

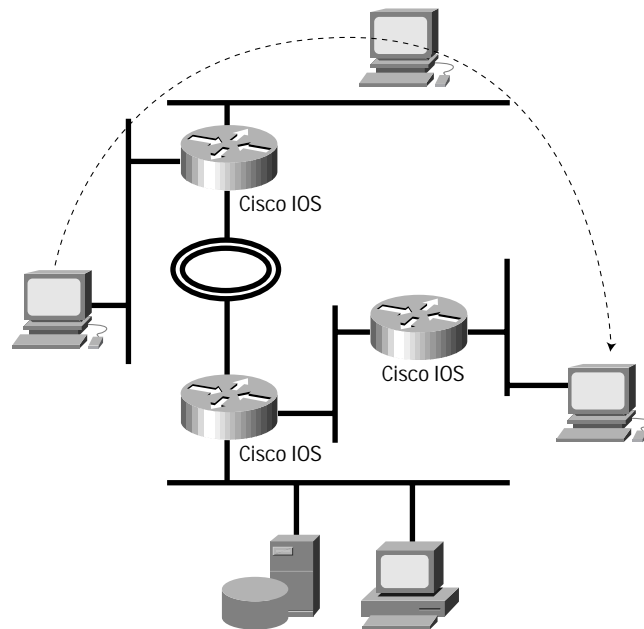
# Cisco IOS Local-Area Mobility— A Cisco IOS Software Solution to Business Needs to Enable Mobility Within the Enterprise Network

## Executive Summary

This paper presents the Cisco IOS™ software innovation local-area mobility, a technology that enables statically addressed hosts/PCs to move from their local subnet to another location within an enterprise network while maintaining transparent connectivity. Figure 1 shows the mobility possible using local-area mobility (LAM). This technique allows hosts the flexibility to roam from their home subnets, connect at other locations within the enterprise, and continue to receive datagrams addressed to their assigned IP address. This unique Cisco IOS feature does not require any software changes on the hosts.

Figure 1

Host Mobility: Hosts Can Be Moved While Reachability is Maintained.



This paper describes the details of the functionality of LAM and outlines areas where this solution can meet networking challenges. This technology is used primarily as an interim step in a gradual migration from an environment where hosts moving between different subnets would have to change their IP addresses or network administrators would have to change their VLAN configuration toward a fully dynamic IP address structure using Dynamic Host Configuration Protocol (DHCP). The paper reviews issues to consider when



deploying this Cisco IOS software technique. It enables administrators to determine the right deployment tactics to maximize the mobility of their users throughout the network. Configuration examples are also provided to assist in the successful implementation of LAM.

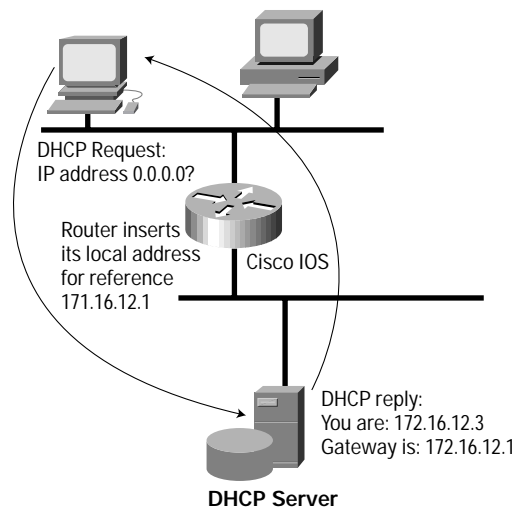
## Introduction

Access to people's home network and internal systems is an essential element to success in business. In today's world, people are often on the move within their corporate campus, but still need to be connected as though they were in their own offices. The need to be constantly connected is becoming a requirement in the business world. E-mail response times are necessarily short to facilitate quick, productive conversations between sometimes widely dispersed personnel. Access to resources in real time is often critical. Presentations sometimes need to be accessed and updated from conference rooms. All employees are expected to have relevant corporate information at their fingertips at all times. The virtual office is also fast becoming a reality, with the nearly full-time telecommuter visiting the corporate office only when necessary. Moving personnel between buildings or offices must not interfere with connectivity; therefore, enabling enterprise mobility is emerging as a key requirement within networks.

## Mobility Solutions

Cisco IOS mobility solutions are available for meeting connectivity challenges from different places throughout the network infrastructure. LAM is a mechanism that is intended to be a solution for mobility needs within an enterprise environment where DHCP is not available. DHCP is another alternative to mobility within a campus environment; it allows for a level of mobility, but it requires hosts to implement newer software. Hosts such as those running Windows 95 commonly use DHCP. This protocol, (described in RFC 1531), enables relocation of hosts by allowing for the leasing of IP addresses to the mobile hosts when they arrive on a subnet. This protocol enables hosts on a network to boot up and send a DHCP (BOOTP) request to a broadcast address in order to gain an IP address for its use (see Figure 2).

Figure 2  
Acquiring an IP address with DHCP





This address can be allocated from a pool, either permanently or for a “lease” period. These broadcast requests can be forwarded by a Cisco IOS router, using the `helper address` command to a server in a centralized location for scalability. Because no host software changes are necessary in deploying LAM, it is a very attractive interim solution to network administrators, for obvious cost-saving reasons. It has the further advantage of allowing the Domain Name System (DNS) structure to retain its current information and enable reachability of the mobile host. This fact makes LAM an ideal transition technology. When DHCP is supported throughout the network, LAM can be disabled.

For Internet-wide mobility or beyond the enterprise, other Cisco solutions are available. Dialup mobility can be achieved with Cisco IOS software Layer 2 Forwarding (L2F) or Layer 2 Tunneling Protocol (L2TP) solutions. Another Internet Engineering Task Force (IETF) mobility solution that Cisco IOS software supports is mobile IP. This protocol is described in RFCs 2002–2006. Mobile IP enables mobility beyond a single enterprise by allowing a router on the mobile host’s home subnet to intercept data and tunnel it to the traveling mobile node. When using this protocol, mobility is transparent to anyone communicating with the mobile node, as well as all other routers within a network or the Internet. This solution is particularly useful in areas where wireless infrastructures are used and where transparent hand-offs mobility is necessary. Each of these IOS solutions functions somewhat differently, and each offers its own set of benefits. Information on these Cisco IOS technologies can be found in the “Routing Solutions” section of the IOS Software Technology pages.

## The Technology

### **The Challenge: Normal Packet Forwarding Background**

Since LAM is based on IP, a brief review of the concepts fundamental to the forwarding of IP packets may be helpful in understanding how this innovative solution operates. In a normal IP network, packets are routed according to some basic premises, the first being subnets. TCP/IP devices look at the address and subnet mask configured on their interface(s) in order to determine what other IP addresses are reachable on the directly connected network media. If the IP address to which the device wants to send a packet falls within the range of its local subnet, the device employs the Address Resolution Protocol (ARP) for the link-layer address in order to forward the packet directly. If the address does not fall within this range, then routing is needed. When a host has data to send to an IP address not on its connected subnet, it forwards the packets to a device that it believes can route the traffic to its destination. From a nonrouting host, the packet is forwarded to its configured default gateway, normally a router on the host’s subnet that can reach the rest of the enterprise network or the Internet.

The next concept to consider is routing. When a router receives a packet, it does a route lookup in order to determine where to forward the packet. The routing table contains information about directly connected subnets, statically configured information, and the dynamic information derived from the routing protocol(s) configured. Routing protocols allow routers to dynamically exchange reachability information about each of the IP networks that they know how to reach. If the route turns out to be known via a directly connected subnet, the router ARPs for the destination’s link-layer address and forwards the packet; otherwise, it determines the next hop router and forwards it to that device via its link-layer address. Devices that remain in their topologically correct subnets may receive their packets using this routing paradigm. However, if a device moves off the subnet where its configured address matches the local subnet information, this model fails to serve them. So far there is no dynamic mechanism to enable the router to learn the location of these mobile hosts. Packets continue to be directed to the subnet where they logically belong. When no ARP reply is received by the router or host at this subnet, the packets are dropped.



An important point is that Cisco IOS routers implement an optimized longest prefix match route lookup. Therefore, routes of a finer granularity than that of subnet ranges can be used to make forwarding decisions. Longest prefix matching enables the use of host routes to forward traffic in a direction different from that of the rest of the subnet range because the most specific route is always preferred. A host route is a route that has a mask of length equal to that of the IP address, or 32 bits. This route specifies a single host. For example, if a subnet route is as follows:

```
RouterA#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
Gateway of last resort is not set
131.108.0.0/16 is variably subnetted, 2 subnets, 2 masks
D 131.108.12.3/32 [1/0] via 171.68.207.12
D 131.108.12.0/24 [1/0] via 171.68.207.18
171.68.0.0/16 is subnetted, 1 subnets
C 171.68.207.0 is directly connected, Ethernet0
```

The subnet route says 131.108.12 (anything in the last 8 bits) goes to 171.68.207.18 as the next hop. The host route from this subnet range says 131.108.12.3 (only) goes to 171.68.207.12 as the next hop.

This means that while a subnet may be directly connected, a host route may be received for a device that would normally be in this subnet, and this more specific route can be used to forward traffic. Of course, static routes to all mobile hosts could represent a lot of configuration overhead and could be difficult to manage. The LAM solution allows for dynamic host mobility using this routing attribute.

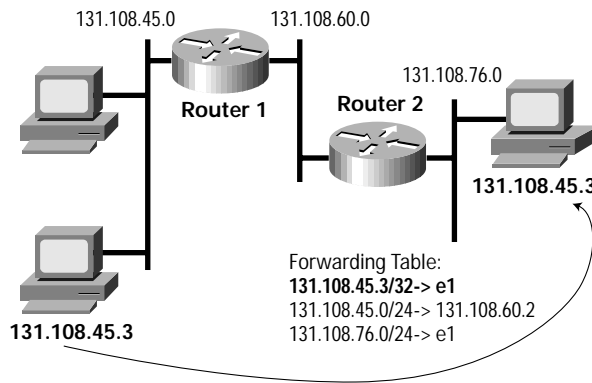
### **The Local-Area Mobility Solution**

Local-area mobility is a Cisco IOS software innovation that allows for the transparent mobility of hosts within an enterprise or campus network. This technology can optionally be implemented on some routers in a network with relatively little impact on the rest of the network. LAM functions in a straightforward manner. A router configured for LAM inspects traffic on its LAN interfaces in order to determine whether there are directly connected hosts that do not belong to the local IP subnet. When this router sees locally originated traffic from a host that does not match the address and mask configured on that interface, the router installs an ARP entry for this mobile host. This router then also installs a host route that points toward this interface.

If configured to do so, this router redistributes this host route into the routing protocol or protocols that it is running, provided the configured protocol is an Interior Gateway Protocol (IGP) that allows for host routes to be carried. These IGPs include Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF), the protocols most predominantly used in enterprise networks today. Routing Information Protocol Version 2 (RIPv2) and Intermediate System-to-Intermediate System (IS-IS) are also usable with this solution. The rest of this routing domain is then able to learn about the new route to this mobile host, as shown in Figure 3.



Figure 3  
Local-Area Mobility Functionality; the Propagation of Host Routes.



Cisco IOS software's longest prefix match lookup combined with these dynamic mobile host routes allows for transparent packet forwarding. This solution maintains reachability from anywhere within the routing domain. Other hosts can now directly communicate with the mobile host. Even hosts on the home subnet can communicate with the mobile host, because the router utilizes proxy ARP (RFC 826) to ensure this transparent connectivity. Proxy ARP is the mechanism by which a router informs a device that it may forward traffic to its Media Access Control (MAC) address, in proxy of another destination address that is not present on the wire. This forwarding is done when the router knows how to reach the missing host. If a Cisco IOS router knows the route to a device and sees an ARP request on the LAN, it proxy ARPs in reply. When a host wants to send traffic to a mobile host, it ARPs. The router, having a route to this mobile host, will proxy APR in reply to enable traffic to continue to be sent to this mobile host.

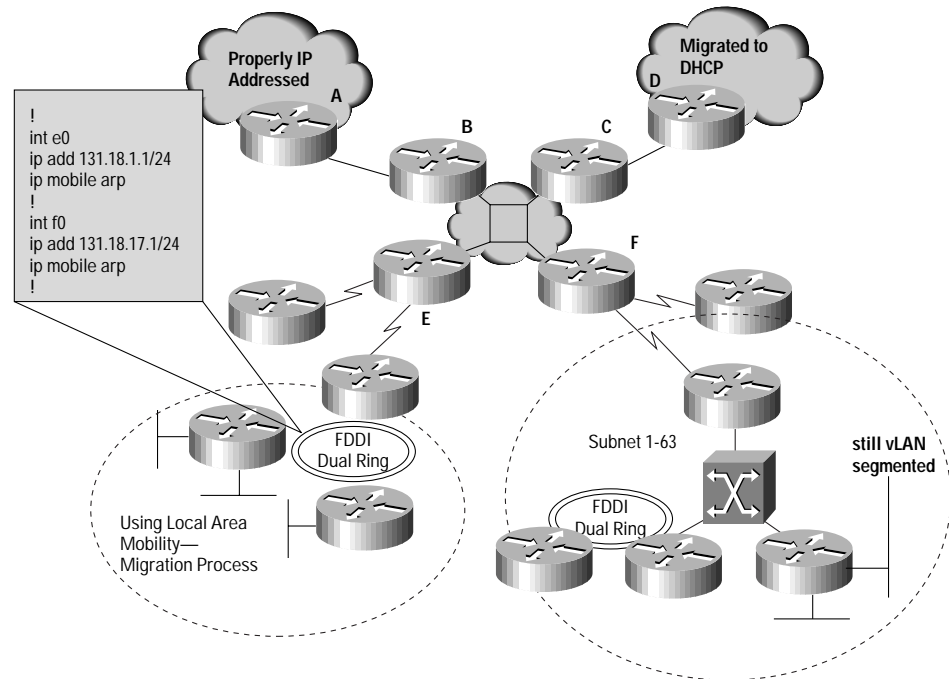
#### Benefits of the Local-Area Mobility Solution

##### Migration to Layer 3 Connectivity

More and more customers, as they grow their enterprises and want to enable network services, are moving toward Layer 3 routing/switching architectures. The prospect of pursuing this migration confronts the network administrator with a tremendous dilemma. Although the ability to offer network- level services, such as quality of service, greater bandwidth management, security, and multicast and multimedia services, is tempting, the work to migrate can seem overwhelming. This transition can be a big task that involves reconfiguration of most host machines. Local-area mobility can be used as a key interim step in this evolutionary migration. While areas of the network are in transition, this unique mechanism can be used. During this time, hosts can then be properly subnetted and addressed, or DHCP client software can be installed and configured on them. After this configuration, the feature can be disabled in that portion of the network and then the next network section can be migrated in order to enable a smoother transition.



Figure 4  
Migration to Layer 3 Enabled by LAM



### Other Uses for Local Area-Mobility within an Enterprise

LAM can also provide a good solution for the mobility of a few hosts within a network. This solution has finite scaling properties, but most enterprises experience no problems. DHCP could potentially be a more scalable alternative for pervasive mobility of hosts throughout an enterprise, if reconfiguration is possible. The scalability of LAM is discussed in the following sections. This feature can offer a simple and dynamic mechanism to facilitate moves, adds, and changes. This IOS solution can enable either transition or, for the decision of continuing to utilize Layer 2 technology, a more permanent and simplified solution to achieve IP host mobility.

### Configuration

Several decisions must be made when deploying LAM; for example, who will be allowed to be mobile, and what IGP will be used. LAM can be used in different ways, depending on your needs. Routing protocols require planned deployment for the addition of numerous host routes, to ensure that the network can scale well. Care must be taken to ease changes into the network and routing protocols. If numerous mobile hosts in a network are constantly changing their subnet attachment points, or if numerous mobile hosts attach simultaneously, for example, at 9:00 a.m. Monday morning, problems may arise. Some host TCP/IP implementations can have difficulty adapting to movement because of their ARP timers. These issues are addressed in the following sections.



## Redistribution of Mobile Routes

The mobile routes are redistributed if the command `redistribute mobile` is configured under the appropriate classless routing protocol (for example, EIGRP, OSPF). If necessary for the routing protocol to accept the route, indication of a default metric may be required either globally or within the `redistribute` command. This metric is required for EIGRP, for example. The redistribution enables the dynamic element of the LAM feature. It is important to ensure that configured or redistributed static routes do not include any host routes for the potentially mobile hosts. Otherwise, a longest match could come up with two routes and cause ambiguity. The only router that can see that a route is mobile is the one in which the host is directly connected. In the redistributing router, this route is marked with an “M” for mobile, to show where the route has been obtained:

```
Router_A#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP,
M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
U - per-user static route, o - ODR
Gateway of last resort is not set
171.68.0.0/16 is subnetted, 1 subnets
M 171.68.23.249 [180/1] via 171.68.23.249, 00:00:10, Ethernet0
131.108.0.0/16 is subnetted, 1 subnets
C 131.108.10.0 is directly connected, Ethernet0
```

However, there is no way to prefer this new route over another host route because of mobility.

The mobile ARP entries can be configured to time out more quickly. The LAM feature allows for the configuration of a keepalive time and a hold time for mobile ARP entries on an interface. The hold time for the mobile ARP entries is by default shorter than that for the subnet appropriate ARP entries. When using LAM, a router periodically checks to ensure that the mobile host is still there by querying it with ARP requests. This ensures that the redistributed route is still valid. The mobile host ARP keepalive times can be altered with the command:

```
ip mobile arp timers [keepalive minutes] [hold-time minutes]
```

These commands can be used to speed the process of invalidation. The default keepalive time is 300 seconds, or 5 minutes, and the default hold time is 900 seconds, or 15 minutes. The keepalive time can be changed to any value from 1 to 1440 minutes, and the hold time can vary from 1 to 14,400 minutes.

## Good Routing Design Practice

Regardless of the routing design or summarization, a component of using LAM is the injection of host routes into a network. General issues that may arise relate to the amount of memory that could be needed in each router because of the number of routes installed, and the number of updates that may be triggered by the movement of hosts. Mobile routes are seen as “external routes” to the configured routing protocol, even within a summarization area; therefore, they are not properly summarized by default. This situation is true even when these routes are advertised at a summarization boundary, if mobile hosts are not on their home subnet. Steps can be taken to help routing protocols better deal with mobile routes. One general suggestion is to ensure the summarization of the fixed location IP



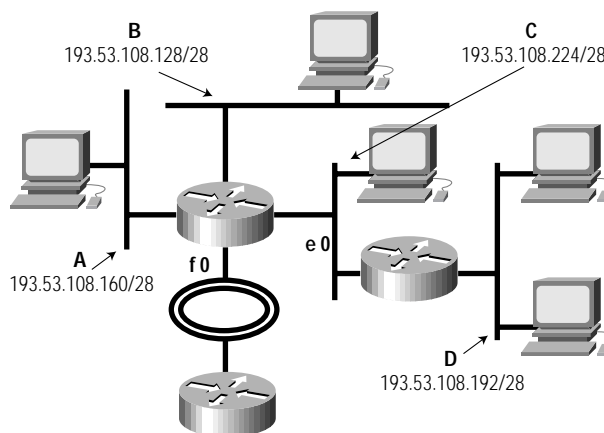
addresses to the best degree possible. Please refer to the Internetwork Design Guide. This summarization will make it possible to carry more mobile routes. When migrating a network to a Layer 3 architecture, the network designer should allow for IP addresses to be neatly and concisely summarized as close to the origin of the route as possible. Limiting any constant physical relocation of mobile hosts between subnets also helps to reduce the number of updates that might be triggered, since updates need to be sent when hosts are moved to new locations.

The only IGP's that can be used in conjunction with LAM are classless routing protocols, since they support host routes. The classless interior routing protocols that Cisco IOS software supports include Enhanced IGRP, OSPF, IS-IS, and RIPv2. These protocols behave differently, and each has its own advantages. Network administrators should be aware of some design issues when using LAM. The two most popular ISPs for the enterprise, Enhanced IGRP and OSPF will be discussed in relation to LAM.

### Enhanced IGRP

The use of Enhanced IGRP with LAM is optimal. The advantages of Enhanced IGRP range from the overall simplicity of configuration and the flexibility of summarization to the localization of routing table changes and fast convergence, which result from the operation of the Diffusing Update Algorithm (DUAL) mechanism. From the perspective of Enhanced IGRP, any routes not originated within the protocol are external routes, as, for example, LAM derived routes. Thus the summarization that occurs by default at major network boundaries in Enhanced IGRP does not include summarization of mobile routes. A mechanism within Enhanced IGRP allows for the configuration of summarization ranges, which can include mobile routes, however. This configuration option is available on a per-interface basis, allowing for more efficient scoping of mobility areas. In order to take full advantage of hierarchical routing structures, manual summarization is a good practice when using LAM. The network in Figure 5 shows that summarization mechanisms increase the scalability of Enhanced IGRP routing and the usefulness of LAM.

Figure 5  
A Network Whose Address Allows for Summarization



Configured summarization allows mobility within different portions of the network and at the same time allows information related to these topological changes to be localized to a subsection of the network. Host movement or relocation between subnets A, B, C, and D can be hidden, while f 0 advertises 193.53.108.128/25. Behind the summarization boundary, the host routes can be propagated to all the routers in these sections of the network, or if desired and applicable, a lower degree of summarization can be done within this area. Hosts moving between subnets



A and B can be completely transparent within the network, if interfaces f 0 and e 0 summarize the two subnets as: 193.53.108.128/26. After a summary route has been created, the routes are known via Enhanced IGRP, which allows them to be summarized further beyond this point. Another scalability factor is that after a summary route is configured, queries are propagated only one hop beyond this summarization point if a route is lost.

Another advantage to using Enhanced IGRP is that after a host has moved off its home subnet and a routing update is sent, barring further movement of this host, no additional routing updates are sent about the location of this moved host. The routing updates do not time out, so no matter how many hosts are mobile, as long as they don't all move at the same time, large routing updates are not caused by this mobility.

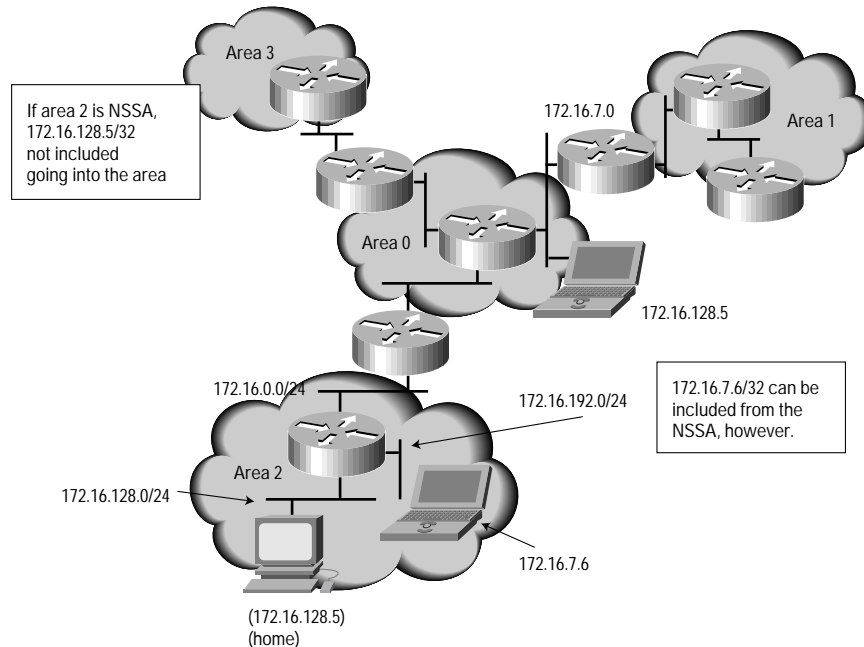
## OSPF

An element of the overall scalability of OSPF is the concept of areas, which allow for the consolidation and summarization of address ranges. Although the area border router (ABR) summary range may include, or overlap, mobile host routes, these routes cannot be summarized when using LAM because OSPF regards any routes not originated within OSPF as external. Only the autonomous system boundary router (ASBR) that originates these routes can summarize them. This makes it difficult to enable any summarization of routes on a truly dynamic basis. However, using the summary-address command, these routes can be aggregated on a per-ASBR basis. In the case of a network migration where the LAM routes are transitory, but fixed, it may be possible to do this sort of aggregation. If this is not possible and the overall number of external host routes becomes very large, it is possible to run two iterations of the OSPF process, allowing for redistribution of OSPF routes into OSPF and for summarization and aid in scalability, while migrating. This process, however, could be quite complex.

If stub areas are defined in a network, LAM must *not* be enabled for hosts from that area because the stub area never has external routes leaked into it. This of course, prevents the network from propagating a route back to the stub area for any mobile host that has moved outside of its stub area. The use of not so stubby areas (NSSA), introduced in Cisco IOS 11.2. NSSA allows the mobility of hosts into this area, if this feature is needed or desired. The mobility of hosts from the NSSA into other areas is not possible, however, since external routes are never leaked into this area, only out of it. This setup is shown in Figure 6.



Figure 6  
OSPF with Enterprise Mobility: The Issue with Stub Areas and NSSA



Type 5 Link State Advertisements (LSAs) (which describe external routes) increase linearly with the mobility of hosts. If the route originates from a different area, a type 4 LSA (which describes the route to the ASBR) is also sent.

Care should be taken when increasing the number of mobile host routes injected at any one time by a significant degree. For example, at 9:00 a.m. Monday, when all users arrive at the office and boot their mobile hosts, there may be an issue. In OSPF, LSAs have a maximum age timer, so at a minimum of every half hour a full LSA must be sent by every router that runs OSPF in order to refresh the routes that it advertises. Therefore, it would be ideal to reduce the number of mobile hosts per area to a manageable number. The design of the backbone area is significant to the scalability of OSPF and the network. This is true with any OSPF network, but issues may become more visible with the addition of LAM to the network. For example, if the core of a network is a mesh of nonbroadcast multi access (NBMA) media, defining the network type as “broadcast”, scales the network better since it allows for the election and use of a designated router (DR) Designated routers control the flooding, which must occur at least every half hour. This configuration reduces the number of LSA packets that traverse the core media. Refer to the OSPF design guide for more information about implementing this routing protocol in networks.

## Security

Although security issues are localized by the fact that this feature is used only within an enterprise, LAM may have security requirements. When using this technology, it is conceivable that someone could get on a campus network and claim ownership of an IP address and cause a host route to be installed. The danger is not generally greater than it is with a DHCP solution, where someone can gain an IP address and utilize it, or in a fixed IP addressed network where a host could configure an IP address and access a network. Security measures need to be activated on top of any sort of connectivity solution, but determining what these solutions are in the LAM environment may be difficult. Also important to remember for security is the need to ensure that access lists allow access to resources for those who



need it, while protecting resources. Essentially, access lists need to account for the possibly mobile hosts. Hosts may now be accessing resources through different interfaces than they normally would, for example. Of course, when using this solution, appropriate configuration commands should be applied only to interfaces that need to listen for foreign ARPs. Cisco IOS LAM allows for granular identification of the hosts that are allowed to be mobile. These privileges can be configured using access lists. The interface command

```
"ip mobile arp access-group []"
```

is used to specify a list of acceptable mobile hosts in order to restrict mobility to a specific group of users or hosts.

### **Host Issues**

Hosts may have issues when allowing this sort of mobility in a network, both the host that is mobile as well as the hosts that are local to the mobile host's home subnet. Rebooting the host that has been moved from its home subnet when it arrives at its new destination is recommended. This rebooting not only ensures that the ARP entry is entered in the router, and therefore the route is propagated, but it also clears the ARP cache of this mobile host. Therefore, it ARPs for hosts that would normally be on its own subnet, but might have been cached earlier. Remember that the router will proxy-ARP for addresses, so the configured default gateway will not be a problem. The hosts from the mobile host home subnet may need their ARP caches to be updated to reflect a proxy-ARP entry, the router's MAC address, so that they may continue to communicate with the host that is now mobile. Ensuring that the mobile host sends traffic first enables the route to propagate all the way to the home subnet, where the home router can proxy-ARP this moved host and prevent any communication problems for these hosts. A future IOS software enhancement will enable the router to send a gratuitous ARP when a host route is received for a normally directly connected subnet. This scenario will enable the updating of binding in the hosts in the event that they cached information when the host was local to the subnet. Almost every TCP/IP host will update ARP cache entries with the proxy's MAC address, including the popular Windows 95 software. LAM can work transparently with all hosts under these conditions.

### **Software Support**

Local-area mobility has been integrated into all major Cisco IOS software releases as of Release 10.2(1). It was integrated into the route switch module (RSM) of the Catalyst® switches in Release 11.2(9)P. LAM is supported on Ethernet, Token Ring, and Fiber Distributed Data Interface (FDDI) interfaces.



## Examples

### Simple

In this example, the router is on several Ethernet segments. It is configured to allow hosts to roam between all the Ethernet subnets attached to it. The router listens for “foreign” ARPs to add them to its routing table and send appropriate updates toward neighbor routers. This configuration allows connected hosts to gain access to the network through LAM.

```
!  
version 11.2  
!  
hostname Local-1  
!  
enable password cisco  
!  
interface Ethernet 0  
 ip address 131.108.10.5 255.255.255.0  
 ! Command enables LAM; timers to increase the keepalive timer to two minutes and the hold time  
 to five minutes  
 ip mobile arp  
!  
interface Ethernet 1  
 ip address 131.108.11.5 255.255.255.0  
 ip mobile arp  
!  
interface Ethernet 2  
 ip address 131.108.12.5 255.255.255.0  
 ip mobile arp  
!  
 ! A classless routing protocol that can carry host routes router eigrp 1  
 network 131.108.0.0  
 ! Allows for the redistribution of LAM routes redistribute mobile  
 ! This is the metric that the redistributed routes take  
 default-metric 80 70 60 70 100  
!  
line con 0  
!  
line aux 0  
line vty 0 4  
 password cisco  
!  
end
```

### LAM with Security

In the configuration of this router, certain hosts are disallowed from using the LAM feature. This can be done by adding an access list to the interface command, which disallows the learning of foreign ARPs.

```
!  
version 11.2  
!  
hostname LAMer  
!  
enable password disco  
!
```

```

interface Ethernet 0
 ip address 172.16.17.1 255.255.255.0
 ! The addition of the access-group on the end allows
 the use of this list in determining whether to add
 LAM routes to the router
 ip mobile arp timers 120 600 access-group 2
 !
interface Ethernet 1
 ip address 172.16.18.1 255.255.255.0
 ip mobile arp timers 120 600 access-group 2
 !
interface Serial 0
 ip address 131.108.12.4 255.255.255.0
 !
router eigrp 1
 network 131.108.0.0

 redistribute mobile
 default-metric 80 70 60 70 100
 !
 ! This access list is used when listening for foreign
 ARP entries on the appropriate interfaces
 access-list 2 deny 172.16.5.0 0.0.0.255
 access-list 2 deny 172.16.12.16 0.0.0.0
 access-list 2 permit 172.16.0.0 0.0.255.255
 !
 line con 0
 !
 line aux 0
 line vty 0 4
 password disco
 !
 end

```



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

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

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

**Asia Pacific Headquarters**  
 Cisco Systems, Inc.  
 Capital Tower  
 168 Robinson Road  
 #22-01 to #29-01  
 Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
 Tel: +65 6317 7777  
 Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the  
**Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. CCIP, CCSP, the Cisco Arrow logo, the Cisco *Powered* Network mark, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, MGX, MICA, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, Stratm, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.  
 (0304R) ETMG 203031—SH 08/03