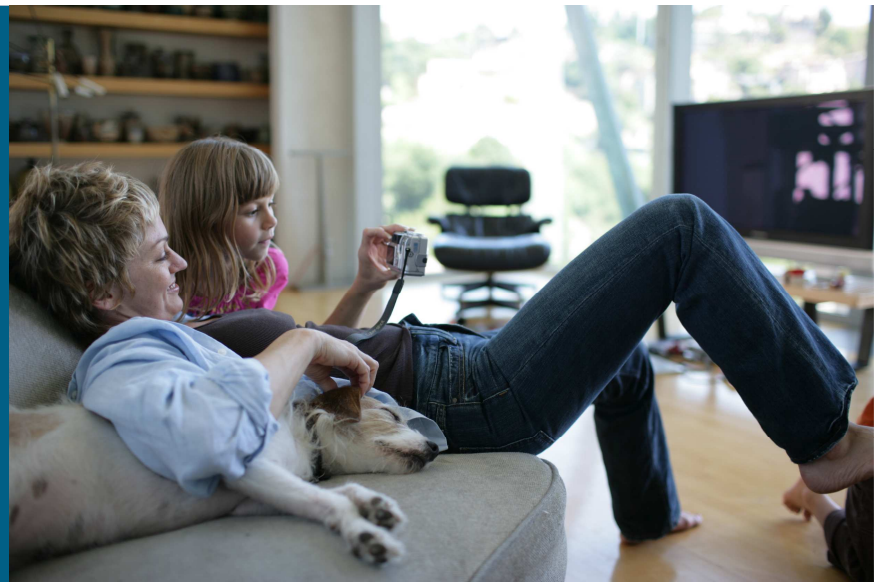
Mobile IP Advanced



Richard Shao
Product Manager

© 2007 Cisco Systems, Inc. All rights reserved.

Agenda

- Introduction to IP Mobility
- Mobile IP Technology
- Cisco Mobile IP Applications
- Summary and References

© 2007 Cisco Systems, Inc. All rights reserved.

“Mobility” in the Context

The First Impression?

© 2007 Cisco Systems, Inc. All rights reserved.

“Mobility” in the Context

The First Impression?	In the Context…	Common Related Buzz Words
 	Where? Location	Nomadic
 	What? Type	Portability
	How? Movement	Roaming

© 2007 Cisco Systems, Inc. All rights reserved.

Mobility in the IP Networking World





Applications

Enables Continuous Application and Service Access over IP Networks
Regardless of Location, Type of Devices, and Movement

Services

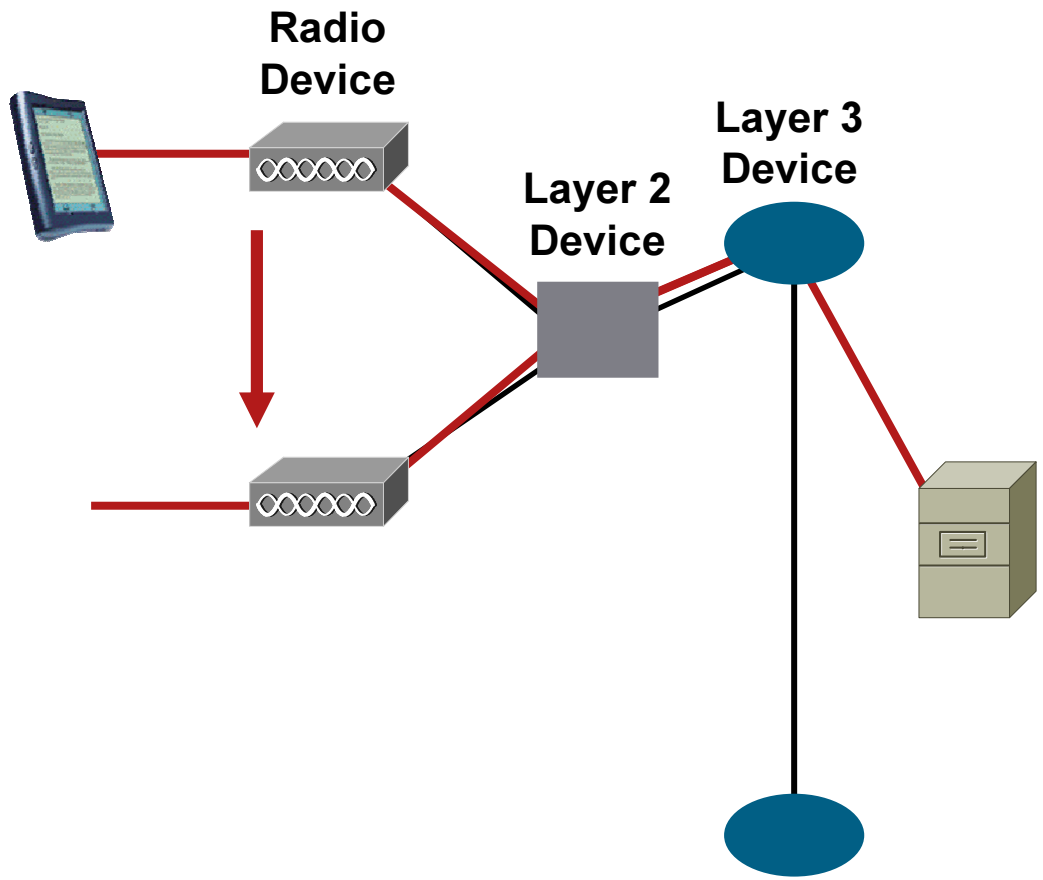
Internet

IP Networks

© 2007 Cisco Systems, Inc. All rights reserved.

Layer 2 Mobility

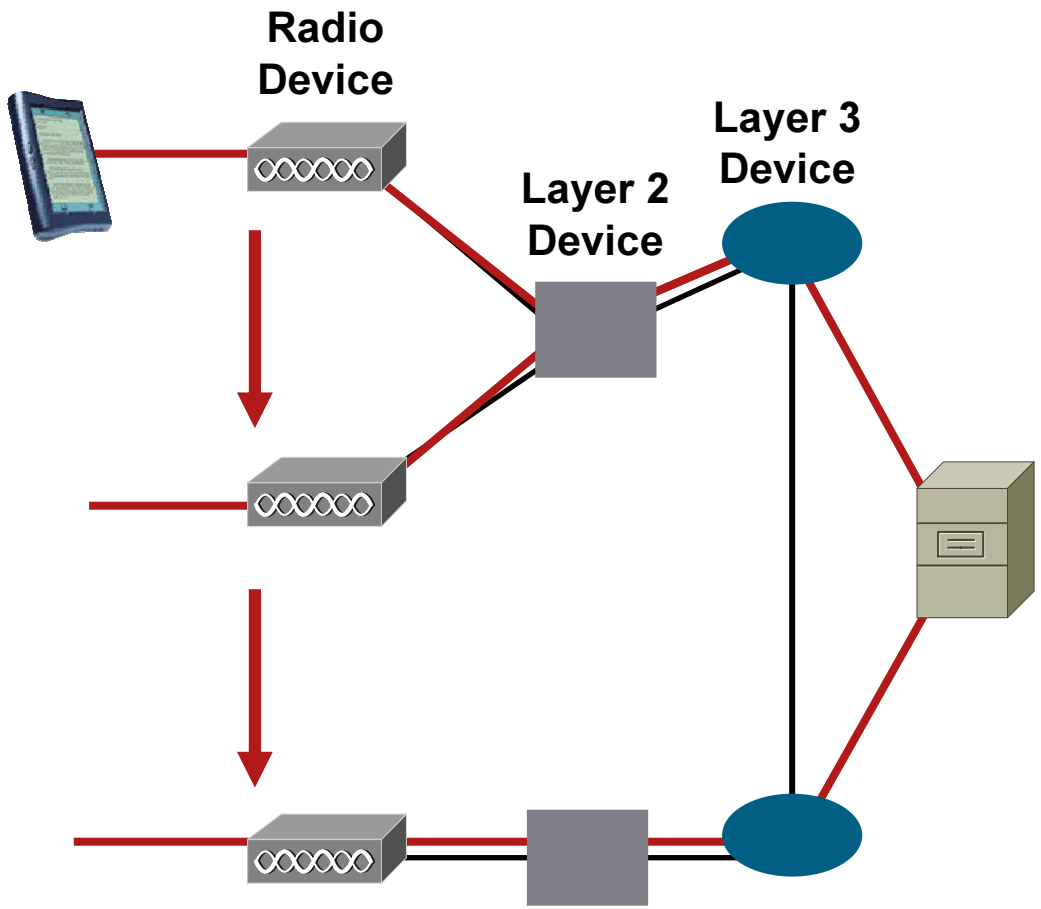
- Movement within a Layer 3 boundary
- IP address does not change
- Application continuity is maintained
- An example is Inter-Access Point Protocol (IAPP) defined in IEEE



© 2007 Cisco Systems, Inc. All rights reserved.

Layer 3 Mobility

- Movement across Layer 3 boundaries
- "IP address" is changed
- Application continuity is maintained even if it is across a Layer 3 boundary
- Examples are
  - LWAPP in WLAN
  - GTP in GPRS
  - Mobile IP in 1xRTT

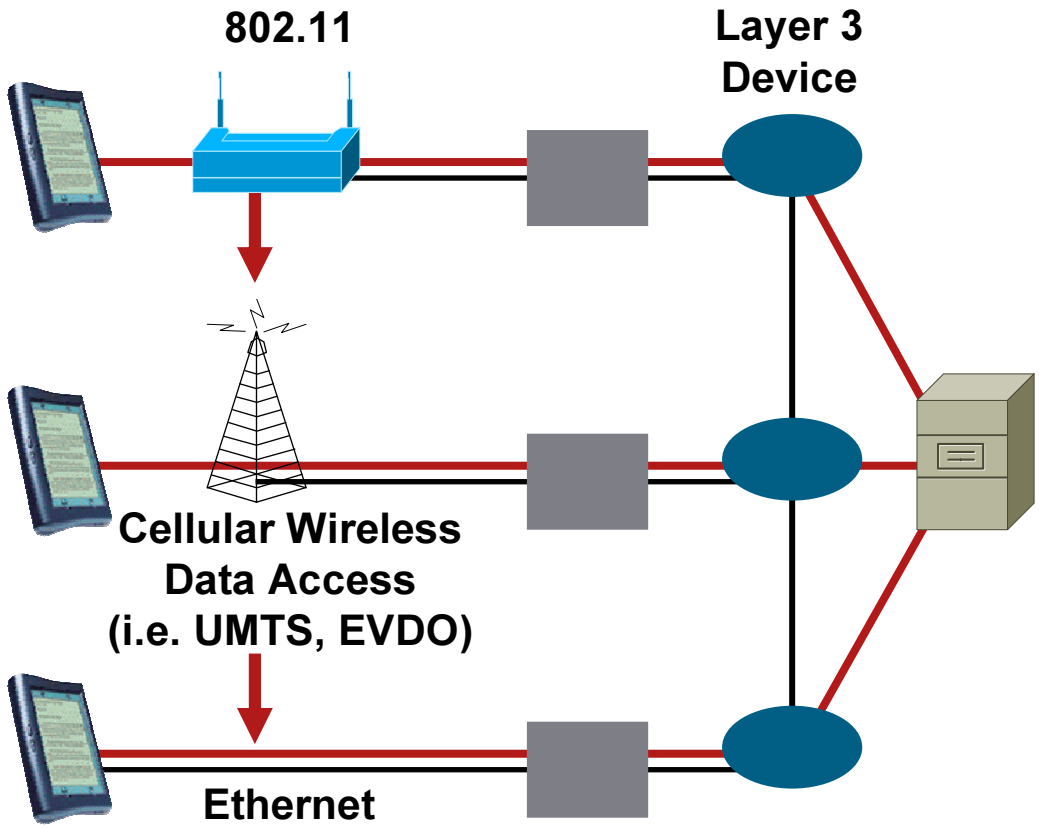


LWAPP: Lightweight Access Point Protocol
GTP: GPRS Tunneling Protocol
1xRTT: One Time Radio Transmission Technology

© 2007 Cisco Systems, Inc. All rights reserved.

Multi-Access Mobility

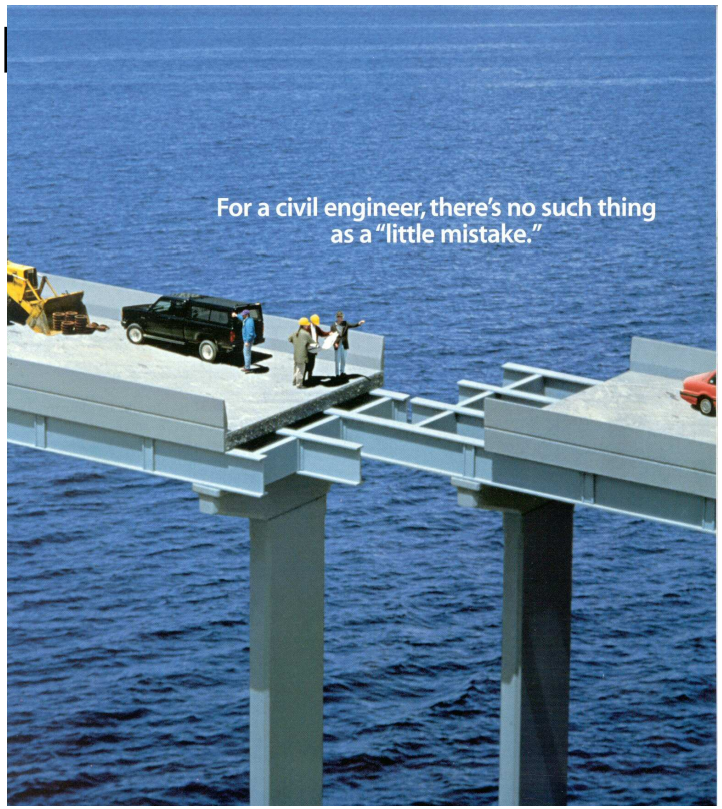
- Movement across different types of access networks
- “IP address” is changed
- Application continuity is maintained even a Layer 3 boundary and an access network are across
- Examples are
  - Mobile IP defined in IETF standard
  - Vendor proprietary protocols



© 2007 Cisco Systems, Inc. All rights reserved.

IP Mobility in Our Context

- L3 Mobility +



Design to Fit?

© 2007 Cisco Systems, Inc. All rights reserved.

Mobile Wireless Service Framework

Mobile Wireless Service Functional Layers

- **Application, Service, Content**
- **IP Networks (IP Mobility)**
- **Wireless**
- **Mobile Device**

Bluetooth
ZigBee

ZigBee™ Alliance

802.11a/b/g
4.9G

CDMA, GSM,
W-CDMA, OFDM

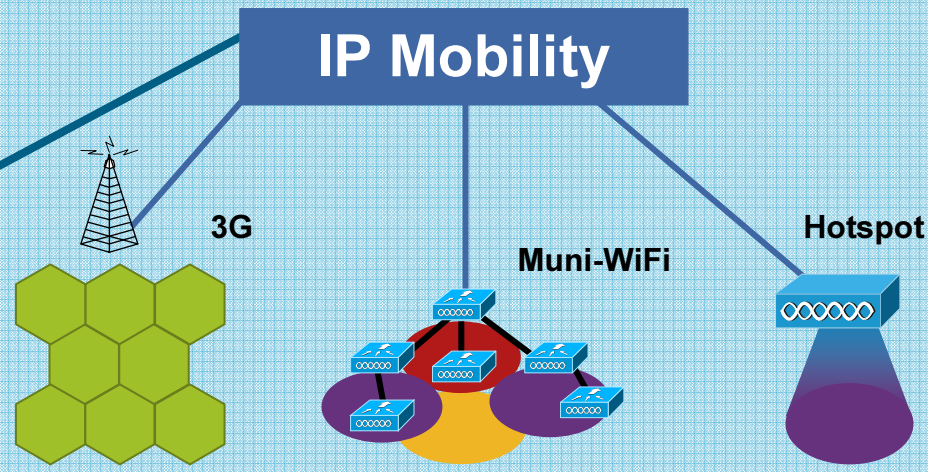
Satellite

© 2007 Cisco Systems, Inc. All rights reserved.

Why Has IP Mobility Been Used in the Framework?

- Extend coverage
- Enhance usability and effectiveness
- Enable new services and applications

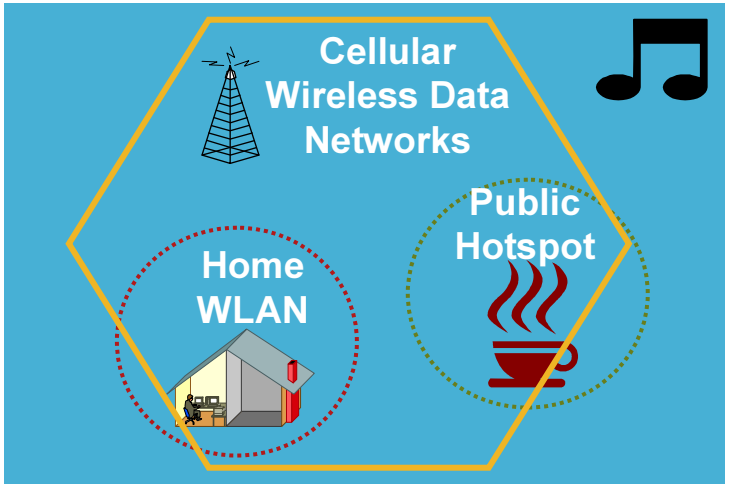
- Wider is perceived better, but…
  - Cost for perfection
  - Bandwidth vs. coverage
- Use IP Mobility to leverage multi-access and multi-IP networks to create one virtual large network



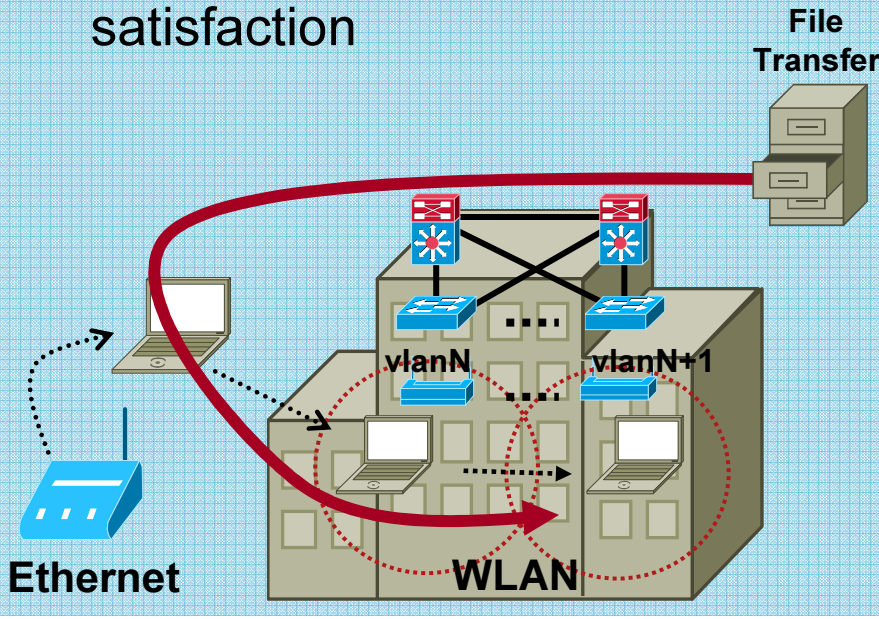
© 2007 Cisco Systems, Inc. All rights reserved.

Why Has IP Mobility Been Used in the Framework?

- Extend coverage
- Enhance usability and effectiveness
- Enable new services and applications



- Always-on and uninterrupted network and application operations
- Hidden network complexity from users
- Better user and customer satisfaction



© 2007 Cisco Systems, Inc. All rights reserved.

Why Has IP Mobility Been Used in the Framework?

- Extend coverage
- Enhance usability and effectiveness
- Enable new services and applications

- Seamless Internet roaming
- Secure mobile VPN access
- Remote mobile office
  - Push software updates
  - Dispatch call and data
  - Fleet management
- Video surveillance
- Internet access for passenger

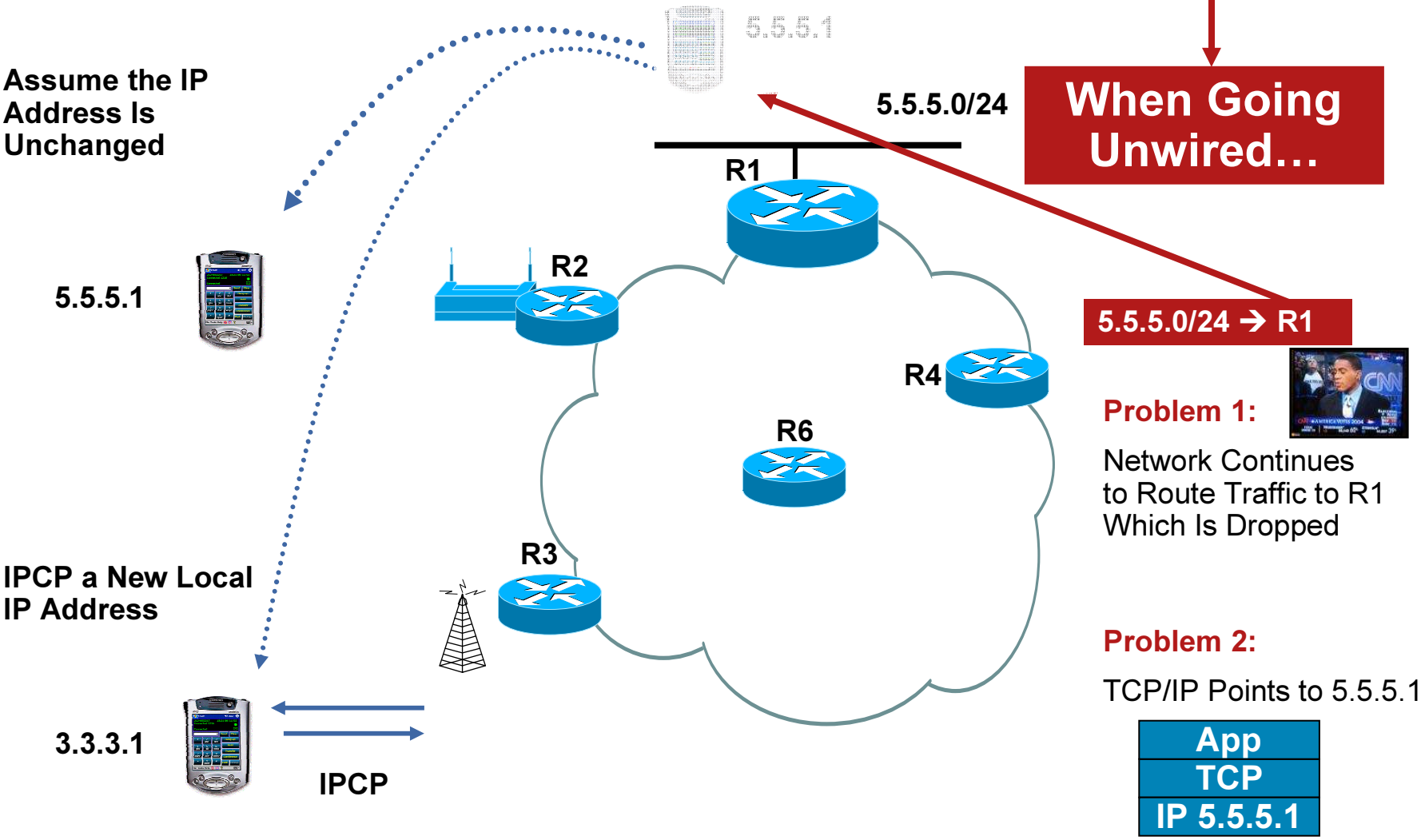
Transportation

© 2007 Cisco Systems, Inc. All rights reserved.

Mobile IP
An IP Mobility Technology

© 2007 Cisco Systems, Inc. All rights reserved.

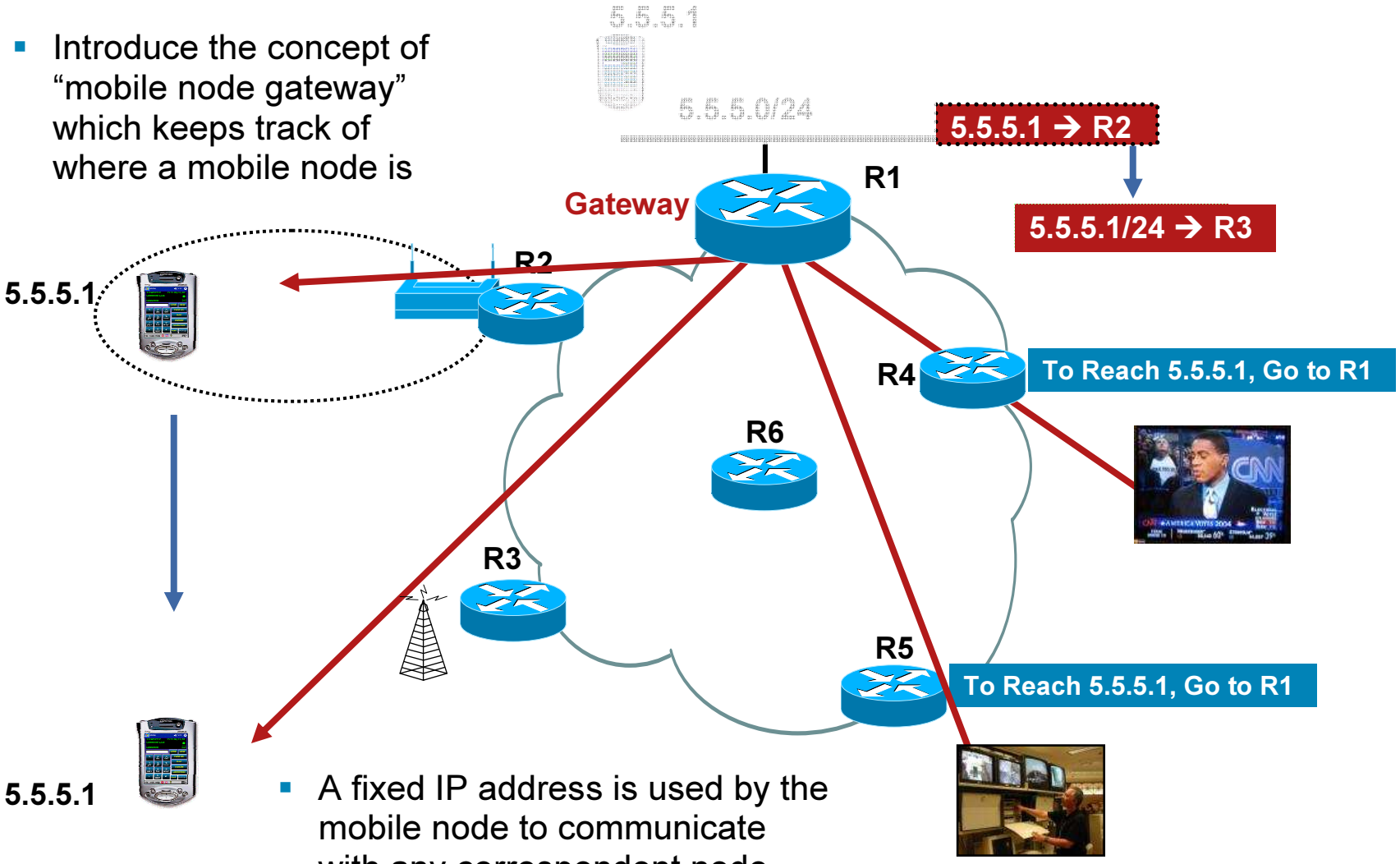
Mobile IP Concept: The Problems



© 2007 Cisco Systems, Inc. All rights reserved.

Mobile IP Concept: The Basics

- Introduce the concept of "mobile node gateway" which keeps track of where a mobile node is

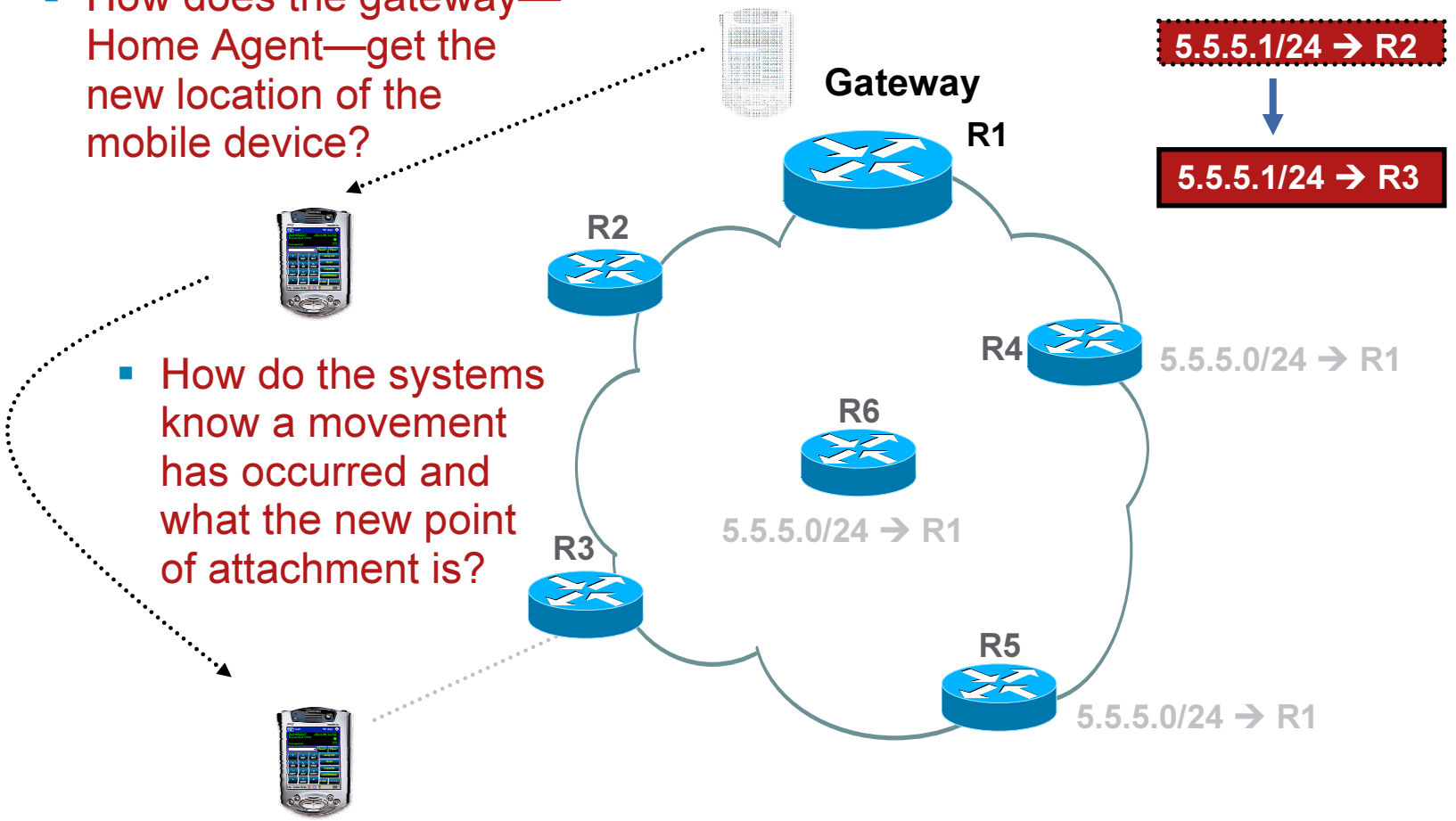


- A fixed IP address is used by the mobile node to communicate with any correspondent node

© 2007 Cisco Systems, Inc. All rights reserved.

Mobile IP Concept: Protocol Operation Requirements

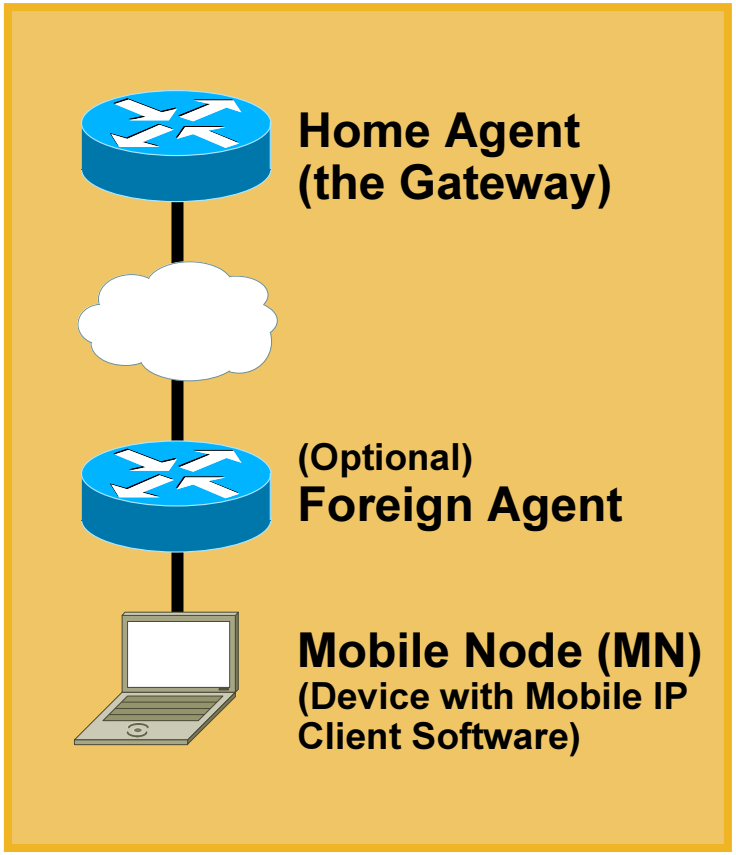
- How does the gateway—Home Agent—get the new location of the mobile device?
- How do the systems know a movement has occurred and what the new point of attachment is?



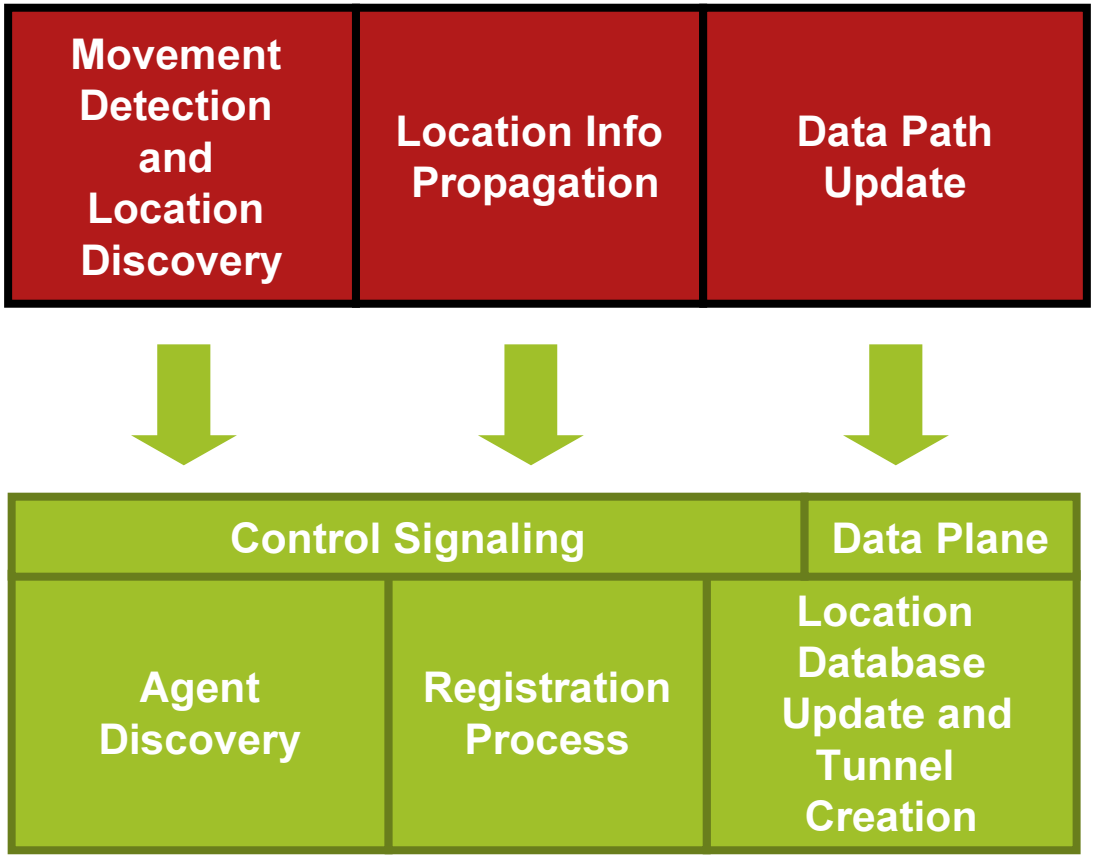
© 2007 Cisco Systems, Inc. All rights reserved.

Mobile IP Protocol Components

Hardware Components



Conceptual Level



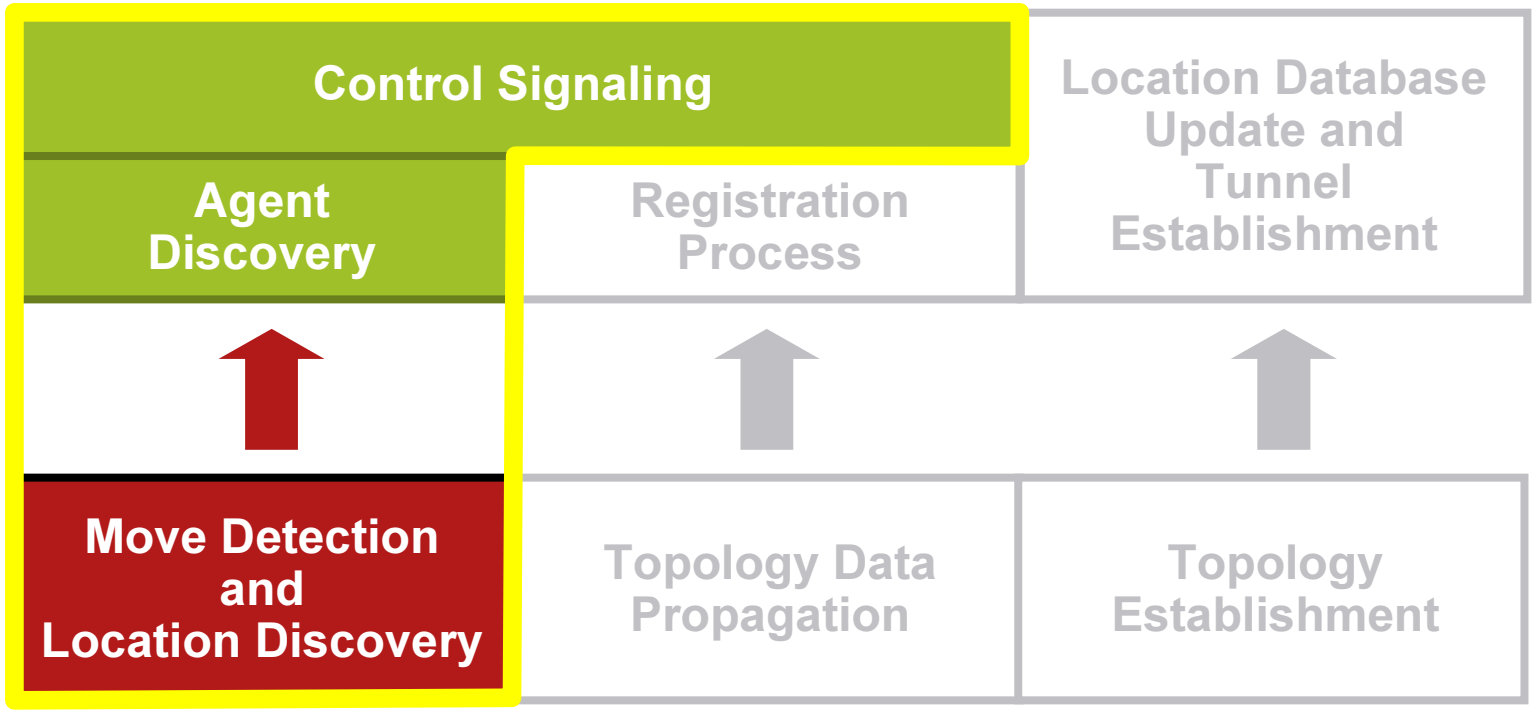
Software Components

© 2007 Cisco Systems, Inc. All rights reserved.

Mobile IP
Protocol Details

© 2007 Cisco Systems, Inc. All rights reserved.

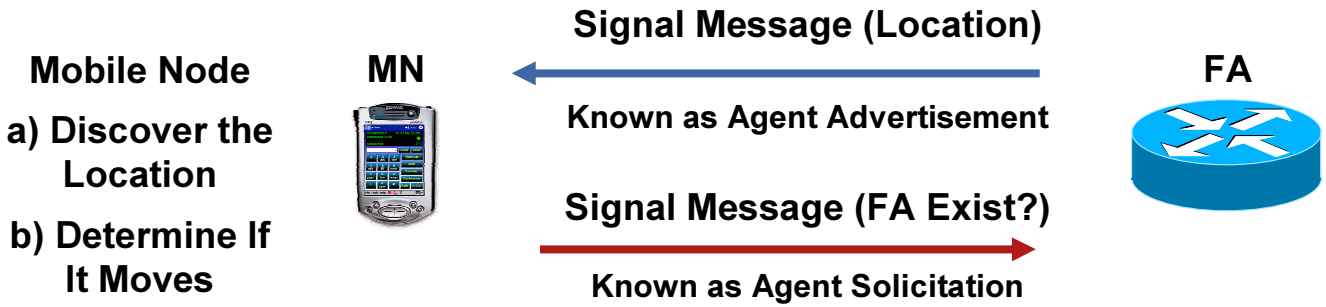
Movement Detection and Location Discovery



© 2007 Cisco Systems, Inc. All rights reserved.

Movement Detection and Location Discovery Overview

- Performed by the mobile node with assistance from networks
- Foreign Agent sends out a signal message including the location information
- Mobile node evaluates the message to detect its movement and discover its location
- Mobile node can send a signal message to seek a foreign agent



© 2007 Cisco Systems, Inc. All rights reserved.

Agent Advertisements Message Format

- What?

  An ICMP packet with Mobility Agent extension

- Who?

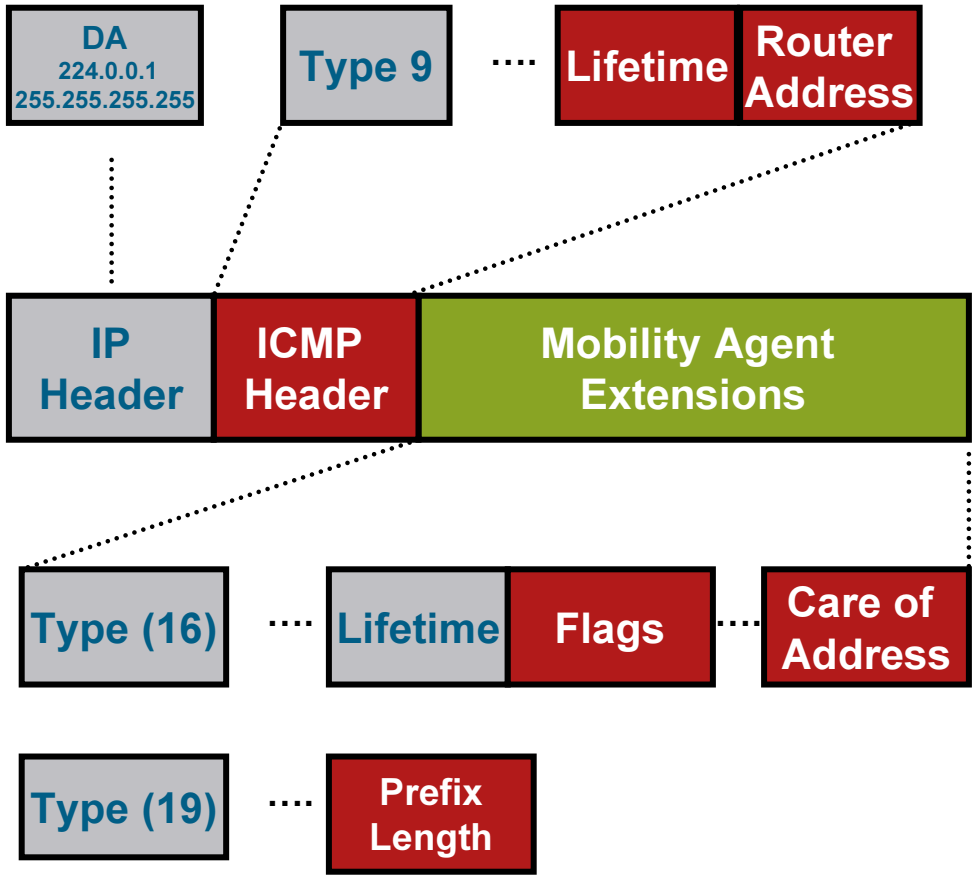
  Used by home agent and foreign agent

  Determined by Flags

- When?

  Periodically sent

  Or response a solicitation from MN



© 2007 Cisco Systems, Inc. All rights reserved.

"How" Does Movement Detection Work?

- Lifetime Expiration (in ICMP Header)

  If not receiving another advertisement from the announced window, MN thinks it has moved

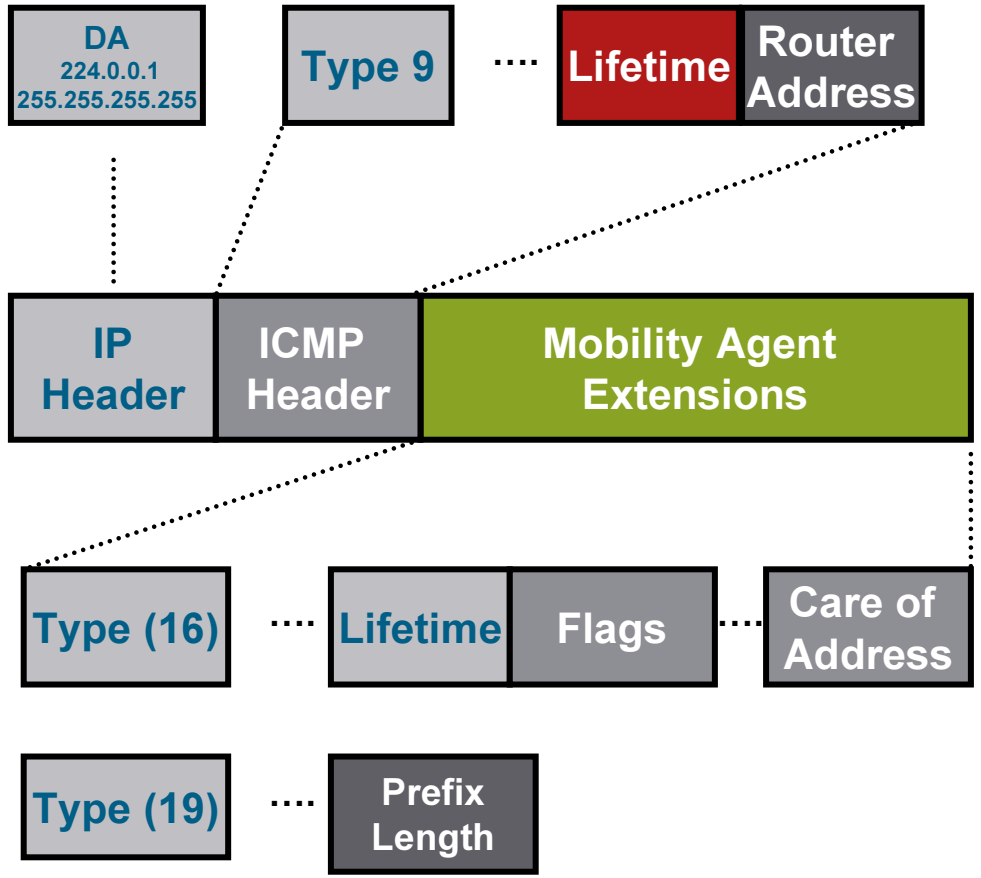
- Prefix Length Extension

  If this FA is on a different subnet, we must have moved

Example:

Agent	Router Addr	Prefix	Subnet
Existing	2.2.2.1	24	2.2.2.0
New	2.2.3.1	24	2.2.3.0

Not Equal → Movement Detected

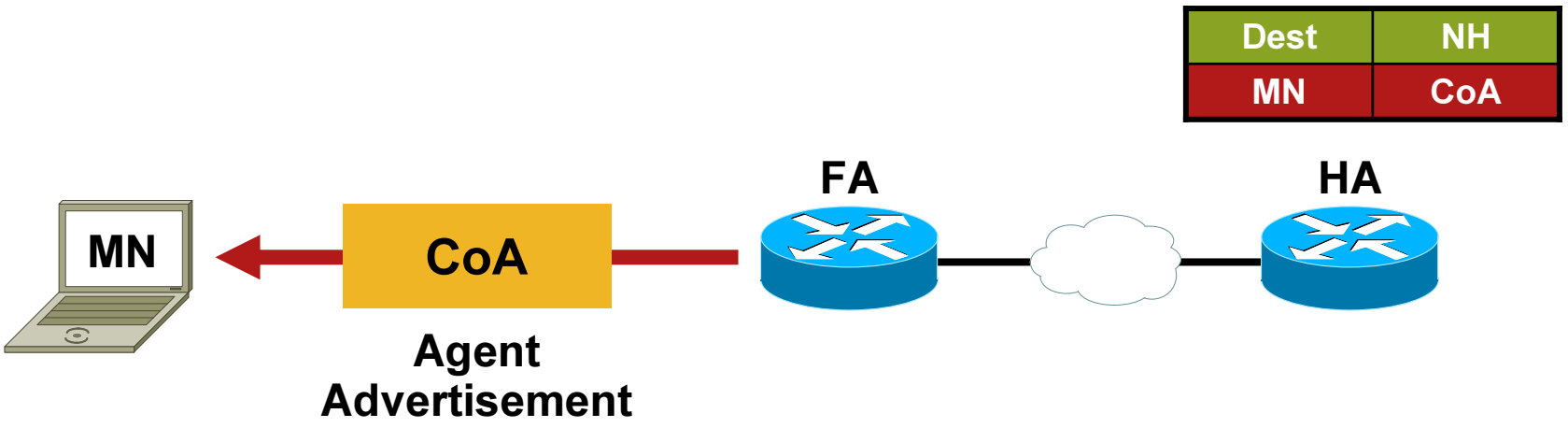


© 2007 Cisco Systems, Inc. All rights reserved.

“How” Does Location Discover Work?

- Care-of-Address (CoA)

  Any address on a FA (the first hop router or known as an access router)



© 2007 Cisco Systems, Inc. All rights reserved.

“How” Does Location Discover Work?

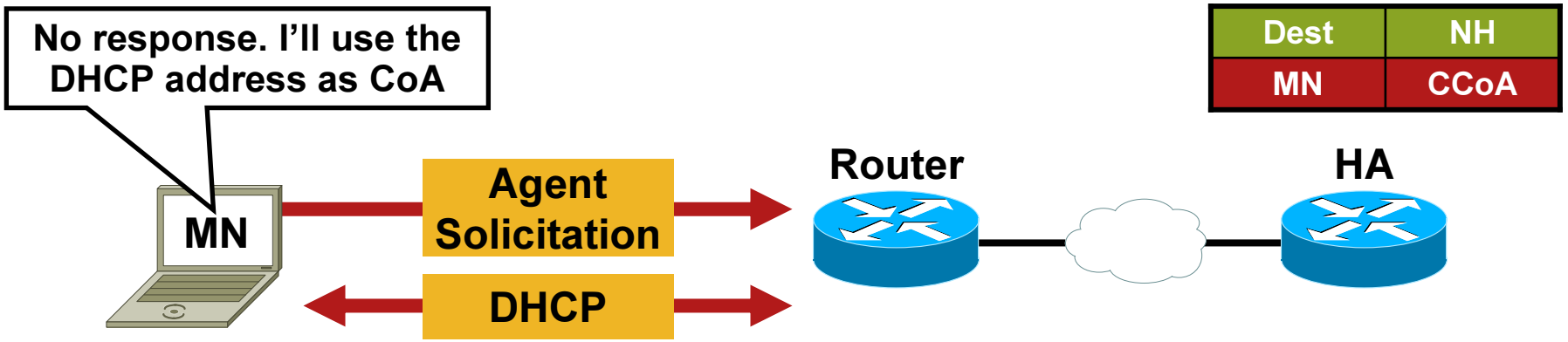
- Care-of-Address (CoA)

  Any address on a FA (the first hop router or known as an access router)

- What if there is no FA?

  Collocated Care-of-Address (CCoA)

  Commonly the IP address acquired via DHCP or IPCP by a mobile node



© 2007 Cisco Systems, Inc. All rights reserved.

What Is Significant?

- Agent Discovery can influence roaming time
- Fast detection = fast roaming

© 2007 Cisco Systems, Inc. All rights reserved.

What Is Significant? (Cont.)

- Adjust Agent Advertisement timer?

  Fast vs. chatty

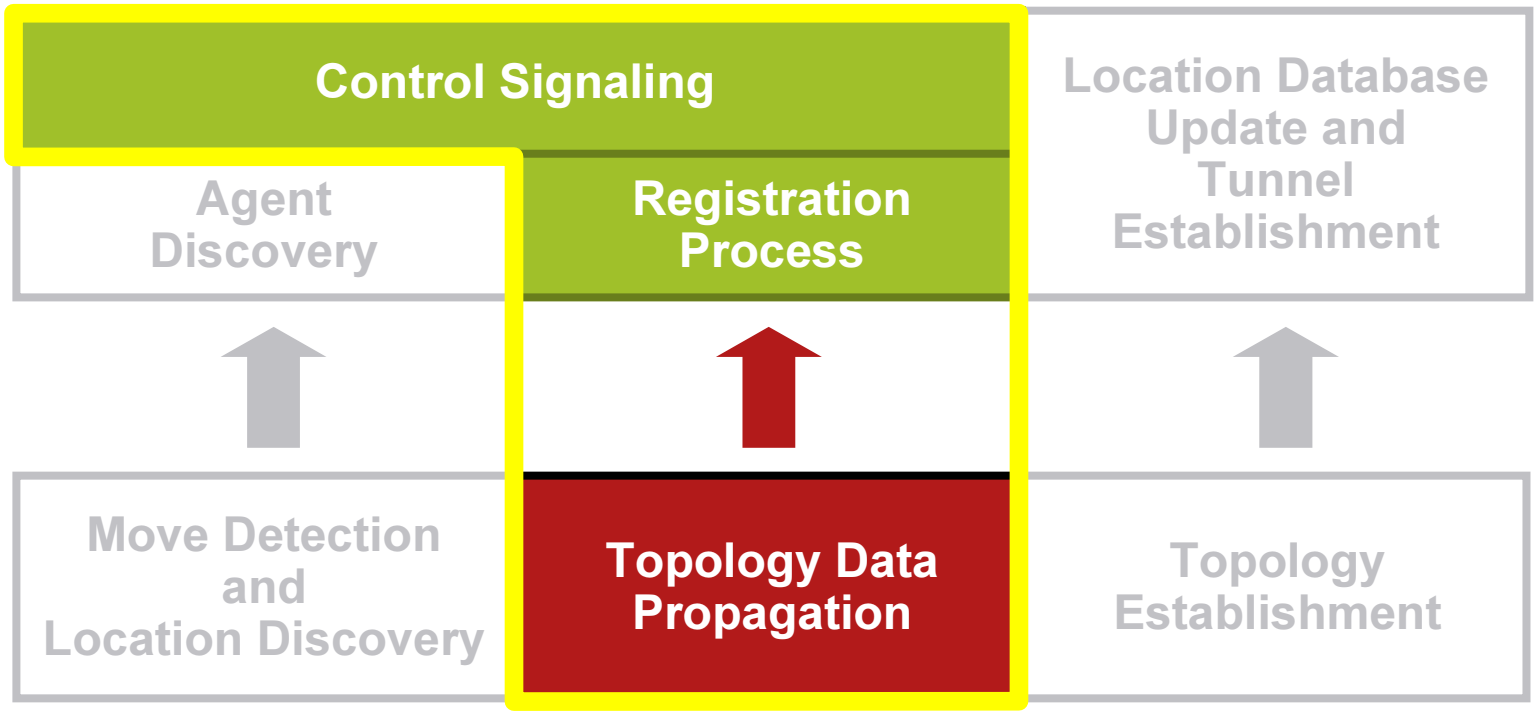
- Proactive approach

  Trigger Agent Solicitation when an interface is up

- When there is no agent at all, DHCP/IPCP operations become an important roaming time factor

© 2007 Cisco Systems, Inc. All rights reserved.

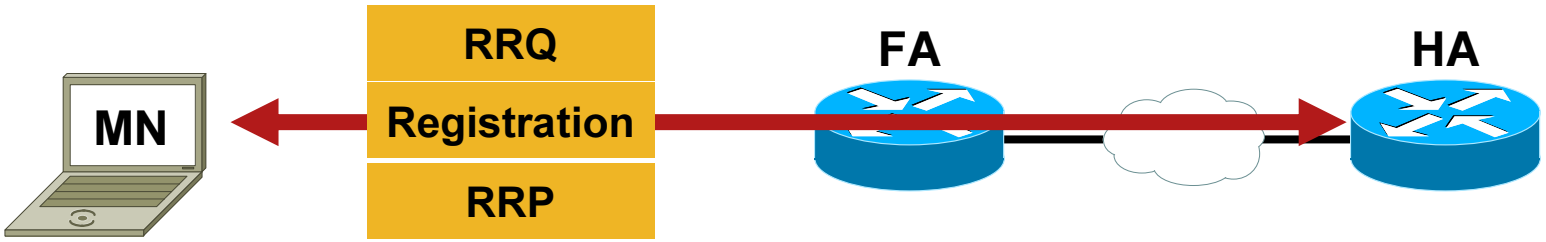
Topology Information Propagation



© 2007 Cisco Systems, Inc. All rights reserved.

Registration Process Overview

- Reporting MN's location to HA
- Occurring periodically or after the movement is detected
- Involving MN, FA, and HA
- Used for deregistration purposes—reporting MN leaving the Mobile IP networks
- Accomplished through Registration Request Message (RRQ) and Registration Reply Message (RRP)



© 2007 Cisco Systems, Inc. All rights reserved.

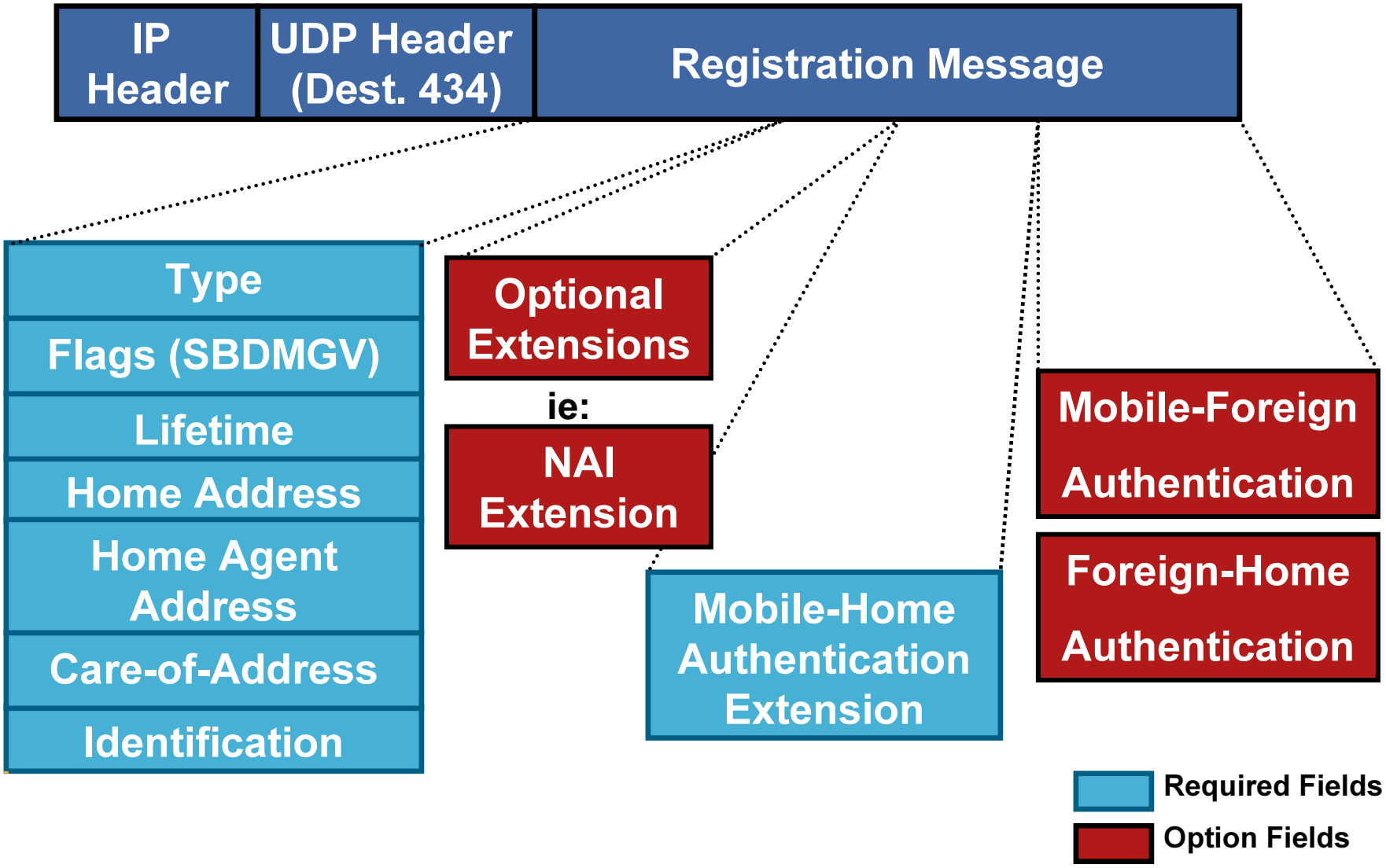
Registration Request Message

Answers the Following Questions

- Who is the mobile node?
- Where is a mobile node's location?
- Where to send the registration message?
- How long is the registration valid?
- How to ensure the MN is an authorized user?

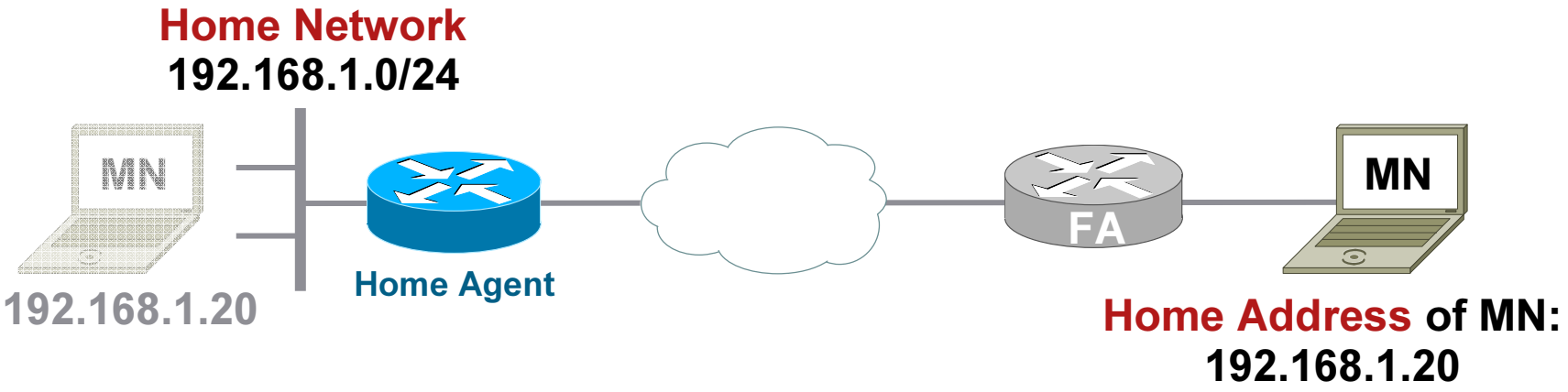
© 2007 Cisco Systems, Inc. All rights reserved.

RRQ Message Format



© 2007 Cisco Systems, Inc. All rights reserved.

Home Address and Home Network

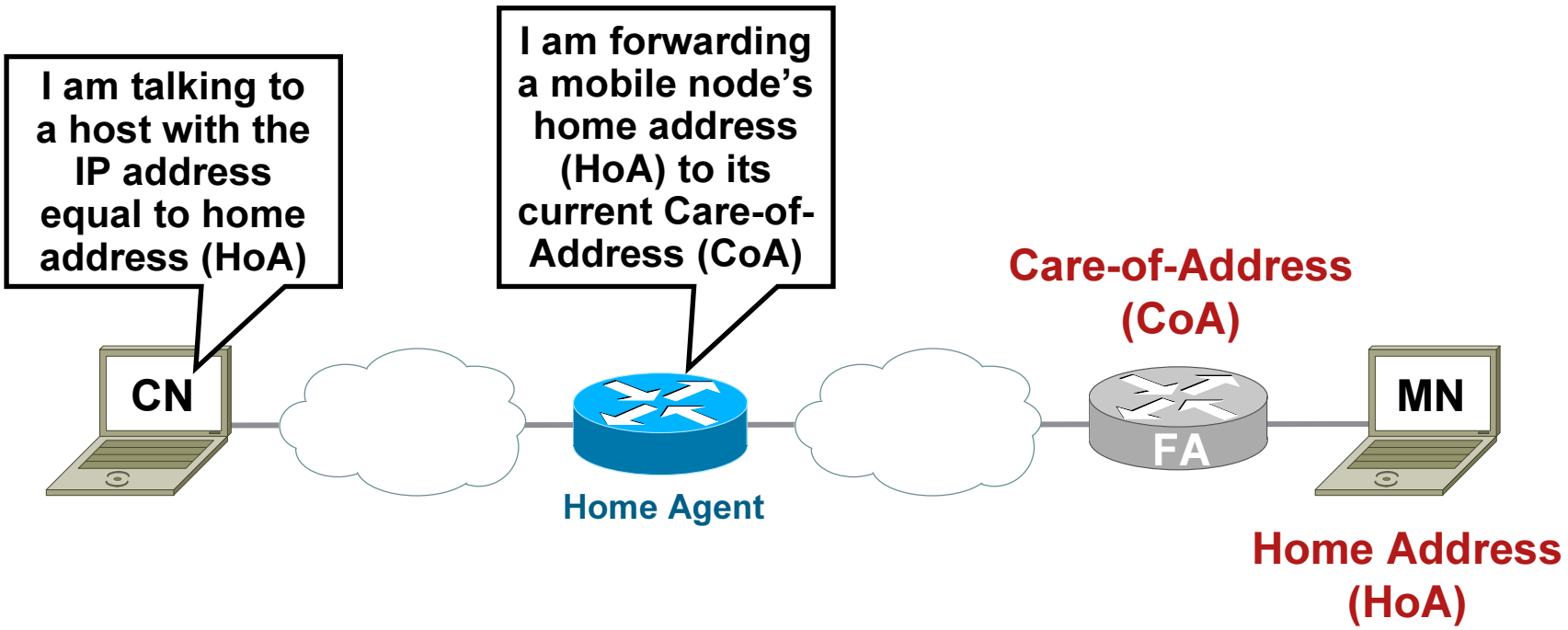


- Home Network
  - Networks attached to a Home Agent
  - Can be a physical or logical interface
  - Logical is usually easier to use
  - Cisco IOS® Software logical networks are called “virtual networks”

- Home Address
  - An IP address on the home network allocated to a Mobile Node
  - Used for all communication

© 2007 Cisco Systems, Inc. All rights reserved.

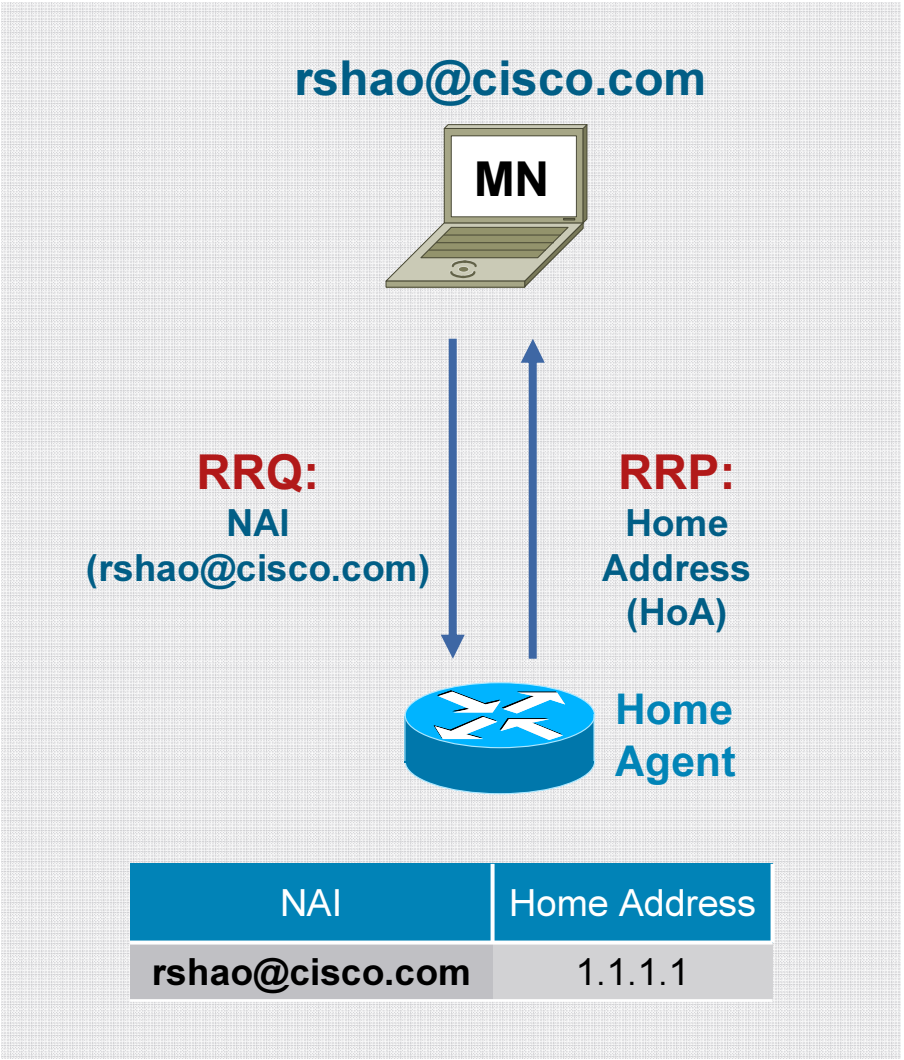
Home Address (HoA) vs. Care-of-Address (CoA)



© 2007 Cisco Systems, Inc. All rights reserved.

Another Method to Identify a Mobile Node

- Network Access Identifier (NAI)
  - Save IP addresses
  - a user name appended as an extension in registration message
  - Formation is either “user” or “user@realm”
- A home address still needs to be allocated to a mobile node when requested



© 2007 Cisco Systems, Inc. All rights reserved.

How Long Is the RRQ Valid?

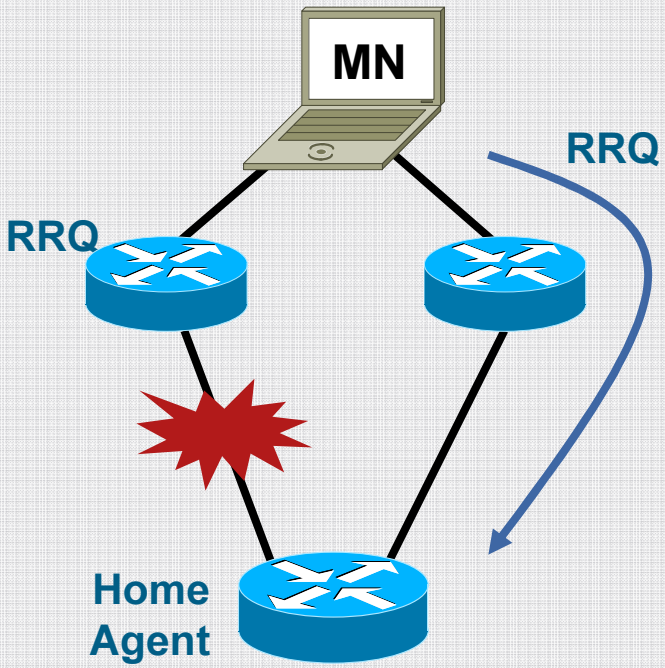
- Lifetime:

  Maximum amount of time a mobile node will be kept active

  RRQ is periodically sent

- Can be used to validate the path to a home agent

  Fast vs. performance



© 2007 Cisco Systems, Inc. All rights reserved.

Secure Authentication Review

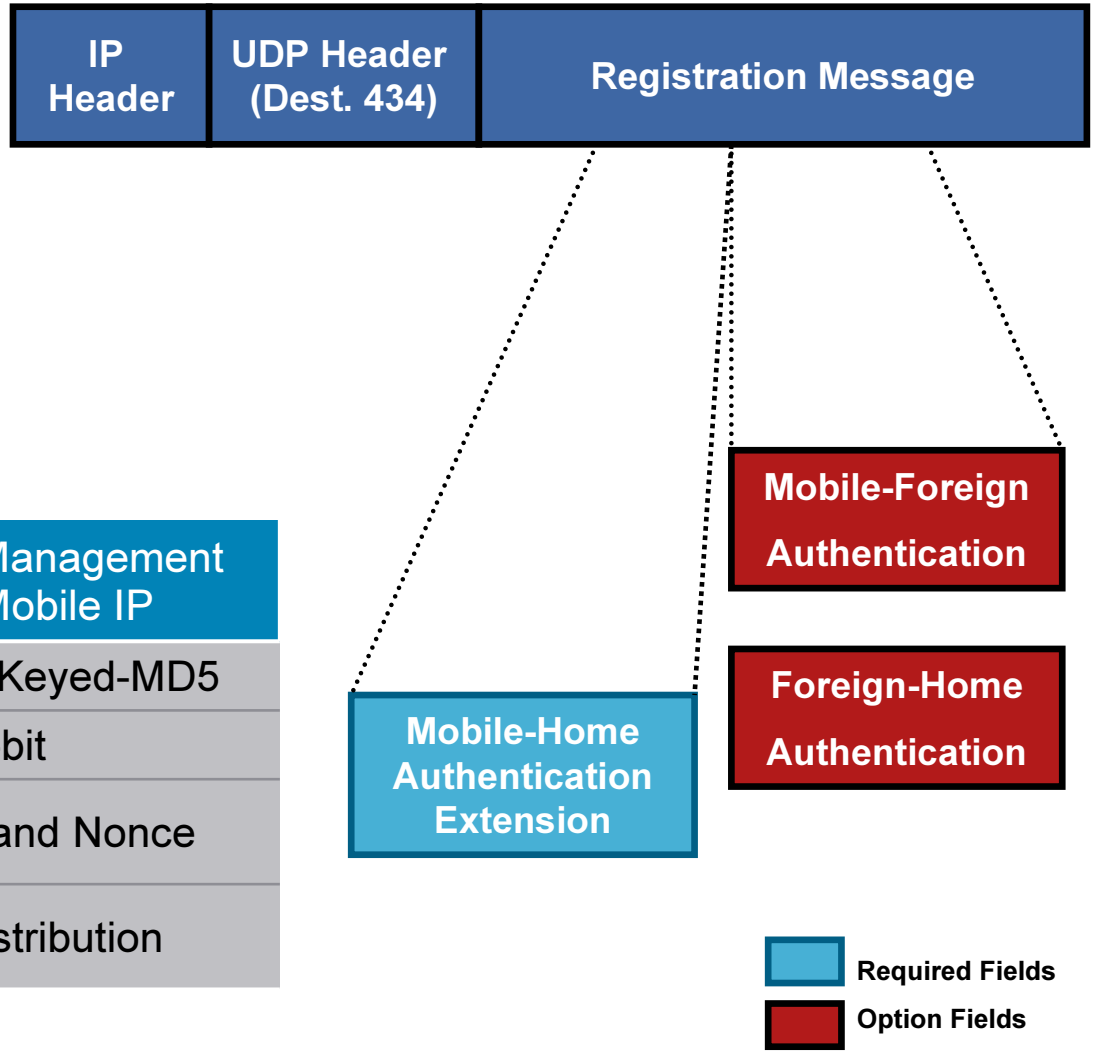
- Security Association (SA)
  - Is a set of security parameters used to sign a message
  - Hash algorithms
  - Key size
  - Replay protection
- Security Parameter Index (SPI)
  - Is a numeric identifier for the SA
  - Allows multiple SAs to be configured between two devices to support multiple sessions
- Key Management
  - Manual key distribution
  - Public Key Infrastructure (PKI)

© 2007 Cisco Systems, Inc. All rights reserved.

Mobile IP Registration Authentication

- Mobile IP authentication can occur between any two Mobile IP components
- The mandatory one is between the mobile node and home agent—known as MHAE

	SA and Key Management Used by Mobile IP
Algorithm	HMAC-MD5; Keyed-MD5
Key	128-bit
Replay Protection	Timestamp and Nonce
Key Management	Manual Distribution



© 2007 Cisco Systems, Inc. All rights reserved.

Registration Authentication MHAE, Example

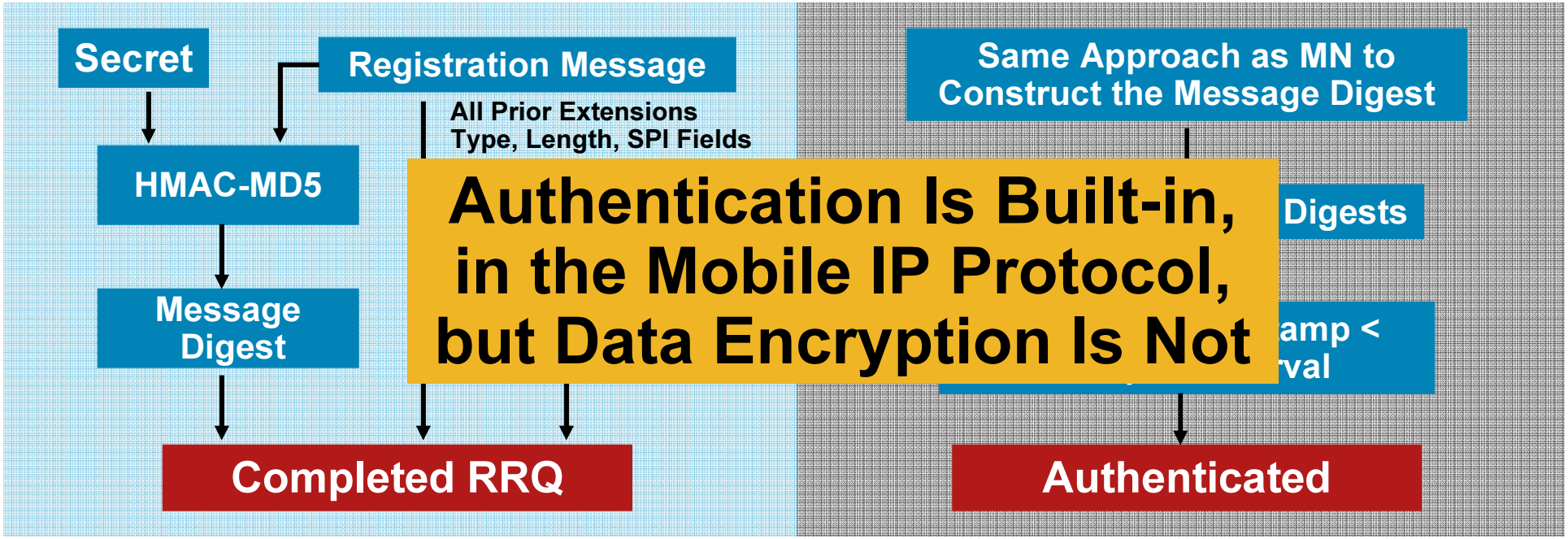
Selects SA Using SPI 100

	SPI 100
Algorithm	HMAC-MD5
Key	Secret
Replay Protection	Timestamp

Home Agent

Selects SA Using MN Home Address and SPI 100

	MN 10.1.1.1/ SPI 100
Algorithm	HMAC-MD5
Key	Secret
Replay Protection	Timestamp



© 2007 Cisco Systems, Inc. All rights reserved.

Registration Reply (RRP)

- Generated by HA to ACK the acceptance or rejection of the registration (RRQ)
- Packet format is similar to RRQ with an additional "code" field
- The code filed is particular useful to indicate what errors may be

- Reply codes range: 0 to 255
  - 0–8: Success
  - 64–127: Error from the Foreign Agent
  - 128–192: Error from the Home Agent
  - 192–255: Unallocated

- 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

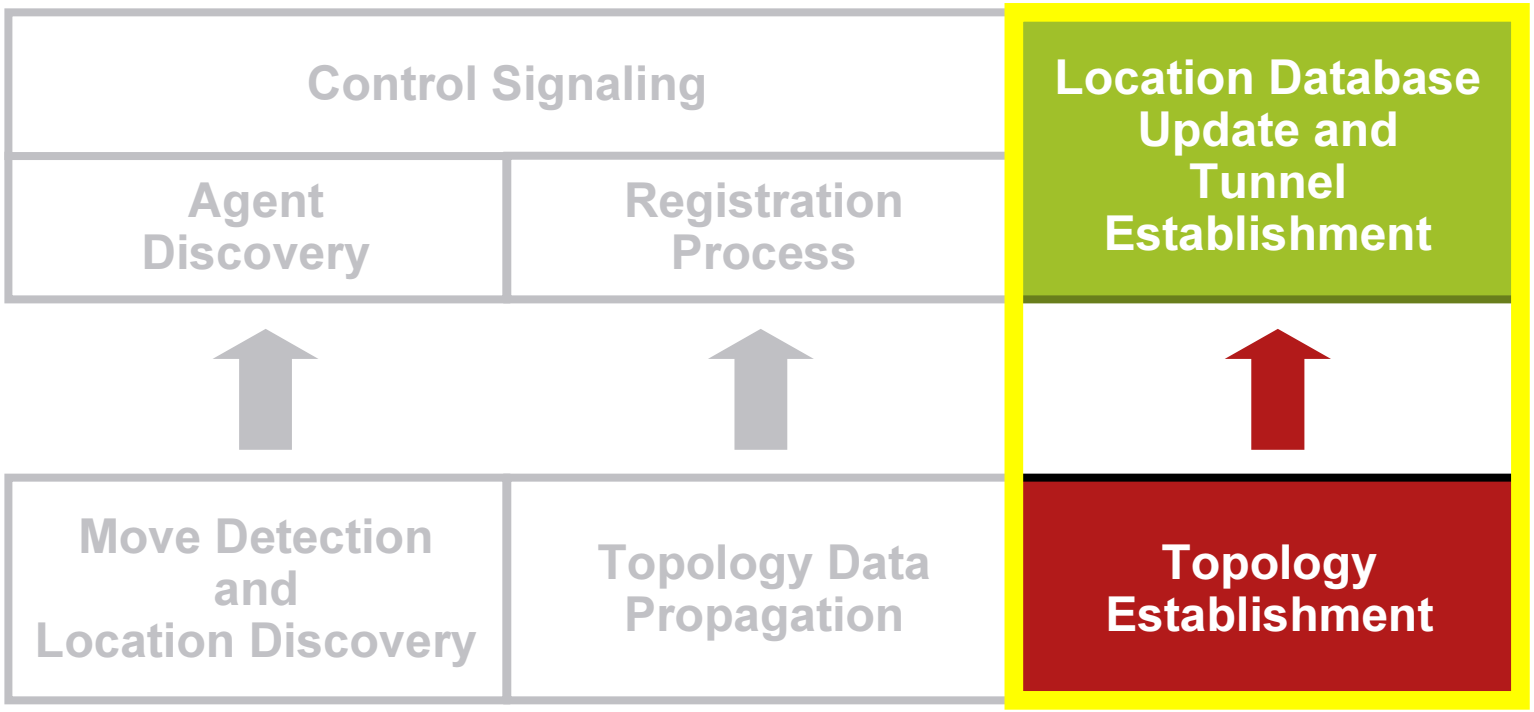
© 2007 Cisco Systems, Inc. All rights reserved.

Registration Messages Review

- What is used to represent the current location?
  - CoA or CCoA
- How to identify an MN?
  - Home address or "NAI"
- What is the destination of the registration messages?
  - Home Agent address
- How long is the registration valid?
  - Lifetime
- How can the network ensure that the MN is an authorized user?
  - Security Association
- How to response the success of registration message?
  - RFP Message

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Topology Establishment



© 2007 Cisco Systems, Inc. All rights reserved.

Topology Establishment

- Location database update

  Contains CoA (the current point of attachment) of a MN

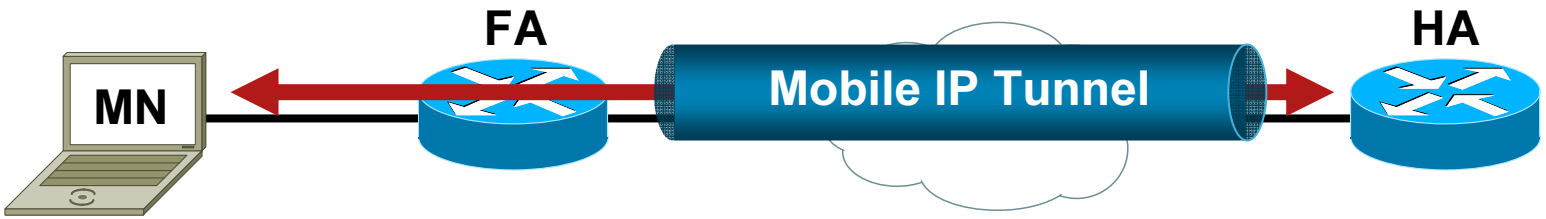
  Similar to a routing protocol's topology table

  The tables are known as "binding table" on a home agent and "visitor table" on a foreign agent in Cisco IOS Software

- Tunnel creation

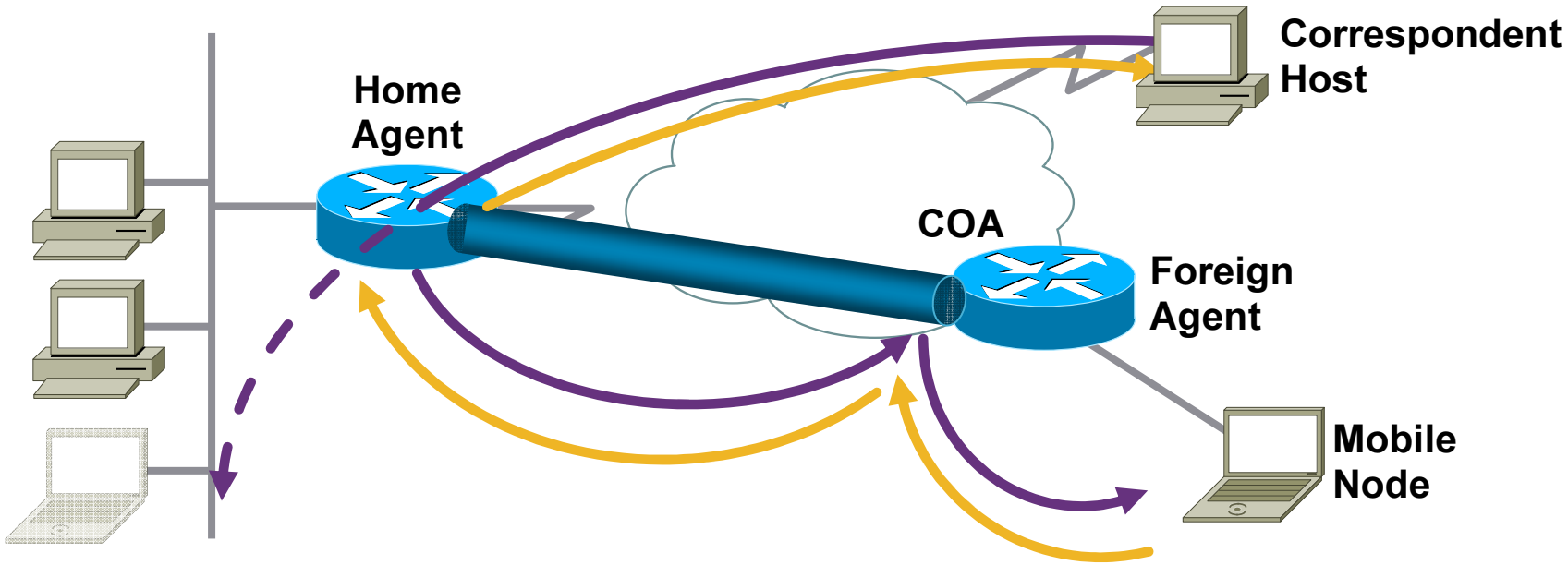
  A logical interface to forward traffic to and from a mobile node

  Can be an IPinIP, GRE, or UDP tunnel or referring to as a Mobile IP tunnel in the Mobile IP context



© 2007 Cisco Systems, Inc. All rights reserved.

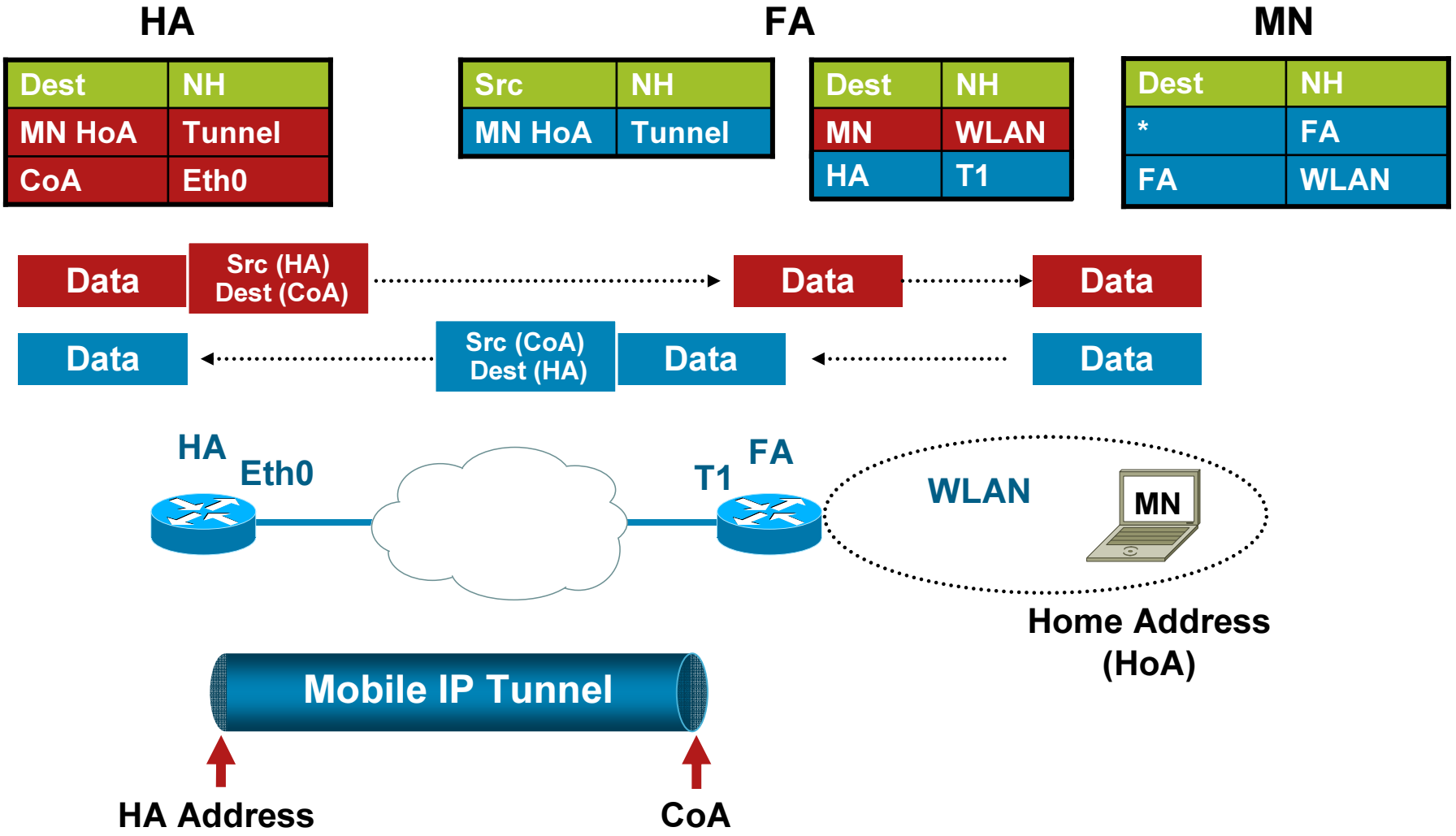
Reverse Tunneling



- Reverse Tunneling—Traffic is sent from the MN to the HA via the tunnel, then delivered via routing
- Ingress filtering and uRPF will drop packets that have topologically incorrect source address

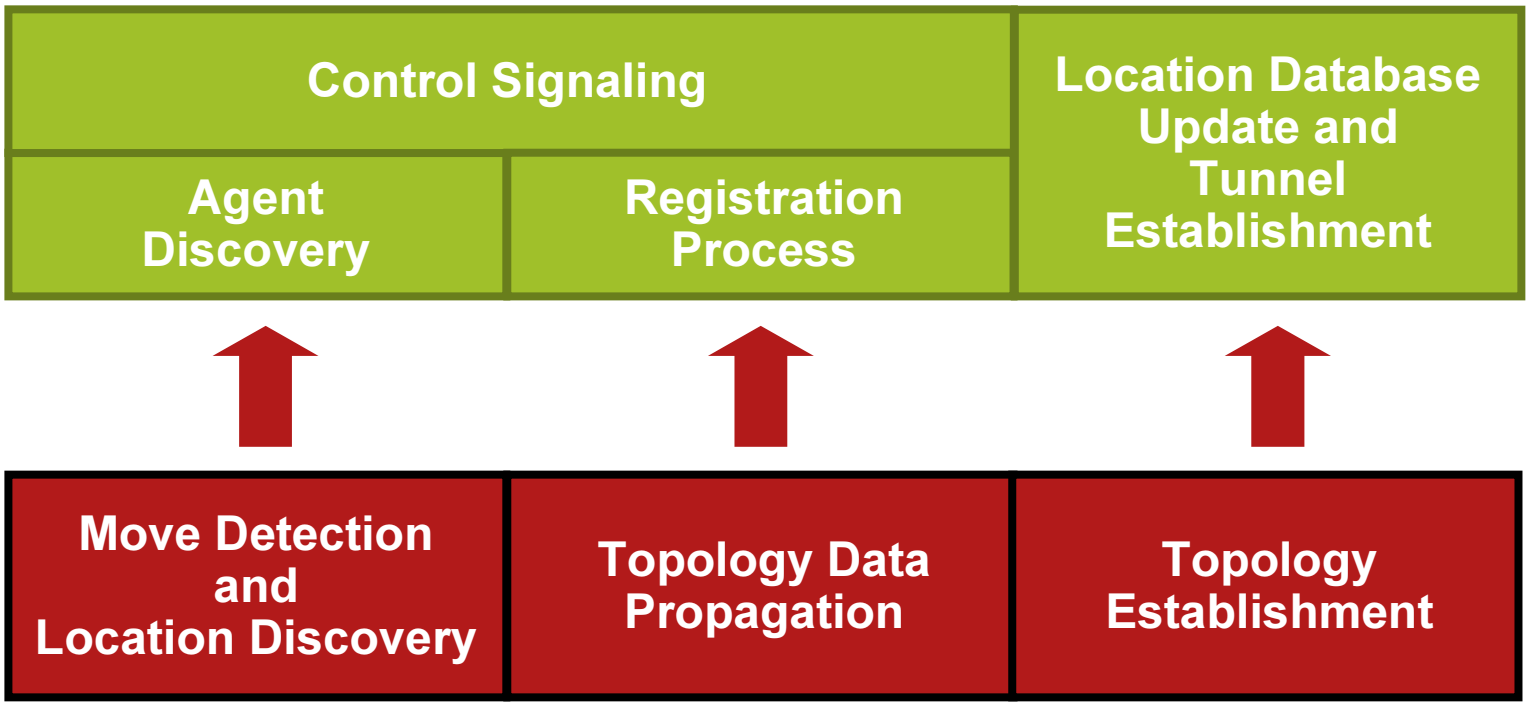
© 2007 Cisco Systems, Inc. All rights reserved.

Topology Establishment Example



© 2007 Cisco Systems, Inc. All rights reserved.

Mobile IP Protocol Summary



© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Mobile IP Implementations and Key Features

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Mobile IP Technology

- IETF RFC 3344 and 3GPP2 compliant
- General availability since January 1999
- Cisco platforms and software for Home Agent and Foreign Agent functions are

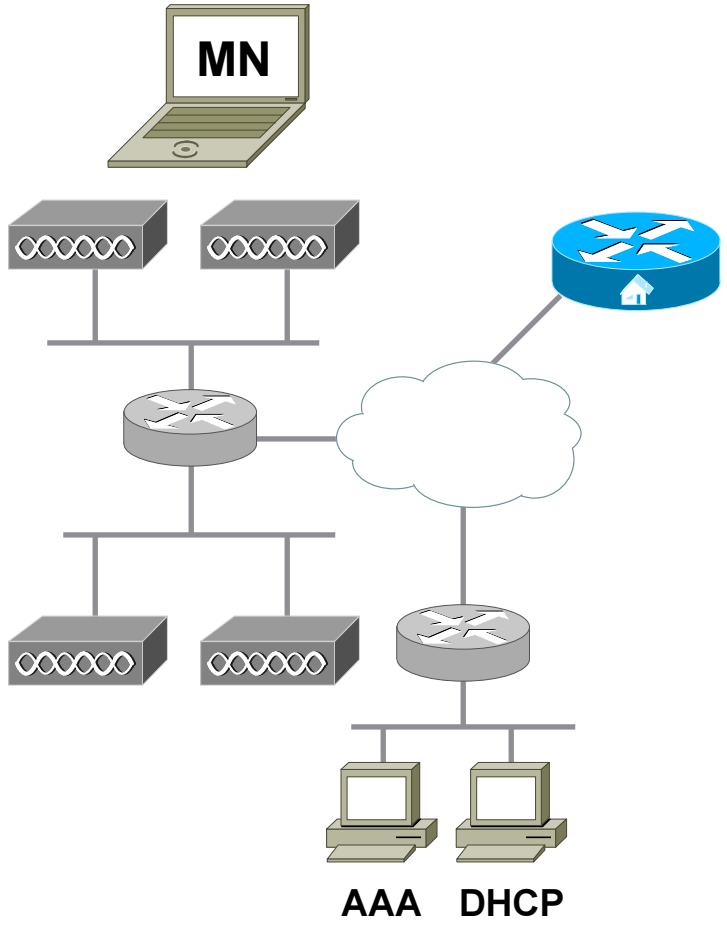
Hardware	Software	Standard Compliance
Cisco 1700, 2600XM, 3700	T Train with IP Plus Feature Set or Above	IETF RFC 3344
Cisco 1800, 2800, 3800, 7200, 7300, 7400	T Train with IP Voice Feature Set or Above	IETF RFC 3344
Cisco 7200, MWAM	SX Image	IETF RFC 3344 and 3GPP2

- 3rd party standard compliant Mobile IP clients can be used with the Cisco Home Agent and Foreign Agent

© 2007 Cisco Systems, Inc. All rights reserved.

Adding Mobile IP

- Adding mobile IP is as simple as adding an HA or enabling the HA on an existing router
- … and installing client software
- Mobile IP can run in co-located Care-of-Address mode



© 2007 Cisco Systems, Inc. All rights reserved.

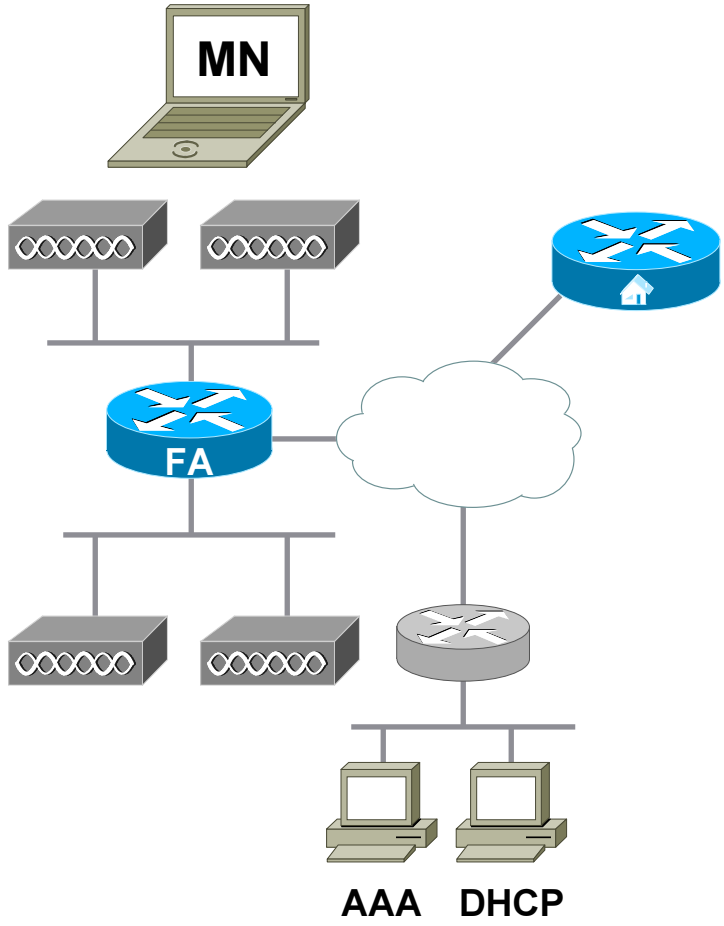
Home Agent Configurations

AAA	aaa new-model aaa authorization ipmobile default group radius !
Home Network	interface FastEthernet0/0 ip address 192.168.1.1 255.255.255. 0 !
Enable Mobile IP Process	router mobile !
Enable HA and Identify Clients Allowed to Roam	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	radius-server host 10.82.70.12 key itsasecret

© 2007 Cisco Systems, Inc. All rights reserved.

Turning on the FA

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



© 2007 Cisco Systems, Inc. All rights reserved.

FA Configuration

COA Interface	interface Loopback0 ip address 192.168.250.1 255.255.255.255 !
Foreign Interface	interface FastEthernet0/1 ip address 192.168.101.1 255.255.255.0 ip irdp ip mobile foreign-service ip mobile prefix-length !
Enable Mobile IP Process	router mobile !
Enable the Foreign Agent	ip mobile foreign-agent care-of Loopback0/0

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Mobile IP
Key Features You Have Most Likely Encountered

© 2007 Cisco Systems, Inc. All rights reserved.

NAT Traversal

Special Consideration Is Required When the CoA Is a Private Address Behind a NAT or PAT

RFC 3519 NAT Traversal

- Supports NAT and PAT
- Uses UDP tunneling
- Auto detect or forced usage
- Cisco IOS Software Release 12.3(7)T
- ip mobile home-agent nat traversal [keepalive <time>] [force <accept | reject>]

Cisco NAT Detection

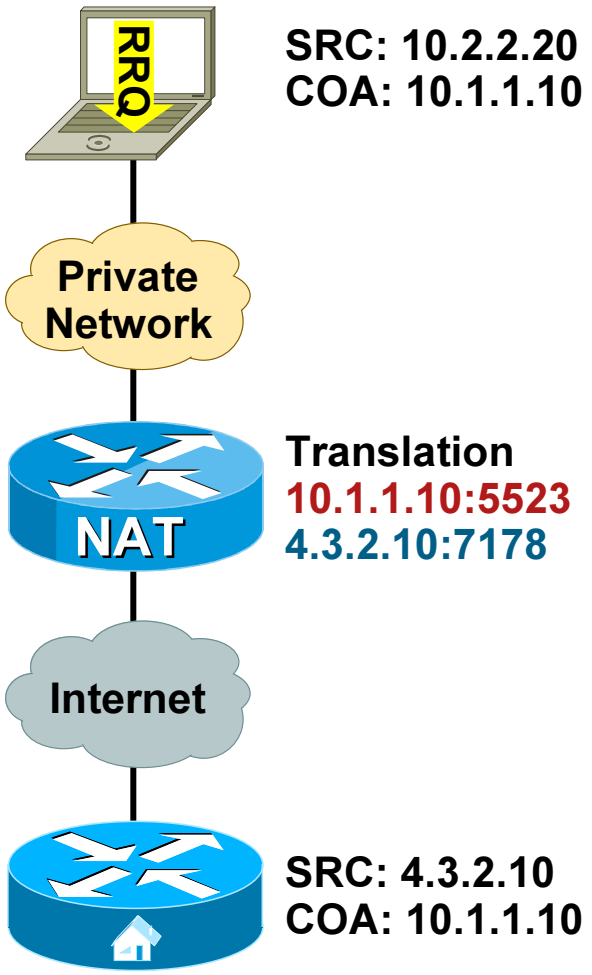
- NAT only
- Uses IPinIP or GRE tunnel
- Release 12.2(13)T
- ip mobile home-agent nat-detect

- Does not support Home Agent behind a NAT

© 2007 Cisco Systems, Inc. All rights reserved.

NAPT Traversal Detection

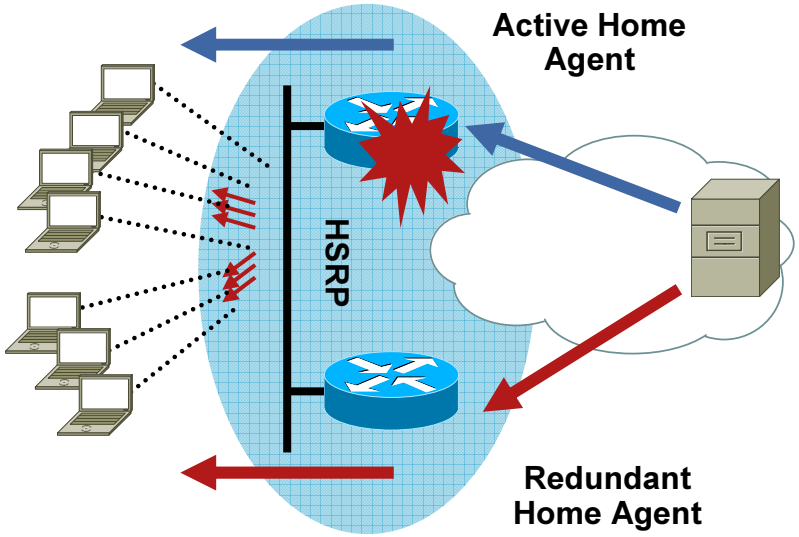
- Outbound registration sets up the NAT translation
- Home Agent detects that source of registration is not the same as CoA
- If RRQ contains UDP tunneling extension, the HA enables UDP tunneling
- MN can force UDP tunneling for firewall traversal

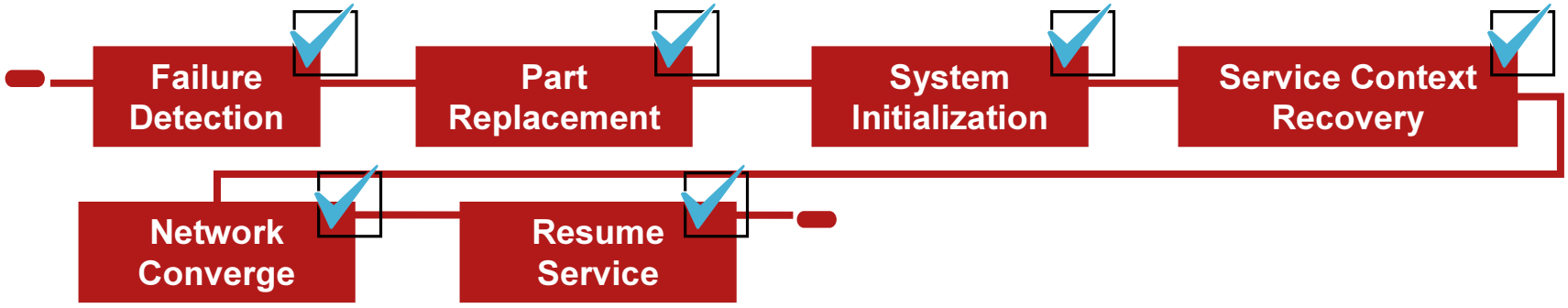


© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Stateful Home Agent Redundancy

- Uses Cisco HSRP to detect the failure within seconds
- The redundant Home Agent is in the “standby” mode
- The redundant Home Agent contains real-time mobile user’s service context
- The redundant Home Agent is participating in the network routing and can forward traffic if needed





Derived from Enterprise Costs: Infonetics Research, September 2000

© 2007 Cisco Systems, Inc. All rights reserved.

Mobile IPv6

© 2007 Cisco Systems, Inc. All rights reserved.

Mobile IPv6 Protocol

- RFC 3775
- Similar to the Mobile IPv4 concept
  - A home agent keeps track of the mobile node's location
  - Including location discovery, movement detection, registration, and topology establishment
- Different from the Mobile IPv4
  - No Foreign Agent
  - Traffic can be sent directly between two communicating nodes
- A driver for IPv6

© 2007 Cisco Systems, Inc. All rights reserved.

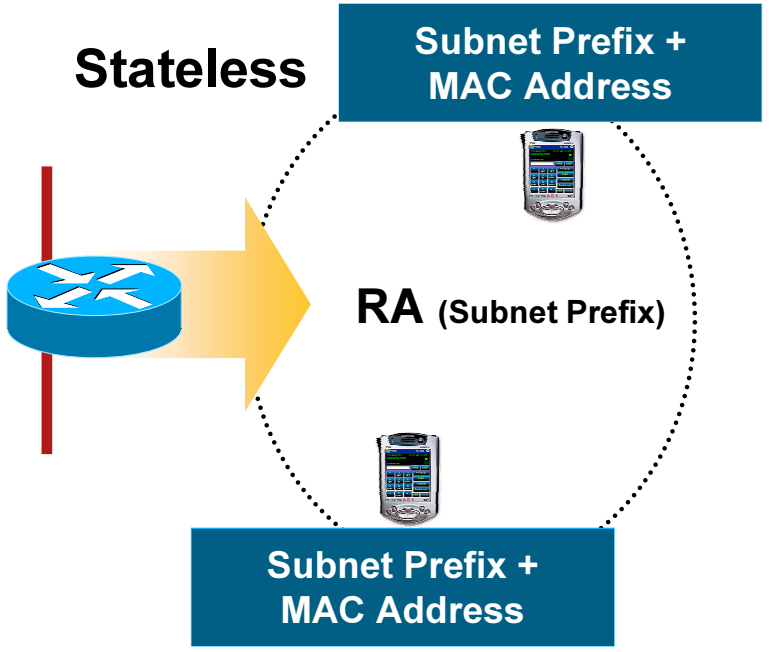
Location Discovery: IPv6 Host Address Auto-Configuration

- Stateless (RFC 2462)

  Host autonomously configures its own Link-Local address

  Router Solicitation (RS) are sent by booting nodes to request Router Advertisement (RA)

- Stateful (DHCPv6) (RFC 3315)
- The acquired address is the CoA—represents the point of attachment



A Host Builds a Link-Local Address, then Its Global IPv6 Address(es) from the RA

© 2007 Cisco Systems, Inc. All rights reserved.

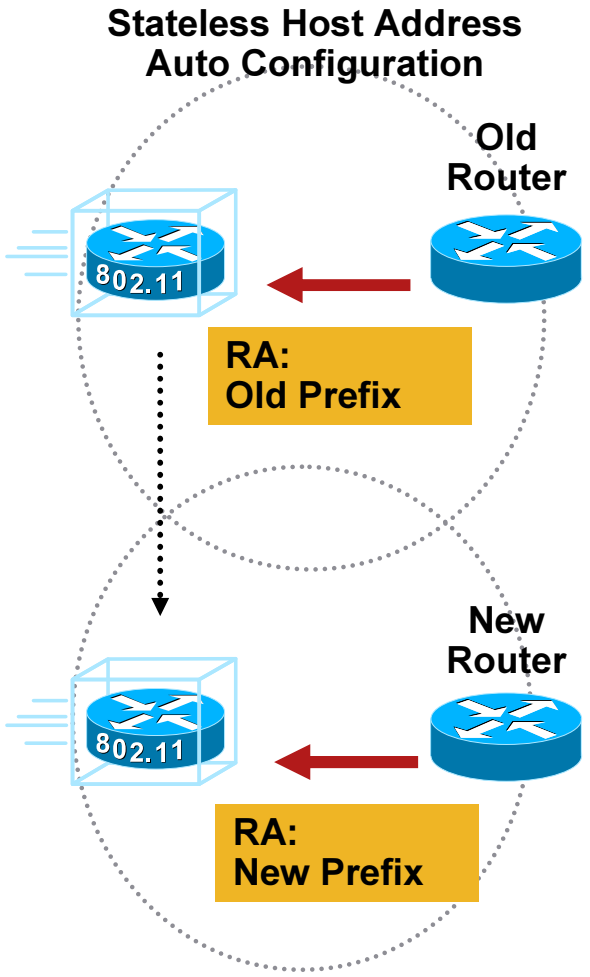
Movement Detection

- Informs Home Agent of a new point of attachment
- How?

  Slightly complicated, but conceptually…

  When a new prefix has appeared and the current default router has disappeared
- Fast detection is possible

  msec vs. sec for Router Advertisement interval
- Can also be done using link layer—up/down

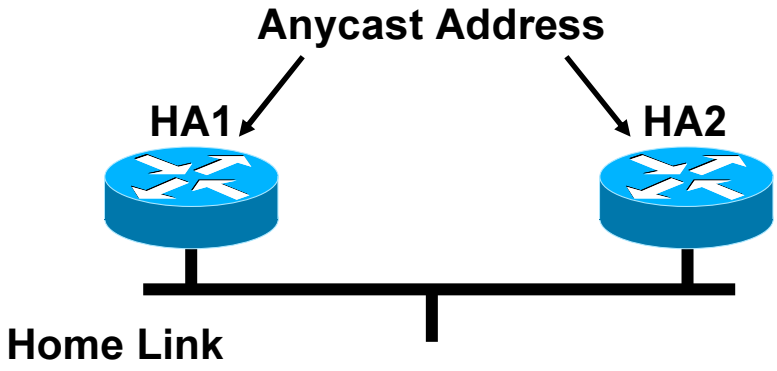


© 2007 Cisco Systems, Inc. All rights reserved.

Dynamic Home Agent Address Discovery (DHAAD)

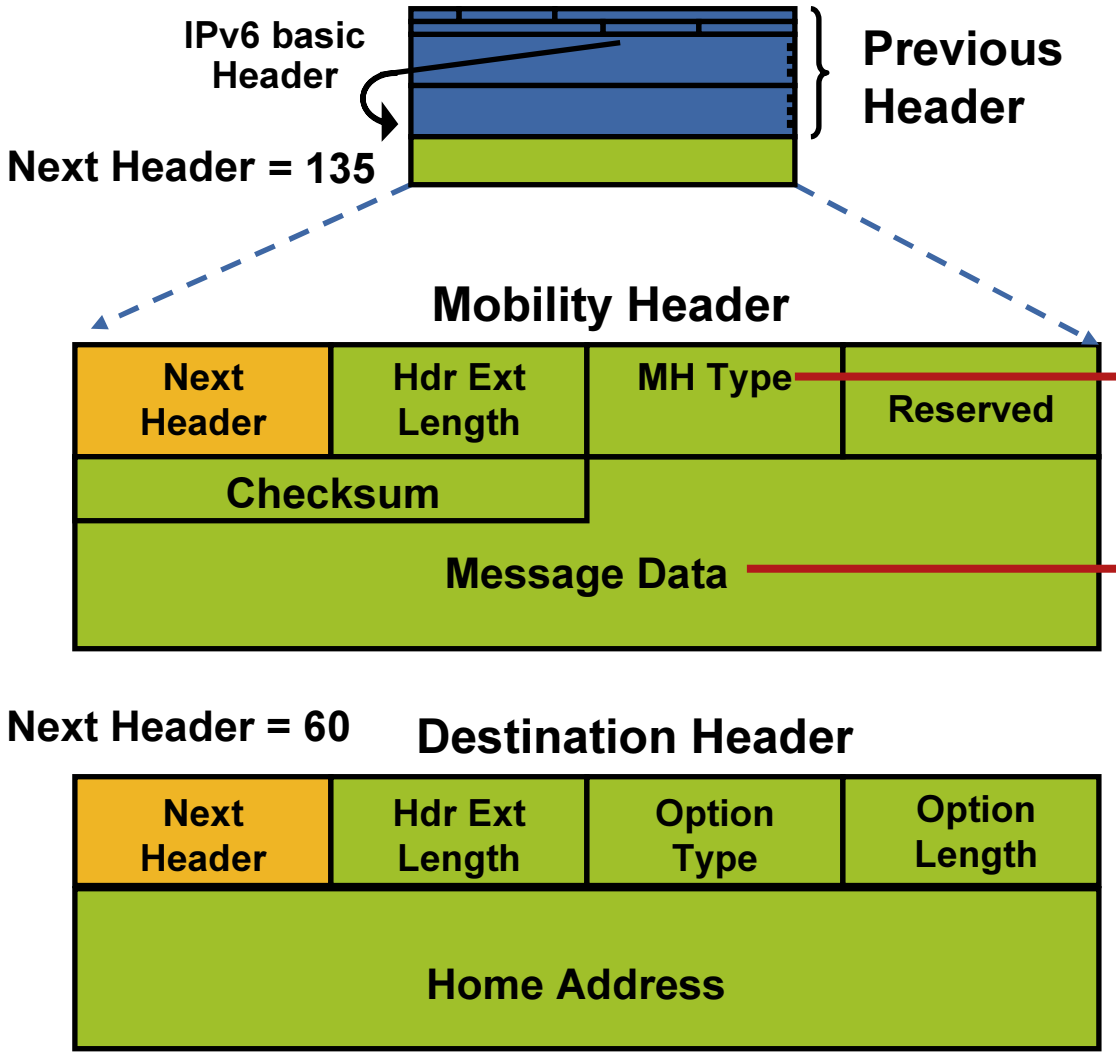
RFC 3775

- A mechanism to find an active home agent in the home link
  - MN still needs to configure the home link address
  - But not the specific home agent address—Anycast address
- Useful if an existing home agent router needs to be replaced
  - Mobile nodes away from home can automatically use the new home agent
- Provides a failover protection
- A non-stateful approach



© 2007 Cisco Systems, Inc. All rights reserved.

IPv6 Protocol Extensions for Mobile IPv6



- Defined for Mobile IPv6 registration and binding creation
- Various types and option extensions
- RFC 3775 for details

Example

MH Value	Message
5	Binding Update
6	Binding Acknowledge
0	Binding Refresh Request

Alternate Care-of-Address Option

© 2007 Cisco Systems, Inc. All rights reserved.

Registration

RFC 3775

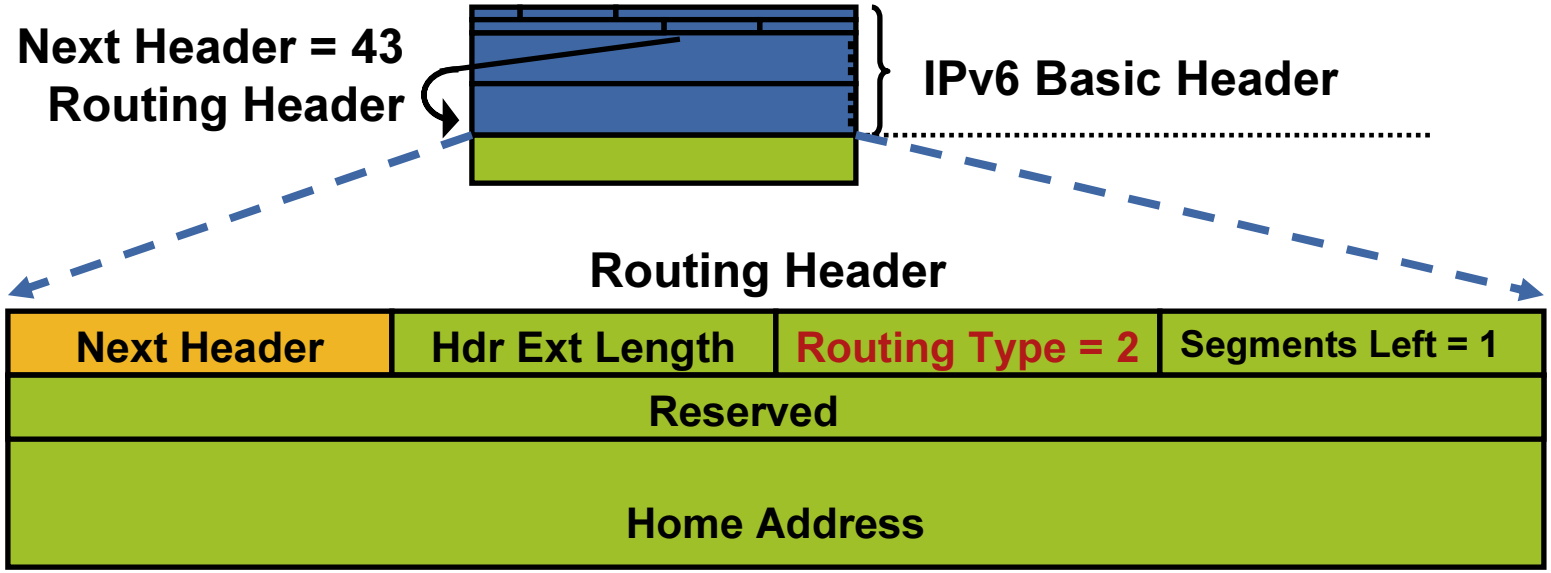
- Two important messages you should know
  - Binding Update (BU) and Binding Acknowledge (BA)
- Encapsulation vs. option extensions
- Care-of-Address
  - Typically derived from the source IP address of the header
  - Optionally stored in the "alternative care of address" field
- Home address
  - Stored in Destination Option header of IPv6

Mobile IPv4 Comparison

- RRQ and RRP
  - UDP (434) encapsulation
- Care of address
  - A field inside of RRQ
- Home address
  - A field inside of RRQ

© 2007 Cisco Systems, Inc. All rights reserved.

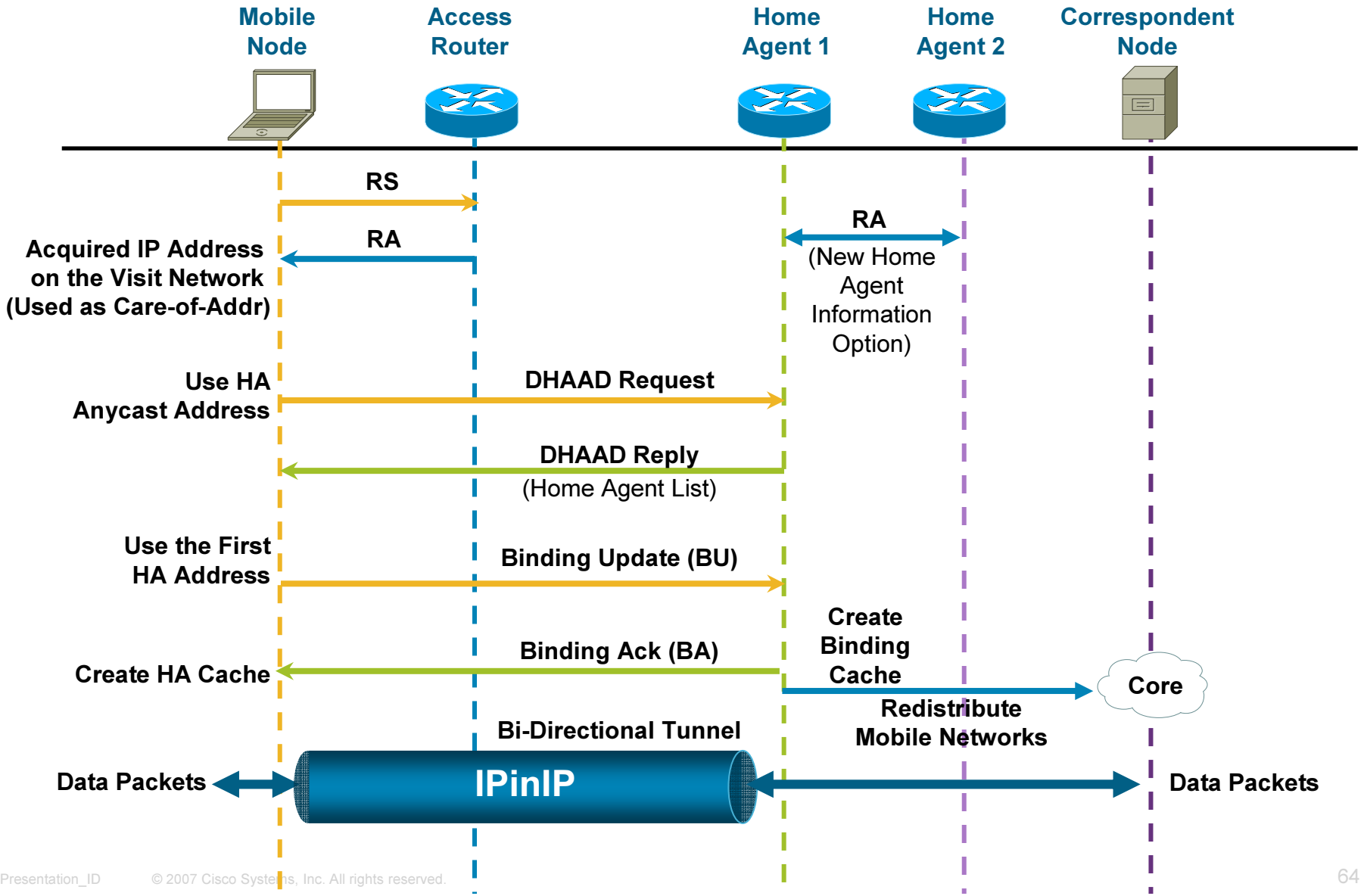
Type 2 Routing Header



- A new routing header variant
- Allows a packet to be routed directly from a CN to an MN CoA
- CoA is inserted in the IPv6 Destination Address field (from CN)
- MN swaps the Home Address in the routing header with the destination address in the IP header (normal IPv6 process)

© 2007 Cisco Systems, Inc. All rights reserved.

Put All Together: Mobile IPv6 Registration



© 2007 Cisco Systems, Inc. All rights reserved.

Mobile IPv6 Product Availability

- Cisco Mobile IPv6 Home Agent available in Cisco IOS Software Release 12.3(14)T
  - RFC 3755 compliance
  - Does not support IPsec yet
- Mobile IPv6 client
  - Microsoft Tech preview for Windows XP and 2000

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Mobile IP Applications
Mobile Networks

© 2007 Cisco Systems, Inc. All rights reserved.

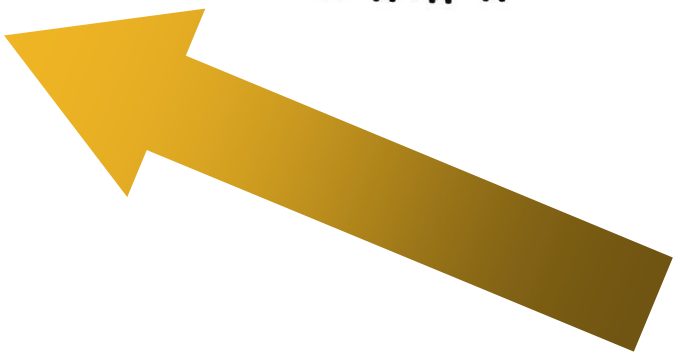
Host Mobility vs. Group Mobility

Host Mobility

I can go anywhere I want!

Group Mobility

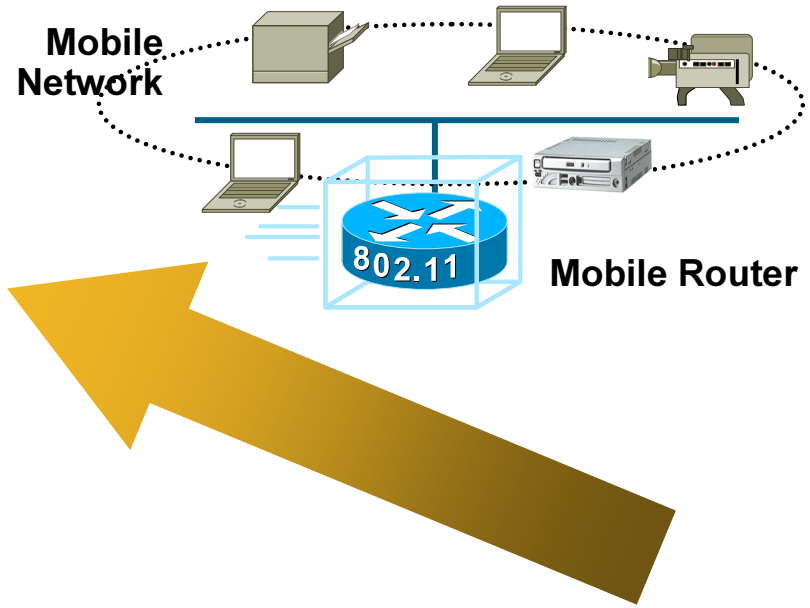
Free ride! Saves us lots of energy!



© 2007 Cisco Systems, Inc. All rights reserved.

Network Mobility

- Capability to enable IP mobility for a group of hosts
- Also known as “Mobile Networks” in Cisco
- The network or subnet where the group of hosts connected to is referring to as “mobile network”
- The router where the mobile network is connected to is referring to as “mobile router”

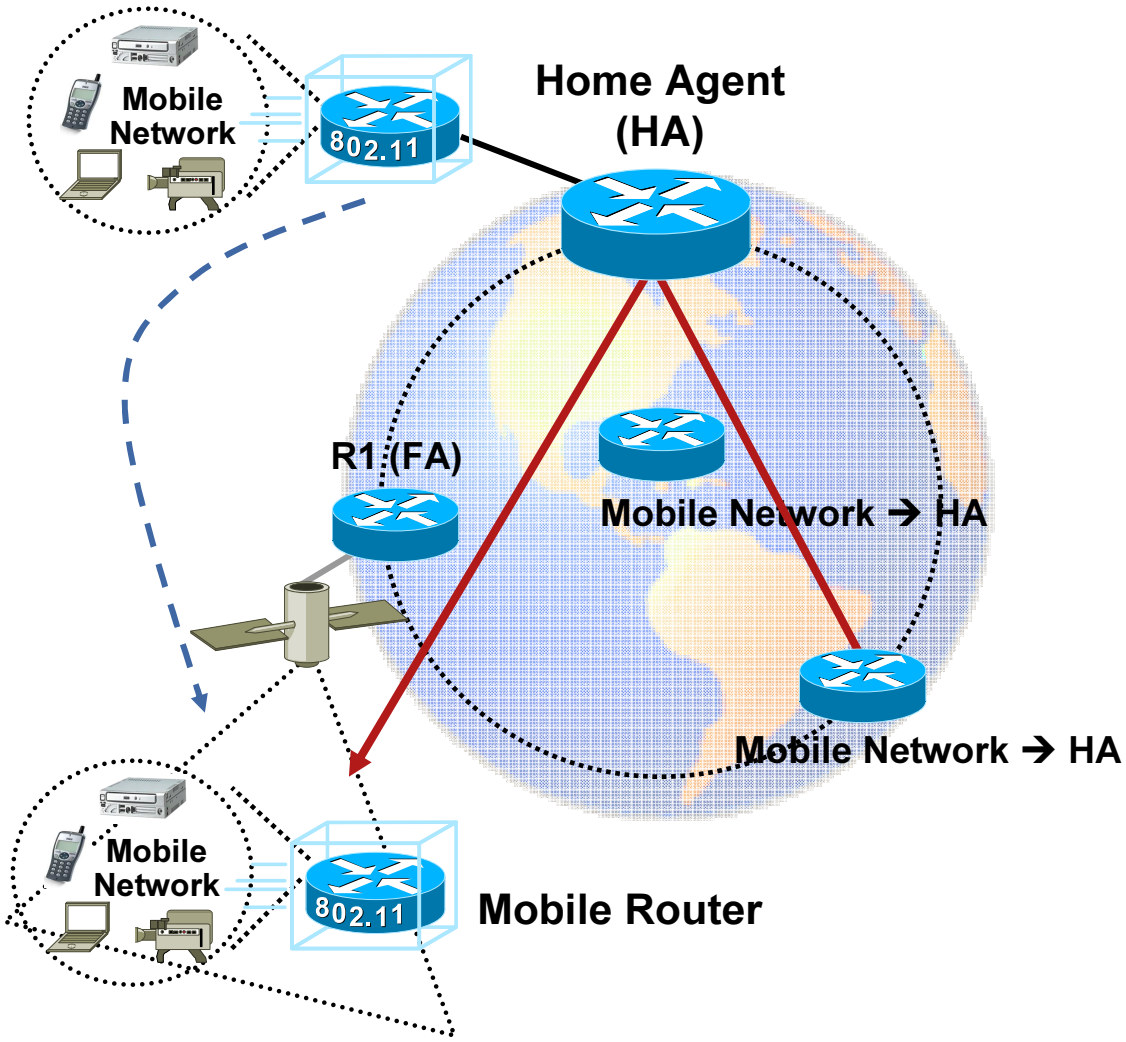


© 2007 Cisco Systems, Inc. All rights reserved.

ANIMATION

Mobile Networks Solution Concept

- Based on the same concept as the Mobile IP
- Home Agent as the gateway to route traffic destined to a mobile network
- Foreign agent is optional
  - Useful for fast roaming, performance, and management improvement
- Mobile Router (MR) is similar to a mobile node but with a network connecting to it



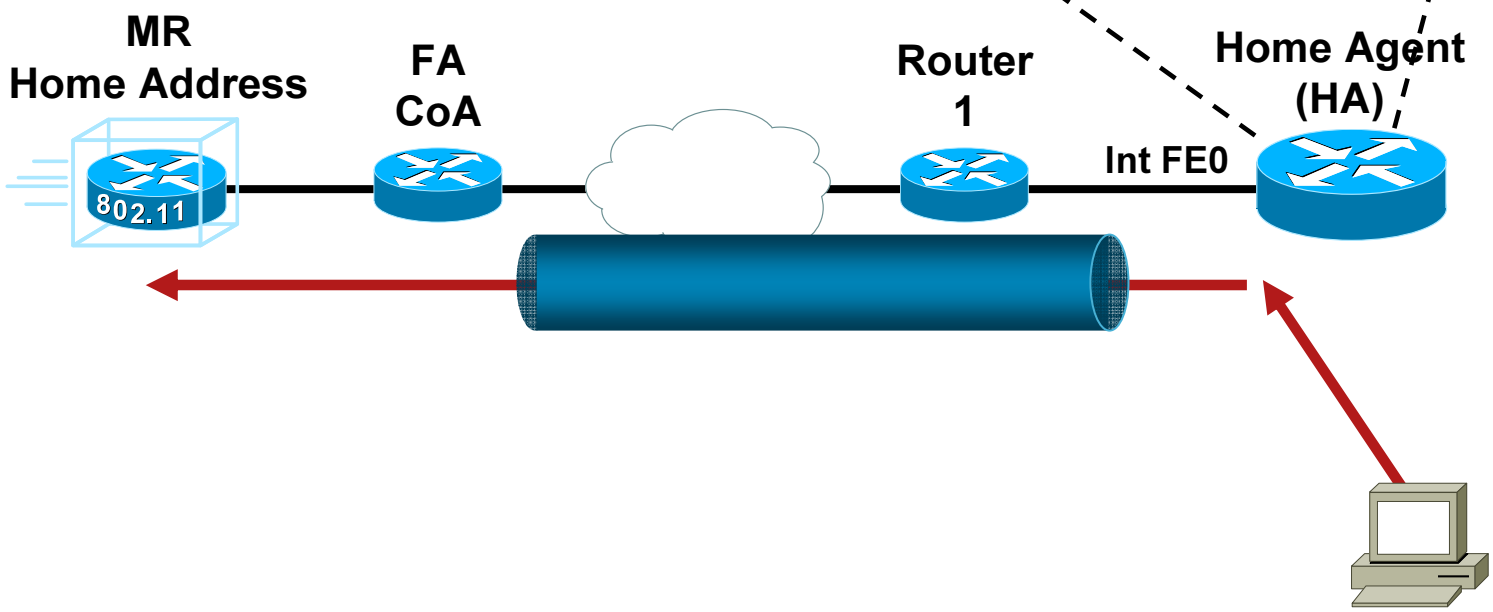
© 2007 Cisco Systems, Inc. All rights reserved.

More Details…

Basic Mobile IP Concept

- For traffic destined to a mobile router, it is routed as usual

Destination	Next Hop	Out Int.
MR Home Address	CoA	Tunnel Blue
CoA	Router 1	Int. FE0

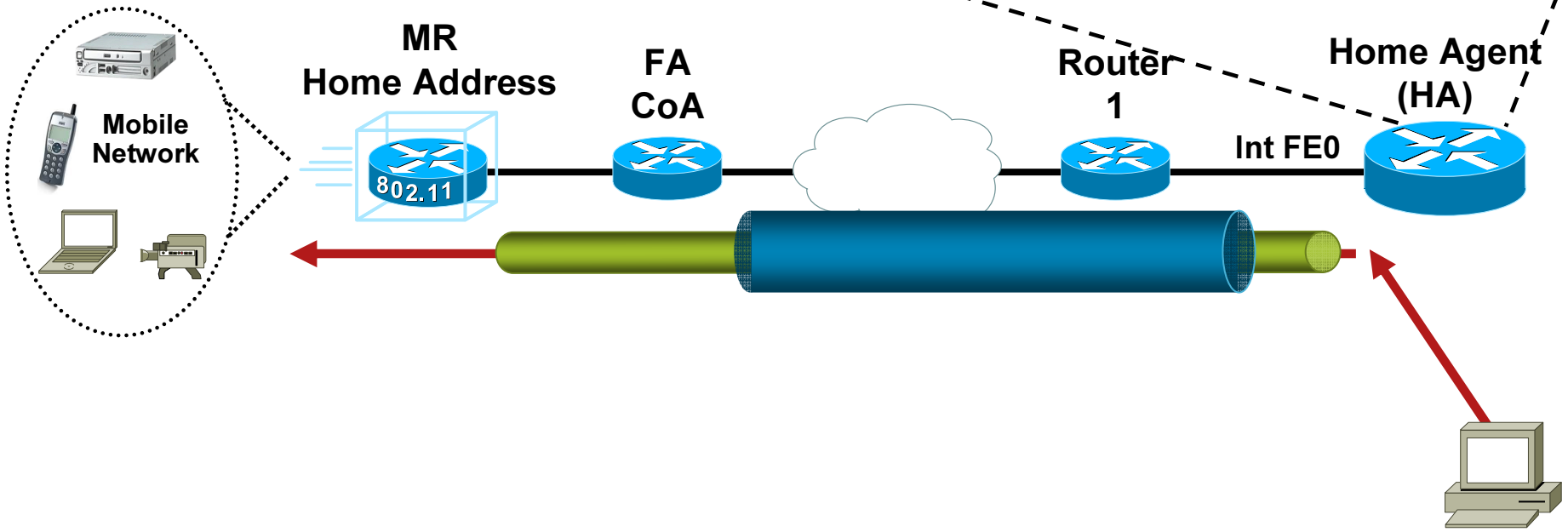


© 2007 Cisco Systems, Inc. All rights reserved.

More Details… (Cont.)

- If I know how to reach a mobile router, then I can simply forward the mobile network associated with the mobile router to that mobile router

Destination	Next Hop	Out Int.
Mobile Network	MR Home Address	Tunnel Green
MR Home Address	CoA	Tunnel Blue
CoA	Router 1	Int. FE0



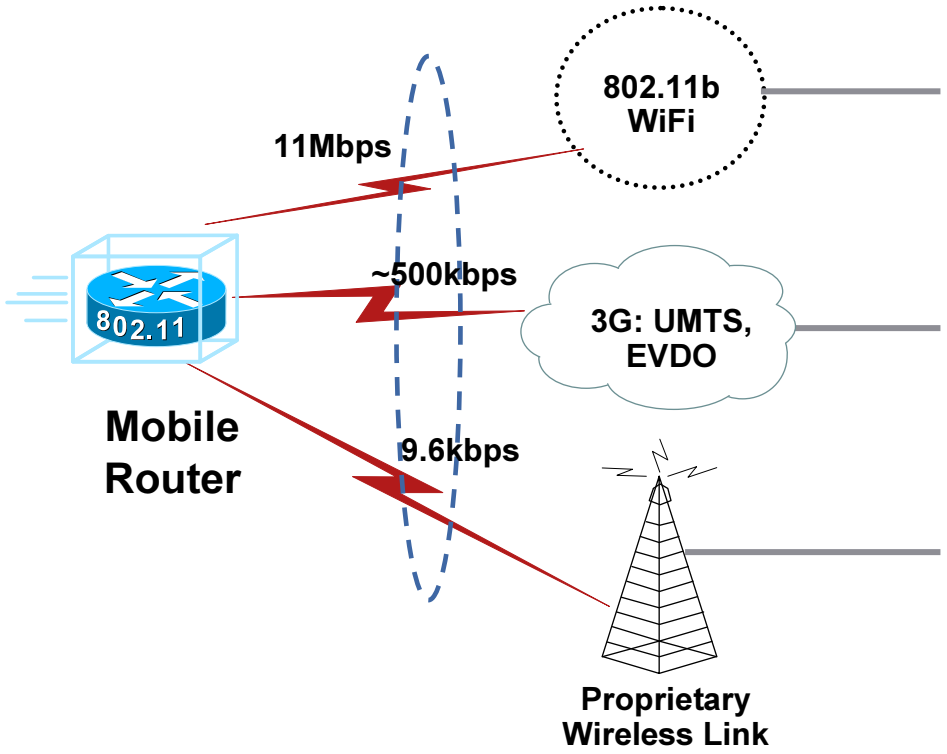
© 2007 Cisco Systems, Inc. All rights reserved.

Connection Management on Cisco Mobile Router

- Multiple links are likely equipped by a mobile router
- Select the “best” link to establish a Mobile IP tunnel

Selection Algorithm

- Priority can be configured on mobile router interfaces (default 100)
- MR prefers to register with higher priority interface
- If priority is equal, the interface with the higher bandwidth is preferred
- If priority and bandwidth are equal, then the interface with the higher IP address is preferred



© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Mobile Networks

- Cisco home agent and foreign agent

  The same home agent routers and the foreign agent routers running Cisco IOS Software Release 12.2T or later for the mobile nodes can be used for the mobile networks

- Cisco mobile routers

  Available in the Cisco IOS Software Release 12.2T or later

- Support Cisco Home Agent Redundancy and NAT traversal features

- Cisco Mobile Networks for IPv6

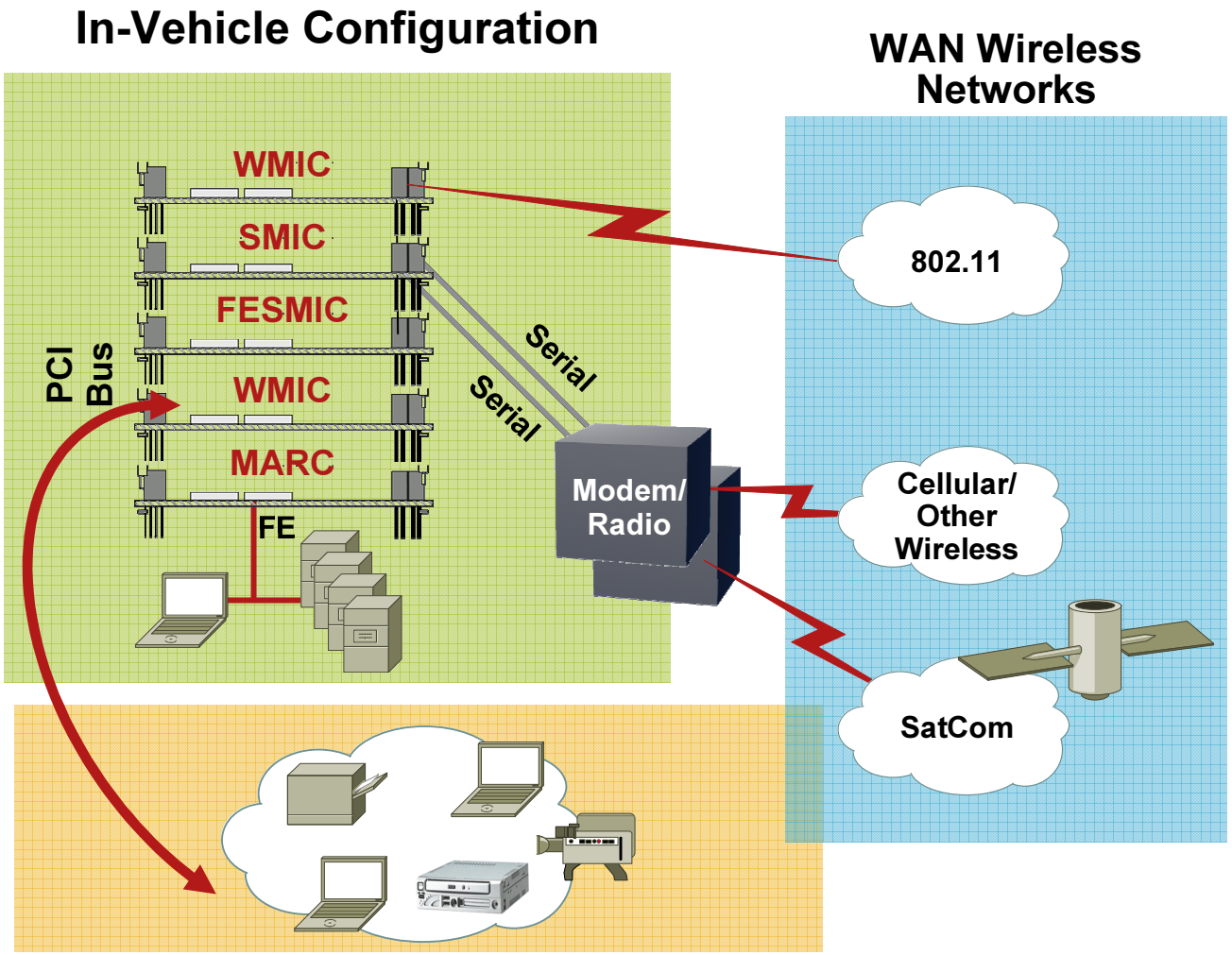
  Implementation is based on IETF RFC3963—NEMO

  Test image is available

© 2007 Cisco Systems, Inc. All rights reserved.

Cisco Mobile Access Router 3200

- A special rugged router
- Equipped with 802.11 wireless cards
- Connecting to an external wireless modem through a serial interface



© 2007 Cisco Systems, Inc. All rights reserved.

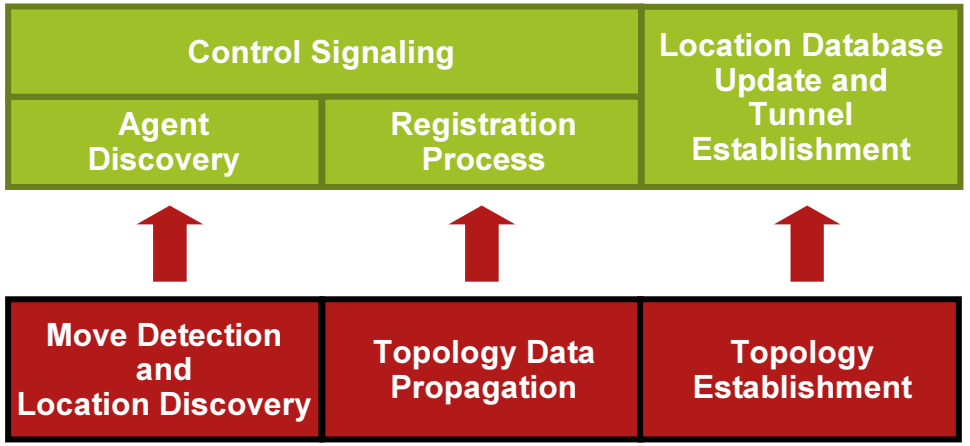
Wrap up

© 2007 Cisco Systems, Inc. All rights reserved.

Summary

- IP Mobility is a key functionality for mobile wireless networking

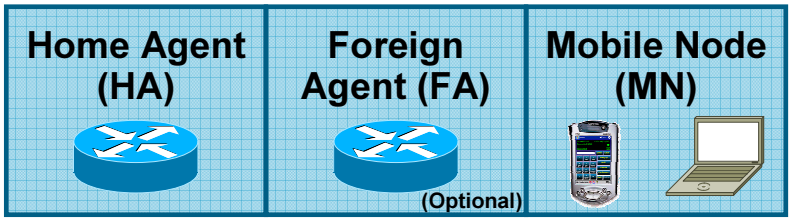
- Mobile IP, a IP Mobility protocol, enables seamless multi-access roaming



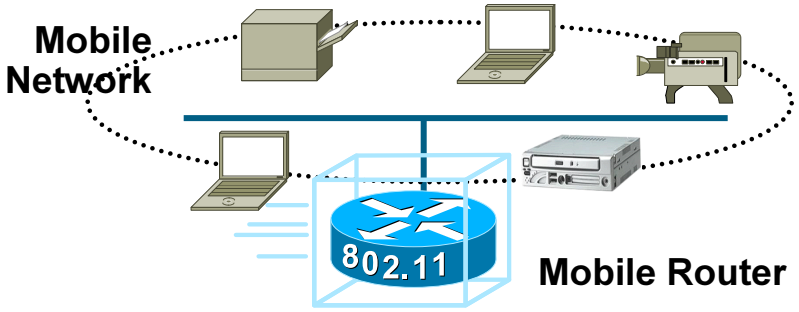
© 2007 Cisco Systems, Inc. All rights reserved.

Summary (Cont.)

- Components to construct a Mobile IP network



- Cisco Mobile Networks enables mobility for an entire subnet



© 2007 Cisco Systems, Inc. All rights reserved.

Reference Materials

- Cisco Mobile IP on CCO

  Collateral: http://www.cisco.com/go/mobile_ip

  Feature Navigator: http://www.cisco.com/go/fn

- Mobile IP Client

  Birdstep: http://www.birdstep.com

  IPunplugged: http://www.ipunplugged.com

- IETF Standards

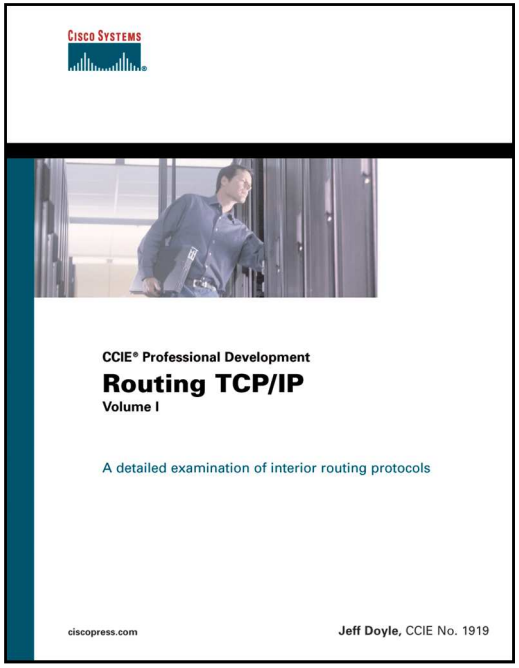
  http://www.mip4.org

  http://www.ietf.org/html.charters/mip4-charter.html

© 2007 Cisco Systems, Inc. All rights reserved.

Recommended Reading

- Mobile IP Technology and Applications, ISBN: 1-58705-132-X
- 802.11 Wireless LAN Fundamentals [1-58705-077-3]
- Wireless Networks First-Step [1-58720-111-9] available August 2004
- Deploying License-Free Wireless Wide-Area Networks [1-58705-069-2]
- 802.11 Wireless Network Site Surveying and Installation [1-58705-164-8] available September 2004



Available On-Site at the Cisco Company Store

© 2007 Cisco Systems, Inc. All rights reserved.

Q and A

© 2007 Cisco Systems, Inc. All rights reserved.

© 2007 Cisco Systems, Inc. All rights reserved.