of the Staging event

Remote Monitoring Suite Support Change for ICM 6.0

Starting with ICM Release 6.0(0), Cisco is adding no new customers to the list of those it currently monitors remotely via the Cisco Remote Monitoring Suite (RMS).

However, the RMS can still be purchased and installed by any customer who wishes to monitor their own ICM system deployment. Sections of this document that refer to RMS or "Phone Home" may not apply to your deployment if you are not using RMS.

More information on RMS can be found on the web at
http://www.cisco.com/en/US/partner/products/sw/custcosw/ps2068/



Enterprise ICM Dedicated Forest/Domain Model

Sample Diagrams

Figure 1 Enterprise ICM Dedicated Forest/Domain Model- Central Controller Sites

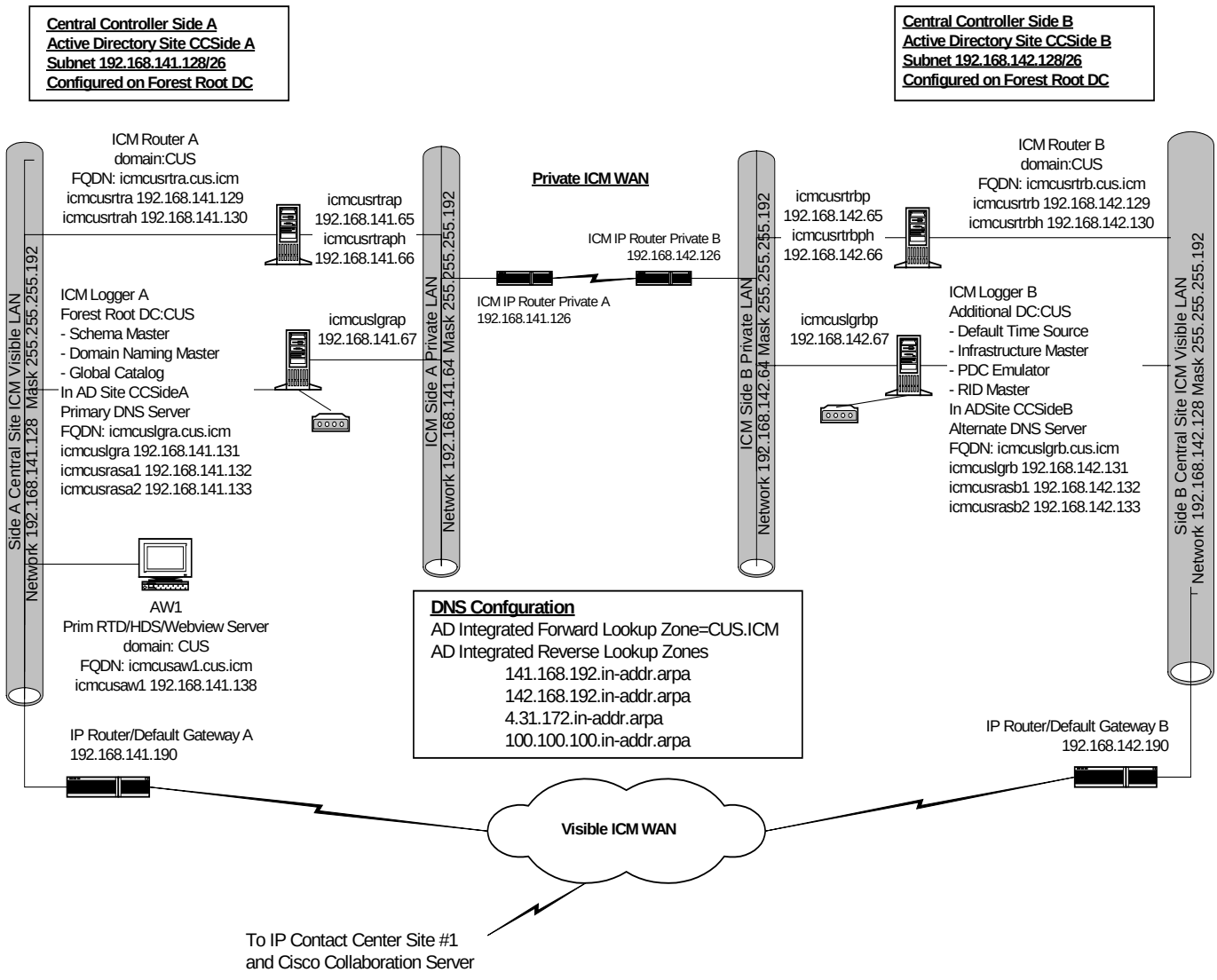
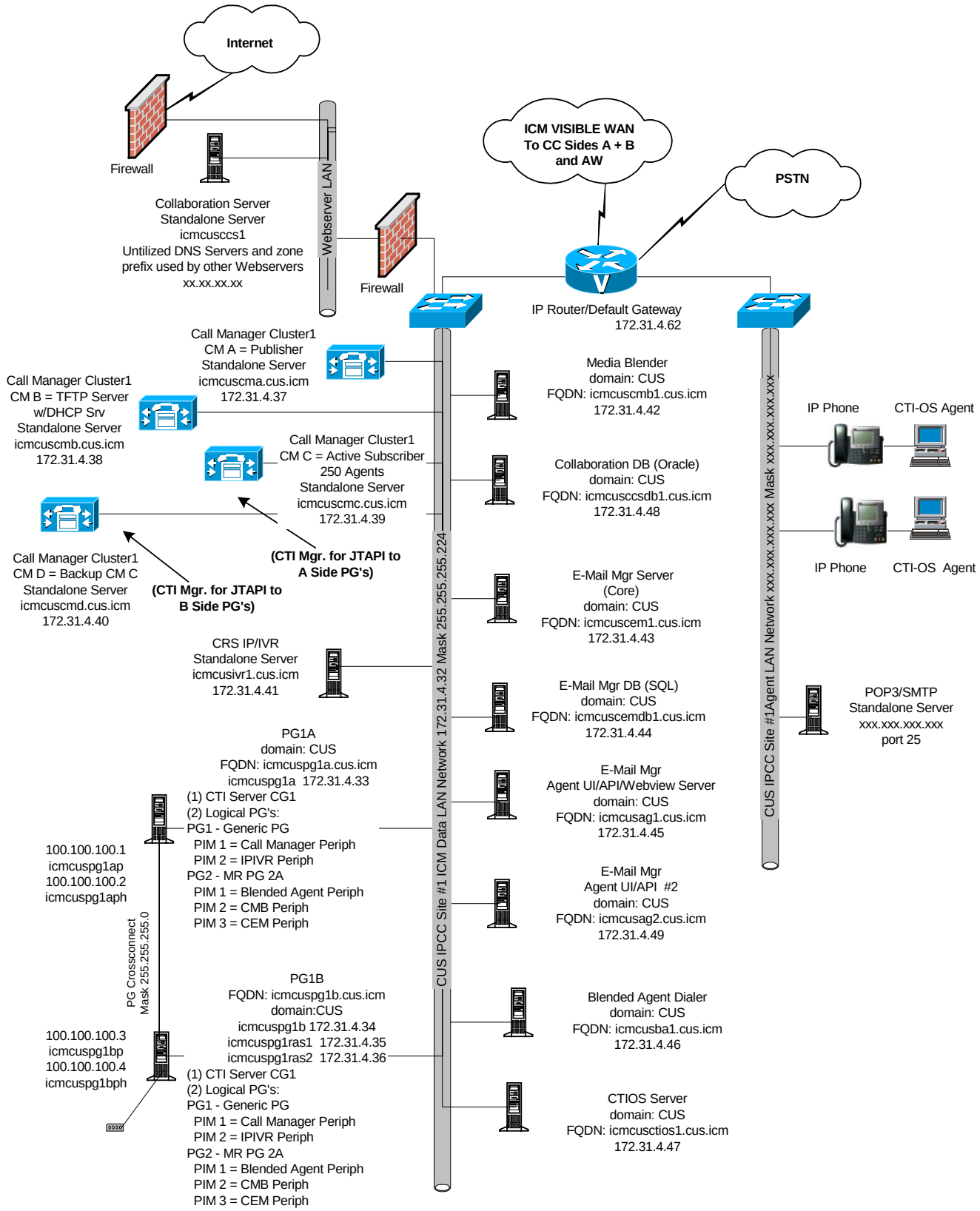


Figure 2 Enterprise ICM Dedicated Forest/Domain Model-Contact Center Site



Staging Tasks

Step No.	Task
1.	Validate that Staging Prerequisites have been met
2.	Install Windows 2000 SP4 on All Servers - Standalone
3.	Apply Custom Settings on All Servers
4.	Install Forest Root Domain Controller/DNS Server
5.	Configure DNS Server on Forest Root Domain Controller
6.	Install Additional Domain Controller
7.	Install and Configure DNS on Additional Domain Controller
8.	Configure Active Directory Sites
9.	Assign Global Catalog and FSMO Roles and Configure Time Source
10.	Configure Trust Relationships
11.	Join Standalone Servers to Domain
12.	Change Domain Controllers to Native Mode
13.	Install PCAnywhere
14.	Validate IP Connectivity and Remote Access
15.	Install SQL Server on Loggers and AW's
16.	Install E-Mail Manager database
17.	Install Collaboration database
18.	Install Webview 3rd Party Software
19.	Install Infomaker on AW's
20.	Install ICM Software on Loggers
21.	Create Logger Databases
22.	Install ICM Software on CallRouters
23.	Start Logger and Router Services
24.	Install ICM Software on Admin Workstations
25.	Expand AW Database
26.	Create HDS Databases
27.	Start AW (Distributor) Services
28.	Configure NIC's, Peripheral Gateways and Peripherals
29.	Configure Multi-Media Nodes
30.	Create and Configure CONAPI Connections
31.	Install ICM Software on Peripheral Gateways
32.	Install ICM Software for CTI Server

Step No.	Task
33.	Install CTI OS Server
34.	Start PG, CTI and CTIOS Services
35.	Install and Start Blended Agent Dialer
36.	Install and Start E-Mail Manager Servers
37.	Install Collaboration Server
38.	Install and Start Media Blender Server
39.	Complete Staging Tests
40.	Complete Settings for Production Environment
41.	Complete Staging Issues Record

Step 1. **Validate that Staging Prerequisites have been met**

See Staging Environment section of this document (see Page 7).

Step 2. **Install Windows 2000 Server and Service Pack 4 on All Servers - Standalone**

Install Windows 2000 Server CD.

Create Drive Partitions according to settings in the 3rd Party Host Form, for the machine being built. You may need to use the equipment manufacturer's drive partitioning/RAID array software to set up the partition. Format the C drive as NTFS.

Recommendations

Logger and AW/HDS: Create the C drive during this phase of the installation and create the D drive in the Custom Settings of this document.

- Drive C: Operating System/Boot Partition, virtual memory swap file space, core ICM software and SQL Server as well as SQL log and temp files.
- Drive D (which you create later): Used by SQL to store ICM database (logger database and HDS database on AW). Keep log and temp files for these databases on Drive C to maximize database performance.

CallRouters, PG's, AW's (non-HDS), CTI Server, CTIOS Server.

- Drive C: single drive partition for OS/Boot Partition, virtual memory, swap file space, core ICM software and for AW non-HDS database, SQL Server and all SQL databases.

The system reboots and displays the Windows 2000 Server Setup wizard. Perform the steps listed below.

1. The first prompt is Regional Settings. You set system local and keyboard layout.
2. Next, enter Company Name and Organization.
3. Select Per Seat Licensing.
4. Enter the hostname for machine and Administrator Password (refer to 3rd Party Host Form).
5. Highlight Management and Monitoring Tools and click **Details**.
   - Only Check Network Monitor Tools.
   - Click **OK**.

6. Under Windows 2000 Components, uncheck IIS unless this machine will host a Webview Server, Collaboration Server, Media Blender or any of E-Mail Manager Servers. In the case of these particular servers, highlight IIS and click on Details. Only check Common Files, Front Page 2000 Server Extensions, Internet Information Services Snap-In, Internet Services Manager, , and World Wide Web Server.
7. Enter the Correct Date/Time.
8. Date and Time Zone Settings.

Note: All central controller systems must be in the same time zone regardless of physical location

9. Under Network Settings, select Custom Settings. Refer to the system diagram and/or third party host form for each server's respective IP and DNS information.
10. For the Visible Ethernet Card, set the properties for **File and Printer Sharing** for Microsoft Networks to maximize data throughput for network applications.
11. For the Visible Ethernet Card, the Protocol is TCP/IP. Click **Properties**.
    - Enter the information for visible IP address, subnet mask, default gateway and preferred and alternate DNS servers for the machine.
    - Click the Advanced tab.
    - Enter the "high" visible addresses from the ICM System Diagram, if applicable.
    - On the DNS Tab, in "DNS suffix for this connection" enter the name of the local DNS zone for the machine and check the "Register" box.
    - If this machine requires access to resources in a different trusting/trusted domain/DNS zone, select "append these DNS suffixes (in order)" and enter the local DNS zone for the machine first and add other secondary zones which represent the trusting/trusted domain.
12. For the Private Ethernet Card: when you click "next" on the networking components, another Networking Components screen opens if the machine has more than one network interface card.
    - Uncheck the Client for Microsoft Networks and File and Print Sharing options.
    - The Protocol is TCP/IP. Click **Properties**.
    - Enter the private IP address and subnet mask for the server. Leave the default gateway field blank.
    - Click on Advanced tab and enter the "high" private addresses, if applicable.
    - For the DNS tab, leave the address space empty and uncheck the "register" box.
13. Under Workgroup or Computer Domain, select "No, this computer is not on a network, or is on a network without a domain." The machine restarts.
14. After the restart, login with new the Username and created during setup. The "Configure Your Server" wizard opens. Select "I will configure this server later." Uncheck "Show this screen at startup."
15. Install Windows 2000 Service Pack 4. Restart the machine upon completion of the Service Pack install.

Step 3. Apply Custom Settings on All Servers

Validate Card Settings and add other protocols (if required)

1. Right-click on My Network Places and select **Properties**. The Network and Dial-Up Connections window opens.
2. Rename each "Local Area Connection" icon to "private", "visible" and "san" as required.
3. On each card right-click **Properties** and select **Configure**.
    - Click on the Advanced tab.
    - Configure the network speed and duplex mode. Do not set to Auto Mode.

4. Right-click on the Visible icon and select **Properties**.

Note: NETBEUI is required on systems that will have Phone Home enabled. Phone Home is typically enabled on Loggers that Phone Home events to Cisco TAC.

5. View the components section and, if NETBEUI is required and does not appear, click **Install**.
   - Highlight Protocol and click **Add.**
   - Highlight NETBEUI Protocol and select **OK.**
   - After NETBEUI installs, you return to the Properties window.
6. Under the Advanced menu, select **Advanced Settings**. The Visible Card should be bound first.
   - View the Connection section of the Adapters and Bindings tab. Sort the section so that the Visible connection is at the top, Privite is second and any remaining connections follow.
   - Highlight the Private connection and, in the Bindings Section, uncheck File and Printer Sharing for Microsoft Networks and Client for Microsoft Networks.
   - Move any disabled Bindings for all connections to the bottom of the list using the Up/Down arrows adjacent to the Bindings Window.

   Note: You only need to complete the following 2 steps if NETBEUI is installed (typically on Loggers).
   - Highlight the Visible connection and uncheck all NETBEUI protocol bindings and move them to the bottom of the bindings list.
   - Highlight the Private connection and uncheck all NETBEUI protocol bindings and use the UP/Down arrows to move them to the bottom of the bindings list.

Create Drive Partitions

These steps show you how to create drive partitions, as detailed on 3rd Party Host Form

1. Click **Start > Programs > Administrative Tools > Computer Managemt**.
2. Under Storage, select **Disk Management**.
3. Assign the drive letter Z to the CD-ROM.
4. Create Drive D as a primary partition using all remaining disk space on a RAID volume. If there is disk space on more than one physical disk, do not create a Volume Set.
5. Format the drive as NTFS and choose whether or not you want to use Quick Format.

Create Shares per Customer Requirements.

There must be a hidden share for the C drive on Loggers. This is required for Listeners to access “phone home” events.

Disable Automatic Updates

1. Open the Control Panel and double-click Automatic Updates.
2. Uncheck “Keep my computer up to date….” and click **OK**.

Configure the Display

1. Open the Control Panel and select Display.
2. Verify that no Screen Saver is selected.
3. Set Display for at least 1024x768 resolution, 65K colors and at least 60 MHz.

Set System Properties

1. Open the Control Panel and double-click on **System**.
2. Click the Advanced tab.
3. Click on Performance Options.
4. Set Virtual Memory as required.
    - If you have less than 2G RAM, set Virtual Memory to 1.5-times the physical size.
    - If greater than 2G RAM, set Virtual Memory to 2G.
5. Click Startup and Recovery.
6. Change the value of the Display list of operation systems to 3 seconds.
7. Click **OK** twice.

Configure the Event Viewer

1. Click **Start > Programs > Administrative Tools > Event Viewer**.
2. Highlight each Type in the left column, right-click, select **Properties** and set the log to 1024Kb. Select **Overwrite Events as Needed**. Install Routing and Remote Access as detailed on the 3rd Party Host Form, if necessary.

Note: Routing and Remote Access is required for Loggers using modems to Phone Home, and for any other remote access points (typically 1 PG per Contact Center Site) for TAC to utilize.

3. Click **Start > Programs > Administrative Tools > Routing and Remote Access**.
4. Highlight the machine name and under the Action menu, select Configure and Enable Routing and Remote Access.
5. Click **Next** to start the Routing and Remote Access Server Setup wizard:
    - On the Common Configurations Screen, select Remote Access Server and click **Next**.
    - On the Remote Client Protocols, verify that TCP/IP (and NETBEUI, if required) are listed. Select "Yes, all of the required protocols are on this list" and click **Next**.
    - Under Network Selection, highlight the visible card and click **Next**.
    - For IP Address Assignment, select "From specified range."
    - Under the Address Range Assignment Screen, add Range of RAS addresses (from System Diagram) and click **Next**.
    - Click **NO** to Radius Server and click **Next**. Finish the setup (ignore the DHCP warning if you get one).

For Machines which allow Dial-In Access:

1. Right-click the Machine Name and select **Properties**.
    - Under General Tab and click **Remote Access Server**.
    - For Machines which allow Dial-In Access for TAC Maintenance:
        - On the IP Tab, enable IP Routing.
        - On the NETBEUI Tab, uncheck "Allow NetBeui remote access."
    - For Listeners**:**

- For the IP Tab, do not Enable IP Routing.
- For the NETBEUI Tab, allow access to "This Computer Only".

2. Open **Computer Management > Local User and Groups > Users**.
   - Double-click on the Administrator account.
   - Select Allow Access on the **Dial In** tab.

   Note: Routing and Remote Access Service is not supported on Windows 2000 Professional. Any Peripheral Gateway used with RRAS must run Windows 2000 Server.

Create a Software directory and load folders, as detailed on the 3rd Party Host Form

Add Persistent Static Routes as detailed on 3rd Party Host Form

For geographically distributed central controller sites, the CallRouters and Loggers have a Private IP WAN connection, used to communicate between side A and side B. Windows only allows one "default gateway" for each machine, which sends the Private Network traffic to the Visible Network. You need to add a set of Static Routes to the CallRouter and Logger systems on both sides of the system to direct this traffic to the Private Network.

1. On CallRouter A and Logger A:

   route add <network number> mask <subnet mask> <gateway IP> -p

   Example: route add 192.168.142.64 mask 255.255.255.192 192.168.141.126 –p

   Where:
   The network number of the remote Private Network is 192.168.142.64
   The subnet mask for this remote network is 255.255.255.192
   The local Private Network Adaptor Card's IP Address is 192.168.141.126

   (-p sets the route as persistent)

2. On CallRouter B and Logger B:

   Example: route add 192.168.141.64 mask 255.255.255.192 192.168.142.126 –p

Configure Telnet Security as detailed on 3rd Party Host Form

Windows 2000 provides a Microsoft standard Telnet utility that comes pre-configured to allow users to start connections without logging into the domain for account validation. To help secure the ICM systems, set this to require users to login using Telnet by using the Windows Registry Editor.

1. Run the file **regedit32.exe**. Expand **HKEY_Local_Machine\Software\Microsoft\Telnetserver\1.0**.
2. Set NTLM to ZERO (0) to require users to login.
3. Set the Telnet Service to Autostart and Stopped/Started.

Step 4. Install Forest Root Domain Controller/DNS Server

Note: The Domain Controllers/DNS Servers do NOT have to be co-located with the ICM Loggers. They may be installed on separate servers.

1. Click **Start > Run**, enter **DCPROMO** and click **OK**. The Active Directory Installation wizard opens.
2. Under the "Domain Controller Type," select the "Domain Controller for a New Domain." The "Create Tree or Child Domain" screen appears.
3. Select "Create a new Domain Tree," the "Create or Join Forest" screen appears.
4. Select "Create a New Forest of Domain Trees" "New Domain Name" screen opens. Type in the full DNS name for the new domain.
5. On the "NetBIOS Domain Name" screen, type in the NetBIOS name.
6. Accept Database and Log Location defaults.
7. Accept the Shared System Volume default. A warning appears claiming that the wizard cannot contact the DNS Server (since you have not configured it yet). Click on **OK** and you are presented with the "Configure DNS Screen." Select "Yes, install and configure DNS on this computer."
8. On the "Permissions" screen, select "Permissions compatible with pre-Windows 2000 servers."
9. On the "Directory Services Restore Mode Administrator Password," input Administrator password as detailed in the 3rd Party Host Form.
10. On the Summary screen, check Settings and click on **Next**. Insert the Windows 2000 CD and setup continues to install Active Directory and DNS Server.
11. Restart when the installation completes.

Step 5. Configure DNS Server on Forest Root Domain Controller

1. Click **Start > Programs > Admin Tools > DNS**.
2. Expand Hostname Tree.
3. Expand Forward Lookup Zones.
4. Right-click the root folder (the folder named ".") and select **delete**. You receive a warning about the zone and click **Yes**.
5. Highlight the machine name, right-click and select **Properties**.
6. On the Interfaces Tab, select "Listen on Only the following IP addresses" and remove all but the visible machine address.
7. Complete the configuration of AD Integrated Forward and Reverse Lookup Zones.
    - Highlight the ICM Domain zone name under Forward Lookup Zones, right-click and select **Properties**.
    - On the General Tab, for "Allow Dynamic Updates," select "Only Secure Updates" from the menu.
    - Only use the Zone Transfers Tab when there is a Trust between this domain and another domain, in which case you need to Transfer Zone updates from this Active Directory Integrated Zone to a Standard Secondary Zone on the DNS Servers in the other domain. You "Allow Zone Transfers" then select "only to the following servers" and enter the IP Addresses of the DNS Servers in the other domain.
    - To configure the required Reverse Lookup Zones, repeat the steps below for each ICM domain level network within the Forward Lookup Zone.

    Note: Networks within a Forward Lookup Zone include all visible and private networks utilized within a DNS Zone. These networks define Reverse Lookup Zones relative to the Forward Lookup Zone.
8. Under the Server Name, right-click on Reverse Lookup Zones and select **New Zone**.
9. Within the New Zone wizard, select "Active Directory Integrated."
10. In the Reverse Lookup Zone screen, select the radio button "Network ID" and enter the required number of octets for the Reverse Lookup Zone. The Reverse Lookup Zone Name automatically enters.
11. Repeat the steps below for each ICM domain Reverse Lookup Zone.

- Highlight the Zone name under Reverse Lookup Zones, right–click and select **Properties**.
- On the General Tab, for "Allow Dynamic Updates," select "Only Secure Updates" from the menu.

Manually complete DNS Host and PTR records

1. Manually enter the hostnames for the machines that house ICM nodes, as well as all NIC's and Peripherals for which ICM Setup requires hostname resolution, into the appropriate DNS Forward Lookup Zone.
2. On the DNS Server, right-click on the Forward lookup Zone Name and select "New Host."(The hostname of this Root Domain Controller should already be in the file.)
3. Add all ICM hostnames (visible, visible high, private, private high, SAN) and their associated IP Addresses. Check the box to create an associated PTR Record (reverse lookup zone record).
4. Manually enter any Peripherals (ACD's/VRU's) and NIC's accessed by the ICM by hostname resolution in the Forward Lookup Zone.

Step 6. Install Additional Domain Controller

Note: The Domain Controllers/DNS Servers do NOT have to be co-located with the ICM Loggers. They may be installed on separate servers.

1. Click **Start > Run** and enter **DCPROMO**. Click **OK**, the Active Directory Wizard opens. Click **Next**.
2. Under "Domain Controller Type," select "Additional Domain Controller for an Existing Domain."
3. At the "Network Credentials" screen, input the domain admin username and password.
4. The Additional Domain Controller screen should already be filled in properly with the fully qualified DNS name.
5. Accept database and log locations defaults.
6. Accept shared System Volume defaults.
7. Input the same Restore Mode Admin password utilized on the Root Domain Controller.
8. Check Summary Settings. AD is not configured through NETLOGON.
9. Reboot when AD Install is complete.

Step 7. Install and Configure DNS on Additional Domain Controller

1. Click **Settings > Control Panel > Add/Remove Programs**.
2. On the Add\Remove Windows Components, check Networking Services and select **Details**.
3. Check only DNS, click **OK** and select **Next**.
4. Browse to the Windows 2000 CD. DNS installs Windows 2000.
5. Validate that all DNS Zones were replicated from the 1st DNS Server in the AD Domain to this DNS Server.
    i. Highlight machine name and right-click, select properties.
    ii. On the Interfaces Tab – select Listen on Only the following IP addresses – remove all but visible machine address

Step 8. Configure Active Directory Sites

On ICM Root Domain Controller:

1. Click **Start > Programs > Admin Tools > AD Sites and Services**.
2. Rename the default first site name as per AD Site Plan in the ICM System Diagram.

- For a geographically separated DC, right-click on Sites, select New Site and enter the site name of the additional domain controller as per the ICM System Diagram.

3. Create subnets for each DC site:
   - Right-click on the Subnets folder and select New Subnet.
   - Enter the subnet address and mask, respective to the LAN at the Domain Controller Site.
   - Highlight the Site Name associated with that subnet.
4. Expand the Servers folder from the original first site folder. For each Server you need to move to a different site, right-click on server name, select **Move** and highlight the Site you want to move it to.
5. Expand "Inter-Site Transport" under Sites.
   - Open the "IP" folder and select "DEFAULTIPSITELINK" from the right pane.
   - Right-click and select **Properties**, and make sure that both sites have been "Added" as entries in the window titled "Sites in this Site Link."
   - Change the "Replicate Every" value to 15 minutes.

Step 9. Assign Global Catalog and FSMO Roles and Configure Time Source

Add Global Catalogs for the GC and FSMO plan in the ICM System Diagram and for settings on 3rd Party Host Forms.

1. Open AD Sites and Services.
2. Connect to the DC designated as the GC.
3. Right-click on NTDS Settings and select **Properties**. Check off Global Catalog.
4. Move FSMO roles, as indicated in the ICM System Diagram and as per settings on 3rd Party Host Forms.
   - **Infrastructure Master, PDC Emulator, RID Master:** On AD DC hosting the role to be moved, open AD Users and Computers – Connect to the DC to which the role needs to be moved
   - Right click on domain name and select Operations Masters. Under the required FSMO role TAB, CHANGE the Operations Master to this designated DC
   - **Domain Naming Master:** On AD DC hosting the role to be moved, open AD Domains and Trusts – Connect to the DC to which the role needs to be moved
   - Right click on Active Directory Domains and Trusts and select Operations Master. Click change to move the role.
   - **Schema Master:** On AD DC hosting the role to be moved, open the Management Console and add the Active Directory Schema snap-in. Note: You may need to run the file named adminpak.msi in the \winnt\system32 directory, in order to add the Active Directory Schema snap-in.
   - Right click on Active Directory Schema and select Change Domain Controller - Select Specify Name and type in the name of the domain controller that you want to transfer the schema master role to
   - Right click Active Directory Schema and select Operations Master. Click change to move the role.
5. On the AD, move the DC hosting the role. Open the AD Users and Computers and connect to the DC to which you're moving the role.
6. Right-click on the domain name and select Operations Masters. Under the required FSMO role Tab, change the Operations Master to this designated DC.

The Forest Time Source defaults to the PDC Emulator, which is originally created on the Forest Root Domain Controller. If the PDC Emulator has been moved to another Domain Controller, the Time Source must be redefined as either that server or an external Time Source may be utilized. Since the PDC Emulator was moved to another Domain Controller, you need to redefine the Time Source as either that server, or using an external Time Source.

On the Server currently running the PDC Emulator, run the following command:

Net time /setsntp: <DNS Name of Time Source >

To synchronize a Server to the Time source:

W32tm -s <DNS Name of Time Source>

Step 10. Configure Trust Relationships

Typically, in the Enterprise ICM Dedicated Forest/Domain Model, a trust relationship with an outside domain is not required, unless there are Administrative Workstations (Real Time Distributors or Real Time Clients) which the customer prefers to place in a domain external to the ICM domain.

Step 11. Join Standalone Servers to Domain

1. Right-click on My Computer and select **Properties > Network Identification Tab > Properties**.
2. Click on the Domain radio button and enter the Fully Qualified Domain Name.
3. Enter the Domain Administrator's username and password.
4. Reboot the Server and login to the Domain.
5. Create shortcuts on desktop as detailed on 3rd Party Host Form.
6. Configure the Command Prompt.
   - Open the Command Prompt from the Desktop Shortcut.
   - Right-click in title bar and select **Default**.
   - For the Options tab, uncheck Quick Edit Mode and Insert Mode.
   - Click on the font tab and set the Command Prompt font size to 7x12.
   - Click on the layout tab and set the Command Prompt screen buffer to 200x9999.

Next, you set the Folder Options:

1. Open Control Panel and select Open Folder Options.
2. On the General Tab, select **Active Desktop > Use Windows Classic Desktop > Web View > Use Classic Folders**.
3. On the View Tab, Display the full path in the address bar and title bar. Click Show hidden files and folders and uncheck Hide file extensions.

Step 12. Change Domain Controllers to Native Mode

Cisco ICM functions with Active Directory in both "Mixed" and "Native" modes. Microsoft recommends that you change an AD domain to native mode if an implementation does not and will not have any future NT domain controllers. You can only change the mode from mixed to native. Once the domain is running in native mode, you cannot change it back to mixed mode.

1. Open the Active Directory Domains and Trusts.
2. Right-click the domain node for the domain you want to administer and then click **Properties**.
3. In the General Tab, click **Change Mode** and then click **Yes**.

Step 13. Install PCAnywhere

1. Run the setup executable (**pcA105r.exe**) and accept the license agreement.
2. Use the TYPICAL setup type.

3. Cancel the Welcome to Live Update window.
4. Skip Registration and click **Finish**. Click **Yes** to reboot.
5. Open PCAnyWhere (Skip Registration).
   - Double-click the Add a Host icon
   - On the Connections Tab, select **TCP/IP**.
   - On the Settings tab, check Launch with Windows, Run Minimized, Run as a Service.
   - On the Callers tab, select Active Directory from Authentication Type menu.
   - Under Caller List click on New Item icon.
   - On the Identification tab, select GROUP and from the Domain menu select domain of this machine and select the Domain Admins Account.
   - On the Privileges Tab, select Superuser and click **OK**.
   - Under the Security Options tab, under the Encryption Level, select PCAnywhere from the menu, check off "Deny Lower Encryption Level" and click **OK**.
   - Give the new Host icon the same name as the machine.
   - Double-click this icon to start the host service.
6. Access Services in the Control Panel. In the Startup button, configure the PCAnywhere service to start automatically

Step 14. Validate IP Connectivity and Remote Access

On each machine, validate the settings on each network card (TCP/IP Properties), including the DNS settings. Referring to the System Diagram, validate that the machine can ping every machine on the visible network and, if applicable, that it can ping to all its private connections.

Validate the Host and PTR records on all DNS Servers to make sure that they contain all required zones and records.

At this time, test remote access through the modem access points. You should be able to access each machine by modem, utilizing PCAnywhere and utilizing Telnet.

Step 15. Install SQL Server on Loggers and AW's

Note: ICM servers must be members of the domain before you install SQL Server. You should not install SQL Server during staging if you do not have access to the domain controller(s) designated for your ICM servers.

1. Select STANDARD EDITION to start SQL Server setup program.
2. At the first screen select Install SQL 2000 Server Components.
3. Select Install Database Server.
4. Click **NEXT** at Welcome Screen.
5. In Computer Name screen, use default Local Computer.
6. In Installation Selection screen, choose default "Create a new instance of SQL Server, or install Client Tools".
7. Enter name for user and company in User Information screen.
8. Agree to License Agreement by clicking **Yes**.
9. In Installation Selection screen, choose default "Create a new instance of SQL Server, or install Client Tools".
10. Enter name for user and company in User Information screen.
11. Agree to License Agreement by clicking **Yes**.
12. In Installation Definition screen choose default "Server and Client Tools".

13. For Instance Name check Default.
14. Select **CUSTOM** for setup type.
15. Install Program Files to C: (the default).
16. For Components Screen accept defaults.
17. Under Services Accounts, select:
    1. CUSTOMIZE
    2. USE THE LOCAL SYSTEM ACCOUNT
    3. AUTO START SERVICES
    4. SQL SERVER AGENT
    5. USE THE LOCAL SYSTEM ACOUNT
    6. AUTO START SERVICE – Check **OK** for the window that appears.
18. On the Authentication Mode Screen, select "mixed mode" and check "blank password".
19. Set Collation Designator to Latin1_General and Check **Binary for Sort Order**.
20. Under Network Libraries deselect all choices except for NAMED PIPES.
21. Read the Start Copying Files screen and click **Next**.
22. Select PER SEAT as the licensing method and set 40 devices at least.
23. A dialog box with message "Setup is installing Microsoft Data Accessing Components (MDAC)" show up.
24. If a message box for Configure SQL Agent pops up, click **OK**.
25. When setup is complete, Reboot.
26. Install SQL Server Service Pack 2.
    - Run the **setup.bat** file.
    - For Computer Name select Local Computer.
    - Accept the license agreement.
    - For the Instance Name, accept the default.
    - Connect to the Server using SQL Server System Administrator login. Select "leave sa password blank".
    - Complete the setup and reboot the machine.
27. Expand the database sizes and logs using SQL Enterprise Manager. Click **Start > Programs > Microsoft SQL Server > Enterprise Manager**. Under Server Name in Enterprise Manager, double-click on Databases. Expand the Server Tree and highlight the Databases folder under the Server name.
28. Double-click the Master Database in the right panel, The Master Properties window appears.
    - On Data Files Tab:
      - Set Space Allocated to 50MB.
      - Uncheck Autogrow.
    - On the Transaction Log Tab:
      - Set Space Allocated to 20MB.
      - Uncheck Autogrow and click **OK**.
29. Double-click on Tempdb in the right panel. The tempdb **Properties** window appears.
    - On the Data Files Tab:
      - Set Space Allocated to 50MB.
      - Uncheck Autogrow.
    - On the Transaction Log Tab:
      - Set Space Allocated to 20MB.
      - Uncheck Autogrow and click **OK**.
    - On the Options Tab – Verify the following settings:

- Uncheck the following: ANSI NULL default, Recursive triggers, Auto close, Auto shrink and Use quoted identifiers.
- Check: Auto update statistics, Torn page detection and Auto create statistics.

o Close the Enterprise Manager.

Step 16. Install E-Mail Manager Database

1. Select STANDARD EDITION to start SQL Server setup program.
2. At the first screen select Install SQL 2000 Server Components.
3. Select Install Database Server.
4. Click NEXT at Welcome Screen.
5. In Computer Name screen, use the default Local Computer.
6. In Installation Selection screen, choose the default "Create a new instance of SQL Server, or install Client Tools".
7. Enter a name for user and company in the User Information screen.
8. Agree to License Agreement by clicking **Yes**.
9. In Installation Definition screen choose default "Server and Client Tools".
10. For Instance Name check **Default**.
11. Accept **TYPICAL** as Setup Type (default).
12. Under Services Accounts select:
    - o CUSTOMIZE
    - o USE THE LOCAL SYSTEM ACCOUNT
    - o AUTO START SERVICES
    - o SQL SERVER AGENT
    - o USE THE LOCAL SYSTEM ACOUNT
    - o AUTO START SERVICE – Check OK for the window that appears.
13. On the Authentication Mode Screen, select "mixed mode" and insert the SA password (for this example the password is left blank).
14. Set Collation Designator to Latin1_General and Check **Binary for Sort Order**.
15. Under Network Libraries, deselect all choices except for NAMED PIPES.
16. Read the Start Copying Files screen and click **Next**.
17. Select PER SEAT as the licensing method and set 20 devices per E-Mail Instance.
18. A dialog box with the message "Setup is installing Microsoft Data Accessing Components (MDAC)" appears.
19. When setup is complete, reboot the machine.
20. Install SQL Server Service Pack 2.
    - o Run **setup.bat**.
    - o For the computer name, select the Local Computer.
    - o Accept the license agreement.
    - o For the Instance Name, accept the default.
    - o Connect to the Server using SQL Server System Administrator login and enter SA for the password.
    - o Complete the Setup and reboot the machine.

Special Notes if Installing Oracle:

- o Use UTF8 character set

- Select at least 20 for Concurrently Connected Users
- Select Dedicated Server Mode.
- Set Maximum Datafiles to 700.
- Set Maximum Log Files to 70.
- Set Maximum Log Members to 5.
- Check Enable Archive Log.
- Set Log Archive Buffers to 5.

Step 17. Install Collaboration Database

1. Run Setup from Oracle Media.
2. Click **Next** on the Welcome screen.
3. Accept the default file locations and click **Next**.
4. Accept the default Oracle8i 8.1.7.0.0 in the Available Products screen and click **Next**.
5. In the Installation Types screen, accept Typical (default) and click **Next**.
6. In the Database Identification screen, the Global Database Name of "Default" automatically fills in the SID field. Click **Next.**
7. In the Summary Screen click **Next.**
8. Install completes.
9. Close the Oracle Installer.
10. To create the Oracle Database for the Collaboration Server, click **Start > Programs > Oracle-OraHome81 > Database > Administration > Database Configuration Assistant**
11. In the Welcome screen, select "Create a Database" and click **Next**.
12. In the Select Database Type screen, select Customer and click **Next**.
13. In the Select Primary Application Type screen, select Multipurpose and click **Next**.
14. In the Concurrently Connected Users screen, accept the default and click **Next**.
15. In the Server Mode screen, select Shared Server Mode and click **Next**.
16. In the Options screen, accept the default and click **Next**.
17. In the Database Identifier screen, name the database "ccsdb". The SID automatically fill-in. Click on Change Character Set. Set both Character Set and National Character Set to "UTF8". Click **OK** and **Next.**
18. In the Password screen, enter and confirm the password (example: Cisco) and click **Next**.
19. In the Control File Information screen, accept defaults and click **Next**.
20. In the System Table Information screen, accept defaults and click **Next**.
21. In the Redo Log File Information screen, accept defaults and click **Next**.
22. In the Logging Information screen, accept defaults and click **Next**.
23. In the Server Information screen, accept defaults and click **Next**.
24. In the Advanced Server Information screen, accept defaults and click **Next**.
25. In the SGA Information screen, accept defaults and click **Next**.
26. In the Trace File Directory screen, accept defaults and click **Next**.
27. In the Create a Database Now screen, click **Finish**. Click **Yes** on the Alert window to proceed.
28. When you receive the message that Database Creation is completed, click **OK**.
29. To create the tablespace and user in the Oracle Database for the Collaboration Server, click **Start > Programs > Oracle-OraHome81 > Database Administration > SQLPlus Worksheet**.

30. In the Enterprise Manager Login Dialog Box, select Connect Directly to a Database:
    - Enter Username "internal"
    - Enter Password "cisco"
    - Enter Service <name of database>: example "ccsdb"
    - Connect As – select SYSDBA from pulldown Menu. Click **OK**.
31. In the SQLPlus Worksheet Application, delete the highlighted text. Copy the text below into this window.

Note: That the text is one line, and that a semicolon indicates a new line. The following names are used on the CollaborationServer.

- Tablespace name – ccstable
- Datafile name – ccsdata
- Username – ccsuser
- Password – Cisco

```
CREATE TABLESPACE <Collaboration DB tablespacename> DATAFILE '<Collaboration DB datafilename>' SIZE 30M;

CREATE USER <Collaboration DB username> IDENTIFIED BY <Collaboration DB password> DEFAULT TABLESPACE <Collaboration DB tablespacename>;

COMMIT;
```

32. Click on the **Execute** icon.

```
GRANT CONNECT, RESOURCE TO <Collaboration DB username>;

COMMIT;
```

33. Click on the **Execute** icon.
34. Click on **File Exit** to finish.

Special Notes if Installing SQL:

- Install SQL2000 using the typical option.
- Use Enterprise Manager to create a database.
- Use Enterprise Manager to create a user.
- Assign that user to the database created for CCS and assign these rights:
  - db_owner
  - db_accessadmin
  - db_securityadmin
  - db_ddladmin
  - db_backupoperator
  - db_datareader
  - db_datawriter

Step 18. Install Webview 3rd Party Software

Print and read the Read Me file on the "Webview 3rd Party Installer CD 6.0." This file describes the software and provides installation instructions. Various settings described in the Read Me file appear on certain setup screens.

1. Check to see if you have the Jaguar 3.5 software already installed on your machine. If Jaguar 3.5 software is installed on your machine, use the control panel's Add/Remove software program to remove that software.
2. Run Setup on the 3rd Party Installer CD 6.0.
3. Reboot the server when setup completes.
4. Use the following procedure to make sure that the cache will be updated at each new view of a real-time report.
   - In the Internet Explorer window, select Internet Options from the Tools menu.
   - If necessary, click the General tab to display the General Settings tab page.
   - On the General Settings tab page, in the Temporary Internet Files sections, click **Settings**.
   - In the Settings dialog box, enable the Every Visit to the Page option, then click **OK**.
   - Click **OK** in the Internet Options dialog box.

   Note: Webview Users are configured through the ICM Configuration Manager and passwords default to a given expiration timeframe set by the User's domain. If a Webview User's password expires, the User cannot reset the password by Webview access, but would have to request that the ICM System Administrator set a new password. Once the User is created, the ICM System Administrator has the option to set Webview User passwords to never expire through Active Directory Users and Computers.

Step 19. Install Infomaker on AW's

Infomaker is only installed on AW's (Real Time Distributors and Real Time Clients) for the purpose of creating Custom Reports.

1. Run Setup from Media for Sybase Powerbuilder (Common Installer).
2. In the Welcome to 8.0 Installer screen, click **Next**.
3. Accept License Agreement and click **Next**.
4. In the Customer Information screen, enter username and company name. Click **Next**.
5. In the Destination Folder screen, accept default and click **Next**.
6. In the Select components screen, select Infomaker and Online Books. Uncheck all other options.
   - You receive an Adaptive Server Anywhere warning. Click **OK** (ignore message).
   - Do not select Adaptive Server Anywhere. Click **No**.
   - You receive a Personal Server (Adaptive Server Anywhere) warning. Click **OK**.
7. Accept default destination locations for all components and select "typical" for all setup types.

   Complete all Wizards and Reboot the server.

Step 20. Install ICM Software on Loggers

You can load the ICM Software Modules on the individual servers. Refer to values as detailed in the System Design Specification as documented in the Planning phase of a deployment program.

When the ICM Logger and Admin Workstation software loads using ICM Setup, it creates specific domain level groups and accounts in the ICM domain it is loaded into.

Cisco provides specific hot fixes to major releases and service packs of the ICM software to address service-impacting issues. You can download these hot fixes from Cisco's web site (http://www.cisco.com/). You should apply them after the initial load of the software. The hot fix installation process only applies fixes required for the specific software module (CallRouter, Logger, type of PG, etc.).

Step 21. Create Logger Databases

After running the ICM Logger setup program and applying all hot fixes, you need to use the ICMDBA tool to finish the SQL Server configuration and build the actual ICM databases on the machine. You also use this tool on the Admin Workstation to create the Historical Database Server database (HDS).

For each Logger:

1. Click **Start > Run**, enter ICMDBA and click **OK**.
2. Click on the Server Name you want to change (Logger A or Logger B).
3. Select Create from the Database menu.
4. ICMDBA question prompts you to configure SQL Server. Click **Yes**.
5. Configure the Logger Screen. If the current value does not equal the recommended value, check the Config Box and verify that the new value equals the recommended value. Click **OK**.
6. Click **Yes** to continue. SQL Server stops and restarts.
7. On the Create Database screen, select Region.
8. Click **Add** and enter Data for Type.
9. Highlight the D drive. The size should be 70% of the available disk space if the Logger is for one customer instance only. If more than one instance resides on the Loggers, determine the DB size with the customer. Click **OK**.
10. Click Add and enter Log for the Type.
11. Highlight the D drive and set the size to 200MB (log device should not be larger than 500MB). Click **OK**.
12. Click Create. Click **Start to Create Database**. When the database is successfully completed, click **OK** and close the database window.
13. Close the ICMDBA.
14. Click **Start > Programs > Microsoft SQL Server > Enterprise Manager**.
15. Expand the Server Tree and Highlight the Databases Folder under the Server name
16. Double-click on ICM Database in the right Panel. In the <cus_sideA> Properties Window:
17. On the Data Files tab:
    - Check Autogrow and set the File Growth to 10%
    - Set the Maximum File Size to [use the following calculation]
      - {80% of free disk space}/{number of ICM database files on this disk}+{database file current size}
      - For example: {10GB * .80}/{1}+{25GB}=33GB
18. On the Transaction Log tab, Uncheck Autogrow and click **OK**.

Step 22. Install ICM Software on CallRouters

ICM Nodes Forms, which identify all values and non-default settings to be used in Setup, are created in the Planning phase of a deployment program and reside in the ICM System Design Specification.

Cisco provides specific hot fixes to major releases and service packs of the ICM software to address service-impacting issues. You can download hot fixes from Cisco's Web site (http://www.cisco.com/). Apply the hot fixes after the initial load of the software. The hot fix installation process only applies fixes required for the specific software module (CallRouter, Logger, type of PG, etc.).

Step 23. Start Logger and Router Services

The ICM is set up with an empty database. You need to add configuration information to complete the basic testing components. In order to add configuration data, the Central Controller and Admin

Workstation(s) must be running. The ICM software loads an "ICM Service Control" tool on the desktop of each server used to control the services loaded on that machine. Start the services in the following order:

- Logger A
- CallRouter A
- CallRouter B
- Logger B

Each service starts several process windows on the task bar of the local machine, each one an ICM program associated with the service. As each node starts up, it looks for the other server components and attempts to register with them. If you completed the ICM Setup and network testing successfully, no major errors should occur.

Verify that the ICM Processes have no errors:

CallRouters:

- Router: UP and synchronized with peer
- Ccagent: [will be in service but not be connected to any peripheral gateways]
- Rtsvr: [no connectivity to AW at this time]

Loggers:

- Logger: connected to its respective database and synchronized with peer. MDS is in service
- Replication: [no connectivity to AW HDS at this time]
- Campaign Manager: [you see errors, no BA Dialer setup at this time]

Step 24. Install ICM Software on Admin Workstation

Complete Setup on all Admin Workstations (see System Design Specification).

When the Admin Workstation software loads using ICM Setup, it creates specific domain level groups and accounts in the ICM domain it is loaded into.

Cisco provides specific hot fixes to major releases and service packs of the ICM software to address service-impacting issues. You can download hot fixes from Cisco's Web site (http://www.cisco.com/). Apply these hot fixes after the initial load of the software. The hot fix installation process only applies fixes required for the specific software module (CallRouter, Logger, type of PG, etc.).

Step 25. Expand AW Database

1. Click **Start > Run**, enter ICMDBA and click **OK**.
2. Expand Tree under the AW Hostname.
3. Highlight <cus_awdb>.
4. Select Expand from the Database menu.
5. Highlight C Drive.
6. Expand Data to 500MB. Click **OK**.
7. Click **Start** on Expand DB window. Click **OK**. Close when complete.
8. Select Expand from the Database menu.
9. Select Log (C drive is automatically highlighted).
10. Expand the Log to 200MB. Click **OK**.
11. Click **Start** on the Expand the database window. Click **OK**. Close when complete.
12. Close the ICMDBA.
13. Click **Start > Programs > Microsoft SQL Server > Enterprise Manager.**
14. Expand the Server Tree and Highlight the Databases folder under the Server name.
15. Double-click on the ICM Database in right panel, now in the <cus_awdb> Properties Window.

16. On the Data Files tab:
    - Check Autogrow and set the File Growth to 10%
    - Set the Maximum File Size to [use the following calculation]

      {80% of free disk space}/{number of ICM db files and aw logs on this disk}+{db file current size}

      example: {4GB * .80}/{2}+{.5GB}=2.1GB
17. On the Transaction Log tab
    - Check Autogrow and set the File Growth to 10%
    - Set Maximum File Size to [use the following calculation]

      {80% of free disk space}/{number of ICM db files and aw logs on this disk}+{db file current size}

      example: {4GB * .80}/{2}+{.2GB}=1.8GB

Step 26. Create HDS Databases

For each HDS:

1. Click **Start > Run**, enter ICMDBA and click **OK**.
2. Expand Servername/Instances/<Instance Name> menus.
3. Highlight "Distributor."
4. Click on the Database Menu and select **Create**.
5. A window indicates that SQL Server is not configured properly. Select **YES** to configure it now.
6. Verify that the "recommended settings" are set correctly for "Memory MB," "Max Async IO" and "Recovery Interval." Check the boxes next to each to fill in the new settings.
7. Stop SQL Server and the Distributor, as prompted, in order to continue.
8. In the Create Database screen, select the correct region for the system.
   - Click **Add** and enter Data for the Type.
   - Highlight the D drive. –Make the size 70% of the available disk space, or as determined with customer. Click **OK**.
   - Click **Add**, Enter **Log** for the type.
   - Highlight the D drive and set the size to 200MB (Don't make the log device larger than 500MB). Click **OK**.
   - Click Create and click Start to Create Database. When database is successfully completed, click **OK** and Close the database window.
9. Close the ICMDBA.
10. Click **Start > Programs > Microsoft SQL Server > Enterprise Manager**.
11. Expand the Server Tree and Highlight the Databases Folder under the Server name
12. Double-click on the ICM Database in the right Panel. In the <cus_hds> Properties Window.
13. On the Data Files tab:
    - Check Autogrow and Set File Growth to 10%
    - Set the Maximum File Size to [use the following calculation]

      {80% of free disk space}/{number of ICM db files and aw logs on this disk}+{db file current size}

      example: {10GB * .80}/{3}+{8GB}=10.6GB
14. On the Transaction Log tab, uncheck Autogrow.

Step 27. Start AW (Distributor) Services

Start the Distributor Service within Cisco Service Control.

Verify that the ICM Processes have no errors:

- CallRouters:
  - Router: UP and synchronized with peer
  - Ccagent: [is inservice, but not connected to any peripheral gateways]
  - Rtsvr: feed activated to AW
- Loggers:
  - Logger: connected to its respective database and synchronized with peer. MDS is in service
  - Replication: connected to AW
  - Campaign Manager: [you see errors. No Blended Agent Dialer setup at this time]
- Admin Workstation:
  - Updateaw: displays “waiting for new work”
  - Iseman: listen thread waiting for client connection
  - Replication: replication and recovery client connection initialized
  - Cms_jserver: unable to initialise until the configuration is done
  - Cmsnode: shutdown in progress..terminating

Step 28. Configure NIC’s, Peripheral Gateways and Peripherals

Before the ICM Services on the SS7 Gateways, NICs and Peripheral Gateways can be turned-up, you need to configure them in the ICM using the NIC and PG Explorer tools.

Refer to ICM System Design Specification, Connection Parameters Section, ICM Configuration Manager, PG Logical Controller ID’s and Peripheral Controller ID’s Table. This table indicates the values and settings, which must be established in ICM Configuration and input during ICM setup of each Peripheral Gateway node.

Note: In addition to establishing the PG logical controller ID’s and Peripheral ID’s, you must also configure the following in the ICM Configuration tool:

- On the Call Manager PG, enter the name for the Agent Desk Settings
- On the IPIVR PG, enter the name for the Network Type 2 VRU (also need to configure the Network VRU)
- On the Media Routing PG, enter the name for an additional Network Type 2 VRU (also configure the Network VRU)

In order to properly run ICM Setup for the NICs and PG’s, you need to plan the Logical and Peripheral ID numbers, as they are required data elements to complete the Setup program. The ICM automatically generates ID numbers from the Explorer tools, so you need to set them up in the Explorers in the exact order they were planned in the ICM System Design Specification.

If the ID numbers are not generated in the proper sequence, you can correct them in the Peripheral Gateway machines by re-running Setup locally. They must match the value in the ICM configuration database to the value in the PG’s registry, or the ICM CallRouter rejects the connection request.

Additionally, if the customer plans to use agent level reporting, you need to set this up after the Peripheral is created in the ICM configuration database. Use the Agent Distribution Tool on the Admin Workstation to point the specific Peripheral (ACD that generates the agent stats) to the Admin Workstation’s “Admin Site Name” for the AW that stores the real-time agent level reporting data. Also, you must set the Peripheral to enable “Agent Reporting” on the “Agent” tab in PG Explorer.

You must set up Agent Level Reporting for each peripheral and they can all point to a central AW/WebView server to allow for sharing of the stats. However, a peripheral can only point to one AW.

Step 29. Configure Multi-Media Nodes

Refer to ICM System Design Specification, Connection Parameters Section, ICM Configuration Manager, Media Routing Domains Table and Application Instance List Table.

1. Start ICM Configuration Manager.
2. Step-by-step/Multimedia/Media Routing Domains.
   - Add Single Session Chat Domain
   - Add Multi-Session Chat Domain
   - Add Blended Collaboration Domain
   - Add E-Mail Domain
   - Confirm or add Voice Domain
3. Step-by-step/Multimedia/Application Instance
   - Add CCS instance
   - Add CEM instance

Step 30. Create and Configure CONAPI Connections

Refer to the ICM System Design Specification, Connection Parameters Section, CMS Control.

1. Open the ICM Program Group
2. Start the CMS Control Tool
3. Click the Application Tab
4. On the Application Connection:
   - Add CCS connection – example: icmcusccs1
   - Add CEM connection – example: icmcuscem1

Step 31. Install ICM Software on Peripheral Gateways

Complete the setup on all Peripheral Gateways (see System Design Specification).

Cisco provides specific hot fixes to major releases and service packs of the ICM software to address service-impacting issues. You can download hot fixes from Cisco's Web site (http://www.cisco.com) and should apply them after the initial load of the software. The hot fix installation process only applies to fixes required for the specific software module (CallRouter, Logger, type of PG, etc.)

Step 32. Install ICM Software for CTI Server

Complete the setup from the ICM media (see System Design Specification).

Step 33. Install CTI OS Server

You must create an ODBC connection – see the *CTI OS System Manager Guide*

- The connection is between the CTIOS Server and any ICM database with agent information. It is recommended that you make the connection to the Logger database.
- Make a note of the ODBC filename that is created and which is to be used during the CTI OS Server Setup.

Complete the Setup on the CTIOS Server from the respective ICM Node Form, which identifies all values and non-default settings used in setup.

You can download hot fixes from Cisco's Web site (http://www.cisco.com/) and should apply them after the initial load of the software. The hot fix installation process applies fixes required for the specific software module (CallRouter, Logger, type of PG, etc.).

Step 34. Start PG, CTI and CTIOS Services

Once the ICM configuration database is set up with the appropriate peripherals, you can start the PG services from the Cisco Service Control application on the desktop of the PG. If the local peripheral (ACD/IVR/etc.) is not available to connect to the PG, disable it in the PG setup. Testing at this level only proves that the PG communications layer is set up properly and that it can communicate with the CallRouters and obtain configuration information.

For this example, the BA Dialer, Media Blender and E-Mail Manager PIM's are enabled on the MR PG. The Call Manager and IPIVR PIM's on the Generic PG remain disabled until the Call Manager and IPIVR peripherals are available during the implementation phase of the project.

Verify that the ICM Processes have no errors:

- CallRouters:
  - Router: UP and synchronized with peer
  - Ccagent: connected to all configured peripheral gateways
  - Rtsvr: feed activated to AW
- Loggers:
  - Logger: connected to its respective database and synchronized with peer. MDS is in service
  - Replication: connected to AW
  - Campaign Manager: [you see errors, no BA Dialer is setup at this time]
- Admin Workstation:
  - Updateaw: displays "waiting for new work"
  - Iseman: listen thread waiting for client connection
  - Replication: replication and recovery client connection initialized
  - Cms_jserver: **cmsnode.exe** process is active. CEM and CCS connection down
  - Cmsnode: initialization complete
- Peripheral Gateways:
  - Generic (IPCC & VRU) PG
    - Mdsproc: inservice
    - Pgagent: inservice and active to one side of central controller
    - [peripheral] PIMs: disabled on node form. PIM windows do not exist
  - MR PG
    - Mdsproc: inservice
    - Pgagent: inservice and active to one side of central controller
    - [peripheral] PIMs: enabled in setup and therefore, is cycling between activating and idle
- CTI Server:
  - Cg[#]ctisvr: active with configured port number
- CTIOS Server:
  - Ctios Server: active with configured port number – driver online
  - Ctidriver: active

Step 35. Install and Start Blended Agent Dialer

1. Configure the Blended Agent Dialer in the ICM Configuration Manager. Open **Configuration Manager > Blended Agent > Blended Agent Dialer**.
2. Retrieve and click **ADD**.
   - Enter the Dialer Name – example: ba1_dialer.
   - Check the "enable" box.
   - Enter Computer Name where the Blended Agent Dialer is installed – example: icmcusba1.
   - From ICM Peripheral Name menu, select the name of the Blended Agent PIM on the MR PG – example: BA1.
   - Enter the data in the local area code field even if this is reconfigured later for the production environment. Click save and close.
3. Validate that the Blended Agent option is enabled on the Logger.

4. Create the Blended Agent Database on Logger A. On Logger A, run ICMDBA.
   - Highlight Logger A, right-click and select "create" from the database menu.
   - Create the Database Screen.
     - The Database type is BA_SideA.
     - Add Device (see Cisco ICM Software Blended Agent Setup and Configuration Guide for database estimation information).
       - For Data, highlight the D drive, enter 500MB and click **OK**.
       - For Log, highlight the D drive, enter 100MB and click **OK**.
     - Click **Create** and click **Start**. When you finish, click **OK** and **Close**. Close ICMDBA.
5. Complete the Setup on the Blended Agent Dialer Server from ICM media for the respective ICM Node Form, which identifies all values and non-default settings to be used in Setup.
6. After reboot, start the Blended Agent Dialer process.

Verify that the ICM Processes have no errors:

- For CallRouters:
  - Router: UP and synchronized with peer
  - Ccagent: connected to all configured peripheral gateways
  - Rtsvr: feed activated to AW
- For Loggers:
  - Logger: connected to its respective database and synchronized with peer – MDS is inservice
  - Replication: connected to AW
  - CampaignManager: process up on logger and connected to BA Dialer
- For the Admin Workstation:
  - Updateaw: displays "waiting for new work"
  - Iseman: listen thread waiting for client connection
  - Replication: replication and recovery client connection initialized
  - Cms_jserver: **cmsnode.exe** process is active
  - Cmsnode: initialization complete
- For Peripheral Gateways:
  - Generic (IPCC & VRU) PG
    - Mdsproc: inservice
    - Pgagent: inservice and active to one side of central controller
    - [peripheral] PIMs: disabled on node form – PIM windows do not exist
  - MR PG
    - Mdsproc: inservice
    - Pgagent: inservice and active to one side of central controller
    - [peripheral] PIMs: enabled in setup – Blended Agent PIM are now active – E-Mail Manager and Media Blender PIM's still cycling
- For CTI Server:
  - Cg[#]ctisvr: active with configured port number
- For CTIOS Server:
  - Ctios Server: active with configured port number – driver online
  - Ctidriver: active
- For BA Dialer:
  - Blended Agent Dialer: EMT connection established and config received

Step 36. Install and Start E-Mail Manager Servers

Install E-Mail Manager Core Server

1. Run Setup from Cisco E-Mail Manager Install Media.
2. Click Welcome and select **Next**.
3. Select the Component Screen and select CEM.

4. Accept defaults on all file location screens.
5. Click Next. Install of 3rd Party Component(s) now completes
6. Information dialog box. The Installer now calls the CEM Services Installer. Click **OK**.
7. For Welcome, click **Next**.
8. Accept the defaults on the file location.
9. Select the Program Folder. Accept defaults and click **Next**.
10. Ready to Copy files screen, click **Next**.
11. Files now copy.
12. On the Information Dialog Box, Setup now launches the Configuration Utility. Click **OK**.
13. Create a New Instance Dialog Box. Refer to the ICM System Design document, Connection Parameters Section and Application Instance Table to enter the following:
    - E-Mail Manager Instance Name
14. Enter the Login Name "root" (from *Cisco E-Mail Manager Installation and Configuration Guide*)
15. Enter the Password "pass" (from *Cisco E-Mail Manager Installation and Configuration Guide*)
16. Click the Dialog Box asking to install the license file and click **Yes**.
    - Go to the URL printed on the front of the CMB Install Media.
    - Enter the Product Code from the CD and an e-mail address and you are e-mailed a FlexLM License File.
    - Copy the License File to a floppy disk.
    - Insert the floppy disk into E-Mail Manager Server.
17. In the Locate and Select CEM License File Dialog Box, navigate to the A drive.
18. Highlight the License File and click on Load License File.
19. For the Configuration Utility, see the *Cisco E-Mail Manager Installation and Configuration Guide*.
    - On the General tab, accept defaults.
    - On the Primary Database tab:
      - Select a Database: SQL 2000
      - Database Information:
        - For the Database Name, enter "cemdb"
        - For the Login name, enter "cemuser"
        - For the Login password, enter "cisco"
        - Confirm the password by entering "cisco"
        - For the Database Hostname, enter the name of the E-Mail Manager Database: ICMCUSCEMDBL
        - For the database port, enter "1433"
      - Click **Run Now**.
      - The Database Administration Login Dialog Box appears.
        - Enter the database Admin Login Name (sa)
        - Leave the database Admin password blank
        - Login
      - The Database Files Dialog Box appears
        - Enter the data and log sizes
          - Minimum database file size is 500MB
          - Minimum log file size is 300MB

Note: Sizing is based on information gathered during the Application Discovery Phase, based on expected number of e-mails received on a daily basis, size of the average e-mail, average size of attachments (if any), and the length of time e-mails should be preserved on the database.

- Click **OK** to create Schema.
- The Database Table Creation Dialog Box appears. –Click **OK**.

- On the Logging tab, accept defaults.
- On the Advanced tab, accept defaults.
- For the HTTPD tab, change the HTTPD port to 80.
- On the LAMBDA Database tab, make note of the database name, as you use it when installing the Agent UI Server. For example: cemdbp.
  - Click RunNow.
  - Enter the login and password information (login name: sa and password: leave blank)
  - The Database Files Dialog Box appears.
    - Enter data and log sizes
    - Set the Database file size (minimum 500MB)
    - Set the Log file size (minimum 300MB)

  Note: Sizing is based on information gathered during Application Discovery Phase, based on expected number of e-mails received on a daily basis, size of the average e-mail, average size of attachments (if any), and the length of time e-mails should be preserved on the database.
    - For the Successful Creation Database Creation Dialog Box, click **OK**.
- On the LAMBDA tab, accept defaults unless information gathered during the discovery indicates that you should enter other values here.
- On the CIR database tab, make note of the database and username. You use them when installing the Agent UI Server. For example: database is cemdbc and username is CEMUSERC
  - Choose to run the script now.
  - Enter the Login and Password: (login name: sa and password: leave blank)
  - The Database Files Dialog Box appears.
    - Enter the Database file size (minimum 500MB)
    - Enter the Log file size (minimum 300MB)

  Note: Sizing is based on information gathered during the Application Discovery Phase, based on expected number of e-mails received on a daily basis, size of the average e-mail, average size of attachments (if any), and the length of time e-mails should be preserved on the database.
  - For the Successful Creation Database Creation Dialog Box, click **OK**.
  - For the Successful Grant Access to CIR Dialog Box, click **OK**.
  - For the Successful Database Table Dialog Box, click **OK**.
- On the CIR tab, enter the Webview Server Name. For example: icmcusag2. Accept all other defaults.
- On the ICM tab, refer to the ICM System Design document, Connection Parameters Section, ICM Configuration Manager, Media Routing Domains Table and Application Instance List Table. You also need to refer to (in this same Section) CMS Control, CONAPI Connections-ICM/E-Mail Manager Table.

  [example]
    - ICM Enterprise Name: CEM
    - ICM Application Key: cisco
    - ICM Description: mmcallcenter

- Media Routing Domain ID: 5003
- ICM Administration connection name: ConnName1 (use this default)
- Service Name on Email Manager Server: CEM
- Registry Port on Email Manager Server: 1099
- ICM Distributor AW Service Name: ICM
- ICM Distributor AW Registry Port: 1099
- ICM Distributor AW Hostname: icmcusaw1

- Click **Finish** and click **OK** on the confirmation dialog box.
- When setup completes, click **Finish**.

Install CEM Agent UI/API/Webview Server

1. Run Setup from Cisco E-Mail Manager Install Media.
2. On the Welcome screen, click **Next**.
3. Select the Component Screen and select UI Server and Webview Standalone.
4. Accept the defaults on all file location screens.
5. For Information, click **Next**. Install of 3rd Party Component(s) now completes.
6. On the Information dialog box, the installer now calls the CEM UI Server Installer. Click **OK**.
7. On the question dialog box, click **Yes**.
8. On the UI Install Shield Wizard, click **Next**.
9. Select the Instance that was created on Core Server. Example: CEM click **Next**.
10. Accept the default for the directory location.
11. For Tserver Properties, click **Next**.
12. For the UI Server Destination Location, accept the default and click **Next**.
13. The application installs.
14. Click **Yes** for the dialog box that appears.
15. Click **Finish** for the Install Shield Wizard Complete screen.
16. For the information dialog box, the installer calls the Webview Installer. Click **OK**.
17. Click Next for the Install Shield Wizard for Webview.
18. Select English for the language and click **Next**.
19. For the CIR Connection Information:
    - Select the Database Type and Version. Example: MS SQL Server 2000
    - Enter the Database Server Hostname. Example: icmcuscemdb1
    - Enter the Database Name. Example: cemdbc
    - Enter the Port. Example: 1433
    - Enter the Username. Example: cemuserc
    - Enter the Password. Example: Cisco
    - Click **Next**.
20. Click **Next** for the Application and Instance to Report Against.
21. Select the Installation Drive. Make a note of the target directory. For example: c:\CEM, click **Next**.
22. For the UI Server Authentication Information:
    - Enter the UI Server Hostname. Example: icmcusag1
    - Enter HTTP for the Select Authentication Protocol
    - Enter 80 for the Port

- Click **Next**.

The Setup Status screen displays and the Application installs. Perform the following steps to confirm and finalize the installation:

1. Confirm that reporting was added to the Dialog Box. Choose whether or not you would like to add another application instance. Example: no
2. The Install Shield Wizard completes. Click **Yes** to restart the machine. Click **Finish**. The system reboots.
3. Click **Start > Programs > New Atlanta > ServletExec 4.1 ISAPI > ServletExec Admin**.
   - The Internet Explorer browser opens to the ServletExec Admin screen.
   - In the left frame, click on **Settings** under the Virtual Machine.
   - In the right frame, set the minimum heap size. Example: with 250 agents set to 81902
   - In the right frame set maximum heap size. Example: with 250 agents set 81902.
   - In the right frame, click **Submit**.
   - Close the browser.

Install CEM Agent UI/API #2 Server

1. Run setup from the Cisco E-Mail Manager Install Media
2. On the welcome screen, click **Next**.
3. Select the UI Server from the Select Component Screen.
4. Accept the defaults on all file location screens.
5. For Information, click **Next**. The install of 3rd Party Component(s) now completes.
6. For the Information dialog box, the installer now calls the CEM UI Server Installer. Click **OK**.
7. Click **Yes** for the question dialog box.
8. Click **Next** for the UI Install Shield Wizard.
9. Select the instance that was created on Core Server. For example: CEM. Click **Next**.
10. Accept the default for directory location.
11. For the Tserver Properties, click **Next**.
12. For the UI Server Destination Location, accept the default and click **Next**.
13. The application installs.
14. For the question dialog box to restart IIS services, click **Yes**.
15. The Install Shield Wizard completes. Click Finish and reboot the machine.
16. Click **Start > Programs > New Atlanta > ServletExec 4.1 ISAPI > ServletExec Admin**
    - Internet Explorer browser opens to the ServletExec Admin page.
    - In the left frame, click on **Settings** under Virtual Machine.
    - In the right frame, set the minimum heap size. Example: with 250 agents set to 81902.
    - In the right frame, set the maximum heap size. Example: with 250 agents set 81902.
    - In the right frame, click **Submit**.
    - Close the Browser.

Start E-Mail Manager Servers

1. Use Windows Services. Start the CEM database first.
2. For the CEM Core Server, two new Services appear: Cisco E-Mail Manager Core Server and Cisco E-Mail Manager CEM.
   - Highlight the Core Server, and rightclick **Properties**.

- On the Login Tab, confirm that Allow Service to Interact with Desktop is checked.
- On the General Tab, click **Start** and click **OK**.

– Highlight CEM and right-click **Properties**.

- On the Login Tab, confirm that Allow Service to Interact with Desktop is checked.
- On the General Tab, click **Start** and then click **OK**.

3. Start the World Wide Web Publishing Services on UI Servers (this starts Webview and UI Servers).

Verify that the ICM Processes have no errors:

- CallRouters:
  - Router: working and synchronized with peer.
  - Ccagent: connected to all configured peripheral gateways.
  - Rtsvr: feed activated to AW.
- Loggers:
  - Logger: connected to its respective database and synchronized with peer and that MDS is in service.
  - Replication: connected to AW.
  - CampaignManager: the process is working on the logger and is connected to the BA Dialer
- Admin Workstation:
  - Updateaw: displays “waiting for new work”.
  - Iseman: listen thread waiting for client connection.
  - Replication: replication and recovery client connection initialized.
  - Cms_jserver: **cmsnode.exe** process is active and the event helper message shows CEM “up”; CCS “down”.
  - Cmsnode: initialization complete .
- Peripheral Gateways:
  - Generic (IPCC & VRU) PG
    - Mdsproc: in service.
    - Pgagent: in service and active to one side of central controller.
    - [peripheral] PIMs: disabled on node form – PIM windows do not exist.
  - MR PG
    - Mdsproc: in service.
    - Pgagent: in service and active to one side of central controller.
    - [peripheral] PIMs: enabled in setup. BA PIM is now ACTIVE. E-Mail Manager PIM is ACTIVE, but Media Blender PIM is still cycling.
- CTI Server:
  - Cg[#]ctisvr: active with a configured port number.
- CTIOS Server:
  - Ctios Server: active with a configured port number and that the driver is online.
  - Ctidriver: active.
- BA Dialer:
  - BA Dialer: EMT connection established and the config is received.
- E-Mail Manager Core:
  - Rules engine process: inbasket authenticated.

Step 37. Install Collaboration Server

1. Run setup from the CCS install media.
2. On the Welcome Screen, click **Next**.
3. On the License Screen, click **Next**.
4. Enter the user information and click **Next**.
5. Accept the default for the Destination Location and click **Next**.
6. Accept the default for the Custom Content Directory and click **Next**.

7. Enter the Customer Name and click **Next**.
8. Click **Next** for the ServletExec Install Shield Wizard.
9. Click **Next** on the License Screen.
10. Click **Next** on the Information Screen.
11. Accept the defaults for the Destination Location and click **Next**.
12. Click **OK** for the Warning dialog box.
13. Click **Finish** for the Install Shield Complete screen.
14. Cisco Collaboration Server 6.0 Java Installer indicates that the install completes. Close the window.
15. Click **Finish**.
16. Install the Oracle JDBC Driver. Obtain the latest Oracle JDBC Driver from Oracle Install Media or Oracle Web site: http://www.oracle.com.
17. Copy the Oracle JDBC Driver to **C:\Cisco_CS\servlet directory**.

Note: Leave the JDBC Driver zipped

18. Install the FlexLM License. Go to the URL printed on the front of the CCS installation media.
19. Enter the Product Code from the CD and your e-mail address. You are e-mailed a FlexLM License File.
20. Copy the License File to a floppy disk.
21. Insert the floppy disk into the Cisco Collaboration Server.
22. Copy the file to **C:\Cisco_CS\license directory**.

Note: Do not reboot the server before the license is in this directory.

23. Reboot the server. After the server reboots, launch the browser.
24. Type in the following URL: **http://icmcusccs1/admin and Return**.
25. For the Cisco Collaboration Server Admin Login Window, the login name is admin and the password is Password (these are defaults).
    - Create Database Connections
      - Click **Next** for the Database Setup Wizard.
      - Select the Database Type (example: Oracle 8/8i) and click **Next**.
      - Click **Next** for the confirmation on the JDBC Driver.
      - For the Database Connection Data:
        - Enter the Host: <collab db>. For example: icmcusdb1.
        - Enter or accept the Port. 1521 is the default.
        - Enter the SID: <from Oracle install on Collab DB>. For example: CCSDB.
        - Enter the Database Login Name: <from Oracle install on Collab DB>. For example: ccsuser.
        - Enter the Password: <from Oracle install on Collab DB>. For example: cisco.
        - Verify the Password: <from Oracle install on Collab DB>. For example: cisco.
        - Click **Next**. The Next Screen verifies the Connection Settings. Click **Apply**.
      - On next screen, click **Finish** to setup the database and create the schema.
      - You may get a security warning dialog box asking if you want to install the database utilities applet. Check “always trust content from Cisco Systems” and click **Yes**.
      - The schema is then created.
    - In the left frame, select **Server Setup\Show**
      - Click **OK** on the Dialog Box to change the Admin Password.
      - In the right frame (top), click **View\Change**.

        - Enter a new admin password (for example: ccsadmin)
        - Enter the Collaboration Server Application Instance Name (refer to the ICM System Design Doc, Connection Parameters section, ICM Configuration Manager\Application Instance List table). For example: CCS.
        - Click **SUBMIT**.
    - In the left frame, select **Server Setup > Integrate with ICM**.
        - The Wizard appears in the right frame. Click Integrate with ICM Web button.
        - Click **OK** on the dialog box.
        - Click on an underlined Application Instance link. On the new/second browser screen, enter the Application Instance Name. Enter the Application Key (refer to ICM System Design Doc, Connection Parameters section, ICM Configuration Manager\Application Instance List table). For example: cisco.
        - Click **SUBMIT**.
        - Click **OK** on the dialog box.
        - Close the second browser.
        - Click on the underlined ICM Administration Connection link. On the new/second browser screen, enter the CONAPI connection information (refer to ICM System Design Doc, Connection Parameters section, CMS Control\CONAPI Connections-ICM/Collaboration table). Examples:
            - ICM Admin connection name: ICMConn1
            - Registry port on Collab Server: 1099
            - Connection port on Collab Server: 1100
            - Service name on Collab Server: CCS
            - ICM Distributor AW host name: icmcusaw1
            - Registry port on ICM Distributor AW: 1099
            - Service Name on ICM Distributor AW: ICM
        - Click **SUBMIT**.
26. Close the second browser.
27. Click **APPLY**.
28. Close the Browser and reboot the Collaboration Server. After the server reboots, launch the browser.
29. Before proceeding with the next steps, validate that the Distributor associated with ICM Connection is started and that cms_jserver and cmsnode are running.
30. Type in the following URL: **HTTP://icmcusccs1/admin and Return**.
31. Cisco Collaboration Server Admin Login Window. Enter the login name and password.
    - In the left frame, select **Server Setup\Integrate with ICM**.
        - Click on the Media Routing Domains link. On the new/second browser screen, use the menus to select the media routing domains that correspond to the media class listed to the left.
        - Click **SUBMIT**.
        - Click **OK** on a dialog box.
        - Close the second browser.
        - Click on the Media Blender Connection link. On the new/second browser screen, select and enter the Media Blender connection data:

            [example]

            - Media Blender Connection Name: <arbitrary> example: cmb1.
            - Registry Port on Collaboration Server: 1099.
            - Connection Port on Collaboration Server: 1100.

- Collab Server Password: cisco (must then verify).
- Media Blender hostname: icmcuscmb1.
- Registry Port on Media Blender: 1099.
- Media Blender Password: <arbitrary> cisco (must verify).
- Make sure that Disable auto connect to Media Blender is checked.
- Close the second browser.

- Click on the ICM Peripherals link. On the new/second browser screen, check the peripherals that are associated with agents and select the appropriate media blender connection from the menu:
  - Click **ENABLE**.
  - Click **OK** on dialog box.
  - Close the second browser.
- Click **NEXT** to continue with the ICM Integration.
- Check the Collaboration Server Descriptions that apply (in this example check both). Click **FINISH**.
- In the left frame, select Server Setup > Queues > Create.
  - Create a Queue applicable to your installation. In the example of IPCC only "ICM QUEUE" is required.
  - Click **NEXT**.
  - Insert the Queue Name. For example: ICM.
  - Select the appropriate Media Blender connection from the menu. For example: cmb1.
  - Select the backup Media Blender connection from the menu. For example: <leave blank>.

32. Click **FINISH** and close the browser and reboot the server.
33. From the Collaboration Server, copy the following two files onto a floppy disk:
    - **Cmbl.properties**. Located in: **C:\Cisco_CS\servlet\properties\cmb\cmb1**.
    - **Collaboration.properties**. Located in: **C:\Cisco_CS\servlet\properties\cmb\Blender**.

Step 38. Install and Start Media Blender Server

1. Run setup from CMB Install Media.
2. Click **Next** at the welcome street.
3. Enter your name and company for the User Information.
4. Accept the default for the Choose Destination Location and click **Next**. Allow the installation to complete.
5. Run the Servlet Exec 4.1.1 ISAPI Setup and click **Next**.
6. Click **Yes** for the License Agreement.
7. Click **Next** for the Information screen.
8. Choose a destination location, accept defaults and click **Next**.
9. As files are being installed you receive an IIS warning. Click **OK**.
10. When the Install Shield wizard complete, click **Finish**.
11. As installation continues, you see the World Wide Web Process started.
12. You see a Cisco Java Installer screen. When it says "Installation Completed", close the screen.

Several command prompt process windows appear and the installation completes.

Note: DO NOT REBOOT the machine now, you must install the license first.

To install the license:

1. Install FlexLM License
   - Go to the URL printed on the front of the CMB Install Media.
   - Enter the Product Code from the CD and an e-mail address and you are e-mailed a FlexLM License File.
   - Copy the File into **C:\CiscoMB\license**.
   - Reboot the server
2. Rename the following file:
   - From **C:\CiscoMB\servlet\Properties\Blender\collaboration.properties**
   - To **C:\CiscoMB\servlet\Properties\Blender\collaboration.properties.old**
3. Take the files that were copied in the final step of Collaboration Server Installation and copy as follows:
   - **cmb1.properties** goes into the **C:\CiscoMB\servlet\Properties** directory
   - **collaboration.properties** goes into the **C:\CiscoMB\servlet\Properties\Blender** directory
4. Open the following file with a text editor: **C:\CiscoMB\servlet\Properties\Blender\ACD.ciscocti.properties** (these settings vary according to peripheral types).

   [example]
   - Uncomment (remove #) “ctistrategy=AgentReserved”
   - Comment (insert # in front of line) “phantompool=phamtoms.properties”
   - Comment (insert # in front of line) “physicallocationfile=phantomagents.properties”
   - Comment (insert # in front of line) “passwordfile=phantompasswords.properties”
   - Comment (insert # in front of line) “agentsfile=agentmapping.properties”
   - Comment (insert # in front of line) “skilltable=skills.properties”
   - Uncomment (remove #) “peripheral.type=IPCC”
   - Enter peripheral id of the call manager PG – peripheral.id=5000
   - Enter peripheral.hostname= <hostname of CTI Server> icmcuspg1a
   - Enter peripheral.hostport=42027
   - Enter peripheral.hostname2=icmcuspg1b (be sure to uncomment)
   - Enter peipheral.hostport2=43027 (be sure to uncomment)
   - Save and close the file.
5. Open the following file with a text editor: **C:\CiscoMB\servlet\Properties\Blender\blender.properties** (these settings vary according to peripheral types).

   [example]
   - Uncomment “**service1=service.fwgw.properties**”
6. Open the following file with a text editor: **C:\CiscoMB\servlet\Properties\firewallgatewayFG.properties** (these setting vary according to whether or not you have duplex PG’s).

   [example]
   - Replace <connectionname> (appears throughout) with the name of the connection to Media Blender that you created on the Collaboration Server during the Integrate with ICM steps. For example: cmb1.

- Enter the Primary and Secondary CTI Server hostnames, which are indicated by: <primaryhostname> and <backuphostname>
- Enter the Primary and Secondary CTI Server ports, where indicated by <primaryserverport> and <backupserverport>.
- Save and Close the file.

To start Media Blender:

1. Open the Browser, enter the URL **http:\\<media blender hostname>**.
2. For the User Name, enter Administrator (with capital A).
3. For the Password, enter <Win2K Admin login password>.
4. Click on the Server Administration link.
5. In the left frame, click on Media Blender > Server > Start > Shutdown.
6. In the right frame, click **Start**.
7. In the left frame, click **Media Blender > Service > Firewall Gateway > Start > Stop**.
8. In the right frame, click **Start**.

Verify that the ICM Processes have no errors:

- CallRouters:
  - Router: UP and synchronized with peer
  - Ccagent: connected to all configured peripheral gateways
  - Rtsvr: feed activated to AW
- Loggers:
  - Logger: connected to its respective database and synchronized with peer – MDS is inservice
  - Replication: connected to AW
  - CampaignManager: process up on logger and connected to BA Dialer
- Admin Workstation:
  - Updateaw: displays “waiting for new work”
  - Iseman: listen thread waiting for client connection
  - Replication: replication and recovery client connection initialized
  - Cms_jserver: cmsnode.exe process is active – event helper message shows CCS and CEM “up”
  - Cmsnode: initialization complete
- Peripheral Gateways:
  - Generic (IPCC & VRU) PG
    - Mdsproc: inservice
    - Pgagent: inservice and active to one side of central controller
    - [peripheral] PIMs: disabled on node form – PIM windows do not exist
  - MR PG
    - Mdsproc: inservice
    - Pgagent: inservice and active to one side of central controller
    - [peripheral] PIMs: enabled in setup – BA PIM will now be ACTIVE – E-Mail Manager PIM will be ACTIVE and Media Blender PIM will be ACTIVE
- CTI Server:
  - Cg[#]ctisvr: active with configured port number
- CTIOS Server:
  - Ctios Server: active with configured port number – driver online
  - Ctidriver: active
- BA Dialer:
  - BA Dialer: EMT connection established and config received
- Email Manager Core:
  - Rules engine process: inbasket authenticated!
- Collaboration Server:

- Admin UI: under Collaboration Server\Server Setup\Connections\Monitor – all services will have an UP status
- Media Blender:
  - Admin UI: under Media Blender\Server\Startup Shutdown – media blender has been running for <time>
  - Admin UI: under Media Blender\Services\Firewall Gateway\Monitor – all gateway stubs will have a RUN status

Step 39. Complete Staging Tests

With the full ICM system in the staging environment, you can test fault tolerance prior to shipping the system to the production environment. Refer to the section in the document on ICM Process Testing in the Staging Environment.

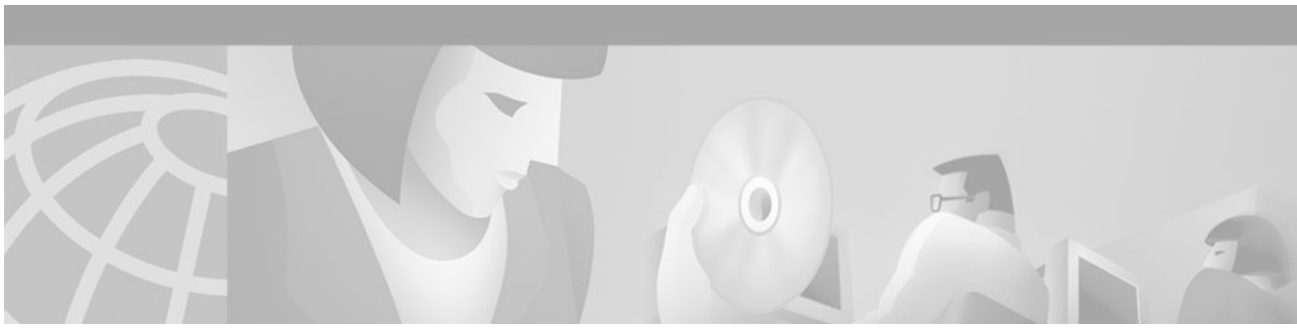
Step 40. Complete Settings for Production Environment

Validate the following settings from the system diagram for the Production Environment and make the required changes prior to shipping systems. If you used “dummy” IP addresses during the staging process, you need to load the actual Host Names/IP Addresses for the system onto the DNS Server (Logger/DNS Server) and the actual/production IP addresses set:

- IPAddresses (visible and private, high and low)
- Default Gateways
- Masks
- DNS preferred and alternate servers on visible cards
- Static Routes
- Active Directory WAN Sites and Subnets
- DNS Forward and Reverse Lookup Zone Records
- Label each Network Card and Port - Label the machine on the front and back with the host name
- Create Emergency Repair Disk
- Clear Event Logs
- Clear any Dr. Watson Application Errors
- Remove any diskettes, CD’s or media from drives
- Make sure that all ICM Services are set to Manual Start – Services are not set to AUTOSTART until after the implementation testing in the production environment.

Step 41. Complete Staging Issues Record

Assure that the System Design Specification has been filled out as and accurate record of the Staging event. Test Detail and note the test cases you run as pass/fail/exceptions. Any outstanding action items from the Staging event should be documented and shared with the team and project manager(s) associated with this project



Enterprise ICM Child Domain Model

Sample Diagrams

Figure 3 Enterprise ICM Child Domain Model-Central Controller Sites

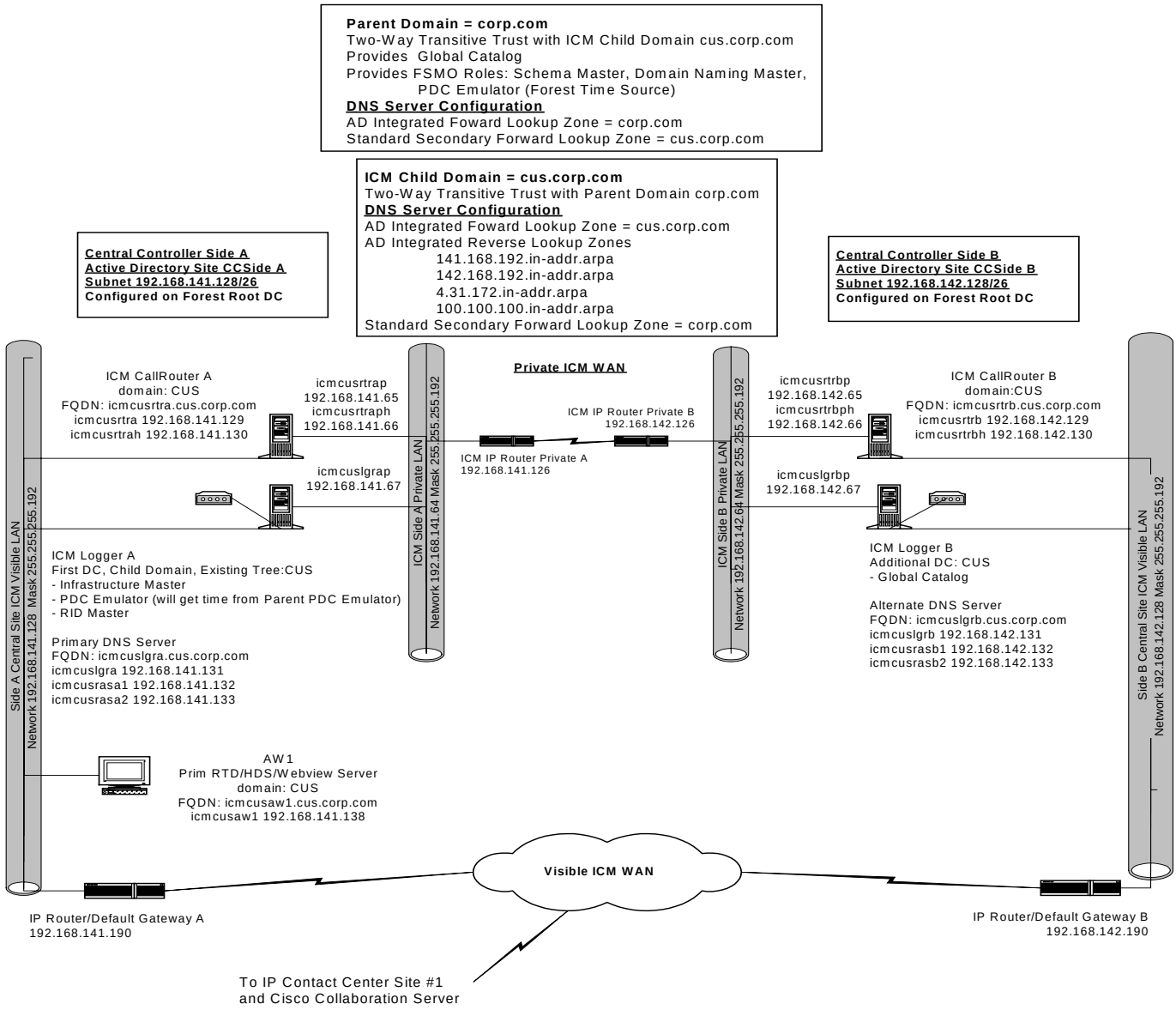
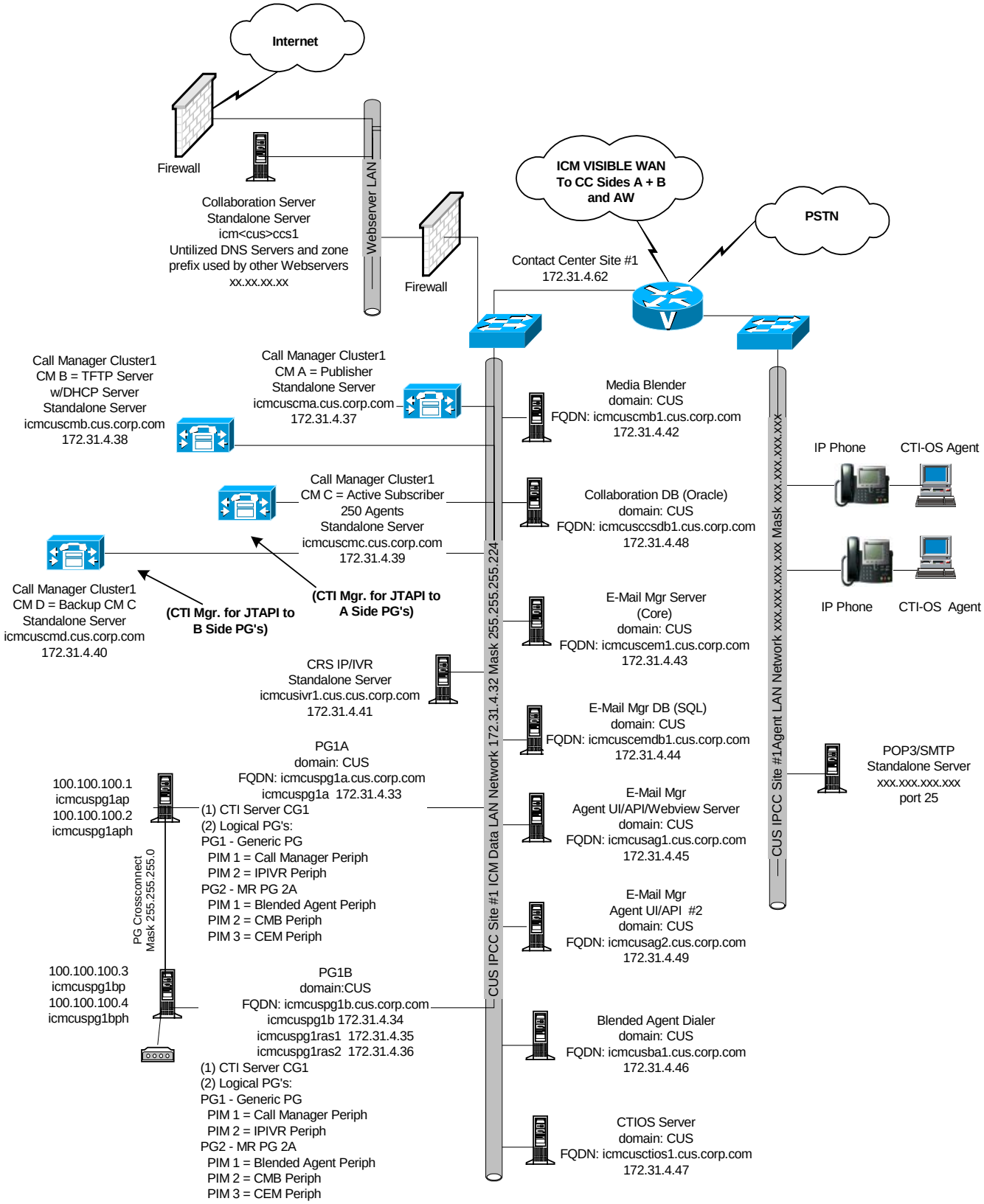


Figure 4 Enterprise ICM Child Domain Model-Call Center Site



Staging Tasks

In this model of deployment, the Enterprise or Parent Forest/Root Domain must already be in place and the customer must supply the Enterprise Forest administrator rights in order to create the ICM Child Domain.

Staging of an Enterprise ICM Child Domain must be done on site, with full network access to the Parent Domain. A Cisco Certified Integration Partner can source and pre-stage the ICM Servers as "standalone" prior to shipping them to the customer's production locations. The ICM Servers must be Domain Members and have network connectivity to the Child Domain Active Directory Domain Controllers. The Child Domain Active Directory Domain Controllers, in turn, must have network connectivity to the Parent Domain Active Directory Domain Controllers.

Cisco also recommends that the ICM Child Domain provide DNS services locally within that domain.

The Visible Network Card, on the First Domain Controller created in the Child Domain, must temporarily have the DNS Settings point to an Enterprise Level (Parent) DNS Server until a DNS Server is available at the Child Domain level.

The Staging Tasks for a Child Domain are similar to the **Staging Tasks for Enterprise ICM Dedicated Forest/Domain Model** with the following additions and substitutions.

First, follow Steps 1-3 featured on pages 12-13 of this document.

Note: The following caveat applies to step 2. The Visible Network Card, on the First Domain Controller created in the Child Domain, must temporarily have the DNS Settings point to an Enterprise Level (Parent) DNS Server until a DNS Server is available at the Child Domain level.

Now, continue by following the instructions below.

1. Click **Start > Run** and enter **DCPROMO**. The Active Directory Installation wizard opens.
2. Under "Domain Controller Type," select "Domain Controller for a New Domain." The "Create Tree or Child Domain" screen appears.
3. Select "Create a New Child Domain in an Existing Domain Tree."
4. On the Network Credentials Screen, enter your username, password and fully qualified domain name for the Parent (Forest Root) domain.
5. For the Child Domain Installation.
   - Enter the full DNS name of the Parent Domain.
   - Under Child Domain, enter the NETBIOS name for the Child and the full DNS name enters at the bottom of the screen.
6. Accept the Database and Log Locations defaults.
7. Accept the Shared System Volume default. You configure this server as a DNS Server in a later step.
8. On the "Permissions" screen, select "Permissions compatible with pre-Windows 2000 servers."
9. For "Directory Services Restore Mode Administrator Password," enter the Administrator password, as detailed in the 3rd Party Host Form.
10. Restart when the installation completes.
11. Delete the Child Domain subfolder on the Parent Level DNS Servers.

When the ICM Child Domain is created, Windows automatically creates a "subfolder" in the Enterprise Root DNS tree as a container for the servers in the new Child Domain. Typically, these folders are only used for a small number of servers, for ease of management and administration. Delete this subfolder and create an individual DNS Zone by following the instructions below.

Step 5: Install DNS Server on First Domain Controller for Child Domain

Substitute Step 5 detailed below for Step 5 from the Enterprise ICM Dedicated Forest/Domain Model.

1. Click **Start > Programs > Admin Tools > DNS > Configure Your Server**.
2. From the left column, select the "Networking" menu and select DNS.
   - Select Setup DNS. You are prompted to insert the Windows 2000 CD.
   - DNS loads after you insert the Windows 2000CD.
3. Click **Start > Programs > Admin Tools > DNS**.
4. Expand the Hostname Tree.
5. Highlight Forward Lookup Zones, right-click and select **New Zone**.
6. Within the New Zone wizard, select "Active Directory Integrated Zone" and enter the full DNS name of the Child Domain DNS zone.
7. Highlight the machine name, right-click and select **Properties.**
8. On the Interfaces Tab, select "Listen on Only the following IP addresses" and remove all but the visible machine address.
9. Complete the configuration of the AD Integrated Forward and Reverse Lookup Zones.
   - Highlight the Child Domain zone name under Forward Lookup Zones, right-click and select **Properties**.
   - On the General Tab, for "Allow Dynamic Updates," select "Only Secure Updates" from the menu.
   - The Zone Transfers Tab is only for use when there is a trust between this domain and another domain. If there is a trust, you must transfer zone updates from this Active Directory Integrated Zone to a Standard Secondary Zone on the DNS Servers in the other domain. Select "Allow Zone Transfers," then choose "only to the following servers" and enter the IP Addresses of the DNS Servers in the other domain.
   - To configure the required Reverse Lookup Zones, repeat the steps below for each ICM domain level network within the Forward Lookup Zone.

   Note: Networks within a Forward Lookup Zone include all visible and private networks utilized in a DNS Zone. These networks define Reverse Lookup Zones relative to the Forward Lookup Zone.
   - Under the server name, right-click on Reverse Lookup Zones and select New Zone.
   - Within the New Zone wizard, select "Active Directory Integrated".
   - In the Reverse Lookup Zone screen, select the radio button "Network ID" and enter required the number of octets for the Reverse Lookup Zone. The Reverse Lookup Zone Name automatically enters.

Repeat the steps below for each ICM domain Reverse Lookup Zone:

1. Highlight the zone name under Reverse Lookup Zones, right-click and select **Properties**.
2. On the General Tab, for "Allow Dynamic Updates," select "Only Secure Updates" from the menu.

Manually complete DNS Host and PTR records

1. Manually enter all hostnames for the machines that house ICM nodes, as well as all NIC's and Peripherals for which ICM Setup requires hostname resolution, into the appropriate DNS Forward Lookup Zone. On the DNS Server, right-click on the Forward lookup Zone Name and select "New Host." The hostname of this Root Domain Controller should already be in the file.
2. Add All ICM hostnames (visible, visible high, private, private high, SAN) and their associated IP Addresses. Check the box to create an associated PTR Record (reverse lookup zone record).
3. You must manually enter any Peripherals (ACD's/VRU's) and NIC's accessed by the ICM through hostname resolution in the Forward Lookup Zone.

Add an Enterprise Level Secondary Forward Lookup Zone

1. Highlight Forward Lookup Zones, right-click and select New Zone.
2. Within the New Zone wizard, select “Standard Secondary” zone and enter the full DNS name of the Parent Domain.
3. Enter the IP addresses of the Enterprise Level DNS Servers. The wizard completes.

Access the enterprise Level DNS Servers and Add Child Domain as a Secondary Forward Lookup Zone

1. Highlight the Forward Lookup Zones, right-click and select **New Zone**.
2. Within the New Zone wizard, select “Standard Secondary” Zone and enter the full DNS name of the Child Domain.
3. Enter the IP addresses of the Child Domain Level DNS Servers and allow the wizard to complete.

Change the DNS settings on this First Domain Controller in the Child Domain to point to this Child Domain level DNS Server.

Follow step 6 on installing additional Domain Controllers from page 18.

Step 7: Install and Configure DNS on Additional Domain Controller

Substitute Step 7 detailed below for Step 7 from the Enterprise ICM Dedicated Forest/Domain Model.

1. Click **Settings > Control Panel > Add/Remove Programs**.
2. Select Add\Remove Windows Components, check Networking Services and select **Details**.
3. Check only DNS, click **OK** and then click **Next**.
4. Browse to the Windows 2000 CD. DNS installs.
5. Validate that all DNS Zones were replicated from the 1st DNS Server in the AD Domain to this DNS Server.
6. Manually add the Enterprise level Standard Secondary Zone.
7. Change DNS Settings on the Firest Domain Controller in the Child Domain to point to this additional Child Domain level DNS Server.

Follow step 7 on creating active directory sites from page 18.

Step 9: Assign Global Catalog and FSMO Roles and Configure Time Source

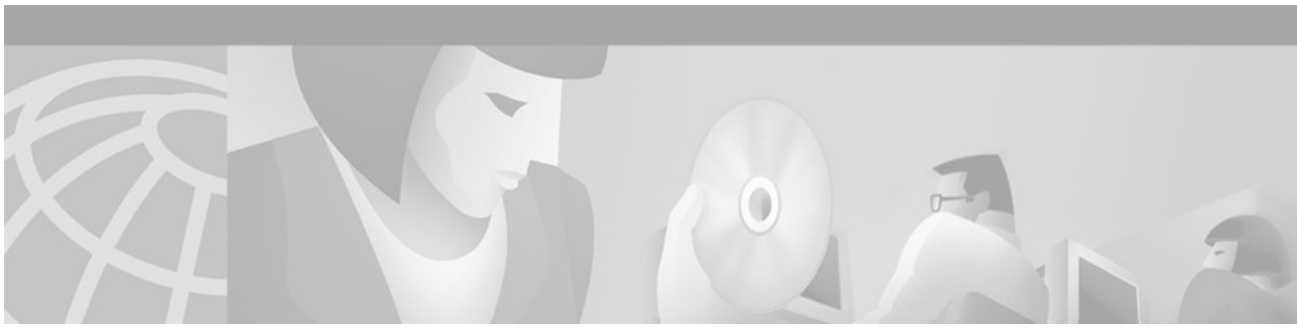
Complete Step 9 as detailed for the Enterprise ICM Dedicated Forest/Domain Model with the following exception.

Child Domain Servers source time from the Child Domain PDC Emulator. The Child Domain’s PDC Emulator sources time from the Parent Domain’s Time Source for System Time.

Step 10: Configure Trust Relationships

Substitute Step 10 detailed below for Step 10 from the Enterprise ICM Dedicated Forest/Domain Model.

The Child Domain has an automatic two-way transitive trust with the Parent Domain. Verify that this trust was created.



Hosted NAM/CICM Model

Sample Diagrams

Figure 5 NAM/CICM Model-NAM Dedicated/Forest Domain-Central Controller Sites

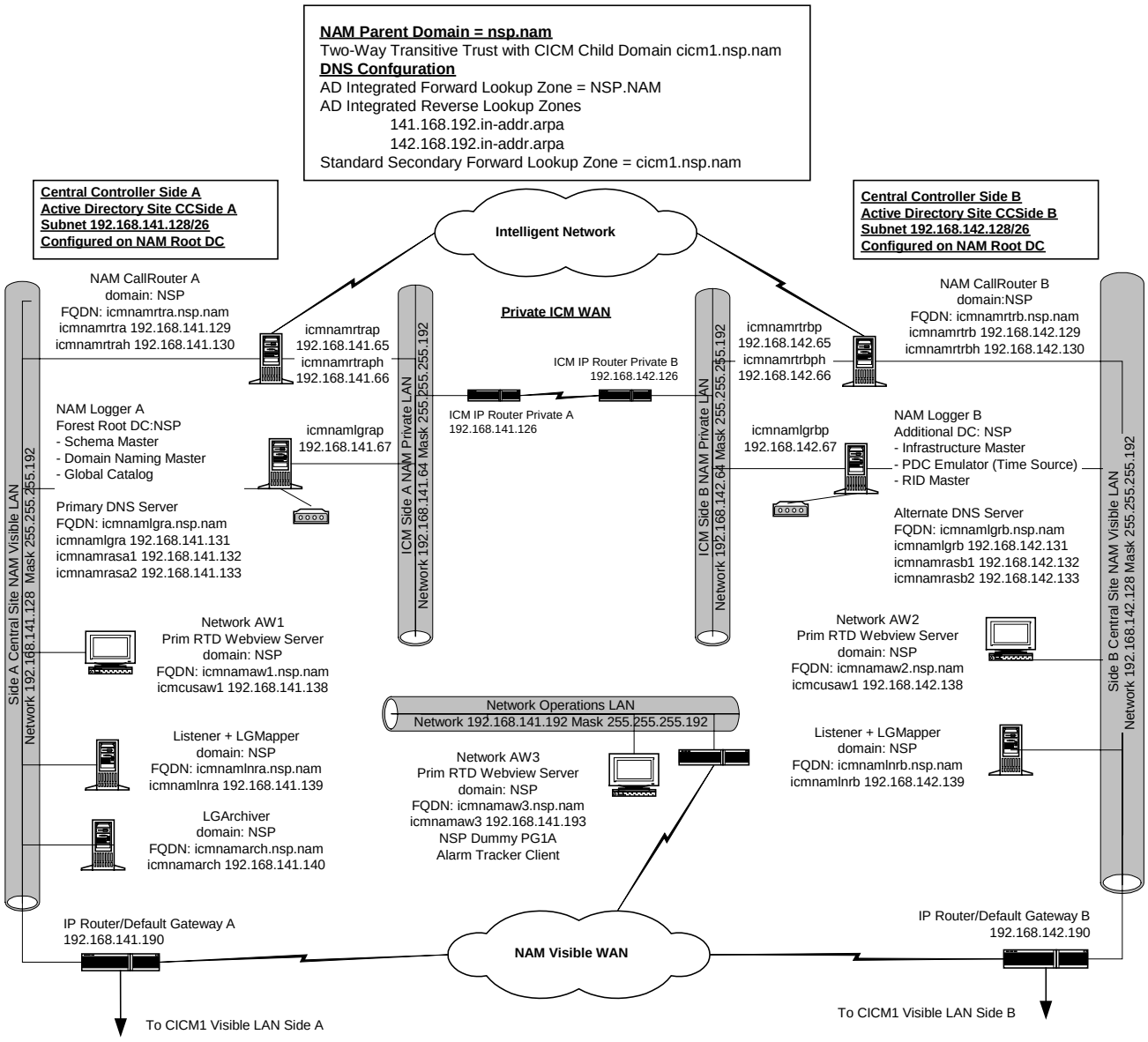


Figure 6 NAM/CICM Model-CICM Child Domain-Central Controller Sites

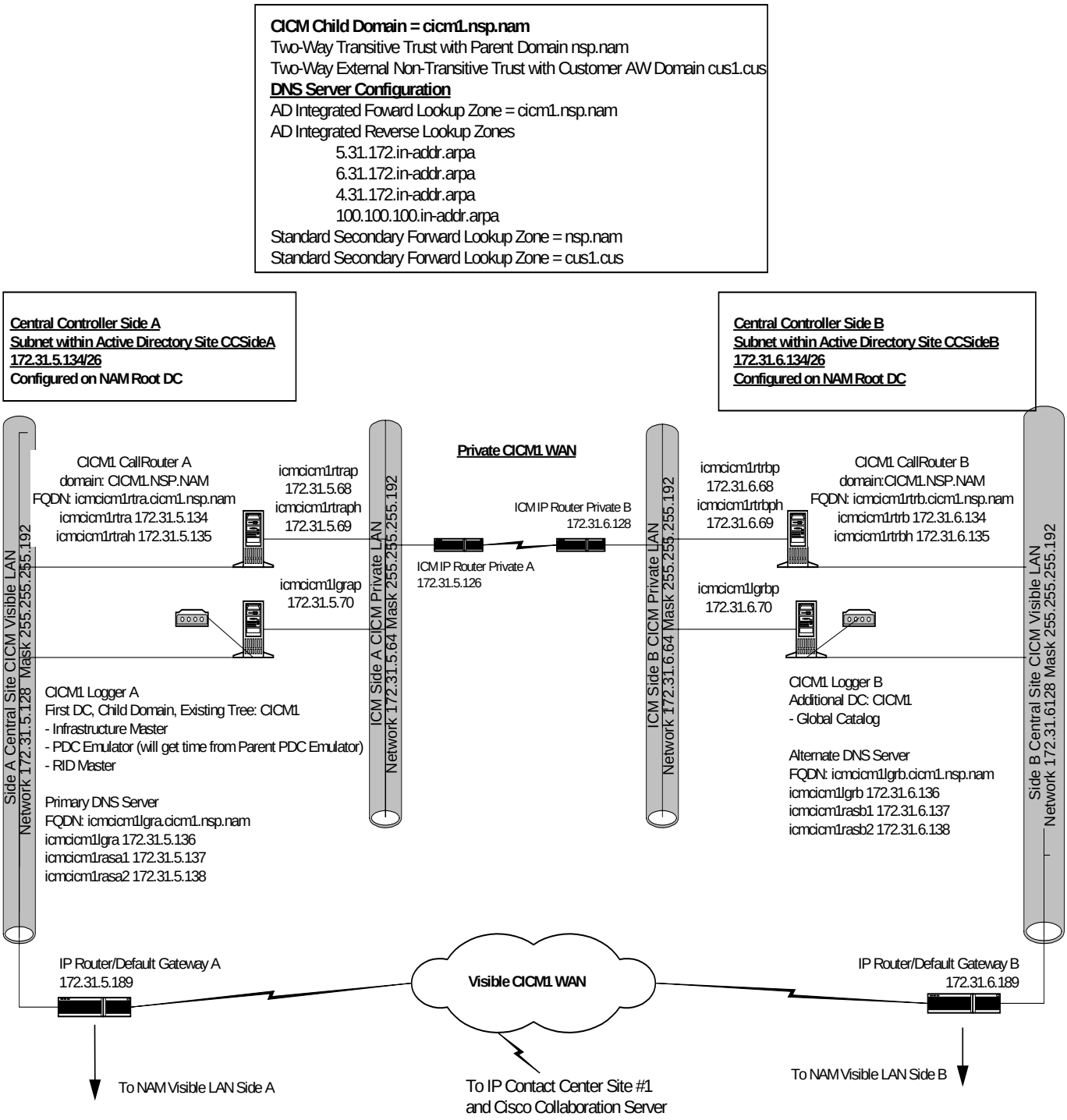
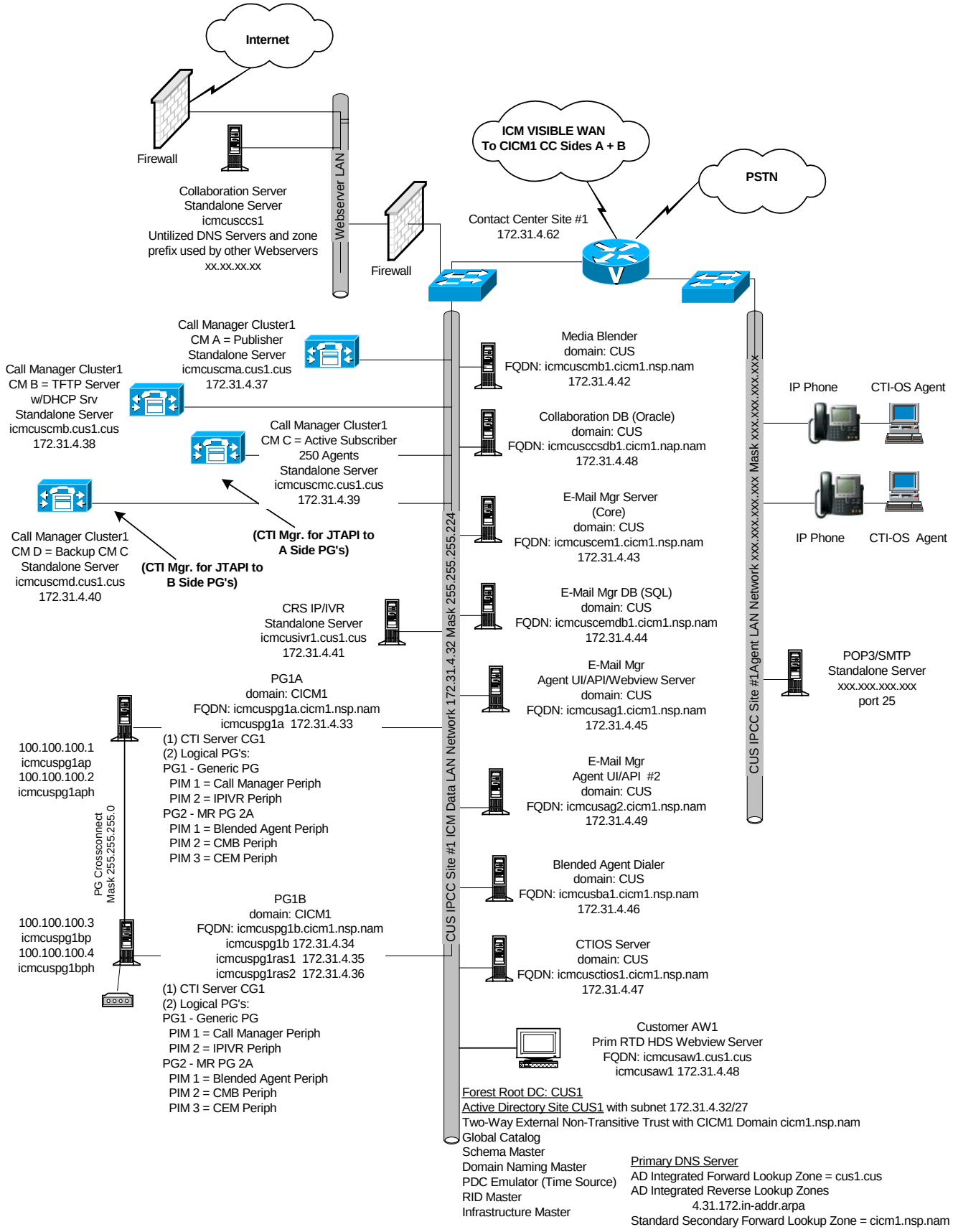


Figure 7 NAM/CICM Model-Customer AW Domain at Call Center Site



Staging Tasks All Servers

Step No.	Task
1.	Validate that Staging Prerequisites have been met
2.	Install Windows 2000 SP4 on All Servers - Standalone
3.	Apply Custom Settings on All Servers
4.	Install PCAnywhere

Step 1. Validate that Staging Prerequisites have been met

Step 2. Install Windows 2000 Servers and Service Pack 4 on All Servers – Standalone

- Install Windows 2000 Server CD.2. Create Drive Partitions according to settings in 3rd Party Host Form, for the machine being built. You may need to use the equipment manufacturer's drive partitioning/RAID array software to set up the partition.
- Format the C drive as NTFS.

Recommendations

Logger and AW/HDS: Create the C drive during this phase of the installation and create the D drive in the Custom Settings of this document.

- Drive C: Operating System/Boot Partition, virtual memory swap file space, core ICM software and SQL Server as well as SQL log and temp files.
- Drive D (which you create later): Used by SQL to store ICM database (logger database and HDS database on AW). Keep log and temp files for these databases on Drive C to maximize database performance.

CallRouters, PG's, AW's (non-HDS), CTI Server, CTIOS Server

- Drive C: single drive partition for OS/Boot Partition, virtual memory, swap file space, core ICM software and for AW non-HDS db, SQL Server and all SQL databases.

The system reboots and displays the Windows 2000 Server Setup wizard. Perform the steps listed below.

1. The first prompt is Regional Settings. You set system local and keyboard layout.
2. Next, enter Company Name and Organization.
3. Select Per Seat Licensing.
4. Enter the hostname for the machine and the Administrator Password (refer to 3rd Party Host Form).
5. Highlight Management and Monitoring Tools and click **Details**.
   - Check Network Monitor Tools.
   - Click **OK**.
6. Under Windows 2000 Components uncheck IIS unless this machine hosts a Webview Server or Collaboration Server, Media Blender or any of Cisco E-Mail Manager Servers. In the case of these particular servers, highlight IIS and click on **Details**. Only check Common Files, Front Page 2000 Server Extensions, Internet Information Services Snap-In, Internet Services Manager, Visual InterDev RAD Remote Deployment Support, and World Wide Web Server.
7. Enter the Correct Date/Time and Time Zone Settings.

Note: All central controller systems must be in the same time zone, regardless of physical location.

8. Under Network Settings, select Custom Settings. Refer to system diagram and/or 3rd party host form for each server's respective information required in IP and DNS sections.
9. For the Visible Ethernet Card, set the properties for File and Printer Sharing to Microsoft Networks to maximize the data throughput for network applications.
10. For the Visible Ethernet Card, select TCP/IP for the Protocol. Click **Properties**.
    - Enter the information for visible IP address, subnet mask, default gateway and preferred and alternate DNS servers for the machine.
    - Click the Advanced Tab.
    - Enter the "high" visible addresses from the ICM System Diagram, if applicable.
    - On the DNS Tab, in the "DNS suffix for this connection", enter the name of the local DNS zone for the machine and check the "Register" box.
    - Since CICM Distributors housed on the NAM Network AW's require access to the Central Controllers in the CICM domain, the NAM Network AW's require access to resources in a different trusting/trusted domain/DNS zone. Therefore, select "append these DNS suffixes" (in order) and enter the local DNS zone for the machine first and add other secondary zones, which represent the trusting/trusted domain.
    - For the NAM Network AW, enter the CICM zone housing the CICM Central Controllers. The CICM instance Distributor needs to access the CICM Central Controllers on that Network AW. Similarly, the CICM Loggers and Routers need to search DNS zones at the NAM Level and at the Customer AW Level. The Customer AW also needs to search DNS Zones at the CICM level.
11. Private Ethernet Card: when you click "Next" on the networking components, another Networking Components screen opens if the machine has more than one network interface card.
    - Uncheck the Client for Microsoft Networks and File and Print Sharing options.
    - The Protocol is TCP/IP. Click **Properties**.
    - Enter the private IP address and subnet mask for the server. Leave the default gateway field blank.
    - Click on the Advanced Tab and enter the "high" private addresses, if applicable
    - For the DNS tab, leave the address space empty and uncheck the "register" box.
12. Under Workgroup or Computer Domain, select "No, this computer is not on a network, or is on a network without a domain." The machine restarts.
13. After the restart, login with new the username created during setup. The "Configure Your Server" wizard opens. Select "I will configure this server later." Uncheck "Show this screen at startup."
14. Install Windows 2000 Service Pack 4. Restart the machine upon completion of the Service Pack install.

Step 3. Apply Custom Settings on All Servers

Validate Card Settings and add other protocols (if required)

1. Right-click on My Network Places and select **Properties**. The Network and Dial-Up Connections window opens.
2. Rename each "Local Area Connection" icon to "private," "visible" and "san" as required.
3. On each card right-click **Properties** and select **Configure**.
    - Click on the Advanced Tab.

- Configure the network speed and duplex mode. Do not set to Auto Mode.

4. Right-click on the Visible icon and select **Properties**.

Note: NETBEUI is required on systems that will have Phone Home enabled. Phone Home is typically enabled on Loggers that Phone Home events to Cisco TAC.

5. View the components section and, if NETBEUI is required and does not appear, click **Install**.
   - Highlight Protocol and click **Add**.
   - Highlight NETBEUI Protocol and select **OK**.
   - After NETBEUI installs, you return to the **Properties** window.
6. Under the Advanced menu, select **Advanced Settings**. Bind the Visible Card.
   - View the Connection section of the Adapters and Bindings Tab. Sort the cards with Visible at the top, Private second and any remaining connection following.
   - Highlight the Private connection and, in the Bindings Section, uncheck the File and Printer Sharing for Microsoft Networks and Client for Microsoft Networks options.
   - Move any disabled Bindings for all connections to the bottom of the list.

   Note: You only need to complete the following two steps if NETBEUI is installed (typically on Loggers).
   - Highlight the Visible connection and uncheck all NETBEUI protocol bindings and move them to the bottom of the bindings list.
   - Highlight the Private connection and uncheck all NETBEUI protocol bindings and use the up/down arrows to move them to the bottom of the bindings list.

Create Drive Partitions

These steps show you how to create drive partitions, as detailed on 3rd Party Host Form

1. Click **Start > Programs > Administrative Tools > Computer Management**.
2. Assign the drive letter Z to the CD-ROM.
3. Under Storage, select Disk Management.
4. Create drive D as a primary partition using all remaining disk space on a RAID volume. If there is disk space on more than one physical disk, do not create a Volume Set.
5. Format the drive as NTFS and utilize Quick Format.

Create Shares per Customer Requirements.

There must be a hidden share for the C drive on Loggers. This is required for Listeners to access “phone home” events.

Disable Automatic Updates

1. Open the Control Panel and double-click Automatic Updates.
2. Uncheck “Keep my computer up to date….” and click **OK**.

Configure the Display

1. Open the Control Panel and select **Display**.
2. Verify that no Screen Saver is selected.
3. Set the display for at least 1024x768 resolution, 65K colors and at least 60 MHz.

Set System Properties

1. Open the Control Panel and double-click on **System**.
2. Click the Advanced Tab.
3. Click on the Performance Options.
4. Set Virtual Memory as required:
   - If you have less than 2G RAM, set Virtual Memory to 1.5 time physical size.
   - If you have more than 2G RAM, set Virtual Memory to 2G.
5. Click **Startup and Recovery**.
6. Change the value of the display list of operation systems to 3 seconds.
7. Click **OK** twice.

Configure the Event Viewer

1. Click **Start > Programs > Administrative Tools > Event Viewer**.
2. Highlight each Type in the left column, right-click, select **Properties** and set the log to 1024Kb. Select **Overwrite Events as Needed**. Install Routing and Remote Access as detailed on the 3rd Party Host Form, if necessary.

   Note: Routing and Remote Access is required for Loggers using modems to Phone Home, and for any other remote access points (typically 1 PG per Contact Center Site) for TAC to utilize.
3. Click **Start > Programs > Administrative Tools > Routing and Remote Access**.
4. Highlight the machine name and under the Action menu, select Configure and Enable Routing and Remote Access.
5. Click **Next** to start the Routing and Remote Access Server Setup wizard.
   - On the Common Configurations Screen, select Remote Access Server and click **Next**.
   - On the Remote Client Protocols, verify that TCP/IP (and NETBEUI, if required) are listed. Select "Yes, all of the required protocols are on this list" and click **Next**.
   - Under Network Selection, highlight the visible card and click **Next**.
   - For IP Address Assignment, select "From specified range."
   - Under the Address Range Assignment Screen, add Range of RAS addresses (from System Diagram) and click **Next**.
   - Click **NO** to Radius Server and click **Next**. Finish the setup (ignore the DHCP warning if you get one).

For Machines which allow Dial-In Access:

1. Right-click the Machine Name and select **Properties**.
   - Under General Tab click Remote Access Server.
   - For Machines which allow Dial-In Access for TAC Maintenance:
     - On the IP Tab, enable IP Routing.
     - On the NETBEUI Tab, uncheck "Allow NetBeui remote access."
   - For Listeners**:**

- For the IP Tab, do not Enable IP Routing.
- For the NETBEUI Tab, allow access to "This Computer Only".

2. Open **Computer Management** and select **Local User and Groups > Users**.
   - Double-click on **Administrator account**.
   - Select **Allow Access** on the Dial In tab.

Note: Routing and Remote Access Service is not supported on Windows 2000 Professional. Any Peripheral Gateway used with RRAS must run Windows 2000 Server.

Create a Software directory and load folders, as detailed on the 3rd Party Host Form

Add Persistent Static Routes as detailed on 3rd Party Host Form

For geographically distributed central controller sites, the CallRouters and Loggers have a Private IP WAN connection, used to communicate between side A and side B. Windows only allows one "default gateway" for each machine, which sends the Private Network traffic to the Visible Network assuming this "remote subnet" was reachable by the defined default gateway. Since this is not the case, there needs to be a set of Static Routes added to the CallRouter and Logger systems on both sides of the system to direct this traffic to the Private Network.

1. On CallRouter A and Logger A:

   route add <network number> mask <subnet mask> <gateway IP> -p

   Example: route add 192.168.142.64 mask 255.255.255.192 192.168.141.126 –p

   Where:
   The network number of the remote Private Network is 192.168.142.64
   The subnet mask for this remote network is 255.255.255.192
   The local Private Network Adaptor Card's IP Address is 192.168.141.126

   (-p sets the route as persistent)

2. On CallRouter B and Logger B:

   Example: route add 192.168.141.64 mask 255.255.255.192 192.168.142.126 –p

Configure Telnet Security as detailed on 3rd Party Host Form

Windows 2000 provides a Microsoft standard Telnet utility that comes pre-configured to allow users to start connections without logging into the domain for account validation. To help secure the ICM systems, set this to require users to login using Telnet by using the Windows Registry Editor.

1. Run **regedit32.exe**. Expand **HKEY_Local_Machine\Software\Microsoft\Telnetserver\1.0**.
2. Set NTLM to ZERO (0) to require users to login.
3. The Telnet Service must be set to Autostart and then stopped and restarted.

Step 4. Install PCAnywhere

1. Run the setup executable (**pcA105r.exe**) and accept the license agreement.
2. Use the TYPICAL setup type.

3. Cancel the Welcome to Live Update window.
4. Skip Registration and click **Finish**. Click **Yes** to reboot.
5. Open PCAnyWhere (Skip Registration).
   - Double-click the Add a Host icon
   - On the Connections Tab, select **TCP/IP**.
   - On the Settings Tab, check Launch with Windows, Run Minimized, and Run as a Service.
   - On the Callers Tab, select Windows from the Authentication Type menu.
   - Under the Caller List, click on the New Item icon.
   - On the Identification Tab: select GROUP and from the Domain menu, select the domain of this machine and select the Domain Admins Account.
   - On the Privileges Tab, select Superuser and click **OK**.
   - Under the Security Options Tab, under Encryption Level, select PCAnywhere from the menu, check off "Deny Lower Encryption Level" and click **OK**.
   - Give the new Host icon the same name as the machine.
   - Double-click this icon to start the host service.
6. Access Services in the Control Panel. In the Startup button, configure the PCAnywhere service to start automatically.

Staging Tasks NAM Domain

Step No.	Task
5.	Install NAM Forest Root Domain Controller/DNS Server
6.	Configure DNS Server on NAM Forest Root Domain Controller
7.	Install Additional Domain Controller
8.	Install and Configure DNS on Additional Domain Controller
9.	Configure Active Directory Sites
10.	Assign Global Catalog and FSMO Roles and Configure Time Source
11.	Configure Trust Relationships
12.	Join Standalone Servers to Domain
13.	Validate IP Connectivity and Remote Access
14.	Install SQL Server on Loggers, AW's, LGMappers and LGArchivers
15.	Install Webview 3rd Party Software
16.	Install Infomaker on AW's
17.	Install ICM Software on Loggers
18.	Create Logger Databases
19.	Install ICM Software on CallRouters
20.	Start Logger and Router Services
21.	Install ICM Software on Admin Workstations
22.	Expand AW Database

Step No.	Task
23.	Start AW (Distributor) Services
24.	Configure NIC's, Peripheral Gateways and Peripherals
25.	Install ICM Software on Peripheral Gateways
26.	Start PG Services

Step 5. Install NAM Forest Root Domain Controller/DNS Server

1. Click **Start > Run**, enter **DCPROMO** and click **OK**. The Active Directory Installation wizard opens.
2. Under the "Domain Controller Type," select the "Domain Controller for a New Domain." The "Create Tree or Child Domain" screen appears.
3. Select "Create a new Domain Tree," the "Create or Join Forest" screen appears.
4. Select "Create a New Forest of Domain Trees." The "New Domain Name" screen opens. Type in the full DNS name for the new domain.
5. On the "NetBIOS Domain Name" screen, type in the NetBIOS name.
6. Accept Database and Log Location defaults.
7. Accept the Shared System Volume default. A warning appears claiming that the wizard cannot contact the DNS Server (since you have not configured it yet). Click on **OK** and you are presented with the "Configure DNS Screen." Select "Yes, install and configure DNS on this computer."
8. On the "Permissions" screen, select "Permissions compatible with pre-Windows 2000 servers."
9. On the "Directory Services Restore Mode Administrator Password," input Administrator password as detailed in the 3rd Party Host Form.
10. On the Summary screen, check settings and click on **Next**. Insert the Windows 2000 CD and setup continues to install Active Directory and DNS Server.
11. Restart when the installation completes.

Step 6. Configure DNS Server on NAM Forest Root Domain Controller

1. Click **Start > Programs > Admin Tools > DNS**.
2. Expand the Hostname Tree.
3. Expand the Forward Lookup Zones.
4. Right-click the root folder (the folder named ".") and select **delete**. You receive a warning about the zone. Click **Yes**.
5. Highlight the machine name, right-click and select **Properties**.
6. On the Interfaces Tab, select "Listen on Only the following IP addresses" and remove all but the visible machine address.
7. Complete the configuration of AD Integrated Forward and Reverse Lookup Zones.
   - Right-click the NAM Domain zone name under Forward Lookup Zones and select Properties.
   - On the General Tab, for "Allow Dynamic Updates," select "Only Secure Updates" from the menu.
   - Only use the Zone Transfers Tab when there is a Trust between this domain and another domain. In this case you need to Transfer Zone updates from this Active Directory Integrated Zone to a Standard Secondary Zone on the DNS Servers in the other domain. You elect to "Allow Zone Transfers," then choose "only to the following servers" and enter the IP Addresses of the DNS Servers in the other domain.

- To configure the required Reverse Lookup Zones, perform the steps below for each NAM domain level network within the Forward Lookup Zone.

  Note: Networks within a Forward Lookup Zone include all visible and private networks used within a DNS Zone. These networks define Reverse Lookup Zones relative to the Forward Lookup Zone.

- Under Server Name, right-click on Reverse Lookup Zones and select **New Zone**.
- Within the New Zone wizard, select "Active Directory Integrated."
- In the Reverse Lookup Zone screen, select the radio button "Network ID" and enter the required number of octets for the Reverse Lookup Zone. The Reverse Lookup Zone Name automatically enters.

Repeat the steps below for each NAM domain Reverse Lookup Zone.

1. Right-click the Zone name under the Reverse Lookup Zones and click **Properties**.
2. On the General Tab, for "Allow Dynamic Updates," select "Only Secure Updates" from the menu.

Manually complete the DNS Host and PTR records

1. Manually enter the hostnames for the machines housing ICM nodes, as well as all NIC's and Peripherals for which ICM Setup requires hostname resolution into the appropriate DNS Forward Lookup Zone.
2. On the DNS Server, right-click on the Forward lookup Zone Name and select "New Host." (The hostname of this Root Domain Controller should already be in the file.)
3. Add all NAM level hostnames (visible, visible high, private, private high, SAN) and their associated IP Addresses and check the box to create an associated PTR Record (reverse lookup zone record).
4. You must also manually enter any Peripherals (VRU's/ISN related nodes) and NIC's accessed by the NAM via hostname resolution in the Forward Lookup Zone.

Step 7. Install Additional Domain Controller

1. Click **Start > Run** and enter **DCPROMO**. The Active Directory wizard opens. Click **Next**.
2. Under the "Domain Controller Type," select "Additional Domain Controller for an Existing Domain."
3. At the "Network Credentials" screen, enter the domain admin username and password.
4. The Additional Domain Controller screen should already be filled in with the fully qualified DNS name.
5. Accept the database and log locations defaults.
6. Accept the shared System Volume defaults.
7. Input the same Restore Mode Admin password that utilized on the Root Domain Controller.
8. Check the Summary Settings. AD is not configured via NETLOGON.
9. Restart after the AD install completes.

Step 8. Install and Configure DNS on Additional Domain Controller

1. Click **Settings > Control Panel > Add/Remove Programs**.
2. Click Add\Remove Windows Components, check Networking Services and click **Details**.
3. Check DNS, click **OK** and then click **Next**.
4. Browse to the Windows 2000 CD. DNS installs.
5. Make sure all DNS Zones were replicated from the 1st DNS Server in the AD Domain to this DNS Server.

Step 9. Configure Active Directory Sites

On the NAM Root Domain Controller:

1. Click **Start > Programs > Admin Tools > AD Sites and Services**.
2. Rename the default first site name as per the AD Site Plan in the ICM System Diagram.
   - For geographically separated DC, right click on Sites, select New Site and enter the site name of the additional domain controller as per the ICM System Diagram.
3. Create subnets for each DC site. Right-click on the Subnets folder and select New Subnet:
   - Enter the subnet address and mask respective to the LAN at the Domain Controller Site.
   - Highlight the Site Name associated with that subnet.
4. Expand the servers folder from the original first site folder. For each Server that you need to move to a different site, right-click on the server name, select **Move** and highlight the site you want to move it to.
   - Expand "Inter-Site Transport" under Sites.
   - Open "IP" folder and select "DEFAULTIPSITELINK" from the right pane.
   - Right-click,and select **Properties**. Make sure you add both sites as entries in the window titled "Sites in this Site Link."
   - Change the "Replicate Every" value to 15 minutes.

Step 10. Assign Global Catalog and FSMO Roles and Configure Time Source

Add Global Catalogs according to Global Catalog and FSMO plan in the ICM System Diagram and according to settings on 3rd Party Host Forms.

1. Open AD Sites and Services.
2. Connect to DC which is designated GC.
3. Right-click on NTDS Settings and select **Properties**. Check off Global Catalog.
4. Move FSMO roles as indicated in the ICM System Diagram and according to settings on the 3rd Party Host Forms.
5. On the AD DC hosting the role you're moving, open AD Users and Computers and connect to the DC to which you're moving the role.
6. Right-click on the domain name and select Operations Masters. Under the required FSMO role tab, change the Operations Master to this designated DC

Since the PDC Emulator has been moved to another Domain Controller, you must refine the Time Source as either that server or utilizing an external Time Source.

On the Server currently running the PDC Emulator, run the following command:

Net time /setsntp: <DNS Name of Time Source >

To synchronize a Server to the Time source:

W32tm -s <DNS Name of Time Source>

Step 11. Configure Trust Relationships

When the CICM Child Domain is created, there is an automatic two-way transitive trust between the NAM and the CICM Domain. Verify that this trust was created.

Step 12. Join Standalone Servers to Domain

1. Right-click on My Computer and select **Properties > Network Identification Tab > Properties**.
2. Click on the domain radio button and enter the Fully Qualified Domain Name.

3. Enter the Domain Administrator's username and password.
4. Restart the server and login to the domain.
5. Create shortcuts on desktop, as detailed on the 3rd Party Host Form.
6. Configure the command prompt:
   - Open the command prompt from the desktop shortcut.
   - Right-click in the title bar and select **Default**.
   - On the Options Tab, uncheck Quick Edit Mode and Insert Mode.
   - Click on the font tab and set the Command Prompt font size to 7x12.
   - Click on the layout tab and set the Command Prompt screen buffer to 200x9999.
7. Set the Folder Options:
   - Open the Control Panel and open Folder Options.
   - On the General Tab For Active Desktop, click Use Windows Classic Desktop and for Web View, click Use Classic Folders.
   - On the View Tab, Display the full path in the address bar and title bar. Show the hidden files and folders, and uncheck the hide file extensions.

Step 13. Validate IP Connectivity and Remote Access

On each machine, validate the settings on each network card (TCP/IP Properties), including the DNS settings. Referring to the System Diagram, validate that the machine can ping every machine on the visible network and, if applicable, that it can ping to all its private connections.

Validate the Host and PTR records on all DNS Servers to make sure that they contain all required zones and records.

Test remote access through the modem access points. You should be able to access each machine via modem, utilizing PCAnywhere and Telnet.

Step 14. Install SQL Server on Loggers, AW's, LGMappers and LGArchivers

1. Select **STANDARD EDITION** to start SQL Server setup program.
2. At the first screen select Install SQL 2000 Server Components.
3. Select Install Database Server.
4. Click **NEXT** at the Welcome Screen.
5. In Computer Name screen, use default Local Computer.
6. In Installation Selection screen, choose default "Create a new instance of SQL Server, or install Client Tools".
7. Enter information in the User Information screen.
8. Agree to the License Agreement by clicking **Yes**.
9. In Installation Selection screen, choose the default "Create a new instance of SQL Server, or install Client Tools"
10. Fill out the User Information screen.
11. Agree to the License Agreement by clicking **Yes**.
12. In the Installation Definition screen, choose the default "Server and Client Tools".
13. For Instance Name, check Default.
14. Select **CUSTOM** for the setup type.
15. Install Program Files to the C: drive (the default).
16. For the Components Screen, accept the defaults.

17. Under the Services Accounts, select:
    - CUSTOMIZE
    - USE THE LOCAL SYSTEM ACCOUNT
    - AUTO START SERVICES
    - SQL SERVER AGENT
    - USE THE LOCAL SYSTEM ACOUNT
    - AUTO START SERVICE – Check **OK** for the window that appears.
18. On the Authentication Mode Screen, select “mixed mode” and check “blank password”.
19. Set Collation Designator to Latin1_General and Check **Binary for Sort Order**.
20. Under Network Libraries deselect all choices except for NAMED PIPES.
21. Read the Start Copying Files screen and click **Next**.
22. Select PER SEAT as the licensing method and set 40 devices at least.
23. A dialog box with the message “Setup is installing Microsoft Data Accessing Components (MDAC)” shows up.
24. If a message box for Configure SQL Agent pops up, click **OK**.
25. When setup completes, reboot.

INSTALL SQL SERVER SERVICE PACK 2

1. Run setup.bat.
2. For Computer Name select Local Computer.
3. Accept the license agreement.
4. For the Instance Name, accept the default.
5. Connect to the Server using SQL Server System Administrator login. Select “leave sa password blank”.
6. Complete the setup and reboot.
7. Expand the database sizes and logs using SQL Enterprise Manager. Click **START > Programs > Microsoft SQL Server > Enterprise Manager**. Under the Server Name in Enterprise Manager, double-click on Databases. Expand the Server Tree and Highlight the Databases Folder under the Server name.
8. Double-click Master Database in in the right panel. The Master Properties window appears.
    - On the Data Files Tab:
        - Set the Space Allocated to 50MB.
        - Uncheck Autogrow.
    - On the Transaction Log Tab:
        - Set the Space Allocated to 20MB.
        - Uncheck Autogrow and click **OK**.
9. Double-click on Tempdb in the right panel. The **tempdb** properties window appears.
    - On the Data Files Tab
        - Set the Space Allocated to 50MB.
        - Uncheck Autogrow.
    - On the Transaction Log Tab:
        - Set Space Allocated to 20MB.
        - Uncheck Autogrow and click **OK**.
    - For the Options Tab, verify the following settings:

- Uncheck - ANSI NULL default, Recursive triggers, Auto close, Auto shrink and Use quoted identifiers
- Check – Auto update statistics, Torn page detection and Auto create statistics

o Close Enterprise Manager.

Step 15. Install Webview 3rd Party Software

Print and read the Read Me file on the "Webview 3rd Party Installer CD 6.0." This file describes the software and provides installation instructions. Various settings described in the Read Me file appear on certain setup screens.

1. Check to see if you have the Jaguar 3.5 software already installed on your machine. If Jaguar 3.5 software is installed on your machine, use the control panel's Add/Remove software program to remove that software.
2. Run Setup on the 3rd Party Installer CD 6.0
3. Reboot the server when setup completes
4. Use the following procedure to make sure that cache is updated at each new view of a real-time report.
   - o In the Internet Explorer window, select Internet Options from the Tools menu.
   - o If necessary, click the General tab to display the General Settings tab page.
   - o On the General Settings tab page, in the Temporary Internet Files sections, click **Settings**.
   - o In the Settings dialog box, enable the Every Visit to the Page option, then click **OK**.
   - o Click **OK** in the Internet Options dialog box.

   Note: Webview users are configured via ICM Configuration Manager and passwords default to a given expiration timeframe set by the user's domain. If a Webview User's password expires, the user cannot reset the password via Webview access, but must request that the ICM System Administrator set a new password. Once the user is created, the ICM System Administrator has the option to set Webview user passwords to NEVER expire through the Active Directory Users and Computers.

Step 16. Install Infomaker on AW's

Infomaker is only installed on AWs (Real Time Distributors and Real Time Clients) to create Custom Reports.

1. Run Setup from Media for Sybase Powerbuilder (Common Installer).
2. In the Welcome to 8.0 Installer screen, click **Next**.
3. Accept the License Agreement and click **Next**.
4. In the Customer Information screen, enter the username and company name. Click **Next**.
5. In the Destination Folder screen, accept the default and click **Next**.
6. In the Select components screen, select Infomaker, and Online Books. Uncheck all other options.
   - o You receive an Adaptive Server Anywhere warning. Click **OK** (ignore message).
   - o Do not select the Adaptive Server Anywhere. Click **No**.
   - o You receive a Personal Server (Adaptive Server Anywhere) warning. Click **OK**.
7. Accept default destination locations for all components and select "typical" for all setup types.

   Complete all Wizards and Reboot Server.

Step 17. Install ICM Software on Loggers

You can load the ICM Software Modules on the individual servers. See the System Design Specification for all values and non-default settings.

When the ICM Logger and Admin Workstation software loads using ICM Setup, it creates specific domain level groups and accounts in the ICM domain it is loaded into.

Cisco provides specific hot fixes to major releases and service packs of the ICM software to address service-impacting issues. You can download these hot fixes from Cisco's Web site (http://www.cisco.com/). You should apply them after the initial load of the software. The hot fix installation process only applies fixes required for the specific software module (CallRouter, Logger, type of PG, etc.).

Step 18. Create Logger Databases

After running the ICM Logger setup program and applying all hot fixes, you need to use the ICMDBA tool to finish the SQL Server configuration and build the actual ICM databases on the machine. You also use this tool on the Admin Workstation to create the Historical Database Server database (HDS).

For each Logger:

1. Click **Start > Run**, enter ICMDBA and click **OK**.
2. Click on the Server Name you want to change (Logger A or Logger B).
3. Select Create from Database menu.
4. The ICMDBA question prompts you to configure SQL Server, click **Yes**.
5. For the Configure Logger Screen: if the current value does not equal the recommended value, check the Configuration Box and verify that the new value equals the recommended value. Click **OK**.
6. Click **Yes** to continue. SQL Server stops and restarts .
7. On the Create Database Screen, select **Region**.
8. Click **Add** and choose type as the Data.
9. Highlight the D drive. Set the size to 70% of the available disk space if the Logger is for one customer instance only. If more than one instance resides on the Loggers, determine the database size with the customer. Click **OK** when finished.
10. Click **Add** and enter Log for the type.
11. Highlight the D drive. And set the size to 200MB (do not set the log device to larger than 500MB). Click **OK**.
12. Click **Create**. Click Start to Create Database. When the database is successfully completed, click **OK** and Close the database window.
13. Close ICMDBA.
14. Click START > Programs > Microsoft SQL Server > Enterprise Manager.
15. Expand the Server Tree and Highlight the Databases Folder under the Server name.
16. Double-click on the ICM Database in the right panel. You are now in the <cus_sideA> Properties Window.
    - On the Data Files Tab:
      - Check Autogrow. Set the File Growth to 10%.
      - Set Maximum File Size to [use the following calculation].

        {80% of free disk space}/{number of ICM db files on this disk}+{db file current size}

        example: {10GB * .80}/{1}+{25GB}=33GB
    - On the Transaction Log Tab:
      - Uncheck Autogrow and click **OK**.

Step 19. Install ICM Software on CallRouters

ICM Nodes Forms, which identify all values and non-default settings to be used in Setup, are created in the Planning phase of a deployment program and reside in the ICM System Design Specification.

Cisco provides specific hot fixes to major releases and service packs of the ICM software to address service-impacting issues. You can download hot fixes from Cisco's Web site (http://www.cisco.com/). Apply the hot fixes after the initial load of the software. The hot fix installation process only applies fixes required for the specific software module (CallRouter, Logger, type of PG, etc.).

Step 20. Start Logger and Router Services

The ICM is set up with an empty database. You need to add configuration information to complete the basic testing components. In order to add configuration data, the Central Controller and Admin Workstation(s) must be running. The ICM software loads an "ICM Service Control" tool on the desktop of each server used to control the services loaded on that machine. Start the services in the following order:

- Logger A
- CallRouter A
- CallRouter B
- Logger B

Each service starts several process windows on the task bar of the local machine, each one an ICM program associated with the service. As each node starts up, it looks for the other server components and attempts to register with them. If you completed the ICM Setup and network testing successfully, no major errors should occur.

Verify that the ICM Processes have no errors:

- CallRouters:
  - Router: UP and synchronized with peer
  - Ccagent: [is in service but is not connected to any peripheral gateways]
  - Rtsvr: [no connectivity to AW at this time]
- Loggers:
  - Logger: connected to its respective database and synchronized with peer – MDS is in service
  - Replication: [no connectivity to AW HDS at this time]

Step 21. Install ICM Software on Admin Workstation

Complete setup on all Admin Workstations (see System Design Specification).

When the Admin Workstation software loads using ICM Setup, it creates specific domain level groups and accounts in the ICM domain it is loaded into.

Cisco provides specific hot fixes to major releases and service packs of the ICM software to address service-impacting issues. You can download hot fixes from Cisco's Web site (http://www.cisco.com/). Apply these hot fixes after the initial load of the software. The hot fix installation process only applies fixes required for the specific software module (CallRouter, Logger, type of PG, etc.).

Step 22. Expand AW Database

1. Click **Start > Run**, enter ICMDBA and click **OK**.
2. Expand Tree under the AW Hostname.
3. Highlight <cus_awdb>.
4. Select Expand from the database menu.
5. Highlight the C drive.
6. Expand data to 500MB. Click **OK**.
7. Click **Start** on the expand database window. Click **OK** and then close the window.
8. Select **Expand** from the Database menu.

9. Select Log (the C drive is automatically highlighted).
10. Expand the Log to 200MB. Click **OK**.
11. Click **Start** on Expand Database window. Click **OK** and close the window.
12. Close ICMDBA.
13. Click **Start > Programs > Microsoft SQL Server > Enterprise Manager**.
14. Expand the Server Tree and Highlight the Databases Folder under the Server name.
15. Double-click on the ICM Database in right panel. You are now in the <cus_awdb> Properties Window.
    - On the Data Files Tab:
      - Check Autogrow and set the File Growth to 10%.
      - Set the Maximum File Size to [use the following calculation].

      {80% of free disk space}/{number of ICM database files and aw logs on this disk}+{database file current size}

      example: {4GB * .80}/{2}+{.5GB}=2.1GB
    - On the Transaction Log Tab:
      - Check Autogrow and set the File Growth to 10%.
      - Set Maximum File Size to [use the following calculation].

      {80% of free disk space}/{number of ICM database files and aw logs on this disk}+{database file current size}

      Example: {4GB * .80}/{2}+{.2GB}=1.8GB

Step 23. Start AW (Distributor) Services

Start the Distributor Service within Cisco Service Control.

Verify that the ICM Processes have no errors:

- CallRouters:
  - Router: running and synchronized with peer
  - Ccagent: [is in service but is not connected to any peripheral gateways]
  - Rtsvr: feed activated to AW
- Loggers:
  - Logger: connected to its respective database and synchronized with its peer. MDS is in service.
- Admin Workstation:
  - Updateaw: displays “waiting for new work”
  - Iseman: listen thread waiting for client connection

Step 24. Configure NIC’s, Peripheral Gateways and Peripherals

Before starting the ICM Services on the SS7 Gateways, NICs and Peripheral Gateways, you need to configure them in the ICM using the NIC and PG Explorer tools. The System Design Specification should indicate the values and setting changes required during the setup of these nodes.

In order to properly run ICM Setup for the NICs and PG’s, you need to pre-plan the Logical and Peripheral ID numbers, as they are required data elements to complete the setup program. The ICM automatically generates ID numbers from the Explorer tools, so you need to set them up in the Explorers in the exact order you planned them using the Node Form.

If the ID numbers are not generated in the proper sequence, you can correct them in the Peripheral Gateway machines by re-running setup locally. They must match the ICM configuration database to the value in the PG’s registry, or the ICM CallRouter rejects the connection request.

The Node Form worksheet lists the NIC interfaces first, although, for the Sprint and MCI NIC, there is no additional platform or specific services to start (they are co-resident in the ICM CallRouter). The ICM Setup program requires the ID values when the CallRouter is set up. When the services start on the CallRouter, these ID values are validated against the ICM configuration database and rejected if they do not match.

Also, you must configure an ICM Gateway for each CICM Instance on the NAM for connectivity from the NAM CIC process to the CICM INCRP NIC.

Step 25. Install ICM Software on Peripheral Gateways

Typically, PG's associated with the NAM Domain are IVR/ISN PG's.

Complete the setup on all Peripheral Gateways (see System Design Specification).

Cisco provides specific hot fixes to major releases and service packs of the ICM software to address service-impacting issues. You can download hot fixes from Cisco's Web site (http://www.cisco.com/) and apply them after the initial load of the software. The hot fix installation process only applies fixes required for the specific software module (CallRouter, Logger, type of PG, etc.).

Step 26. Start PG Services

Once the ICM configuration database is set up with the appropriate peripherals, you can start the PG services using the Cisco Service Control application on the desktop of the PG. If the local peripheral (IVR/ISN) is not available to connect to the PG, "disable" it in the PG setup. Testing only proves that the PG communications layer is set up properly and that it can talk to the CallRouters and obtain configuration information.

Verify that the ICM Processes have no errors:

- CallRouters:
  - Router: UP and synchronized with peer
  - Ccagent: connected to all configured peripheral gateways
  - Rtsvr: feed activated to AW
- Loggers:
  - Logger: connected to its respective database and synchronized with peer – MDS is in service
- Admin Workstation:
  - Updateaw: displays "waiting for new work"
  - Iseman: listen thread waiting for client connection
- Peripheral Gateways:
  - Mdsproc: inservice
  - Pgagent: inservice and active to one side of central controller
  - [peripheral] PIMs: disabled on node form – PIM windows do not exist

Staging Tasks CICM Domain

Step No.	Task
27.	Install First Domain Controller Server for CICM Child Domain
28.	Install DNS Server on First Domain Controller for CICM Child Domain
29.	Install Additional Domain Controller
30.	Install and Configure DNS on Additional Domain Controller
31.	Configure Active Directory Sites
32.	Assign Global Catalog and FSMO Roles and Configure Time Source

Step No.	Task
33.	Configure Trust Relationships
34.	Join Standalone Servers to Domain
35.	Validate IP Connectivity and Remote Access
36.	Install SQL Server on Loggers
37.	Install E-Mail Manager database
38.	Install Collaboration database
39.	Install ICM Software on Loggers
40.	Create Logger Databases
41.	Install ICM Software on CallRouters
42.	Start Logger and Router Services
43.	Install ICM Software on Admin Workstations
44.	Expand AW Database
45.	Start AW (Distributor) Services
46.	Configure NIC's, Peripheral Gateways and Peripherals
47.	Configure Multi-Media Nodes
48.	Create and Configure CONAPI Connections
49.	Install ICM Software on Peripheral Gateways
50.	Install ICM Software for CTI Server
51.	Install CTIOS Server
52.	Start PG, CTI and CTIOS Services
53.	Install and Start Blended Agent Dialer
54.	Install and Start E-Mail Manager Servers
55.	Install and Start Collaboration Server
56.	Install and Start Media Blender Server

Creating the CICM Child Domain requires the use of administrative privileges from the NAM domain System Administrator.

Cisco recommends that the CICM Child Domain provide DNS services locally within that domain.

The Visible Network Card on the First Domain Controller created in the CICM Child Domain must temporarily have the DNS Settings point to an Enterprise Level (Parent/NAM) DNS Server until a DNS Server is available at the Child Domain level.

Step 27. Install First Domain Controller Server for CICM Child Domain

1. Click **Start > Run**, enter **DCPROMO** and click **OK**. The Active Directory Installation wizard opens.
2. Under "Domain Controller Type," select "Domain Controller for a New Domain." The "Create Tree or Child Domain" screen appears.
3. Select "Create a New Child Domain in an Existing Domain Tree."

4. Enter the username, password and fully qualified domain name for the Parent (Forest Root) domain (the NAM Domain) on the Network Credentials Screen.
5. For Child Domain Installation:
   - Enter full DNS name of Parent (NAM) Domain.
   - Under Child Domain, enter the NETBIOS name for the Child and the full DNS name automatically enters at the bottom of the screen.
6. Accept Database and Log Locations defaults.
7. Accept the Shared System Volume default.
8. On the "Permissions" screen, select "Permissions compatible with pre-Windows 2000 servers."
9. On the "Directory Services Restore Mode Administrator Password," input Administrator password, as detailed in the 3rd Party Host Form.
10. Restart when the installation completes.
11. Delete the Child Domain subfolder on the Parent Level (NAM) DNS Servers.

When the ICM Child Domain is created, Windows automatically creates a "subfolder" in the Enterprise Root DNS tree to contain the servers in the new Child Domain. Typically, these folders are only used for a small numbers of servers, for ease of management and administration. In light of this subfolder you create an individual DNS zone for the new Child Domain.

Step 28. Install DNS Server on First Domain Controller for CICM Child Domain

1. Click **Start > Programs > Admin Tools > DNS > Configure Your Server**.
2. From the left column, select the "Networking" menu and select DNS.
   - Select Setup DNS and you are prompted to insert the Windows 2000 CD
   - DNS then loads
3. Click **Start > Programs > Admin Tools > DNS**.
4. Expand the hostname tree.
5. Right-click the Forward Lookup Zones and select New Zone.
6. Within the New Zone wizard, select "Active Directory Integrated Zone" and enter the full DNS name of the Child Domain DNS zone. Allow the wizard to complete.

   Note: Refresh may take a long time.
7. Right-click the machine name and click **Properties**.
8. On the Interfaces Tab, select "Listen on Only the following IP addresses" and remove all but the visible machine address.

Now, you need to complete the configuration of the AD Integrated Forward and Reverse Lookup Zones.

1. Right-click the CICM Domain zone name under the Forward Lookup Zones and click **Properties**.
2. On the General Tab, for "Allow Dynamic Updates," select "Only Secure Updates" from the menu.
3. Only use the Zone Transfers Tab when there is a Trust between this domain and another domain. In this case, you need to transfer zone updates from this Active Directory Integrated Zone to a Standard Secondary Zone on the DNS Servers in the other domain. You "Allow Zone Transfers," then select "only to the following servers" and enter the IP Addresses of the DNS Servers in that other domain. The IP addresses are the machine addresses of the servers.
4. To configure the required Reverse Lookup Zones, repeat the steps below for each CICM domain level network within the Forward Lookup Zone.

   Note: Networks within a Forward Lookup Zone include all visible and private networks, which are utilized within a DNS Zone. These networks define Reverse Lookup Zones relative to the Forward Lookup Zone.
5. Under Server Name, right-click on Reverse Lookup Zones and select New Zone.

6. Within the New Zone wizard, select "Active Directory Integrated."
7. In the Reverse Lookup Zone screen, select the radio button "Network ID" and enter the required number of octets for the Reverse Lookup Zone. The Reverse Lookup Zone Name automatically enters.
8. Repeat the steps below for each CICM domain name under the Reverse Lookup Zone.
9. Right-click the Zone name under the Reverse Lookup Zones and click **Properties**.
10. On the General Tab, for "Allow Dynamic Updates," select "Only Secure Updates" from the menu.

Now, you need to manually complete DNS Host and PTR records.

1. Manually enter hostnames for the machines that house CICM nodes, as well Peripherals for which CICM setup requires hostname resolution into the appropriate DNS Forward Lookup Zone.
2. On the DNS Server, right-click on the Forward lookup Zone Name and select "New Host." (The hostname of this Root Domain Controller is already in the file.)
3. Add all CICM Level hostnames (visible, visible high, private, private high, SAN) and their associated IP Addresses.
4. Check the box to create an associated PTR Record (reverse lookup zone record).
5. Manually enter any Peripherals (ACD's/VRU's) accessed by the CICM via hostname resolution in the Forward Lookup Zone.

Add the Enterprise Level (NAM) Secondary Forward Lookup Zone

1. Right-click on the Forward Lookup Zones and select **New Zone**.
2. Within the New Zone wizard, select "Standard Secondary" Zone and enter the full DNS name of the Parent (NAM) Domain.
3. Enter the IP addresses of the Enterprise Level DNS Servers. Allow the wizard to complete.

Access the Enterprise Level DNS Servers (NAM DNS Servers) and add Child Domain as a Secondary Forward Lookup Zone

1. Right-click the Forward Lookup Zones and select **New Zone**.
2. Within the New Zone wizard, select the "Standard Secondary" Zone and enter the full DNS name of the Child Domain.
3. Enter the IP addresses of the Child Domain Level DNS Servers. Allow the wizard to complete.

Change DNS settings on this First Domain Controller in the CICM Child Domain to point to this CICM/Child Domain DNS Server.

Step 29. Install Additional Domain Controller

1. Click **Start > Run**, enter **DCPROMO** and click **OK**. The Active Directory wizard opens. Click **Next**.
2. Under "Domain Controller Type" select "Additional Domain Controller for an Existing Domain."
3. At the "Network Credentials" screen, input your domain admin username and password.
4. The Additional Domain Controller screen already contains the fully qualified DNS name.
5. Accept database and log locations defaults.
6. Accept shared System Volume defaults.
7. Input the same Restore Mode Admin password utilized on the Root Domain Controller.
8. Check Summary Settings. AD is not configured by NETLOGON.
9. Restart when the AD Install completes.

Step 30. Install and Configure DNS on Additional Domain Controller

1. Click **Settings > Control Panel > Add/Remove Programs**.
2. On the Add\Remove Windows Components, check Networking Services and select **Details**.
3. Check only DNS and click **OK**. Click **Next**.
4. Browse to Windows 2000 CD. DNS installs.
5. Validate that all DNS Zones were replicated from the 1st DNS Server in the AD Domain to this DNS Server.
6. Manually Add the Enterprise level Standard Secondary Zone (see the previous page).
7. Change DNS settings on the First Domain Controller in the CICM/Child Domain to point to this additional CICM/Child Domain server.

Step 31. Configure Active Directory Sites On Forest Root Domain Controller

1. Click **Start > Programs > Admin Tools > AD Sites and Services**.
2. Right-click on New Sites.
3. The AD sites with the CICM Domain Controllers are likely the same local LAN sites as the NAM Domain Controllers. Therefore, the AD Sites are already created, so you now need to create the CICM subnets and place the CICM DC's in the appropriate subnet.
4. Right-click on the Subnets folder and select **New Subnet**.
   - Define the subnets and masks respective to each LAN at each Domain Controller Site.
   - Associate each subnet with each site.
   - Double-click on the servers from the original first site folder, select **Move** and indicate the site you want to move them to.

Step 32. Assign Global Catalog and FSMO Roles and Configure Time Source

Add Global Catalogs according to the Global Catalog and FSMO plan in the ICM System Diagram and according to the settings on 3rd Party Host Forms.

1. Open the AD Sites and Services.
2. Connect to the DC designated as GC.
3. Right-click on NTDS Settings and check off Global Catalog.

The FSMO Roles of Infrastructure Master, PDC Emulator and RID Master are automatically created on the first Domain Controller in this Child Domain, and therefore do not have to be moved.

CICM Domain Servers source time from the CICM Domain PDC Emulator. The CICM Domain's PDC Emulator sources time from the NAM Domain's Time Source for System Time.

Step 33. Configure Trust Relationships

The CICM Child Domain has an automatic two-way transitive trust with the Parent Domain. The Customer AW Domain, which requires access to its Central Controller in the CICM domain, has a two-way external non-transitive trust with the CICM domain. Verify that this trust is set up after the creation of the Customer AW Domain.

Step 34. Join Standalone Servers to Domain

1. Right-click on My Computer and select **Properties > Network Identification Tab > Properties**.
2. Click on the Domain radio button and enter the Fully Qualified Domain Name.
3. Enter the Domain Administrator's username and password.

4. Restart the Server and login to the Domain.
5. Create shortcuts on the desktop, as detailed on the 3rd Party Host Form.

Configure the Command Prompt.

1. Open the Command Prompt from the desktop shortcut.
2. Right-click in title bar and select **Default**.
3. On the Options Tab, uncheck Quick Edit Mode and Insert Mode.
4. Click on the font tab and set the Command Prompt font size to 7x12.
5. Click on the layout tab and set the Command Prompt screen buffer to 200x9999.

Set Folder Options:

1. Open the Control Panel and open Folder Options.
2. On the General Tab, select **Active Desktop > Use Windows Classic Desktop** and select **Web View > Use Classic Folders**.
3. On the View Tab, display the full path in address bar and title bar. Show hidden files and folders and uncheck hide file extensions.

Step 35. Validate IP Connectivity and Remote Access

On each machine, validate the settings on each network card (TCP/IP Properties), including the DNS settings. Referring to the System Diagram, validate that the machine can ping every machine on the visible network and, if applicable, that it can ping to all its private connections.

Validate the Host and PTR records on all DNS Servers, to make sure that they contain all required zones and records.

Test remote access through the modem access points. You can access each machine by modem, utilizing PCAnywhere and Telnet.

Step 36. Install SQL Server on Loggers

1. Select **STANDARD EDITION** to start the SQL Server setup program.
2. At the first screen select Install SQL 2000 Server Components.
3. Select Install Database Server.
4. Click **NEXT** at Welcome Screen.
5. In the Computer Name screen, use default Local Computer.
6. In the Installation Selection screen, choose the default “Create a new instance of SQL Server, or install Client Tools”.
7. Enter the user and company in the User Information screen.
8. Agree to the License Agreement by clicking **Yes**.
9. In the Installation Selection screen, choose default “Create a new instance of SQL Server, or install Client Tools”.
10. Enter the user and company in the User Information screen.
11. Agree to the License Agreement by clicking **Yes**.
12. In the Installation Definition screen, choose default “Server and Client Tools”.
13. For the Instance Name, check **Default**.
14. Select **CUSTOM** for the setup type.
15. Install the Program Files to C: (the default).

16. For the Components Screen, accept the defaults.
17. Under Services Accounts, select:
    7. CUSTOMIZE
    8. USE THE LOCAL SYSTEM ACCOUNT
    9. AUTO START SERVICES
    10. SQL SERVER AGENT
    11. USE THE LOCAL SYSTEM ACOUNT
    12. AUTO START SERVICE – Check **OK** for the window that appears.
18. For the Authentication Mode Screen, select "mixed mode" and check "blank password".
19. Set the Collation Designator to Latin1_General and Check **Binary for Sort Order**.
20. Under Network Libraries, deselect all choices except for NAMED PIPES.
21. Read the Start Copying Files screen and click **Next**.
22. Select PER SEAT as the licensing method and set at least 40 devices. A dialog box with the message "Setup is installing Microsoft Data Accessing Components (MDAC)" appears.
23. If a message box for Configure SQL Agent pops up, click **OK**.
24. When setup completes, reboot the machine.

INSTALL SQL SERVER SERVICE PACK 2

1. Run **setup.bat**.
2. For the Computer Name, select Local Computer.
3. Accept the license agreement.
4. For the Instance Name, accept the default.
5. Connect to the Server using SQL Server System Administrator login. Select "leave sa password blank".
6. Complete setup and reboot.
7. Expand the database sizes and logs using SQL Enterprise Manager. Click **START > Programs > Microsoft SQL Server > Enterprise Manager**. Under the Server Name in Enterprise Manager, double-click on **Databases**. Expand the Server Tree and Highlight the Databases Folder under the Server name.
8. Double-click the Master Database in the right panel. You are now in the Master Properties Window.
    - On the Data Files Tab:
        - Set Space Allocated to50MB
        - Uncheck Autogrow
    - On the Transaction Log Tab:
        - Set Space Allocated to 20MB
        - Uncheck Autogrow and click **OK**.
9. Double-click on the Tempdb in right panel. You are now in the tempdb Properties Window.
    - On the Data Files Tab:
        - Set the Space Allocated field to 50MB
        - Uncheck Autogrow
    - On the Transaction Log Tab:
        - Set the Space Allocated field to 20MB
        - Uncheck Autogrow and click OK.
    - For the Options Tab, verify the following settings:
        - Uncheck - ANSI NULL default, Recursive triggers, Auto close, Auto shrink and Use quoted identifiers

- Check – Auto update statistics, Torn page detection and Auto create statistics

o Close Enterprise Manager.

Step 37. Install E-Mail Manager Database

1. Select STANDARD EDITION to start the SQL Server setup program.
2. At the first screen, select Install SQL 2000 Server Components.
3. Select Install Database Server.
4. Click **NEXT** at Welcome Screen.
5. In the Computer Name screen, use the default Local Computer.
6. In the Installation Selection screen, choose the default "Create a new instance of SQL Server, or install Client Tools."
7. Enter a user and company in the User Information screen.
8. Agree to the License Agreement by clicking **Yes**.
9. In the Installation Definition screen choose the default "Server and Client Tools".
10. For the Instance Name, check **Default**.
11. Accept **TYPICAL** as the Setup Type (default)
12. Under Services Accounts select:
    - o CUSTOMIZE
    - o USE THE LOCAL SYSTEM ACCOUNT
    - o AUTO START SERVICES
    - o SQL SERVER AGENT
    - o USE THE LOCAL SYSTEM ACOUNT
    - o AUTO START SERVICE – Check OK for the window that appears.
13. For the Authentication Mode Screen, select "mixed mode" and insert SA password (for this example password is left blank).
14. Set Collation Designator to Latin1_General and Check **Binary for Sort Order**.
15. Under the Network Libraries, deselect all choices except for NAMED PIPES.
16. Read the Start Copying Files screen and click **Next**.
17. Select PER SEAT as the licensing method and set 20 devices for E-Mail Instance.
18. A dialog box with the message "Setup is installing Microsoft Data Accessing Components (MDAC)" shows up.
19. When setup completes, reboot.

INSTALL SQL SERVER SERVICE PACK 2

1. Run **setup.bat**.
2. For Computer Name, select Local Computer.
3. Accept the license agreement.
4. For the Instance Name, accept the default.
5. Connect to Server using SQL Server System Administrator login. Enter sa as the password.
6. Complete setup and reboot the machine.

Special Notes if Installing Oracle:

- o Use UTF8 character set.
- o Select at least 20 for Concurrently Connected Users.

- Select Dedicated Server Mode.
- Set Maximum Datafiles to 700.
- Set Maximum Log Files to 70.
- Set Maximum Log Members to 5.
- Check Enable Archive Log.
- Set Log Archive Buffers to 5.

Step 38. Install Collaboration Database

- Run setup from the Oracle Media.
- Click **Next** on the Welcome Screen.
- Accept the default file locations and click **Next**.
- Accept the default Oracle8i 8.1.7.0.0 in the Available Products screen and click **Next**.
- In the Installation Types screen, accept Typical (default) and click **Next**.
- In the Database Identification screen, the Global Database Name of "Default" automatically fills in the SID field. Click **Next**.
- In the Summary Screen, click **Next**.

The Install completes. Perform the following steps:

1. Close the Oracle Installer.
2. To create the Oracle Database for Collaboration Server, click **Start > Programs > Oracle-OraHome81 > Database > Administration > Database Configuration Assistant**.
3. In the Welcome screen, select "Create a Database" and click **Next**.
4. In the Select Database Type screen, select Customer and click **Next**.
5. In the Select Primary Application Type screen, select Multipurpose and click **Next**.
6. In the Concurrently Connected Users screen, accept the default and click **Next**.
7. In the Server Mode screen, select the Shared Server Mode and click **Next**.
8. In the Options screen, accept default and click **Next**.
9. In the Database Identifier screen, name the database "ccsdb". The SID automatically fills in. Click on **Change Character Set**. Set both Character Set and National Character Set to "UTF8". Click **OK** and **Next**.
10. In the Password screen, enter and confirm the password (example: Cisco) and click **Next**.
11. In the Control File Information screen, accept defaults and click **Next**.
12. In the System Table Information screen, accept defaults and click **Next**.
13. In the Redo Log File Information screen, accept defaults and click **Next**.
14. In the Logging Information screen, accept defaults and click **Next**.
15. In the Server Information screen, accept defaults and click **Next**.
16. In the Advanced Server Information screen, accept defaults and click **Next**.
17. In the SGA Information screen, accept defaults and click **Next**.
18. In the Trace File Directory screen, accept defaults and click **Next**.
19. In the Create a Database Now screen, click **Finish**. Click **Yes** on the Alert window to proceed.
20. When you receive the message that Database Creation is completed, click **OK**.
21. To create the tablespace and user in the Oracle Database for the Collaboration Server, click **Start > Programs > Oracle-OraHome81 > Database Administration > SQLPlus Worksheet**.

22. In the Enterprise Manager Login dialog box, select Connect Directly to a Database.
    - Enter “internal” for the Username.
    - Enter “Cisco” for the Password.
    - Enter the <name of database> for the Service. Example “ccsdb”.
    - For the Connect As screen, select SYSDBA from the menu. Click **OK**.
23. In the SQL Plus Worksheet Application, delete the highlighted text. Copy the text below into this window. The text is one line, and that a semicolon indicates a new line.

The following names are used on the Collaboration Server:

- Tablespace name – ccstable
- Datafile name – ccsdata
- Username – ccsuser
- Password – Cisco

```
CREATE TABLESPACE <Collaboration DB tablespacename> DATAFILE '<Collaboration DB datafilename>' SIZE 30M;

CREATE USER <Collaboration DB username> IDENTIFIED BY <Collaboration DB password> DEFAULT TABLESPACE <Collaboration DB tablespacename>;

COMMIT;
```

Click on the **Execute** icon

```
GRANT CONNECT, RESOURCE TO <Collaboration DB username>;

COMMIT;
```

Click on the **Execute** icon

Click on **File > Exit** to finish

Special Notes if Installing SQL:

- Install SQL2000 using the typical install.
- Use the Enterprise Manager to create a database.
- Use the Enterprise Manager to create a user.
- Assign that user to the database created for CCS and assign these rights:
    - db_owner
    - db_accessadmin
    - db_securityadmin
    - db_ddladmin
    - db_backupoperator
    - db_datareader
    - db_datawriter

Step 39. Install ICM Software on Loggers

You can now load the ICM Software Modules on the individual Servers (see System Design Specification).

When ICM Setup loads the ICM Logger and Admin Workstation software, it creates specific domain level groups and accounts in the ICM domain it is loaded into.

To run the ICM Setup for the Loggers, Administrative Workstations and CallRouters, you must be logged in with a Domain Admin level account. You can perform a Peripheral Gateway setup with a user account that has “admin” rights on the server itself.

Cisco provides specific hot fixes to major releases and service packs of the ICM software to address service-impacting issues. You can download hot fixes from Cisco's Web site (http://www.cisco.com/) and apply them after the initial load of the software. The hot fix installation process only applies fixes required for the specific software modules (CallRouter, Logger, type of PG, etc.).

Step 40. Create Logger Databases

After running the ICM Logger setup program and applying all hot fixes, you need to use the ICMDBA tool to finish the SQL Server configuration and build the actual ICM databases on the machine. You also use this tool on the Admin Workstation to create the Historical Database Server database (HDS).

For each Logger:

1. Click **Start > Run**, enter ICMDBA and click **OK**.
2. Click on the Server Name you want to change (Logger A or Logger B).
3. Select Create from the Database menu.
4. The ICMDBA question prompts you to configure SQL Server. Click **Yes**.
5. On the Configure Logger Screen, if the current value does not equal the recommended value, check the Configuration Box and verify that the new value equals the recommended value. Click **OK**.
6. Click **Yes** to continue. SQL Server stops and restarts.
7. Create the Database Screen. Select Region.
8. Click Add. Enter Data for the Type.
9. Highlight the D drive. –The size should be 70% of the available disk space if the Logger is for one customer instance only. If more than one instance resides on the Loggers, determine database size with a customer. Click **OK**.
10. Click **Add**. Log is the type.
11. Highlight the D drive and set the size to 200MB (do not make the log device larger than 500MB). Click **OK**.
12. Click **Create**. Click Start to Create Database. When the database is successfully completed, click **OK** and Close the database window.
13. Close ICMDBA.
14. Click **START > Programs > Microsoft SQL Server > Enterprise Manager**.
15. Expand the Server Tree and Highlight the Databases Folder under the Server name.
16. Double-click on the ICM Database in the right panel. You are now in the <cus_sideA> Properties Window.
17. On the Data Files Tab:
    - Check Autogrow and set the File Growth to 10%.
    - Set the Maximum File Size to [use the following calculation].

      {80% of free disk space}/{number of ICM database files on this disk}+{database file current size}

      Example: {10GB * .80}/{1}+{25GB}=33GB
18. On the Transaction Log Tab, uncheck Autogrow and click **OK**.

Step 41. Install ICM Software on CallRouters

ICM Nodes Forms, which identify all values and non-default settings used in setup, are created in the Planning phase of a deployment program and reside in the ICM System Design Specification.

Cisco provides specific hot fixes to major releases and service packs of the ICM software to address service-impacting issues. You can download hot fixes from Cisco's web site (http://www.cisco.com/).

Apply the hot fixes after the initial load of the software. The hot fix installation process only applies fixes required for the specific software module (CallRouter, Logger, type of PG, etc.).

Step 42. Start Logger and Router Services

The ICM is set up with an empty database. You need to add configuration information to complete the basic testing components. In order to add configuration data, the Central Controller and Admin Workstation(s) must be running. The ICM software loads an "ICM Service Control" tool on the desktop of each server used to control the services loaded on that machine. Start the services in the following order:

- Logger A
- CallRouter A
- CallRouter B
- Logger B

Each service starts several process windows on the task bar of the local machine, each one an ICM program associated with the service. As each node starts up, it looks for the other server components and attempts to register with them. If you completed the ICM setup and network testing successfully, no major errors should occur.

Verify that the ICM Processes have no errors:

- CallRouters:
  - Router: UP and synchronized with peer
  - Ccagent: [is in service, but not connected to any peripheral gateways]
  - Rtsvr: [no connectivity to AW at this time]
- Loggers:
  - Logger: connected to its respective database and synchronized with peer – MDS is in service
  - Replication: [no connectivity to AW HDS at this time]
  - Campaign Manager: [see errors, no Blended Agent Dialer is set up at this time]

Step 43. Install ICM Software on Admin Workstation

Complete Setup on all "Network" Admin Workstations (see System Design Specification). The CICM Instance Distributors are Setup on the NAM Domain AW machines. Thus, setup requests the Administrator credentials from the CICM domain before completing setup.

When setup completes, click **Start > Run**, enter ICMDBA and click **OK**. Expand the database to 500MB and the Log devices to 200MB.

Cisco provides specific hot fixes to major releases and service packs of the ICM software to address service-impacting issues. You can download hot fixes from Cisco's Web site (http://www.cisco.com/) and apply them after the initial load of the software. The hot fix installation process only applies fixes required for the specific software modules (CallRouter, Logger, type of PG, etc.).

Step 44. Expand AW Database

1. Click **Start > Run**, enter ICMDBA and click **OK**.
2. Expand Tree under the AW Hostname.
3. Highlight <cus_awdb>.
4. Select Expand from the Database menu.
5. Highlight C Drive.
6. Expand Data to 500MB. Click **OK**.

7. Click **Start** on Expand DB window. Click **OK**. Close the window when it is complete.
8. Select Expand from the Database menu.
9. Select Log (C drive is automatically highlighted).
10. Expand Log to 200MB. Click **OK**.
11. Click Start on Expand DB window. Click **OK**. Close when complete.
12. Close ICMDBA.
13. Click **Start > Programs > Microsoft SQL Server > Enterprise Manager**.
14. Expand Server Tree and Highlight the Databases Folder under the Server name.
15. Double-click on the ICM Database in the right panel. Now in <cus_awdb> Properties Window.
    - On the Data Files Tab
      - Check Autogrow and set File Growth to 10%
      - Set Maximum File Size to [use the following calculation]

      {80% of free disk space}/{number of ICM db files and aw logs on this disk}+{db file current size}

      example: {4GB * .80}/{2}+{.5GB}=2.1GB
    - On the Transaction Log Tab
      - Check Autogrow and set File Growth to 10%
      - Set the Maximum File Size to [use the following calculation]

      {80% of free disk space}/{number of ICM db files and aw logs on this disk}+{db file current size}

      Example: {4GB * .80}/{2}+{.2GB}=1.8GB

Step 45. Start AW (Distributor) Services

Start the Distributor Service within Cisco Service Control.

Verify that the ICM Processes have no errors:

- CallRouters:
  - Router: UP and synchronized with peer
  - Ccagent: [is in service but is not connected to any peripheral gateways]
  - Rtsvr: feed activated to AW
- Loggers:
  - Logger: connected to its respective database and synchronized with peer – MDS is in service
  - Campaign Manager: [you see errors – no Blended Agent Dialer is set up at this time]
- Admin Workstation:
  - Updateaw: displays “waiting for new work”
  - Iseman: listen thread waiting for client connection
  - Cms_jserver: unable to intitialize until the configuration is done
  - Cmsnode: shutdown in progress…terminating

Step 46. Configure NIC’s, Peripheral Gateways and Peripherals

Before you can turn up the ICM Services on the SS7 Gateways, NICs and Peripheral Gateways, you need to configure the ICM using the NIC and PG Explorer tools.

Refer to the ICM System Design Specification, Connection Parameters Section, ICM Configuration Manager, PG Logical Controller ID’s and Peripheral Controller ID’s Table. This table indicates the values and settings, which you must establish in the ICM Configuration and input during ICM setup of each

Peripheral Gateway node. In addition to establishing PG logical controller ID's and Peripheral ID's you must also configure the following the ICM Configuration tool:

- On Call Manager PG – Name for Agent Desk Settings
- On IPIVR PG – Name for Network Type 2 VRU (Also configure the Network VRU)
- Media Routing PG - Name for an additional Network Type 2 VRU (Network VRU must also be configured)

In order to properly run ICM Setup for the NICs and PG's, the Logical and Peripheral ID numbers need to be pre-planned as they are required data elements to complete the Setup program. The ICM automatically generates ID numbers from the Explorer tools, so you need to set them up in the Explorers in the exact order they were planned in the ICM System Design Specification.

If the ID numbers are not generated in the proper sequence, correct them in the Peripheral Gateway machines by re-running Setup locally. They must match what is in the ICM configuration database to the value in the PG's registry, or the ICM CallRouter rejects the connection request.

Additionally, if the customer plans to use agent level reporting, you need to set this up as well after the Peripheral is created in the ICM configuration database. Use the Agent Distribution Tool on the Admin Workstation to point the specific Peripheral (ACD that generates the agent stats) to the Admin Workstation's "Admin Site Name" for the AW that stores the real-time agent level reporting data. Also, you must set the Peripheral to enable "Agent Reporting" on the "Agent" tab in PG Explorer.

You must set up Agent Level Reporting for each peripheral and they can all point to a central AW/WebView server to allow for sharing of the stats. However, a peripheral can only point to one AW.

Step 47. Configure Multi-Media Nodes

Refer to ICM System Design Specification, Connection Parameters Section, ICM Configuration Manager, Media Routing Domains Table and Application Instance List Table.

1. Start ICM Configuration Manager
2. Step-by-step/Multimedia/Media Routing Domains
   - Add Single Session Chat Domain
   - Add Multi-Session Chat Domain
   - Add Blended Collaboration Domain
   - Add E-mail Domain
   - Confirm or add Voice Domain
3. Step-by-step/Multimedia/Application Instance
   - Add CCS instance
   - Add CEM instance

Step 48. Create and Configure CONAPI Connections

Refer to ICM System Design Specification, Connection Parameters Section, CMS Control.

1. Open ICM Program Group
2. Start CMS Control Tool
3. Application Tab
4. Application Connection
   - Add CCS connection – example: icmcusccs1
   - Add CEM connection – example: icmcuscem1

Step 49. Install ICM Software on Peripheral Gateways

Complete setup on all Peripheral Gateways (see System Design Specification).

Cisco provides specific hot fixes to major releases and service packs of the ICM software to address service-impacting issues. You can download hot fixes from Cisco's Web site (http://www.cisco.com/) and apply them after the initial load of the software. The hot fix installation process only applies fixes required for the specific software modules (CallRouter, Logger, type of PG, etc.).

Step 50. Install ICM Software for CTI Server

Complete Setup from ICM media (see System Design Specification).

Step 51. Install CTIOS Server

First you must create an ODBC connection – see *CTI OS System Manager Guide*

- The connection is between CTIOS Server and any ICM database with agent information. That connection should be to the Logger database.
- Make a note of ODBC filename that is created, which will be used during CTI OS Server Setup.

Complete Setup on the CTIOS Server from the respective ICM Node Form, which identifies all values and non-default settings used in setup.

You can download hot fixes from Cisco's Web site (http://www.cisco.com/). Apply them after the initial load of the software. The hot fix installation process applies fixes required for the specific software module (CallRouter, Logger, type of PG, etc.).

Step 52. Start PG and CTI and CTIOS Services

Once the ICM configuration database is set up with the appropriate peripherals, you can start the PG services using the Cisco Service Control application on the desktop of the PG. If the local peripheral (ACD/IVR/etc.) is not available to connect to the PG, "disable" it in the PG setup. Test to ensure that the PG communications layer is set up properly and that it can communicate to the CallRouters and obtain configuration information.

For this example, the Blended Agent Dialer, Media Blender and E-Mail Manager PIM's are enabled on the MR PG. The Call Manager and IPIVR PIM's on the Generic PG remain disabled until the Call Manager and IPIVR peripherals are available during the Implementation phase of the project.

Verify that the ICM Processes have no errors:

- CallRouters:
  - Router: UP and synchronized with peer
  - Ccagent: connected to all configured peripheral gateways
  - Rtsvr: feed activated to AW
- Loggers:
  - Logger: connected to its respective database and synchronized with peer – MDS is inservice
  - Campaign Manager: [see errors, no Blended Agent Dialer is setup at this time]
- Admin Workstation:
  - Updateaw: displays "waiting for new work"
  - Iseman: listen thread waiting for client connection
  - Cms_jserver: cmsnode.exe process is active – CEM and CCS connection down
  - Cmsnode: initialization complete
- Peripheral Gateways:
  - Generic (IPCC & VRU) PG
    - Mdsproc: in service
    - Pgagent: in service and active to one side of central controller
    - [peripheral] PIMs: disabled on node form – PIM windows do not exist
  - MR PG
    - Mdsproc: in service

        - Pgagent: in service and active to one side of central controller
        - [peripheral] PIMs: enabled in setup – and therefore, is cycling between activating and idle
    - CTI Server:
        - Cg[#]ctisvr: active with configured port number
    - CTIOS Server:
        - Ctios Server: active with configured port number – driver online
        - Ctidriver: active

Step 53. Install and Start Blended Agent Dialer

1. Configure Blended Agent Dialer in the ICM Configuration Manager. Open **Configuration Manager** > **Blended Agent** > **Blended Agent Dialer**
2. Retrieve and click **ADD**.
    - Enter the Dialer Name. For example: ba1_dialer
    - Check the "enable" box
    - Enter the Computer Name where Blended Agent Dialer is installed. For example: icmcusba1
    - From the ICM Peripheral Name menu, select the name of the Blended Agent PIM on the MR PG. For example: BA1.
    - Enter the data in the local area code field even if this will be reconfigured later for the production environment. Click save and close.
3. Validate that the Blended Agent option is enabled on Logger.
4. Create BA Database on Logger A - On Logger A run ICMDBA
    - Highlight Logger A, right click and select "create" from the database menu.
    - On the Create Database Screen:
        - The Database type is BA_SideA
        - Add a Device (see Cisco ICM Software Blended Agent Setup and Configuration Guide for database estimation information)
            - Click Data. Highlight the D drive. Enter 500MB and click **OK**.
            - For the Log, highlight the D drive, enter 100MB and click **OK**.
        - Click Create > Start and when finished click **OK** and Close. Close ICMDBA.
5. Complete the setup on Blended Agent Dialer Server from the ICM media for the respective ICM Node Form, which identifies all values and non-default settings to be used in setup.
6. After reboot, start the Dialer process.

Verify that the ICM Processes have no errors:

- CallRouters:
    - Router: running and synchronized with its peer
    - Ccagent: connected to all configured peripheral gateways
    - Rtsvr: the feed is activated to AW
- Loggers:
    - Logger: connected to its respective database and synchronized with the peer. MDS is in service.
    - CampaignManager: the process is running on the logger and connected to the Blended Agent Dialer
- Admin Workstation:
    - Updateaw: displays "waiting for new work"
    - Iseman: listen thread waiting for client connection
    - Cms_jserver: **cmsnode.exe** process is active
    - Cmsnode: initialization complete
- Peripheral Gateways:
    - Generic (IPCC & VRU) PG
        - Mdsproc: in service

        - Pgagent: in service and active to one side of central controller
        - [peripheral] PIMs: disabled on node form – PIM windows do not exist
    - MR PG
        - Mdsproc: in service
        - Pgagent: in service and active to one side of central controller
        - [peripheral] PIMs: enabled in setup – Blended Agent PIM is now ACTIVE – E-Mail Manager and Media Blender PIM's are still cycling.
- CTI Server:
    - Cg[#]ctisvr: active with configured port number
- CTIOS Server:
    - Ctios Server: active with configured port number – driver online
    - Ctidriver: active
- Blended Agent Dialer:
    - Blended Agent Dialer: EMT connection established and configured.

Step 54. Install and Start E-Mail Manager Server

Install E-Mail Manager Core Server

1. Run setup from Cisco E-Mail Manager Install Media
2. For the Welcome and click Next.
3. Select the Component Screen. Select CEM.
4. Accept the defaults on all file location screens.
5. For the Information screen click **Next** and the install of 3rd Party Component(s) now completes.
6. For the Information Dialog Box, the installer now calls the CEM Services Installer. Click **OK**.
7. On the Welcome screen, click **Next**.
8. Accept the defaults on the file location.
9. Select a Program Folder, accept the defaults and click **Next**.
10. On the Ready to Copy files screen, click **Next**.
11. Files now copy.
12. On the Information Dialog Box, the setup launches the Configuration Utility. Click **OK**.
13. Create a New Instance Dialog Box. Refer to the ICM System Design document, Connection Parameters Section, Application Instance Table to enter the following:
    - E-Mail Manager Instance Name
14. Enter the Login Name "root" (see the *Cisco E-Mail Manager Installation and Configuration Guide* for more information).
15. Enter the Password "pass" (see the *Cisco E-Mail Manager Installation and Configuration Guide* for more information).
16. Click **Yes** for the Dialog Box asking to install the license file.
    - Go to the URL printed on the front of the CMB Install Media.
    - Enter the Product Code from the CD and an e-mail address and you are e-mailed a FlexLM License File.
    - Copy the License File to a floppy disk.
    - Insert the floppy disk into the E-Mail Manager Server.
17. In the Locate and Select CEM License File Dialog Box, navigate to the A drive.
18. Highlight the License File and click on **Load License File**.
19. For the Configuration Utility, see the Cisco E-Mail Manager Installation and Configuration Guide
20. On the General Tab, accept the defaults.
21. On the Primary database Tab:

- Select a Database: SQL 2000
- Enter the following database information:
  - For Database Name enter “cemdb”
  - For Login name enter “cemuser”
  - For Login password enter “cisco”
  - For Confirm password enter “cisco”
  - For Database Hostname enter the name of the E-Mail Manager database – icmcuscemdb1
  - For Database port enter “1433”
- Run now
- The Database Administration Login Dialog Box appears:
  - Enter the database Admin Login Name (sa).
  - Enter the database Admin password (leave blank).
  - Login.
- The Database Files Dialog Box appears.
  - Enter the data and log sizes.
    - Enter the database file size (minimum 500MB)
    - Enter the log file size (minimum 300MB)

    Note: Sizing is based on information gathered during Application Discovery Phase based on expected number of e-mails received on a daily basis, size of the average e-mail, average size of attachments (if any), and the length of time e-mails should be preserved on the database.
- Click **OK** to create the Schema.
- Database Table Creation dialog box appears –click **OK**.

Follow these steps to complete the procedure

1. On the Logging Tab, accept the defaults.
2. On the Advanced Tab, accept the defaults.
3. On the HTTPD Tab, change the HTTPD port to 80.
4. On the LAMBDA Database Tab, make note of database name, as you use it when installing the Agent UI Server. For example: cemdbp.
5. Choose to run the script now.
6. Enter the Login and Password: login name (sa) and password (leave blank)
7. The Database Files dialog box appears:
   - Enter the data and log sizes
   - Enter the Database file size (minimum 500MB)
   - Enter the Log file size (minimum 300MB)

   Note: Sizing is based on information gathered during Application Discovery Phase based on expected number of e-mails received on a daily basis, size of the average e-mail, average size of attachments (if any), and the length of time e-mails should be preserved on the database.
   - For the Successful Creation Database Creation dialog box, click **OK**.
8. On the LAMBDA Tab, accept the defaults unless the information you gathered indicates that other values should be entered here.
9. On the CIR database Tab, make note of the database and username. You use it when installing the Agent UI Server. For example: the database is cemdbc and the username is cemuserc
10. Choose to run the script now.
11. Enter your Login and Password. The login name is sa, leave the password blank.

12. The Database Files Dialog Box appears. Enter the data and log sizes:
    - Enter the Database file size (minimum 500MB)
    - Enter the Log file size (minimum 300MB)

    Note: Sizing is based on information gathered during the Application Discovery Phase based on the expected number of e-mails received on a daily basis, size of the average e-mail, average size of attachments (if any), and the length of time e-mails are preserved on the database.
13. Click **OK** on the Successful Creation Database Creation dialog box.
14. Click **OK** for the Successful Grant Access to CIR dialog box.
15. Click **OK** for the Successful Database Table dialog box.
16. On the CIR Tab, enter the Webview Server Name. For example: icmcusag2. Accept all other defaults.
17. On the ICM Tab, refer to the ICM System Design document, Connection Parameters Section, ICM Configuration Manager, Media Routing Domains Table and Application Instance List Table. You also need to refer to (in this same section) CMS Control, CONAPI Connections-ICM/E-Mail Manager Table.

    [example]
    - ICM Enterprise Name: CEM
    - ICM Application Key: cisco
    - ICM Description: mmcallcenter
    - Media Routing Domain ID: 5003
    - ICM Administration connection name: ConnName1 (use this default)
    - Service Name on E-Mail Manager Server: CEM
    - Registry Port on E-Mail Manager Server: 1099
    - ICM Distributor AW Service Name: ICM
    - ICM Distributor AW Registry Port: 1099
    - ICM Distributor AW Hostname: icmcusaw1
18. Click **Finish**. For the confirmation dialog box, click **OK**.
19. When the setup completes, click– **Finish**.

Install CEM Agent UI/API/Webview Server

1. Run the setup from Cisco E-Mail Manager Install Media.
2. Welcome and click **Next**.
3. Select the Component Screen, and select the UI Server and Webview Standalone.
4. Accept the defaults on all file location screens.
5. Click **Next**.I Install of the 3rd Party Component(s) now completes.
6. For the Information dialog box, The installer now calls the CEM UI Server Installer. Click **OK**.
7. For the Question dialog box, click **Yes**.
8. For the UI Install Shield Wizard, click **Next**.
9. Select the Instance that was created on Core Server. For example: CEM. Click **Next**.
10. Accept the default for directory location.
11. For the Tserver Properties, click **Next**.
12. For the UI Server Destination Location, accept the default and click **Next**.
13. The application installs.
14. On the Question dialog box, click **Yes** to restart IIS services.
15. When the Install Shield Wizard Complete screen appears, click **Finish**.

16. For the Information dialog box, click OK and the installer calls the Webview Installer.
17. On the Install Shield Wizard for Webview, click **Next**.
18. Select English for the Language and click **Next**.
19. For CIR Connection Information:
    - Select the database type and version. Forexample: MS SQL Server 2000.
    - Enter the Database Server Hostname. For example: icmcuscemdb1.
    - Enter the Database Name. For example: cemdbc.
    - Enter the Port. For example: 1433.
    - Enter the Username. For example: cemuserc.
    - Enter the Password. For example: Cisco.
    - Click **Next**.
20. Click **Next** for the Application and Instance to Report Against.
21. Select the Installation Drive (make a note of the target directory). For example: C:\CEM. Click **Next**.
22. For the UI Server Authentication Information:
    - Enter the UI Server Hostname. For example: icmcusag1.
    - Select the Authentication Protocol. For example: HTTP.
    - Enter the Port. For example: 80.
    - Click **Next**.
23. During setup, the Status screen displays and the application installs.
24. Confirm that reporting was added by click **OK** on the dialog box. Elect whether or not to add another application instance.
25. When the Install Shield Wizard completes, click **Yes** to restart the machine. Click **Finish** and the system reboots.
26. Click **Start > Programs > New Atlanta > ServletExec 4.1 ISAPI > ServletExec Admin**. The Internet Explorer browser opens to the ServletExec Admin page.
    - In the left frame, click on Settings under the Virtual Machine.
    - In the right frame, set the minimum heap size. For example: with 250 agents set to 81902.
    - In the right frame, set the maximum heap size. For example: with 250 agents set 81902.
    - In right frame, click **Submit**.
    - Close the Browser.

Install CEM Agent UI/API #2 Server

1. Run setup from Cisco E-Mail Manager Install Media
2. On the Welcome screen, click **Next**.
3. Select the Component screen. Select the UI Server.
4. Accept the defaults on all file location screens.
5. For the Information screen, click **Next**. Install of 3rd Party Component(s) completes.
6. If necessary, click OK for the Information dialog box. The installer now calls the CEM UI Server Installer. Click **OK**.
7. On the Question dialog box. Click **Yes**.
8. Click Next for the UI Install Shield Wizard.
9. Select the Instance created on the Core Server. For example: CEM. Click **Next**.
10. Accept the default for directory location.

11. Click Next for Tserver Properties.
12. Accept the default for the UI Server Destination Location and click **Next**.
13. The application installs.
14. Click Yes for the Question dialog box to restart IIS services.
15. Click Finish when the Install Shield Wizard completes. Reboot the machine.
16. Click **Start > Programs > New Atlanta > ServletExec 4.1 ISAPI > ServletExec Admin**.
20. Internet Explorer Browser Opens to the ServletExec Admin page.
21. In the left frame, click on **Settings** under Virtual Machine.
22. In the right frame, set the minimum heap size. For example: with 250 agents set to 81902.
23. In the right frame set maximum heap size. For example: with 250 agents set 81902.
24. In the right frame, click **Submit**.
25. Close the Browser.

Start E-Mail Manager Servers

1. Use the Windows Services and start the CEM database.
2. Under CEM Core Server, two new services appear: Cisco E-Mail Manager Core Server and Cisco E-Mail Manager CEM.
   - Right-click the Core Server and select **Properties**.
     - On the Login Tab, confirm that Allow Service to Interact with Desktop is checked
     - On the General Tab, click Start and click **OK**.
   - Right-click CEM and select **Properties**.
     - On the Login Tab, confirm that Allow Service to Interact with Desktop is checked.
     - On the General Tab, click Start and then click **OK**.
3. Start the World Wide Web Publishing Services on UI Servers (this starts Webview and UI Servers).

Verify that the ICM Processes have no errors:

- CallRouters:
  - Router: running and synchronized with peer
  - Ccagent: connected to all configured peripheral gateways
  - Rtsvr: feed activated to AW
- Loggers:
  - Logger: connected to its respective database and synchronized with the peer. The MDS is in service
  - CampaignManager: the process is up on the logger and connected to Blended Agent Dialer
- Admin Workstation:
  - Updateaw: displays “waiting for new work”
  - Iseman: the listen thread is waiting for a client connection
  - Cms_jserver: the **cmsnode.exe** process is active. The event helper message shows CEM “up”; CCS “down”
  - Cmsnode: initialization complete
- Peripheral Gateways:
  - Generic (IPCC & VRU) PG
    - Mdsproc: inservice
    - Pgagent: inservice and active to one side of central controller
    - [peripheral] PIMs: disabled on node form – PIM windows do not exist
  - MR PG
    - Mdsproc: inservice
    - Pgagent: is in service and active to one side of the central controller

        - [peripheral] PIMs: enabled in setup. The BA PIM is now active. E-Mail Manager PIM is active, but the Media Blender PIM is still cycling
- CTI Server:
    - Cg[#]ctisvr: active with configured port number
- CTIOS Server:
    - Ctios Server: active with configured port number. The driver is online
    - Ctidriver: active
- BA Dialer:
    - BA Dialer: EMT connection established and configuration received
- E-Mail Manager Core:
    - Rules engine process: inbasket is authenticated

Step 55. Install and Start Collaboration Server

1. Run setup from the CCS install media.
2. Click **Next** on the Welcome screen.
3. Click **Next** on the License screen.
4. Enter the user information and click **Next**.
5. Accept the default for the destination location and click **Next**.
6. Accept the default for the Custom Content Directory and click **Next**.
7. Enter the Customer Name and click **Next**.
8. Click **Next** for the ServletExec Install Shield wizard.
9. Click **Next** on the License screen.
10. Click **Next** for the Information screen.
11. Accept the defaults and click **Next** for the destination location.
12. Click **OK** for the Warning dialog box.
13. Click **Finish**.
14. Cisco Collaboration Server 6.0 Java Installer indicates that the install is complete. Close the window.
15. Click Finish.
16. Install the Oracle JDBC driver. Obtain the latest Oracle JDBC Driver from Oracle Install Media or Oracle Web site.
17. Copy the Oracle JDBC driver to **C:\Cisco_CS\servlet directory**.

    Note: Leave the JDBC driver zipped.
18. Install the FlexLM License. Go to the URL printed on the front of the CCS Install Media.
19. Enter the Product Code from the CD and an e-mail address and you are e-mailed a FlexLM License file.
20. Copy the license file to a floppy disk.
21. Insert the floppy disk into the Cisco Collaboration Server.
22. Copy the file to **C:\Cisco_CS\license** directory.

    Note: Do not reboot the server before the license is in this directory.
23. Reboot the server. After the server reboots, launch the browser.
24. Type in the following URL: http:\\icmcusccs1\admin and Return.
25. Cisco Collaboration Server Admin login window. The login name is admin, the password is Password (these are defaults, and case-sensitive).
26. Create Database Connections:
    - For the Database Setup wizard, click **Next**.
    - Select the database type. For example: Oracle 8/8i. Click **Next**.

- Click **Next** to confirm the JDBC driver.
- For Database Connection Data:
  - Enter the Host: <collab db>. For example: icmcusdb1.
  - Enter the Port. The default is 1521 (default).
  - Enter the SID: <from Oracle install on Collaboration database>. For example: CCSDB.
  - Enter the Database Login Name: <from Oracle install on Collaboration database>. For example: ccsuser.
  - Enter the Password: <from Oracle install on Collaboration database>. For example: Cisco.
  - Verify that the password is correct: <from Oracle install on Collaboration database>. For example: Cisco.
  - Click **NEXT**.
- Verfy the Connection Settings and click **Apply**.
- On next screen, click **Finish** to setup the database and create schema.
- You may get a security warning dialog box asking if you want to install the database utilities applet. Check “always trust content from Cisco Systems” and click **Yes**.

The schema is then created.

1. In the left frame, select “Server Setup\Show”.
2. Click **OK** for the dialog box concerning the Admin Password change.
3. In the right frame (top), click View\Change.
4. Enter the new admin password (example: ccsadmin).
5. Enter the Collaboration Server Application Instance Name (refer to ICM System Design Doc, Connection Parameters section, ICM Configuration Manager\Application Instance List table. For example: CCS).
6. Click **Submit**.
7. In the left frame, select **Server Setup > Integrate with ICM**.
8. The wizard appears in the right frame. Click the Integrate with ICM Web button.
9. Click **OK** on the dialog box.
10. Click on the underlined Application Instance link. On the new/second browser screen, enter the Application Instance Name. Enter the Application Key (refer to ICM System Design Doc, Connection Parameters section, ICM Configuration Manager\Application Instance List table. For example: cisco).
11. Click **Submit**.
12. Click **OK** on the dialog box.
13. Close the second browser.
14. Click on the underlined ICM Administration Connection link. On the new/second browser screen, enter the CONAPI connection information (refer to ICM System Design Doc, Connection Parameters section, CMS Control\CONAPI Connections-ICM/Collaboration table). Here are some examples:
    - ICM Admin connection name: ICMConn1
    - Registry port on Collab Server: 1099
    - Connection port on Collab Server: 1100
    - Service name on Collab Server: CCS
    - ICM Distributor AW host name: icmcusaw1
    - Registry port on ICM Distributor AW: 1099
    - Service Name on ICM Distributor AW: ICM

15. Click Submit.
16. Close the second browser.
17. Click **Apply**.
18. Close the browser and reboot the Collaboration Server. After the server reboots, launch the browser.
19. Before proceeding with the next steps, validate that the Distributor associated with the ICM Connection is started and that cms_jserver and cmsnode are running.
20. Type in the following URL: http:\\icmcusccs1\admin and Return.
21. Cisco Collaboration Server Admin Login Window. Enter the login name and password.
22. In the left frame, select **Server Setup > Integrate with ICM**.
23. Click on the Media Routing Domains link. On the new/second browser screen, select from the menus the media routing domains that correspond to the media class listed to the left.
24. Click on **Submit**.
25. Click **OK** on the dialog box.
26. Close the second browser.
27. Click on the Media Blender Connection link. On the new/second browser screen, select and enter Media Blender connection data:

    [example]

    - Media Blender Connection Name: <arbitrary> example: cmb1
    - Registry Port on Collaboration Server: 1099
    - Connection Port on Collaboration Server: 1100
    - Collaboration Server Password: cisco (must then verify)
    - Media Blender hostname: icmcuscmb1
    - Registry Port on Media Blender: 1099
    - Media Blender Password: <arbitrary> cisco (must verify)
    - Make sure that Disable auto connect to Media Blender is checked
    - Close the second browser
28. Click on the ICM Peripherals link. On the new/second browser screen, check the peripherals associated with agents and select the appropriate Media Blender connection from the menu.
29. Click **Enable**.
30. Click **OK** on the dialog box.
31. Close the second browser.
32. Click **Next** to continue with the ICM Integration.
33. Check both the Collaboration Server descriptions and click **Finish**.
34. In the left frame, select **Server Setup > Queues > Create**.
    - Create a Queue applicable to your installation. In the example of IPCC only “ICM QUEUE” is required.
    - Click **Next**.
    - Insert the Queue Name. For example: ICM.
    - Select the appropriate Media Blender connection from the menu. For example: cmb1.
    - Select the backup Media Blender connection from the menu. For example: <leave blank>.
35. Click **Finish**. Close the Browser and reboot the server.
36. From the Collaboration Server, copy the following 2 files onto a floppy disk:
    - **Cmb1.properties**, locatecd in: **C:\Cisco_CS\servlet\properties\cmb\cmb1**
    - **Collaboration.properties**, located in **C:\Cisco_CS\servlet\properties\cmb\Blender**

Step 56. Install and Start Media Blender Server

1. Run setup from the CMB Install Media.
2. On the Welcome screen, click **Next**.
3. Enter the company user information.
4. Accept the default destination location and click **Next**. Allow the installation to complete.
5. For the Servlet Exec 4.1.1 ISAPI setup, click **Next**.
6. Click **Yes** for the License Agreement.
7. Click **Next** at the Information screen.
8. Accept the defaults for the destination location and click **Next**.
9. As files are being installed, you receive an IIS warning. Click **OK**.
10. Click Finish for the Install Shield wizard.
11. As the installation continues, the World Wide Web process starts.
12. When you see "Installation Completed" close the wizard.
13. Several command prompt process windows appear and the installation completes.
14. Do not reboot, you must install the license first (see below).

To Install the FlexLM License

1. Go to the URL printed on the front of the CMB Install Media.
2. Enter the Product Code from the CD and an e-mail address and you are e-mailed a FlexLM license file.
3. Copy the file into **C:\CiscoMB\license**.
4. Reboot the server.
5. Rename the following file:
   - **Collaboration.properties**, from the **C:\CiscoMB\servlet\Properties\Blender** directory to **collaboration.properties.old**.
6. Take the files that were copied in the final step of the Collaboration Server Installation and copy as follows:
   - Put the **cmb1.properties** file into the **C:\CiscoMB\servlet\Properties** directory.
   - Put the **collaboration.properties** file into the **C:\CiscoMB\servlet\Properties\Blender** directory.
7. Open the **ACD.ciscocti.properties** (located in the **C:\CiscoMB\servlet\Properties\Blender** directory) with the text editor and edit the following values:

   Note: These setting vary according to peripheral types.

   [example]
   - Uncomment (remove #) "ctistrategy=AgentReserved"
   - Comment (insert # in front of line) "phantompool=phamtoms.properties"
   - Comment (insert # in front of line) "physicallocationfile=phantomagents.properties"
   - Comment (insert # in front of line) "passwordfile=phantompasswords.properties"
   - Comment (insert # in front of line) "agentsfile=agentmapping.properties"
   - Comment (insert # in front of line) "skilltable=skills.properties"
   - Uncomment (remove #) "peripheral.type=IPCC"
   - Enter peripheral id of the call manager PG – peripheral.id=5000
   - Enter peripheral.hostname= <hostname of CTI Server> icmcuspg1a

- Enter peripheral.hostport=42027
- Enter peripheral.hostname2=icmcuspg1b (be sure to uncomment)
- Enter peipheral.hostport2=43027 (be sure to uncomment)
- SAVE and CLOSE file

8. Open the **blender.properties** file (from the directory **C:\CiscoMB\servlet\Properties\Blender**) with a text editor and make the following edits:

   Note: these setting vary according to peripheral types.

   [example]

   - Uncomment "service1=service.fwgw.properties"

9. Open the firewallgatewayFG.properties file with a text editor (located in the **C:\CiscoMB\servlet\Properties** directory) and make the following edits:

   Note: These setting vary according to whether or not you have duplex PG's.

   [example]

10. Replace <connectionname> (appears throughout) with the name of the connection to Media Blender that you created on the collaboration server during the Integrate with ICM steps. For example: cmb1.
11. Enter the Primary and Secondary CTI Server hostnames, where indicated by <primaryhostname> and <backuphostname>.
12. Enter the Primary and Secondary CTI Server ports, where indicated by <primaryserverport> and <backupserverport>.
13. Save and Close.

To Start Media Blender:

1. Open the Browser and enter the URL **http:\\<media blender hostname>**.
2. For the user name, enter Administrator (with capital A).
3. For the password, enter <Win2K Admin login password>.
4. Click on the Server Administration link.
5. In the left frame, click on **Media Blender > Server > Start > Shutdown**.
6. In the right frame, click Start.
7. In the left frame, select **Media Blender > Service > Firewall Gateway > Start > Stop**.
8. In the right frame, click **Start**.

Verify that these ICM Processes have no errors:

- CallRouters:
  - Router: running and synchronized with its peer
  - Ccagent: connected to all configured peripheral gateways
  - Rtsvr: feed activated to the AW
- Loggers:
  - Logger: connected to its respective database and synchronized with its peer. MDS is in service
  - CampaignManager: the process is running on the logger and connected to the Blended Agent Dialer.
- Admin Workstation:
  - Updateaw: Displays "waiting for new work"
  - Iseman: the listen thread is waiting for a client connection
  - Cms_jserver: the **cmsnode.exe** process is active. The event helper message shows CCS and CEM running.
  - Cmsnode: the initialization is complete
- Peripheral Gateways:
  - Generic (IPCC & VRU) PG
    - Mdsproc: in service

        - Pgagent: in service and active to one side of central controller
        - [peripheral] PIMs: disabled on node form. PIM windows do not exist
    - MR PG
        - Mdsproc: in service
        - Pgagent: in service and active to one side of the central controller
        - [peripheral] PIMs: enabled in setup. The Blended Agent PIM is now ACTIVE. E-Mail Manager PIM is ACTIVE and the Media Blender PIM is ACTIVE.
- CTI Server:
    - Cg[#]ctisvr: active with configured port number
- CTIOS Server:
    - Ctios Server: active with configured port number. The driver is online
    - Ctidriver: active
- Blended Agent Dialer:
    - Blended Agent Dialer: EMT connection is established and configuration received
- E-Mail Manager Core:
    - Rules engine process: inbasket is authenticated
- Collaboration Server:
    - Admin UI: under Collaboration Server > Server Setup > Connections\Monitor, all services have an UP status.
- Media Blender:
    - Admin UI: under Media Blender > Server > Startup Shutdown. Media Blender has been running for <time>.
    - Admin UI: under Media Blender > Services > Firewall Gateway > Monitor, all gateway stubs have a RUN status.

Staging Tasks Customer AW Domain

Step No.	Task
57.	Install 1st Customer AW as Forest Root Domain Controller/DNS Server
58.	Configure DNS Server on AW Forest Root Domain Controller
59.	Configure Active Directory Sites
60.	Assign Global Catalog and FSMO Roles and Configure Time Source
61.	Configure Trust Relationships
62.	Join Standalone Servers to Domain
63.	Complete IP Configuration and Connectivity Testing
64.	Install Infomaker on AW's
65.	Install SQL Server AW's
66.	Install Webview 3rd Party Software
67.	Install ICM Software on Admin Workstations
68.	Expand AW Database
69.	Create HDS Databases
70.	Start AW (Distributor) Services

Step 57. Install 1st Customer AW as Forest Root Domain Controller/DNS Server

1. Click **Start > Run**, enter DCPROMO and click **OK**. The Active Directory Installation wizard opens.
2. Under "Domain Controller Type," select "Domain Controller for a New Domain." The "Create Tree or Child Domain" screen appears.
3. Select "Create a new Domain Tree." The "Create or Join Forest" screen appears.
4. Select "Create a New Forest of Domain Trees."
5. On "New Domain Name" screen, type in the full DNS name for the new domain.
6. On the "NetBIOS Domain Name" screen, type in the NetBIOS name.
7. Accept Database and Log Locations defaults.
8. Accept the Shared System Volume default. You receive an AD warning that the wizard cannot contact DNS Server. Click on **OK** to open the "Configure DNS Screen." Select "Yes, install and configure DNS on this computer."
9. On the "Permissions" screen, select "Permissions compatible with pre-Windows 2000 servers."
10. On the "Directory Services Restore Mode Administrator Password," input the Administrator password, as detailed in the 3rd Party Host Form.
11. On the Summary screen, check the settings and click on **Next**. You are prompted to insert the Windows 2000 CD and setup continues to install the Active Directory and DNS Server.
12. Restart when installation completes.

Step 58. Configure DNS Server on AW Forest Root Domain Controller

1. Click **Start > Programs > Admin Tools > DNS**.
2. Expand the Hostname Tree.
3. Expand the Forward Lookup Zones.
4. Right-click the root folder (the folder named ".") and select delete. Click **Yes** for the warning that appears.
5. Right-click the machine name and click **Properties**.
6. On the Interfaces Tab, select "Listen on Only the following IP addresses" and remove all but visible machine address.
7. Complete the configuration of the AD Integrated Forward and Reverse Lookup Zones.
8. Right-click the AW Domain zone name under Forward Lookup Zones and click **Properties**.
9. On the General Tab, for "Allow Dynamic Updates," select "Only Secure Updates" from the menu.

Only use the Zone Transfers Tab when there is a trust between this domain and another domain. In this case you need to Transfer Zone updates from this Active Directory Integrated Zone to a Standard Secondary Zone on the DNS Servers in the other domain. You "Allow Zone Transfers," then choose "only to the following servers" and enter the IP Addresses of the DNS Servers in that other domain (the IP addresses are the machine addresses of CICM DNS Servers).

To configure the required Reverse Lookup Zones, repeat the steps below for each AW Domain level network within the Forward Lookup Zone.

1. Under Server Name, right-click on the Reverse Lookup Zones and select **New Zone**.
2. Within the New Zone wizard, select "Active Directory Integrated."
3. In the Reverse Lookup Zone screen, select the radio button "Network ID" and enter the required number of octets for the Reverse Lookup Zone. The Reverse Lookup Zone Name automatically enters.
4. Repeat the steps below for each AW Domain Reverse Lookup Zone.
    - Right-click on the Zone name under Reverse Lookup Zones and click **Properties**.
    - On the General Tab, for "Allow Dynamic Updates," select "Only Secure Updates" from the menu.

Add the CICM Level Secondary Forward Lookup Zone

1. Right-click the Forward Lookup Zones and select **New Zone**.
2. Within the New Zone wizard, select "Standard Secondary" Zone and enter the full DNS name of the CICM Domain.
3. Enter the IP addresses of the CICM Level DNS Servers and let the wizard complete.
4. Access the CICM Level DNS Servers and add the AW Domain as a Secondary Forward Lookup Zone.
5. Right-click the Forward Lookup Zones and select **New Zone**.
6. Within the New Zone wizard, select "Standard Secondary" Zone and enter the full DNS name of the AW Domain.
7. Enter the IP addresses of the AW Domain Level DNS Server(s) and allow wizard to complete.

Step 59. Configure Active Directory Sites

1. Define the AD Sites on the AW Root Domain Controller.
2. Click **Start > Programs > Admin Tools > AD Sites and Services**.
3. Rename the default first site name for the AD Site Plan in System Diagram.
4. Click **Start > Programs > Admin Tools > AD Sites and Services**, right-click on the **Subnets** folder and select **New Subnet**.
    - Define subnet and mask respective for the AW Domain Controller Site.
    - Associate the subnet with the site.
    - Double-click on Server from original first site folder. Select Move and indicate site you want to move it to.

Step 60. Assign Global Catalog and FSMO Roles and Configure Time Source

By default, the AW Root Domain Controller is a Global Catalog and has all FSMO Roles. You may configure the AW's PDC Emulator to source its time from the CICM PDC Emulator to assure NAM System Wide Time Synchronization.

Run: Net time /setnstp: <DNS Name of Time Source at CICM level>

Step 61. Configure Trust Relationships

You must create a two-way external trust between the CICM and the Customer AW domain.

To create and validate trusts, access **Programs > Administrative Tools > Active Directory Domains and Trusts > Trusts Tab**.

Step 62. Join Standalone Servers to Domain

Add other Client AWs or other Real Time Distributors to the Customer Domain.

1. Right-click on My Computer and select **Properties > Network Identification Tab > Properties**.
2. Click on the Domain radio button and enter the name of the Domain.
3. Enter the Domain Administrator's username and password.
4. Restart the server and login to the Domain.

Step 63. Complete IP Configuration and Connectivity Testing

On each machine, validate the settings on each network card (TCP/IP Properties), including the DNS settings. Referring to the System Diagram, validate that the machine can ping every machine on the visible network and, if applicable, that it can ping to all its private connections.

Validate the Host and PTR records on the DNS Server to make sure that it contains all required zones and records.

Test remote access through the modem access points. You should be able to access each machine via modem, utilizing PCAnywhere and Telnet.

Step 64. Install SQL Server on AW's

1. Select STANDARD EDITION to start the SQL Server setup program.
2. At the first screen select Install SQL 2000 Server Components.
3. Select Install Database Server.
4. Click **NEXT** at Welcome Screen.
5. In Computer Name screen, use the default (Local Computer).
6. In Installation Selection screen, choose default "Create a new instance of SQL Server, or install Client Tools".
7. Enter your user and company information in the User Information screen.
8. Agree to the License Agreement by clicking **Yes**.
9. In the Installation Selection screen, choose the default ("Create a new instance of SQL Server, or install Client Tools").
10. Enter your user and company information in the User Information screen
11. Agree to the License Agreement by clicking **Yes**.
12. In the Installation Definition screen, choose the default "Server and Client Tools".
13. For the Instance Name, check **Default**.
14. Select **CUSTOM** for setup type.
15. Install Program Files to the default location on the C:.
16. For Components Screen, accept the defaults.
17. Under the Services Accounts, select:
    13. CUSTOMIZE
    14. USE THE LOCAL SYSTEM ACCOUNT
    15. AUTO START SERVICES
    16. SQL SERVER AGENT
    17. USE THE LOCAL SYSTEM ACOUNT
    18. AUTO START SERVICE – Check **OK** for the window that appears.
18. On the Authentication Mode screen, select "mixed mode" and check "blank password".
19. Set the Collation Designator to Latin1_General and Check **Binary for Sort Order**.
20. Under Network Libraries, deselect all choices except for NAMED PIPES.
21. Read the Start Copying Files screen and click **Next**.
22. Select PER SEAT as the licensing method and set 40 devices at least.
23. A dialog box with message "Setup is installing Microsoft Data Accessing Components (MDAC)" appears.
24. If a message box for Configure SQL Agent pops up, click **OK**.
25. When setup is complete, reboot the machine.

Install SQL Server Service Pack 2

1. Run the **setup.bat** file.
2. For the Computer Name, select Local Computer.
3. Accept the license agreement.
4. For the Instance Name, accept the default.
5. Connect to the Server using the SQL Server System Administrator login. Select "leave sa password blank".
6. Complete setup and reboot the server.
7. Expand the database sizes and logs using SQL Enterprise Manager. Click **START > Programs > Microsoft SQL Server > Enterprise Manager**. Under Server Name in the Enterprise Manager, double-click on Databases. Expand the server tree and highlight the Databases Folder under the server name.
8. Double-click Master Database in the right panel. The Master Properties window opens.
9. On the Data Files tab:
   - Set the Space Allocated to 50MB
   - Uncheck Autogrow
10. On the Transaction Log Tab:
    - Set the Space Allocated to 20MB
    - Uncheck Autogrow and click **OK**
11. Double-click on Tempdb in the right panel. The tempdb Properties window opens.
12. On the Data Files tab:
    - Set the Space Allocated to 50MB
    - Uncheck Autogrow
13. On the Transaction Log tab:
    - Set the Space Allocated to 20MB
    - Uncheck Autogrow and click **OK**
14. For the Options tab, verify the following settings:
    - **Unchecked** - ANSI NULL default, Recursive triggers, Auto close, Auto shrink and Use quoted identifiers
    - **Checked** – Auto update statistics, Torn page detection and Auto create statistics
15. Close the Enterprise Manager

Step 65. Install Webview 3rd Party Software

Print and read the Read Me file on the "Webview 3rd Party Installer CD 6.0." This file describes the software and provides installation instructions. Various settings described in the Read Me file appear on certain setup screens.

1. Check to see if you have the Jaguar 3.5 software already installed on your machine. If Jaguar 3.5 software is installed on your machine, use the control panel's Add/Remove software program to remove that software.
2. Run the setup on the 3rd Party Installer CD 6.0.
3. Reboot the server when setup completes.
4. Use the following procedure to make sure that the cache updates at each new view of a real-time report.
   - In the Internet Explorer window, select Internet Options from the Tools menu.
   - If necessary, click the General tab to display the General Settings tab page.
   - On the General Settings tab page, in the Temporary Internet Files sections, click **Settings**.

- In the Settings dialog box, enable the "Every Visit to the Page" option, then click **OK**.
- Click **OK** in the Internet Options dialog box.

Step 66. Install Infomaker on AW's

Infomaker is only installed on AWs (Real Time Distributors and Real Time Clients) for the purpose of creating Custom Reports.

1. Run setup from Media for Sybase Powerbuilder (Common Installer).
2. In the Welcome to 8.0 Installer screen, click **Next**.
3. Accept the License Agreement and click **Next**.
4. Fill out the Customer Information screen and click **Next**.
5. In the Destination Folder screen, accept the default and click **Next**.
6. In the Select Components screen, select Infomaker, and Online Books. Uncheck all other options.
   - You receive an Adaptive Server Anywhere warning. Click **OK** (ignore message).
   - Do not select Adaptive Server Anywhere. Click **No**.
   - You receive a Personal Server (Adaptive Server Anywhere) warning. Click **OK**.
7. Accept the default destination locations for all components and select "typical" for all setup types.

Complete all Wizards and reboot the server.

Step 67. Install ICM Software on Admin Workstation

Complete the setup on all Admin Workstations (see System Design Specification).

When setup completes, click **Start > Run**, enter ICMDBA and click **OK**. Expand the database to 500MB and the Log devices to 200MB.

Cisco provides specific hot fixes to major releases and service packs of the ICM software to address service-impacting issues. You download hot fixes from Cisco's Web site (http://www.cisco.com/) and apply them after the initial load of the software. The hot fix installation process only applies fixes required for the specific software modules (CallRouter, Logger, type of PG, etc.).

Step 68. Expand AW Database

1. Click **Start > Run**, enter ICMDBA and click **OK**.
2. Expand the Tree under the AW Hostname.
3. Highlight <cus_awdb>.
4. Select Expand from the Database menu.
5. Highlight the C drive.
6. Expand the Data to 500MB. Click **OK**.
7. Click **Start** on Expand the database window. Click **OK**. Close when complete
8. Select Expand from the Database menu.
9. Select Log (C drive is automatically highlighted).
10. Expand Log to 200MB. Click **OK**.
11. Click Start on the Expand database window. Click **OK**. Close when complete.
12. Close ICMDBA.
13. Click **Start > Programs > Microsoft SQL Server > Enterprise Manager.**
14. Expand Server Tree and highlight the Databases Folder under the Server name.
15. Double-click on ICM Database in the right panel. The <cus_awdb> Properties window opens.

16. On the Data Files tab:
    - Check Autogrow andset the File Growth to 10%
    - Set the Maximum File Size to [use the following calculation]

      {80% of free disk space}/{number of ICM database files and AW logs on this disk}+{database file current size}

      Example: {4GB * .80}/{2}+{.5GB}=2.1GB
17. On the Transaction Log Tab
    - Check Autogrow and set the File Growth to 10%
    - Set the Maximum File Size to [use the following calculation]

      {80% of free disk space}/{number of ICM database files and AW logs on this disk}+{database file current size}

      Example: {4GB * .80}/{2}+{.2GB}=1.8GB

Step 69. Create HDS Databases

For each HDS:

1. Click **Start > Run**, enter ICMDBA and click **OK**.
2. Expand Servername/Instances/<Instance Name> menus.
3. Highlight "Distributor."
4. Click on the Database menu and select **Create**.
5. A window indicates that SQL Server is not configured properly. Select **YES** to configure it now.
6. Verify that the "recommended settings" are set correctly for "Memory MB," "Max Async IO" and "Recovery Interval." Check the boxes next to each to fill in the new settings.
7. Stop SQL Server and the Distributor, as prompted, in order to continue.
8. In the Create Database screen, select the correct region for the system.
    - Click Add, the type is Data
    - Highlight the D drive. – Set the size to 70% of the available disk space, or to an amount determined with customer. Click **OK**.
    - Click Add and set the Type to Log.
    - Highlight the D drive and set the size to 200MB (do not make the log device larger than 500MB). Click **OK**.
    - Click Create and click Start to Create Database. When the database is successfully completed, click **OK** and Close the database window.
9. Close ICMDBA.
10. Click **START > Programs > Microsoft SQL Server > Enterprise Manager**.
11. Expand the server tree and highlight the Databases folder under the server name.
12. Double-click on ICM Database in the right panel. You are in the <cus_hds> Properties window.
13. On the Data Files tab:
    - Check Autogrow and set the File Growth to 10%
    - Set the Maximum File Size to [use the following calculation]

      {80% of free disk space}/{number of ICM database files and AW logs on this disk}+{database file current size}

      Example: {10GB * .80}/{3}+{8GB}=10.6GB
14. On the Transaction Log tab, uncheck Autogrow

Step 70. Start AW (Distributor) Services

Verify that the ICM Processes have no errors:

- CallRouters:
  - Router: running and synchronized with peer
  - Ccagent: connected to all configured peripheral gateways
  - Rtsvr: feed activated to AW
- Loggers:
  - Logger: connected to its respective database and synchronized with peer. The MDS is in service
  - Replication: connected to AW
  - CampaignManager: process up on logger and connected to the Blended Agent Dialer
- Admin Workstation:
  - Updateaw: displays “waiting for new work”
  - Iseman: listen thread waiting for client connection
  - Replication: replication and recovery client connection initialized
  - Cms_jserver: **cmsnode.exe** process is active. The event helper message shows CCS and CEM are running
  - Cmsnode: initialization complete
- Peripheral Gateways:
  - Generic (IPCC & VRU) PG
    - Mdsproc: in service
    - Pgagent: in service and active to one side of central controller
    - [peripheral] PIMs: disabled on node form. PIM windows do not exist
  - MR PG
    - Mdsproc: in service
    - Pgagent: in service and active to one side of central controller
    - [peripheral] PIMs: enabled in setup. The Blended Agent PIM is now ACTIVE. E-Mail Manager PIM is now ACTIVE and Media Blender PIM is ACTIVE
- CTI Server:
  - Cg[#]ctisvr: active with configured port number
- CTIOS Server:
  - Ctios Server: active with configured port number. The driver is online
  - Ctidriver: active
- Blended Agent Dialer:
  - Blended Agent Dialer: EMT connection established and configuration received
- E-Mail Manager Core:
  - Rules engine process: inbasket authenticated
- Collaboration Server:
  - Admin UI: under Collaboration Server > Server Setup > Connections\Monitor – all services have an UP status.
- Media Blender:
  - Admin UI: under Media Blender > Server > Startup Shutdown. Media Blender has been running for <time>.
  - Admin UI: under Media Blender > Services > Firewall Gateway > Monitor. All gateway stubs have a RUN status.

Final NAM/CICM Staging Tasks

Step No.	Task
71.	Change Domain Controllers to Native Mode
72.	Install Listeners, LG Mappers and LGArchiver
73.	Complete Staging Tests
74.	Complete Settings for Production Environment
75.	Complete Staging Issues Record

Step 71. Change Domain Controllers to Native Mode

Cisco ICM functions with Active Directory in both “Mixed” and “Native” modes. Microsoft recommends that you change an AD domain to native mode if an implementation does not and will not have any future NT domain controllers. You can only change the mode from mixed to native. Once the domain is running in native mode, you cannot change it back to mixed mode.

On NAM, CICM and Customer AW Domains Controllers:

1. Open Active Directory Domains and Trusts.
2. Right-click the domain node for the domain you want to administer and then click **Properties**.
3. In the General Tab, click Change Mode and then click **Yes**.

Step 72. Install Listeners, LGMappers and LGArchiver

Refer to the Remote Monitoring Suite Administration Guide for instructions on installing and configuring Listeners, LGMappers and LGArchivers. The NAM and CICM Loggers are configured in setup to “Phone Home” events to the Listeners over the NAM/CICM network. Service providers install Alarm Tracker Clients to monitor and manage the event stream from the LGMappers.

Step 73. Complete Staging Tests

With the full ICM system in the staging environment, you can test fault tolerance prior to shipping the system to the production environment. Refer to the section in the document on ICM Process Testing in the Staging Environment.

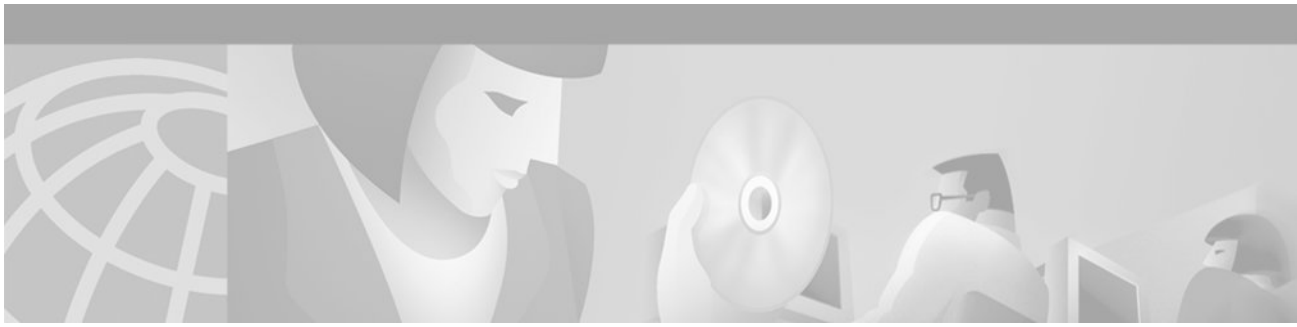
Step 74. Complete Settings for Production Environments

Validate the following settings from the system diagram for Production Environment and make the required changes prior to shipping systems. If you used a “dummy” IP addresses during the staging process, you need to load the actual Host Names/IP Addresses for the system onto the DNS Server (Logger/DNS Server) and set the actual/production IP addresses:

- IPAddresses (visible and private, high and low)
- Default Gateways
- Masks
- DNS preferred and alternate servers on visible cards
- Static Routes
- Active Directory WAN Sites and Subnets
- DNS Forward and Reverse Lookup Zone Records
- Label each Network Card and Port - Label the machine on the front and back with the host name
- Create Emergency Repair Disk
- Clear Event Logs
- Clear any Dr. Watson Application Errors
- Remove any diskettes, CD’s or media from drives
- Make sure that all ICM Services are set to Manual Start. Do not set Services to AUTOSTART until after Implementation Testing in the Production environment.

Step 75. Complete Staging Issues Record

Assure that the System Design Specification has been filled out as accurate records of the Staging event. Detail and note any test cases that were run as pass/fail/exceptions. Document any outstanding action items from the Staging event and share them with the team and project manager(s) associated with this project



ICM Process Testing In The Staging Environment

The sample test cases in this section allow you to validate the ICM inter-process communications and fault tolerance in the Staging Environment. When you install the system in the Production Environment, the Routing Application and Scripting are configured. At that time, begin Application Testing.

Table 1 Sample Test 1-RTTEST

Test Number:	1
Test Title:	RTTEST
Test Purpose:	Verify the current state of all ICM Central Site Processes and that all devices (PG's and Peripherals) are identified correctly by each CallRouter.
Test Setup:	All ICM Services start in full Duplex Mode – Run RTTEST on each CallRouter
Procedure:	1. Run: Rttest /system <CallRouterHostname> /cust <instance name> /node routera Rttest: status 2. Take a screen shot of the results and append to the Staging Report 3. Quit to exit out of the command prompt when you are finished on each CallRouter

Expected Results:	
1. All configured processes are OK as seen by CallRouters	Pass: ☐ Fail: ☐
2. All configured physical controllers are communicating (CFO) with CallRouters	Pass: ☐ Fail: ☐
3. All configure/in-service Peripherals are properly identified by that CallRouter and are online	Pass: ☐ Fail: ☐

Passed: (initial)	
Failed: (initial)	
Reason for Failure:	
Remarks:	**C** Signifies that the ICM peripheral gateway server successfully downloaded a configuration from the ICM call router. **F** Signifies that the ICM peripheral gateway is fully configured and that the configuration is valid. **O** Signifies that the ICM PG is on lineand that it is communicating with the ICM call router Peripherals are not online (O), since there are no live peripherals in the Staging Environment. The test is re-run in Production.

Table 2 Sample Test 2-ICM Process Logs

Test Number:	2
Test Title:	ICM Process Logs
Test Purpose:	Verify that Process Windows on each Server display no errors.
Test Setup:	All ICM Services start in full Duplex Mode
Procedure:	1. Do a visual check of all process windows on each ICM Server. 2. Never close an ICM Process window, as that stops the process. Minimize all windows after examination.

Expected Results:

1. Process windows on Loggers show zero errors: • Each Logger is connected to its respective database • Each Logger is synchronized with its duplex pair • There are no "waiting for MDS" messages	Pass: ☐ Fail: ☐
2. Process windows on CallRouters show zero errors: • Routers are up and Synchronized • CCAgent indicates <all>/<all> configured PG's are in service • NAM only: each CIC Side is connected to each INCRP Side • CICM only: each INCRP NIC indicates 2 NICR's online • Mdsproc is enabled	Pass: ☐ Fail: ☐
3. Process windows on AW's show zero errors and Updateaw is "waiting for new work".	Pass: ☐ Fail: ☐
4. Process windows on PG's show zero errors since PIM's are disabled at this time. Pgagent is in service.	Pass: ☐ Fail: ☐

Passed: (initial)	
Failed: (initial)	
Reason for Failure:	
Remarks:	

Table 3 Sample Test 3-Call Router Fault Tolerance

Test Number:	3
Test Title:	CallRouter Fault Tolerance
Test Purpose:	Verify that CallRouters function in Simplex Mode
Test Setup:	All ICM Services start in full Duplex Mode
Procedure:	1. Stop Router Service on CallRouter A. 2. On CallRouter B, open Router process and check for any messages that indicate Router A processes are down. 3. Start Router Service on CallRouter A. 4. On Router B check for any messages that indicate that CallRouter A Router and Logger processes are now OK. 5. Repeat steps 1-4, stopping Router B and validating Simplex Mode on Router A.

Expected Results:	
1. CallRouter B indicates that Side A Central Site is down when Router Service stops on CallRouter A	Pass: ☐ Fail: ☐
2. CallRouter B indicates that it is synchronized with CallRouter A when Router Service starts on CallRouterA.	Pass: ☐ Fail: ☐
3. Call Router B indicates that Side A Router and Logger Processes are OK when Router Service starts on CallRouterA.	Pass: ☐ Fail: ☐
4. CallRouter A indicates that Side B Central Site is down when Router Service stops on CallRouter B.	Pass: ☐ Fail: ☐
5. CallRouter A indicates that it is synchronized with CallRouter B when Router Service starts on CallRouterB.	Pass: ☐ Fail: ☐
6. Call Router A indicates that Side B Router and Logger Processes are OK when Router Service starts on CallRouterB.	Pass: ☐ Fail: ☐
7. Call Processing functions as designed when Routers are in Simplex Mode.	Pass: ☐ Fail: ☐

Passed: (initial)	
Failed: (initial)	
Reason for Failure:	
Remarks:	

Table 4 Sample Test 4-PG Fault Tolerance

Test Number:	4
Test Title:	PG Fault Tolerance
Test Purpose:	Verify that PG's communicate with Central Controller in Simplex Mode and that PIM's remain active.
Test Setup:	All PG Services start in Duplex Mode
Procedure:	1. Ensure that PGA is Active. 2. Ensure that PGB is Idle. 3. Stop Service on PGA. 4. Observe PGB change of state from Idle to Active. 5. Start Service on PGA. 6. Observe PGA state as Idle.

Expected Results:	
1. B Side PG maintains connectivity to the Central Contoller and the PIM is Active.	Pass: ☐ Fail: ☐
2. Upon restart of A side PG, A side MDS/OPC processes notes the state change into idle state while the B Side PG remains Active.	Pass: ☐ Fail: ☐
	Pass: ☐ Fail: ☐

Passed: (initial)	
Failed: (initial)	
Reason for Failure:	
Remarks:	