WHITE PAPER

ENTERPRISE LAYER 3 MOBILITY SOLUTION—USING CISCO MOBILE IP ZERO CONFIGURATION CLIENT

This document describes an Enterprise Layer 3 mobility solution using the standard-based Mobile IP protocol, Cisco Dynamic Security Association and Key Distribution feature, and Dynamic Host Configuration Protocol (DHCP) option 68.

PART I: SOLUTION OVERVIEW

1.0 Background—Layer 3 Mobility and Mobile IP

Today, enterprises are deploying wireless local area networks (WLAN) to meet their employees' mobility requirements and to boost company productivity. WLAN allows employees to stay connected while moving around their workplace. While deploying WLAN improves company productivity, it also introduces some challenges in the user's mobility experiences. For example, users' application may be interrupted (i.e:. lost of packets) every time when they switch between a high-speed Ethernet and WLAN connection. Users may require re-authenticating and re-login network applications when they roam out of a network boundary (i.e.: subnet boundary). These two scenarios introduce a new question to network administrators – how to help users to maintain their application connections, while they are switching between wired and wireless networks and across IP subnets, and thus further boost the productivity?

Mobile IP is a standard technology that can address the aforementioned challenges. It provides smooth uninterrupted application continuity to mobile users, while they are roaming either between different network media (i.e. Ethernet and WLAN) or across various IP subnets. Mobile IP achieves seamless application connectivity by providing a fixed IP address to a mobile device and ensuring its routing reachability, while the device moves across different network media and IP networks. This ensures that application traffic always flows to a current location of the mobile device where the application is running. As a result, it provides users with a seamless IP connectivity and application continuity.

For more Mobile IP information, please refer to References section.

2.0 Cisco Zero Configuration Client Solution Overview

Cisco Zero Configuration Client (ZECC) solution is a Mobile IP based solution for enterprise that requires layer 3 mobility for either IP subnet crossing or media type roaming. The solution is designed to simplify provision efforts for network administrators and ease mobility experiences for end users. To achieve the objectives, the ZECC solution uses Cisco Dynamic Security Associations and Key Distribution feature and standard DHCP option 68, as well as enhancements on Mobile IP client software to support the Cisco Dynamic Security Associations and Key Distribution feature. Currently, Birdstep Mobile IP client software supports the Cisco feature.

Security Associations and Key Provisioning Challenge

Alike many networking protocols, the standard-based Mobile IP requires mobile users to be authenticated by the networks before using IP mobility service. To perform the authentication it requires common security associations and a secure key (a.k.a a pre-share key) between a supplicant (a mobile node) and an authenticator (the Home Agent router). Provisioning common security associations and pre-share key is a known deployment challenge. One simple approach is to manually (or via a password generator software) generate pre-share key and to configure the security associations and key information on a supplicant and its authenticator (or mobile node and Home Agent in the Mobile IP context). While this approach is simple, it is also time consuming and error-prone for medium and large scale deployments. If there are thousands of mobile devices, a network administrator would need to provision, distribute, and configure the thousands of security associations and keys on the mobile devices.

Security Associations and Key Provisioning Simplified Using Cisco Dynamic Security Association and Key Distribution

To address the provisioning challenge, the ZeCC solution uses Cisco Dynamic Security Associations and Key Distribution feature. The feature defines a framework that enables Mobile IP Client and Home Agent to use a mobile user's Windows domain login information to perform Mobile IP authentication. Once a user logs in the Windows domain, the mobile node generates security associations and derives a secure key (session key) for Mobile IP. On the Home Agent side it creates the necessary security associations and the secure key based on the user's login information from a Windows Domain Controller. This effectively eliminates the need to provision a new key for a mobile user to use Layer 3 mobility service.

Network Configurations Challenge

It is not uncommon for networking client software to configure some settings for a proper operation. Similarly, Mobile IP client software also needs some network settings before it can operate properly. Configurations can be done by the mobile users when the user installs the software. Alternatively, the configurations can be stored or preconfigured in the client software prior to delivering them to the user. Making configurations earlier is obviously less desirable, as the user can make mistakes and delay the network deployment. Making configurations later is better, but if the network settings would have changed, the user would still need to be involved and to make the necessary changes.

Network Configurations Simplified Using Cisco Dynamic Security Association and Key Distribution And DHCP Option 68

The ZECC solution eliminates all of the necessary network configurations, such as Domain Name System (DNS) (in the home network of the mobile node) and the network prefix mask (of the home address of the mobile node) for the mobile user. This is accomplished mostly by the "network parameter pushing capability" in Cisco Dynamic Security Associations and Key Distribution feature. The capability allows a Home Agent to push network parameters to a mobile node during the mobile node's initial registration and authentication processes. The network parameter is carried in Mobile IP Vendor Specific Extensions (VSE) in a Registration Reply message (RRP). Because the network configurations are pushed from the networks, changes on them do not require end users to be aware.

The only remaining network setting that the feature cannot use effectively is the Home Agent address. This happens because the client needs to know how to access the Home Agent router before sending a registration request (RRQ). This "chicken and egg" problem is solved by using DHCP option 68. The DHCP option 68 is a standard DHCP option that allows a DHCP server to return a Home Agent address during normal DHCP processes. Thus, when a mobile node boots up and starts the DHCP process, it acquires the DHCP IP address as well as the Home Agent address.

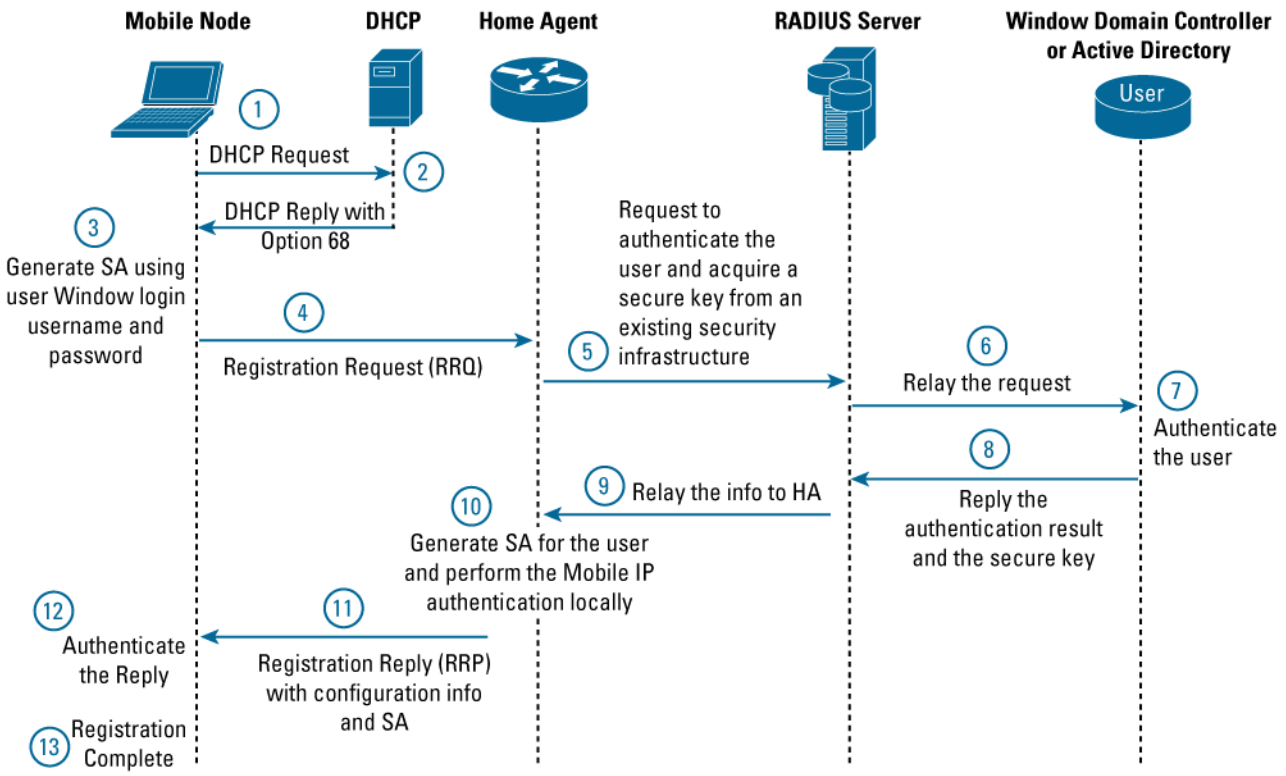
Furthermore, by being able to activate the Mobile IP client software along with the Window login process, the solution essentially creates a "plug and play" experience for end users. Users would only need to login one time* for both: their Windows domain login and Layer 3 mobility service. This provides a good "user transparency" for mobile users to enjoy Layer 3 mobility service.

With the combination of Cisco Dynamic Security Association and Key Distribution feature and DHCP option 68, a mobile user no longer needs any configurations or additional procedures to enjoy IP mobility service after installing Mobile IP client software. Yet, a network administrator does not need to provision an additional pre-shared key and security associations for Mobile IP. This greatly simplifies enterprise IP mobility deployment.

Figure 1 provides more details about the authentication processes using the ZECC solution. A brief description of this process follows the figure.

* Similar to Cisco LEAP login process, where users can login into both: Windows domain and WLAN services at the same time. Now with this new feature, a mobile user can login to the Windows domain, WLAN, and Mobile IP all at once.

Figure 1. ZECC Operation Overview


Mobile Node
DHCP
Home Agent
RADIUS Server
Window Domain Controller or Active Directory
User
1
DHCP Request
2
DHCP Reply with Option 68
3
Generate SA using user Window login username and password
4
Registration Request (RRQ)
5
Request to authenticate the user and acquire a secure key from an existing security infrastructure
6
Relay the request
7
Authenticate the user
8
Reply the authentication result and the secure key
9
Relay the info to HA
10
Generate SA for the user and perform the Mobile IP authentication locally
11
Registration Reply (RRP) with configuration info and SA
12
Authenticate the Reply
13
Registration Complete

Note: Steps 6, 7, and 8 are optional. If the user data is stored in Access Control Server (ACS) database, those steps are not necessary.

Step 1. Mobile node sends DHCP requests to DHCP server.

Step 2. DHCP server responds to the requests and includes DHCP optional 68 information.

Step 3. User logins to Windows Domain normally. Mobile IP client on the mobile node generates MS-CHAPv2* information based on the user's Windows login password.

Step 4. Mobile node carries the MS-CHAPv2 information in Vendor Specific Extensions (VSE) of an RRQ and sends it to Home Agent. The RRQ also contains Mobile-Home Authentication Extension (MHAE) extension, which is a mandatory Mobile IP authentication extension.

Step 5. Home Agent processes the RRQ** and relays*** the MS-CHAPv2 information to a Radius server using a Radius Access-Request message for user authentication.

Step 6. Radius server relays the Access-Request message to a selected Domain Controller or Active Directory to authenticate the user.

* The MS-CHAPv2 is the method to authenticate a mobile user in the initial registration process. The subsequent re-registration does not use MS-CHAPv2.

** The Home Agent differentiates the special RRQ from the normal MHAE by examining the special key distribution VSE existence.

*** Here it assumes that the home agent does not have the Security Parameter Index (SPI) for the mobile node, and thus relays to a backend authentication server.

Step 7. The Domain Controller/Active Directory authenticates the user successfully.

Step 8. The DC/AD replies to the authenticated result and sends secure key (double hashed of the user's password) to the Radius server.

Step 9. Radius server, which has configured the return of MS-CHAP-MPPE key attribute, relays the secure key to Home Agent via an Access-Accept message.

Step 10. Home Agent upon receiving the Access-Accept message derives another key, known as a session key, based on the received secure key from the Radius server. Home Agent authenticates the MHAE based on the derived session key and creates Mobile IP binding. Home Agent discards the original secure key from the Radius server and only keeps the session key.

Step 11. Home Agent sends RRP with network configuration parameters and security associations (DNS server IP address and Home Agent-mobile node security parameter index (SPI)) to mobile node.

Step 12. Mobile node authenticates the RRP.

Step 13. Mobile node completes the initial registration process and can start send and receive mobile data traffic.

Note: The mobile node would periodically re-register with the Home Agent. The authentication for the re-registration is based on the session key and the dynamically generated SA between the Home Agent and a mobile node. It does not involve Radius and Domain Controller/Active Directory.

3.0 Benefits

- Seamless application continuity between different media access networks, such as Ethernet and WLAN, and across IP subnet boundary
- Plug and Play mobility experience for end users: no client configurations and no mobile service login is required (the mobile service authentication is incorporated with user's Windows domain login)
- Light-weighted network provisioning for network administrator: no need to provision secure associations and pre-shared key; only one additional router is needed to enable the service
- Enhanced mobility security through dynamic re-keying

4.0 ZECC Solution System Requirements

- Mobile IP Home Agent router with Dynamic Security Association and Key Distribution feature—any Cisco routers running Cisco IOS® Software Release 12.3(7)T* with IP plus feature set
- Mobile Node—PC running Windows O.S with Mobile IP client software that supports ZECC features.
  - Currently, the Birdstep vendor provides the Cisco ZECC enabled Mobile IP client. Please contact Birdstep (www.birdstep.com) for the product availability.
- Radius Server—For example, Cisco ACS server 3.2
- Windows Domain Controller (or Active Directory)
- DHCP Server with option 68 support

* The feature is available in Cisco IOS Software Release 12.3(4)T. However, as there is an implementation improvement for the feature after Release 12.3(4)T, it is recommended to use Release 12.3(7).

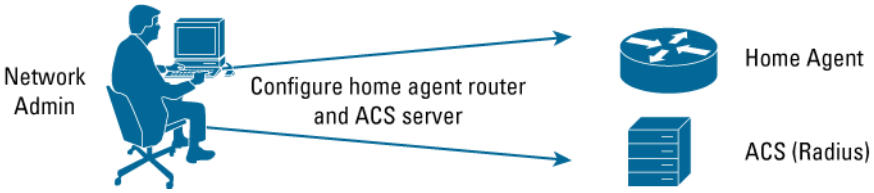
PART II: DEPLOYMENT

5.0 Deployment Overview

Deploying the ZECC Layer 3 mobility solution can be divided into three simple tasks that are described below:

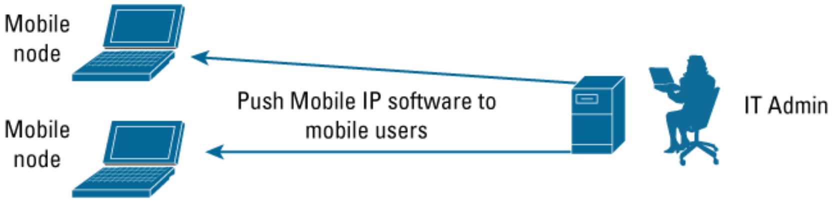
Task 1:

Network administrators provision a Home Agent router into the enterprise networks and, if needed, modify the existing ACS (or an equivalent Radius server) configurations.



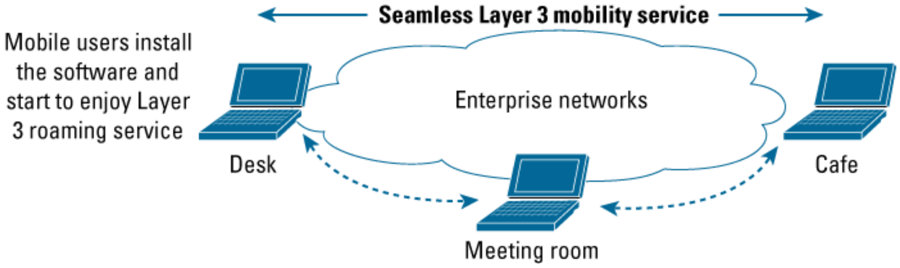
Task 2:

IT administrator pushes Mobile IP client software to mobile users.



Task 3:

Mobile users install the client software and enjoy the Layer 3 mobility service.


Seamless Layer 3 mobility service
Mobile users install the software and start to enjoy Layer 3 roaming service
Enterprise networks
Desk
Cafe
Meeting room

Only task one involves configurations for the network components involved in the ZECC solution. Thus, the next configuration discussion will focus on the task one only.

6.0 Configuration Example

Description

This section provides configuration examples to implement Cisco ZECC Layer 3 Mobility solution. The example is based on the following components:

Hardware Component	Software Component	Function
1 x Cisco 7200VXR Series Router	Cisco IOS Software Release 12.3(7)T with IP plus feature set	Home Agent
1 x Desktop	• Cisco ACS 3.2 • Windows 2000 server (as a DHCP server and a Domain Controller)	• Radius Server • Domain Controller • DHCP Server
1 x Laptop	Birdstep Mobile IP Client v2.1.2.20020	Mobile Node

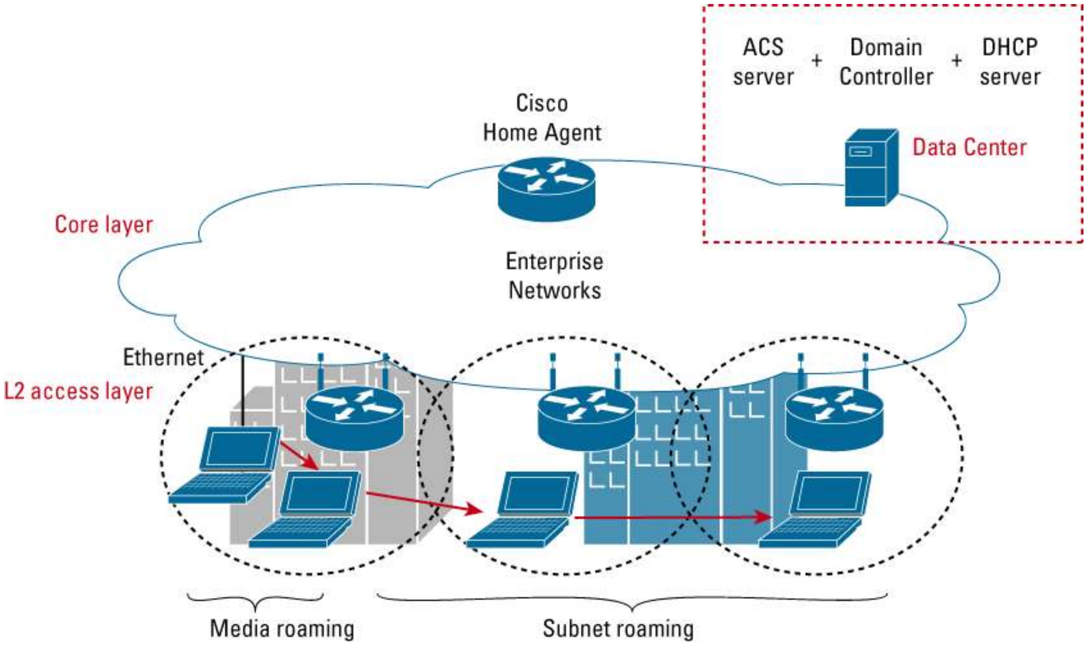
The Cisco 7200VXR Series Router with Cisco IOS Software Release 12.3(7)T is used as a Home Agent router. It is placed in the core layer of the networks and is accessible by the mobile node. The accessibility is done by assigning a routable IP address (200.1.1.5) to the Home Agent router in the enterprise network. The IP address is used as the Home Agent address.

The desktop PC is loaded with Windows 2000 server and Cisco ACS. It is used as a Windows Domain Controller, DHCP server, and Radius server. It is placed in the data center and is accessible by the Cisco 7200 Series Router (Home Agent). The name of the Windows domain is “MOBILEIP”.

The laptop is loaded with a Birdstep Cisco ZECC Mobile IP client. It is used as the mobile node and located in Layer 2 access layer, where both Ethernet and WLAN network access are available. The IP addressing for the subnets (foreign) in the L2 access layers are served by the DHCP server in the data center.

Figure 2 below illustrates the sample topology.

Figure 2. Sample Network Topology



Configuration

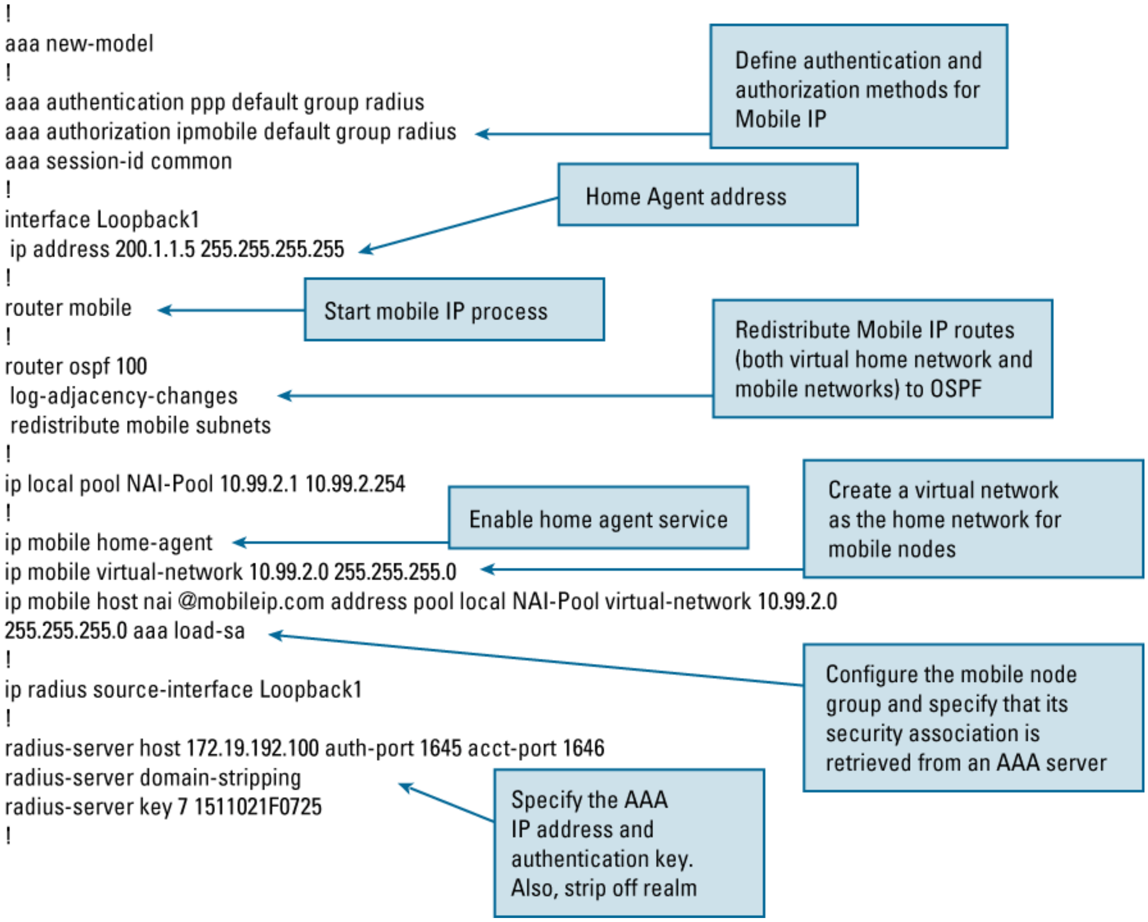
The configuration example assumes the following:

- Windows Domain controller or Active Directory already has Windows login information for the mobile user. This should be true for most enterprise networks.
- DHCP server is configured to provide IP addressing for the foreign subnets, where the mobile user will boot the mobile node.
- ACS server belongs to the same Windows Domain as the Windows Domain Controller.

Home Agent Configuration

There is no special ZECC configuration required on a Home Agent router to enable the solution. A Home Agent with generic Home Agent router configuration can support the solution and should not need to modify its configurations. Home Agent should be aware of authentication, authorization, and accounting (AAA) server, and AAA server should be reachable from Home Agent. Below is a generic Home Agent configuration:

Figure 3. Home Agent Configurations



```
!
aaa new-model
!
aaa authentication ppp default group radius
aaa authorization ipmobile default group radius
aaa session-id common
!
interface Loopback1
 ip address 200.1.1.5 255.255.255.255
!
router mobile
!
router ospf 100
 log-adjacency-changes
 redistribute mobile subnets
!
ip local pool NAI-Pool 10.99.2.1 10.99.2.254
!
ip mobile home-agent
ip mobile virtual-network 10.99.2.0 255.255.255.0
ip mobile host nai @mobileip.com address pool local NAI-Pool virtual-network 10.99.2.0
255.255.255.0 aaa load-sa
!
ip radius source-interface Loopback1
!
radius-server host 172.19.192.100 auth-port 1645 acct-port 1646
radius-server domain-stripping
radius-server key 7 1511021F0725
!
```

Define authentication and authorization methods for Mobile IP

Home Agent address

Start mobile IP process

Redistribute Mobile IP routes (both virtual home network and mobile networks) to OSPF

Enable home agent service

Create a virtual network as the home network for mobile nodes

Configure the mobile node group and specify that its security association is retrieved from an AAA server

Specify the AAA IP address and authentication key. Also, strip off realm

Foreign Agent (Optional)

Foreign Agent is an optional component in Mobile IP. It adds additional management options and improves scalability for Mobile IP networks.

Foreign Agent, similar to a Home Agent, does not require any special configuration on Foreign Agent router to enable the ZECC solution. Foreign Agent supports this solution if it is running Cisco IOS Software Release 12.3(7)T or later with ip plus feature set.

Please refer to References section for the foreign agent configurations.

Cisco ACS Server Configuration

Typically, in a Mobile IP deployment Cisco ACS server is used as an authenticator and offers security associations and pre-share key of a mobile user to a Home Agent (acting as a Network Access Server (NAS)) to authenticate the mobile user. This scheme requires a network administrator to provision the security associations and the key on both: the ACS server's local database and the mobile user's Mobile IP client software. As discussed in Part I, this can be a deployment challenge. Cisco ZECC L3 mobility solution addresses this deployment challenge by using the mobile user's Windows domain login information located in either a Windows domain controller or Active Directory.

Below is an example how to configure Cisco ACS server to use a Windows domain controller for mobile users' authentication.

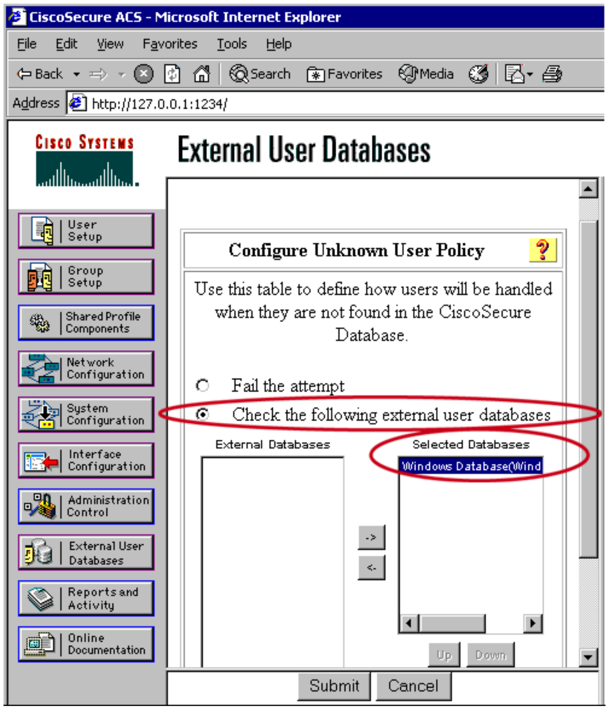
Note: The ACS server does not need to be configured if it has already used Windows domain controller to authenticate a network user. In this case, make sure the user profile or the group profile of the user is configured to return MS-CHAP-MPPE attribute. To see how to configure this, go to "Enable MS-CHAP-MPPE attribute for the ACS group" section below.

1. Configuring Unknown User Policy

If the realm stripping is not configured on the Home Agent, it uses "Domain\username" format or "Domain\usernam.realm" format to identify a Mobile IP user. The format is used in the username attribute in the Access-Request message sent to the ACS server. The ACS server treats the user as an unknown user (assuming there is no identical username configured in its local user database). Thus, the ACS server needs to be instructed how and where to authenticate an unknown user.

To perform this task click External User Databases>Unknown User Policy. A window similar to the following should appear.

Figure 4. Configure Unknown User Policy in ACS



External User Databases

Configure Unknown User Policy

Use this table to define how users will be handled when they are not found in the CiscoSecure Database.

○ Fail the attempt

● Check the following external user databases

External Databases	Selected Databases
	Windows Database(Wind

In the window, move the “Windows Database” from the “External Database” section to the “Selected Database” section and select the “Check the following external user database” radio button.

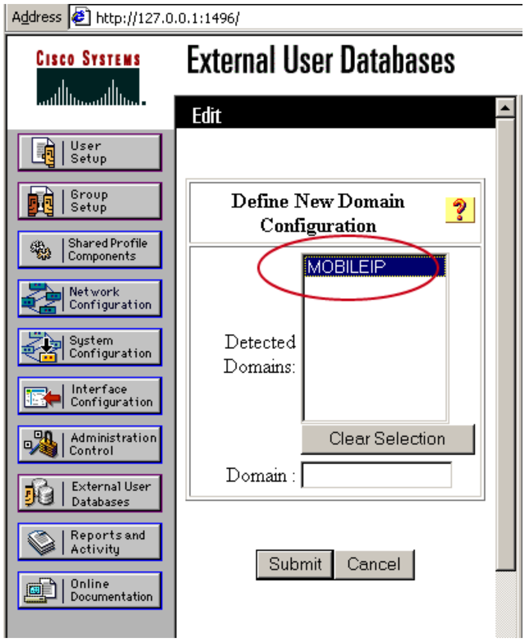
2. Mapping the Unknown User to a ACS Local Group

By default, an unknown user is mapped to the default group in the ACS user database.

In this step the unknown users that belong to a MOBILEIP Windows Domain will be mapped to an ACS group named Mobile-IP.

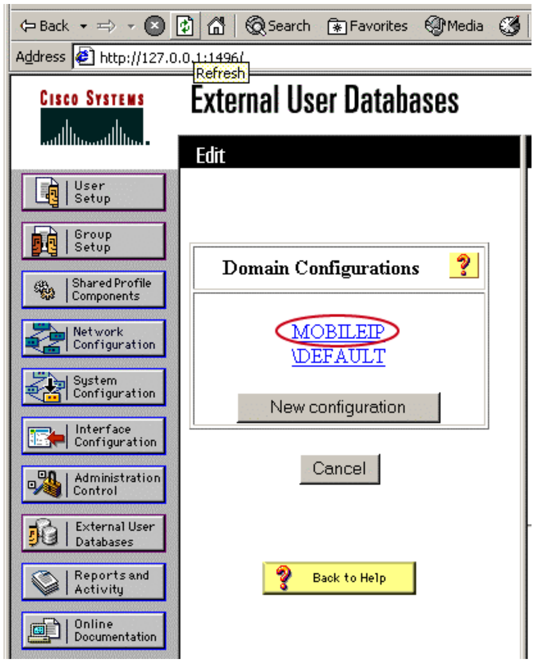
To perform the task click External User Databases>Database Group Mapping>Windows Database>New configuration. In the “Detected Domains” section select the MOBILEIP domain and click submit. Note that ACS server belongs to the “MOBILEIP” domain and automatically detects it.

Figure 5. Adding a New Domain



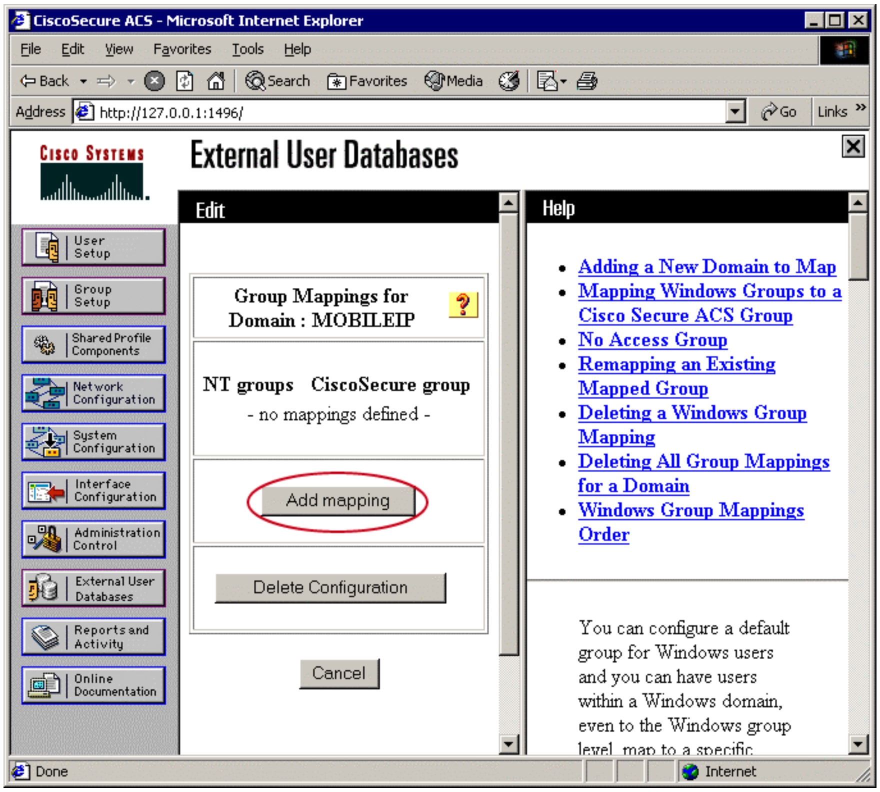
The following window will pop up with MOBILEIP added in the domain configurations. Click the MOBILEIP.

Figure 6. Two External Domains—MOBILIP and DEFAULT



The following window pops up next. To add the Windows domain group to an ACS group click on “Add mapping”.

Figure 7. Windows Domain Group and ACS Group Mapping



Group Mappings for Domain : MOBILEIP

NT groups CiscoSecure group

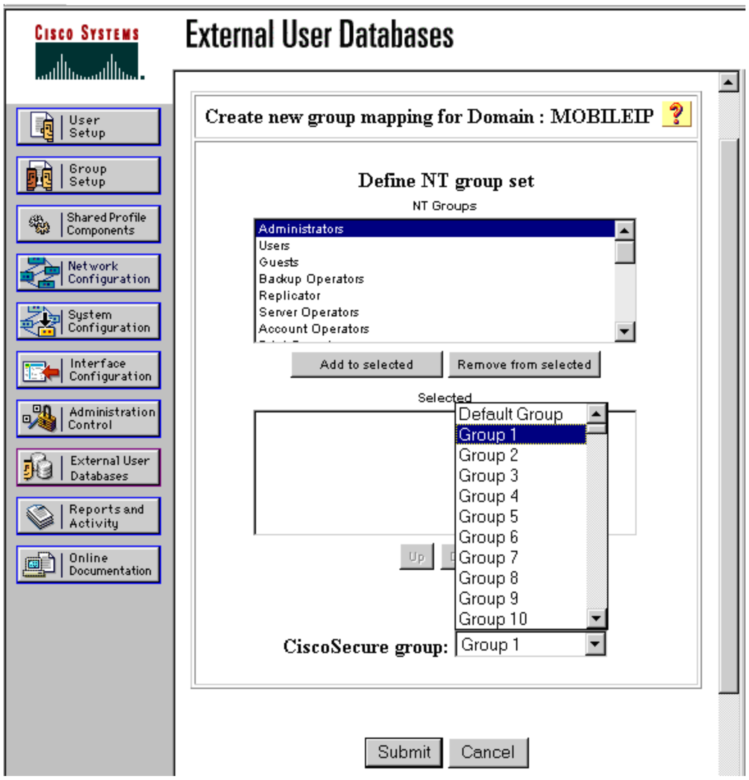
- no mappings defined -

- Adding a New Domain to Map
- Mapping Windows Groups to a Cisco Secure ACS Group
- No Access Group
- Remapping an Existing Mapped Group
- Deleting a Windows Group Mapping
- Deleting All Group Mappings for a Domain
- Windows Group Mappings Order

You can configure a default group for Windows users and you can have users within a Windows domain, even to the Windows group level, map to a specific

Select an ACS group (CiscoSecure Group)—Group1—to map to the Windows groups in the MOBILEIP domain. Then click Submit.

Figure 8. Mapping ACS Group 1 to Windows MOIBLIEIP Group



External User Databases

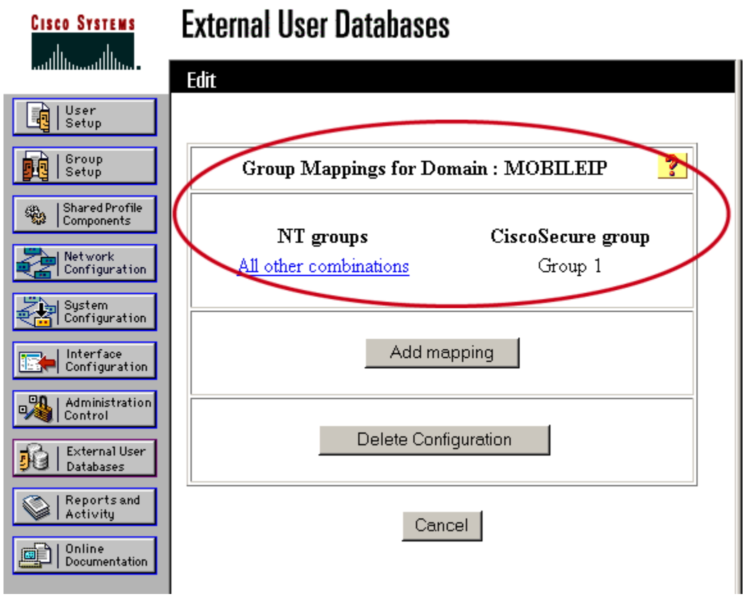
Create new group mapping for Domain : MOBILEIP

Define NT group set

CiscoSecure group: Group 1

The following window should pop indicating all Windows groups in Domain MOBILEIP maps to the ACS Group 1.

Figure 9. Group Mapping Result



External User Databases

Edit

Group Mappings for Domain : MOBILEIP

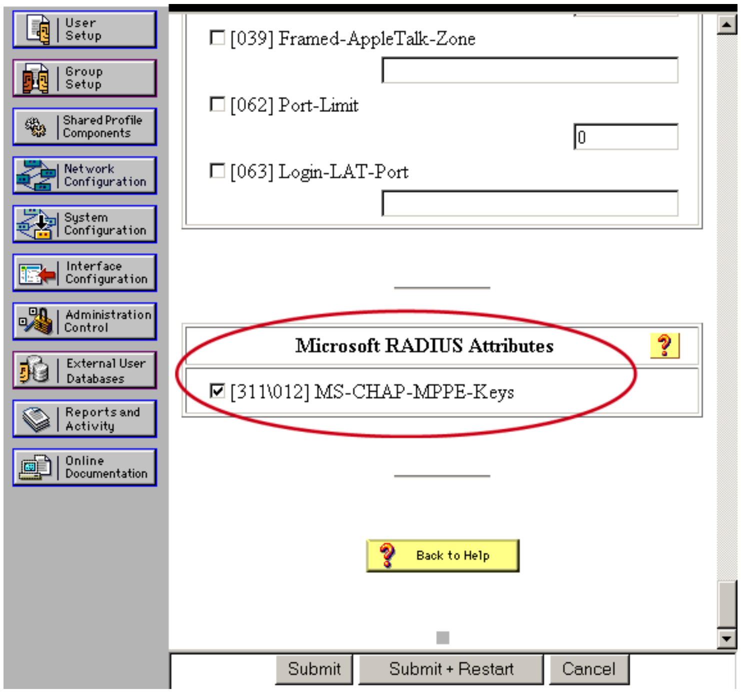
NT groups	CiscoSecure group
All other combinations	Group 1

3. Enabling MS-CHAP-MPPE Attribute forthe ACS Group

Once the Windows Domain authenticates the user, the Windows Domain Controller will return a secure key (hash of the hash of Windows login password) to the ACS server. Then ACS server will need to relay the secure key to the Home Agent. This secure key is known as MS-CHAP-MPPE-Keys under the Microsoft Radius attribute. The ACS needs to be instructed to return the secure key for the authenticated user to the Home Agent.

To perform the task, click Group Setup and select Group 1. Find “Microsoft Radius Attributes” section and check the MS-CHAP-MPPE-Keys radio button as shown below.

Figure 10. Check MS-CHAP-MPPE Key



□ [039] Framed-AppleTalk-Zone

□ [062] Port-Limit 0

□ [063] Login-LAT-Port

Microsoft RADIUS Attributes

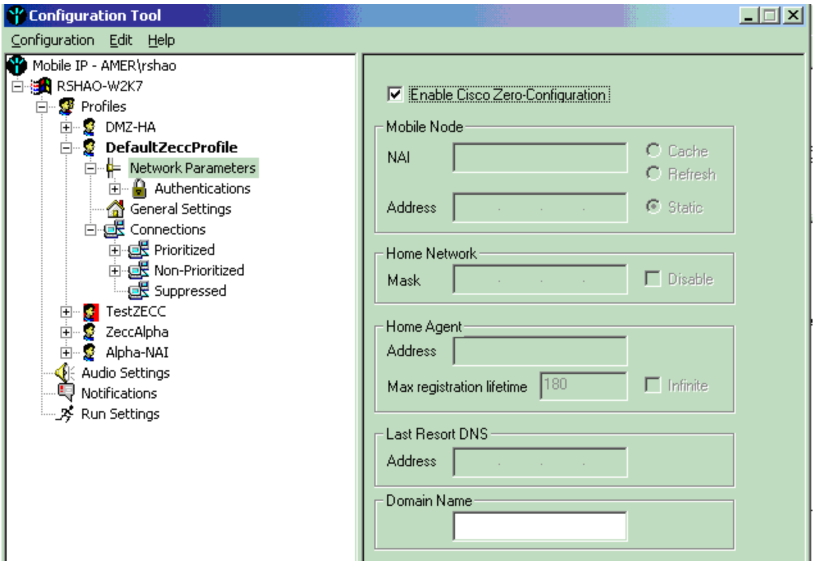
☑ [311\012] MS-CHAP-MPPE-Keys

Mobile Device

Mobile device does not need any configuration. After installing the Birdstep Mobile IP client, the client software will prompt the user to select available network interfaces to be used for roaming. Select interfaces for Mobile IP client use.

Settings can be confirmed from the Birdstep Configuration Tool. Below is the screen capture from the Tool.

Figure 11. Birdstep Configuration Tool



☑ Enable Cisco Zero-Configuration

Mobile Node
NAI
Address
○ Cache
○ Refresh
● Static

Home Network
Mask
☐ Disable

Home Agent
Address
Max registration lifetime 180
☐ Infinite

Last Resort DNS
Address

Domain Name

A "DefaultZECCProfile" is created automatically on the left side of the window. The "Enable Cisco Zero-Configuration" box is checked in the right side of the window.*

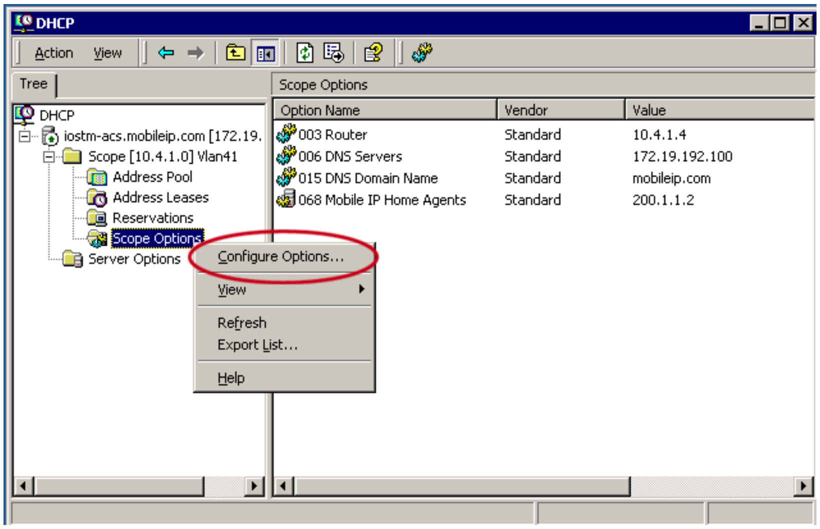
* Note that client used an evaluation release from Birdstep for the ZECC support. The final version of the client may have different appearance and setup procedures. Contact Birdstep for the setup details if a different setup procedure is experienced.

DHCP Server Configuration

Below is an example on how to configure the option 68 on a Windows 2000 DHCP server. The DHCP server has configured 200.1.1.2 as the Mobile IP Home Agent address.

To configure the Home Agent address, right click Scope Options>Configuration Options and then select option 68. Enter Home Agent address in the IP address field and click Add>OK.

Figure 12. Windows DHCP Server Configuration Tool



Option Name	Vendor	Value
003 Router	Standard	10.4.1.4
006 DNS Servers	Standard	172.19.192.100
015 DNS Domain Name	Standard	mobileip.com
068 Mobile IP Home Agents	Standard	200.1.1.2

7.0 References

- Mobile IP Dynamic Security Association and Key Distribution: http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d2d6e.html
- Cisco IOS Software Mobile IP: http://www.cisco.com/warp/public/732/Tech/mobile/ip/
- Configuring Mobile IP: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfmobip.htm

APPENDIX—DEBUG OUTPUTS

Below is a “debug ip mobile” output captured from Home Agent when a Cisco ZECC-enabled mobile node is first registered with it.

Debug ip mobile output

```
R26-RA#
! HA receives RRQ and parse the NAI VSE (131)
*Sep 10 02:01:56.193: MobileIP: ParseRegExt type NAI(131) addr 7C0474C end 7C04813
*Sep 10 02:01:56.193: MobileIP: ParseRegExt skipping 19 to next
! HA parses the RRQ with NVSE (134) vendor NVSE for key distribution (15) along with
! various subtypes.  Home Agent uses this extension to differentiate “ZECC” RRQ from
! regular  MHAE only  RRQ
*Sep 10 02:01:56.193: MobileIP: ParseRegExt type NVSE(134) addr 7C04761 end 7C04
813, type key distribution NVSE(15) subtype 5 (session identifier) session id MOIP-IBMC1, size 10
*Sep 10 02:01:56.193: MobileIP: ParseRegExt skipping 22 to next
*Sep 10 02:01:56.193: MobileIP: ParseRegExt type NVSE(134) addr 7C04779 end 7C04
```

```
813, type key distribution NVSE(15) subtype 1 (root key) spi 1127, algorithm HMAC-MD5, replay
protection timestamps
*Sep 10 02:01:56.193: MobileIP: ParseRegExt skipping 18 to next
*Sep 10 02:01:56.193: MobileIP: ParseRegExt type NVSE(134) addr 7C0478D end 7C04
813, type key distribution NVSE(15) subtype 2 (session key) spi 1128, algorithm
HMAC-MD5, replay protection timestamps
*Sep 10 02:01:56.197: MobileIP: ParseRegExt skipping 18 to next
*Sep 10 02:01:56.197: MobileIP: ParseRegExt type NVSE(134) addr 7C047A1 end 7C04
813, type key distribution NVSE(15) subtype 3 (challenge) challenge size 16, cha
llenge c801010ac8010105c3090494c5c10060
*Sep 10 02:01:56.197: MobileIP: ParseRegExt skipping 28 to next
*Sep 10 02:01:56.197: MobileIP: ParseRegExt type NVSE(134) addr 7C047BF end 7C04
813, type key distribution NVSE(15) subtype 4 (windows domain) domain name MOBILEIP, size 8
*Sep 10 02:01:56.197: MobileIP: ParseRegExt skipping 20 to next
*Sep 10 02:01:56.197: MobileIP: ParseRegExt type NVSE(134) addr 7C047D5 end 7C04
813, type key distribution NVSE(15) subtype 6 (authentication response) auth protocol in S key SA -
MS-CHAPv2
*Sep 10 02:01:56.197: MobileIP: ParseRegExt skipping 38 to next
*Sep 10 02:01:56.197: MobileIP: ParseRegExt type MHAE(32) addr 7C047FD end 7C048
13
*Sep 10 02:01:56.197: MobileIP: ParseRegExt skipping 20 to next
*Sep 10 02:01:56.201: MobileIP: HA 154 rcv registration for MN alpesh@mobileip.c
om on FastEthernet0/0 using HomeAddr 0.0.0.0 COA 200.1.1.5 HA 200.1.1.10 lifetim
e 180 options sbdmg-t- identification C3090494C5C10060
*Sep 10 02:01:56.201: MobileIP: Authenticating response for MN alpesh@mobileip.com, protocol MS-
CHAPv2
*Sep 10 02:01:56.201: MobileIP: Username for AAA request is MOBILEIP\alpesh@mobileip.com
*Sep 10 02:01:56.201: MobileIP: Key Gen chap id is 1177881130
*Sep 10 02:01:56.201: MobileIP: MS-Chapv2 response is 33a4e93e3db65e28b2cee43978
ad500c0000000000000000d428cae93c0a22b2d10424a4f5f677fc8730cf0c1c277f3d
*Sep 10 02:01:56.201: MobileIP: Generating dynamic key using AAA infrastructure
! HA sends out Access-Request message
*Sep 10 02:01:56.205: RADIUS(0000000F): Config NAS IP: 200.1.1.10
*Sep 10 02:01:56.205: RADIUS/ENCODE(0000000F): acct_session_id: 15
*Sep 10 02:01:56.205: RADIUS(0000000F): sending
*Sep 10 02:01:56.205: RADIUS(0000000F): Send Access-Request to 172.19.192.100:1645 id 1645/61, len
131
*Sep 10 02:01:56.205: RADIUS:  authenticator C8 01 01 0A C8 01 01 05 - C3 09 0494 C5 C1 00 60
! Note the User-Name has “domain+username” format  i.e. “MOBILEIP\alpesh” without
! realm in the end.
*Sep 10 02:01:56.205: RADIUS:  User-Name           [1]   17  "MOBILEIP\alpesh"
*Sep 10 02:01:56.209: RADIUS:  Vendor, Microsoft   [26]  24
*Sep 10 02:01:56.209: RADIUS:   MSCHAP_Challenge   [11]  18
```

```
*Sep 10 02:01:56.209: RADIUS:   C8 01 01 0A C8 01 01 05 C3 09 04 94 C5 C1 00 60 [???????????????`]
*Sep 10 02:01:56.209: RADIUS:  Vendor, Microsoft   [26]  58
*Sep 10 02:01:56.209: RADIUS:   MS-CHAP-V2-Response[25]  52  *
*Sep 10 02:01:56.209: RADIUS:  Service-Type        [6]   6   Framed       [2]
*Sep 10 02:01:56.209: RADIUS:  NAS-IP-Address      [4]   6   200.1.1.10
! HA receives Access-Accept message from ACS with various attributes
! including MS-CHAPv2 MPPE key
*Sep 10 02:01:56.281: RADIUS: Received from id 1645/61 172.19.192.100:1645, Access-Accept, len 161
*Sep 10 02:01:56.281: RADIUS:  authenticator 80 57 A0 B1 B3 8C D3 68 - 64 3F 35 95 DF 2D 7F AB
*Sep 10 02:01:56.281: RADIUS:  Vendor, Microsoft   [26]  51
*Sep 10 02:01:56.281: RADIUS:   MS-CHAP-V2-Sucess  [26]  45  "*S=64C89F7A313119A
7A4577FD8065C999D491FFE11"
*Sep 10 02:01:56.281: RADIUS:  Vendor, Microsoft   [26]  40
*Sep 10 02:01:56.281: RADIUS:   MS-CHAP-MPPE-Keys  [12]  34  *
*Sep 10 02:01:56.281: RADIUS:  Framed-IP-Address   [8]   6   255.255.255.255
*Sep 10 02:01:56.285: RADIUS:  Class               [25]  44
*Sep 10 02:01:56.285: RADIUS:   43 49 53 43 4F 41 43 53 3A 30 30 30 30 34 64 62
 [CISCOACS:00004db]
*Sep 10 02:01:56.285: RADIUS:   33 2F 63 38 30 31 30 31 30 61 2F 4D 4F 42 49 4C
 [3/c801010a/MOBIL]
*Sep 10 02:01:56.285: RADIUS:   45 49 50 5C 61 6C 70 65 73 68 [EIP\alpesh]
*Sep 10 02:01:56.285: RADIUS(0000000F): Received from id 1645/61
! HA processes the MPPE key and derives a root key and session key (S’).
*Sep 10 02:01:56.289: MobileIP: Key information retrieved from AAA is a00b9194be
db81fea7f0de81ce8ee8049232244573ccc229 len 24
*Sep 10 02:01:56.289: MobileIP: In HA, K'' is 00000000000000009232244573ccc229
*Sep 10 02:01:56.289: MobileIP: HA processing registration from MN alpesh@mobileip.com after AAA
Access-Accept
*Sep 10 02:01:56.289: MobileIP: Root spi 1127 (0x467), key 0947dae610daca8bb424266231f391d5
*Sep 10 02:01:56.289: MobileIP: Key material for S' is 0947dae610daca8bb42426623
1f391d5010000b400000000c801010ac8010105c3090494c5c10060
*Sep 10 02:01:56.289: MobileIP: Session spi 1128 (0x468), key d637f44af466a5a2931bb448b0b7cb05
*Sep 10 02:01:56.293: MobileIP: Refreshed the session key
*Sep 10 02:01:56.293: MobileIP: Name for local pool is MOIP-IBMC1.alpesh
*Sep 10 02:01:56.293: MobileIP: Addr alloc 65.1.1.1 from Local Dynamic pool
*Sep 10 02:01:56.293: MobileIP: Mobility binding for MN alpesh@mobileip.com session-id MOIP-IBMC1
created
*Sep 10 02:01:56.293: MobileIP: Tunnel0 (IP/IP) created with src 200.1.1.10 dst 200.1.1.5
*Sep 10 02:01:56.297: MobileIP: MN alpesh@mobileip.com Insert route for 65.1.1.1
/255.255.255.255 via gateway 200.1.1.5 on Tunnel0
*Sep 10 02:01:56.297: MobileIP: Roam timer started for MN alpesh@mobileip.com se
ssion-id MOIP-IBMC1 using 65.1.1.1, lifetime 180
*Sep 10 02:01:56.297: MobileIP: MN alpesh@mobileip.com session-id MOIP-IBMC1 is now roaming
```

```
*Sep 10 02:01:56.297: MobileIP: Mask for address is 24
*Sep 10 02:01:56.297: MobileIP: HA accepts registration from MN alpesh@mobileip.
com session-id MOIP-IBMC1
! HA prepares RRP with prefix length parameter to mobile nodes.
*Sep 10 02:01:56.297: MobileIP: Added prefix length vse in reply
*Sep 10 02:01:56.297: MobileIP: Authentication algorithm HMAC-MD5 and 16 byte key
*Sep 10 02:01:56.297: MobileIP: MN alpesh@mobileip.com MHAE added to MN alpesh@m
obileip.com using SPI 2ECC
*Sep 10 02:01:56.301: MobileIP: MN alpesh@mobileip.com - HA sent reply to 30.1.3.5.5
*Sep 10 02:01:57.295: MobileIP: swif coming up Tunnel0
*Sep 10 02:01:58.164: MobileIP: agent advertisement byte count = 48
```

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

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA