Introduction to Cisco IOS® Mobile IP

Derick Linegar
Consulting System Engineer
dlinegar@cisco.com

Agenda

- Internet Mobility
  - Challenges
  - The Solution - Mobile IP
- Target Markets
- Cisco IOS & Mobile IP
- Deployment Scenarios
- Summary

Goals of Internet Mobility

- Not constrained by location
- Always on IP connectivity
- Transport Independent
- Robust Roaming Connections
- Application Mobility
- Application Continuity
- IPv4 and IPv6

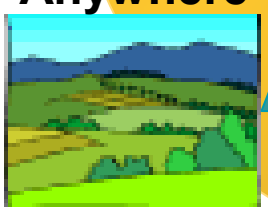
Mobility Vision

Office

Hotspots

Home

Anywhere



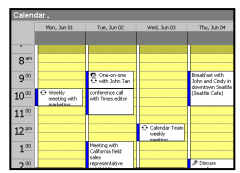
Access Footprint

- Mobile
- Secure
- Access anywhere
- Same look and feel
- Ease of use
- Personalised
- Single sign-on
- Multiple, billable sessions

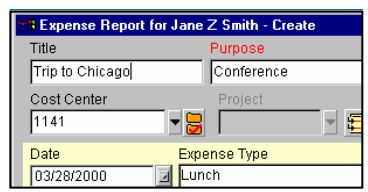
Email

Intranet

Web



Calendar



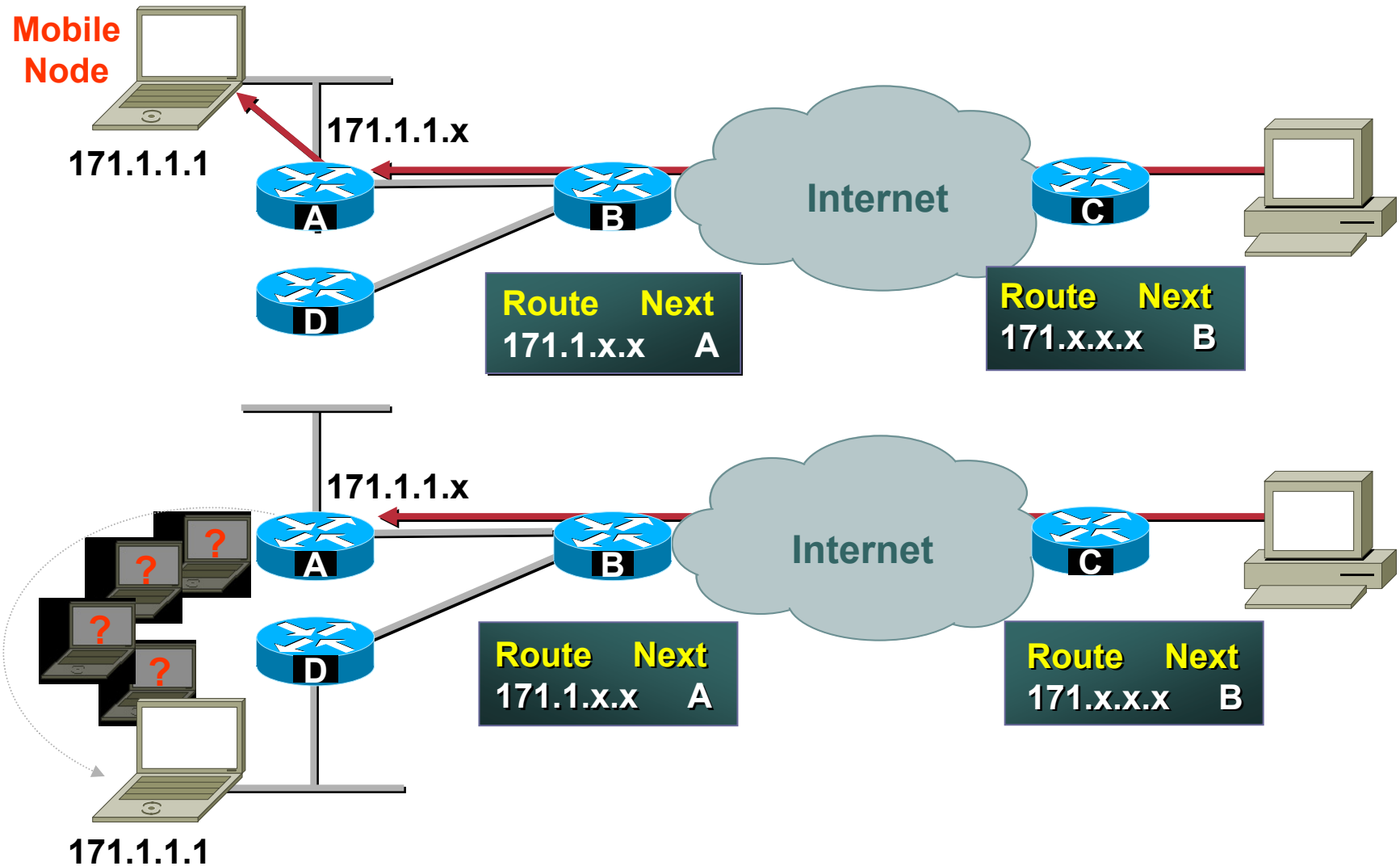
Workforce optimisation

eLearning/ eCommunication

What's the Challenge?

Maintaining *continuous* IP connectivity while crossing network boundaries, e.g. subnets or between networks

Challenge of Mobility in the Internet



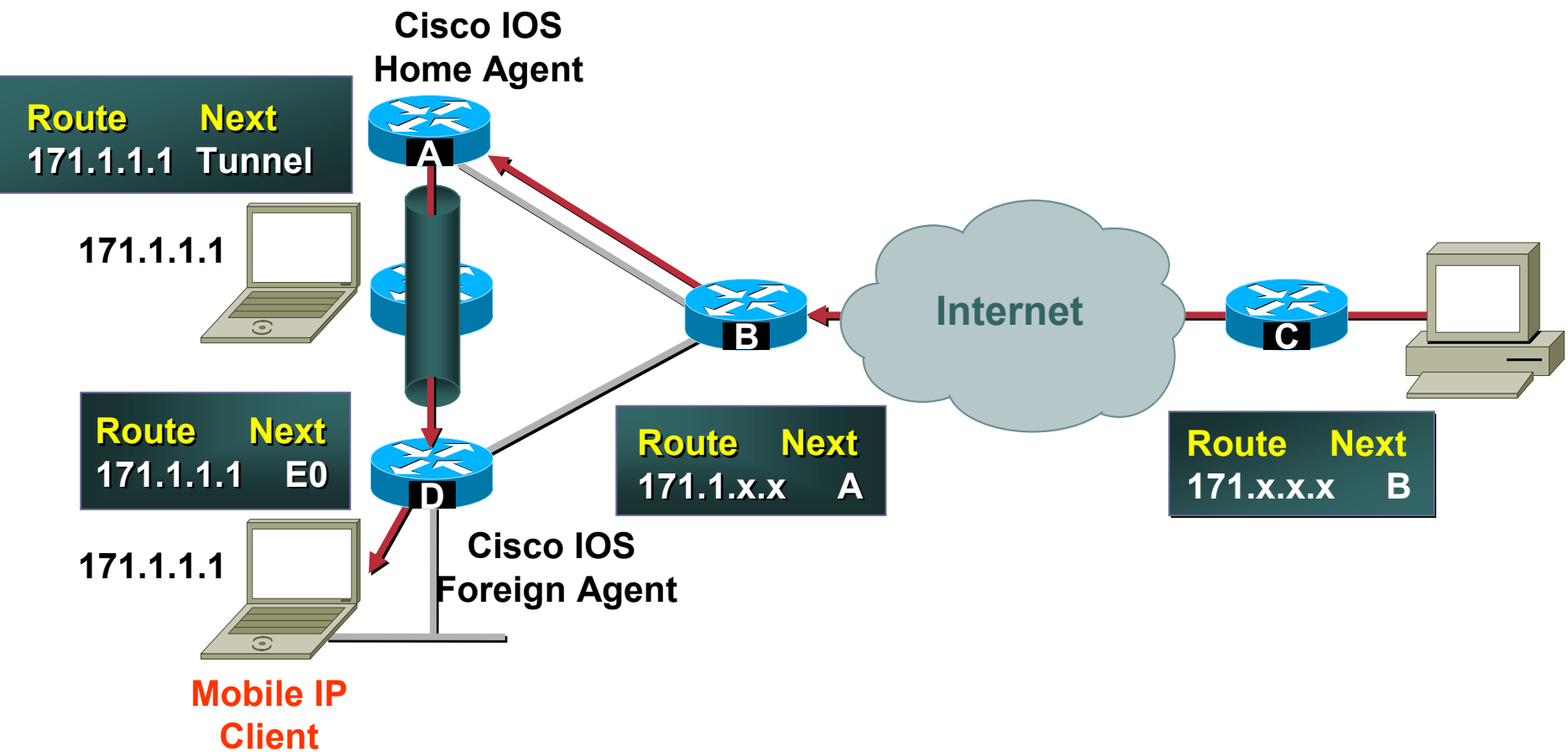
What are the Options?

- Dynamic Host Configuration Protocol (DHCP)
  - Fine for most applications, but won't allow applications to maintain connections across subnet/network boundaries
- Host Routes
  - Enables continuous connectivity but doesn't scale
  - Local Area Mobility (LAM) in Cisco IOS

What are the Options?

- **Wireless IP solutions:**
  - **CDPD, PCS, GPRS, 802.11**
  - **Link-Layer IP mobility:**
    - **Wireless Layer 2 protocols that support IP**
    - **Mobility tied to a single Layer 2 protocol**
  - **IP Addressing is still subject to change if crossing subnet boundaries**

The Solution - Mobile IP



The Solution - Mobile IP

“An IP node’s ability to retain the same IP address and maintain existing communications while traveling from one link to another”

IETF Standard Based Solution

- Approved by the Internet Engineering Steering Group (IESG) in June 1996; published proposed standard in Nov. 1996
- Mobile IP is an IETF proposed standard solution for mobility at Layer 3 IP
  - RFC3344 - Mobile IP
  - RFC2003 and RFC2004 - Tunnel encapsulation
  - RFC2005 - Mobile IP applicability
  - RFC2006 - Mobile IP MIB
- Associated RFCs
  - RFC1701 GRE – Generic Routing Encapsulation
  - RFC3024 - Reverse Tunneling for Mobile IP

Three Components

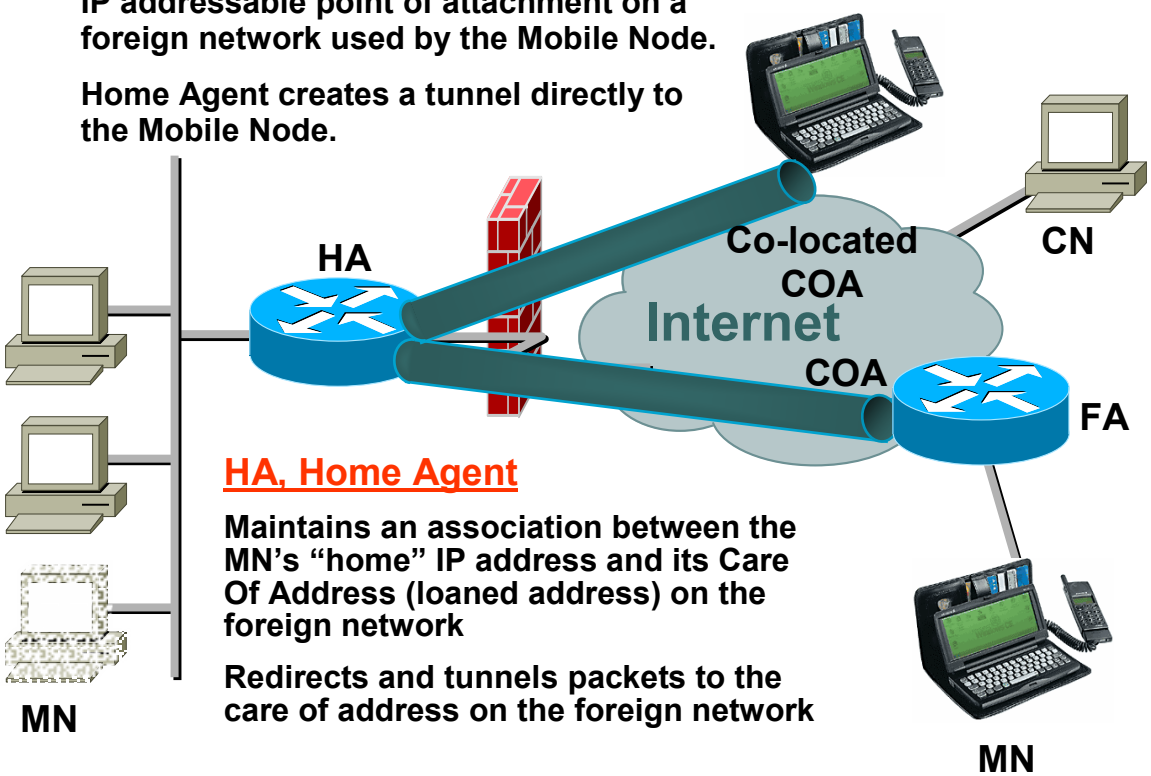
- **Mobile IP is comprised of three components:**
  - **Mobile Node (MN):** IP clients (notebooks, cell phones, PDAs)
  - **Home Agent (HA):** Routers and Layer 3 switches
  - **Foreign Agent (FA):** Routers and Layer 3 switches

How it Works?

Co-located COA

IP addressable point of attachment on a foreign network used by the Mobile Node.

Home Agent creates a tunnel directly to the Mobile Node.



HA, Home Agent

Maintains an association between the MN's "home" IP address and its Care Of Address (loaned address) on the foreign network

Redirects and tunnels packets to the care of address on the foreign network

CN, Correspondent Node

Destination IP host in session with a Mobile Node

FA, Foreign Agent

Provides an addressable point of attachment to the MN called Care Of Address (COA)

Maintains an awareness for all visiting MNs

Acts as a 'relay' between the MN and its Home Agent

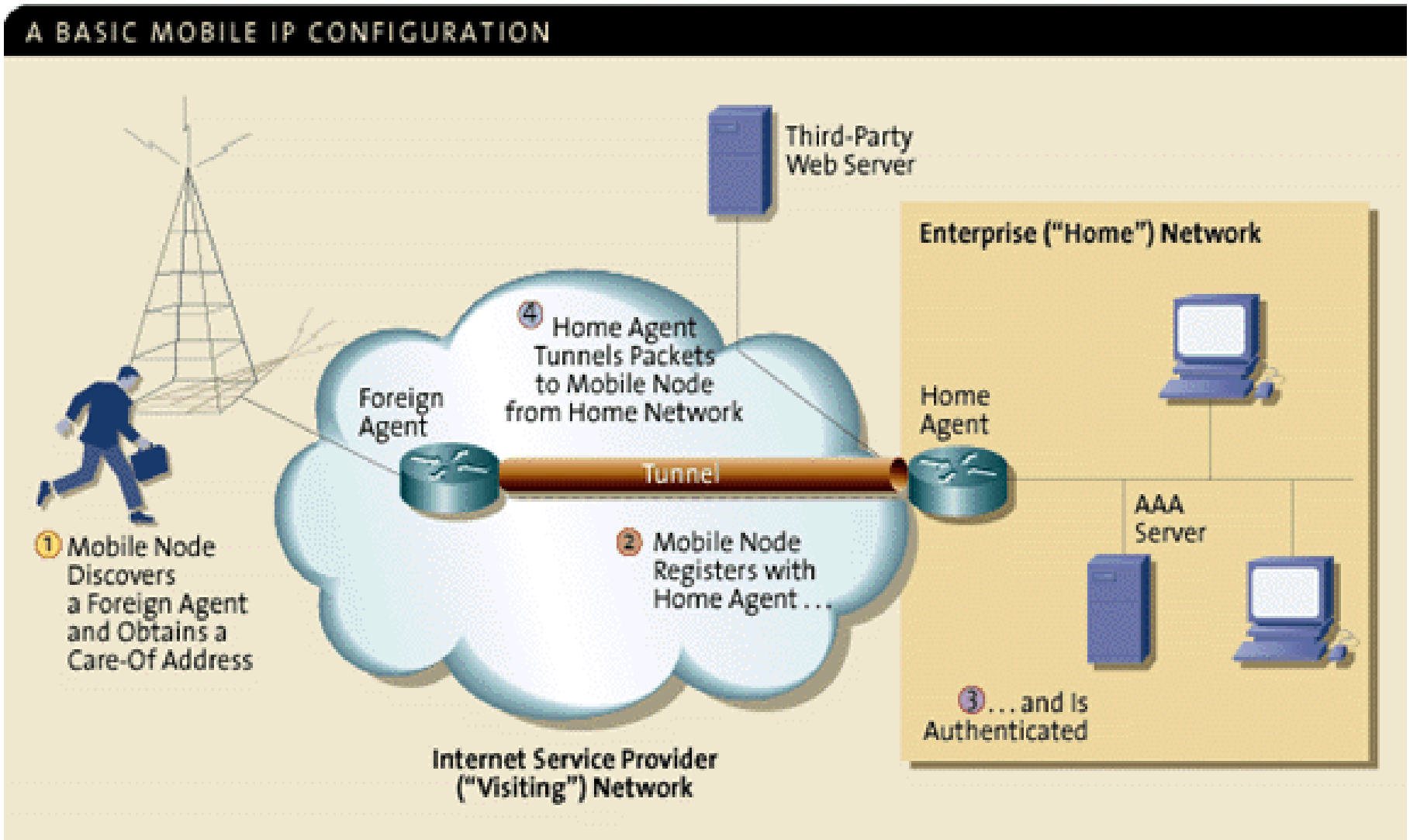
Receives all packets for the MN from the MN's Home Agent

MN, Mobile Node

An IP host that maintains network connectivity using its "home" IP address, regardless of which subnet (or network) it is connected to

Mobile IP Overview

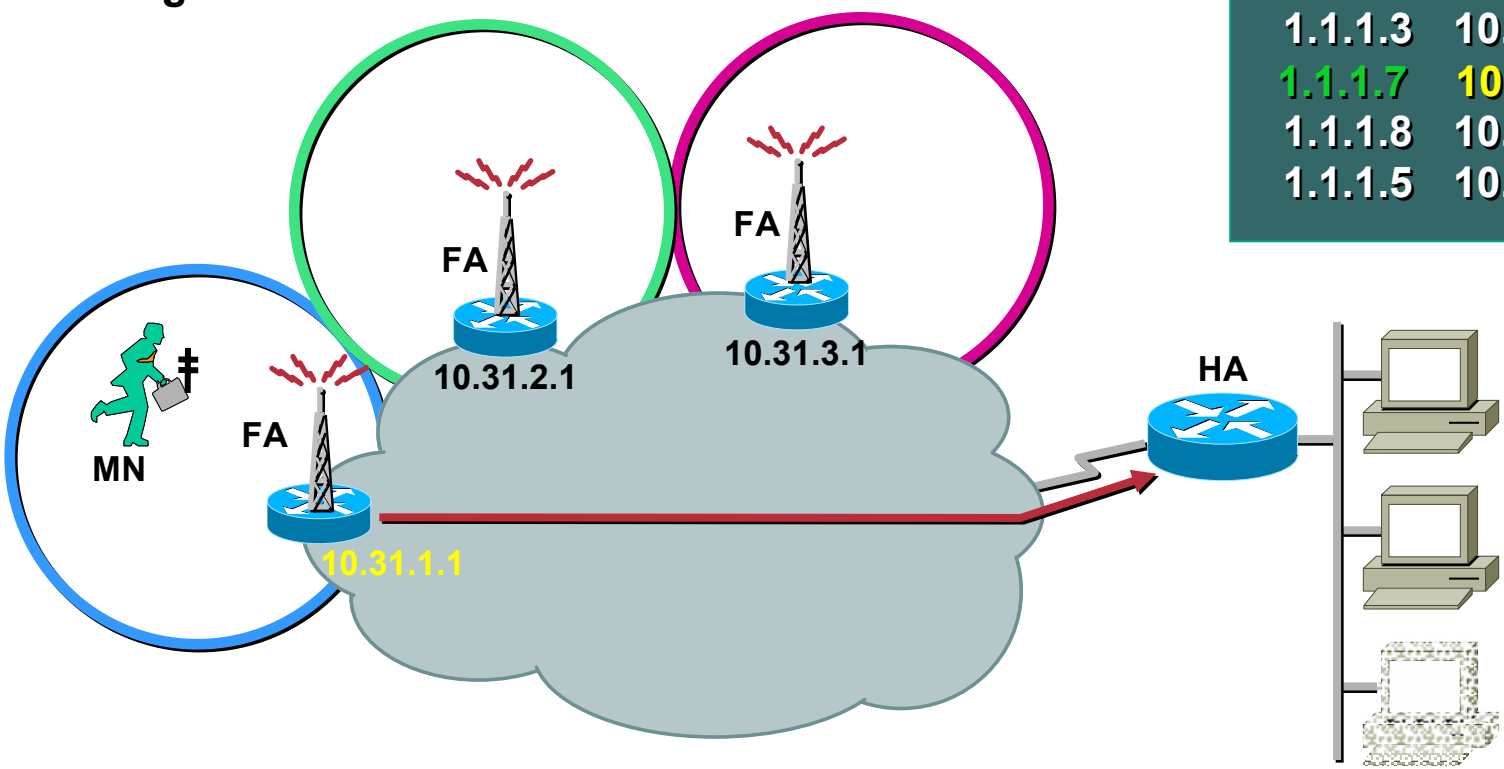
Cisco.com



Roaming with Mobile IP

MN Realizes It Has Moved to a new segment

MN Registers with the “discovered” FA

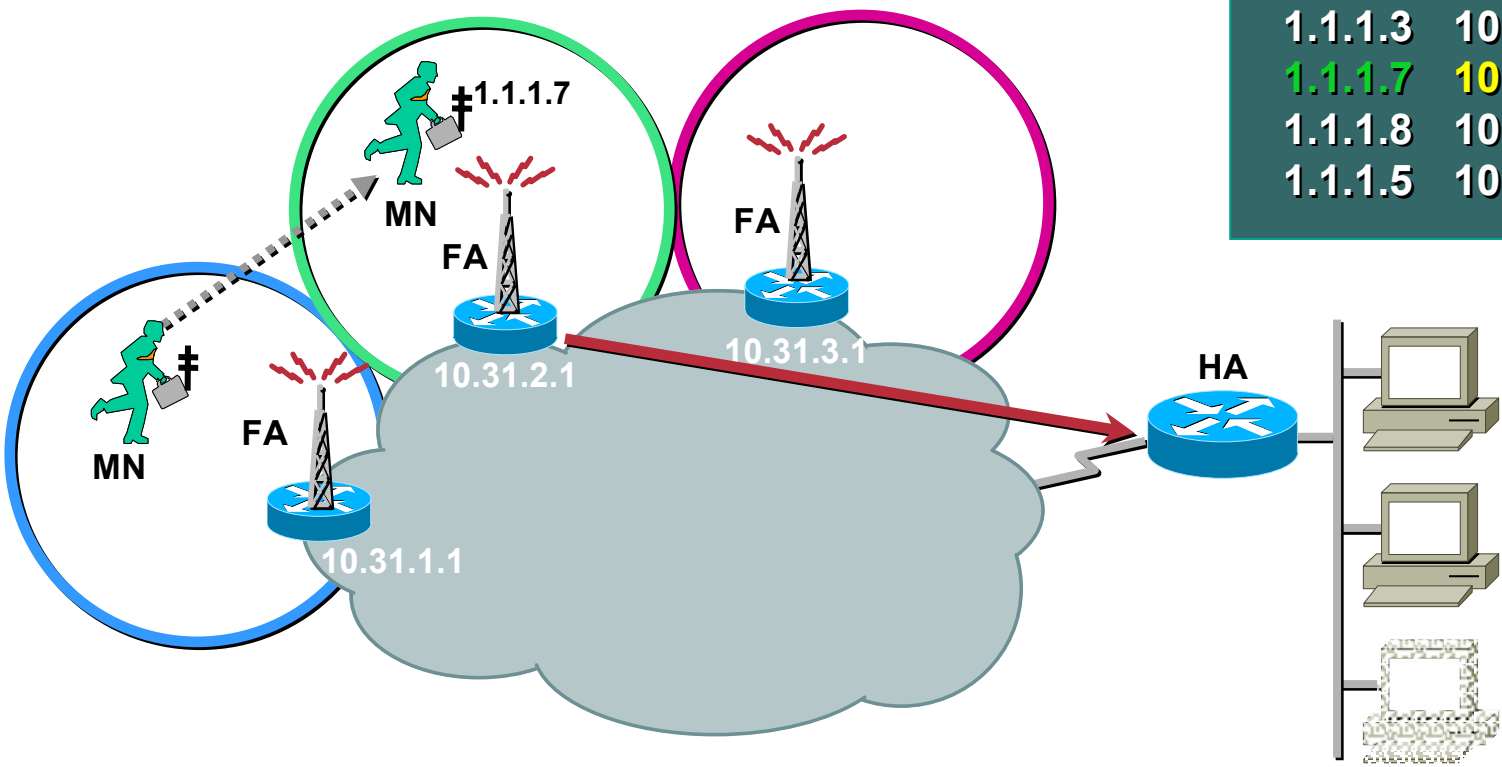


Mobility Binding Table:	
MN	CoA
1.1.1.3	10.31.1.1
1.1.1.7	10.31.1.1
1.1.1.8	10.31.2.1
1.1.1.5	10.31.3.1

Roaming with Mobile IP

MN Realizes It Has Moved to a Network

MN Registers With this New FA

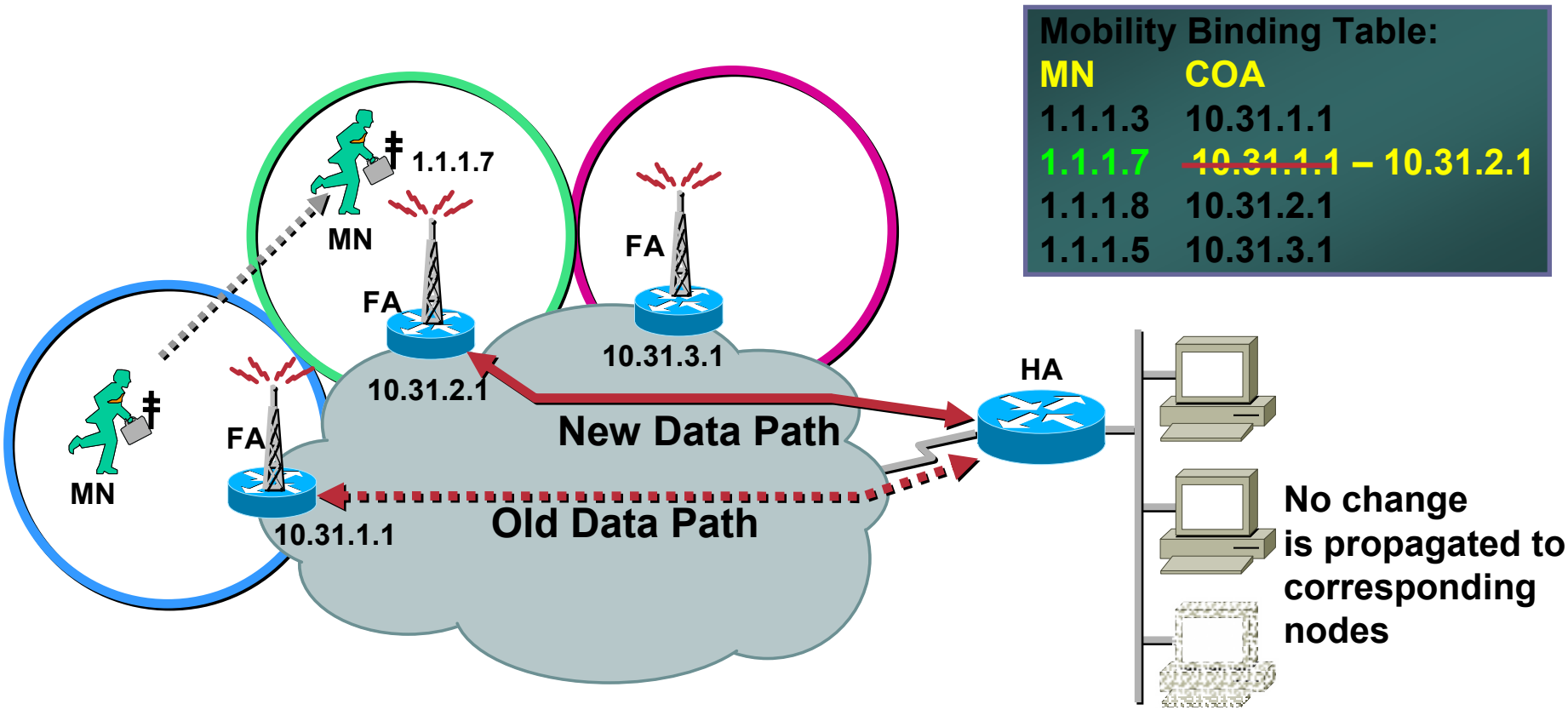


Mobility Binding Table:

MN	CoA
1.1.1.3	10.31.1.1
1.1.1.7	10.31.1.1
1.1.1.8	10.31.2.1
1.1.1.5	10.31.3.1

When the MN Moves It Re-Registers via Its New FA

Roaming with Mobile IP



The Movement is Transparent to all other Devices

The Mobile IP Protocol

- **Media independent protocol:**
  - **Any media that supports IP can support Mobile IP**
  - **Wired (Ethernet), Wireless (Cellular – CDMA, 3G and WLAN 802.11…)**
- **Protocol is part of IRDP (ICMP Router Discovery Protocol)**
- **Is able to detect movement between subnets and transition from 1 to another, transparent to the IP host**
- **Maintains the same IP source address while roaming**

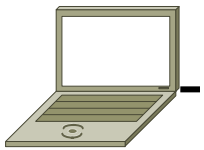
Mobile IP – Connection Models

Cisco.com

Scenario 1 – IPv4

Scenario 2 – IPv4 and IPv6

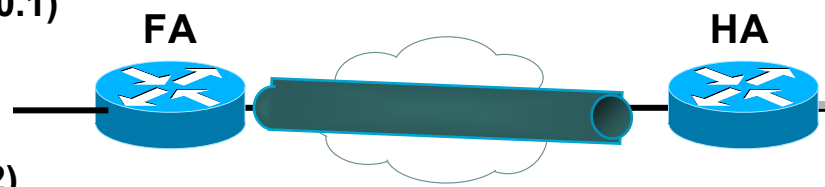
Mobile IPv4 Call Flow - Scenario 1

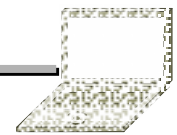


MN
1.1.1.7

Advertisement (224.0.0.1)

FA/HA advertise their presence via IRDP
MN detects movement by network prefix
MN obtains COA from advertisement





1.1.1.7

Solicitation (224.0.0.2)

MN optionally might solicit for an Agent, FA or HA
Solicitation prompts FA or HA to send an advertisement

Registration Request Sequence (UDP port 434)

MN sends unicast registration request to FA (UDP DP=434)
Request includes Type of "MN's Address, HA, COA, authenticator, Tunnel type, Lifetime, Broadcast…"
FA inspects the request, if no objections "relays" the request to the defined HA

Registration Reply Sequence (UDP port 434)

HA
Inspects the request (can it fulfill options requested, performs Authorization check)
If okay, HA adds a Mobility Binding that associates the MN IP Address with the COA
builds a Layer 3 tunnel to the COA (FA or direct to MN), if one doesn't already exist
sends Registration Reply (UDP DP=UDP SP or request) to the COA (FA or direct to MN)

FA
Inspects the reply, if no objections "relays" the reply to the MN
adds MN to list of visitors
acts as default router for MN packets

HA
Sends out a Gratuitous ARP associating MN IP address with the HA's MAC address
responds to ARP requests for MN IP address with its MAC address
Keeps an eye out for packets routed to the MN's IP address and redirects them to the current COA

MN
if authorized MN is set to maintain active or future application traffic
if rejected the MN can inspect the return code and attempt to re-register

De-registration Request (UDP port 434)

MN
Detects it's on home subnet
Sends Registration Request with a lifetime of 0

Mobile IP Clients Types

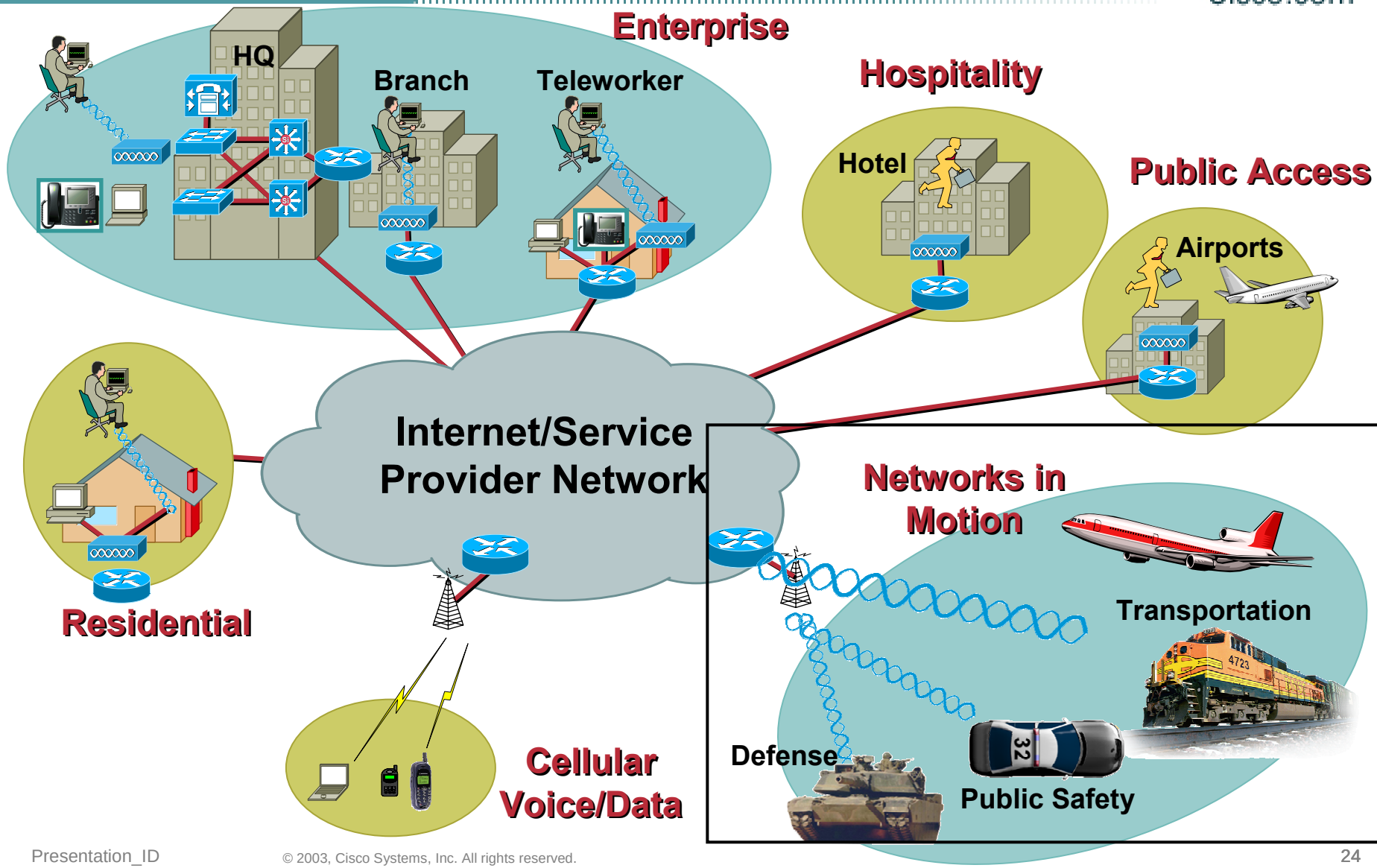
	Host Device	Pros	Cons
Software Client	Laptops, PDAs, etc.	More Features, Better Security, Interop with other services like IPSec	Client Software may need deployment and management support
Embedded Proxy	Handset, Access Point, etc.	Transparent to Attached Clients, Easier to Manage	Supports single media type, Fewer Features, Less Security
Mobile Networks	Router	Mobile LANs, Clients need not be Mobile, Central Management	Large scale deployment could require provisioning support

Application Transparency across Networks

- **Browsing, FTP, email**
  - All IP applications work as is
- **One time Logon**
  - No need to re-login to the network or application directories as the individual roams across networks
  - User is always at same IP Address & DNS Name
- **Secure Mobile VPNs**
  - IPSec VPNs over Mobile IP, Authentication built-in to Mobile IP RFC 3344
- **IM, Unified Messaging**
  - Ability to “Push” to the mobile user any time anywhere
- **VoIP, VoD, Video Conferencing**
  - Mobile IP enables continuous connectivity

Target Markets

Major Markets for Mobility

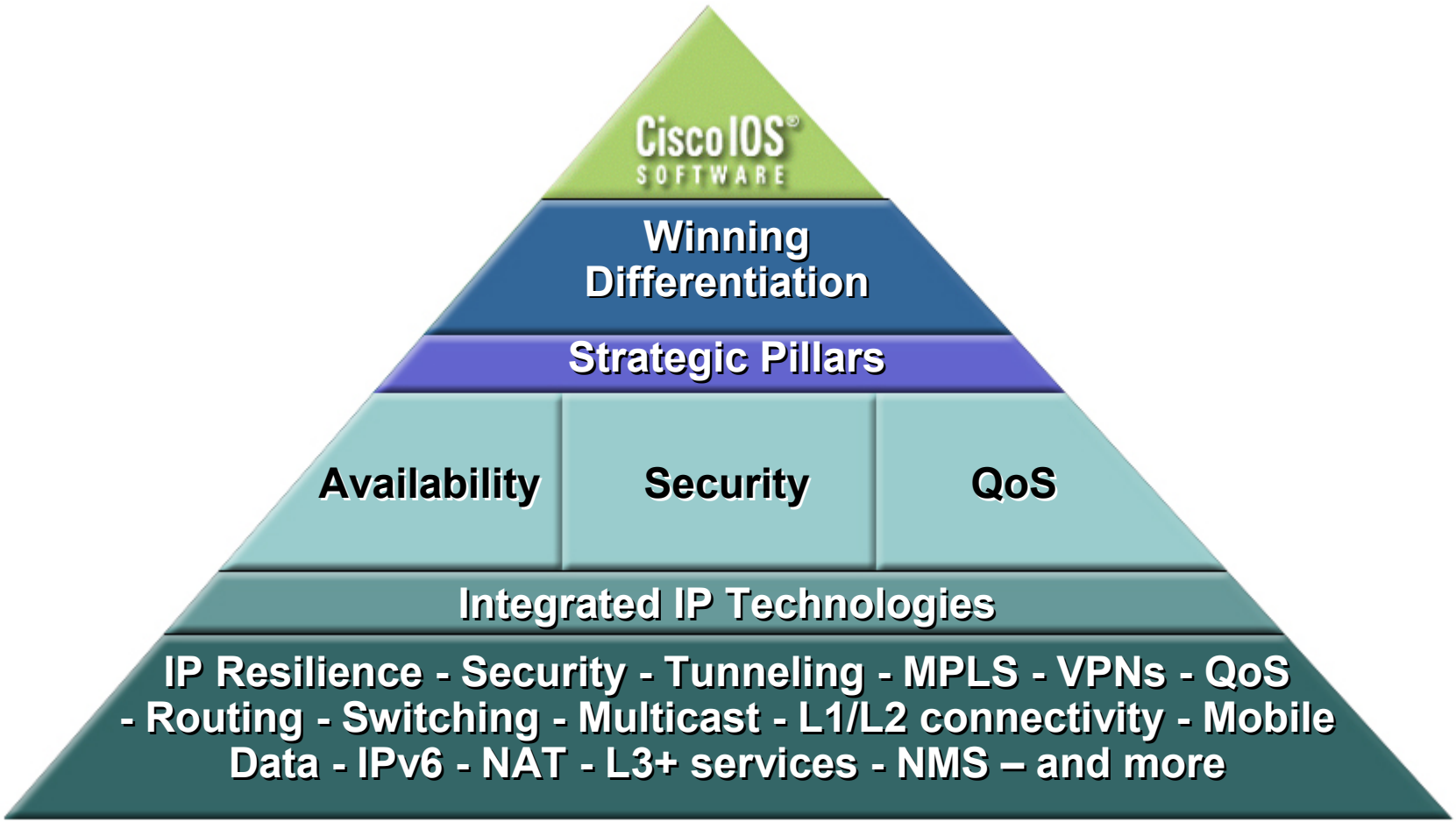


Areas of Focus within each Market

- **Enterprise**
  - **Campus Mobility - Ethernet to WLAN or just WLAN**
  - **Public access back to corporate**
- **Commercial**
  - **Public Safety – Police, Fire, Ambulance, City and Community Networks**
  - **Transportation – Railroads, Airlines**
- **Military & Federal Government**
  - **Navy – JTRS, Army – 82nd Airborne, WIN-T, others**
  - **NASA, Coastguard (similar requirements as Military)**
  - **Boeing, GD, Mitre, LM – Ad hoc, Mobile Networks**
- **Service Provider**
  - **Wireless WAN, Public WLAN hotspots**
  - **Roaming between networks, 4G**

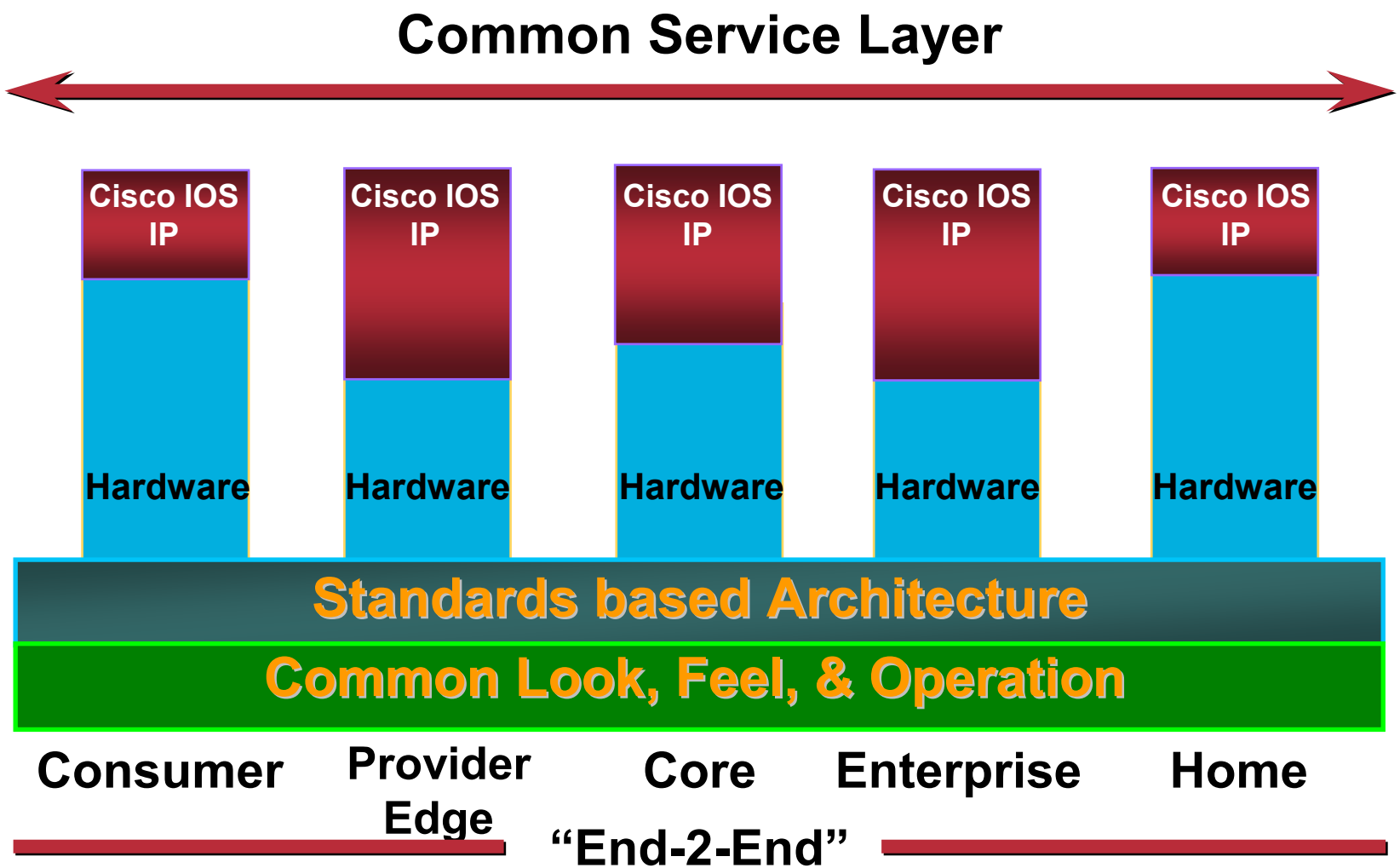
Cisco IOS and Mobile IP

Cisco IOS® Software: Integrated IP Infrastructure



Integrated IP Infrastructure

The role of Cisco IOS
IP Software for End to End Services



Mobile IP @ Cisco

3rd Party
Mobile IP Client

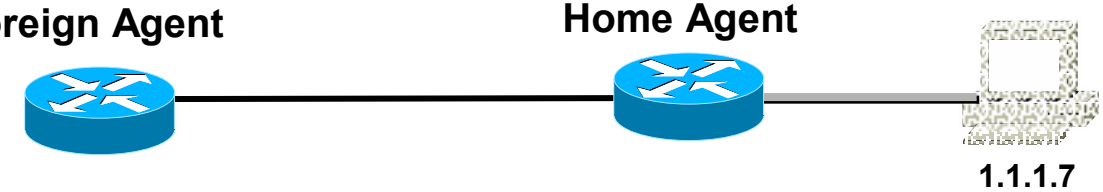
1.1.1.7

- Clients today for
  - Windows 95/98
  - Windows NT
  - Linux
- Motorola has an embedded Mobile IP client

- Microsoft is developing a IPv6 client

Cisco IOS
Foreign Agent

Cisco IOS
Home Agent



1.1.1.7

- Cisco Delivers the Foreign and Home Agents
- Software is available across a range of platforms 1700, 2500 through 7500, Cat5K RSM, Cat6K MSFC
- In Production since 1999 and Cisco IOS 12.0(1)T

Mobile IP @ Cisco

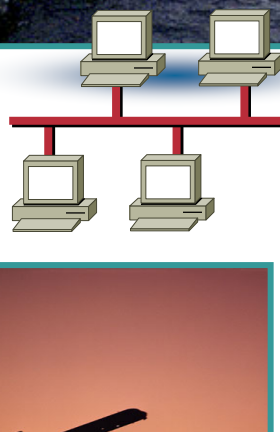
- **Mobile IPv4: In Production since 1998 [12.0(1)T]**
  - **Home Agent and Foreign Agent**
  - **Home Agent Redundancy – 12.0(2)T**
  - **Mobile Networks – Subnet mobility – 12.2(4)T**
  - **Proxy Mobile Node (PDSN & WLAN)**
- **1700, 2600, 2700, 3700, 7200, c6500, MWAN, Mobile Access Router 3200, Cisco Access Points**
- **Plus Feature set option (names with 's-', e.g., c7200-is-mz**

Mobile IP @ Cisco

- **IPv6**
  - **General IPv6 software now in production from Cisco**
  - **Mobile IPv6 is part of the planned IPv6 rollouts**
    http://www.cisco.com/warp/public/732/Tech/ipv6/ipv6_learnabout.shtml
    http://www.cisco.com/warp/public/732/Tech/ipv6/
- **Mobile IPv6**
  - **Home Agent & Correspondent Node – Field Trial CY01**
    - **Draft 18 compliant today**
    - **Draft 20 planned for March 2003 Connectathon**
  - **Mobile Networks – In development - Field trial Q3 CY03**

Cisco IOS Mobile Networks
"Networks in Motion"

- IP devices don't have to be Mobile IP aware
- Cisco IOS device incorporates a Mobile Client



Mobile Networks - Connection Models

Scenario 1

No 3rd Party Mobile IP Client required

Scenario 2

No 3rd Party Mobile IP Client required

Mobile IP @ Cisco

- **Authored 8 IETF drafts, contributed to over 10+ other drafts and working on more**
- **IETF RFC support**
  - **IETF RFC 3344 Mobile IP**
  - **IETF RFC 2003 IPinIP Encapsulation**
  - **IETF RFC 2006 Mobile IP MIBs**
  - **IETF RFC 2794 NAI**
  - **IETF RFC 2344 Reverse Tunnel**
  - **IETF RFC 3115 Vendor Specific Extensions**

Mobile IP @ Cisco - Cisco Value Add

- **New market requirements since the standard:**
  - **Redundancy, 7x24 availability √**
    - **1x1+ Home Agent Redundancy, leveraging HSRP Informational RFC 2281 for transparent fail-over**
  - **Integration with Authorization systems √**
    - **Ability to store user information, Security Associations, profiles centrally with AAA (Authentication, Authorization & Accounting), easing network provisioning**
  - **User & Service Authorization & Selection Overlay √**
    - **Service Selection Gateway (SSG)**
    - **Billing and Provisioning systems**

Mobile IP @ Cisco - Cisco Value Add

- **New market requirements since the standard, cont'd:**
  - **Dynamic addressing vs. static configurations √**
    - **Applying Network Address Translation to Mobile traffic, and detection of NAT in the path**
    - **Use of DHCP & Dynamic DNS - in progress**
  - **VPN support & Secured Tunnels √**
    - **Mobile IPsec VPNs over Mobile IP**
    - **IPsec between Mobile Agent, and Securing Control/Data Planes between Agent**
- **Additional Cisco IOS Value Add**
  - **Flexability: Cisco IOS is available across a wide range of platforms**
  - **Multicast - Support of Multicast traffic with the Mobile Networks "Mobile Router" implementation**

Mobile IP @ Cisco
Working Relationships with…

- **Mobile IPv4:**

  Intel

  Birdstep www.birdstep.com

- **Mobile IPv6:**

  Microsoft, Lancaster Univ. & Orange UK

  Founding member of Mobile IPv6 LAB at Lancaster Univ.

  http://www.mobileipv6.net/

Mobile IP Clients

- **Birdstep (GPRS, CDMA, 802.11b) www.birdstep.com**

  W95, W2k, NT, [PocketPC, XP – Soon]

  http://www.cisco.com/warp/public/732/Tech/mobile/ip/clients/

- **SecGo/Lifix Go! Mobile Node**

  Windows 2000, Linux, … http://www.lifix.fi

- **Microsoft Research Mobile IPv6 Client**

- **Cisco IOS embedded client**

  Cisco IOS Mobile Router, as of IOS 12.2.(4)T CY01

  WLAN Proxy Mobile Node (delivered in the Access Point)

  PDSN Proxy Mobile Node (delivered in the PDSN)

Key Areas of Focus

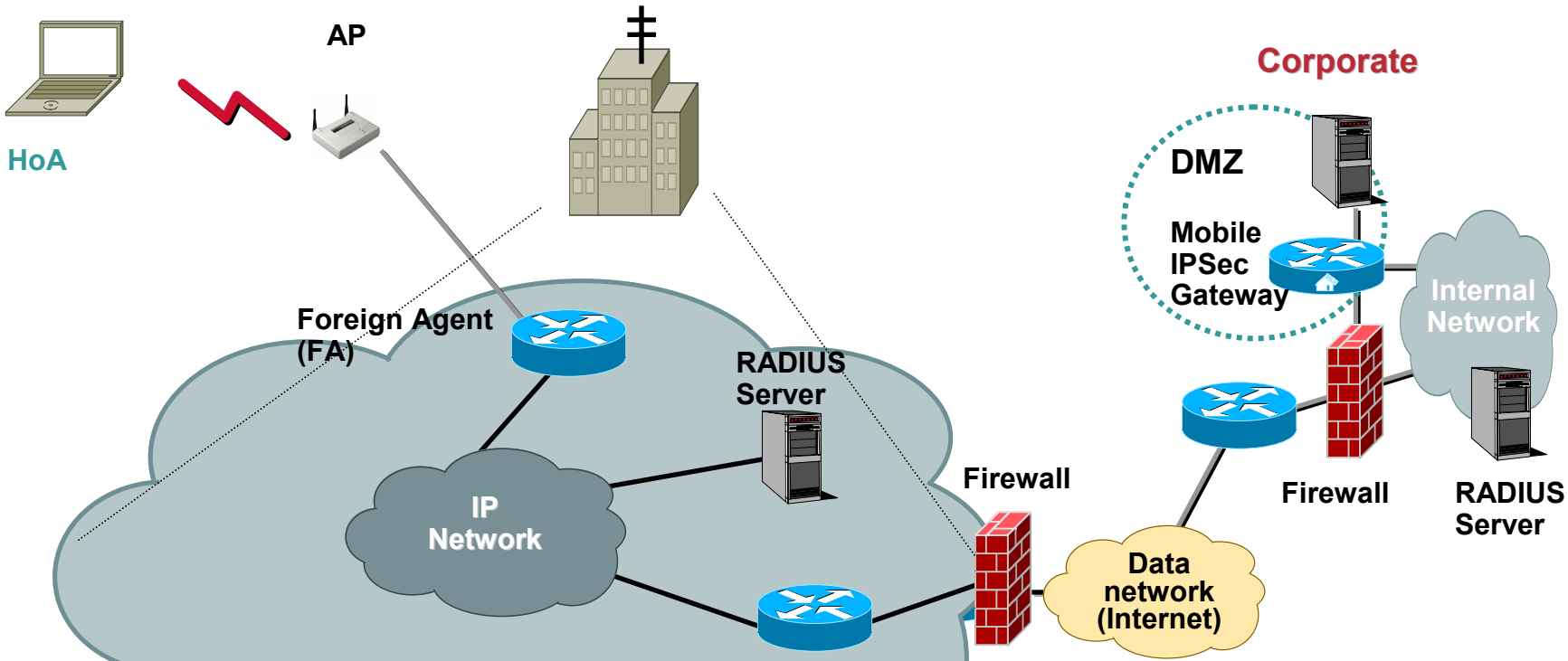
- Engage with Mobile IP clients
- Dynamic Addressing and Discovery
- Security

  User Authentication, Mobile IPsec VPNs, Traversing security nodes 'Firewall, NAT'
- High Availability - Stateful Redundancy
- Advanced Protocols 'VoIP, Video, Multicast'
- User Identification, Policy & Services

  Identification of the user, Location awareness, billing resolution, Destination based & Application level "path" decisions
- Geographic mobility challenges, "Adhoc", Private Addressing, Multiple paths to home, …

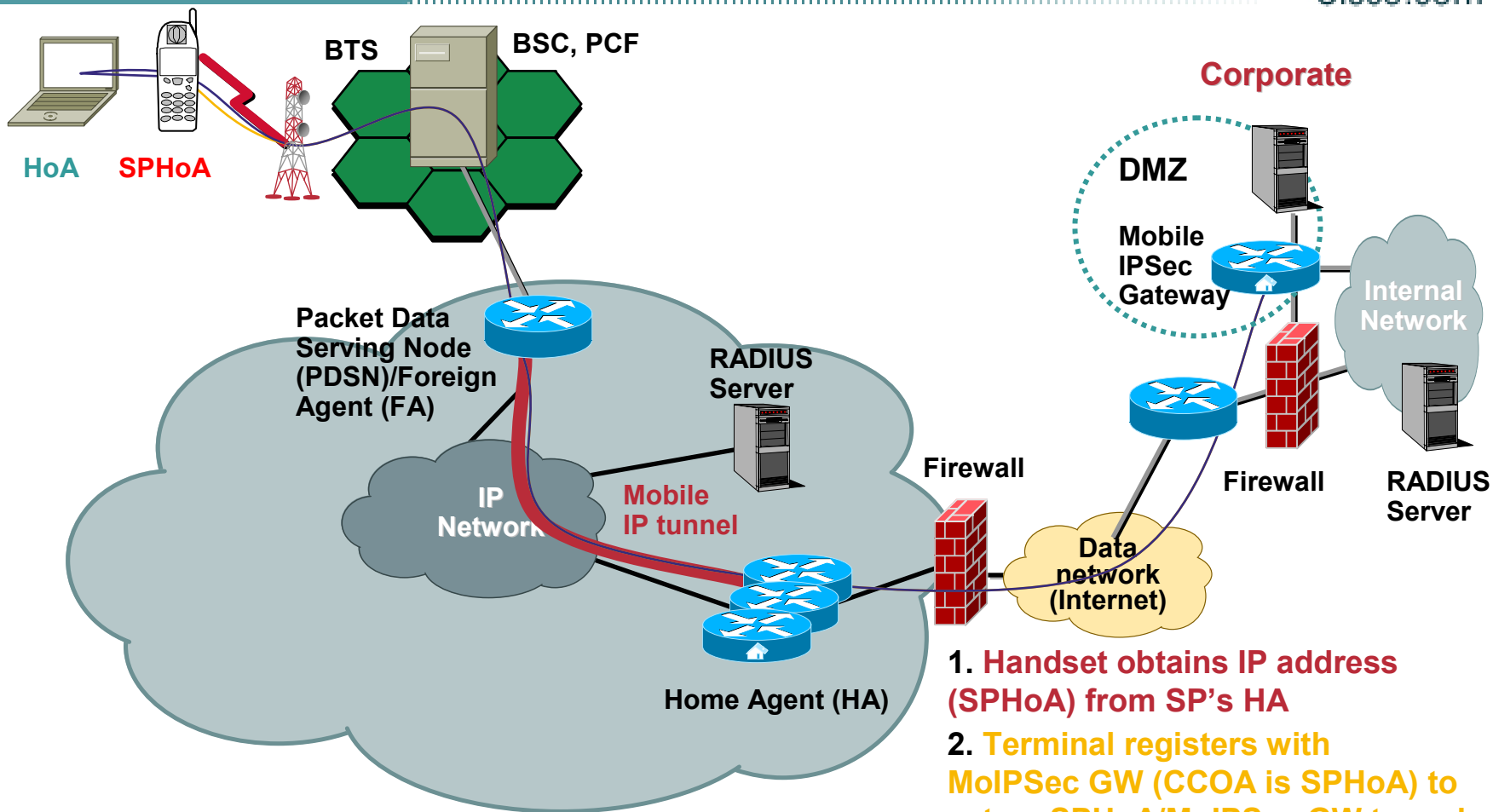
Deployment Scenarios

WLAN Access



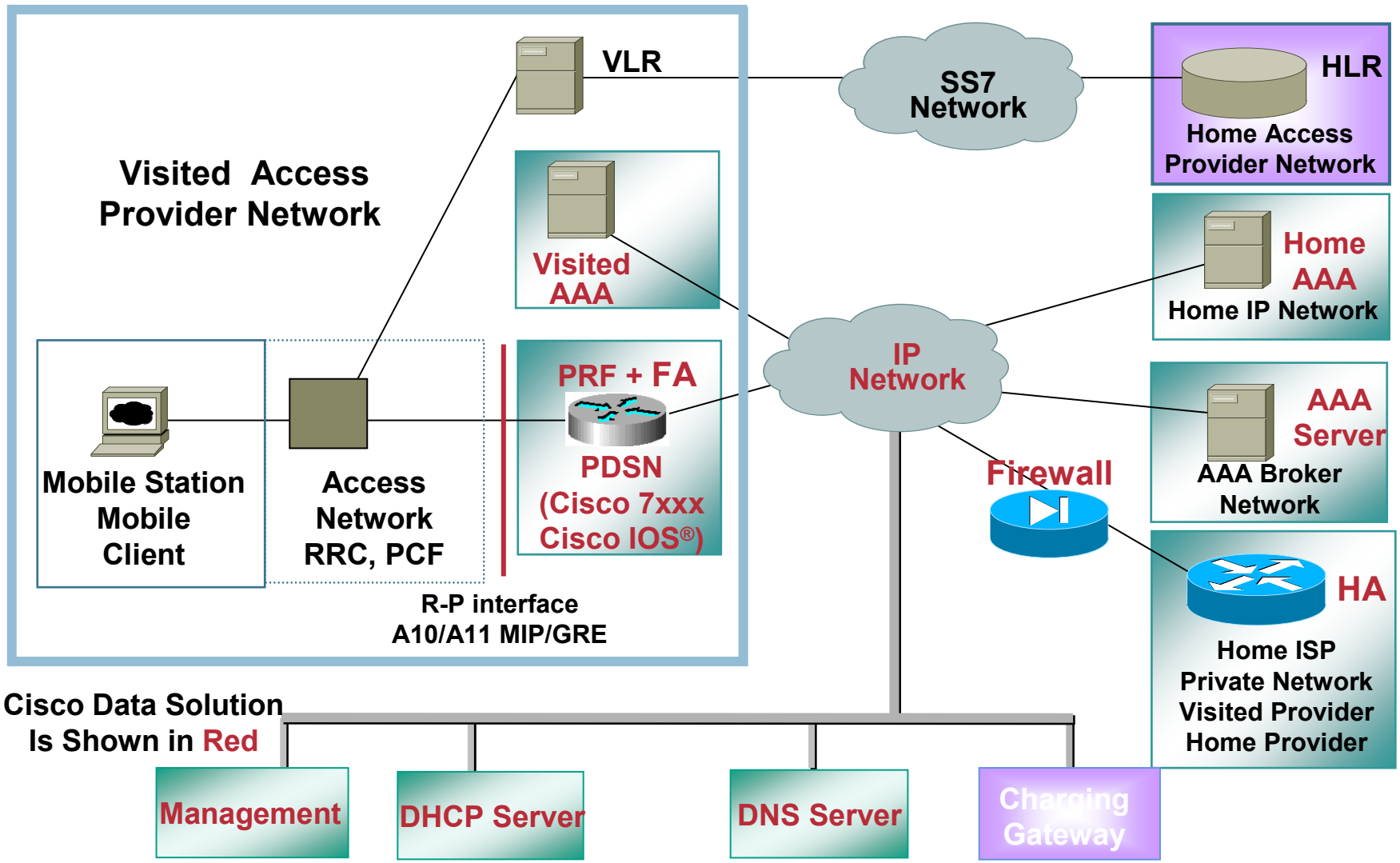
1. Terminal discovers FA after AP authorization
2. Terminal registers with MoIPSec GW (COA is FACOA)
3. FA sets up FACOA/MoIPSec GW tunnel
4. IPSec traffic between HoA and MoIPSec GW starts/continues within FACOA/MoIPSec GW tunnel

CDMA 2000 Access

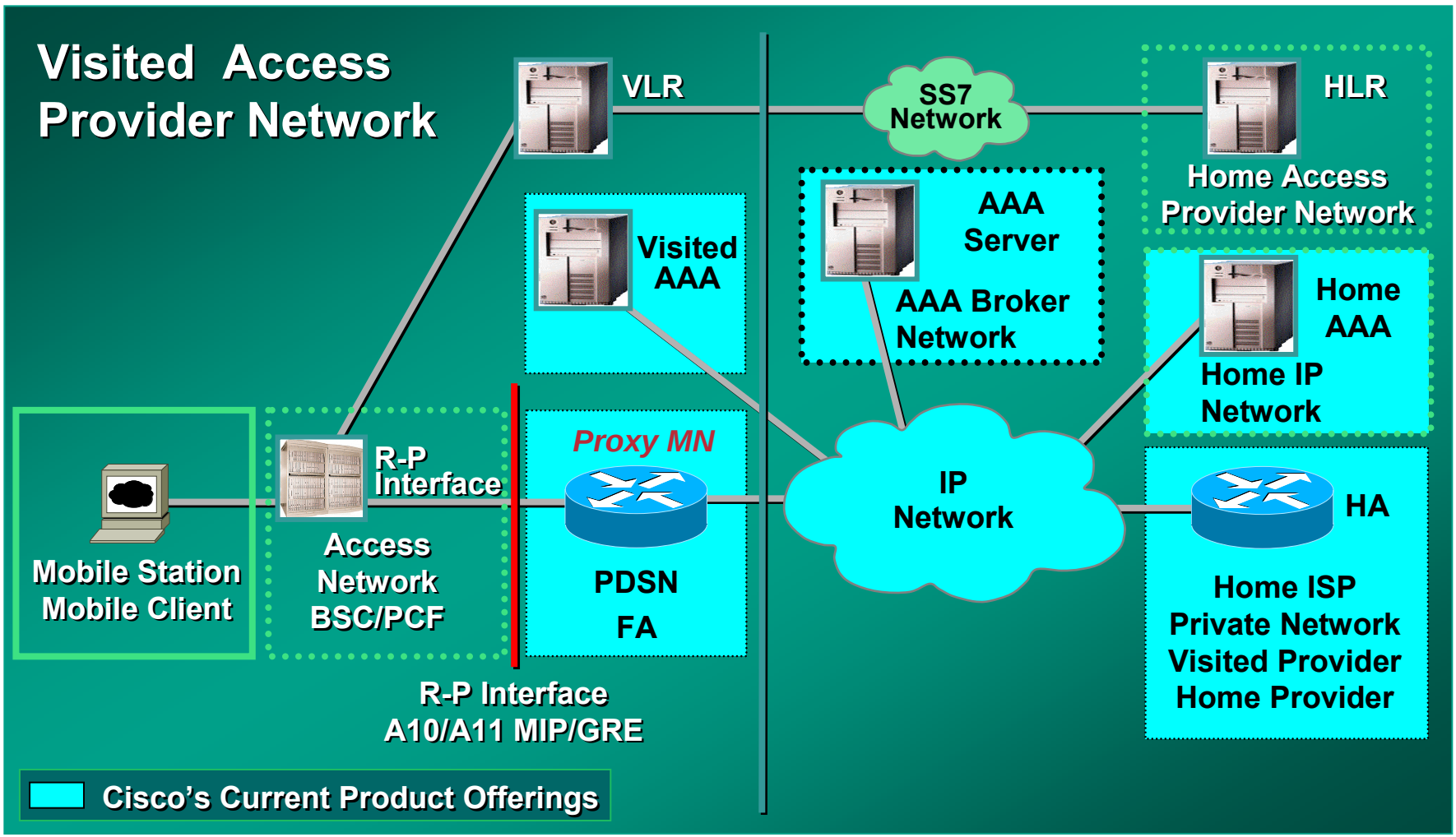


1. Handset obtains IP address (SPHoA) from SP's HA
2. Terminal registers with MoIPSec GW (CCOA is SPHoA) to set up SPHoA/MoIPSec GW tunnel
3. IPSec traffic between HoA and MoIPSec GW starts/continues within SPHoA/MoIPSec GW tunnel

Cisco Packet Data Serving Node v1.2

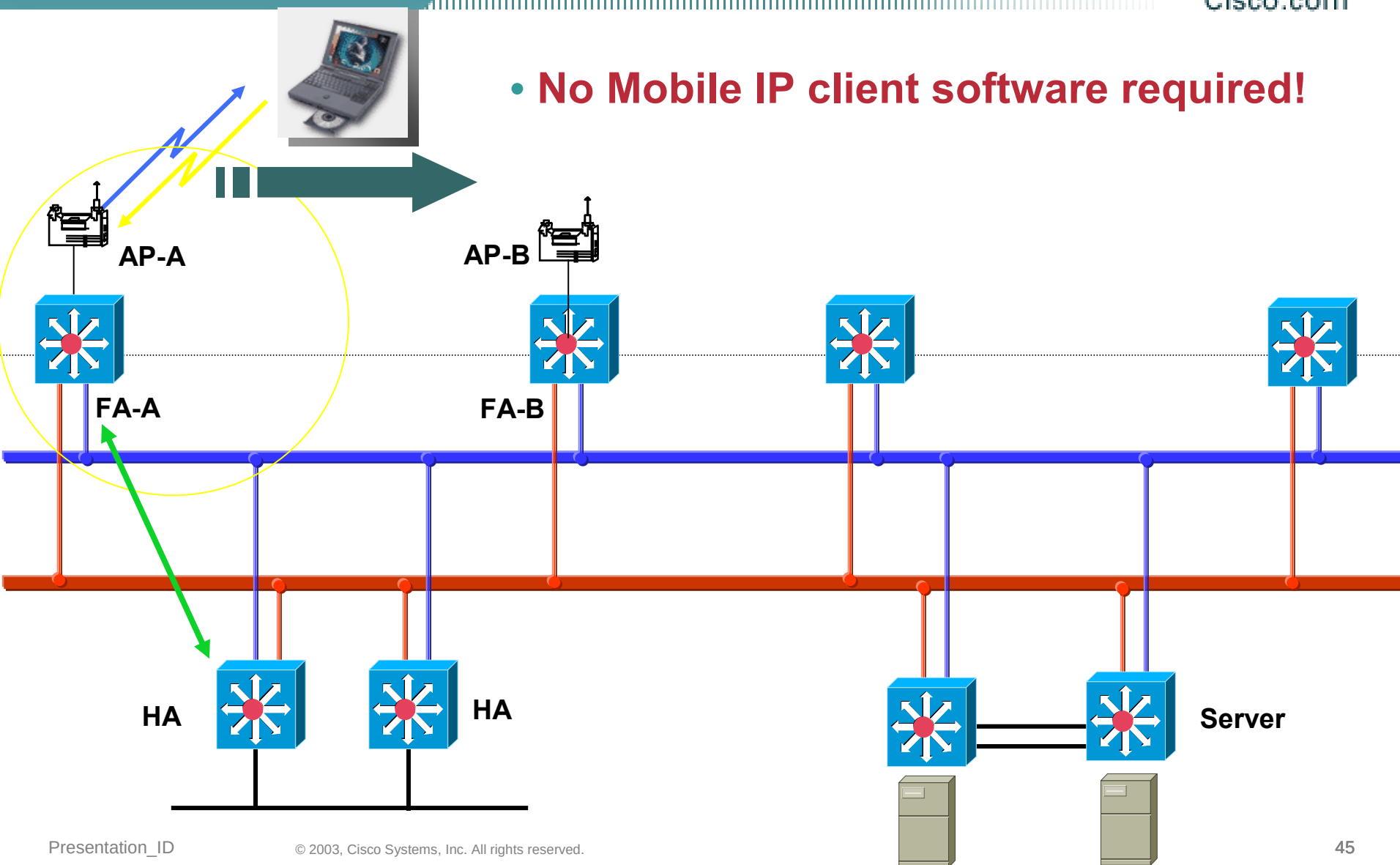


PDSN Proxy Mobile Node



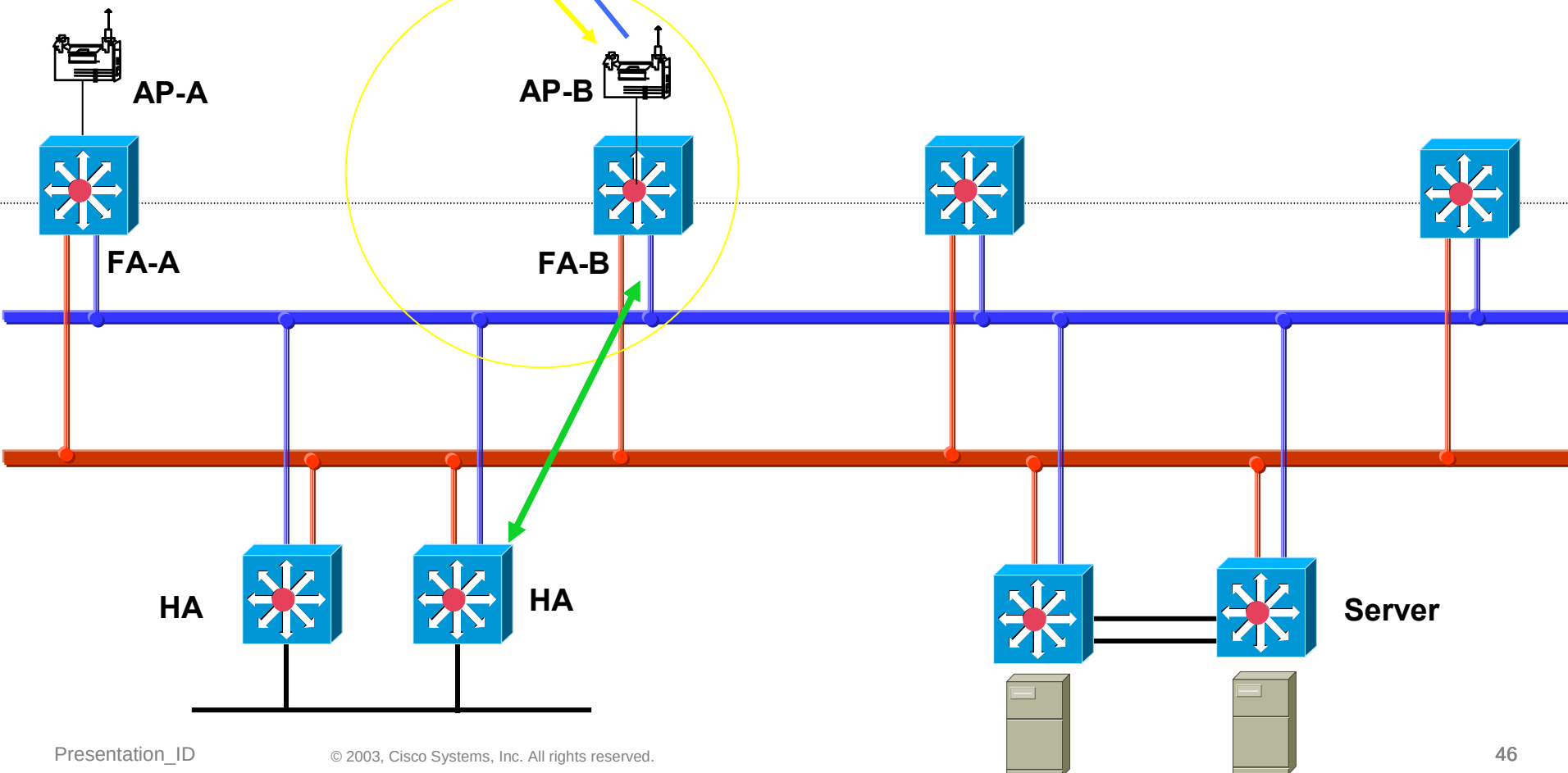
Proxy Mobile Node and Wireless LAN

- No Mobile IP client software required!



Proxy Mobile Node and Wireless LAN

- No Mobile IP client software required!

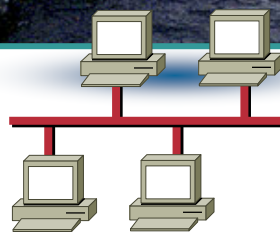


Proxy Mobile Node and Wireless LAN

- Mobile IP Client integrated with the WLAN Access Point, acts as a Proxy for IP hosts
- Proxy Mobile Node (MN), enables mobility without requiring a mobile IP stack on the client device
  - Proxy integrated with the FA, registers on behalf of the mobile
  - Wireless devices are integrated with the Proxy MN service
- Allows for traditional subnet design

Cisco IOS Mobile Networks
"Networks in Motion"

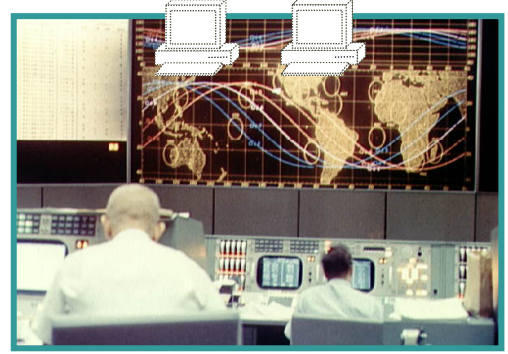
- IP devices don't have to be Mobile IP aware
- Cisco IOS device incorporates a Mobile Client



FA

Mobile Network
(client software)
with
Foreign Agent

HA



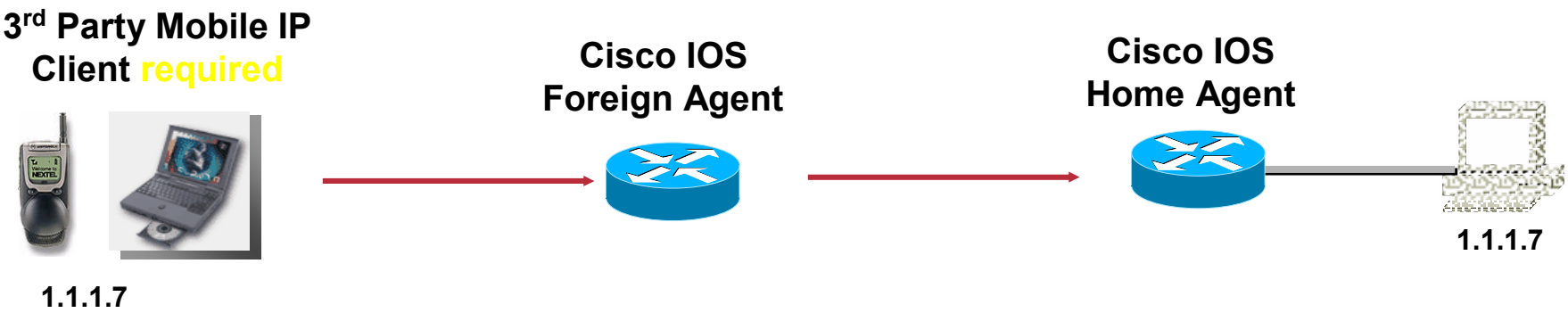
Cisco IOS Mobile Networks
What is It?

- Enables “always on roaming” IP connectivity for entire LAN segments
- Subnets are mobile without devices on those subnets being aware
- Mobile Router (MR) is in effect a Mobile IP Client
- Standards based solution RFC 2002 Mobile IP
- Both non-mobile IP clients as well as mobile IP-aware clients are supported
- MR can detect Foreign Agent’s (FA) or connect in a co-located COA design directly to the HA

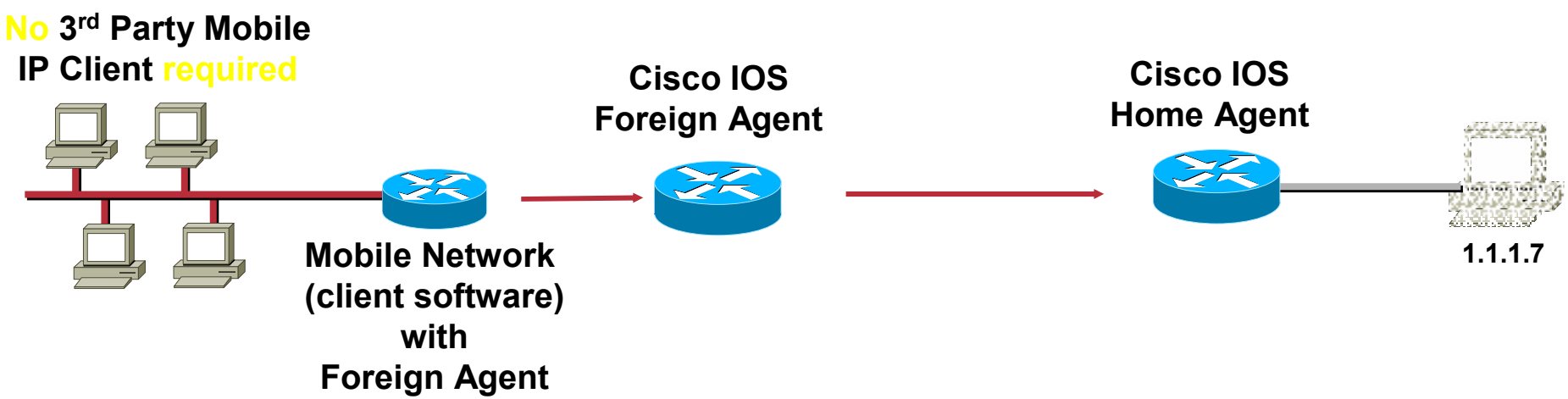
Mobile Networks - Connection Models

Cisco.com

Typical Mobile IP Connection Model

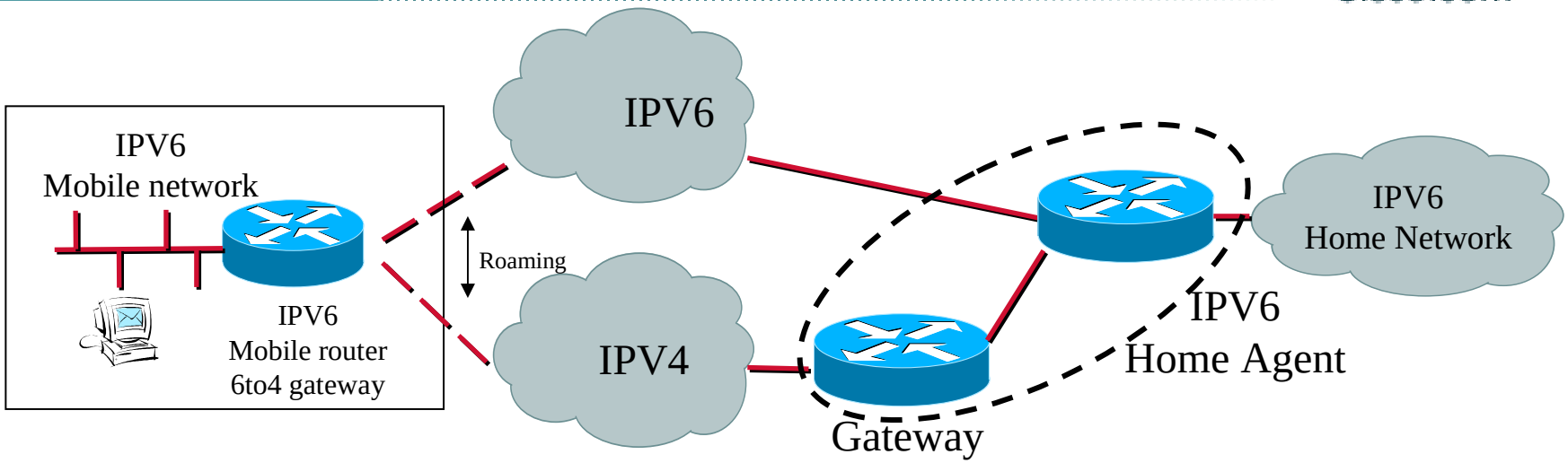


Mobile Networks Connection Model

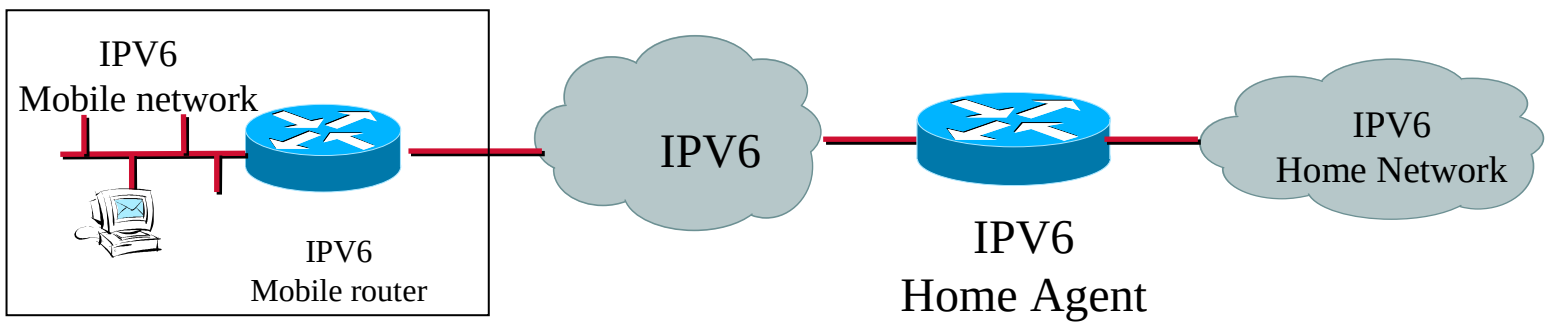


Mobile Networks Tunneling Packet Flow

Mobile Networks: Roaming Scheme



Mobile IPV6 router roaming into a V4 or V6 network



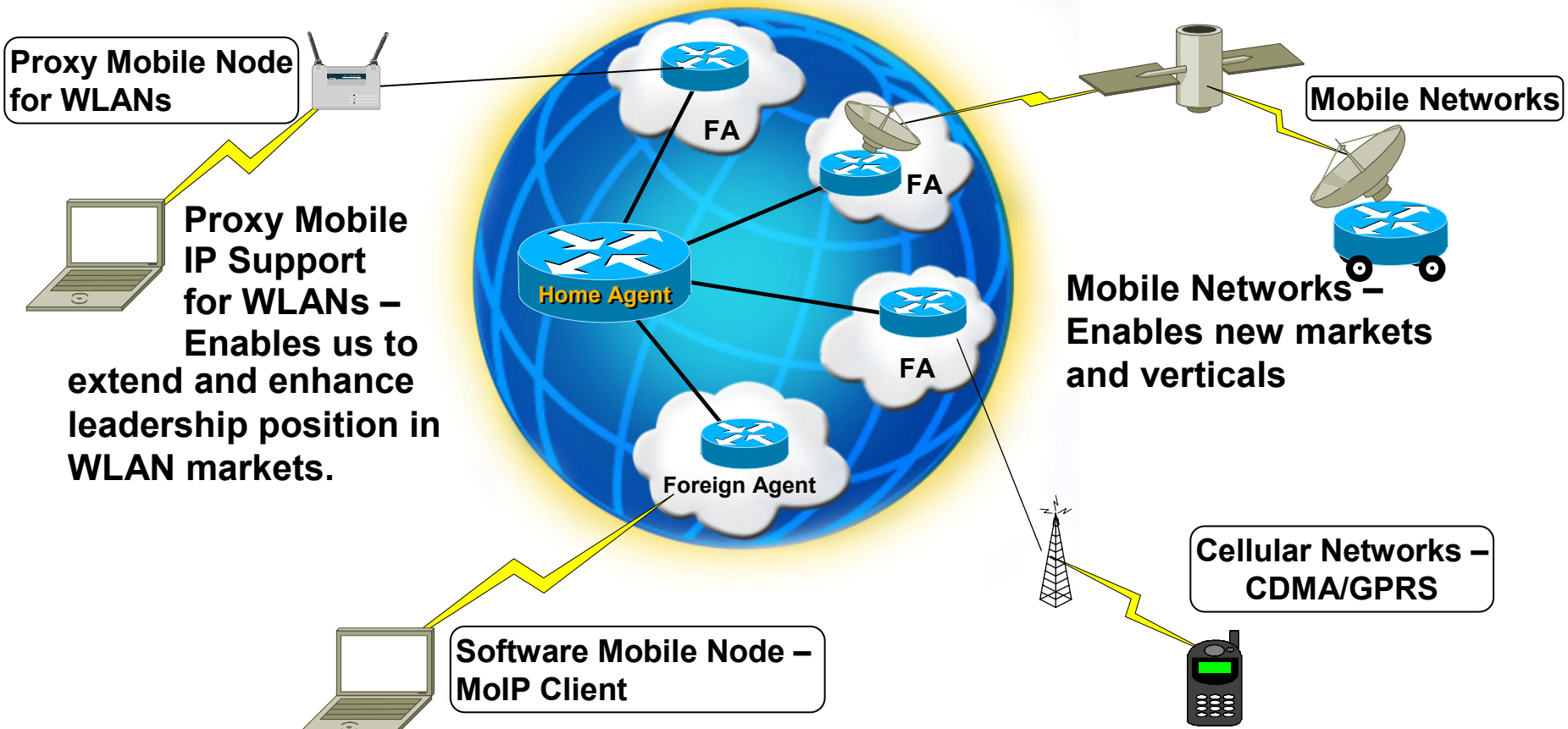
Ideal topology

Summary

Mobile IP – End 2 End Service Architecture

IP Service Integration – Integrate Mobile IP with IPSec VPNs, Multicast, QoS etc. Pushing the edge of the network out to the Mobile environment while reinforcing our IP leadership

Standards based solution. Best in class



Reference Material

- **Cisco Mobile IP Web Page**

  www.cisco.com/go/mobile_ip

- **Cisco Networkers Mobile IP Sessions**

  www.cisco.com/networkers/nw00/pres/2307.pdf

- **IETF Working Group URL**

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

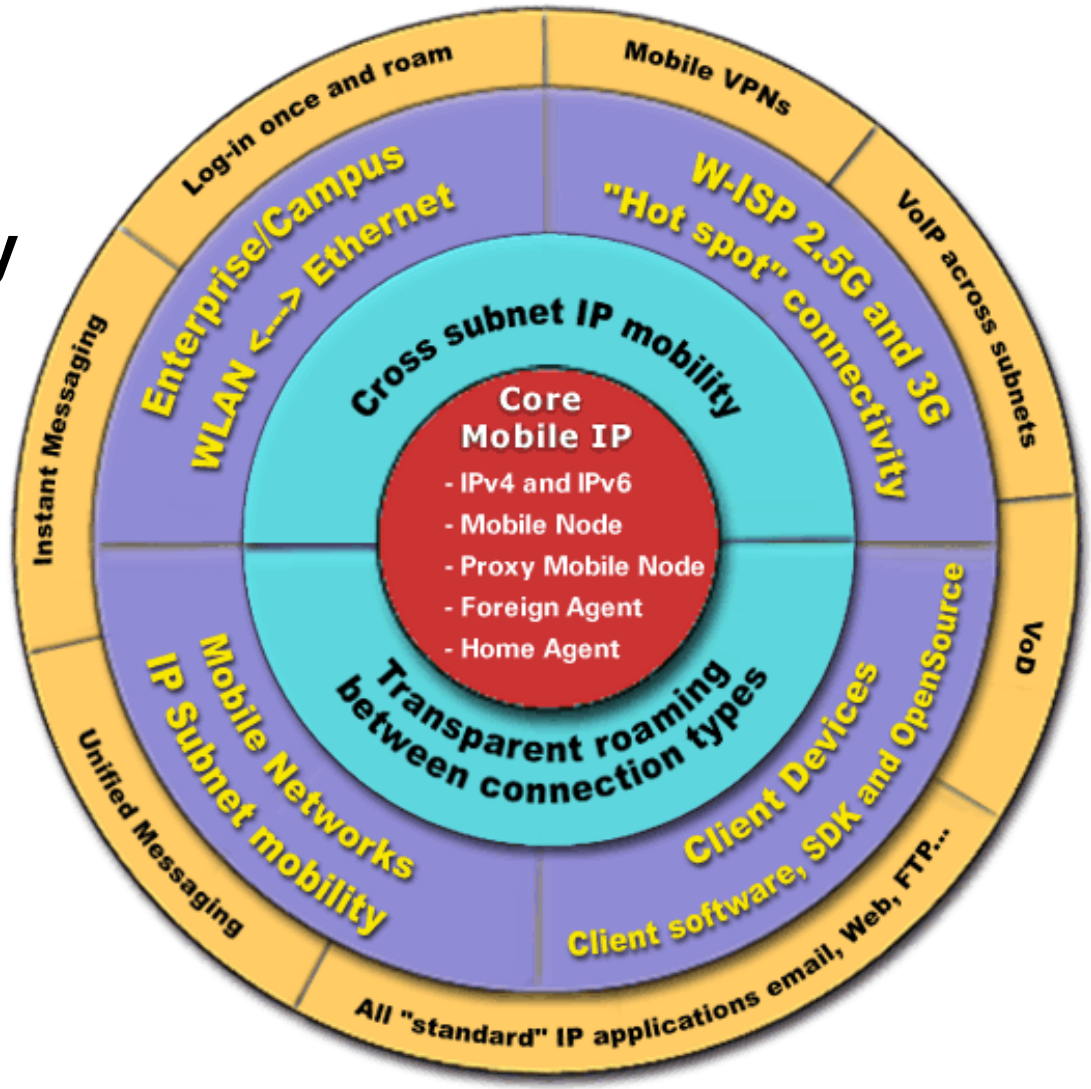
- **Books**

  – MOBILE IP The Internet Unplugged, ISBN 0-13-856246-6
  James D. Solomon

  – Mobile IP Design Principles and Practices, ISBN 0-201-63469-4
  Charles E. Perkins

Mobile IP – Delivering Convergence

- Unifying access
- Ultimate commonality
  - Access
  - Applications
  - Billing
- Improving the user experience
  - Promote usage
  - Increase loyalty



Backup
Mobile IP Details

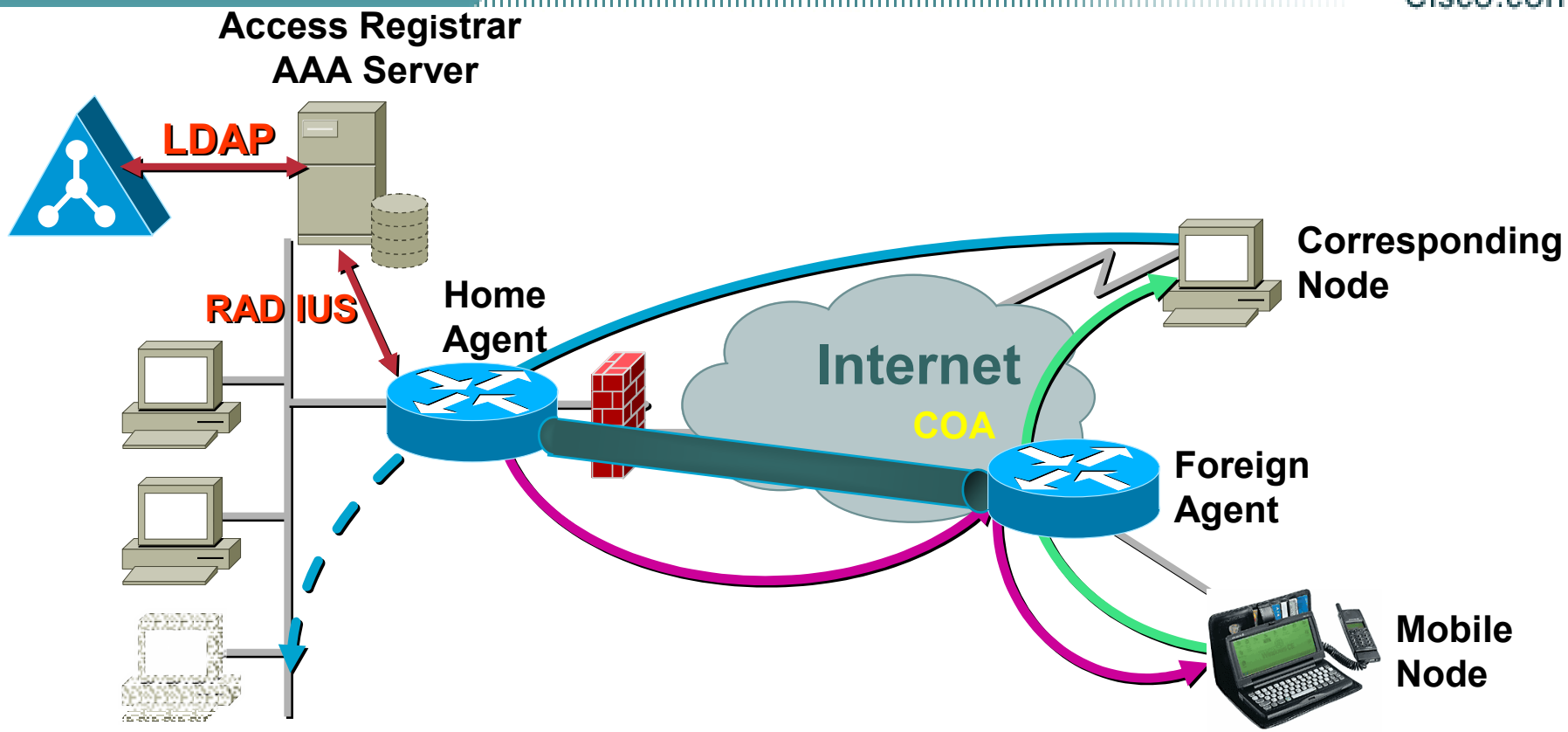
Foreign Agent Functionality

- Ability to configure maximum MN's able to visit or register with the respected Agent
- Configurable advertisement period
- Restricting Registration via ACLs
- MN-FA and FA-HA Authentication supported
- Foreign Agent can advertise out multiple interfaces
- Foreign Agent can force co-located MN's to register

Home Agent Functionality

- Home Agent (HA) is configured to the entire router, it can listen on all interfaces
- Ability to configure maximum MN's able to visit or register with the respected Agent
- Configurable advertisement period
- Restricting Registration via ACLs
- HA Redundancy, leveraging HSRP
- HA supports Tunneling broadcasts to MN's
- HA supports Reverse Tunnel
- 'Virtual Networking' support
  - Concept of MN never being at home, but always roaming
  - Single Home Agent supporting multiple 'virtual subnets'
  - MN and HA can have different network prefix, e.g. MN at 10.1.1.1 and HA at 1.1.1.1

AAA to Centrally store User Profile Information

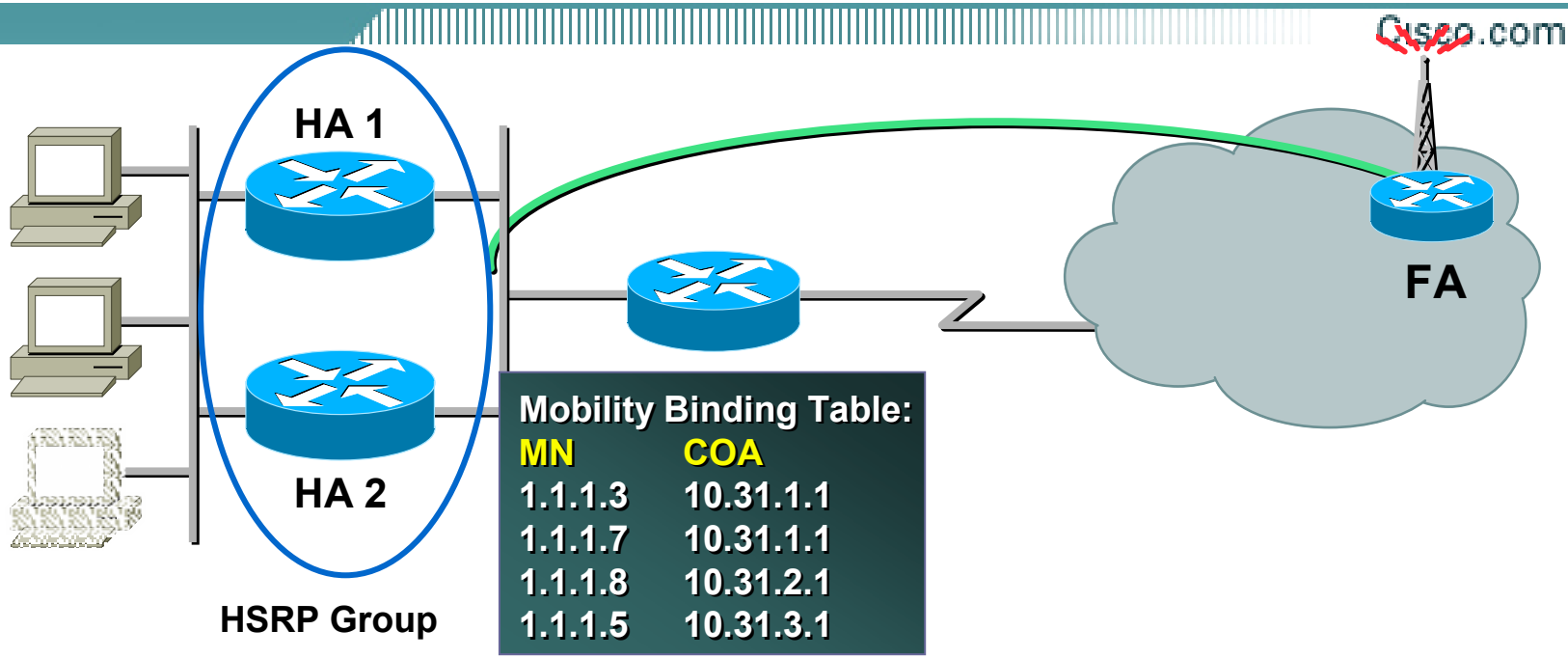


- User information (such as authentication information) is accessed via AAA server

AAA to Centrally store User Profile Information

- TACACS+ or RADIUS
- Centralize administration
- Retrieve MN's SA (key)
- HA authenticates/AAA Authorization
- Load SA versus retrieve each time
- NVRAM limitation
- Processing registrations

Home Agent Redundancy



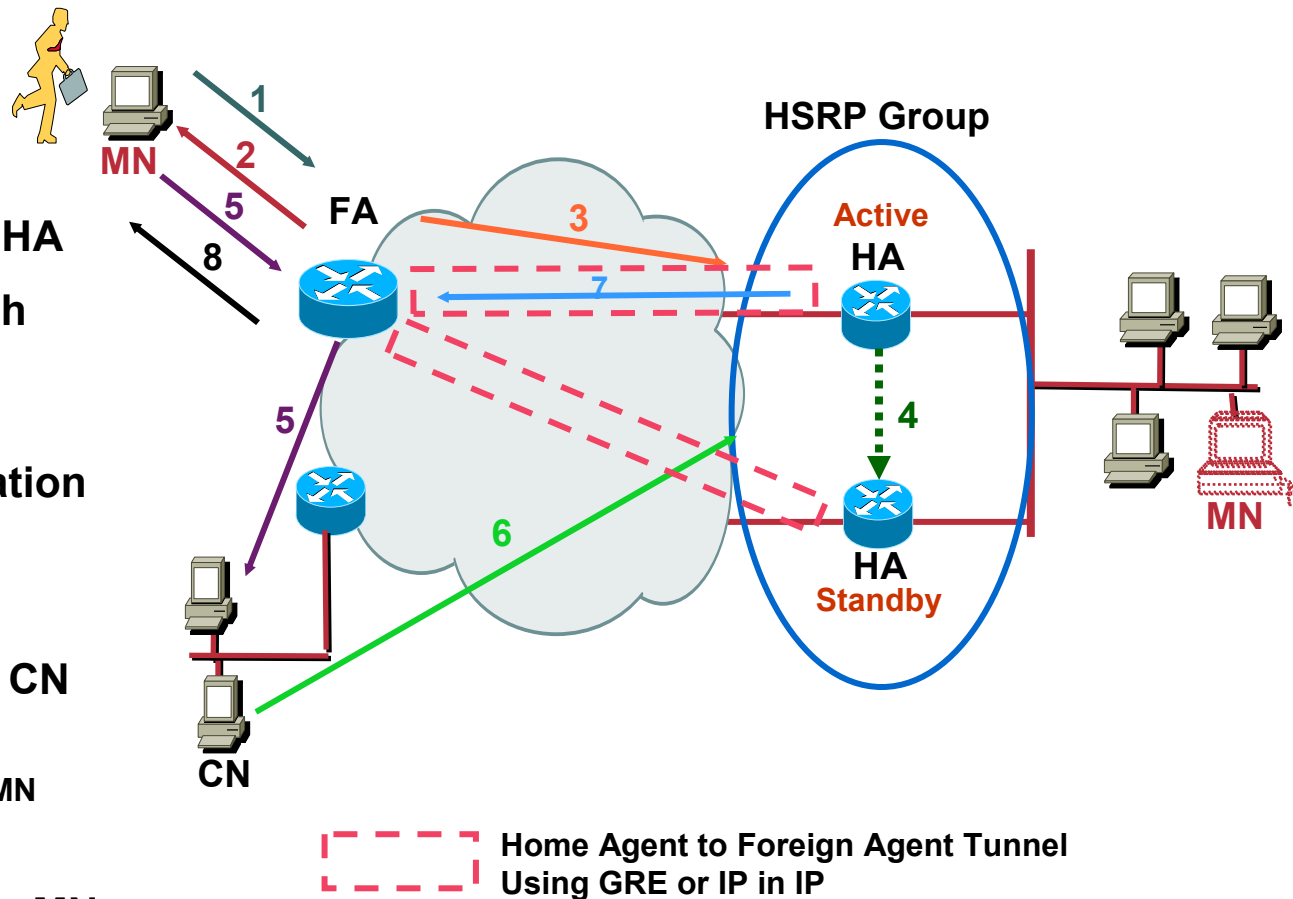
- **What happens if the HA fails?**
- **Based on Cisco IOS HSRP (Hot Standby Router Protocol)**
- **Available since 12.0(2)T**
- **Enables back-up in the case of a failure**
- **Ensures that mobility bindings stay in sync**
- **Load balancing**

Home Agent Redundancy

- **Home Agent Redundancy**
  - **Available since Cisco IOS 12.0(2)T**
  - **Use's Cisco IOS Hot Standby Routing Protocol (HSRP)**
    - **concept of an HSRP Group with 2 or more devices**
    - **Active and Standby device sharing a Virtual IP Address**
    - **1 or more HSRP Groups could be configured**
  - **Mobility Binding information is 'replicated' on the Standby (backup) HA**
  - **MN to HA Control traffic flows to the Active HA**
  - **CN to MN Data flow could use either Active or Standby HA based on routing protocol and network design**
  - **Standby HA will immediately take over FA-HA relationship(s) in the event of a failure to the Primary HA**

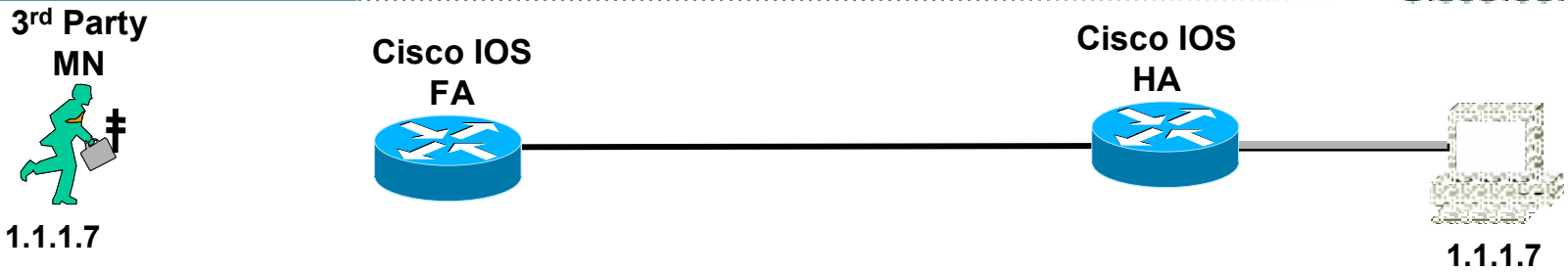
Home Agent Redundancy

1. MN discovers an FA
   - Agree on services
2. MN obtains COA
3. MN registers with Active HA
4. Active HA duplicates each Mobility Binding to the Standby HA
5. MN connects to a destination IP host (CN)
6. CN sends packets to MN
7. HA tunnels packets from CN to MN
   - Either HA might tunnel data to MN
   - L3 tunnel using GRE or IP in IP
8. FA forwards packets from MN to CN



Cisco IOS Mobile IP Registration/Advertisement Options

Cisco.com



FA Options

Registration Lifetime
B - Busy
F – Foreign Agent
G - GRE and IP-in-IP Tunneling
M - Minimal Encapsulation
R - Registration required, regardless if it has a co-located COA (FA only)
S - Simultaneous Bindings
V - VJ Header Compression
Authentication
T – Reverse Tunneling

HA Options

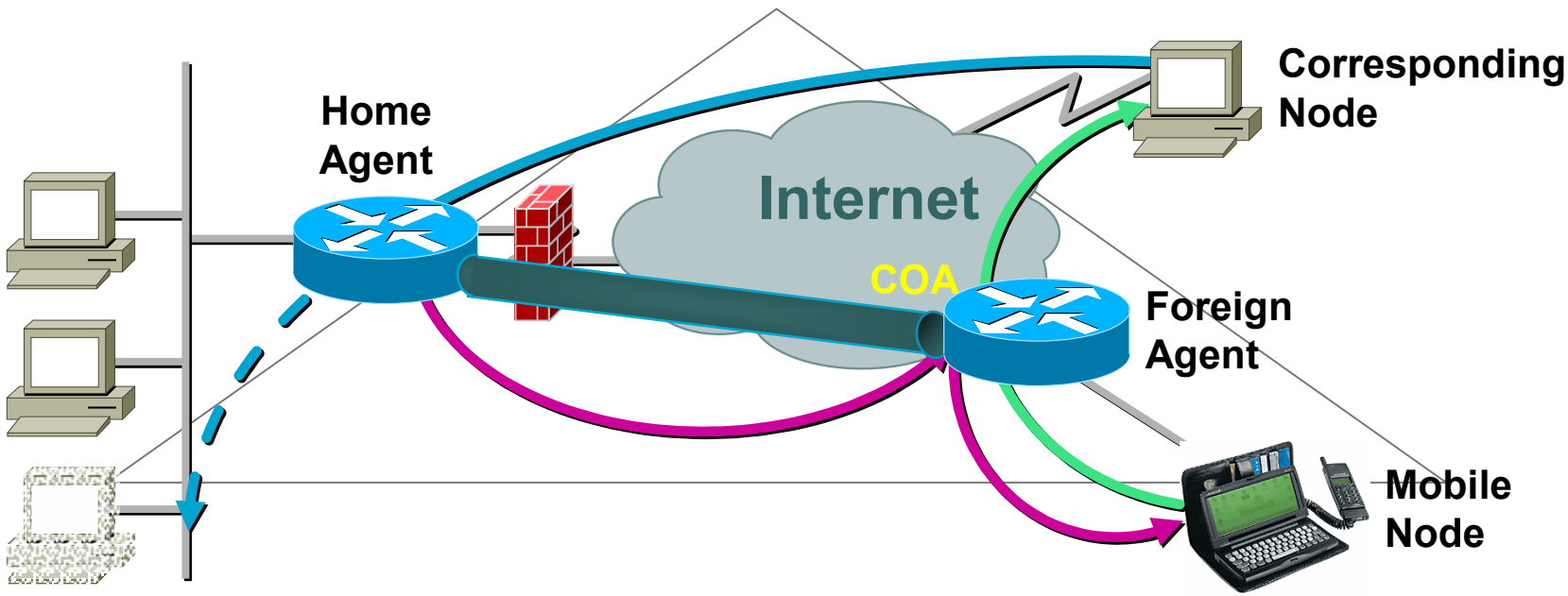
B – Busy
Registration Lifetime
D - Decapsulation (Co-Located COA)
G - GRE Tunneling
H – Home Agent
M - Minimal Encapsulation
S - Simultaneous Bindings
V - VJ Header Compression
Authentication
T – Reverse Tunneling

Not currently supported

Authentication - Mobile Node & Agents

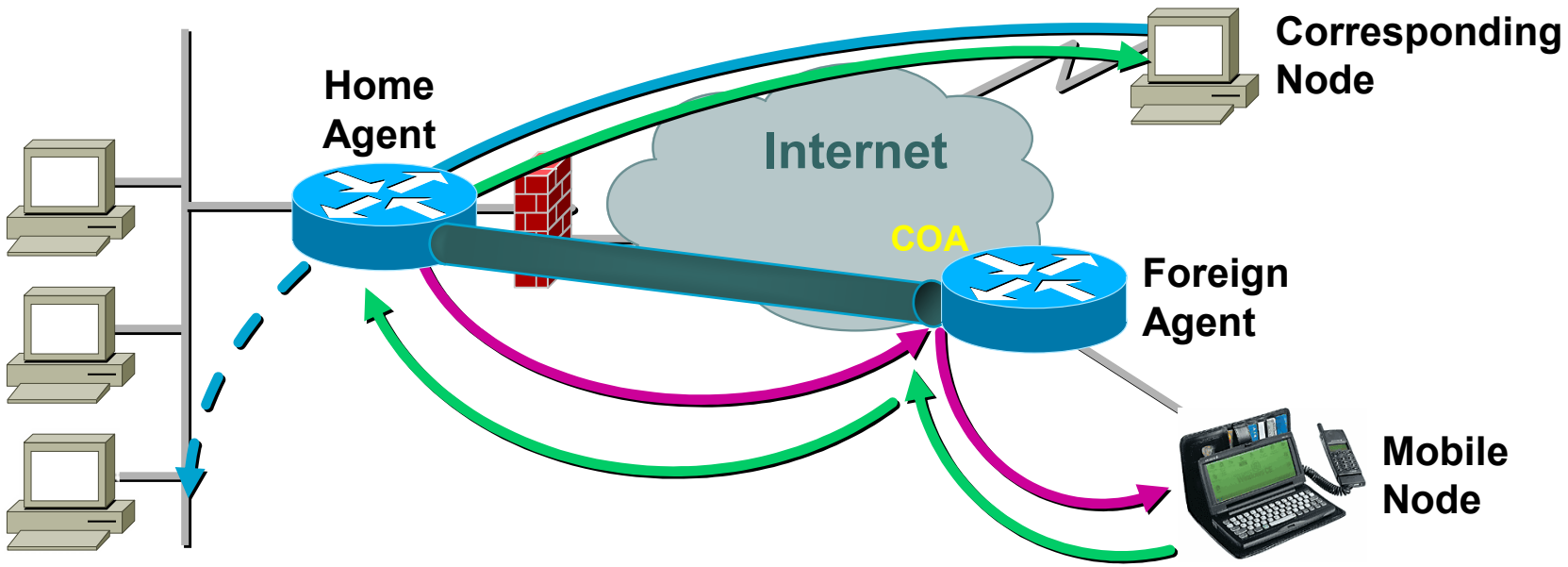
- **Authentication support**
  - **Mobile – Foreign Authentication Extension (MFAE)**
  - **Foreign – Home Authentication Extension (FHAE) Mobile – Home Authentication Extension (MHAE)**
  - **Keyed MD5**
  - **Identification via Time stamps**
  - **HA can optionally store MN SA info in a AAA Server (Radius or Tacacs)**
  - **HA identifies each MN using it's IP Address**
  - **Ability to set filters on the FA and HA to control access**

Typical Packet Forwarding "Triangle Routing"



- Traffic to the MN routes to the home network
- HA is responsible for redirecting this traffic to the MN's current location
- Traffic from the MN uses standard routing using the FA as it's router to the CN

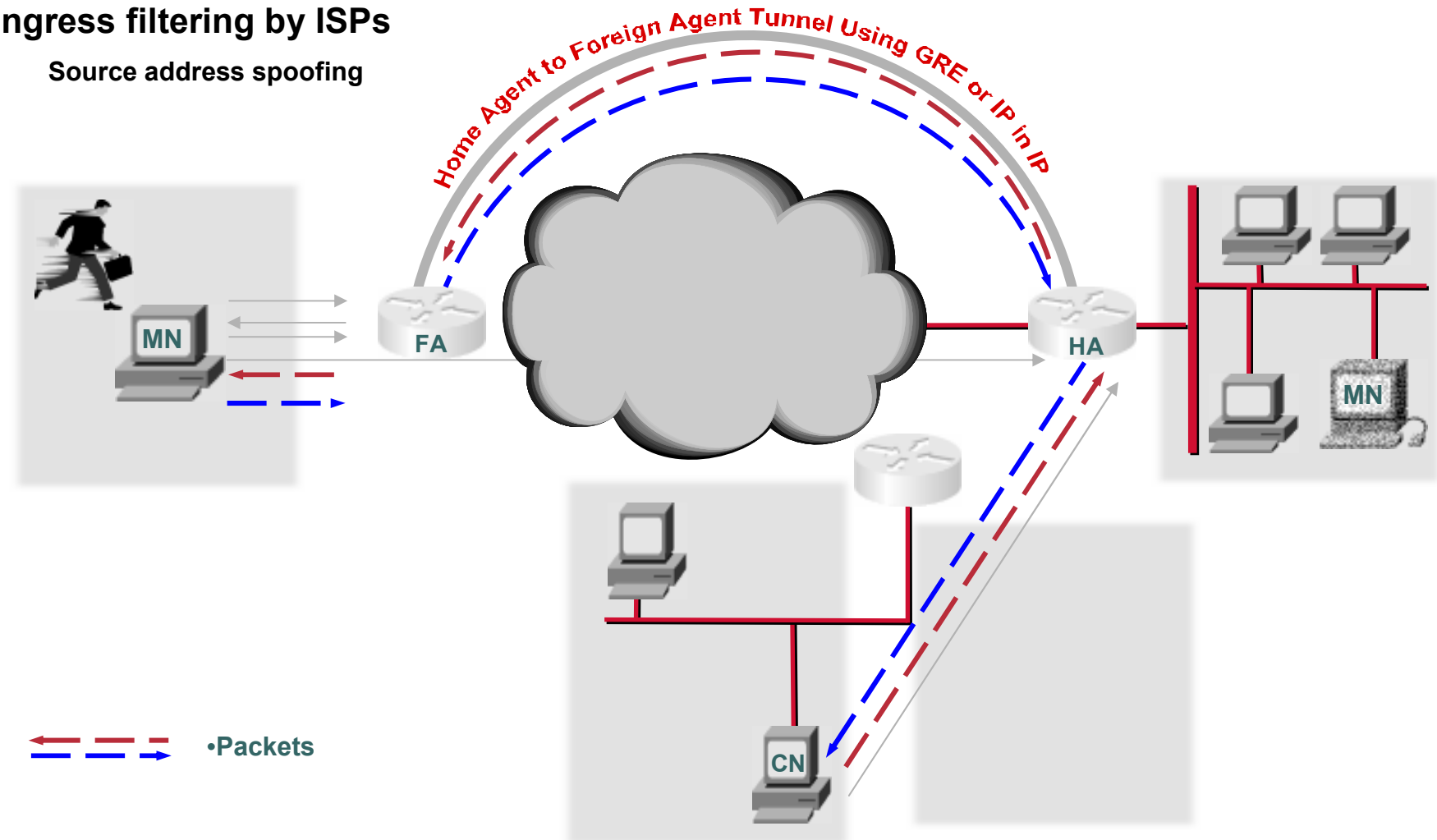
Reverse Tunnel - Alternate Packet Forwarding



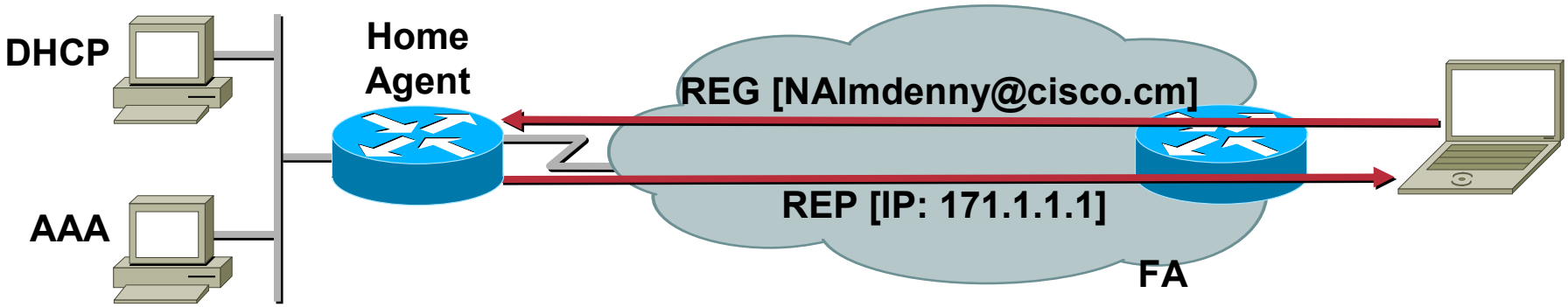
- All traffic to and from MN traverses the home network
- Enables MN traffic on a foreign network which is performing 'ingress filtering'
  - topologically incorrect source addresses
- Also used in NAT, Multicast, VPN behind the HA scenario

Reverse Tunnel - Alternate Packet Forwarding

- **Ingress filtering by ISPs**
  - **Source address spoofing**



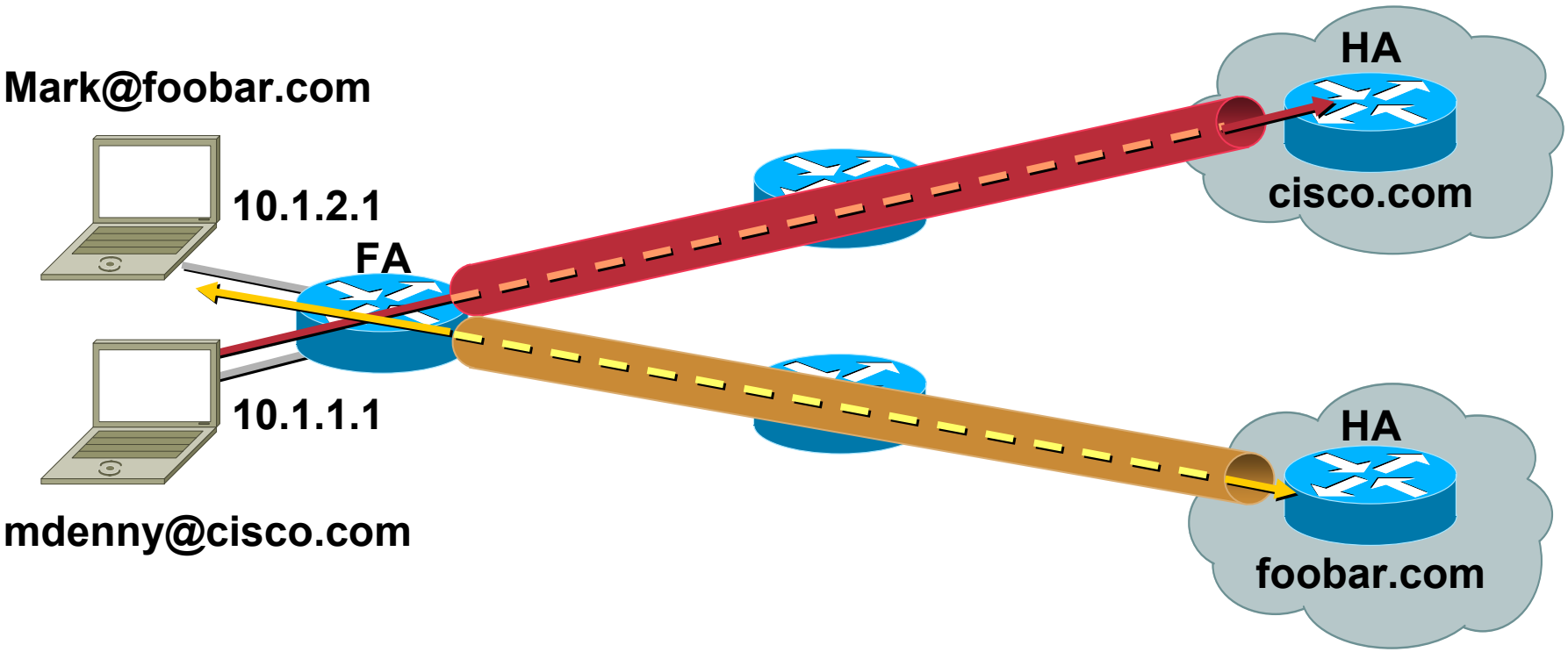
NAI and Dynamic Addressing



- **Basic mobile IP (RFC2002) only supports mobiles with fixed IP addresses**
- **NAI (Network Access Identifier) identifies the mobile**
- **IP address is dynamically allocated during registration**

  Use DHCP, AAA or Local Pool for allocating the address

Private Address Support



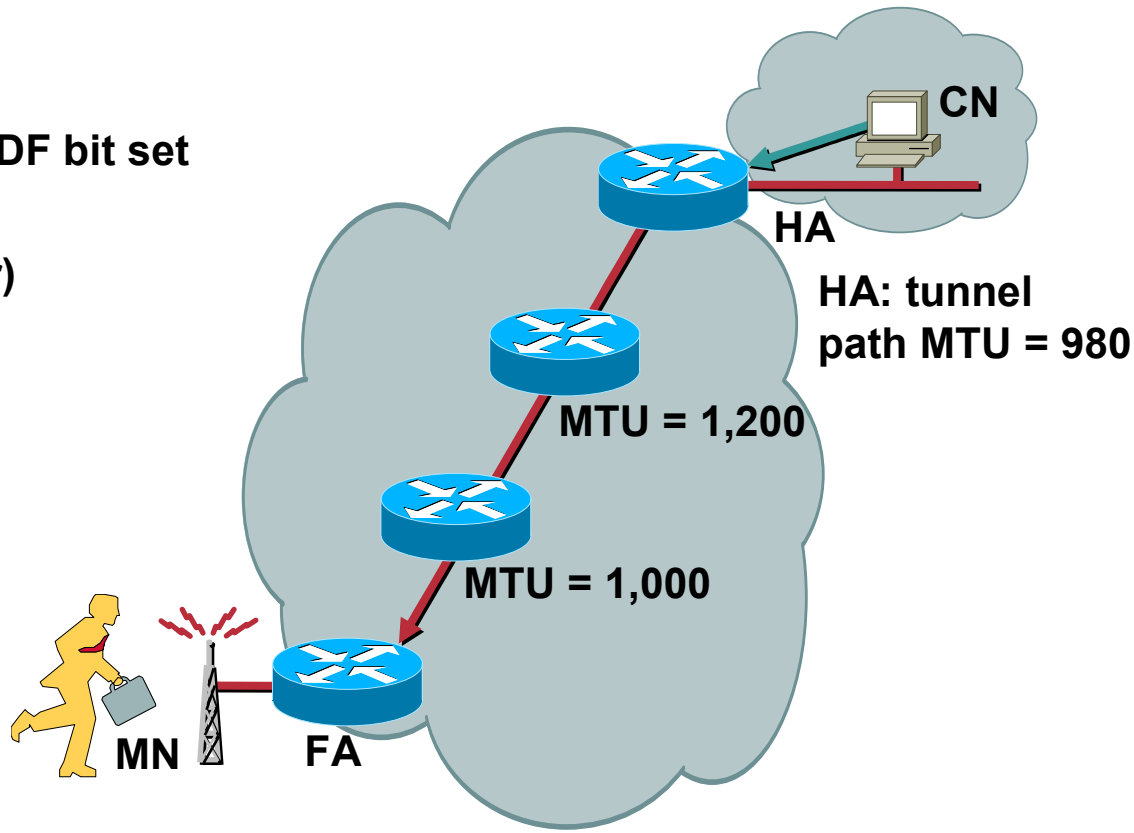
- Reverse Tunneled to the HA

Mobile IP Tunnels

- **Tunnel encapsulation support**
  - **IP in IP, GRE**
- **Mobile IP maintains what is referred to as “Soft State”**
  - **Path MTU**
  - **Tunnel Reach ability**

Mobile IP Tunnel

- **Path MTU Discovery**
  - CN sends packet with DF bit set
  - HA tunnels packet (DF bit set on outer header)
  - Router send ICMP unreachable
  - HA sets tunnel path MTU (minus tunnel header size)
  - HA sends ICMP unreachable to CN if packet too big

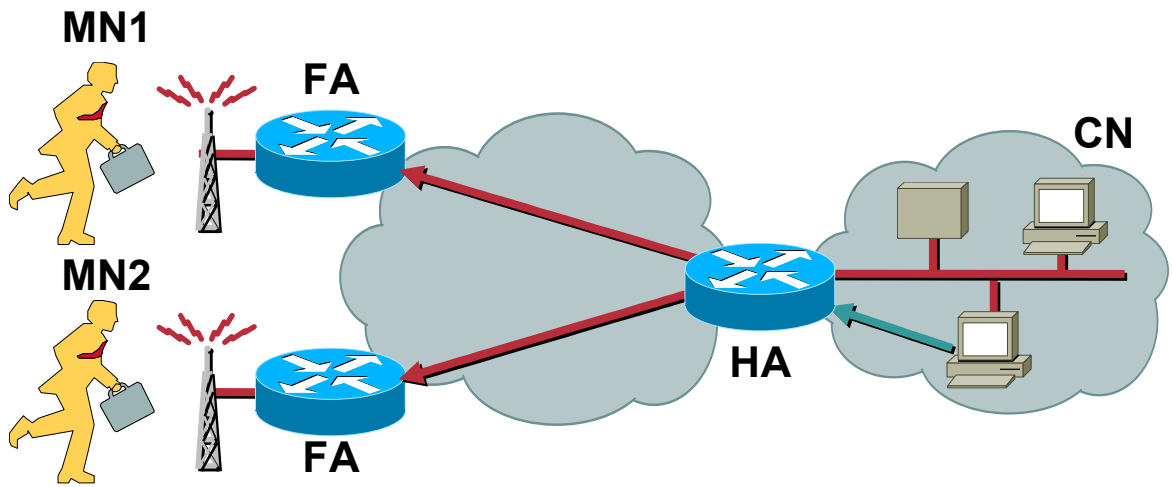


Mobile IP Tunnels

- An appropriate ICMP message can be sent to the originating host when a tunnel receives a packet to be encapsulated if;
  - Destination is unreachable
  - The packet has DF bit on and path MTU is to small
- Path MTU, tunnel origination point can decrease it's path MTU estimate
- Reset MTU in ten minutes, configurable

Routing of Broadcast Packets

- **Broadcast:**
  - Duplicate copies
  - Tunnel to co-located COA
  - Extra encap. to FA's COA
  - Disabled by default

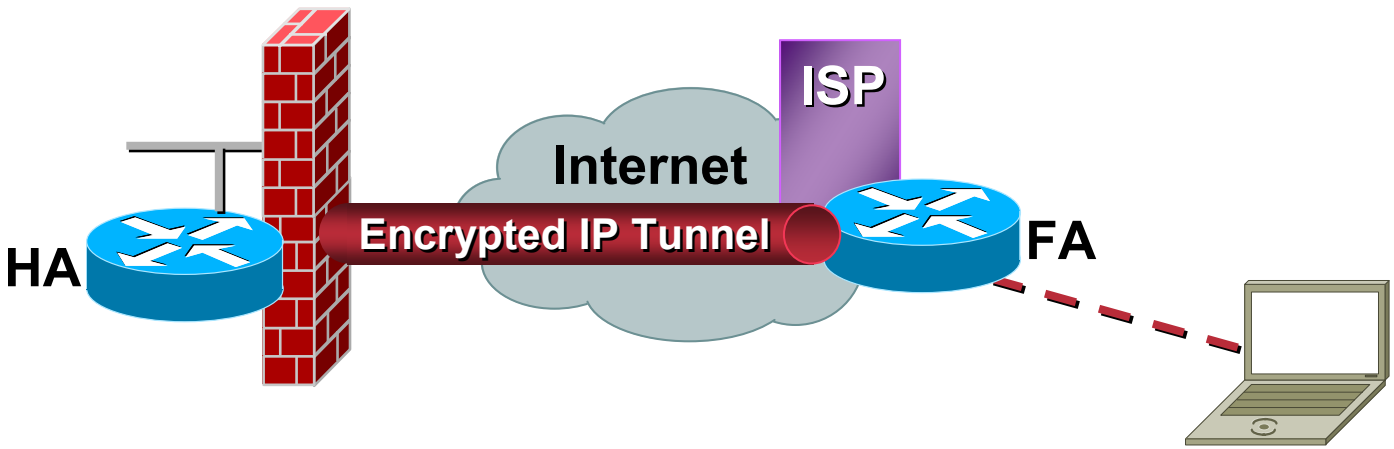


HA to FA	HA to MN	CN to All	IP Data

Mobile IP Capacity

- **Memory Footprint Sizing Mobile IP**
  - **1000 bytes/Mobile Node**
  - **14,000 bytes/Tunnel**
- **Tunnel capacity ranges from 250 to 3000 concurrent depending on platform in question**
- **Mobile Node capacity is limited by memory, however…**
  - **Internal Testing: 7200vxr with, 256mb, 1 FA-HA Tunnel, Cisco Access registrar RADIUS AAA Server to store Security Association:**
    - **Achieved in excess of 225,000 bindings**
    - **>100 registrations/sec**
    - **~15 ms/registration into AAA (10 AAA process configured)**
  - **In Production: A major Wireless Provider is supporting 200,000 concurrent Mobile Nodes per Home Agent**

Mobile IP and IP Security



- Use IKE to establish/negotiate IP security
- IP security can be used to encrypt mobile IP registration request/reply
- IP security can be used to encrypt the tunneled data
- Other features: IKE (Internet Key Exchange) using shared keys, digital certificates (X.509v3), etc.