



Global Knowledge®

Expert Reference Series of White Papers

Integrating CUUCM 6.X and Active Directory (AD)

Integrating (CUCM) 6.X and Active Directory (AD)

James "Mac" McInville, Global Knowledge Instructor, Certified Cisco Systems Instructor (CCSI #31293)

Introduction

Although Active Directory (AD) and Cisco Unified Communications Manager (CUCM) are very diverse systems owned by two completely separate companies, the use of AD for management of users in a CUCM system is a common consideration. Microsoft's AD structure is as ubiquitous as any system used in enterprise networks today. Most organizations using an AD system already have an easy way to manage their users. Tying this ease of use system into CUCM is the next logical step.

To understand the management of users using AD, one first has to understand the categories of users defined in CUCM. In previous versions of Cisco Call Manager (CCM), users were simply defined as users; whether they were maintained within the CCM database or integrated with AD, users were all the same. With CUCM, users are defined as End Users and Application Users. End Users are typically associated with a real person and include an interactive login (that is, a login that is entered by a real person when prompted to do so). Application Users are other users that will not be associated with one real person but will be associated with an end application or potentially multiple users. For example, when a CUCM system is first built, an Application User is created and is typically named CCMAAdministrator (although this is not a required name, it is a popular name amongst Integrators and Partners doing these installations). This Application User may be used by multiple individuals for full administrative access to the CUCM Administration and Serviceability pages. Other Application User types include Auto Attendant and IP Manager-Assistant (IPMA) configurations. Application Users are beyond the scope of this discussion as we will focus on End Users and their association with AD.

Another consideration to consider is whether just simple synchronization is going to be enabled or synchronization with authentication. With simple synchronization, the End User information is provisioned and managed from the perspective of AD. That is, the user ID information and other user-associated attributes are synchronized and shared with the CUCM, but the passwords for authentication are maintained and controlled locally within the CUCM database. With synchronization with authentication, both the user ID and associated attributes and the users' passwords are managed centrally within the AD system.

The introduction of an appliance-based CUCM significantly changed how directory integration is performed. This integration is required to do full corporate directory queries from phones, provisioning of users from the corporate directory, and the authentication of End Users and administrators of CUCM using corporate directory credentials. This is all made possible by the Directory Architecture (Figure 1).

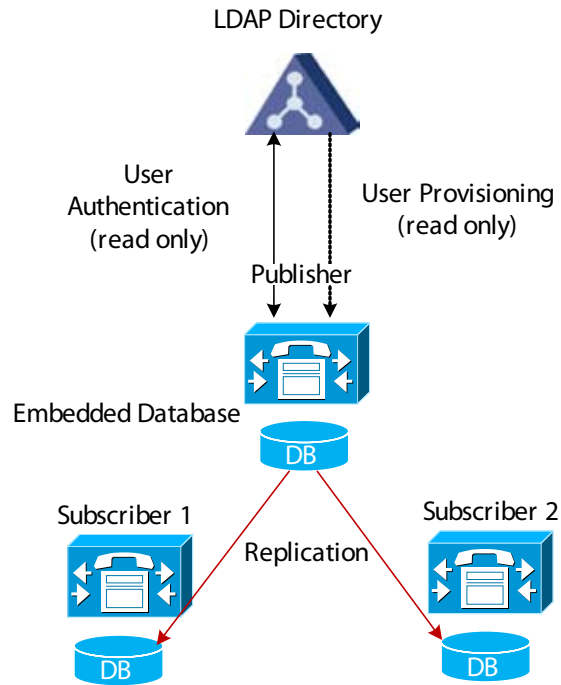


Figure 1. High-Level Directory Architecture

Figure 1 includes the AD server (LDAP Directory), the CUCM cluster, including the publisher and two subscribers, and a representation of the cluster database replicated from the publisher to the other subscribers in the cluster. It also displays the directional travel of End User authentication (both ways) and end user provisioning (one-way) traffic. Also notice that the communications between CUCM and AD are read-only, which would meet most AD administration and security requirements.

Synchronization

If a business is already taking advantage of centralized management of users with the database structure of AD, it is a common next step to use this same central authority for end user management and provisioning for CUCM administration. For example, with some simple configurations on both the CUCM and AD side, a system can be implemented where if a new user were to be added to a company, that user would already need to be added to the AD domain for e-mail access and other corporate requirements. That same user added to AD would be automatically populated in the local CUCM database. Then that user would simply need to be modified on the CUCM side to make certain that they had proper access to specific locations within the CUCM configuration pages or that they had the correct access for personal phone configuration and modification. In other cases, if an employee were to leave, that same individual would be marked for deletion on the AD side and in turn marked for deletion on the CUCM side. After a specified amount of time, that individual marked for deletion would indeed be removed from the database permanently. This is accomplished through scheduled synchronization intervals that define when the AD system will be queried by CUCM for updates to current users that are already synchronized. When synchronization is enabled for the first time on a CUCM publisher, users' accounts that exist in the corporate directory are imported into the CUCM database. From that point forward, user accounts are activated or removed according to the following process.

- All pre-existing user accounts are marked inactive in the CUCM publisher database. During synchronization, all accounts that match with an account in the AD database are marked active again.
- After the synchronization is completed, any accounts still marked inactive for at least 24 hours will be deleted at the next garbage collection event. Garbage collection runs automatically at 3:15 a.m. This is a non-configurable system value.
- As other changes are made in the Corporate Directory, CUCM will receive these changes during the next scheduled synchronization period.
- The synchronization agreement specifies a time for synchronizing to begin and the period for re-synchronization specified in hours, days, weeks, or months (6 hours minimum).

For example: If account A were added to the LDAP database on Day 0, the account is available for use on Day 1. If account A were disabled on Day 2, the user's personal CCM page would be unavailable almost immediately, marked inactive in the CUCM database after the first synchronization period, then other user services, such as Extension Mobility, would be disabled. Finally, after being in the inactive state for 24 hours, the user would then be removed but not until the Garbage Collection interval has been reached again (Figure 2).

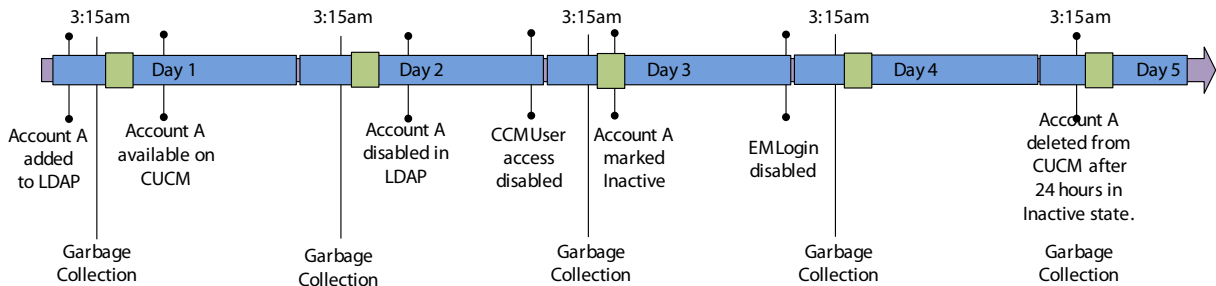


Figure 2. Synchronization Example

Another consideration is what level of information must be accessible from the CUCMs' perspective in order to be able to synchronize with the correct user base. This will be discussed in the configuration section specific to the CUCM configuration, but based on the Organizational Unit Structure (OU) on the AD side. In other words, is it more important to be able to synchronize and use all users within the AD structure or just within specific OUs.

LDAP Authentication

The LDAP authentication feature enables Unified CM to authenticate end user passwords against a corporate LDAP directory instead of using the embedded database. This authentication is accomplished with an LDAPv3 connection established between the IMS module within Unified CM and a corporate directory server.

To enable authentication, a single authentication agreement may be defined for the entire cluster. The authentication agreement supports configuration of up to three LDAP servers for redundancy and also supports secure connections LDAP over SSL (SLDAP), if desired. Authentication can be enabled only when LDAP synchronization is used.

The following statements describe Unified CM's behavior when authentication is enabled.

- End user passwords are authenticated against the corporate directory by a simple bind operation.
- Application user passwords are authenticated against the Unified CM database.
- End user PINs are authenticated against the Unified CM database.

This behavior is in line with the guiding principle of providing single logon functionality for end users while making the operation of the real-time IP Communications system independent of the availability of the corporate directory.

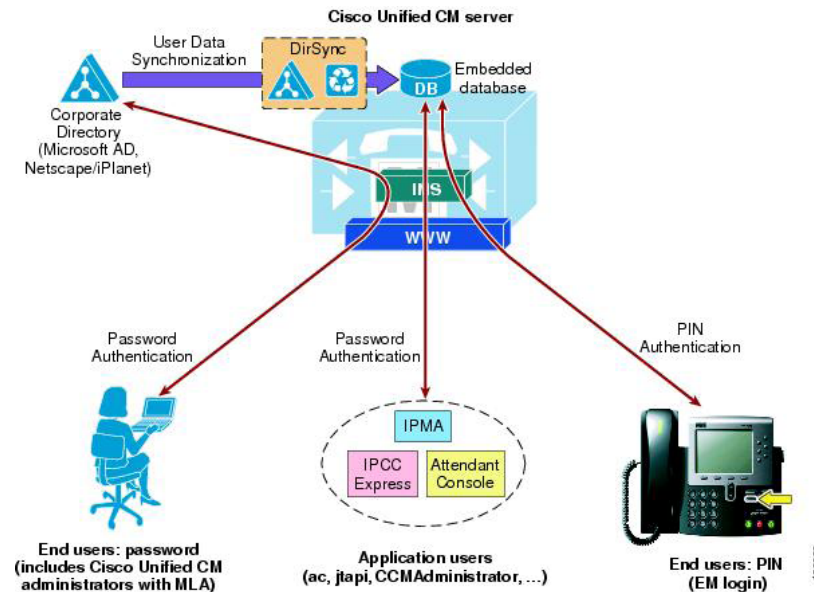


Figure 3. Authentication Example

Unified CM adopted this process to allow authentication for an end user against a corporate LDAP directory:

1. A user connects to the Unified CM User Options page via HTTPS and attempts to authenticate with a user name and password. In this example, the user name is jsmith.
2. Unified CM issues an LDAP query for the user name jsmith, using the value specified in the LDAP Search Base on the LDAP Authentication configuration page as the scope for this query. If SLDAP is enabled, this query travels over an SSL connection.
3. The corporate directory server replies via LDAP with the full Distinguished Name (DN) of user jsmith (for example, "cn=jsmith, ou=Users, dc=vse, dc=lab").
4. Unified CM then attempts to validate the user's credentials by using an LDAP bind operation to pass the full DN and password provided by the user.
5. If the LDAP bind is successful, Unified CM allows the user to proceed to the configuration page requested.

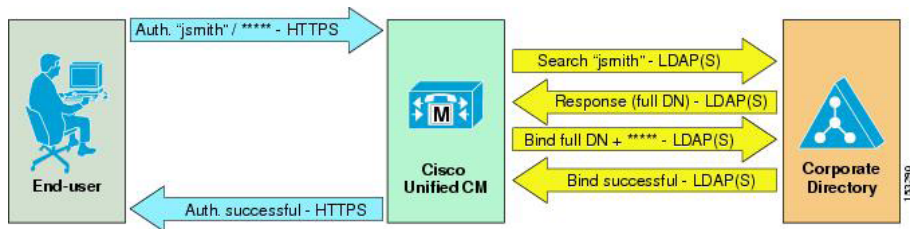


Figure 4. End User Authentication

Observe the following design and implementation best-practices when deploying LDAP authentication with Cisco Unified CM.

- Create a specific account within the corporate directory to allow Unified CM to connect and authenticate to it. Cisco recommends that you use an account dedicated to Unified CM, with minimum permissions set to “read” all user objects within the desired search base and with a password set to never expire. The password for this account in the directory must be kept in synchronization with the password configuration of the account in Unified CM. If the account password changes in the directory, be sure to update the account configuration in Unified CM. If LDAP synchronization is also enabled, you can use the same account for both functions.
- Enable LDAP authentication on Unified CM by specifying the credentials of the aforementioned account under LDAP Manager Distinguished Name and LDAP Password, and by specifying the directory subtree where all the users reside under LDAP User Search Base.
- Configure at least two LDAP servers for redundancy. You can use IP addresses instead of host names to eliminate dependencies on Domain Name System (DNS) availability.
- This method provides single logon functionality to all end users: when they log in to the Unified CM User Options page, they can now use their corporate directory credentials.
- Manage end-user passwords from within the corporate directory interface. Note that the password field is no longer displayed in the Unified CM Administration pages when authentication is enabled.
- Manage end-user PINs from the Unified CM Administration web pages or from the Unified CM User Options page.
- Manage Application User passwords from the Unified CM Administration web pages. Remember that these application users facilitate communication and remote call control with other Cisco Unified Communications applications and are not associated with real people.
- Enable single logon for Unified CM administrators by adding their corresponding end user to the Unified CM Super Users user group from the Unified CM Administration web pages. Multiple levels of administrator rights can be defined by creating customized user groups and roles.

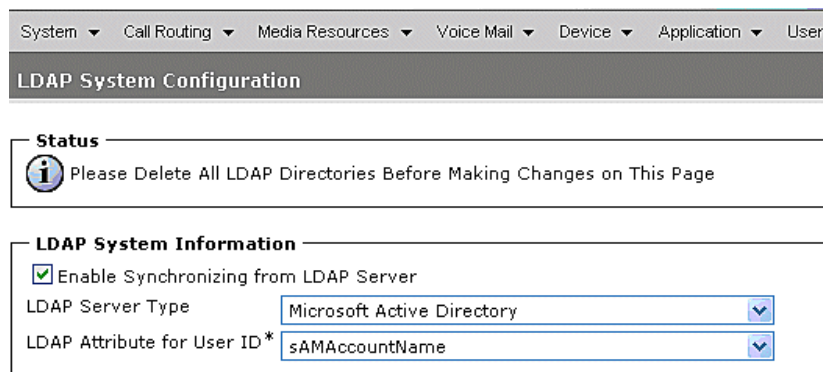
Configuration

Configuration is a two-fold process in that the AD requires minimum configuration and the CUCM has its own configuration requirements. For both synchronization and authentication with synchronization, the configuration is similar. The difference with authentication configuration will be discussed a little later in this document.

One of the first things that has to be considered is that the AD system might be managed and controlled by a completely separate group than the ones maintaining and installing the CUCM appliance. It is always important to communicate the reason and functionality to these teams to help them to better understand their role with this requirement.

On the AD side an account has to be provisioned for communicating with CUCM during these synchronization intervals. This account must be able to read all user objects within a defined search base, and the password must be set to never expire. Best practice specifies that an account must be named according to local naming conventions as it applies to the CUCM cluster and/or user account naming conventions, but otherwise the name is of little importance. In our example, we are considering this account a service and, therefore, we are using a service account naming convention (svcCUCMsynch).

Although still quite simple, there are a few more configuration requirements on the CUCM side. One of the first requirements is to enable to CUCM service that allows for synchronization. Navigate to the CUCM Serviceability page (<https://Server Name or IP address/ccmservice>) and choose Tools -> Service Activation, select the name/IP address of the publisher server from the drop-down and scroll down to the Directory Services section. Check the box to the left of the Cisco DirSync service and then click Save to activate that service. Now navigate back to the main Call Manager Administration page by choosing it from the drop-down or by entering the URL for CUCM Administration (<https://Server Name or IP Address/ccmadmin>). Now navigate to the LDAP section by choosing System -> LDAP -> LDAP System. Next, enable synchronization by checking the box titled Enable Synchronizing from LDAP Server. From the LDAP Server Type, drop-down select Microsoft Active Directory. The last piece on the LDAP System configuration page is to select from the drop-down for LDAP Attribute for user ID and choose sAMAccountName. See Figure 5 below for a sample of what this might look like on your system.



System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User

LDAP System Configuration

Status

i Please Delete All LDAP Directories Before Making Changes on This Page

LDAP System Information

Enable Synchronizing from LDAP Server

LDAP Server Type: Microsoft Active Directory ▾

LDAP Attribute for User ID*: sAMAccountName ▾

Figure 5 – LDAP System Configuration Page

Best Practices for LDAP Synchronization

Observe the following design and implementation best practices when deploying LDAP synchronization with Cisco Unified CM.

- Use a specific account within the corporate directory to allow the Unified CM synchronization agreement to connect and authenticate to it. Cisco recommends that you use an account dedicated to Unified CM,

with minimum permissions set to “read” all user objects within the desired search base and with a password set never to expire. The password for this account in the directory must be kept in synchronization with the password configuration of the account in Unified CM. If the service account password changes in the directory, be sure to update the account configuration in Unified CM.

- All synchronization agreements on a given cluster must integrate with the same family of LDAP servers (Microsoft AD, iPlanet, or Sun ONE).
- Stagger the scheduling of synchronization agreements so that multiple agreements are not querying the same LDAP servers simultaneously. Choose synchronization times that occur during quiet periods (off-peak hours).
- If security of user data is required, enable Secure LDAP (SLDAP) by checking the Use SSL field on the LDAP Directory configuration page in Unified CM Administration.
- Ensure that the LDAP directory attribute chosen to map into the Unified CM UserID field is unique within all synchronization agreements for that cluster.
- The attribute chosen as UserID must not be the same as that for any of the Application Users defined in Unified CM.
- An existing account in the Unified CM database before synchronization is maintained only if an account imported from the LDAP directory has a matching attribute. The attribute that is matched to the Unified CM UserID is determined by the synchronization agreement.
- Configure at least two LDAP servers for redundancy. You can use IP addresses instead of host names to eliminate dependencies on Domain Name System (DNS) availability.
- Administer end-user accounts through the LDAP directory’s management tools, and manage the Cisco-specific data for those accounts through the Unified CM Administration web page.
- For AD deployments, the ObjectGUID is used internally in Unified CM as the key attribute of a user. The attribute in AD that corresponds to the Unified CM User ID may be changed in AD. For example, if sAMAccountname is being used, a user may change their sAMAccountname in AD, and the corresponding user record in Unified CM would be updated.

With all other LDAP platforms, the attribute that is mapped to User ID is the key for that account in Unified CM. Changing that attribute in LDAP will result in a new user being created in Unified CM, and the original user will be marked inactive.

Security Considerations

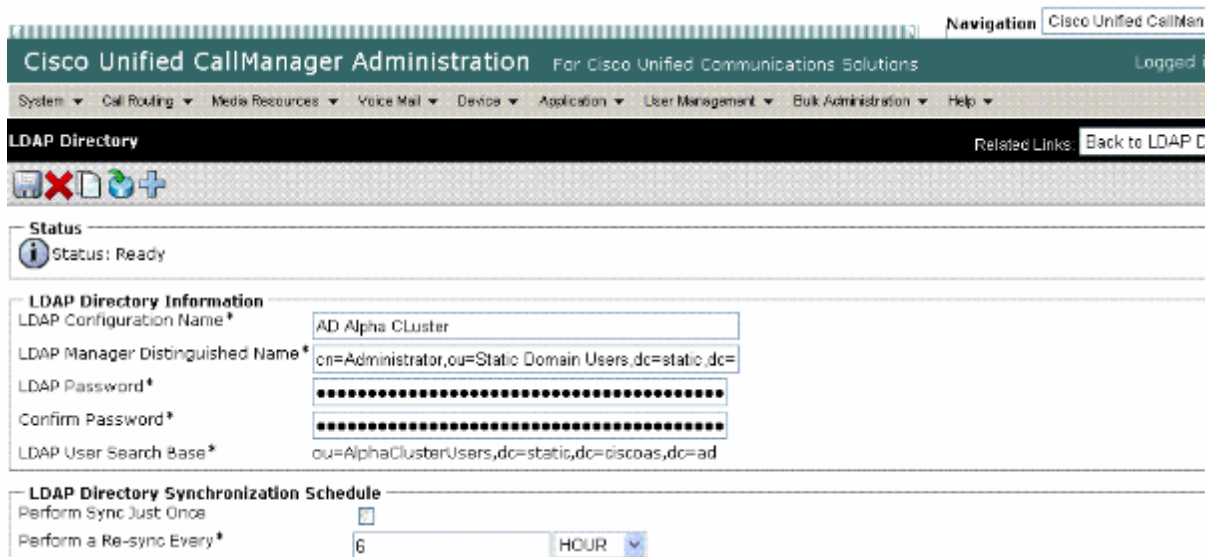
During the import of accounts, no passwords or PINs are copied from the LDAP directory to the Unified CM database. If LDAP synchronization is not enabled in Unified CM, the password for the end user is managed by using Unified CM Administration. The password and PIN are stored in an encrypted format in the Unified CM database. The PIN is always managed on Unified CM.

The connection between the Unified CM publisher server and the directory server can be secured by enabling Secure LDAP (SLDAP) on Unified CM and the LDAP server. Secure LDAP enables LDAP to be sent over a Secure Socket Layer (SSL) connection and can be enabled by uploading the SSL certificate from within the Unified CM Platform Administration.

Troubleshooting – LDAP Authentication Fails on Distinguished Name

This issue occurs when you use the incorrect LDAP Manager Distinguished Name in the LDAP Directory configuration.

- Make sure that the LDAP Manager Distinguished Name contains the complete canonical name. For example, cn=Administrator,ou=Static Domain Users,dc=static,dc=ciscoas,dc=ad.
- For the LDAP Manager Distinguished Name, you need to enter the user ID, which can be up to 128 characters, of the LDAP Manager, who is an administrative user that has access rights to the LDAP directory.



The screenshot displays the Cisco Unified CallManager Administration web interface. The page title is "Cisco Unified CallManager Administration" with a subtitle "For Cisco Unified Communications Solutions". The navigation menu includes "System", "Call Routing", "Media Resources", "Voice Mail", "Devices", "Application", "User Management", "Bulk Administration", and "Help". The current page is "LDAP Directory", with a "Related Links" section containing "Back to LDAP C".

The "LDAP Directory" section includes a "Status" indicator showing "Status: Ready". Below this is the "LDAP Directory Information" section, which contains the following fields:

- LDAP Configuration Name*: AD Alpha Cluster
- LDAP Manager Distinguished Name*: cn=Administrator,ou=Static Domain Users,dc=static,dc=
- LDAP Password*: [Redacted]
- Confirm Password*: [Redacted]
- LDAP User Search Base*: ou=AlphaClusterUsers,dc=static,dc=ciscoas,dc=ad

The "LDAP Directory Synchronization Schedule" section includes the following options:

- Perform Sync Just Once:
- Perform a Re-sync Every*: 6 HOUR

Figure 6. LDAP Directory Distinguished Name Verification

Conclusion

Directories are specialized databases that are optimized for a high number of reads and searches, and occasional writes and updates. Directories typically store data that does not change often, such as employee information, user policies, user privileges, and group membership on the corporate network.

Directories are extensible, meaning that the type of information stored can be modified and extended. The term directory schema defines the type of information stored, its container (or attribute), and its relationship to users and resources.

Summary

The Lightweight Directory Access Protocol (LDAP) provides applications with a standard method for accessing and potentially modifying the information stored in the directory. This capability enables companies to centralize all user information in a single repository available to several applications, with a remarkable reduction in maintenance costs through the ease of moves, adds, and changes (i.e., MAC). This is the benefit of associating the Call Manager cluster to the existing or new Active Directory database.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses:

[ACUCW1 – Administering Cisco Unified Communications Workspace Part 1: Basic](#)

[ACUCW2 – Administering Cisco Unified Communications Workspace Part 2: Advanced](#)

[CIPT1 v6.x/7.x – Implementing Cisco Unified Communications IP Telephony Part 1](#)

For more information or to register, visit www.globalknowledge.com or call **1-800-COURSES** to speak with a sales representative.

Our courses and enhanced, hands-on labs and exercises offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 1,200 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and business training needs.

About the Author

Currently, Mr. McInville is a Certified Cisco Systems Instructor (CCSI #31293) for Cisco Learning Partner Global Knowledge as well as contract consultant. As an instructor, he is responsible for training students worldwide and consulting in the deployment of routing, switching, and IP Telephony solutions. Previously, Mr. McInville was a Solutions Engineer for EDS for the Bank of America voice transformation project. Prior to EDS, Mr. McInville was a Senior Network Engineer for iPath Technologies based in Reston, VA. In this role, he provided technical training and professional services to Service Providers and Enterprise users of Juniper Networks routing and security product line. During this time, Mr. McInville earned his Juniper Networks Certified Internet Professional (JNCIP #297) certification. Prior to iPath, Mr. McInville was the Lead Technical Consultant (LTC) for the Carolina's region of Dimension Data, NA. As an LTC, his responsibilities included the support and guidance to five engineers and technicians involved in the consultation, implementation, delivery and training of VoIP and IP Telephony solutions as well as high-level routing and switching designs. In his spare time, Mr. McInville and his beautiful wife Lupe enjoy riding their Harley-Davidson near their home in Kershaw, SC.