

• NETWORKERS


NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

1

CISCO SYSTEMS





Cisco.com

Deploying Mobile IP

Session NSC-261

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

3

Prerequisites

Cisco.com

- **NSC-161 Intro to IP Mobility and Mobile IP Configuration**
- **A basic understanding of how Mobile IP and IP routing work**
- **A good understanding of IOS CLI configurations**

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

4

Agenda

Cisco.com

- Integrating Mobile IP into an Enterprise Network
- Deployment Options
- Clients
- IOS Mobile IP References
- Q & A

NSC-261
5065_04_2002_c1

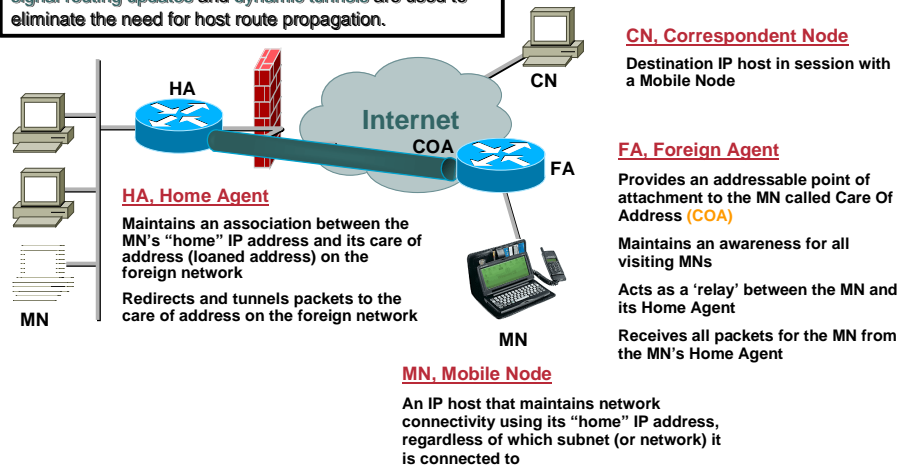
© 2002, Cisco Systems, Inc. All rights reserved.

5

Mobile IP in a Nutshell

Cisco.com

Mobile IP is a dynamic routing protocol where end devices signal routing updates and dynamic tunnels are used to eliminate the need for host route propagation.



NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

6

Acronym Soup

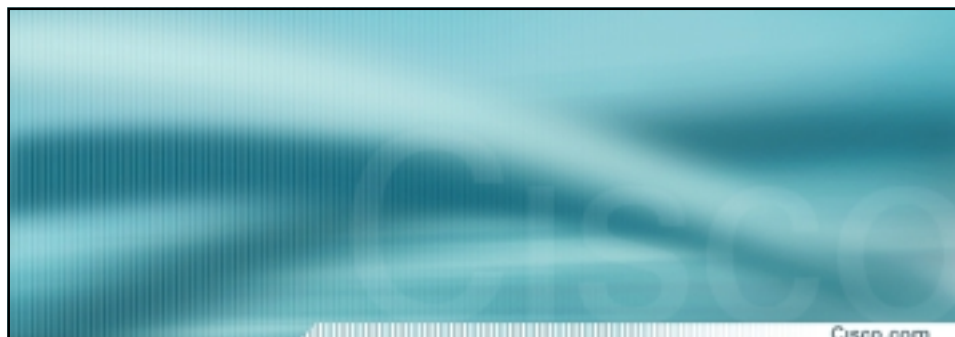
Cisco.com

- **HA**—Home Agent (not High Availability)
The fixed anchor point in the network
- **FA**—Foreign Agent
The local anchor and tunnel end point
- **MN**—Mobile Node
The Mobile Device
- **CoA**—Care of Address
The tunnel destination address
- **CCoA**—Co-located Care of Address
MN is the tunnel end point using a second address

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

7



Cisco.com

Integrating Mobile IP into an Enterprise Network

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

8

Wireless LAN Rollout

Cisco.com

- **Good fixed network design promotes subnetting**
- **Wireless design requires all access points in 1 subnet to achieve mobility**
- **Most people don't want to run a new physical network to support wireless**
- **Mobile IP to the Rescue!**

NSC-261
5065_04_2002_c1

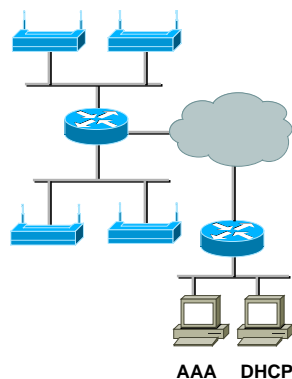
© 2002, Cisco Systems, Inc. All rights reserved.

9

Enterprise Network

Cisco.com

- **Designed to use what is already in place**
- **Most enterprise networks already have AAA and DHCP servers**
- **802.11 is likely 1 subnet per floor or per building**



NSC-261
5065_04_2002_c1

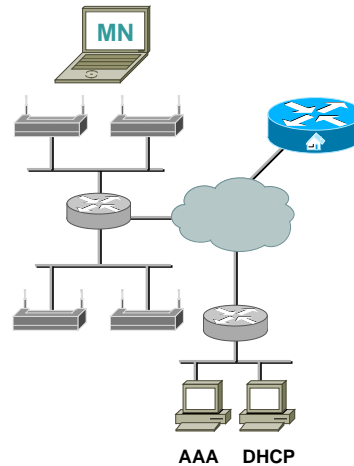
© 2002, Cisco Systems, Inc. All rights reserved.

10

Adding Mobile IP

Cisco.com

- Adding Mobile IP is as simple as adding a HA or enabling the HA on an existing router
- ...And installing client software
- Mobile IP will run in **Co-located Care of Address mode**



NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

11

HA Configuration

Cisco.com

```
aaa new-model
aaa authorization ipmobile default group radius
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255. 0
!
router mobile
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.1.255
ip mobile home-agent
ip mobile host nai @example address pool dhcp-proxy-client
 dhcp-server 10.82.70.10 interface FastEthernet0/0 aaa load-sa
!
radius-server host 10.82.70.12 key itsasecret
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

12

Verifying the HA

Cisco.com

```
HomeAgent#show ip mobile globals
IP Mobility global information:
```

Home Agent

```
Registration lifetime: 10:00:00 (36000 secs)
Broadcast disabled
Replay protection time: 7 secs
Reverse tunnel enabled
ICMP Unreachable enabled
Strip realm disabled
NAT Traversal disabled
```

```
Foreign Agent is not enabled, no care-of address
```

```
1 interface providing service
Encapsulations supported: IPIP and GRE
Tunnel fast switching enabled
Tunnel path MTU discovery aged out after 10 min
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

13

Client Configuration

Cisco.com

- All clients are different
- Minimum configuration

NAI and/or Home address

Home Agent Address

SPI and Key

Enter Network Settings

Network Name: Enterprise Mobile IP

NAI: user@example

Home Address: 8.0.0.0 Mask (in bits): 32

Home Agent: 192.168.1.1

Home Gateway: 192.168.1.1

Tunnel Mode: Tunnel Forward Broadcast

Security Associations

Network: Enterprise Mobile IP

SPI: 0x

Replay Protection: Checksum Auth Method: EspdMGCS

Shared Key: 12 34 56 78 90 AB CD EF 12 34 56 78 90 AB CD EF

OK Apply Cancel

Screenshot from Lifix Go!

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

14

Verifying Registration

Cisco.com

- **Check for a valid binding**

```
HomeAgent#show ip mobile binding nai user@example
Mobility Binding List:
user@example (Bindings 0):
```

- **Check for errors**

```
HomeAgent#show ip mobile host nai user@example
Mobile Host List:
user@example:
  Allowed lifetime 10:00:00 (36000/default)
  Roam status -Unregistered-, Home link on int G3/0
  Accepted 0, Last time -never-
  Overall service time -never-
  Denied 2, Last time 03/18/02 14:49:12
  Last code 'insufficient resources (130)'
  Total violations 1
  Tunnel to MN - pkts 0, bytes 0
  Reverse tunnel from MN - pkts 0, bytes 0
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

15

Common Error Codes

Cisco.com

- **129—Administratively Prohibited**
Denied by an access list
- **130—Insufficient Resources**
Could not assign a Home Address
- **131—Mobile Node Failed Authentication**
Mismatched keys or SPI
- **133—Registration Identification Mismatch**
Clocks out of sync; should retry automatically

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

16

Troubleshooting Registration

Cisco.com

```
HomeAgent#debug ip mobile host nai user@example
IP mobility for mobile node debugging is on
HomeAgent#
MobileIP: ParseRegExt ...
MobileIP: HA 113 rcv registration for MN user@example on
FastEthernet0/0 using HomeAddr 0.0.0.0 COA 10.82.79.18 HA
10.82.79.19 lifetime 7200 options sbdmgt
MobileIP: Authenticating MN user@example using SPI 100
MobileIP: Invalid authenticator for MN user@example
%IPMOBILE-6-SECURE: Security violation on HA from MN user@example
- errcode MN failed authentication (131), reason Bad
authenticator (2)
MobileIP: HA rejects registration for MN user@example - MN failed
authentication (131)
MobileIP: MN user@example MHAЕ added (SPI 100) to MN user@example
MobileIP: MN user@example - HA sent reply to 0.0.0.0
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

17

A Good Binding

Cisco.com

- **user@example has successfully registered and has an active binding**

```
HomeAgent#show ip mobile binding nai user@example
Mobility Binding List:
user@example (Bindings 1):
  Home Addr 192.168.250.10
  Care-of Addr 10.82.79.18, Src Addr 0.0.0.0
  Lifetime granted 02:00:00 (7200), remaining 01:59:33
  Flags sbdmgt, Identification C0696445.7D1FE629
  Tunnel1 src 10.82.79.19 dest 10.82.79.18 reverse-allowed
  Routing Options -
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

18

Adding an FA

Cisco.com

- At a minimum Co-Located Care-of Addressing requires 2 addresses per MN
- Reduces DHCP server load
- Conserves HA tunnel resources
- The Foreign Agent was introduced to help conserve address space
- Mobile IPv6 does not use an FA

NSC-261
5065_04_2002_c1

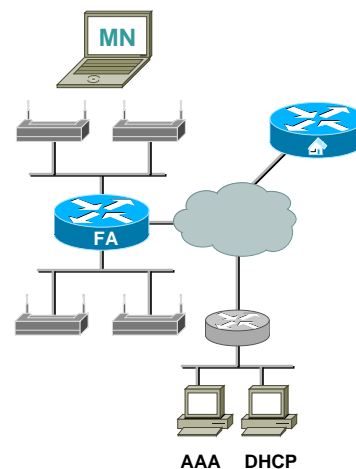
© 2002, Cisco Systems, Inc. All rights reserved.

19

Turning on the FA

Cisco.com

- The FA needs be enabled on all your edge routers
- FA is only minimal overhead
- Reverse tunneling may not be needed inside an enterprise network



NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

20

FA Configuration

Cisco.com

```
interface FastEthernet0/0
 ip address 10.82.79.21 255.255.255.0
 ip irdp
 ip mobile foreign-service
 ip mobile prefix-length
!
interface FastEthernet0/1
 ip address 192.168.101.1 255.255.255.0
 ip irdp
 ip mobile foreign-service
 ip mobile prefix-length
!
router mobile
!
 ip mobile foreign-agent care-of FastEthernet0/0
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

21

Validating the FA

Cisco.com

- **Same basic idea as the Home Agent**
- **Check the global configuration**
`show ip mobile global`
- **Check the visitor tables**
`show ip mobile visitor`

NSC-261
5065_04_2002_c1

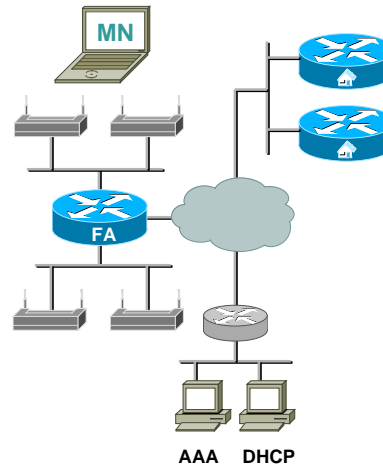
© 2002, Cisco Systems, Inc. All rights reserved.

22

HA Redundancy or “HA HA”

Cisco.com

- **MN does not learn about HA failure until re-registration**
- **Bindings are stateful**
- **HA usually hosts a large number of MNs**
- **Supports Load balancing**
- **Very flexible, but usually used in it's simplest form**



NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

23

HA Redundancy Config

Cisco.com

- **Primary and Secondary must have the same Home Agent configuration**
- **Security Association must be defined between the two Home Agents**

```
interface FastEthernet0/0
ip address 10.82.79.19 255.255.255.240
standby ip 10.82.79.18
standby name mip
!
ip mobile home-agent standby mip
ip mobile secure home-agent 10.82.79.20 spi 100 key hex
1234567890abcdef1234567890abcdef
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

24

FA Redundancy

Cisco.com

- **FA Redundancy is built into the Mobile IP protocol**
- **MN listens for advertisements**
- **Prefix length helps determine if it has moved**
- **Lower IRDP timer to speed failure detection**

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

25

Monitoring and Managing with SNMP

Cisco.com

- **CPU and Memory Utilization (as always) are good indicators of box health**
- **RFC 2006 MIB**
 - Good fault management support
 - Total and per user counters for registrations and errors
- **Cisco Mobile IP MIB**
 - Adds features requested by customers
 - Total number of active bindings
 - NAI support
 - Performance Data
 - Currently an active IETF Draft

NSC-261
5065_04_2002_c1

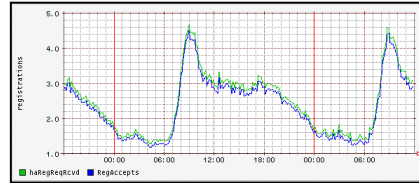
© 2002, Cisco Systems, Inc. All rights reserved.

26

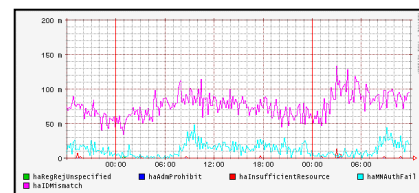
Home Agent Health

Cisco.com

- Watch Registration Rates with **haRegReqRcvd** and **haRegAccepts**
- Watching individual error codes to find wide spread problems
- **Mobile IP traffic patterns are always intuitive**



Registrations Received and Accepted



Registrations Failure Codes

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

27

Home Agent Performance

Cisco.com

- Available via CLI and SNMP

```
HomeAgent>show ip mobile performance
```

Mobile IP Performance:

Messages:

Received Rate:

Last minute 563, 9.3 registration/sec

Peak minute 1067, 17.7 registration/sec

Home Agent:

Processed Rate:

Local registration, total 34150113

Last minute count 545, 9.0 registration/sec

Peak minute 1054, 17.5 reg.../sec, 03/06/02 06:56:42

AAA registration time (ms), total 106930

Most recent 168, minimum 128, maximum 3712, average 254


Last minute count 0, 0.0 registration/sec

Peak minute 464, 7.7 registration/sec, 02/16/02 08:22:15

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

28



Cisco.com

Deployment Options

NSC-261
5065_04_2002_c1 © 2002, Cisco Systems, Inc. All rights reserved. 29

Mobile IP Virtual Networks

Cisco.com

- **Most common configuration**
- **The MN is always roaming; it does not have a physical home network**
- **Works just like a loopback**
- **Mobile IP has more control how packets are handled**

NSC-261
5065_04_2002_c1 © 2002, Cisco Systems, Inc. All rights reserved. 30

Virtual Networks (Cont.)

Cisco.com

- **CLI Config:**

```
ip mobile virtual-network 10.0.0.0 255.255.255.0
```

- **Always represented with network number and mask**

- **Can be redistributed into your IGP**

```
router rip
  redistribute mobile
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

31

NAI

Cisco.com

- **Network Access Identifier**
- **Defined in RFC 2794**
- **Can be either `user` or `user@realm`**
- **CLI Config:**

`user` or `user@realm` identifies a specific user

`@realm` identifies all users in a realm

`@` identifies all users in all realms

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

32

Home Addressing Options

Cisco.com

- Addressing is the most critical part of deployment
- Three Home Address Options
 1. Static Address
 2. Static Address with NAI
 3. Dynamic Address with NAI
- **Any** or **All** can be used on the HA at once

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

33

Static Addressing

Cisco.com

- Traditional RFC 2002-style Mobile IP
- Required for some legacy implementations
- Not used as often as NAI solutions
- MN is identified by its home address
- CLI Config:

```
ip mobile host 10.0.0.10 10.0.0.15 interface F0/0
```
- Home IP address is AAA username

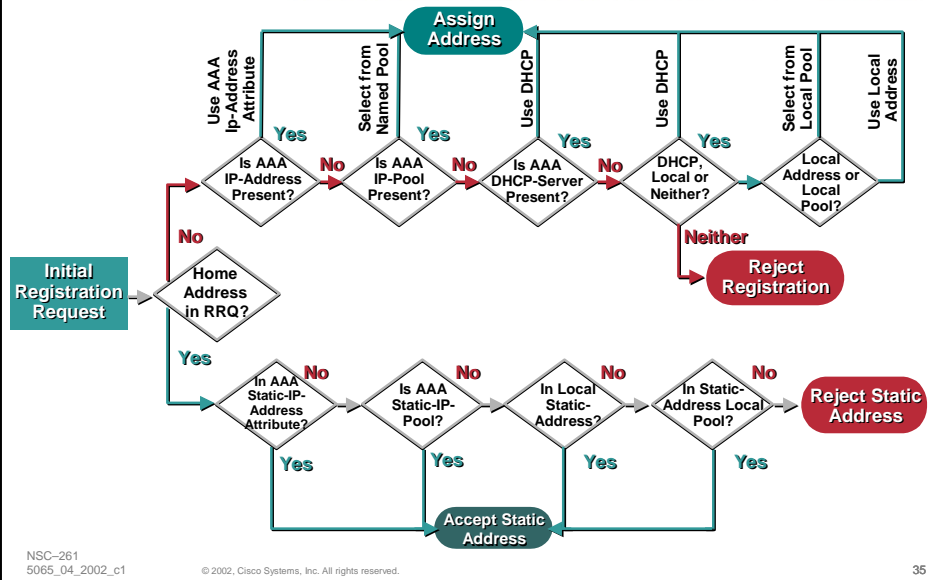
NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

34

NAI Home Addressing Flow

Cisco.com



Static Addressing with NAI

Cisco.com

- **Good for Mobile Server Deployments**
- **Similar to traditional Mobile IP**
- **MN is pre-configured with a Home Address**
- **Home Address is authorized with NAI**
- **HA will reassign if address is in use**

Use `ip mobile home-agent reject-static-addr` to disable

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

36

Static Address in AAA (common)



- Requires one or more addresses
- Allows users to be authorized for specific addresses
- Easy way to manage static addressing.
- Radius AV Pair lists allowable addresses

```
Cisco-AVPair = "mobileip:static-ip-addresses=10.0.0.1  
10.0.0.2 10.0.0.3"
```

- **CLI Config:**

```
ip mobile host nai @example interface F0/0 aaa
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

37

Static Pool in AAA



- Difficult to manage, Not a likely deployment
- Good for assigning class of service based on Home Address
- Radius AV Pair lists local pool of allowable addresses

```
Cisco-AVPair = "mobileip:static-ip-pool=static-pool"
```

- **CLI Config:**

```
ip local pool static-pool 10.0.0.5 10.0.0.10  
ip mobile host nai @example interface F0/0 aaa
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

38

Local Static Address



- Simple way to manage a small number of static addressed hosts
- Good for testing
- CLI Config:

```
ip mobile host nai user@example static-address  
10.0.0.1 10.0.0.2 interface FastEthernet0/0
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

39

Local Static Pool



- Easy way to manage a small group of static users
- No control over who uses an address
- CLI Config:

```
ip local pool pool-name 10.0.0.5 10.0.0.10  
ip mobile host nai @example local-pool pool-name  
interface FastEthernet0/0
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

40

Dynamic Addressing

Cisco.com

- The most common solution
- Client does not need to be configured with an address
- Can be from a pool, semi-static or fixed
- Not all solutions work with redundancy

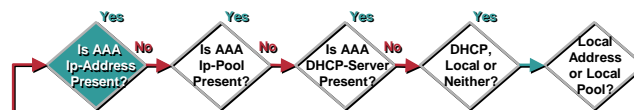
NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

41

AAA Assigned IP Address (Common)

Cisco.com



- Most Common configuration for service provider
- Can be a fixed address or from a AAA pool
AAA assignment is similar to what is used for Dialup
- Router Config

```
ip mobile host nai @example interface F0/0 aaa
```

- Radius Attribute

```
Cisco-AVPair = "mobileip:ip-address=65.0.0.71"
```

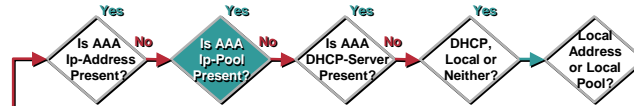
NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

42

AAA Assigned Local Pool

Cisco.com



- Manage Addresses at the HA
- Manage pools in AAA
- **Can not be used with HA redundancy**
- CLI Config:

```
ip local pool dynamic-pool 10.0.0.5 10.0.0.10
ip mobile host nai @example interface F0/0 aaa
```
- Radius command

```
Cisco-AVPair = "mobileip:ip-pool=dynamic-pool"
```

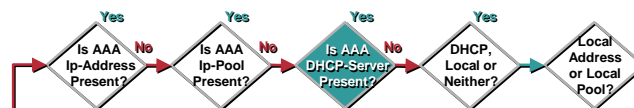
NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

43

Assigned DHCP Server

Cisco.com



- Minimize HA configuration
- Allows per user DHCP Server selection
- User portion of NAI is sent as the hostname
- Very flexible solution for using existing Address Management solution
- CLI Config:

```
ip mobile host nai @example interface F0/0 aaa
```
- Radius Config

```
Cisco-AVPair = "mobileip:dhcp-server=10.1.5.10"
```

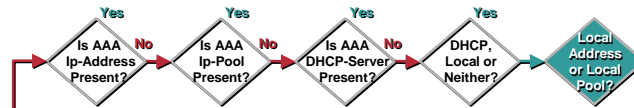
NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

44

Locally Configured DHCP Server (Common)

Cisco.com



- Great enterprise solution
- CLI Config:

```
ip dhcp-server 10.1.2. 3
ip mobile host nai @example address pool
dhcp-proxy-client int F0/0

ip mobile host nai @example address pool
dhcp-proxy-client dhcp-server 10.1.2.3 int F0/0
```
- DHCP can not be used with a virtual network
- DHCP server must differentiate on Client ID

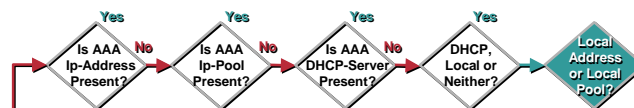
NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

45

Local Pool Address

Cisco.com



- Simple self-contained addressing solution
- Good for testing
- Can not be used with HA redundancy
- CLI Config:

```
ip local pool mipool 10.0.0.5 10.0.0.250
ip mobile host nai @example address pool local
mipool virtual-network 10.0.0.0 255.255.255.0
```

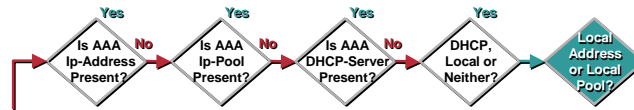
NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

46

Local Address

Cisco.com



- **Good for testing**
- **Difficult to manage and scale**
- **CLI Config:**

```
ip mobile host nai user@example address  
10.0.0.9 virtual-network 10.0.0.0  
255.255.255.0
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

47

Authentication

Cisco.com

- **Authentication is handled via Authentication Extensions (...AE)**
- **Extension type and/or subtype define the relationship**
- **SPI defines the context**
- **Authenticator protects only data between the UDP header and Authenticator**

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

48

Authentication Extensions

Cisco.com

| | | |
|-------------------------|---|----------------------------|
| MN-HA (MHAE) | Protects Registration Request and Reply | Required |
| MN-FA (MFAE) | Insecure | Optional and Rarely Used |
| HA-FA (HFAE) | Allow only Trusted FA To Be Used | Optional and Rarely Used |
| MN-AAA (GNAE) | Alternative to MN-FA | Optional, Requires FA-CHAP |

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

49

SPI

Cisco.com

- **Security Parameter (set) Index also referred to as Security Association or SA**
 - Replay Protection
 - Hash Type (algorithm and mode)
 - Key
- **Multiple SPIs can be used for each MN**
- **Not an IPSec SPI, but similar concept**

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

50

SPI Continued

Cisco.com

- **SPI numbers 0–255 are Reserved**
 - SPI # 2 is used for PPP style CHAP
- **SPI numbers 256–4294967295 are for general use**
- **HMAC-MD5 is more secure than Keyed MD5 (prefix-suffix) Both are supported**
- **IOS only supports timestamp replay protection**
- **Hardware tokens can only be used with MN-AAA**

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

51

Local Authentication

Cisco.com

- **Very fast, but not very scalable**
- **Can be used for MN-HA, HA-HA, or HA-FA SPI**
- **CLI Config:**

```
ip mobile secure host—MN-HA
ip mobile secure home-agent—HA-HA and HA-FA
ip mobile secure foreign-agent—HAFA
ip mobile secure visitor—MN-FA

ip mobile secure host nai user1@example spi 100 key
ascii itsasecret algorithm md5

ip mobile secure home-agent 10.10.10.10 spi 100 key
hex 1234567890ABCDEF1234567890ABCDEF
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

52

AAA Authentication

Cisco.com

- TACACS+ is supported, but is not recommended because of the TCP overhead
- Can only be used for MN-HA
- **AAA Does not authenticate, it only stores the pre-shared key**
- **Server must authenticate null password or the user password must be "cisco"**
- **Must complete the phrase:**
 - “ip mobile secure host w.x.y.z ...”
 - “ip mobile secure host nai user ...”

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

53

AAA Authentication Continued

Cisco.com

- **Router config:**

```
aaa new-model
aaa authorization ipmobile default group radius
!
ip mobile host ... aaa [load-sa]
```

- **Radius attribute:**

```
cisco-avpair = "mobileip:spi#0= spi 100 key hex
ffffffffffffffffffffffffffffffff algorithm hmac-md5"

Cisco-avpair = "mobileip:spi#1= spi 101 key ascii
itsasecret replay timestamp within 10 algorithm md5"
```

- **TACACS+ attribute:**

```
Service=mobileip {
  "spi#0= spi 100 key hex ffff...f"
}
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

54

MN-AAA and FA CHAP

Cisco.com

- Solves replay protection and MN-FA SA problem
- Allows the FA to authenticate without a SA
- **Forward MFCE if using AAA for MN-HA SA**
- **CLI Config:**

```
aaa authentication ppp default group radius
aaa authorization ipmobile default group radius

ip mobile foreign-service challenge forward-mfce
timeout 10 window 10
```
- **Radius server must be configured for PPP CHAP style authentication**

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

55

SA Cache

Cisco.com

- **SAs can be cached locally to limit AAA transactions**
- **SAs are replicated with HA redundancy**
- **Cache invalidation**

```
clear ip mobile secure host ...
```

Cache is refreshed on auth Failure

```
ip mobile home-agent resync-sa <retry>
```

<retry> is the number of seconds to wait between successive AAA queries for the same MN

Can be updated or cleared with an SNMP set

For NAI cache is cleared when binding expires

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

56

SA Preload

Cisco.com

- **Configuration command**
Download SAs from AAA server onto HA at a given rate
`ip mobile secure aaa-download <rate>`
`<rate>` is queries per second
- **Console command**
Clear cache and download SAs from AAA
`clear ip mobile secure all load`
`clear ip mobile secure empty load`

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

57

Other Features


Cisco.com

- **Care-of Access lists**
- **Tunnel NAT and route maps**
- **VPN-realm—route maps with dynamic addressing**

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

58



Cisco.com

Clients

NSC-261
5065_04_2002_c1 © 2002, Cisco Systems, Inc. All rights reserved. 59

Clients

Cisco.com

- **Mobile IP client run at the stack level of the Mobile Node**
- **MN signals it's own routing update**
- **Transparent to upper layer applications**

NSC-261
5065_04_2002_c1 © 2002, Cisco Systems, Inc. All rights reserved. 60

Clients Types

Cisco.com

| | Host Device | Pros | Cons |
|----------------|-----------------------------|---|--|
| Terminal-Based | Laptops, PDAs, etc. | More Features | Hard to Deploy and Manage |
| Embedded Proxy | Handset, Access Point, etc. | Transparent to Attached Clients, Easier to Manage | Tied to Media, Fewer Features, Less Security |
| Mobile Router | Router | Clients not Mobile, Central Management | Harder to Provision and Deploy |

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

61

PC Clients

Cisco.com

- **Full featured, stable commercial clients available from Birdstep, Lifix, and others**
- **HUT Dynamics is a good open source client for Linux (and Windows)**
- **Support WLAN roaming and inter-link roaming**

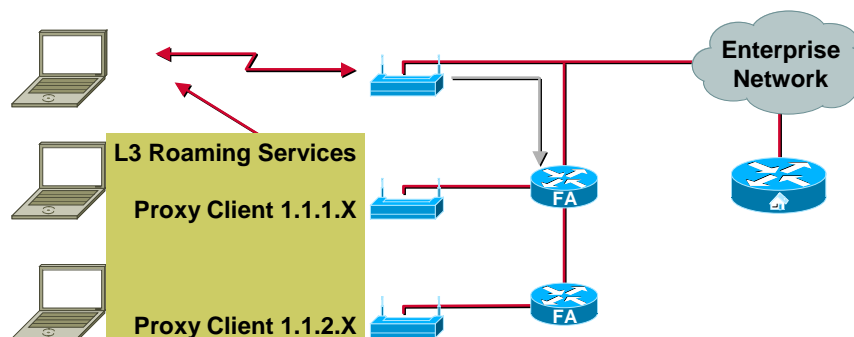
NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

62

WLAN Proxy Mobile Node

Cisco.com



- **Fast subnet roaming through Inter Access Point Protocol (IAPP)**
- **Proxy Mobile Services (AP, Upstream switch/router)**
 - Session maintained for critical applications (voice, video, etc.)
 - Coexists with DHCP and static addresses schemes

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

63

WLAN Proxy Mobile Node (Cont.)

Cisco.com

- **Access Point discovers FA**
- **Client associates with AP**
- **AP registers to FA for client**
- **Registration completes**
- **HA tunnels client's traffic to FA, which forward to AP**

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

64

IOS Mobile Networks

Cisco.com

- Allows a whole network to roam with the hosts being aware
- Supports legacy devices without MN client software
- Available as of 12.2(4)T
- Supports Static Network, Preferred Path, Reverse Tunnel and Hold Down
- Useful in transportation and shipping, but can also be good for mobile teams

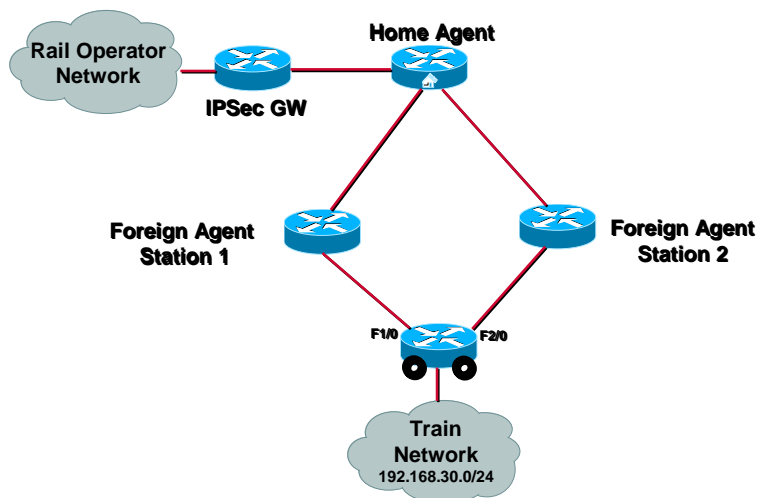
NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

65

Mobile Networks – Rail Example

Cisco.com



NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

66

Mobile Networks Config

Cisco.com

```
interface Loopback0
 ip address 192.168.50.1 255.255.255.255
!
interface FastEthernet0/1
 ip address 192.168.30.1 255.255.255.0
!
interface FastEthernet1/0
 ip mobile router-service roam
 ip mobile router-service solicit
!
interface FastEthernet2/0
 ip mobile router-service roam priority 10
 ip mobile router-service solicit
!
router mobile
!
ip mobile secure home-agent 192.168.101.2 spi 100 key ascii itsasecret
ip mobile router
 address 192.168.50.1 255.255.255.0
 home-agent 192.168.101.2
 register lifetime 7200
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

67

Mobile Networks HA Config

Cisco.com

- **Not much new here!**

```
router mobile
!
ip mobile home-agent
ip mobile virtual-network 192.168.50.0 255.255.255.0
ip mobile host 192.168.50.1 192.168.50.100 virtual-network
 192.168.50.0 255.255.255.0
 ip mobile mobile-networks 192.168.50.1
  network 192.168.30.0 255.255.255.0
ip mobile secure host 192.168.50.1 spi 100 key ascii cisco
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

68

Mobile Networks IPSec Option

Cisco.com

- Integrated IPSec is not part of the initial release
- IPSec must be configured on the outbound interface
- Outbound interface changes
- Use existing IOS features to solve the problem

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

69

IPSec Config

Cisco.com

- Bounce traffic through the loopback to be encrypted

```
crypto isakmp ...
crypto ipsec transform-set ...
crypto map tocorp 10 ipsec-isakmp
  set peer 192.168.101.1
  set transform-set ts
  match address 101
!
interface Loopback0
  crypto map tocorp
!
interface FastEthernet0/1
  ip policy route-map cryptotrick
!
access-list 101 permit ip 192.168.30.0 0.0.0.255 192.168.100.0
  0.0.0.255
!
route-map cryptohack permit 10
  match ip address 101
  set interface Loopback0
```

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

70

Traffic Flow Issues

Cisco.com

- Both tunneling and triangle routing can cause some traffic flow issues
- Mobile IP is not alone, IPSec and PPPoE have similar issues
- Most issues are caused by “over” firewalling

NSC-261
5065_04_2002_c1

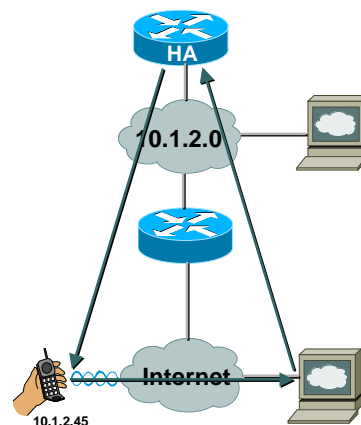
© 2002, Cisco Systems, Inc. All rights reserved.

71

Ingress Filtering

Cisco.com

- A “classic” problem in MIP
- Network designers block incoming traffic with an internal source address
- Unicast RPF is probably a more dangerous problem
- Reverse Tunnels are the solution



NSC-261
5065_04_2002_c1

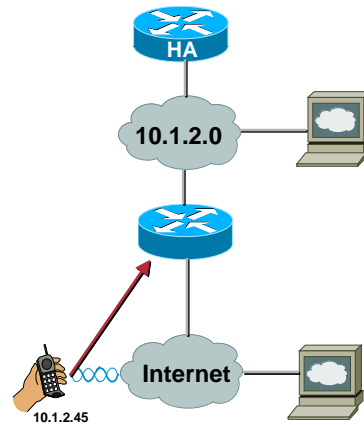
© 2002, Cisco Systems, Inc. All rights reserved.

72

Ingress Filtering

Cisco.com

- A “classic” problem in MIP
- Network designers block incoming traffic with an internal source address
- Unicast RPF is probably a more dangerous problem
- Reverse Tunnels are the solution



NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

73

Path MTU Discovery

Cisco.com

- Many network designers block all inbound ICMP
- A problem for both Triangle and reverse tunnel
- TCP Session opens, but “hangs”
- **No perfect solution, but several options**

Change MTU on the MN

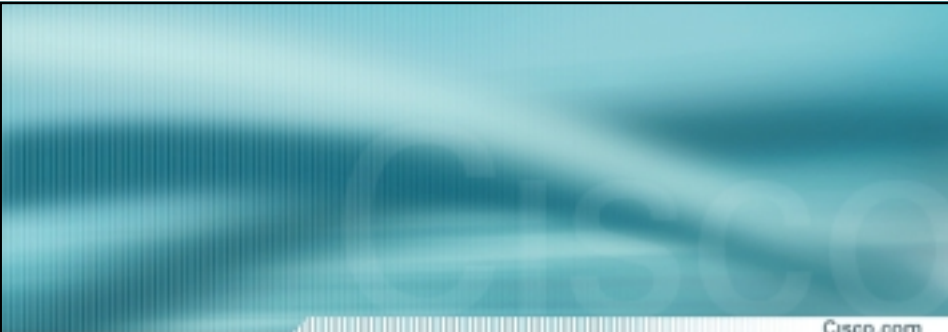
```
ip tcp adjust-mss 1400 on an interface
```

Works well, but needs to in all outbound paths

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

74



Cisco.com

IOS Mobile IP References

NSC-261
5065_04_2002_c1 © 2002, Cisco Systems, Inc. All rights reserved. 75

Cisco IOS Mobile IP

Cisco.com

- **Early Field Trial since 1997**
- **General Availability January 1999**
 - Introduced in Cisco IOS **12.0(1)T**
 - 12.0(2)T** Home Agent Redundancy
- **Mobile IPv4 RFC 3220 (2002), 2003, 2005, 2006 compliant**
- **Foreign Agent, Home Agent, Proxy Mobile Node and Mobile Router**
- **Platforms supported**
 - 2600 through 7500, Cat5K RSM, Cat6K MSFC
- **<http://www.cisco.com/go/fn>**

NSC-261
5065_04_2002_c1 © 2002, Cisco Systems, Inc. All rights reserved. 76

Deployments

Cisco.com

- **Several Service Providers all over the world**
- **Used in both 2.5G and 3G wireless networks**
- **Enterprise deployments are in the early stages**
- **Actively being used in Cisco's Alpha Network**

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

77

Other Networkers Sessions

Cisco.com

- **ACC-131—Introduction to Wireless Data Networks**
- **ACC-231—Deploying and Managing 802.11 Wireless Networks**
- **ACC-233—Designing and Deploying Public Access Networks**
- **ACC-234—Deploying IP Services for Mobile Wireless Networks**
- **NSC-110—Introduction to Network Management**
- **RST-221—Router Architecture and Operation**

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

78

References

Cisco.com

- http://www.cisco.com/go/mobile_ip
- <http://www.cisco.com/go/fn>
- <http://www.ietf.org/html.charters/mobileip-charter.html>

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

79

Client Links

Cisco.com

- <http://www.birdstep.com/>
- <http://www.lifix.fi/>
- <http://www.cs.hut.fi/Research/Dynamics/>

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

80

Summary

Cisco.com

- **Integrating Mobile IP into an Enterprise Network**

Easily add Mobile IP, leverage existing DHCP and AAA, use FA, add redundancy, monitor, manage and troubleshoot

- **Deployment Options**

Virtual, NAI, Addressing and Authentication

- **Clients**

PC based, Proxy, Mobile Router and Traffic Flow issues

- **IOS Mobile IP References**

Platforms, Releases, Deployments, References Networks and Links

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

81

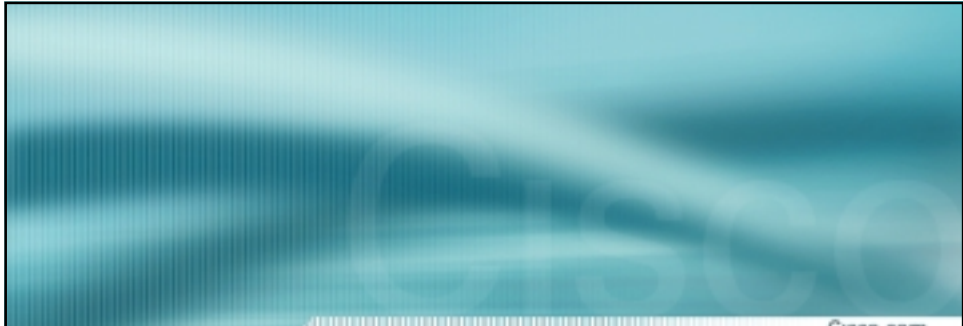
Cisco.com

Questions?

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

82



Cisco.com

Please Complete Your Evaluation Form

Session NSC-261

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

83

CISCO SYSTEMS



EMPOWERING THE
INTERNET GENERATION

NSC-261
5065_04_2002_c1

© 2002, Cisco Systems, Inc. All rights reserved.

84