



Cisco ICM
Windows 2000 Planning
For Release 5.0
April 2003

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100



Contents

Contents	2
Figures	5
About This Guide	6
Purpose and Audience	6
Other Publications	6
ICM Deployment Planning	7
ICM Environment on Windows 2000	9
Cisco Intelligent Contact Management Architecture	9
Dedicated Domain	9
Domain Administration	9
Domain Users	10
Implications for Third Party Software Integration	10
Supported Windows 2000 Active Directory Models	10
Hosted NAM/CICM Model	10
Enterprise ICM Dedicated Forest/Root Domain Model	10
Enterprise ICM as a Child Domain in an existing corporate Forest Model	11
Special Note: Enterprise ICM within a Corporate Domain	11
Comparing Enterprise ICM Domain Models on Windows 2000	11
Security	11
Staging	11
DNS	12
Active Directory Sites	12
Naming Convention	12
Enterprise ICM Dedicated Forest/Domain Model	14
Active Directory Plan	16
Naming Convention	16
Domain Controllers	16

Trust Relationships	16
Domain Members	16
Non-Domain Members (standalone servers)	17
Active Directory Sites	17
Global Catalog and FSMO Roles Placement	17
Time Source	18
DNS Plan	18
DNS Naming Convention	18
DNS Servers and Clients	18
DNS Forward and Reverse Lookup Zones and Records	19
Enterprise ICM Child Domain Model	20
Active Directory Plan	22
Naming Convention	22
Domain Controllers	22
Trust Relationships	22
Domain Members	23
Non-Domain Members (standalone servers)	23
Active Directory Sites	23
Global Catalog and FSMO Roles Placement	23
Time Source	24
DNS Plan	24
DNS Naming Convention	24
DNS Servers and Clients	24
DNS Forward and Reverse Lookup Zone Records	25
Hosted NAM/CICM Model	26
NAM Dedicated Forest/Domain	26
Active Directory Plan	27
Naming Convention	27
Domain Controllers	27
Trust Relationships	27
Domain Members	28
Non-Domain Members (standalone servers)	28
Active Directory Sites	28
Global Catalog and FSMO Roles Placement	28
Time Source	29
DNS Plan	29
DNS Naming Convention	29
DNS Servers and Clients	29
DNS Forward and Reverse Lookup Zones and Records	29

CICM Child Domain	30
Active Directory Plan	31
Naming Convention	32
Domain Controllers	32
Trust Relationships	32
Domain Members	32
Non-Domain Members (standalone servers)	33
Active Directory Sites	33
Global Catalogs and FSMO Roles Placement	33
Time Source	34
DNS Plan	34
DNS Naming Convention	34
DNS Servers and Clients	34
DNS Forward and Reverse Lookup Zone Records	35
Customer AW Separate Forest/Domain	36
Active Directory Plan	37
Naming Convention	37
Domain Controllers	37
Trust Relationships	37
Domain Members	37
Active Directory Sites	37
Global Catalogs and FSMO Roles Placement	38
Time Source	38
DNS Plan	38
DNS Naming Convention	38
DNS Servers and Clients	38
DNS Forward and Reverse Lookup Zones and Records	39



Figures

Figure 1	Enterprise ICM Dedicated Forest/Domain Model – Central Controller Sites	14
Figure 2	Enterprise ICM Dedicated Forest/Domain Model – Call Center Site	15
Figure 3	Enterprise ICM Child Domain Model – Central Controller Sites	20
Figure 4	Enterprise ICM Child Domain Model – Call Center Site	21
Figure 5	NAM/CICM Model-NAM Dedicated Forest/Domain-Central Controller Sites	26
Figure 6	NAM/CICM Model-CICM Child Domain-Central Controller Sites	30
Figure 7	NAM/CICM Model-Customer AW Domain at CICM Call Center Site	36



About This Guide

Purpose and Audience

This document is for individuals responsible for planning Cisco Enterprise ICM or Hosted NAM/CICM deployments 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. You can find this information in specific documentation from Cisco and/or Microsoft.

This document describes the Cisco supported Windows 2000 Models for:

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

Other Publications

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

<http://www.cisco.com/univercd/cc/td/doc/product/icm/icm50/index.htm>

You can refer to the companion guide, *Cisco ICM 5.0 Staging on Windows 2000*, during the planning phase of an ICM/NAM deployment project to define the required staging tasks, once a supported Windows 2000 Model has been selected.



ICM Deployment Planning

Understanding and planning for a supported Windows 2000 model is a critical task during the Planning phase of an ICM/NAM deployment.

During this phase, you must document the specifications of the ICM/NAM system and the customer must accept them prior to the start of staging a new system. This System Design Specification should include a detailed description and diagrams of the Windows 2000 Model for Active Directory and DNS implementation. Make sure the System Design Specification contains all of the following information:

- 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
- ICM Configuration and CMS Control Settings
- 3rd Party Host Forms – Fill out entries and values for fields which are blank or different from the defaults utilized when setting up 3rd Party Software
- ICM Node Forms – Fill out entries and values for fields which are blank or different from the defaults utilized when setting up ICM Software
- Hardware and 3rd Party Software Specifications
 - New deployments of Release 5.0 on Windows 2000 require SQL Server Version 2000.
 - Cisco maintains a standard “Hardware Bill of Materials” that lists recommended platform sizing guidelines (not specific brands or models of servers), based on the types

of available hardware systems, for a specific release of ICM.

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_usage_guidelines_list.html



ICM Environment on Windows 2000

Cisco Intelligent Contact Management Architecture

Cisco Intelligent Contact Management version 5.0 must run on Windows 2000.

The ICM uses the Microsoft SQL Server database for the configuration, scripting, real time and historical databases used by the system. Release 5.0 supports SQL Server 7.0 for systems upgrading from 4.6.2 to 5.0. New systems must be built with SQL 2000. To simplify administration of the application, the ICM leverages the Microsoft security features of SQL on Windows. The SQL database authenticates users in the Windows domain to provide access and control rather than maintaining a separate user account and encrypted password table internal to the ICM.

Dedicated Domain

Leveraging Microsoft's "Integrated Security" model, the ICM can secure the database and application with the industry standard encryption and security control built into Microsoft Windows. Users who need access to the ICM application must have valid user accounts in the domain that are mapped to specific user roles within the ICM, controlling access levels within the application.

Along with the integrated security model, the ICM expects to find all the user and machine accounts and groups in a single domain model. The ICM does not reference Windows 2000 Organizational Units (OU's) when creating these groups and accounts. There is a Windows 2000 model in which an enterprise has two domains: a resource domain and a user domain. All the physical machines and servers are located in the resource domain and the user login accounts are in the user domain, using a specific trust relationship between the two domains to ensure the security of the resources. The ICM is not designed to manage multiple domains in this manner.

In this dedicated domain model, you can only use numbers and letters for the ICM domain name, user name, or any of the server names. ICM does not accept "special" characters.

Domain Administration

In order to leverage this level of security, you must initially install the ICM using an account with domain-level administrator rights. The ICM setup program validates user rights when it is started and does not allow a user without domain admin rights to run ICM setup. The ICM setup program requires domain level admin rights to create domain-level groups and administrative accounts that are used by the ICM to perform admin tasks and to map user rights into the database.

Domain Users

Additionally, the ICM application provides a User Manager tool to allow the ICM system manager to create new users within the ICM application. This function attempts to create the user account in the domain, which requires more than a standard set of user account rights in the domain.

Once you create a user account, the tool associates the user account with the ICM database and maps it to the appropriate rights and controls granted to the user. Typically, only users who perform configuration and scripting tasks are created in the application. Agents who only use the ICM for the CTI Desktop functions do not need access to the ICM domain.

Implications for Third Party Software Integration

The Cisco AVVID Partner Program was created to validate complementary software applications as they integrate to the products under the AVVID umbrella. Through this program, many of the leading contact-center products have integrated to the ICM. These include voice recording, workforce management, voice response, and customer relationship management applications.

The methods for integrating to the ICM (including CTI Server, Application Gateway, etc.) are implemented via socket/port combinations, not by Windows authentication. Thus, integrated applications and agent desktops connected to the ICM software can connect without setting up Windows user accounts or permissions.

Supported Windows 2000 Active Directory Models

Microsoft recommends installation of all user and machine/resource accounts in a simple domain model. Customers can have multiple domains to secure applications and groups of users. However, in Windows 2000, these domains are all tied back to a centralized “Forest” model to provide enterprise-wide administration and control.

Under Windows 2000, the ICM requires the use of Active Directory and DNS to maintain the Active Directory model. The account database that validates users in the domain is kept in the Active Directory. Windows 2000 has built-in methods to replicate this account database to the domain controllers within the forest and domain, across the various Active Directory sites.

The ICM has been tested and documented for use in the following domain models:

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

Hosted NAM/CICM Model

The Hosted NAM/CICM Model is a multiple domain model. The NAM layer is in a Dedicated Forest/Root Domain and has a two-way transitive trust with the CICM Child Domain. The CICM Layer rests in a Child Domain within the NAM Forest and has two types of trusts relationships:

- A two-way transitive trust with the NAM Parent Domain.
- A two-way external non-transitive trust with its associated Customer AW Domain(s).

The Customer Administrative Workstations are placed in a separate Forest/Root Domain, which has a two-way external non-transitive trust with their associated CICM Domain.

Enterprise ICM Dedicated Forest/Root Domain Model

This model follows the same design as the ICM being deployed under NT with a separate domain that is isolated from the rest of the customer Forest and Active Directory components. As with NT, the isolated

ICM domain can have an “external trust relationship” with an existing customer NT or 2000 domain to allow for administration tasks like reviewing log files and backing up the servers.

Enterprise ICM as a Child Domain in an existing corporate Forest Model

The Child Domain model still maintains isolation of the ICM users and servers in their own domain. However, the domain is a child of the existing corporate Forest and leverages the common DNS, Flexible Single Master Operation (FSMO) Roles at the Forest Domain Controllers, and the Forest Active Directory Sites and subnets that already exist to support the corporation. Load ICM “on-site” in this model, as only an administrator who holds Enterprise/Forest-wide admin rights can create the ICM Child Domain. In addition, the administrator must create the ICM Child Domain while on the corporate network. The child domain also maintains a default “transitive trust” relationship with the root domain, which allows for cross-domain access within the forest. This allows users to gain access to reporting within the ICM domain automatically. However, this may create a security concern if you don’t manually control the access.

Customers should consider the issues presented in the following section.

Special Note: Enterprise ICM within a Corporate Domain

A third (and less secure) Enterprise Model could include co-loading the ICM into the customer’s existing Forest/Root Domain model when the customer has migrated all of the applications into a single domain model. Cisco cannot model every customer Active Directory design, so this model is not tested by Cisco.

There are concerns about security in this model, as the ICM still maintains the use of the integrated security model with SQL Server and Windows 2000. The system requires domain admin rights to run the ICM Setup program, both to initially install the software and to re-run setup and make any changes to the program settings on an on-going basis. Domain admin rights, in this model, imply rights at the Forest/Root Domain level, which would grant almost unlimited access to the entire environment.

Comparing Enterprise ICM Domain Models on Windows 2000

The correct model for a customer deployment of Enterprise ICM on Windows 2000 depends upon the security considerations of the environment. Some customers do not want to mix their ICM domain with the corporate domain. Others may find that, for the small number of users and servers, the Child Domain is easier to administer.

Security

The Dedicated Forest/Domain Model is an isolated environment. You can manually set up external trusts to control access to the domain. Run the setup with domain administrative rights for the ICM domain.

The Child Domain lies in a shared environment with the Parent or Forest Root Domain. There is an automatic two-way transitive trust between the two domains. You must run setup with domain administrative rights for the ICM domain. You need Enterprise/Forest-wide administrative rights to create the Windows 2000 Child Domain.

Staging

You can set up the Dedicated Forest/Domain at a staging location and load the ICM software in the staging area. The ICM setup program can create the required users and groups in this staging model, allowing the ICM to be brought up and tested prior to on-site installation. When the system is installed on-site limited modification to the system needs to be performed to reflect the actual sites and DNS zones/subnets in the customer network.

You must create the Child Domain on-site with Enterprise/Forest-wide Administrative rights. The ICM Setup program only creates the users and groups within the Child Domain on-site. Multi-site deployments can increase the complexity, and may require on-site installation teams to install the ICM software at each site.

DNS

DNS is a required component to implementing the Active Directory (AD) in Windows 2000. ICM requires a domain security model, which is Active Directory in Windows 2000. Therefore, Active Directory and DNS go hand in hand, as opposed to Windows NT 4.0, where DNS was an optional software component. Starting with version 4.6.2, ICM supports using DNS as a name server to resolve ICM node names to an IP Address, instead of utilizing the Hosts file. Although Microsoft supports non-Windows DNS servers that are BIND 8.2.3 compliant, Cisco Systems has only tested ICM and supporting applications on Microsoft DNS Server to support Active Directory deployments and Name Resolution Services.

In the Dedicated Forest/Domain Model, a DNS Server runs on the first domain controller where the ICM forest was initially created. Given the AD's reliance on DNS, this server or another must be running the DNS Server when the AD is added. This DNS server is also authoritative for the zone where the ICM hosts are created and looked up against for name resolution. You need to add additional name servers to avoid a single point of failure.

In the Child Domain Model, customers may choose to centralize all DNS services to the root of the corporate forest where all sub-level domains fall back on the servers hosting the various domains' zones. Cisco's preferred DNS implementation for the Child Domain Model segregates all DNS traffic from ICM nodes to DNS servers residing on the domain controllers of the ICM Child domain. This is a preferable option for traffic and security reasons. This implementation provides reduced latency in resolving names, especially when the corporate DNS servers are a few hops away from the ICM network. You can configure DNS servers at both levels to cross-reference each other, in case intercommunication is required to establish trusts or simply resolve names of hosts residing on either such networks for which the name servers are authoritative.

Active Directory Sites

Active Directory Domain Controllers use sites during *authentication* and *replication*. A *site*, in Active Directory terminology, is defined as a group of computers on one or more Internet Protocol subnets that are well connected.

Well-connected means that the systems share a network transport that provides low-cost, high-speed communications between the machines and typically refers to systems in a single location that are connected by LANs. Systems that aren't well connected use relatively slow, expensive communications. Active Directory consists of one or more sites, but sites aren't part of the namespaces you deal with when you create the Active Directory hierarchy.

The basic reasons for dividing an enterprise network into sites is to take advantage of the efficient communications between well-connected systems while regulating the traffic over slower, costlier connections.

Definition of subnets and placement of Domain Controllers into AD Sites depends on the physical location of the Domain Controllers and if they are LAN or WAN connected. Adding and Naming AD Sites is performed by an administrator at the Forest Root level. Therefore, the domain administrator for ICM in the Dedicated Forest/Domain Model will name, add and manage the AD Sites. An ICM in the Child Domain Model would have to follow the convention and be subject to the management of the Forest/Root domain administrator.

Naming Convention

In the Dedicated Forest/Domain ICM Model, you can establish a unique naming convention tailored to the ICM.

Child Domains are subject to the naming convention established by the Forest Root. If the existing convention violates the ICM naming convention (you cannot use the underscore character in any ICM-related names), the customer must change or deploy in an isolated domain.



Enterprise ICM Dedicated Forest/Domain Model

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

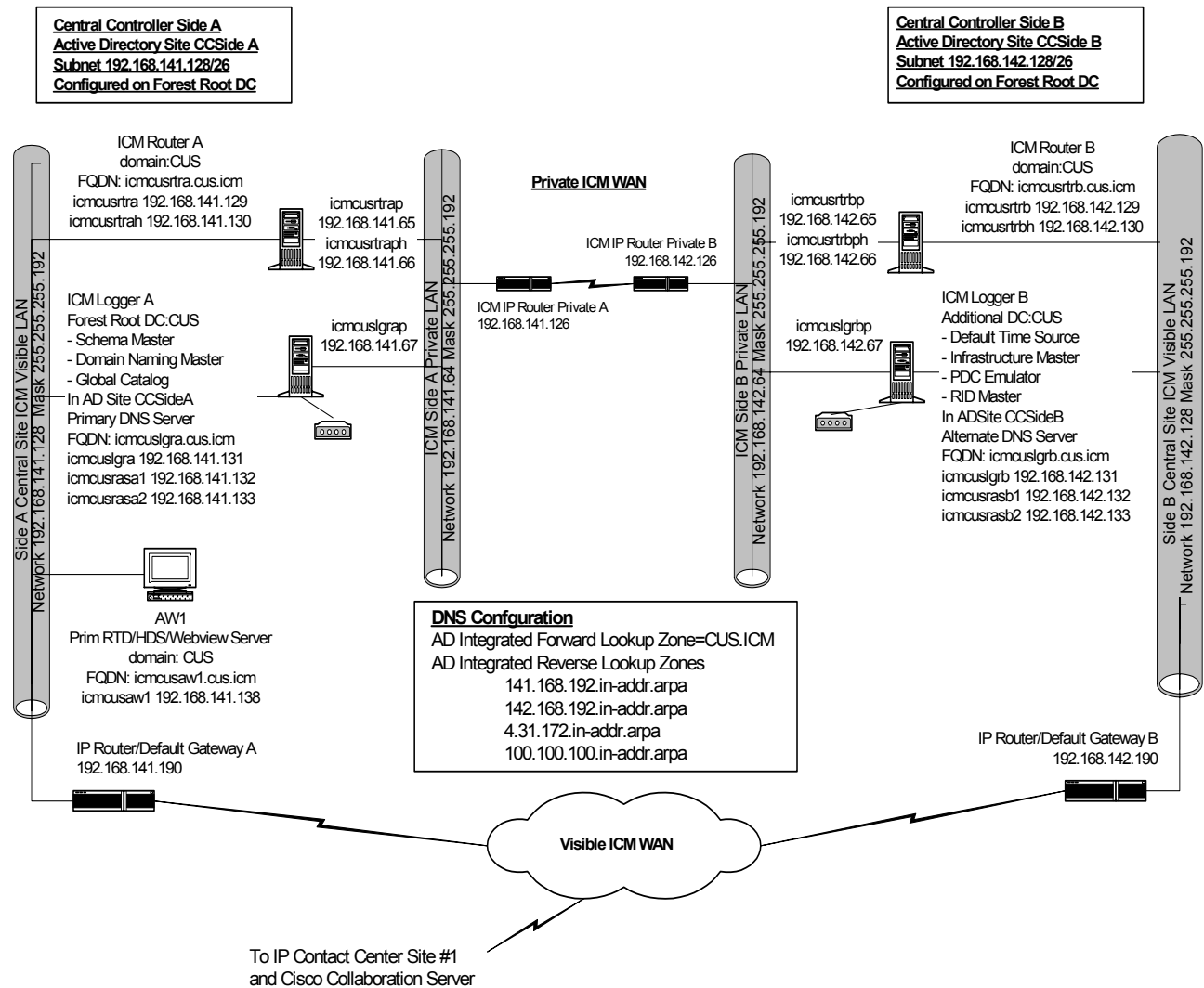
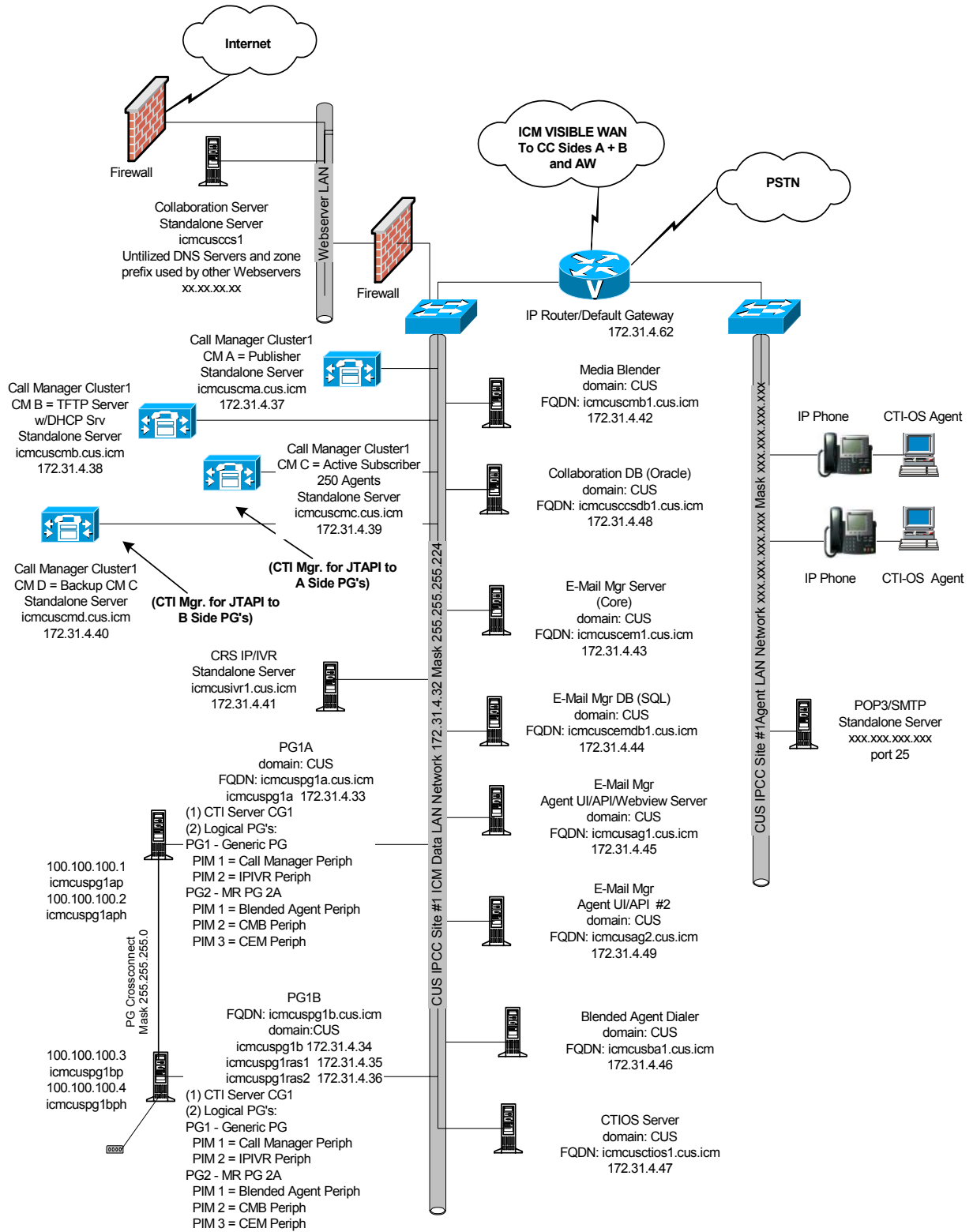


Figure 2 Enterprise ICM Dedicated Forest/Domain Model – Call Center Site



Active Directory Plan

You deploy the ICM in a Dedicated Forest/Domain model with no access to existing Windows 2000 Forest/Domain architectures. Customers may purchase additional hardware platforms to provide specific Domain Control or FSMO roles as part of their deployment. These additional platforms do not need to co-reside on the ICM servers. However, they do require the Cisco recommended minimum configurations to support the Windows 2000 Active Directory and DNS functions. The descriptive sections that follow assume that the AD and DNS functions are co-resident with the ICM Application Servers.

Naming Convention

A sample hostname is ICMSSSCCCM. See the hostname definition below:

- SSS is a unique short code (maximum five letters) that identifies the entire system.
- CCC is a two or three-letter code indicating the component type
- M is a one or two-character machine identifier (typically, the side and/or a device number).

A sample domain name would be XXX. When naming a domain, the ICM software requires that the domain name must start with a letter and contain only letters and numbers. Do not use any other characters. Although Windows 2000 would accept a domain name with other characters, such as a “_,” the ICM does not accept these characters and does not function properly if they are used.

- ICM NETBIOS Domain Name: <XXX>
- DNS Suffix: <ICM>
- FQDN of the Domain: <XXX.ICM>
- FQDN of a Machine: <ICMSSSCCCM.XXX.ICM>

Domain Controllers

The Active Directory Plan must define the specific servers to be used in the design for Active Directory Domain Controllers, and their relationship in the Windows 2000 Forest and root domain model. By default, a Windows 2000 Forest and root domain must have at least one Domain Controller. Domains should also have a second or additional Domain Controller for redundancy.

To minimize the number of servers required to support the ICM in Windows 2000, use the Logger/Database Servers as the Domain Controllers for the ICM dedicated Forest and Domain. For geographically distributed central controllers, this allows for local Domain Control and Active Directory replication across the sites and keeps the domain and account authentication local to the site. See the sample System Diagrams in the beginning of this section (see Figures 1 and 2, pages 14-15).

Optionally, you can add additional servers to support these functions and domain roles, if the customer does not allow “application servers” to also be Domain Controllers in their environment. Distribute these servers as noted above, to support geographically distributed central controller sites and minimize the cross-network traffic for the domain and account authentication of the ICM central controller servers.

Trust Relationships

The customer may add external non-transitive trust relationships from their Forest/Domain to the ICM environment for management and administrative purposes. The ICM in this model does not require any trust relationships, so you can set it up as “one-way,” to allow the ICM environment to trust the customer environment.

Domain Members

- Loggers (unless they are already Domain Controllers)

- CallRouters
- Admin Workstations (Real Time Distributors and Real Time Clients)
- CTIOS Server
- Peripheral Gateways
- Collaboration Database
- Media Blender
- E-Mail Manager Core
- E-Mail Manager Database
- E-Mail Manager Agent UI/API/Webview Server
- E-Mail Manager Agent UI/API #2
- Blended Agent Dialer

Non-Domain Members (standalone servers)

- Collaboration Server
- Call Manager Cluster Server Members
- CRS IP/IVR Server
- POP3/SMTP Server

Active Directory Sites

If you deploy the ICM with a co-located central controller (both sides A and B are at the same physical site), only create one Active Directory Site for the Central Site.

If you deploy the ICM with geographically distributed central controllers (Side A and Side B are in different physical locations), you need to define each physical site and IP subnet as its own Active Directory Site.

Active Directory Sites are only required for locations that will have Domain Controllers. Windows 2000 uses this information to maintain the Active Directory replication process between the Domain Controllers within a Forest and Domain, and for authentication purposes.

Global Catalog and FSMO Roles Placement

You define the FSMO (Flexible Single Master Operations) Roles and Global Catalogs within the Windows 2000 environment at both the Parent and Child Domain levels within a Forest. Assign these roles to the Domain Controllers.

Microsoft recommendations:

- Only one Schema Master and one domain Naming Master per Forest, and they must exist at the root of the Forest.
- Put the Schema Master and Domain Naming Master on same Domain Controller. The Domain Naming Master must co-reside with a Global Catalog.
- There must be at least one Global Catalog per Forest, but no more than one Global Catalog per Domain.
- Each Domain only has ONE RID Master, PDC Emulator, and Infrastructure Master.
- The RID Master and PDC Emulator roles should be on the same Domain Controller.
- When multiple Domain Controllers exist within a Domain, the Infrastructure Master and Global Catalog cannot be on the same Domain Controller.

- If a Domain has only one Domain Controller, it contains all FSMO roles and the Global Catalog. See the Central Controller System Diagram in the beginning of this section for a recommended placement of the Global Catalog and FSMO Roles.

Time Source

Since the PDC Emulator is moved in this Model to another Domain Controller, you must redefine the Time Source as either that server, or utilize an external Time Source.

DNS Plan

The DNS Plan must define the method for the ICM domain to access and control the Active Directory and DNS services. Active Directory uses DNS to manage the security and account data replication process between the Domain Controllers in the Domains and Forest.

The ICM 5.0 software has been qualified for use with Microsoft Windows 2000 DNS host name/IP address resolution. You need to plan carefully to ensure that you can resolve all required IP addresses using the DNS services provided by Microsoft Windows 2000. Otherwise, you may still require a local hosts file on the ICM servers to resolve some or all of the required addresses.

Windows 2000 manages DNS by creating DNS Zones. Each DNS Zone may define one or more IP Subnets where an Active Directory Domain Controller is found and provides a reference for these servers to find their Active Directory components. Set up the DNS Zones using the following recommendations:

- “Active Directory Integrated” Forward Lookup Zones. Store the DNS Zone information in the Active Directory to leverage the automatic Active Directory replication for DNS information.
- “Dynamic DNS” – Enables DNS client computers to register and automatically update their own host records, reducing manual administration of the DNS Zone records.

Each DNS domain/namespace has a Forward Lookup Zone and Reverse Lookup Zone defined. Forward Lookup Zones resolve an IP Address from a host name. Reverse Lookup Zones resolve a host name from an IP Address.

DNS Naming Convention

ICM NETBIOS Domain Name: <XXX>

DNS Suffix: <ICM>

FQDN of the Domain: <XXX.ICM>

DNS Servers and Clients

When setting up the DNS options for the ICM servers, select the “Preferred DNS Server” and the “Alternate DNS Server” to “load balance” the DNS servers and to minimize traffic between central sites.

Point the ICM Servers, co-located with the A-Side Central Controller (Router A, AW’s, PG’s, etc.), to the local, First Domain Controller/DNS Server. This is typically Logger A at that site. Then, list the “Alternate DNS Server” as Logger B, an additional Domain Controller/DNS Server.

Point the ICM Servers, co-located with the B-Side Central Controller (Router B, AW’s, PG’s, etc.), to the local additional Domain Controller/DNS Server. This is typically Logger B at that site. Next, list the “Alternate DNS Server” as Logger A, an additional Domain Controller/DNS Server.

Load balance any other ICM Servers not co-located across the DNS Servers remotely.

Servers related to the ICM which are not in the domain (such as Call Manager Cluster Server Members, CRS IP/IVR Server) may utilize DNS and the same set of DNS Servers as the domain members for hostname resolution.

DNS Forward and Reverse Lookup Zones and Records

The ICM Dedicated Forest/Domain utilizes an Active Directory Integrated Forward Lookup Zone. The networks within this Forward Lookup Zone include all visible and private networks, which are utilized within a DNS Zone or the ICM Domain. These networks define Reverse Lookup Zones relative to the Forward Lookup Zone.

ICM machines utilizing DNS service register with the DNS Servers when they boot up or join the domain. You must manually add all ICM hostnames (visible high, private, private high, SAN) as well as NIC and Peripheral hostnames entered into ICM setup, which require hostname resolution, into the DNS Forward Lookup Zone. Also, configure the associated PTR Record (reverse lookup zone record).



Enterprise ICM Child Domain Model

Figure 3 Enterprise ICM Child Domain Model – Central Controller Sites

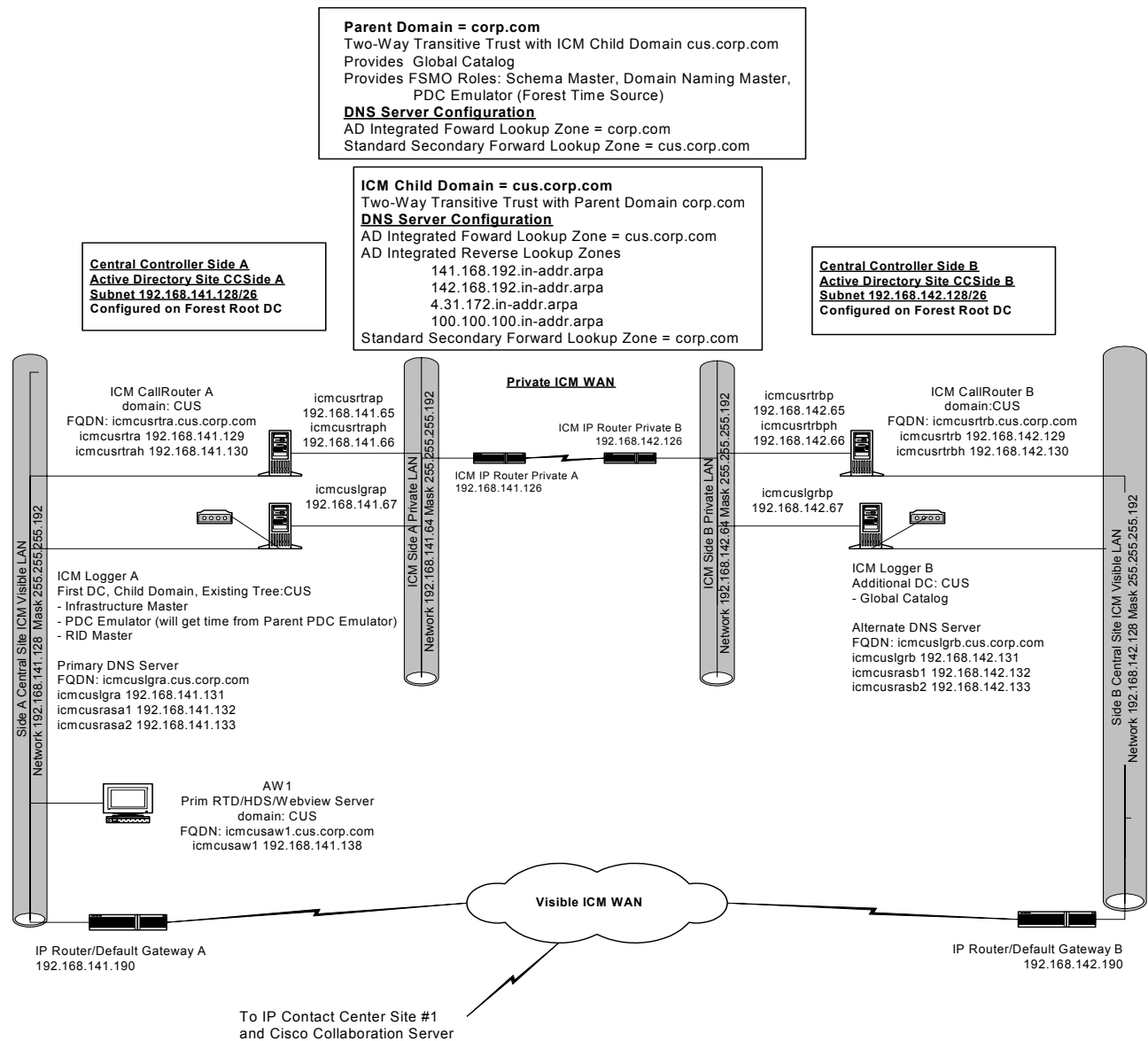
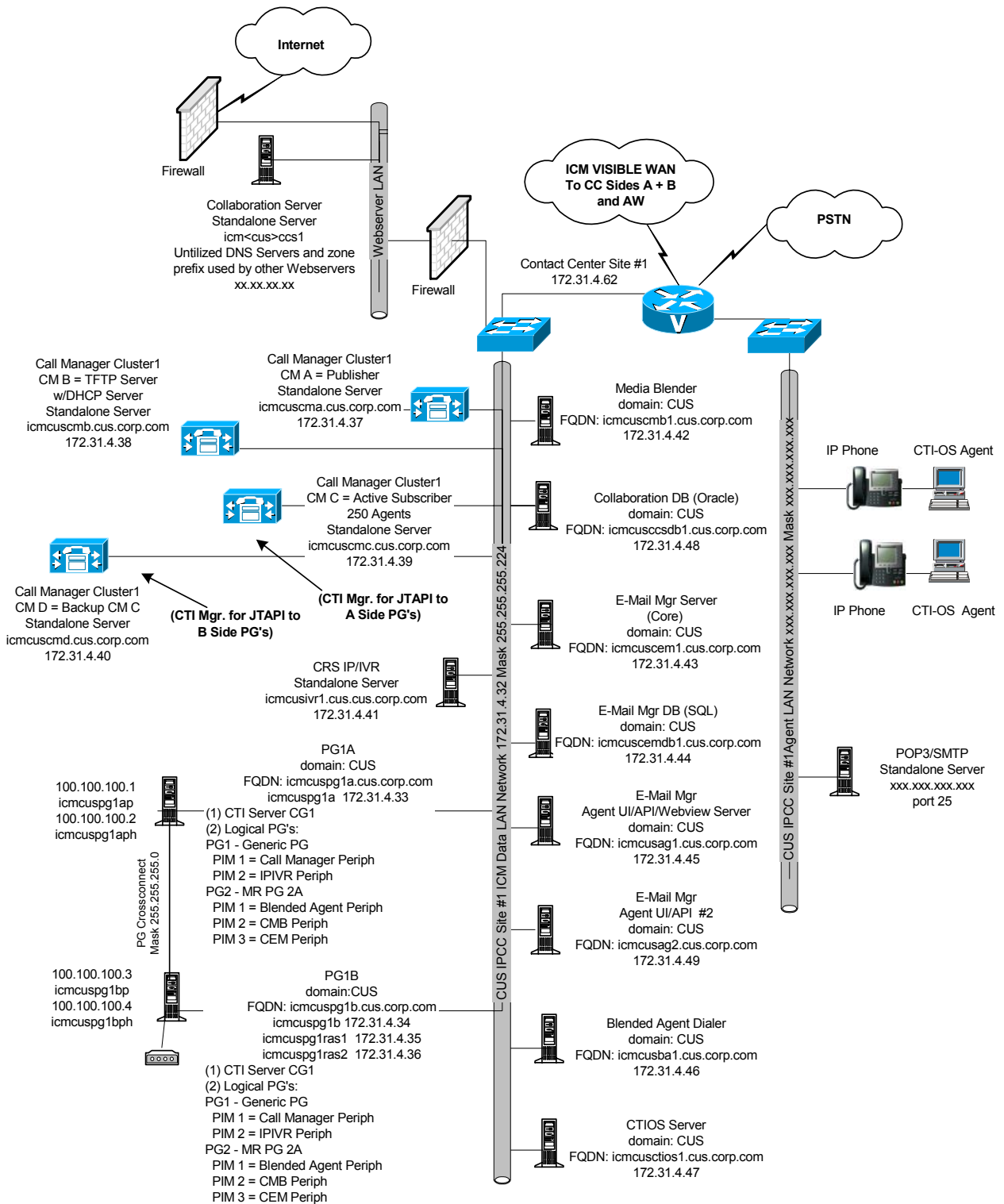


Figure 4 Enterprise ICM Child Domain Model – Call Center Site



Active Directory Plan

You deploy the ICM in an existing Windows 2000 Forest, in an isolated Child Domain. Customers may purchase additional hardware platforms to provide specific Domain Control or FSMO roles as part of their deployment. These additional platforms do not need to co-reside on the ICM servers. However, they do require the Cisco recommended minimum configurations to support the Windows 2000 Active Directory and DNS functions. The sections that follow assume that the AD and DNS functions co-reside with the ICM Application Servers within the Child Domain.

To install Active Directory Domain Controllers for a Child Domain, the Domain Controllers must have network access to the Parent Domain. Also, you need an Enterprise Administrator account to install the Child Domain Controllers.

You must stage a new system within an Enterprise ICM Child Domain on site, with full network access to the Parent Domain. You can enlist a Cisco Certified Integration Partner to source and pre-stage the ICM Servers as “standalone” prior to shipping them to the customer’s production locations.

Naming Convention

A sample hostname is ICMSSSCCM. The hostname is defined below:

- SSS is a unique short code (maximum five letters) that identifies the entire system.
- CCC is a two or three-letter code indicating the component type
- M is a one or two-character machine identifier (typically, the side and/or a device number).

A sample domain name is XXX. The domain name must start with a letter and contain only letters and numbers. Do not use any other characters. Although you can have a domain name with other characters in Windows 2000, the ICM does not accept those characters and does not function properly if you use them.

- ICM NETBIOS Domain Name: <XXX>
- DNS Suffix: <CORP.COM>
- FQDN of the Domain: <XXX.CORP.COM>
- FQDN of a Machine: <ICMSSSCCM.XXX.CORP.COM>

Domain Controllers

The Active Directory Plan must define the specific servers to be used in the design for Active Directory Domain Controllers and their relationship in the Windows 2000 Child Domain model. By default, a Windows 2000 Child Domain must have at least one Domain Controller. Domains should also have a second or additional Domain Controller for redundancy.

To minimize the number of servers required to support the ICM in Windows 2000, the Logger/Database Servers can be used as the Domain Controllers for the Domain. For geographically distributed central controllers, this allows for local Domain Control and Active Directory replication across the sites and keeps the domain and account authentication local to the site. See the sample System Diagrams in the beginning of this section (see Figures 3 and 4, pages 20-21).

Optionally, you can add additional servers to support these functions and domain roles if the customer does not allow “application servers” to also be Domain Controllers in their environment. You should distribute these servers as noted above, to support geographically distributed central controller sites and minimize the cross-network traffic for the domain and account authentication of the ICM central controller servers.

Trust Relationships

A two-way transitive trust is automatically setup between the Parent and Child Domain.

Domain Members

- Loggers (unless they are already Domain Controllers)
- CallRouters
- Admin Workstations (Real Time Distributors and Real Time Clients)
- CTIOS Server
- Peripheral Gateways
- Collaboration DB
- Media Blender
- E-Mail Manager Core
- E-Mail Manager DB
- E-Mail Manager Agent UI/API/Webview Server
- E-Mail Manager Agent UI/API #2
- Blended Agent Dialer

Non-Domain Members (standalone servers)

- Collaboration Server
- Call Manager Cluster Server Members
- CRS IP/IVR Server
- POP3/SMTP Server

Active Directory Sites

If you deploy the ICM with a co-located central controller (both sides A and B are at the same physical site), only one Active Directory Site is created for the Central Site.

If you deploy the ICM with geographically distributed central controllers (Side A and Side B are in different physical locations), you need to define each physical site and IP subnet as its own Active Directory Site.

Active Directory Sites are only required for locations that will have Domain Controllers. Windows 2000 uses this information to maintain the Active Directory replication process between the Domain Controllers within a Forest and Domain, and for authentication purposes.

Global Catalog and FSMO Roles Placement

You define the FSMO (Flexible Single Master Operations) Roles and Global Catalogs within the Windows 2000 environment at both the Parent and Child Domain levels within a Forest. Assign these roles to the Domain Controllers.

Follow the Microsoft recommendations listed below:

- Only one Schema Master and one domain Naming Master per Forest, and they must exist at the root of the Forest.
- Put the Schema Master and Domain Naming Master on same Domain Controller. The Domain Naming Master must co-reside with a Global Catalog.
- There must be at least one Global Catalog per Forest, but no more than one Global Catalog per Domain. There should be one Global Catalog per site, which may constitute placing a Global Catalog on a Child Domain Controller at an alternate site.

- Each Domain only has one RID Master, PDC Emulator, and Infrastructure Master.
- Put the RID Master and PDC Emulator roles should be on the same Domain Controller.
- When multiple Domain Controllers exist within a Domain, you cannot put the Infrastructure Master and Global Catalog on the same Domain Controller.
- If a Domain has only one Domain Controller, it contains all FSMO roles and the Global Catalog.
- The PDC Emulators run each Domain's Time Service and synchronize time with the Root PDC Emulator or with the configured Time Source.

See the ICM Central Controller System Diagram in the beginning of this section for a recommended placement of the Global Catalog and FSMO Roles (see Figures 3 and 4, pages 20-21).

Time Source

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.

DNS Plan

The DNS Plan must define the method for the ICM domain to access and control the Active Directory and DNS services. Active Directory uses the DNS to manage the security and account data replication process between the Domain Controllers in the Domains and Forest.

The ICM 5.0 software has been qualified for use with Microsoft Windows 2000 DNS host name/IP address resolution. In prior versions, a local HOSTS files was required on each machine to identify the ICM servers, their private network addresses, and any peripheral or carrier network specific addressing required by the ICM. You must plan carefully to ensure that all required IP addresses can be resolved using the DNS services provided by Microsoft Windows 2000. Otherwise, a local host file may still be required on the ICM servers to resolve some or all of the required addresses.

Windows 2000 manages DNS by creating DNS Zones. Each DNS Zone may define one or more IP Subnets where an Active Directory Domain Controller is found and provides a reference for these servers to find their Active Directory components. In this model, set up the DNS Zones using the following recommendations:

- "Active Directory Integrated" Forward Lookup Zones– Store the DNS Zone information in the Active Directory to leverage the automatic Active Directory replication for DNS information.
- "Dynamic DNS" – Enables DNS client computers to register and automatically update their own host records, reducing manual administration of the DNS Zone records.

Each DNS domain/namespace has a Forward Lookup Zone and Reverse Lookup Zone defined. Forward Lookup Zones resolve an IP Address from a host name. Reverse Lookup Zones resolve a host name from an IP Address.

DNS Naming Convention

ICM NETBIOS Domain Name: <XXX>

DNS Suffix: <CORP.COM>

FQDN of the Domain: <XXXX.CORP.COM>

DNS Servers and Clients

Cisco recommends that the Child Domain receive DNS Services from DNS Servers explicitly set up for the Child Domain DNS Zone.

When setting up the DNS options for the ICM servers, select the “Preferred DNS Server” and the “Alternate DNS Server” to “load balance” the DNS servers and to minimize traffic between central sites.

Point the ICM Servers, co-located with the A-Side Central Controller (Router A, AW’s, PG’s, etc.) to the local, First Domain Controller/DNS Server, which is typically Logger A at that site, then list the “Alternate DNS Server” as Logger B, as an additional Domain Controller/DNS Server.

Point the ICM Servers, co-located with the B-Side Central Controller (Router B, AW’s, PG’s, etc.), to the local additional Domain Controller/DNS Server, which is typically Logger B at that site, then list the “Alternate DNS Server” as Logger A, as an additional Domain Controller/DNS Server.

Load balance the ICM Servers that are not co-located across the DNS Servers remotely.

Servers related to the ICM which are not in the domain (such as Call Manager Cluster Server Members, CRS IP/IVR Server) may utilize DNS and the same set of DNS Servers as the domain members for hostname resolution.

DNS Forward and Reverse Lookup Zone Records

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 numbers of servers, for ease of management and administration. In lieu of this subfolder, you create an individual DNS zone for the new Child Domain.

The ICM Child utilizes an Active Directory Integrated Forward Lookup Zone. The networks within this Forward Lookup Zone include all visible and private networks, which are utilized within a DNS Zone or the ICM Domain. These networks define Reverse Lookup Zones relative to the Forward Lookup Zone.

ICM machines utilizing DNS service register with the DNS Servers when they start up or join the domain. You must manually add all ICM hostnames (visible high, private, private high, SAN) as well as NIC and Peripheral hostnames entered into ICM Setup (which require hostname resolution), into the DNS Forward Lookup Zone. Configure associated PTR Record (reverse lookup zone record).

You use Zone Transfers 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. The Enterprise/Parent DNS Servers host a Standard Secondary Zone for the ICM Domain. The ICM DNS servers host a Standard Secondary Zone for the Enterprise/Parent DNS Servers. You must “Allow Zone Transfers” from the AD Integrated Forward Lookup Zone to the DNS Servers hosting the Standard Secondary Zone.

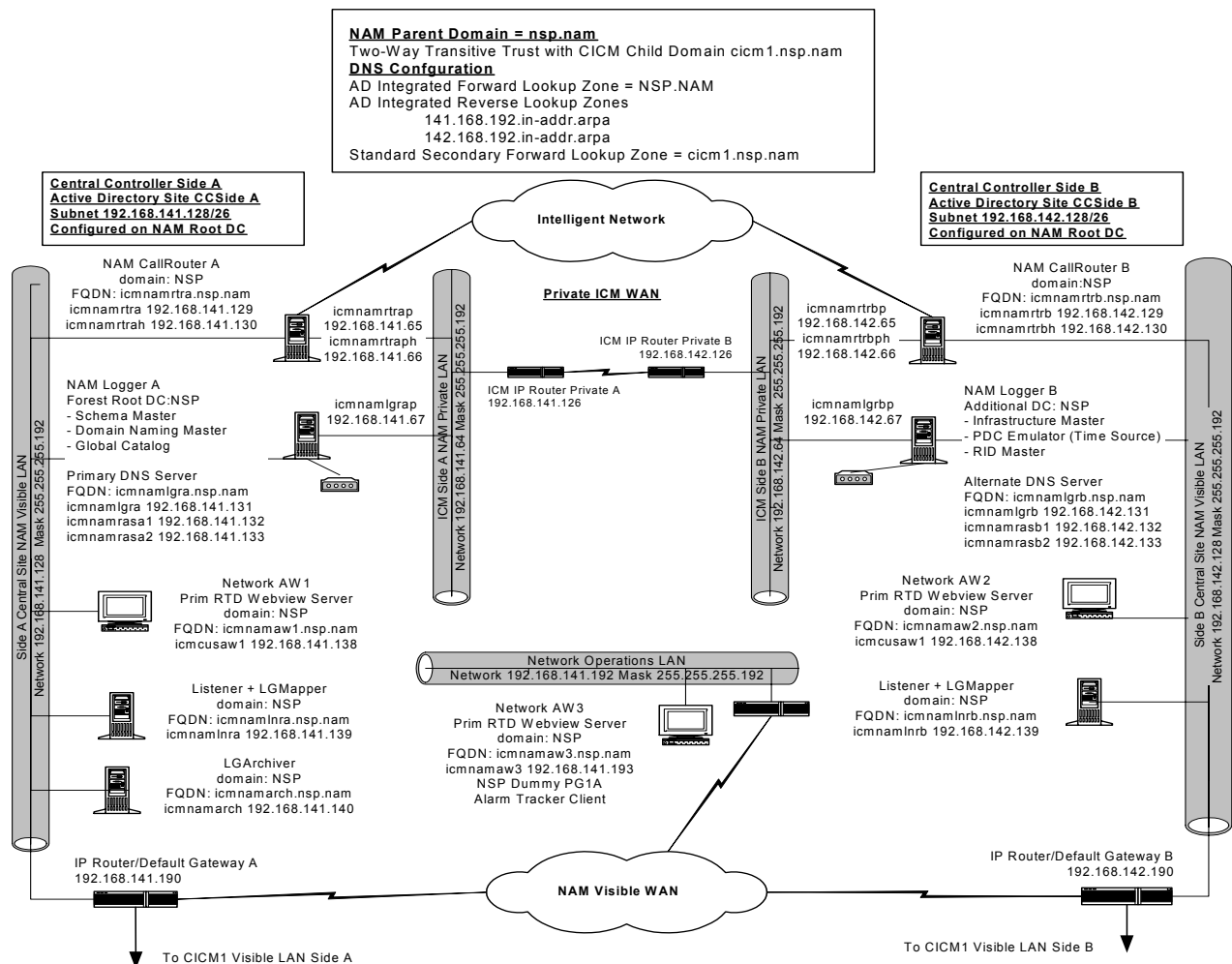


Hosted NAM/CICM Model

The Hosted NAM/CICM Model consists of at least the following three Domain Models.

NAM Dedicated Forest/Domain

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



Active Directory Plan

You deploy the NAM in a Dedicated Forest/Domain with no access to existing Windows 2000 Forest/Domains. Customers may purchase additional hardware platforms to provide specific Domain Control or FSMO roles as part of their deployment. These additional platforms do not need to co-reside on the ICM servers. However, they do require the Cisco recommended minimum configurations to support the Windows 2000 Active Directory and DNS functions. The descriptive sections that follow assume that the AD and DNS functions are co-resident with the ICM Application Servers.

If you are deploying a Multiple NAM, all Multiple NAM related components are deployed in a Windows 2000 Dedicated Forest/Domain. The platforms that support the Windows 2000 Active Directory and DNS functions may also host NAM level ICM application nodes (preferably the NPP's) if necessary. Customers are encouraged to purchase additional hardware platforms to segregate these specific DNS and Domain Control roles from the ICM application nodes as part of their Multiple NAM deployment for highest availability of all services.

Naming Convention

A sample hostname would be ICMSSSCCCM. The sample hostname is defined below:

- SSS is a unique short code (maximum five letters) that identifies the Service Provider.
- CCC is a two or three-letter code indicating the component type
- M is a one or two-character machine identifier (typically, the site and/or a device number).

A sample domain name is XXX. When naming a domain, the ICM software requires that the domain name start with a letter and contain only letters and numbers. Do not use any other characters. Although Windows 2000 can have a domain name with other characters, the ICM does not accept them and does not function properly if you use them.

- NAM NETBIOS Domain Name: <XXX>
- DNS Suffix: <NAM>
- FQDN of the Domain: <XXX.NAM>
- FQDN of a Machine: <ICMSSSCCCM.XXX.NAM>

Domain Controllers

The Active Directory Plan must define the specific servers to be used in the design for Active Directory Domain Controllers and their relationship in the Windows 2000 Forest and root domain model. By default, a Windows 2000 Forest and root domain must have at least one Domain Controller. Domains should also have a second or additional Domain Controller for redundancy.

To minimize the number of servers required to support the ICM in Windows 2000, you can use the Logger/Database Servers as the Domain Controllers for the ICM dedicated Forest and Domain. For geographically distributed central controllers, this allows for local Domain Control and Active Directory replication across the sites and keeps the domain and account authentication local to the site. See the sample System Diagrams in the beginning of this section (see Figure 5, page 26).

You can also add additional servers to support these functions and domain roles if the customer does not allow “application servers” to also be Domain Controllers in their environment. Distribute these servers as noted above, to support geographically distributed central controller sites and minimize the cross-network traffic for the domain and account authentication of the ICM central controller servers.

Trust Relationships

In Windows 2000 Active Directory, a two-way transitive trust is established by default between a parent and subordinate child domains. Therefore the NAM domain has a two-way transitive trust with the CICM domain(s).

Domain Members

- NAM Loggers (unless they are already Domain Controllers)
- NAM CallRouters
- Network Admin Workstations (Real Time Distributors and Real Time Clients which house NAM instance distributors as well as multiple CICM instance distributors)
- Listeners, LGMappers, LGArchivers
- Network VRU Peripheral Gateways
- ISN SDDSN Servers

Non-Domain Members (standalone servers)

- ISN Application Servers
- Voice Browsers
- Multi-Media Servers

Active Directory Sites

You deploy a NAM with geographically distributed central controllers (Side A and Side B are in different physical locations). You define each physical central controller site and IP subnet as its own Active Directory Site.

You only need Active Directory Sites for locations that will have Domain Controllers. Windows 2000 uses this information to maintain the Active Directory replication process between the Domain Controllers within a Forest and Domain, and for authentication purposes.

Global Catalog and FSMO Roles Placement

You define the FSMO (Flexible Single Master Operations) Roles and Global Catalog within the Windows 2000 environment at both the Parent and Child Domain levels within a Forest. Assign these roles to the Domain Controllers.

Microsoft's recommendations appear below:

- Only one Schema Master and one domain Naming Master per Forest, and they must exist at the root of the Forest.
- Put the Schema Master and Domain Naming Master on same Domain Controller. The Domain Naming Master must co-reside with a Global Catalog.
- There must be at least one Global Catalog per Forest, but no more than one Global Catalog per Domain. There should be one Global Catalog per site, which may constitute placing a Global Catalog on a Child Domain Controller at an alternate site.
- Each Domain only has one RID Master, PDC Emulator, and Infrastructure Master.
- Put the RID Master and PDC Emulator roles on the same Domain Controller.
- When multiple Domain Controllers exist within a Domain, you cannot put the Infrastructure Master and Global Catalog on the same Domain Controller
- If a Domain has only one Domain Controller, it contains all FSMO roles and the Global Catalog.

See the NAM Central Controller System Diagram in the beginning of this section for a recommended placement of the Global Catalog and FSMO Roles (see Figure 5, page 26).

Time Source

Since the PDC Emulator is moved in this Model to another Domain Controller, you must redefine the Time Source as either that server or an external Time Source.

DNS Plan

The DNS Plan must define the method for the NAM domain to access and control the Active Directory and DNS services. Active Directory uses the DNS to manage the security and account data replication process between the Domain Controllers in the Domains and Forest.

The ICM 5.0 software has been qualified for use with Microsoft Windows 2000 DNS host name/IP address resolution. In prior versions a local HOSTS files was required on each machine to identify the ICM servers, their private network addresses, and any peripheral or carrier network specific addressing required by the ICM. You need to ensure that the DNS services provided by Microsoft Windows 2000 can resolve all required IP addresses. Otherwise, you may still require a local host file on the ICM servers to resolve some or all of the required addresses.

Windows 2000 manages the DNS by creating DNS Zones. Each DNS Zone may define one or more IP Subnets, where an Active Directory Domain Controller is found and provides a reference for these servers to find their Active Directory components. In this model, set up the DNS Zones using the following recommendations:

- “Active Directory Integrated” Forward Lookup Zones– Store the DNS Zone information in the Active Directory to leverage the automatic Active Directory replication for DNS information.
- “Dynamic DNS” – Enables DNS client computers to register and automatically update their own host records, reducing manual administration of the DNS Zone records.

Additionally, each DNS domain/namespace has a Forward Lookup Zone as well as a Reverse Lookup Zone defined. Forward Lookup Zones resolve an IP Address from a host name. Reverse Lookup Zones resolve a host name from an IP Address.

DNS Naming Convention

NAM NETBIOS Domain Name: <XXX>

DNS Suffix: <NAM>

FQDN of the Domain: <XXXX.NAM>

DNS Servers and Clients

When setting up the DNS options for the ICM servers, select the “Preferred DNS Server” and the “Alternate DNS Server” to “load balance” the DNS servers and to minimize traffic between central sites.

Point the ICM Servers that are co-located with the A-Side Central Controller (Router A, AW’s, PG’s, etc.) to the local, First Domain Controller/DNS Server. This server is typically Logger A at that site. Then, list the “Alternate DNS Server” as Logger B, as an additional Domain Controller/DNS Server.

Point the ICM Servers that are co-located with the B-Side Central Controller (Router B, AW’s, PG’s, etc.) to the local additional Domain Controller/DNS Server. This server is typically Logger B at that site. Then, list the “Secondary DNS Server” as Logger A, as an additional Domain Controller/DNS Server.

Load balance other ICM Servers that are not co-located across the DNS Servers remotely.

DNS Forward and Reverse Lookup Zones and Records

The NAM Dedicated Forest/Domain utilizes an Active Directory Integrated Forward Lookup Zone. The networks within this Forward Lookup Zone include all visible and private networks, which are utilized

within a DNS Zone or the ICM Domain. These networks define the Reverse Lookup Zones relative to the Forward Lookup Zone.

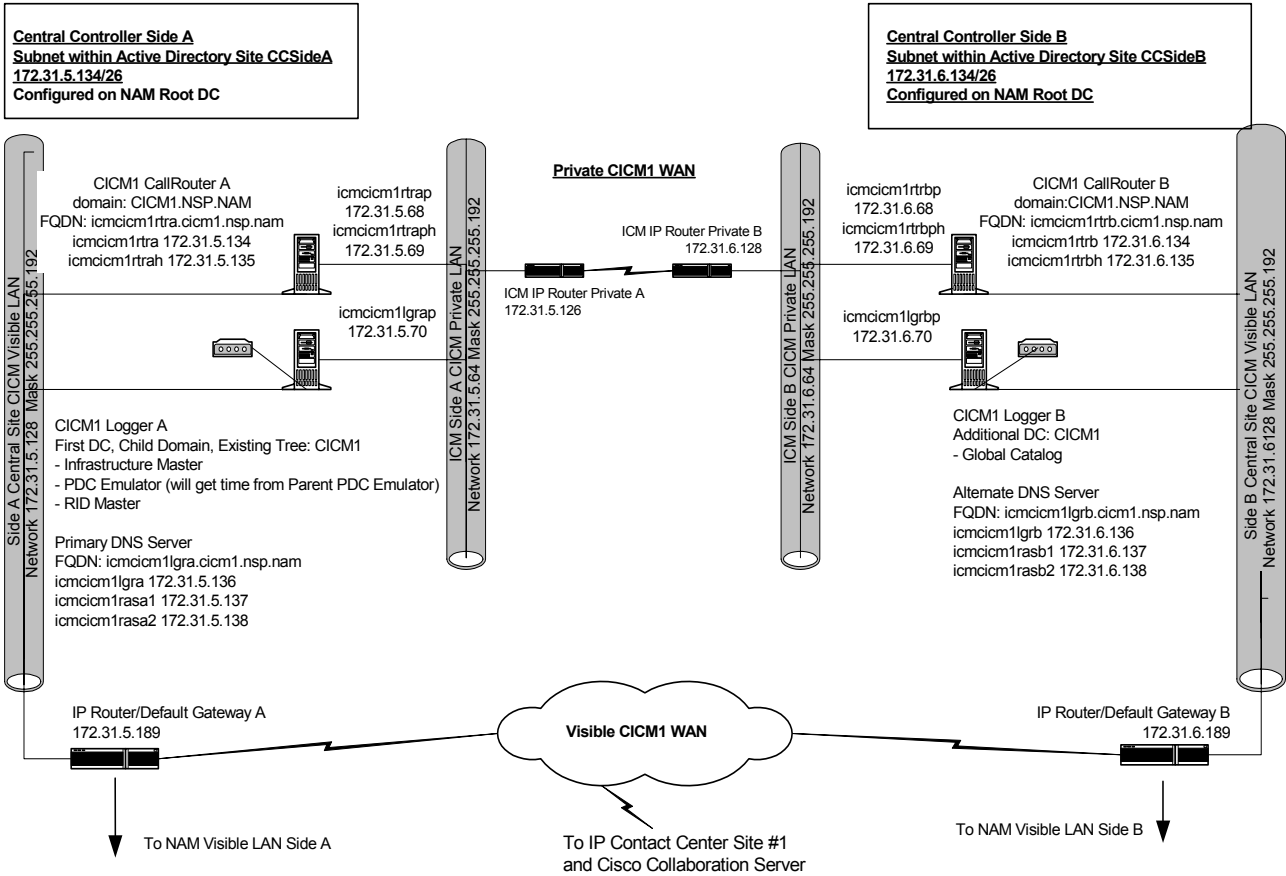
ICM machines utilizing the DNS service register with the DNS Servers when they start up or join the domain. You must manually add all ICM hostnames (visible high, private, private high, SAN, as well as NIC and Peripheral hostnames entered into ICM Setup) that require hostname resolution into the DNS Forward Lookup Zone. Also, you should configure the associated PTR Record (reverse lookup zone record).

You use Zone Transfers when there is a trust between this domain and another domain, in which 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. The NAM DNS Servers host a Standard Secondary Zone for the CICM Domain(s). The CICM DNS Servers host a Standard Secondary Zone for the NAM Domain. You must “Allow Zone Transfers” from the AD Integrated Forward Lookup Zone to the DNS Servers hosting the Standard Secondary Zone.

CICM Child Domain

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

CICM Child Domain = cicm1.nsp.nam
 Two-Way Transitive Trust with Parent Domain nsp.nam
 Two-Way External Non-Transitive Trust with Customer AW Domain cus1.cus
DNS Server Configuration
 AD Integrated Forward Lookup Zone = cicm1.nsp.nam
 AD Integrated Reverse Lookup Zones
 5.31.172.in-addr.arpa
 6.31.172.in-addr.arpa
 4.31.172.in-addr.arpa
 100.100.100.in-addr.arpa
 Standard Secondary Forward Lookup Zone = nsp.nam
 Standard Secondary Forward Lookup Zone = cus1.cus



Active Directory Plan

You deploy the CICM Complexes in an existing Windows 2000 Forest in a Child Domain. Customers may purchase additional hardware platforms to provide specific Domain Control or FSMO roles as part of their deployment. These additional platforms do not need to co-reside on the CICM servers. However, they do require the Cisco recommended minimum configurations to support the Windows 2000 Active Directory and DNS functions. The following section assumes that the AD and DNS functions co-reside with the ICM Application Servers within the Child Domain.

To install Active Directory Domain Controllers for a CICM Domain, the Domain Controllers must have network access to the NAM Domain. You need a NAM Administrator Account to install the CICM Domain Controllers.

Naming Convention

A sample hostname would be ICMSSSCCCM. The hostname definition is below:

- SSS is a unique short code (maximum five letters) that identifies the entire system.
- CCC is a two- or three-letter code indicating the component type
- M is a one- or two-character machine identifier (typically, the side and/or a device number).

A sample domain name is XXX. The ICM software requires that the domain name must start with a letter and contain only letters and numbers. Do not use any other characters. Although Windows 2000 can have a domain name with another character, the ICM does not recognize it, and does not function properly if you use it.

- CICM NETBIOS Domain Name: <CICM1>
- DNS Suffix: <XXX.NAM.>
- FQDN of the Domain: <CICM1.XXX.NAM>
- FQDN of a Machine: <ICMSSSCCCM.CICM1.XXX.NAM>

Domain Controllers

The Active Directory Plan must define the specific servers used in the design for Active Directory Domain Controllers and their relationship in the Windows 2000 model. By default, a Windows 2000 Child Domain must have at least one Domain Controller. Domains should also have a second or additional Domain Controller for redundancy.

To minimize the number of servers required to support the ICM in Windows 2000, use the Logger/Database Servers as the Domain Controllers for the ICM Child Domain. For geographically distributed central controllers, this allows for local Domain Control and Active Directory replication across the sites and keeps the domain and account authentication local to the site. See the sample System Diagrams in the beginning of this section.

Optionally, you can add additional servers to support these functions and domain roles if the customer does not allow “application servers” to also be Domain Controllers in their environment. You should also distribute these servers as noted above, to support geographically distributed central controller sites and minimize the cross-network traffic for the domain and account authentication of the ICM central controller servers.

Trust Relationships

A two-way transitive trust is automatically setup between the NAM and CICM Domains. However, you need to manually set up a two-way external non-transitive trust between the CICM Domain and related Customer AW Domains.

Domain Members

- Loggers (unless they are already Domain Controllers)
- CallRouters
- Admin Workstations (Real Time Distributors and Real Time Clients)
- CTIOS Server
- Peripheral Gateways
- Collaboration database
- Media Blender
- E-Mail Manager Core

- E-Mail Manager Database
- E-Mail Manager Agent UI/API/Webview Server
- E-Mail Manager Agent UI/API #2
- Blended Agent Dialer

Non-Domain Members (standalone servers)

- Collaboration Server
- Call Manager Cluster Server Members
- CRS IP/IVR Server
- POP3/SMTP Server

Active Directory Sites

You deploy CICM Complexes with geographically distributed central controllers (Side A and Side B are in different physical locations). You need to define each physical site and IP subnet as its own Active Directory Site.

Active Directory Sites are only required for locations that will have Domain Controllers. Windows 2000 uses this information to maintain the Active Directory replication process between the Domain Controllers within a Forest and Domain, and for authentication purposes.

In a Hosted Model, the AD sites with the CICM Domain Controllers are the same local LAN sites as the NAM Domain Controllers. Therefore, the AD Sites are already created. Now, you need to associate the CICM subnets with a site and place the CICM Domain Controller's in the appropriate site.

Global Catalogs and FSMO Roles Placement

You define the FSMO (Flexible Single Master Operations) Roles and Global Catalog within the Windows 2000 environment at both the NAM and CICM Domain levels within a Forest. Assign these roles to the Domain Controllers.

Follow the Microsoft recommendations below:

- Only one Schema Master and one domain Naming Master per Forest, and they must exist at the root of the Forest.
- Put the Schema Master and Domain Naming Master on same Domain Controller. The Domain Naming Master must co-reside with a Global Catalog.
- There must be at least one Global Catalog per Forest, but no more than one Global Catalog per Domain. There should be one Global Catalog per site, which may constitute placing a Global Catalog on a Child Domain Controller at an alternate site.
- Each Domain only has one RID Master, PDC Emulator, and Infrastructure Master.
- Put the RID Master and PDC Emulator roles on the same Domain Controller.
- You cannot put the Infrastructure Master and Global Catalog on the same Domain Controller when multiple Domain Controllers exist within a Domain.
- If a Domain has only one Domain Controller, it contains all FSMO roles and the Global Catalog.
- The PDC Emulators run each Domain's Time Service and synchronize time with the Root PDC Emulator or with the configured Time Source.

See the CICM Diagram in the beginning of this section for a recommended placement of the Global Catalog and FSMO Roles.

Time Source

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.

DNS Plan

The DNS Plan must define the method for the ICM domain to access and control the Active Directory and DNS services. Active Directory uses the DNS to manage the security and account data replication process between the Domain Controllers in the Domains and Forest.

The ICM 5.0 software has been qualified for use with Microsoft Windows 2000 DNS host name/IP address resolution. In prior versions, a local HOSTS files was required on each machine to identify the ICM servers, their private network addresses, and any peripheral or carrier network specific addressing required by the ICM. Ensure that you can resolve all required IP addresses using the DNS services provided by Microsoft Windows 2000. Otherwise, a local host file may still be required on the ICM servers to resolve some or all of the required addresses.

Windows 2000 manages the DNS by creating DNS Zones. Each DNS Zone may define one or more IP Subnets where an Active Directory Domain Controller is found and provides a reference for these servers to find their Active Directory components. In this model, set up the DNS Zones using the following recommendations:

- “Active Directory Integrated” Forward Lookup Zones– Store the DNS Zone information in the Active Directory to leverage the automatic Active Directory replication for DNS information.
- “Dynamic DNS” – Enables DNS client computers to register and automatically update their own host records, reducing manual administration of the DNS Zone records.

Additionally, each DNS domain/namespace has a Forward Lookup Zone as well as a Reverse Lookup Zone defined. Forward Lookup Zones resolve an IP Address from a host name. Reverse Lookup Zones resolve a host name from an IP Address.

DNS Naming Convention

CICM NETBIOS Domain Name: <CICM1>

DNS Suffix: <XXX.NAM.>

FQDN of the Domain: <CICM1.XXX.NAM>

DNS Servers and Clients

Cisco recommends that the CICM Domain receive DNS Services from DNS Servers explicitly set up for the CICM Domain DNS Zone.

When setting up the DNS options for the ICM servers, select the “Preferred DNS Server” and the “Alternate DNS Server” to “load balance” the DNS servers and to minimize traffic between central sites.

Point the ICM Servers co-located with the A-Side Central Controller (Router A, AW's, PG's, etc.) to the local, First Domain Controller/DNS Server. This server is typically Logger A at that site. Then, list the “Alternate DNS Server” as Logger B, as an additional Domain Controller/DNS Server.

Point the ICM Servers co-located with the B-Side Central Controller (Router B, AW's, PG's, etc.) to the local additional Domain Controller/DNS Server. The server is typically Logger B at that site. Then, list the “Alternate DNS Server” as Logger A, as an additional Domain Controller/DNS Server.

You should “load balance” other ICM Servers that are not co-located across the DNS Servers remotely.

DNS Forward and Reverse Lookup Zone Records

When you create the CICM/Child Domain, Windows automatically creates a “subfolder” in the NAM/Root DNS tree as a container for the servers in the new CICM/Child Domain. Typically, these folders are only used for a small numbers of servers, for ease of management and administration. In lieu of this subfolder you create an individual DNS zone for the new CICM/Child Domain

The CICM utilizes an Active Directory Integrated Forward Lookup Zone. The networks within this Forward Lookup Zone include all visible and private networks, which are utilized within a DNS Zone or the ICM Domain. These networks define Reverse Lookup Zones relative to the Forward Lookup Zone.

ICM machines utilizing DNS service register with the DNS Servers when they start up or join the domain. You must manually add the following into the DNS Forward Lookup Zone:

- All ICM hostnames (visible high, private, private high, SAN)
- Peripheral hostnames entered into ICM Setup which require hostname resolution,

Also, configure the associated PTR Record (reverse lookup zone record).

Use Zone Transfers 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.

The NAM DNS Servers host a Standard Secondary Zone for the CICM Domain. The CICM DNS Servers host a Standard Secondary Zone for the NAM DNS Servers and a Standard Secondary Zone for the Customer AW DNS Server(s). You must “Allow Zone Transfers” from the AD Integrated Forward Lookup Zone to the DNS Servers hosting the Standard Secondary Zone.

Active Directory Plan

You should deploy the Customer AW Domain in a Dedicated Forest/Domain model. Customers may purchase additional hardware platforms to provide specific Domain Control or FSMO roles, as part of their deployment. These additional platforms do not need to co-reside on the ICM servers. However, they do require the Cisco recommended minimum configurations to support the Windows 2000 Active Directory and DNS functions. The following section assumes that the AD and DNS functions are co-resident with the ICM Application Servers.

Naming Convention

A sample hostname would be ICMSSSCCCM. This hostname signifies:

- SSS is a unique short code (maximum five letters) that identifies the Service Provider.
- CCC is a two or three-letter code indicating the component type.
- M is a one or two-character machine identifier (typically, the side and/or a device number).

A sample domain name would be XXX. When naming a domain, the ICM software requires that the domain name must start with a letter and contain only letters and numbers. Do not use any other characters. Although Windows 2000 can have a domain name with other characters, the ICM does not accept it.

- Customer AW NETBIOS Domain Name: <XXX>
- DNS Suffix: <CUS>
- FQDN of the Domain: <XXX.CUS>
- FQDN of a Machine: <ICMSSSCCCM.XXX.CUS>

Domain Controllers

The Active Directory Plan must define the specific servers used in the design for Active Directory Domain Controllers and their relationship in the Windows 2000 Forest and root domain model. By default, a Windows 2000 Forest and root domain must have at least one Domain Controller.

To minimize the number of servers required to support the ICM in Windows 2000, use the Admin Workstation Server as the Domain Controllers for the ICM dedicated Forest and Domain.

Optionally, you can add another server to support these functions and domain roles if the customer does not allow “application servers” to also be Domain Controllers in their environment.

Trust Relationships

The Customer AW Domain has a two-way external non-transitive trust with its related CICM domain.

Domain Members

Domain Members include the following:

- Customer AW (if it is not already the Domain Controller) – Distributors act as Historical Data Servers and Webview Servers
- Client AW's

Active Directory Sites

Active Directory Sites are only required for locations that have Domain Controllers. Windows 2000 uses this information to:

- Maintain the Active Directory replication process between the Domain Controllers within a Forest and Domain, and
- For authentication purposes.

You define the Active Directory Site for the Customer AW Domain Controller on that Domain Controller.

Global Catalogs and FSMO Roles Placement

All FSMO (Flexible Single Master Operations) Roles and Global Catalog, by default, are created on this first and only domain controller within the domain.

See the Customer AW Call Center Site Diagram in the beginning of this section for a recommended placement of the Global Catalog and FSMO Roles (see page 36).

Time Source

You may configure the AW's PDC Emulator to source its time from the CICM PDC Emulator to assure NAM System Wide Time Synchronization.

DNS Plan

The DNS Plan must define the method for the domain to access and control the Active Directory and DNS services.

Windows 2000 manages the DNS by creating DNS Zones. Each DNS Zone may define one or more IP Subnets where an Active Directory Domain Controller is found and provides a reference for these servers to find their Active Directory components. In this model, set up the DNS Zones using the following recommendations:

- "Active Directory Integrated" Forward Lookup Zones– Store the DNS Zone information in the Active Directory to leverage the automatic Active Directory replication for DNS information.
- "Dynamic DNS" – Enables DNS client computers to register and automatically update their own host records, reducing manual administration of the DNS Zone records.

Additionally, each DNS domain/namespace has a Forward Lookup Zone as well as a Reverse Lookup Zone defined. Forward Lookup Zones resolve an IP Address from a host name. Reverse Lookup Zones resolve a host name from an IP Address.

DNS Naming Convention

Customer AW NETBIOS Domain Name: <XXX>

DNS Suffix: <CUS>

FQDN of the Domain: <XXX.CUS>

DNS Servers and Clients

When setting up the DNS options for the ICM servers, if there is more than one Customer AW level DNS Server, select the "Preferred DNS Server" and the "Alternate DNS Server" to "load balance" the DNS servers and to minimize traffic between central sites.

DNS Forward and Reverse Lookup Zones and Records

The Customer AW Domain utilizes an Active Directory Integrated Forward Lookup Zone. The networks within this Forward Lookup Zone include the visible networks, which are utilized within a DNS Zone or the ICM Domain. These networks define Reverse Lookup Zones relative to the Forward Lookup Zone.

ICM machines utilizing DNS service register with the DNS Servers when they start up or join the domain.

You use Zone Transfers 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. The CICM DNS Servers host a Standard Secondary Zone for the Customer AW domain. The Customer AW DNS Server(s) host a Standard Secondary Zone for the CICM Domain. You must “Allow Zone Transfers” from the AD Integrated Forward Lookup Zone to the CICM DNS Servers hosting the Standard Secondary Zone.