Analysis of Layer 2 and 3 Hand off Techniques for Train Based Mobile Networks When Used With VoIP Enabled Client Devices

by

Doug Doran

A project submitted for

MINT 709

University of Alberta

2006

First Reader: **Dr. Mike MacGregor**
Second Reader: **Dr. Bob Davies**

ABSTRACT

Mobile device technology is developing at an extremely rapid pace. With the developments in the 3GPP Generic Access Network (GAN) technologies cell phones will soon transition seamlessly from cell networks to Wi-Fi networks in hot spots and residences. Currently work is progressing rapidly with various cell phone manufacturers releasing products that have this capability. With this capability and the implementation of wireless hot spots on mobile platforms such as planes, trains, and ships an area of research has become apparent in examining the uplink handoff processes for these mobile networks that will allow for voice quality communication from the mobile network. This paper's ultimate focus will deal specifically with roaming systems able to support voice traffic on the mobile network of a passenger train.

Two areas of the mobile network uplink are particularly apparent in their impact on voice traffic. The round trip delay for some currently used uplink systems is too long for acceptable voice traffic. As a result this paper will focus on an uplink system that can avoid this uplink delay. Proprietary implementations based on the 802.16e standard are already beginning to be used for terrestrial mobile network uplinks. The other significant issue that affects voice traffic is the delays incurred when the mobile network changes its connection point to the terrestrial network. This roaming process can introduce unacceptable pauses in voice communication while the connection transitions.

One system that allows for mobile network roaming and that will be examined is Mobile IP. Due to the lack of a current 802.16e simulator a current proprietary 802.11 implementation of Mobile IP will be examined to illustrate its limitations in supporting voice traffic. Tests will be done using Cisco's Proxy Mobile IP implementation.

Various components of the 802.16e standard will be discussed and appropriate components selected that should optimize the performance of a system specifically designed for train uplinks. An analysis based on the handoff delay will be performed to determine which features provide optimum performance during a handoff.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

GLOSSARYTRIED TO MAKE ALL OF THESE COMPLETE SENTENCES

802.11R The 802.11R standard is designed to reduce the handoff delay for devices moving within an 802.11 network. While this is an important function in Wi-Fi networks it is probably not going to be used much for mobile network uplinks because 802.11 standard is not likely to be the best uplink technology.[4]

802.20 This proposed standard will be designed to support global roaming including vehicle mobility. The 802.20 working group is currently suspended pending an investigation into possible inappropriate influence in the working group.

Access Point An access point is a wireless device in a local area wireless network that both receives and transmits. It allows for communication between other nodes on the network and often provides wireless clients with access to the wired network.

Access Service Network In 802.16 an ASN is composed of one or more ASN gateways and associated base stations. The ASN can also host a Mobile IP Foreign Agent.

Authoritative Access Point **An authoritative access point** keeps a subnet map to record the home agents for all foreign mobile systems.[5]

Base Station A base station performs a role very similar to that of an access point except instead of being in a local area network it is in a wireless MAN.

Bi-casting This is a process where a serving BS sends copies of MAC frames to potential target BSs so that when a HO occurs delays are minimized.

Connectivity Server Network The CSN provides services such as the AAA server, Mobile IP Home agents, and coordinates mobility between ASN's.

EDGE Enhanced Data Rates for GSM Evolution is, as the name implies, a standard for increasing the data speed of GPRS in GSM networks.

EVDO 1xEV-DO is a standard used with CDMA cell phones and stands for 1x Evolution-Data Optimized. It was standardized in the "cdma2000 High Rate Packet Air Interface Specification." This system allows data through put considerably higher than GSM in the range of 2.5Mbps to 3.1 Mbps.

Fast BS Switching (FBSS) Similar to SHO a MSS is registered with several BSs at the same time. The MS transmits and receives data from one primary serving BS at a time.

Fat AP This is an access point that has a considerable amount of built in functionality. These APs will likely be replaced over time in enterprise implementations with thin APs due to security and QOS issues.

GPRS General Packet Radio Service is a data service available to users of GSM based cell phones and compatible devices.

GSM Global System for Mobile Communications is a standard used in much of the world for cell phones.

GSM-R **This is** wireless communication for networks on railways. This standard was adopted as a standardized railway standard across the European Community and is being implemented in many EC countries. It operates in the 876 – 880 MHz and 921 – 925 MHz bands. Towers are located every 3 – 4 km. Performance is maintained at speeds of up to 500 km/h.

HSDPA High-Speed Downlink Packet Access called 3.5G is linked to the WCDMA standard and is used for data access on cell phone networks.

Leaky Coaxial Cable This is a coaxial cable with a slotted or grooved outer surface that can be used as an antenna. These have been run along railway lines to provide the train access to a ground based data network.

Macro Mobility This term is used to describe roaming that crosses a layer 3 boundary and as a result a new IP address is required.

Micro Mobility This term is used to describe roaming from one access point to another that does not cross a network or layer 3 boundary.

Proxy Mobile IP This system allows mobile devices that do not have a mobile IP client to still roam and be represented on the network. In Cisco's implementation the APs can be set up as proxies for the mobile client and allow for the establishment of a tunnel from the AP to the FA and on to the MC's HA.

Serving BS This is the BS that is currently communicating directly with a MS. In a roaming situation it is the first BS before a roam occurs.

Session Initiation Protocol (SIP) SIP is an application layer system used for call setup and control for VoIP telephone communication over a network.

Soft Handover (SHO) In a SHO an MSS is simultaneously registered to several BSs. In this system duplicate data is transmitted by several BSs to the MSS at the same time. It is also known as a Make Before Break handoff.

Target BS This is the BS to which a MS is going to connect as it moves away from the serving BS.

Thin AP This is an access point that has minimal functionality built in and can be viewed as almost a radio.

Wi-Fi and Wi-Fi CERTIFIED These are terms developed by the alliance of companies that formed the Wi-Fi Alliance. This alliance was put in place to ensure interoperability of wireless devices that met the 802.11b standard but did not necessarily communicate with each other. The "Wi-Fi Certified" brand displayed on 802.11 products indicates that the product has met the Wi-Fi Alliance standard for interoperability and should be able to be used with other Wi-Fi certified devices.

Wi-MAX Wi-MAX is a term used to describe 802.16 broadband metropolitan area networks.

Wireless Domain Services This is a Cisco proprietary service that uses a AP to coordinate layer 2 roaming handoffs using a system called Fast Secure Roaming.

ABREVIATIONS AND ACRONYMS

AAA	Authentication, Authorization, and Accounting
AAP	Authoritative Access Point
AP	Access Point
ASN	Access Service Network
BS	Base Station
BWA	Broadband Wireless Access
CSN	Connectivity Service Network
DL	Down Link
EDGE	Enhanced Data Rates for GSM Evolution
eMLPP	Multi-Level Precedence and Pre-emption
ERTMS	European Railway Traffic Management System
EVDO	1x Evolution-Data Optimized
FSR	Cisco Fast Secure Roaming
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HO	Handover or Handoff – used interchangeably in this paper
HSDPA	High-Speed Downlink Packet Access
MC	Mobile Client
MDHO	Macro Diversity Handover
MIMO	Multiple Input Multiple Output
MIP	Mobile IP
MS	Mobile Station – same as MSS in this paper
MSS	Mobile Subscriber Station
OSI	Open System Interconnect Model
Phy	Physical Layer
PMIP	Proxy Mobile IP
PUSC	Partial Usage of Sub-Channels
SIP	Session Initiation Protocol (SIP)
SSID	Service Set Identifier
UIC	International Union of Railways
UL	Up link
VoIP	Voice over IP
WDS	Wireless Domain Services
WLCCP	Wireless LAN Context Control Protocol

INTRODUCTION

Device mobility is a rapidly evolving field and as such it is composed of a wide assortment of deferring standards that attempt mobility from various points of view. This diversity of technology and systems has been caused by many factors.

These include:

-convergence of separate technology fields. Cell phone systems are converging with wireless networking devices as both system struggle to add features from the other environment in a manner that works with their existing technology. Cell phones and cell providers are adding more data features and incorporating IP technology. Networking companies are incorporating features that allow for voice technologies to use both wired and wireless networks and achieve the quality of service required for voice and video. Even within the networking realm there are competing technologies that are tackling the same problem.

-competing technologies from various vendors in the cellular arena. As the field is international in scope competing technologies produced in different global regions compete for new market share in areas where they overlap or want to spread.

These combined technology and geographic convergences have produced a technology dog's breakfast of competing standards and technologies and allow for a multitude of permutations and combinations of technology. All of these technologies and their various promoters are all competing to achieve the goal of providing voice and data services to mobile devices with the best quality of service possible.

The application of these converging and diverse technologies to mobile train-based networks is one that could produce a wide variety of possible outcomes. As an example of the scope of this area these are some of the standards that overlap to some degree in this area. 802.11a,b,g,n,e,r,u, 802.16 (WiMAX), 802.21, 3g, cdma, w-cdma, cdma2000, umts, edge, GAN/UMA, TD-SCDMA, FLASH-OFDM, 1xev-do. Some of these technologies are used in cell phone voice services, some are use for data, but the solution that should ultimately be most widely applied for these uplinks will be a data service with high quality of service characteristics.

In data networks, Network layers have been defined and are used to isolate engineering tasks. The International Standard Organization's Open System Interconnect model is composed of seven layers as shown in the figure below. This paper will focus on interactions that occur at layer 2 and layer 3 of the OSI model. In comparison to typical local area network devices layer 2 devices include switches and generally deal with a devices Media Access Control or MAC address while layer 3 devices include routers and deal with devices IP addresses. In this

paper layer 3 roaming occurs when a device moves from one IP subnet into another IP subnet. This will either require a new IP address or an implementation of Mobile IP for further communication to the mobile device. In a layer 2 roam the IP address can remain constant but the network devices must be aware of the change of the connection point as it relates to the relocation of a devices MAC address from one connection point to another.

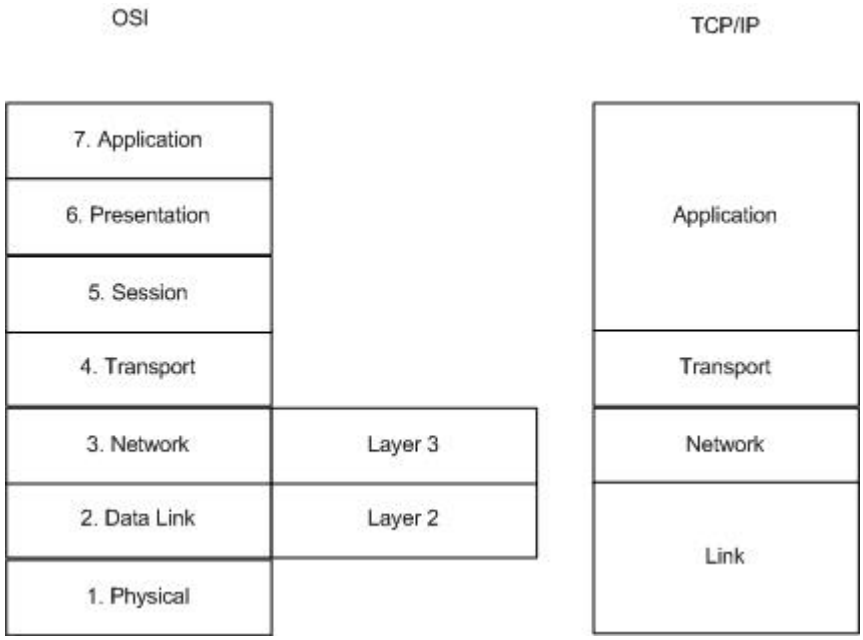

Figure 1 OSI and TCP/IP Layers

In comparison to data networks many of the cellular technologies have well developed methods for layer 2 and layer 3 roaming. The primarily data-centric technologies have in the past not been nearly as good at roaming. The two main methods of dealing with layer 3 mobility of wireless devices have been Mobile IP and SIP. Mobile IP allows a mobile device to move to different subnet without changing IP addresses but maintain connectivity as if the device were still connected to its home network. SIP is an application layer protocol that attempts to work independently of the lower layer protocols. Both of these methods approach the problem of IP mobility from very different points of view.

In this paper layer 2 and layer 3 roaming as it has been implemented in 802.11 implementation will be examined and then the focus will narrow to the layer 2 roaming technologies that can be optimized in the new mobile WiMAX standard 802.16e.

MOBILE IP

The Mobile-IP (MIP) protocol was originally specified by RFC2002[1] in 1996 and subsequently updated to its current version RFC 3344[2]. While Mobile-IP is successful in providing roaming capabilities to mobile data devices there are questions as to how well suited it is for the emerging demands of VoIP in wireless networks.

Mobile-IP specifies that a given device will have the same IP address regardless of its current location. This is accomplished by having a home agent and a foreign agent as shown in Figure 2. The home agent is responsible for keeping track of the mobile device's home address and also allows a "care of" address to be registered for the device by a foreign agent. When the mobile node moves out of range of the home agent and into range of the foreign agent the mobile node will register with the foreign agent who then notifies the home agent of the mobile nodes "care of" address. Then when a remote client attempts to contact the mobile node at its home address the home agent will create a tunnel to the foreign agent and send the data. The foreign agent then uses the data-link address of the mobile node to send the data to the mobile node. The mobile node will then send its response directly to the remote client.

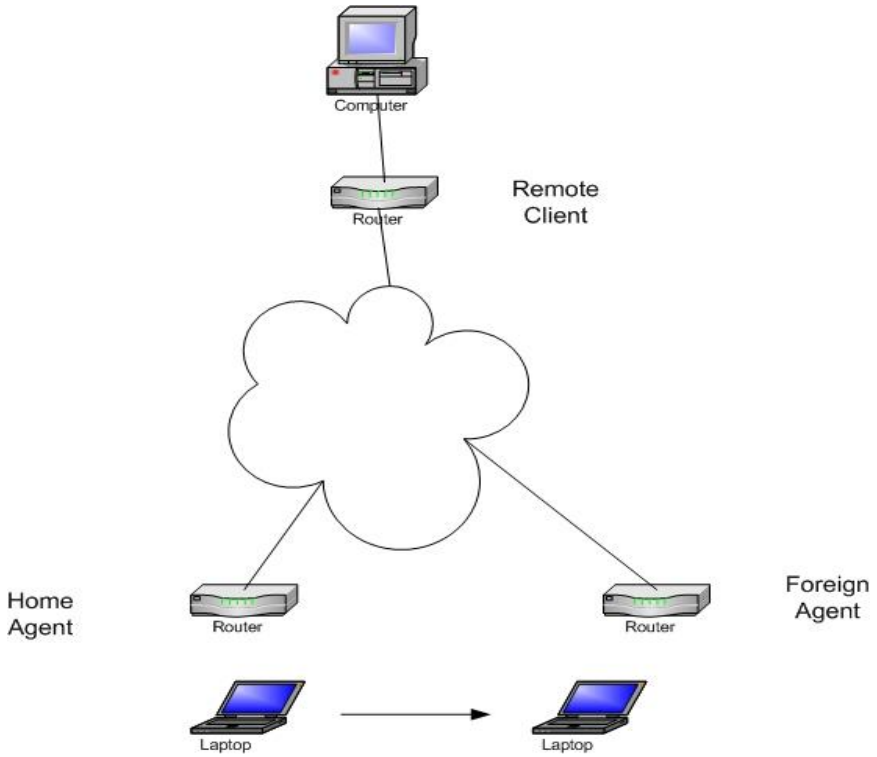

Figure 2. Simple Mobile IP

The situation can become much more complex however when the network to which the mobile node connects is its self mobile, such as on a train or an aircraft. This could result in nested tunnels as in Figure 3 and 4.

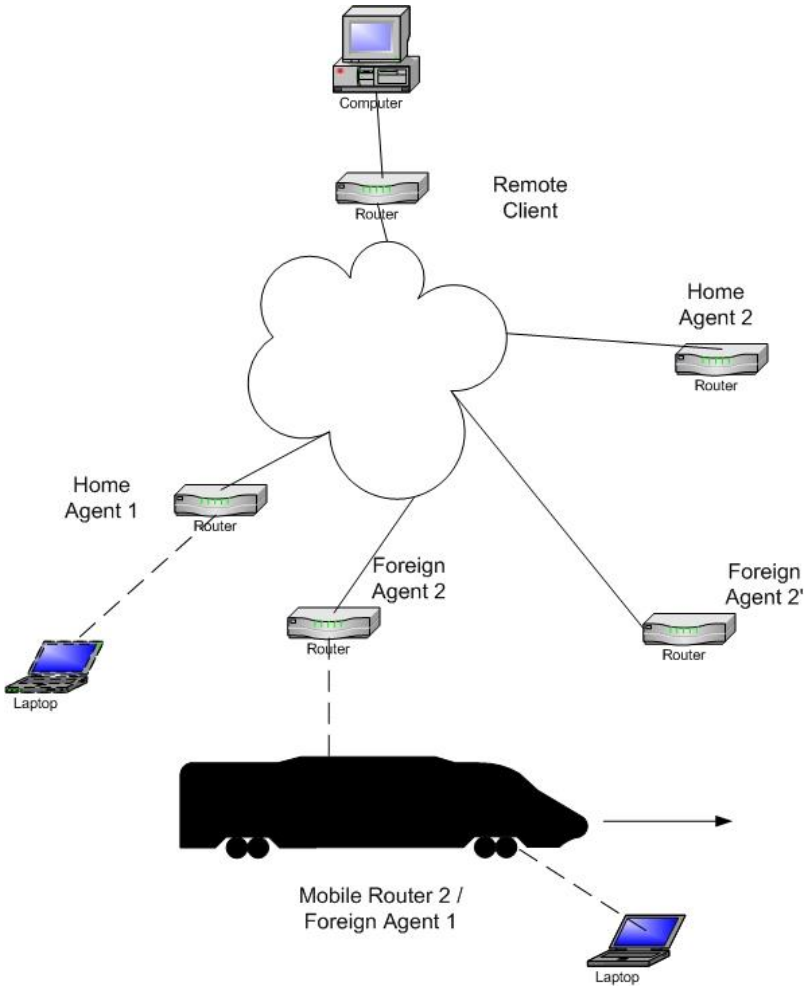

Figure 3. Nested Mobile IP

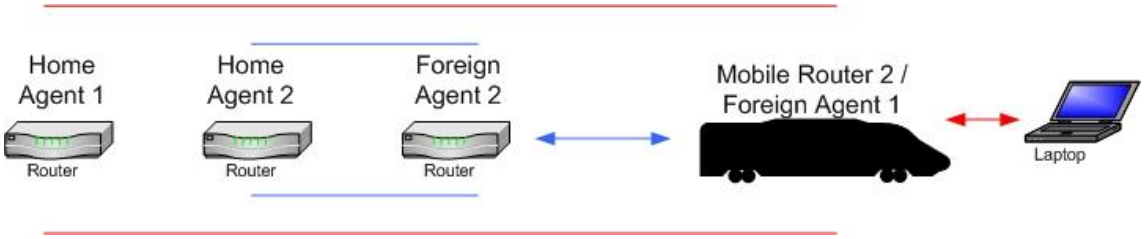

Figure 4 Nested Tunnels

In Figure 3 the mobile device (laptop) has a home address in the network shared with Home Agent 1. When the device is connected to the train's network the train's router acts as the foreign agent for the laptop. Since the train is mobile however this mobile router is itself behaving as a mobile node and has a Home Agent (Home Agent 2) and connects to various foreign agents (Foreign Agent 2 and Foreign Agent 2') as it moves.
The laptop has registered with Foreign Agent 1. Foreign Agent 1 is also Mobile Router 2 and is currently registered with Foreign Agent 2. Foreign Agent 2 is recognized by Home Agent 2. Home Agent 2 has registered itself as the Foreign Agent with Home Agent 1.

Micro Mobility will be discussed here as being a layer 2 roam. In a LAN for instance unplugging a device from a switch and plugging it into a different switch is a layer 2 roam so long as the switches are in the same IP subnet.. The new switch must update its CAM table so that it is sending the data for the mobile device to the correct port but the mobile devices IP address stays the same.

Macro Mobility will be discussed as a layer 3 roam. This could be compared to a device moving from one router to another. Generally the device would need a new IP address in the new IP subnet. Mobile IP (MIP) however can allow the device to keep the same IP address but the connected network then tunnels the data to the devices home network.

While proprietary implementations and the upcoming 802.11R standard allow 802.11 devices to roam there are many issues that will limit the use of 802.11 technologies for train based uplinks. However given the current development state of 802.16e this paper will examine some typical 802.11 roaming issues that will help highlight 802.16e issues that need to be considered. Since this paper is dealing specifically with the uplink from the train an experiment is performed to measure the types of delay that MIP introduces in traffic using Cisco's proprietary Proxy Mobile IP (PMIP) implementation[5] in access points (APs) in combination with a standards-based MIP implemented on Cisco routers. In order to separate the delay induced by Mobile IP as opposed to the delay associated with simple layer 2 roaming between access points two sets of trials are performed. The first set of trials will illustrate delays incurred with micro mobility as a connection moves from one access point to another using both a standard 802.11g setup as well as a proprietary Cisco's Fast Secure Roaming (FSR) setup. The second set of trials will illustrate delays associated with macro mobility when MIP and PMIP are used.

Overview

In the micro mobility trial a steady stream of data traffic is generated by a packet generator on the mobile station. This stream of traffic is targeted at a Cisco switch whose only function is to reply to these pings. The Fluke Optiview can view these packets as they are being delivered and will measure traffic characteristics. The inter-frame arrival time will be looked at over many trials to establish a baseline handoff time for the layer 2 roaming that is occurring in this trial. Two types of roaming will be tested. The first is a standard 802.11g roam, the next type is a proprietary Cisco implementation called Fast Secure Roaming (FSR).

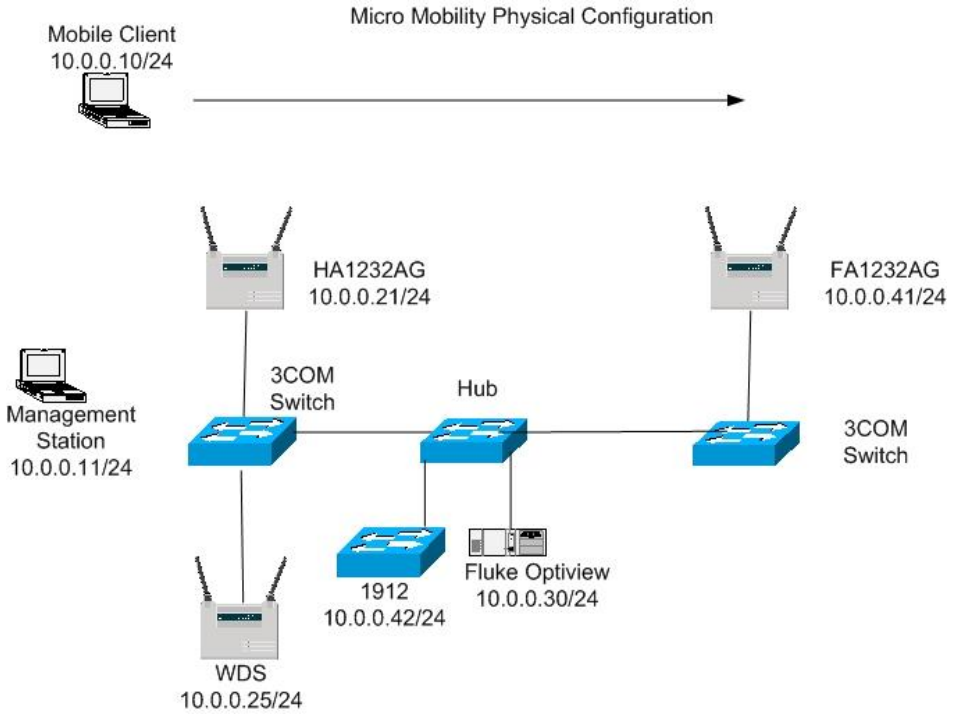

Figure 5. Micro Mobility test configuration

Device	IP	MAC
HA1232AG	10.0.0.21/24	0014.6a40.4513
WDS	10.0.0.25/24	0013.c493.ab6a
FA1232AG	10.0.0.41/24	0014.6a40.44f4
MC	10.0.0.10/24	0040.96a9.c13e
Management Stn.	10.0.0.11/24	000e.358b.435b
1912	10.0.0.42/24	0004.9af5.ca46
Optiview	10.0.0.30/24	00c0.17a1.0c13

Table 1. Micro Mobility Tests Device IP and MAC addresses

Standards-based implementations of 802.11G have the ability to roam between APs that share the same SSID. These roams however tend not to be pretty and as a result proprietary systems have been developed that allow for faster roaming. 802.11R is also designed to improve the mobility of 802.11 based devices but no current implementation of this is available.

Cisco access points running IOS version 12.2 and higher can be configured to use Cisco's Fast Secure Roaming (FSR) to improve the layer 2 roaming speed especially in secure 802.1x environments. In this test the security systems were disabled and both access points had open authentication with no encryption to help eliminate complexity that might obscure the actual roaming HO time. Fast Secure Roaming however does provide "improved 802.11 channel scanning during physical roaming".[6]

This improvement in roaming speed depends on the client providing information to the new AP regarding its previous AP connection. The actual roaming process and trigger events are controlled by the client so significant variability can be found in roaming ability depending on the client used or the settings used on a client. Tests were performed using an onboard Intel 2200BG and the Intel Proset client software and a Cisco C21AG a/b/g card with the Cisco Aironet client utility.

Initially it was planned to use a packet generator and either craft or copy a typical voice packet for testing process. The test was limited to a Windows-based packet generator for the test due to Wireless client issues related to fast secure roaming. The only Windows-based packet generators that were found required that the client utility be disabled and thereby disabled the FSR capability. Upon re-evaluation it was concluded that the handoff delay would not be affected by the type of packet used anyway so a continuous ping was used instead. Since the windows ping utility can not fire icmp packets very quickly a small

program called Fping[7] that is able to send pings at configurable time intervals was used. Both the time interval between packets and the wait before retransmission are configurable using this program so it provided a good packet source.

In order to encourage roaming the power output on both APs was set to 1mw (-1dbm) for both CCK and OFDM. Client power settings on both APs was also set to 1mw.

In addition, it waas found that even with such low settings in a straight line hallway situation roaming would not occur until the MC was significantly past the other AP. To encourage faster roaming one AP was placed around a corner from the other AP. This significantly reduced the amount of work required to make an individual roam. The roam trigger is not based on seeing a better power setting and then roaming, it is triggered by either a loss of connection or poor throughput. This roam type is also Break before Make so the client will not roam to a new AP until it has broken the initial connection.

The command syntax for packet generation on the mobile client was fping 10.0.0.42 –c –t 20 –w 20. This produces a constant stream of echo requests at 20ms intervals. This provided sufficient traffic to gauge the magnitude of the handoff delay with a 20ms base unit. 10 ms timing for the wait interval was initially used but it was found that a significant number of echo reply packets did not make it back in time.

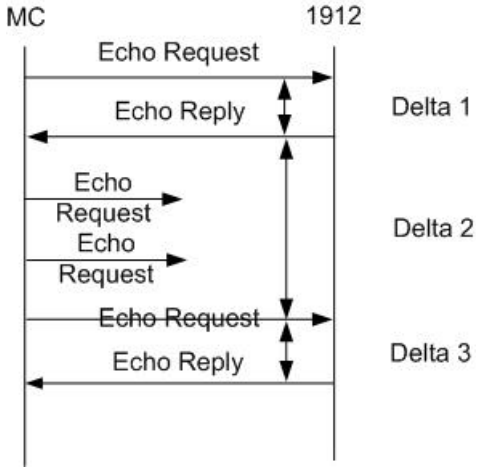

Figure 6. Fping Delta

The figure above indicates what the delta time's represent. Note that the deltas between the echo request and echo reply are captured before they are sent wirelessly and as a result are expected to be very consistent. See test 1 below.

Initially the Optiview had been used as the ping receptor but it was found that under test load the Optiview did not perform consistently depending on what other tasks it was performing.

As a result a Cisco 1900 switch (1912) was added into the network and given an IP address to act as the echo source for the tests.

One of the great dilemmas in testing these processes is how changing versions of the Cisco IOS affect implementations of various technologies. During the experimental set at several stages it was found that the specific implementation that was required to perform testing was either not available yet on certain IOS versions or had been discontinued on newer IOS version. As a result different equipment had to be used between the Micro and Macro roaming tests.

Test 1 Standard Configuration baseline with no FSR

These tests were performed with an Intel 2200BG internal card.
To establish a delay baseline this test was performed with only one AP active. This allowed examination of the range in deltas that could be expected with only one AP present. The MC physically moved during this test and took the connection to its limit and then back.

Two histograms were created below showing the deltas when the source was the MC and then when the source was the 1912. The histograms show as expected no variability in the 1912 ->MC deltas and they therefore will not be analyzed for the remaining tests.

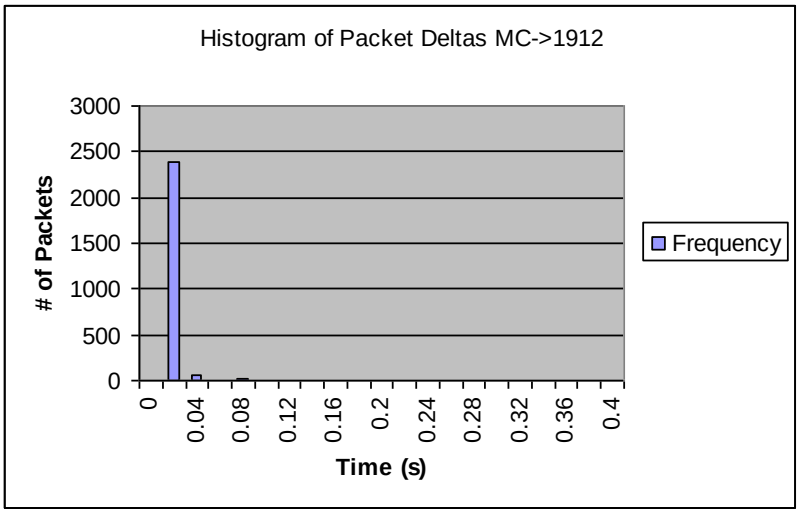

Figure 7. Packet Deltas Baseline Histogram MC ->1912

It should be noted that the above graph was truncated for visual purposes. 3 packets had values in the 1.5 s area when connectivity was temporarily lost at the extreme end of the coverage range. Also important to note here that with the 20 ms packet retransmission and

20 ms wait times this result would support that the FPing timing is fairly accurate. Test 7 examines this further.

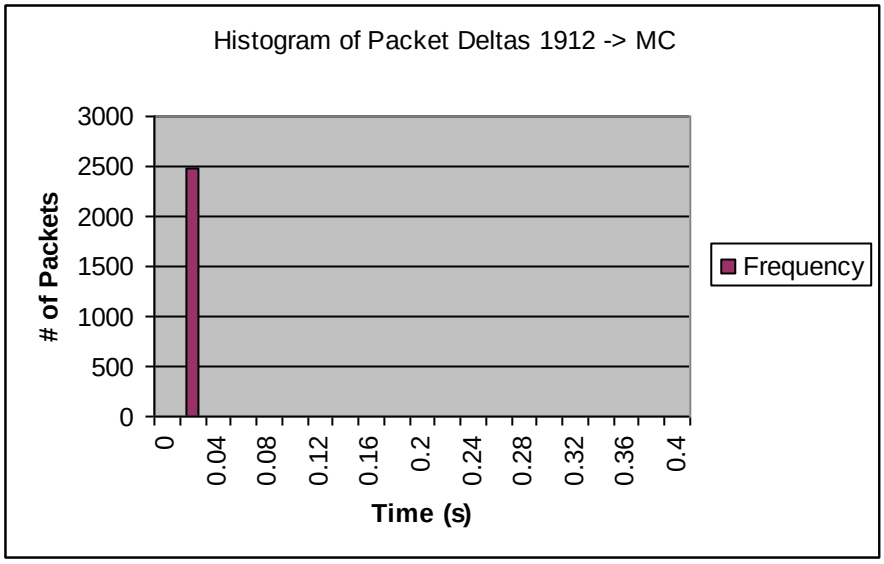

Figure 8. Packet Deltas Histogram 1912 -> MC

Test 2 Standard Configuration No FSR

These tests were performed using the internal Intel 2200BG card.
This is a roam and back test and is designed to limit the volume of captured data in order to make it easier to isolate key parts of the roam process when looking at the captured packets. Fping was not used for this test.

In examining the data traffic it included management traffic for the optiview, CDP, Cisco multicast traffic, and spanning tree traffic. No inter-AP traffic was captured. This is significant for comparison purposes when compared with test 5 with FSR wired traffic.

Test 3 Standard Configuration No FSR

These tests were performed using the internal Intel 2200BG card.

This test is composed of a series of 5 roam and back cycles to provide significant data to look at. Fping is running with –t 20 and –w 20 and the MC simply moves back and forth from one AP to the other.

During the 5 cycles there will be a total of 10 roams. By filtering, sorting and manual examination of packet captures it is possible to identify packets that should correspond to the time periods when the roams occurred. Table 2 shows several candidate roam packets. It is

important to note that this measure is not the same as a HO time as it reflects only the time between the last echo reply and the next echo request.

One unexpected result was a surprising number of very small deltas. 0.6 % of the packets had deltas of less than 10 ms. This will be caused by the short wait for retransmission interval. If it takes more than 20ms for the echo reply to reach the MC it will send another request. Given that, then it is possible for the request and reply to get out of sync and give some results that are very low. Since the primary concern in these trials was to determine the maximum deltas the affect on the test should be minimal and has been ignored.

It is difficult to identify exactly all the deltas that represent a roam event but in the 5 roam cycle there is a significant jump from a large grouping of packets that declines up to 0.25 s then 6 packets in the 1.6 second region. These 6 upper limit packets will have been roam events.

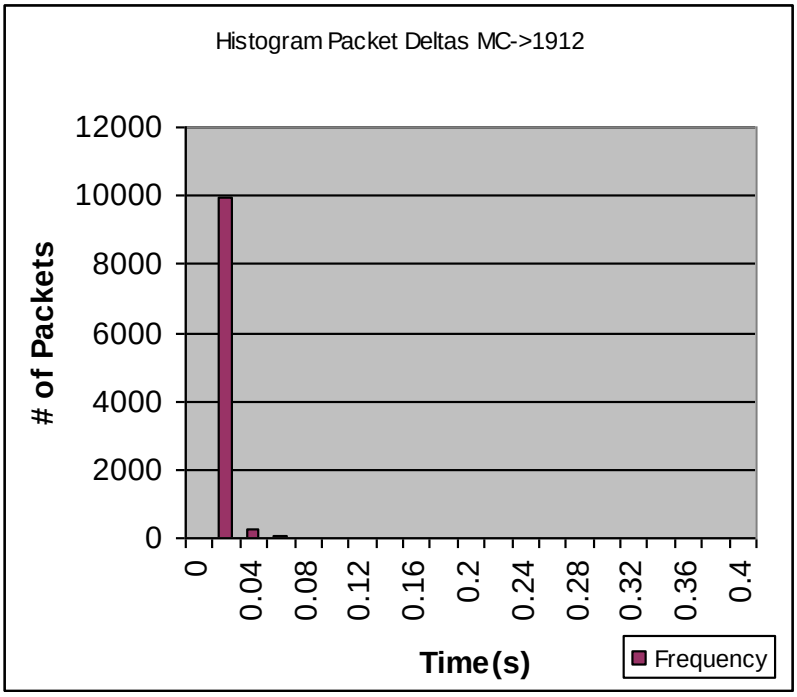

Figure 9. Histogram Packet Deltas MC->1912

No.	Time	Source	Destination	Protocol	Delta
15721	168.7237	10.0.0.10	10.0.0.42	ICMP	0.231918
1433	14.775	10.0.0.10	10.0.0.42	ICMP	0.236352
4403	46.37072	10.0.0.10	10.0.0.42	ICMP	1.621075
5309	57.13491	10.0.0.10	10.0.0.42	ICMP	1.633803
5727	63.32738	10.0.0.10	10.0.0.42	ICMP	1.609888
12769	136.4866	10.0.0.10	10.0.0.42	ICMP	1.631556
14323	153.706	10.0.0.10	10.0.0.42	ICMP	1.609696
15797	171.3455	10.0.0.10	10.0.0.42	ICMP	1.615962

Table 2. Identification of Roam Packets No FSR.

Test 4 No FSR

This test is to analyze wired traffic between the APs. This data will be used to look at roaming management traffic that is generated by the APs. It should also allow for an analysis of the FSR traffic system.

In this test no wired traffic between the APs was noted during roam. Only normal Cisco discovery protocol (CDP) traffic was captured.

For tests 5 through 7 a Wireless Domain Services (WDS) AP is added to the network so that the APs will support Cisco's Fast Secure Roaming. For these tests LEAP is used to authenticate the APs on the network while the client access remains open.
A Radius server is also required to implement this system but the Cisco 1130 that is used as the WDS AP has an on board Radius server that is used for this function. Please refer to the Appendix for all AP configuration files.

Test 5 WDS added FSR Active

These tests were performed with both the Intel 2200BG and a Cisco C21AG card.

I captured the wired and wireless packets to AP FA1232AG for one roam cycle. Figure 10 illustrates the traffic back and forth between FA1232AG and the WDS. It illustrates a series of four UDP packets (in blue) that are generated during each roam event.

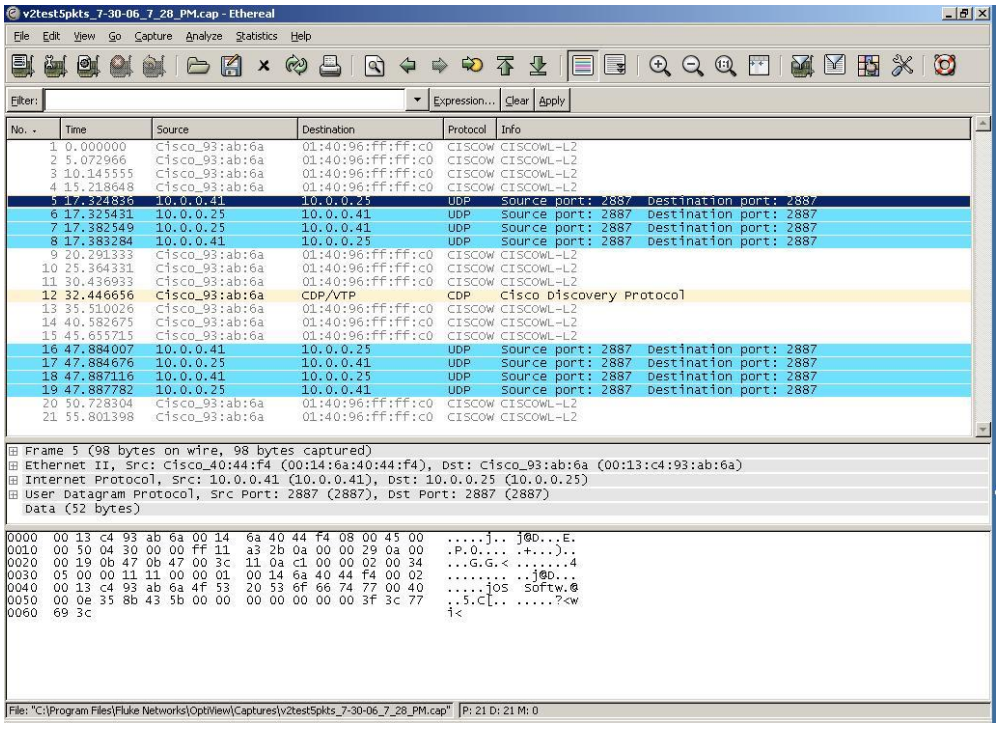

Figure 10. Wired traffic from AP to WDS

Figure 11 below shows a wireless association process with FSR enabled. Packets 582 through 590 show this in process. This traffic was captured using a second laptop running CommView. CommView is a packet sniffing application for wireless analysis.

Unfortunately due to equipment availability it was not possible to capture the wireless packets associated with the roam with the Cisco 21AG card. It may have produced some different wireless traffic to show the FSR implementation as it relates to the client.

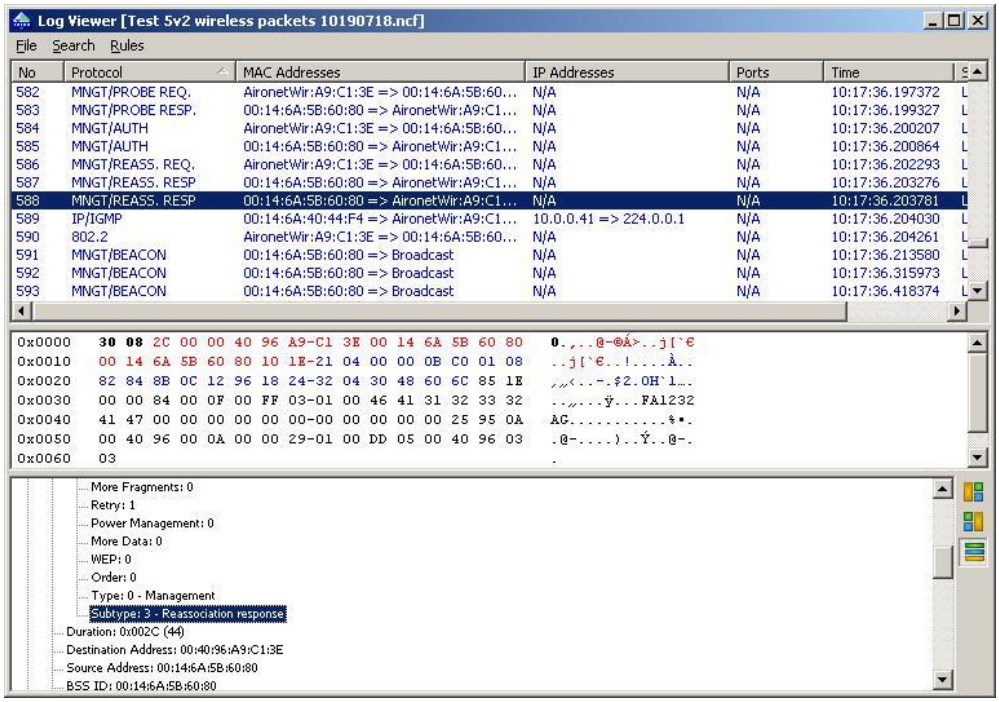

Figure 11. Wireless Packets for FSR roam

Test 6 Bulk Test of 5 roaming cycles using FSR

Packets generated by ICT108708 and captured on Optiview through hub.

Part A: Tests performed using Intel 2200BG internal card.

No.	Time	Source	Destination	Protocol	Delta
12443	132.9822	10.0.0.10	10.0.0.42	ICMP	0.191449
1191	12.86866	10.0.0.10	10.0.0.42	ICMP	0.305042
3953	43.07198	10.0.0.10	10.0.0.42	ICMP	0.377136
16527	178.5256	10.0.0.10	10.0.0.42	ICMP	0.555193
15047	160.9003	10.0.0.10	10.0.0.42	ICMP	1.590458
16525	177.9648	10.0.0.10	10.0.0.42	ICMP	1.601819
8029	87.79599	10.0.0.10	10.0.0.42	ICMP	1.615652
1737	20.25966	10.0.0.10	10.0.0.42	ICMP	1.63939
3995	45.33549	10.0.0.10	10.0.0.42	ICMP	1.672075
18107	196.6617	10.0.0.10	10.0.0.42	ICMP	1.713243

Table 3. Identification of Roam Packets FSR 2200BG

Several interesting issues arise from these packets. Why are there 6 packets when five roams should produce 10? Both the Non-FSR and FSR roams have produced 6 packets with values in this range. The fact that the roam times have not increased would seem to indicate that while the UDP traffic generated by the roam events indicates that fast secure roaming is in place it is highly likely that the Intel client is not able to support FSR features in practice. The client plays a very significant role in FSR and if it does not provide the necessary information to the AP then FSR probably does not occur.

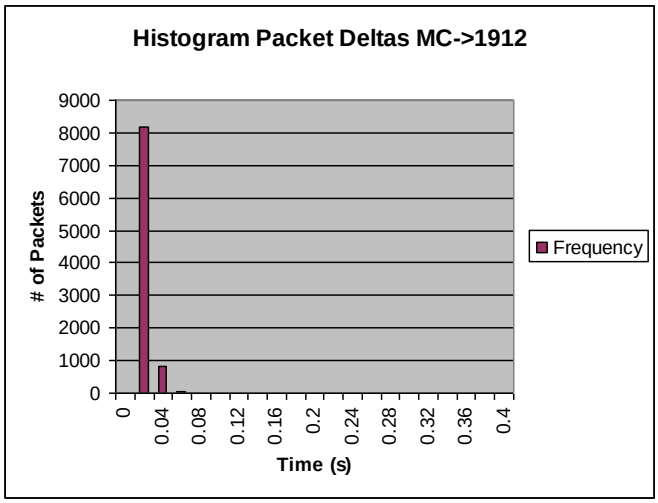

Figure 12. Histogram Packet Deltas MC->1912 with FSR Cisco ABG Card

Part B: This test was performed using a Cisco C21AG card.

The results in table 4 illustrate the same test performed using a Cisco card with the Cisco client utility program. This client should definitely support FSR. The results indicate some improvement in the roam time although not to the level expected.

In the roam with the Cisco ABG card in Table 4 only two packets are in the 1.6 s range. This may be expected as with FSR the APs learn of neighboring APs from the client so the first roam on each would be expected to take longer. Also interesting to note here is that 10 packets have been identified as being significantly higher than the rest. This is as expected. It is noted that FSR roaming, while significantly faster than the 1.6 second range measured without it, is still well above acceptable levels for real time traffic.

No.	Time	Source	Destination	Protocol	Delta
13877	144.9432	10.0.0.10	10.0.0.42	ICMP	0.090851
1573	16.35386	10.0.0.10	10.0.0.42	ICMP	0.112294
8937	92.40689	10.0.0.10	10.0.0.42	ICMP	0.168515
17129	181.4099	10.0.0.10	10.0.0.42	ICMP	0.967031
5565	58.69304	10.0.0.10	10.0.0.42	ICMP	0.987429
7271	76.00087	10.0.0.10	10.0.0.42	ICMP	0.989755
10579	111.7605	10.0.0.10	10.0.0.42	ICMP	1.01019
12287	129.6948	10.0.0.10	10.0.0.42	ICMP	1.012741
3677	39.03529	10.0.0.10	10.0.0.42	ICMP	1.055335
13887	146.018	10.0.0.10	10.0.0.42	ICMP	1.063343
1759	19.49714	10.0.0.10	10.0.0.42	ICMP	1.074655
9051	95.25601	10.0.0.10	10.0.0.42	ICMP	1.608721
15601	164.6945	10.0.0.10	10.0.0.42	ICMP	1.617922

Table 4. Identification of Roam Packets FSR with C21AG.

Test 7 FPING baseline

To establish the accuracy of the FPING timing as compared to the Optiview's arrival time echo requests were sent directly to the Optiview. 5000 packets were captured from MC through FA1232AG to Optiview. The MC was not moved during this test and both the retransmission and wait time were set to 20ms.

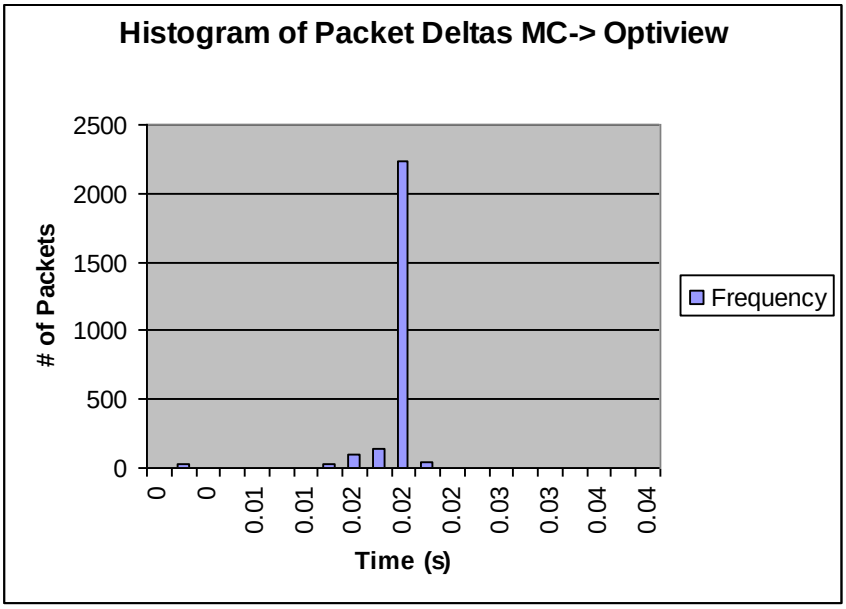

Figure 13. Histogram Fping Test

The large number of packets in the 0.020 s time period would again support the Fping timing accuracy.

MACRO MOBILITY TESTING USING MOBILE IP, PROXY MOBILE IP AND 802.11B

Overview

In the macro mobility trial a steady stream of ping traffic is used as in the previous micro mobility tests. This stream of traffic is targeted at the Cisco 1900 switch. The inter-frame arrival time will be looked at to establish a baseline handoff time for the combined layer 2 / layer 3 roaming that is occurring in this trial. It is to be expected that the layer 2 roams in this test have a higher latency than in the micro mobility tests as the SSIDs between the APs are different in these tests. This was done deliberately as it would be unlikely that a macro roam would occur if the SSID stays the same. It does however increase the time it takes for the client to scan for and attach to another AP.

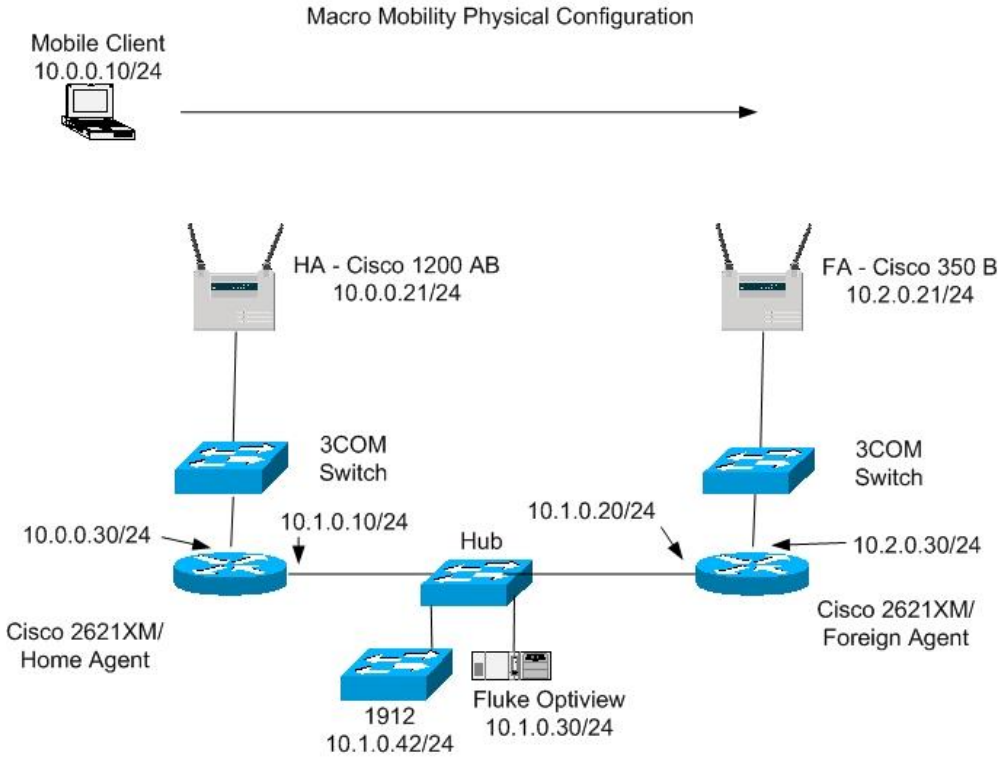

Figure 14. Macro Mobility Test Configuration

Device	IP	MAC
HA FA 0	10.0.0.21/24	000c.ce8a.3ee5
HA RA 802.11B	10.0.0.21/24	000c.8544.7b96
FA FA 0	10.2.0.21/24	0040.9658.a0d9
FA RA 802.11B	10.2.0.21/24	0008.2131.66b4
MC	10.0.0.10/24	0040.96a9.c13e
MS	10.0.0.11/24	000e.358b.435b
1912	10.0.0.42/24	0004.9af5.ca40
Optiview	10.0.0.30/24	00c0.17a1.0c13
Home Agent fa0/0	10.0.0.30/24	0004.c178.58a0
Home Agent fa0/1	10.1.0.10/24	0004.c178.58a1
Foreign Agent fa0/0	10.2.0.30/24	0006.28a9.d120
Foreign Agent fa0/1	10.1.0.20/24	0006.28a9.d121

Table 5. Macro Mobility Tests Device IP and MAC addresses

Procedure

It took much longer than expected to get the complete Mobile IP system and the Proxy Mobile IP to work together nicely even though all the devices were Cisco. Various versions of Mobile IP depending on the IOS combined with the removal of Proxy Mobile IP from newer Cisco APs resulted in a real quagmire of conflicting setting and IOS versions given the various networking devices which were available. Eventually the IOS was downgraded on the APs and even then it took a considerable amount of time to get the devices configured and working properly. Several points of interest were observed during the testing.

The tunnel registration period prevented the roaming back of the MC once it had roamed. The IP mobile registration was set to its minimum settings from the default setting of 10 hours so that the MC could roam back and forth. Otherwise once the tunnel was formed even if the MC associated on the home agent's network it could not connect at layer 3. This minimum registration time leads to a natural delay in the reconnection process and it also produces a significant amount of traffic to reregister the mobile node every few seconds.

Layer 2 roaming also took longer as the APs were no longer on the same SSID. This was done deliberately as it is a likely roaming scenario when dealing with layer3 roams.

It would be interesting to do a further comparison of allowing DHCP and SIP and comparing this speed to this mobile IP implementation.

For the macro mobility tests Cisco Proxy Mobile IP was used. Proxy Mobile IP is designed for situations where the mobile device does not have its own Mobile IP client software. In this case the tests are being performed with a Windows XP laptop that does not natively support Mobile IP.

Results

The Cisco routers are configured with static routes to reduce any potential interference due to routing updates and to make the system as simple as possible.

For these tests the results provided were performed using the Cisco C21AG card and Cisco client. The Cisco client proved to be superior to the Intel client in its fast and automatic scanning ability during these tests. The Intel card seemed to often require manual intervention to produce a faster roam and as a result was not used.

If DHCP is enabled on the mobile client then media sense would need to be turned off in the systems registry.[5][9] Since the goal of this test is to ensure that the device's IP address will not change and yet connectivity will be maintained the mobile client in these tests had a static IP address implemented.

Test Macro Roaming 1

This test will capture the wired traffic generated by a Layer 3 roam event. Figure 15 shows that when a roam event occurs two packets are used for registration from the foreign agent to the home agent.

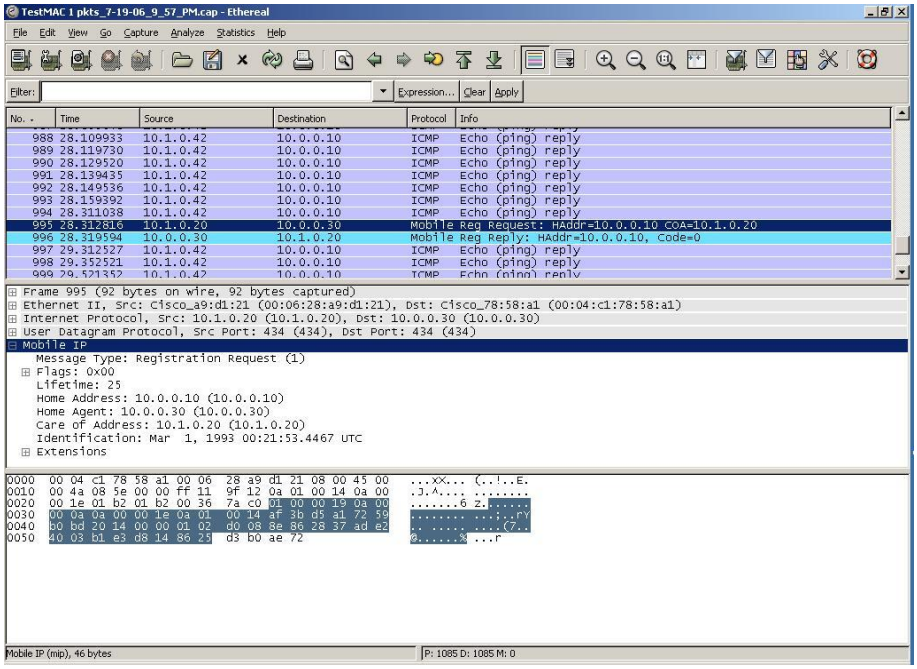

Figure 15. Mobile IP Registration Foreign Agent to Home Agent

Test Macro Roaming 2

This test captured the icmp packet deltas for a total of 5 roam cycles. Figure 16 shows a histogram of the majority of these packets.

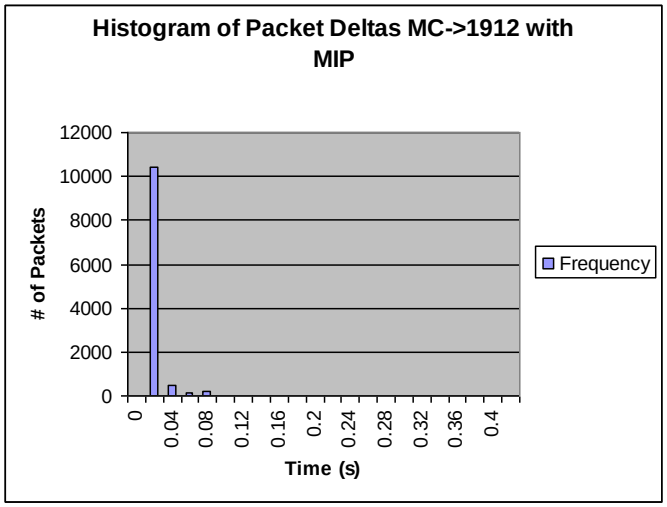

Figure 16. Histogram of Packet Deltas MC ->1912 with MIP

In the figure above it is noted that the majority of packets still have relatively low deltas even with the MIP tunnel in place for roughly half of these packets. While the MIP tunnel did introduce some latency the histogram comparison with Figure 9 shows the effect is actually fairly small. When packets that are beyond the scale of this histogram are examined however a very different story is seen.

During the handoff, due to the large amount of scanning required by the client with separate SSIDs, it was often observed that disconnects occurred followed by reconnects to the same AP. This means that there is a significantly higher number of large deltas and the scale of those high deltas is very significant. See Table 6.

No.	Time	Source	Destination	Protocol	Delta
18893	373.7995	10.0.0.10	10.1.0.42	ICMP	0.326488
6775	112.7252	10.0.0.10	10.1.0.42	ICMP	0.370325
6749	109.9778	10.0.0.10	10.1.0.42	ICMP	0.948538
10872	193.5571	10.0.0.10	10.1.0.42	ICMP	1.27793
6765	111.8715	10.0.0.10	10.1.0.42	ICMP	1.376261
14898	275.6963	10.0.0.10	10.1.0.42	ICMP	1.414232
1011	11.76685	10.0.0.10	10.1.0.42	ICMP	1.607328
1977	24.08518	10.0.0.10	10.1.0.42	ICMP	1.6177
10852	191.9476	10.0.0.10	10.1.0.42	ICMP	1.642456
18887	373.3272	10.0.0.10	10.1.0.42	ICMP	1.684941
2023	27.97213	10.0.0.10	10.1.0.42	ICMP	3.427537
14913	316.2667	10.0.0.10	10.1.0.42	ICMP	4.79955
8718	167.8798	10.0.0.10	10.1.0.42	ICMP	4.91453
16883	350.1999	10.0.0.10	10.1.0.42	ICMP	13.85648
2039	42.72156	10.0.0.10	10.1.0.42	ICMP	14.1112
10904	209.9749	10.0.0.10	10.1.0.42	ICMP	15.66834
4521	85.74264	10.0.0.10	10.1.0.42	ICMP	17.18822
6777	130.8374	10.0.0.10	10.1.0.42	ICMP	18.1085
18925	392.2512	10.0.0.10	10.1.0.42	ICMP	18.27612
12856	252.0198	10.0.0.10	10.1.0.42	ICMP	20.66192
20779	447.3685	10.0.0.10	10.1.0.42	ICMP	35.70164

Table 6. Mobile IP Roam Packet Identification

Macro Test Discussion

Just getting Mobile IP and Proxy Mobile IP working at the same time proved to be a very significant challenge with many IOS version issues along the way. The proxy mobile IP system implemented on the APs allows for the client devices to not support Mobile IP. The Proxy Mobile IP system however is no longer supported on later IOS versions. Cisco now has a MIP client that forms part of a larger proprietary solution they have moved to. It is interesting to note however that they have proposed a Proxy Mobile IP system for Cisco 802.16e devices.

802.11 Layer 2 and Layer 3 Roaming Combined Discussion

The above analysis is showing that handoff delay will be a significant problem for VoIP usage on an 802.11 wireless network. There are proprietary solutions in 802.11 that do allow for faster layer 2 roaming such as those implemented by Airespace which was recently acquired by Cisco. This solution using thin APs is a growing trend in the 802.11 area and allows for a

more centralized administrative system that spans multiple APs. This can allow for faster roaming across APs. As will be shown in the coming discussion of a specific 802.16e implementation for train based networks, these systems should have the ability to perform both layer 2 and layer 3 roaming faster than the 802.11 systems that were experimented with here. It should be noted that the experiments performed above used Fat APs and as a result do not reflect the performance that is possible with some of the proprietary systems currently on the market. They do however illustrate the problems that roaming will have to deal with to effectively handle VoIP traffic. It is also worth noting here that the upcoming 802.11R standard will significantly improve the standards based roaming capabilities of 802.11 wireless devices.

The roaming delay measured in the above experimental process will also be a very significant challenge for a train based mobile network. Several factors will affect the data uplink from a train that will make the connection challenge even more difficult.

These include:

-high velocity that high speed trains in particular will need to support. Current expectations are that 360 km/h[12][13] will be required within a few years.

-significant data throughput that would be desired to support multiple users.

-handoff delay should be as small as possible to support voice. People can detect handoff delays that exceed 40 to 70 ms.[14] The WiMAX Forum have identified that for voice traffic latency should be less than 160 ms.[20]

-to reduce initial implementation costs systems should be examined that will allow for different uplink technologies. Many different technologies are available including cell phone based data systems, evdo, leaky coaxial cable[15] but 802.16 and especially 802.16e show much promise. 802.20 may be an option in the future but it is still in the very early stages of development. It should be noted however that high vehicle speed may pose a problem for 802.16e systems.

-heterogeneous roams may be required if a train crosses an international boundary or onto a different company's tracks.

One of the technologies that is being developed currently is 802.16e or mobile WiMAX. This technology can address several of the issues that a train based mobile network will experience. Its longer range will reduce the initial deployment costs of the terrestrial network. It is designed for mobility. Currently 802.16e is designed to support a maximum speed of 120 km/h but future adaptation for higher velocities is anticipated. Mobile IP is essential for the general implementation of 802.16e and is well integrated into the standard. As a result 802.16e MIP should perform better than the 802.11 implementations experimented with in this paper. The macro roaming functionality is also in place for mobile WiMAX to support heterogeneous roams.

In order to limit the scope of this analysis several assumptions were made. These assumptions will help to identify the specific 802.16e technologies that need to be applied to this problem as well as to identify areas of the 802.16e standard that do not satisfactorily address the technology need of a mobile train network.

These assumption are:

-Using the current standard train velocity will be limited to 120km/h. For the large majority of train systems this velocity will be adequate.

-Physical layer systems will for the most part be ignored as part of my analysis.

-The system is homogenous were the network administration of both the mobile router and the track networking gear is controlled by one organization only.
-A centralized hierarchical layout (not flat) will be used with the three BSs all belonging to the same access service network (ASN). See Figure 17 below. Since a homogenous environment is assumed, by using a centralized hierarchical layout, the layer 3 roaming will be minimized or potentially totally avoided. By making the system involve layer 2 roaming only the added complexities and delay that is associated with a layer 3 roam using Mobile IP are avoided. A flat layout would require a layer 3 roam every time a MS moves to a new target BS.[16]

The assumption that over the course of an entire rail line a single ASN can support all of the BSs is one that will require further research. One major technical problem will be that in order to support fast base station switching (FBSS) the BSs must be synchronized. This will not be trivial over a large geographic area.

To help frame the context for analysis consider the network outlined in Figure 17 below.

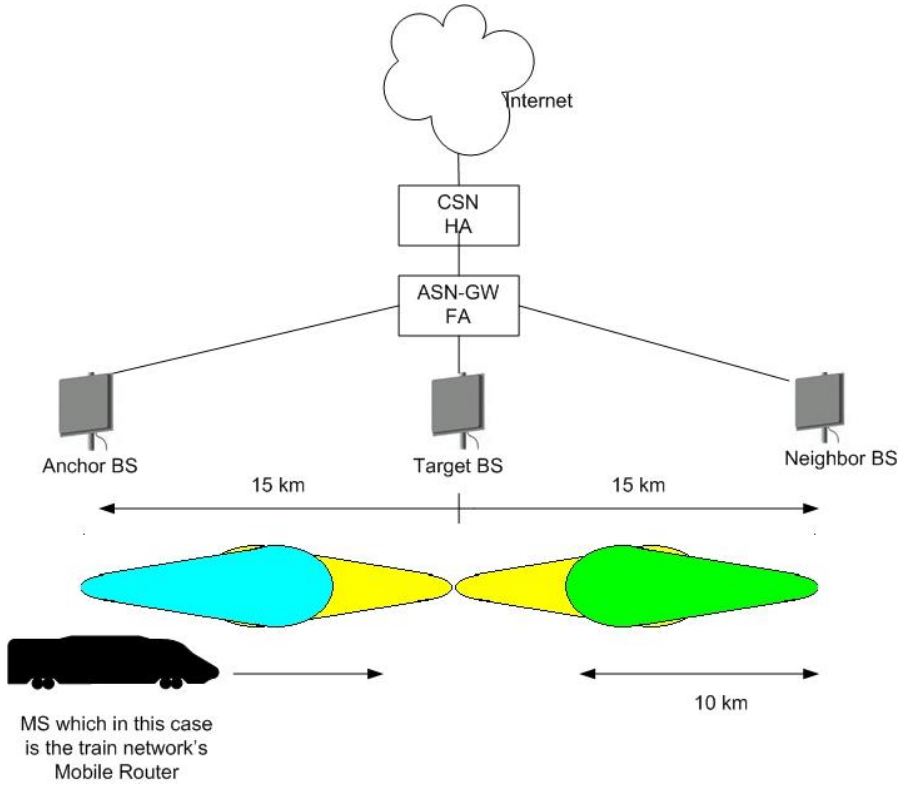

Figure 17. Proposed Network

Recommendations

Based on the scenario outlined above and the stated assumptions the following details the specific aspects of the 802.16e standard that are believed to be optimal for this application. There are many aspects to the standard that are optional or have multiple possible applications. Due to this built in adaptability of the standard the only modification to the existing 802.16e standard required will be to support high train velocities. Currently the standard will support speeds of up to 120 km/h but consideration has been made for potential evolution to higher vehicle speeds.[19]

Using the existing 802.16e standard as a base then this examination is limited to only those areas of the standard that are best suited to dealing with train mobility.

To do this a brief discussion of some of the relevant 802.16e terms and technologies is important.

In 802.16e three types of handoffs are discussed. A hard handoff involves the complete breaking of the current wireless link before the new link is formed. This is similar to the 802.11g roam processes experimented with earlier. A soft handoff (SHO) using Macro Diversity Handover (MDHO) and a Fast Base Station Switching (FBSS) handoff both allow a mobile subscriber (MS) to have multiple active connections. These are both known as make-before-break algorithms. Only the FBSS handoffs will be considered here as it has less delay than hard handoffs and produces less overhead than SHO.[16] BS's are required to be synchronized using a common time source. The BS's also operate using the same frequency channels.

Since this system is designed specifically for trains the coverage cells will be designed such that they cover the train track area and minimal coverage to other areas. This would allow for large antenna gains and the use of very directional antennas.

Based on the diagram above and assuming 120km/h with a maximum usage of one train every 3 minutes per direction[12] one can calculate the maximum number of trains in the coverage area.

Distance Between Trains

$$Distance = 120km/h * 3\min/ 60\min/ h$$

$$Distance = 6km$$

$$Trains/cell = 20km/6km * 2tracks = 6$$

A directional cell coverage area of 10 km will be assumed. The distance was limited to 10km so that large tower heights would not have to be used to deal with earth curvature factors and

since track curves and dips would require additional BSs than this perfect scenario is likely to account for. Some estimates predict a 15 km maximum range for 802.16e.[17] Given the number of trains partial usage of sub-channels (PUSC) will likely be the best choice for this scenario as it will allow the BS sectors (one in either direction from the BS) to be not overlapping and can be set up to eliminate interference from neighboring BSs. It is possible that full usage of sub-channels (FUSC) may also be a good choice if the load on the system is low.[16] Another point to note here is that inter-sector movement of the MS within the cell is not being looked at as part of this analysis. In practice it might be necessary to implement a third sector to cover the train as it passes directly past the BS.

In this 30 km stretch of track then the train will be forced to roam twice and will at most have 2 active BSs in range at a given time period. The handoffs will occur when the train is within range of two BSs so that FBSS can be used to give a low delay handoff.

Roaming will be initiated by the train router based on physical layer signal characteristics. In 802.11 roaming is not just controlled by the physical layer characteristics and this leads to a delay in roaming until the signal from the first AP has been lost. This creates significant delays in roaming to the stronger signal that is quite noticeable when performing experiments. Triggering a roam based on signal strength will allow for the roam process to occur while still in range of the initial BS and will allow for more complex handoff methods such as FBSS which will minimize the handoff delay. In 802.16e roams can also be triggered by congestion but in this linear system with limited train traffic only Phy triggered roams are considered.

The MS uses the flow chart in Figure 18 for its scanning and HO processes.

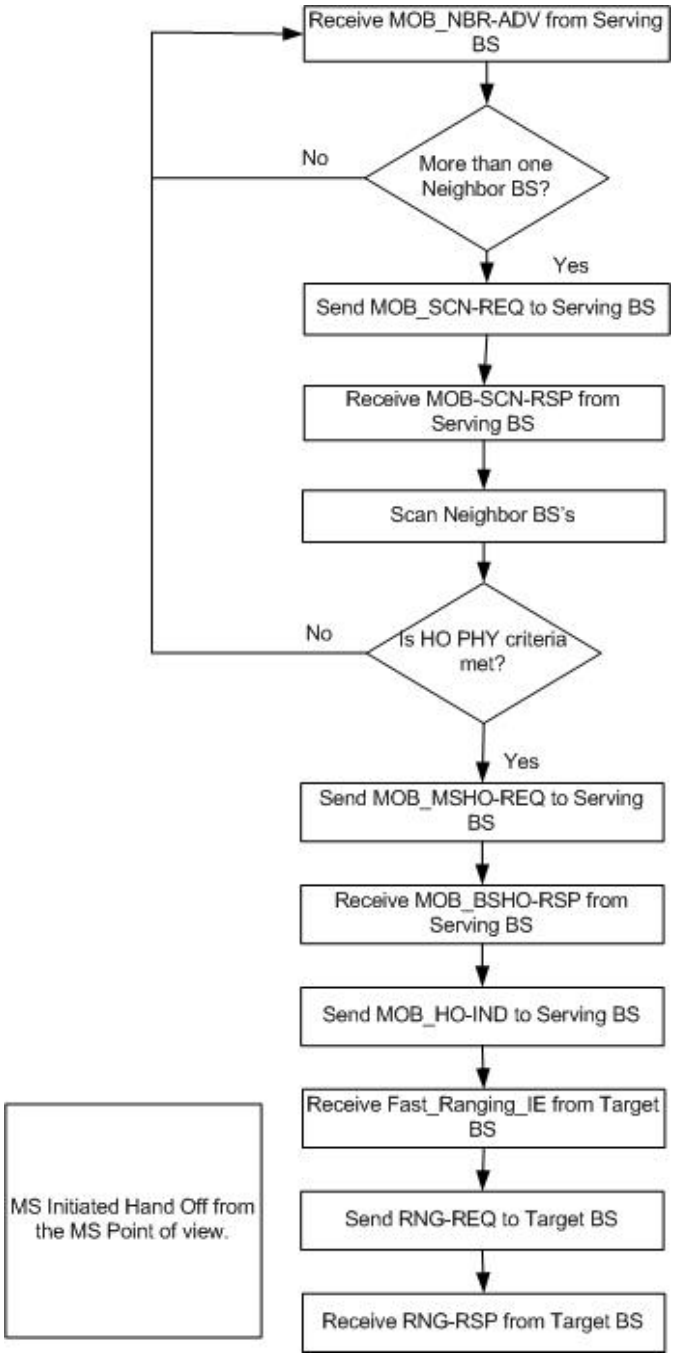

Figure 18. MS Communication Flow Chart[18]

The MS learns about potential target BSs from the serving BS in the MOB_NBR-ADV. The MS will then request a scanning time from the serving BS and identify that it would like to associate with the potential target BS. The serving BS gets further information from the potential target BS and requests a time for the MS to synchronize. The serving BS notifies the MS of the required information in the MOB_SCN-RSP. The MS goes into scanning mode and synchronizes with the possible target BS and sends its CDMA ranging code. Since in this proposal the target BS has assigned a non-contention based time slot to the MS this can proceed faster than the standard contention based HO model. The potential target BS then sends the RNG_RSP to the serving BS who forwards it to the MS. This technique is called network assisted association reporting or association Level 2 in the standard.[18] It was selected for use in this proposed process since it is faster than the level 0 or level 1 process and should be superior for QOS. It is also the most complex and is more likely to fail but given this very controlled and low volume application would seem to be ideal. Figure 19 details this process graphically.

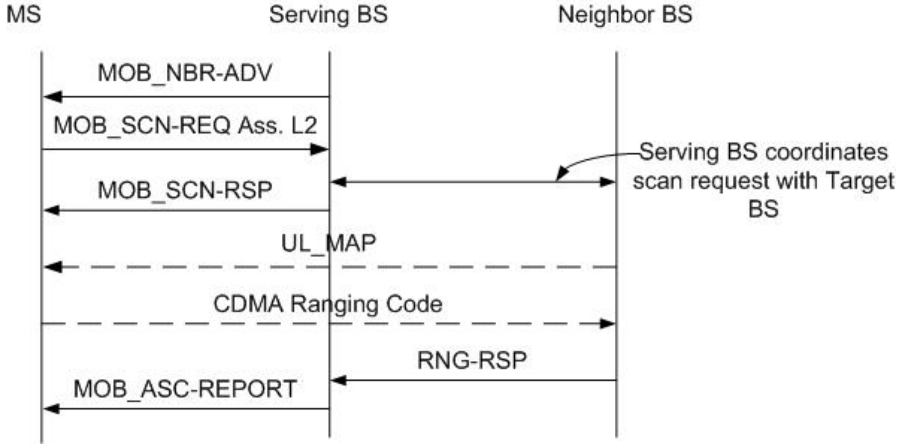

Figure 19. Association with Neighbor BS's.

While this neighbor association process can preoccupy the MS and reduce QOS it does not stop data flow to and from the MS. The biggest impact on QOS occurs during the actual HO process when the data flow between the MS and the serving BS is stopped completely during the transition.

The Handover Process

An interesting note on this proposed system is that the train is likely to be within range of a maximum of 2 cells at any given time. As a result the time for network topology acquisition through scanning will be reduced in a similar manner to a proposed fast handover algorithm.[21] While this paper proposes using the non-contention based ranging process in

this model the MS's BS scanning and ranging process will be reduced without implementing the fast handover algorithm that these authors propose simply because of the limit of one possible target BS.

In this model both MS and BSs must support FBSS although it is listed as optional by the standard.

As can be seen in the previous section in the proposed implementation the MS will be associated with the target BS before the HO process is initiated. This will reduce the time required to perform a roam to the target BS. The HO process is anticipated to occur immediately after the process in Figure 19 so that the physical link properties will remain constant.

The MS will base its decision to roam on the physical characteristics of the connections it has to associated BSs. A key characteristic is the Carrier to Interference plus Noise Ratio (CINR). The CINR is used to add and remove BSs from the MS's active BS set as well as acting as a HO trigger.

The MS can initiate a HO in two ways. It can use the channel quality indication channel (CQICH) or it can send a MOB_MSHO-REQ message. Only the latter will be considered here. After the MS has decided to HO it sends the MOB_MSHO-REQ message to the serving BS. This message will indicate to the BS the identity of the target BS the MS wants to connect to.

The serving BS then connects to the Target BS to gather connection information that it then sends to the MS in a MOB_BSHO-RSP message. The serving BS then begins what is known as the bicasting initiation stage where it prepares a tunnel to the target BS which will be used for forwarding a copy of data for the MS during the handoff. These copies are to prevent lost or delayed data during the handoff stage. As data comes in to the serving BS it continues to forward the data to the MS interspersed in this process to prevent delays.[16] Once the tunnel is formed however it begins bicasting and sends a copy of all MS data to the target BS.

The MS will send a MOB_HO-IND to the serving BS. This is the start of the service interruption as the MS will now not receive any more data until it has connected to the target BS. The serving BS then begins forwarding the MAC state to the target BS through the tunnel. Since the MS is already associated with the target BS the network re-entry and ranging stage is shortened significantly. Also since the MS is still in the same ASN, AAA and Foreign Agent (FA) change procedures are not required. Given this specific approach the standard was not clear on how the tunnel is torn down and all data flow now goes through the target BS. It is reasonable to assume that the target BS would first notify the ASN-GW of the transition so that further data for the MS would be sent to the target BS rather than tunneling through the source BS. Once this notification is complete the target BS or MS

could then wait for the last tunneled data from the source BS and then tear down the tunnel. Other authors have indicated that the MS sends another MOB_HO-IND to the serving BS but this could not be confirmed from the standard.[21] Based on the experimental problems with the MIP tunnel teardown under 802.11 this implementation will be crucial to maintaining high QOS.

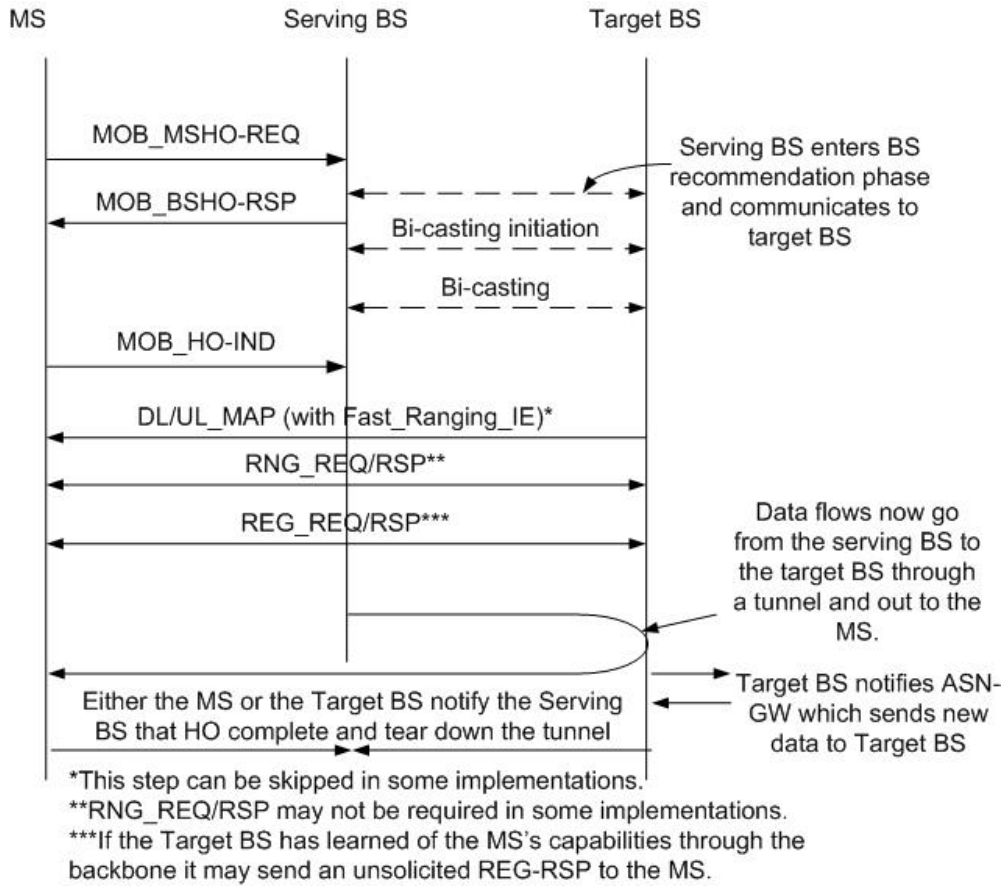

Figure 20. Recommended HO

To implement this process several recommendations have been made that while they are based on the 802.16e standard are very specific implementations of parts of the standard. It is therefore likely that to implement this system in a tight package the solution is likely to be vendor specific and the solution is more likely to function well if all components come from the same vendor.

ANALYSIS

To clarify the effects of the various options discussed an analysis was performed that looked at the effects of choosing the various systems with the goal of identifying the optimum system.

In the paper by Choi et al.[10] they performed a performance analysis on their proposed handover scheme that forms the basis for this analysis. Their analysis assumes real time traffic and an OFDMA TDD system with frame duration of 5 ms. In addition it is being assumed that backbone processes will be dealing with the target BS authentication process as this will not be a layer 3 roam.

The following variables will be used:[10]

Tsync- average time required to synchronize with new downlink. The MS listens for the Downlink Channel Descriptor (DCD) message and then uses this information to synchronize with the target BS.
Tcont resol- average time required for contention resolution procedure during contention based ranging process. In contention based ranging the target BS has not allocated a Fast_Ranging_IE field for the MS in the DL_MAP. The ranging process is then more time consuming to perform.
Trng- average time required for ranging process during HO. This is the time to perform the final RNG-REQ/RSP step of the ranging process.
Treg- average time required for re-registration during HO. Once ranging has been completed the MS will send a REG-REQ to the target BS. The target BS will respond with a REG-RSP indicating successful registration. It is possible for the serving BS to provide the target BS with sufficient information that it will send an unsolicited REG-RSP to the MS.
Tauth- average time required for re-authorization during HO. This will be disregarding as the MS is not performing a layer 3 roam and so has the same ASN-GW.
Congestion Factor- Since performance degradation with load of a OFDMA system is close to linear[23] initially this factor is used as a rough indicator of the affect of traffic load on HO processes.

In Figure 20 data traffic can be sent from the serving BS to the MS up until MOB_HO-IND message has been sent. At that point however the MS needs to establish a link with the target BS before data flow can resume either tunneled or directly. The ranging and registration time after the MOB_HO-IND is the most crucial when considering service interruption for real time traffic and as a result is the aspect analyzed here.

Four scenarios will be considered. In each case it is assumed that the MS authentication information has been forwarded to the target BS and that authentication is not required.

Type 1
Contention Based Registration (CBR) occurs when the MS does not receive a Fast Ranging IE in the DL/DL_MAP. This means the target BS has not allocated a ranging time for the MS.

HO Delay = Tcont_resol + Tsync + Trng + Treg

Type 2
Non-Contention based Ranging (NCR). In this scenario the DL/UL_MAP from the target BS contains the Fast_Ranging_IE but the MS is not synchronized with target BS.

HO Delay = Tsync + Trng + Treg

Type 3
No Ranging (NR). In this scenario the target BS and the MS are synchronized and only require registration.

HO Delay = Treg

Type 4
Unsolicited REG-RSP (URR). In this scenario the target BS has received all required information from the source BS and simply sends a REG-RSP to the MS. While this option is available in the standard it appears that it is left to manufacturers to figure out the backbone systems that can accomplish this.

HO Delay = Treg/2

Using the following variable values[10] calculations were performed with various congestion factors.

Variable	Time (ms)
Tcont_resol	50
Tsync	10
Trng	25
Treg	35

Table 7. Variable Values

Congestion Factor	1	1.5	2	2.5	3
CBR	120	180	240	300	360
NCR	70	105	140	175	210
NR	35	52.5	70	87.5	105
URR	17.5	26.25	35	43.75	52.5
Acceptable	160	160	160	160	160

Table 8. HO Delay values

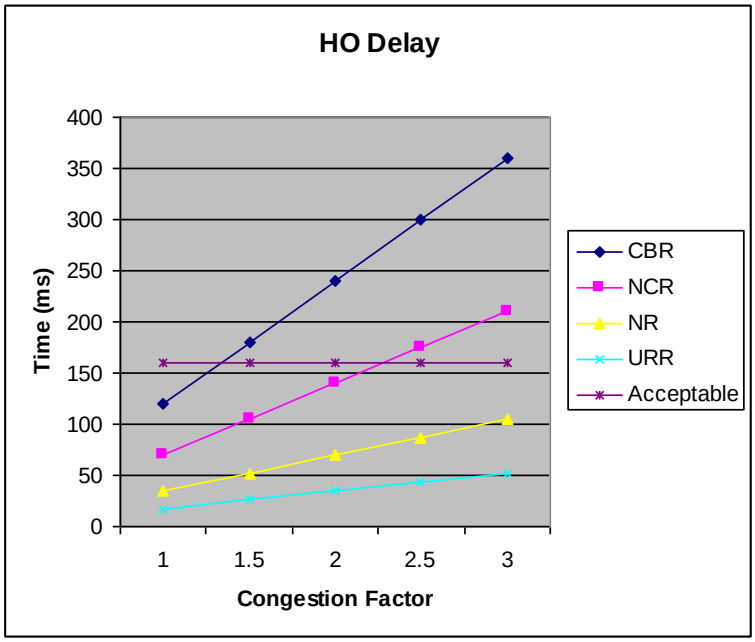

Figure 21. HO Delay at various Congestion Factors

As can be seen there is a significant delay even in these relatively high performance layer 2 roams. Performance of systems with hard handoffs or layer 3 roams can be expected to be worse than this. As people can hear delays at a minimum value of 40 – 70 ms only two of these systems would be acceptable for the range of this test. The WiMAX forum indicated that HO values of up to 160ms are acceptable for real time traffic so using that criteria three of these handoffs would be satisfactory under the no load condition. As load increases only the two Non-Ranging options meet the HO delay criteria. A more rigorous system of factoring congestion degradation should be developed and as such these results should be regarded as comparative only.

Based on these results it is very apparent that backbone processes that are not necessarily part of the 802.16e standard directly are going to be crucial in determining the ultimate QOS performance of which a mobile WiMAX train uplink system is capable.

From this analysis it is recommended that the following aspects of the 802.16e standard should be implemented to minimize handoff delay in these systems.

-802.16e using OFDMA.
-PUSC (1/2 frequency reuse) or FUSC
-FBSS
-Network Assisted Association
-Implemented systems for allowing the target BS to register the MS through the backbone with information from the serving BS and the ASN-GW.

CONCLUSION:

The use of dual mode cell phones on mobile networks will soon be a reality. As shown in the 802.11 testing performed, while Layer 3 roaming through Mobile IP provides an adequate solution for mobile data only networks it does not provide the seamless QOS service required by the real time traffic that will be generated on mobile networks in the near future.

The Mobile IP implementation under 802.16e will be faster than the 802.11 equivalent as tested as it is much better integrated into the standard than 802.11 but it will still produce much more latency than a strictly layer 2 roam. The solution proposed in this paper illustrates an implementation of 802.16e technologies to a train based mobile network. The particular aspects of 802.16e that would be implemented in this system would be a hierarchical, 0FDMA based, PUSC (or FUSC), FBSS, with network assisted association. Some aspects of this solution would have to use modifications to the 802.16e standard, specifically as it relates to dealing with high speed rail systems.

Several questions regarding the technical feasibility of implementing this system remain to be answered and will require further research; The practical ability to synchronize significant numbers of geographically dispersed BS's so that FBSS can be used needs to be examined. A simulation of the proposed handoff mechanism needs to be created to better analyze system performance under load. The optimum process for the wired communication between the BS's and the ASN-GW needs to be determined and defined more clearly so that an implementation of this proposed handover process can be implemented or standardized.

The issues identified above should be able to be resolved and given that this proposed solution to train based mobile network uplinks has significant potential to increase QOS during the crucial handoff period. This improved QOS performance will directly affect the use of VoIP on train based networks.

BIBLIOGRAPHY

[1] Perkins, C., Ed, "IP Mobility Support", RFC 2002, October 1996.

[2] Perkins C., Ed., "IP Mobility Support for IPv4," RFC 3344, 2002.

[3] Hills Tom, "SIP Guide", Available at http://www.lightreading.com/document.asp?doc_id=77756

[4] Calhoun Pat, O'Hara Bob, "802.11r strengthens wireless voice", Technology Update[Online Serial], Available at http://www.networkworld.com/news/tech/2005/082205techupdate.html

[5] "Configuring Proxy Mobile IP," Cisco IOS Software Configuration Guide for Cisco Aironet Access Points, , Cisco, April 2004, Available at http://www.cisco.com/en/US/products/hw/wireless/ps4570/products_configuration_guide_chapter09186a00802091bd.html

[6] McMurdo Bruce, Cisco Fast Secure Roaming Application Note, Cisco, 2004, Available at http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_technical_reference09186a00801c5223.html

[7] Dhondt Wouter, Fast Pinger version 2.15, Available at http://www.kwakkelflap.com/downloads.html

[8] Wireless Domain Services AP as an AAA Server Configuration Example, Cisco, Available at http://www.cisco.com/en/US/products/hw/wireless/ps430/products_configuration_example09186a008059a559.shtml

[9] "How to Disable the "Media Sensing" for TCP/IP in Windows," Microsoft Knowledge Base, Available at http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q239924&

[10] Choi Sik, Hwang Gyung-Ho, Kwon Taesoo, Lim Ae-Ri, Cho Dong-Ho, "Fast Handover Scheme for Real-Time Downlink Services in IEEE 802.16e BWA System," Vehicular Technology Conference, 2005

[11] Amir Yair, Danilov Claudia, Hilsdale Michael, Musaloiu-Elefteri, Rivera Nilo, "Fast Handoff for Seamless Wireless Mesh Networks," MobiSys'06, 2006

[12] Oliver Keating, "High Speed Rail (HSR)," Available at http://www.o-keating.com/hsr/

[13] Eric Sandblom, "Korean HSR Opens in April," High Speed Rail News, Available at http://www.artech.se/~sandblom/archive/hst.html

[14] Kempf J, Ed, "Goals for Network-based Localized Mobility Management," IETF Draft, 2006, Available at http://mirror.switch.ch/cgi-bin/search/nph-findstd?preview=draft-ietf-netlmm-nohost-req-03.txt&scope=draft

[15] "Japanese Bullet Train Gets its Wi-Fi On," Digital World Tokyo, June 2006, Available at http://www.digitalworldtokyo.com/2006/06/japanese_bullet_train_gets_its.php

[16] "System Aspects and Handover Management for IEEE 802.16e," Bell Labs Technical Journal, 11(1) 2006, Wiley Periodicals.

[17] Kitroser Itzik, Segal Yossi, Leiba Yigal, Hadad Zion, IEEE 802.16e Mobility System Perspective, IEEE, 2003.

[18] "IEEE Standard for Local and Metropolitan area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems," IEEE, 2006

[19] Gray Doug, "Mobile WiMAX: A Performance and Comparitive Summary," WiMAX Forum, 2006.

[20] "Mobile WiMAX – Part 1: A Technical Overview and Performance Evaluation," WiMAX Forum, 2006

[21] Lee Doo, Kyamakya Kyandoghere, Umondi Jean, "Fast Handover Algorithm for IEEE 802.16e Broadband Wireless Access System," 1st International Symposium on Wireless Pervasive Computing, 2006

[22] "WiMAX Forum Overview", Available at http://www.wimaxforum.org/about/WiMAX_Forum_Overview/

[23] Liu Hui, "Network diversity in Broadband wireless systems," ONR Workshop, 2003, Available at http://danube.ee.washington.edu/downloadable/hliu/network%20diversity.ppt

[24] "The Connected Carriage System," QinetiQ, 2006, Available at http://www.qinetiq.com/home_qinetiq_rail/qinetiqrail_services/connected_carriage.html

APPENDIX

MicroMobility AP Configuration

HA1232AG Configuration File

```
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname HA1232AG
!
enable secret 5 $1$b4y7$3uGDNJ3egLEafJ2taCsnO/
!
username Cisco password 7 047802150C2E
ip subnet-zero
!
!
no aaa new-model
!
dot11 ssid Mint709
   authentication open
   guest-mode
!
!
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid Mint709
 !
 short-slot-time
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 power local cck 1
 power local ofdm 1
 power client 1
 packet retries 16
 channel 2412
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 !
 ssid Mint709
 !
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
```

```
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 10.0.0.21 255.255.255.0
 no ip route-cache
!
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
logging snmp-trap emergencies
logging snmp-trap alerts
logging snmp-trap critical
logging snmp-trap errors
logging snmp-trap warnings
!
control-plane
!
bridge 1 route ip
!
!
wlccp ap username ha password 7 0718255F
!
line con 0
 transport preferred all
 transport output all
line vty 0 4
 login local
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 login
 transport preferred all
 transport input all
 transport output all
!
end
```

FA1232AG Configuration File

```
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname FA1232AG
!
enable secret 5 $1$3hhh$sJVCEb60Zg4rAdYVDYXwX0
!
username Cisco password 7 112A1016141D
ip subnet-zero
!
!
no aaa new-model
!
dot11 ssid Mint709
   authentication open
   guest-mode
!
!
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
```

```
 ssid Mint709
 !
 short-slot-time
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 power local cck 1
 power local ofdm 1
 power client 1
 packet retries 16
 channel 2462
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 !
 ssid Mint709
 !
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 station-role root
 no dot11 extension aironet
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 10.0.0.41 255.255.255.0
 no ip route-cache
!
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
!
logging snmp-trap emergencies
logging snmp-trap alerts
logging snmp-trap critical
logging snmp-trap errors
logging snmp-trap warnings
!
control-plane
!
bridge 1 route ip
!
!
wlccp ap username fa password 7 10590D0A
!
line con 0
 transport preferred all
 transport output all
line vty 0 4
 login local
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 login
 transport preferred all
 transport input all
 transport output all
!
end
```

WDS Configuration

```
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname WDS
!
enable secret 5 $1$otaa$3CZoJ0GRwEmkZ/OP2g5WQ0
!
username Cisco password 7 14341B180F0B
ip subnet-zero
!
aaa new-model
!
!
aaa group server radius rad_eap
 server 10.0.0.25 auth-port 1812 acct-port 1813
!
aaa group server radius rad_mac
!
aaa group server radius rad_acct
!
aaa group server radius rad_admin
!
aaa group server tacacs+ tac_admin
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa group server radius Infrastructure
 server 10.0.0.25 auth-port 1812 acct-port 1813
!
aaa authentication login eap_methods group rad_eap
aaa authentication login mac_methods local
aaa authentication login method_Infrastructure group Infrastructure
aaa authorization exec default local
aaa accounting network acct_methods start-stop group rad_acct
aaa session-id common
power inline negotiation prestandard source
!
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 no ip route-cache
 !
 ssid tsunami
    authentication open
    guest-mode
 !
 short-slot-time
 speed basic-1.0 basic-2.0 basic-5.5 6.0 9.0 basic-11.0 12.0 18.0 24.0 36.0 48.0 54.0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface Dot11Radio1
 no ip address
 no ip route-cache
 shutdown
 !
 ssid tsunami
    authentication open
    guest-mode
 !
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
```

```
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 10.0.0.25 255.255.255.0
 no ip route-cache
!
ip http server
no ip http secure-server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag
ip radius source-interface BVI1
logging snmp-trap emergencies
logging snmp-trap alerts
logging snmp-trap critical
logging snmp-trap errors
logging snmp-trap warnings
radius-server local
  no authentication eapfast
  no authentication mac
  nas 10.0.0.25 key 7 111E1D16
  user ha nthash 7 106F2D4B21344B5328517879750910140443534355240678 7B0A70595B49427D7B
  user fa nthash 7 15332F5E2009727C0C6667704226352227060D0D05715E223B4F7D0F0F02067177
  user wds nthash 7 106F2D4B21344B5328517879750910140443534355240678 7B0A70595B49427D7B
!
radius-server attribute 32 include-in-access-req format %h
radius-server host 10.0.0.25 auth-port 1812 acct-port 1813 key 7 111E1D16
radius-server vsa send accounting
bridge 1 route ip
!
!
wlccp ap username wds password 7 111E1D16
wlccp authentication-server infrastructure method_Infrastructure
wlccp wds priority 254 interface BVI1
!
line con 0
 transport preferred all
 transport output all
line vty 0 4
 transport preferred all
 transport input all
 transport output all
line vty 5 15
 transport preferred all
 transport input all
 transport output all
!
end
```

Macro Mobility Access Point Configuration

HA Access Point Configuration File

```
show run
Building configuration...

Current configuration : 1781 bytes
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname HA
!
enable password 7 112A1016141D
!
username Cisco password 7 047802150C2E
ip subnet-zero
!
ip proxy-mobile enable
ip proxy-mobile aap 10.0.0.21 10.2.0.21
dot11 holdoff-time 600
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 ip proxy-mobile
 no ip route-cache
 !
 ssid HA
    authentication open
    guest-mode
    infrastructure-ssid optional
    ip proxy-mobile
 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 power local 1
 power client 1
 channel 2452
 station-role root
 no cdp enable
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface Dot11Radio1
 no ip address
 ip proxy-mobile
 no ip route-cache
 !
 speed basic-6.0 9.0 basic-12.0 18.0 basic-24.0 36.0 48.0 54.0
 rts threshold 2312
 station-role root
 no cdp enable
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
 bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 ip proxy-mobile
 no ip route-cache
 duplex auto
speed auto
 bridge-group 1
 no bridge-group 1 source-learning
```

```
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 10.0.0.21 255.255.255.0
 ip proxy-mobile priority 101
 no ip route-cache
!
ip default-gateway 10.0.0.30
ip http server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100
bridge 1 route ip
!
line con 0
line vty 0 4
 login local
line vty 5 15
 login
!
ntp server 10.0.0.30
end
```

FA Access Point Configuration File

```
show run
Building configuration...

Current configuration : 1527 bytes
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname FA
!
enable secret 5 $1$rHyj$VZcG7h400IzsOklgZ5TSp1
!
username Cisco password 7 0802455D0A16
ip subnet-zero
!
ip proxy-mobile enable
ip proxy-mobile aap 10.0.0.21
ip proxy-mobile secure node 10.0.0.0 10.0.0.254 spi 102 key hex aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
!
bridge irb
!
!
interface Dot11Radio0
 no ip address
 ip proxy-mobile
 no ip route-cache
 !
 ssid FA
    authentication open
    guest-mode
    infrastructure-ssid optional
    ip proxy-mobile
 !
 speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
 rts threshold 2312
 power local 1
 power client 1
 channel 2422
 station-role root
 bridge-group 1
 bridge-group 1 subscriber-loop-control
 bridge-group 1 block-unknown-source
 no bridge-group 1 source-learning
 no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled
!
interface FastEthernet0
 no ip address
 ip proxy-mobile
 no ip route-cache
 duplex auto
 speed auto
 bridge-group 1
```

```
 no bridge-group 1 source-learning
 bridge-group 1 spanning-disabled
!
interface BVI1
 ip address 10.2.0.21 255.255.255.0
 ip proxy-mobile
 no ip route-cache
!
ip default-gateway 10.2.0.30
ip http server
ip http help-path http://www.cisco.com/warp/public/779/smbiz/prodconfig/help/eag/ivory/1100
ip radius source-interface BVI1
bridge 1 route ip
!
!
line con 0
 stopbits 1
line vty 0 4
 login local
line vty 5 15
 login
!
ntp clock-period 17209335
ntp server 10.1.0.10
end
```

Macro Mobility HomeAgent Configuration

```
Current configuration : 1461 bytes
!
! Last configuration change at 03:56:25 UTC Mon Mar 1 1993
! NVRAM config last updated at 00:11:21 UTC Mon Mar 1 1993
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname HomeAgent
!
!
memory-size iomem 10
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
call rsvp-sync
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.0.0.30 255.255.255.0
 ip irdp
 ip irdp maxadvertinterval 4
 ip irdp minadvertinterval 3
 ip irdp holdtime 12
 ip mobile registration-lifetime 3
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 no fair-queue
!
interface FastEthernet0/1
 ip address 10.1.0.10 255.255.255.0
 ip irdp
 duplex auto
```

```
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
!
router mobile
!
ip classless
ip route 10.2.0.0 255.255.255.0 10.1.0.20
ip http server
ip mobile home-agent
ip mobile host 10.0.0.10 interface FastEthernet0/0 lifetime 5
ip mobile host 10.0.0.11 interface FastEthernet0/0
ip mobile host 10.0.0.21 interface FastEthernet0/0
ip mobile foreign-agent care-of FastEthernet0/1
ip mobile secure host 10.0.0.10 spi 102 key hex aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
ip mobile secure host 10.0.0.11 spi 102 key hex aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
!
access-list 1 permit 10.0.0.0 0.0.0.255
!
!
dial-peer cor custom
!
!
!
!
!
line con 0
 password excal5iber
 login
line aux 0
line vty 0 4
 password excal5iber
 login
!
ntp master
end
```

Macro Mobility ForeignAgent Configuration

```
ForeignAgent#show run
Building configuration...

Current configuration : 917 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ForeignAgent
!
!
memory-size iomem 10
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
!
call rsvp-sync
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 10.2.0.30 255.255.255.0
 ip irdp
 ip irdp maxadvertinterval 4
 ip irdp minadvertinterval 3
 ip irdp holdtime 12
 ip mobile foreign-service
```

```
 ip mobile registration-lifetime 3
 duplex auto
 speed auto
!
interface Serial0/0
 no ip address
 shutdown
 no fair-queue
!
interface FastEthernet0/1
 ip address 10.1.0.20 255.255.255.0
ip irdp
 duplex auto
 speed auto
!
interface Serial0/1
 no ip address
 shutdown
!
router mobile
!
ip classless
ip route 10.0.0.0 255.255.255.0 10.1.0.10
ip http server
ip mobile foreign-agent care-of FastEthernet0/0
!
!
!
dial-peer cor custom
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
!
end
```