Title
California Trains Connected

Authors
Kanafani, Adib
Benouar, Hamed
Chiou, Bensen
et al.

Publication Date
2006-04-01

CALIFORNIA PATH PROGRAM
INSTITUTE OF TRANSPORTATION STUDIES
UNIVERSITY OF CALIFORNIA, BERKELEY

California Trains Connected

**Adib Kanafani, Hamed Benouar,
Bensen Chiou, Jean-Luc Ygnace,
Kazuhiro Yamada, Adam Dankberg**

California PATH Research Report
UCB-ITS-PRR-2006-4

This work was performed as part of the California PATH Program of the University of California, in cooperation with the State of California Business, Transportation, and Housing Agency, Department of Transportation, and the United States Department of Transportation, Federal Highway Administration.

The contents of this report reflect the views of the authors who are responsible for the facts and the accuracy of the data presented herein. The contents do not necessarily reflect the official views or policies of the State of California. This report does not constitute a standard, specification, or regulation.

Final Report for Task Order 5106

April 2006

ISSN 1055-1425

CALIFORNIA PARTNERS FOR ADVANCED TRANSIT AND HIGHWAYS

California Trains Connected
Final Project Report

Task Order PATH 5106

By

Professor Adib Kanafani
Principal Investigator
Department of Civil and Environmental Engineering
University of California, Berkeley

Dr. Hamed Benouar
Director, California Center for Innovative Transportation
University of California, Berkeley

Bensen Chiou
Project Manager, California Center for Innovative Transportation
University of California, Berkeley

Dr. Jean-Luc Ygnace
Visiting Scholar
Institut National de Recherche sur les Transports et leur Sécurité, France

Kazuhiro Yamada
Visiting Scholar
Central Japan Rail Company

Adam Dankberg
Graduate Student Researcher
University of California, Berkeley

Acknowledgement

The project team would like to thank many people from Caltrans and the Capitol Corridor Joint Power Authority (CCJPA) who provided various inputs, feedback, guidance and other assistance, particularly Caltrans Project Manager, Dan Lovegren, Caltrans Chief of the Division of Rail Bill Bronte and CCJPA Senior Planner, Jim Allison.

We would like to thank Mr. Douglas Cooper, Ms. Ipsita Banerjee and Ms. Sin Yi Chu for their assistance in conducting surveys and developing business models; Dr. Harsh Verma, who provided leadership on technical and security research; and the Mangers of the Central Japan Rail Company, who loaned to CCIT Mr. Kazuhiro Yamada to support the project team in researching wireless technology landscape and performing mobile Internet Protocol related improvement. We would also like to thank Dr. Susan Shaheen, PATH program manager who reviewed this report and provided valuable input.

Abstract

“California Trains Connected”

This project is to assist the Capitol Corridor Joint Power Authority (CCIPA) and the California Department of Transportation (Caltrans) assemble a decision framework for selecting wireless Internet access on behalf of customers riding the three California State sponsored Intercity Rail Services. To accomplish this objective, we researched the state of worldwide deployment of service based on the wireless technologies, such as wireless fidelity (WiFi) and **W**orldwide **I**nteroperability for **M**icrowave **Acc**ess (WiMAX), conducted a survey of the WiFi service at San Francisco Airport, and examined the historical ridership data on train routes of the Intercity Rail service. In addition, we conducted a survey on the trains offering trial Internet access based on low bandwidth communication infrastructure. The results are used with other data to develop business model options.

To support the business mode options, the project technical team researched the wireless technology landscape, examined the technology trends and options, and the specific characteristics of the operating environment of the target rail service, researched the emerging technology for enabling the mobile connectivity, and researched the vulnerability and viable security technologies.

The business model options and the technical guidelines can be used to formulate a performance specification for a high-bandwidth trackside infrastructure to connect end user devices to Internet. The specification, in turn, can be used for writing a Request for Quotation (RFQ) to solicit qualified service providers for the Internet service on trains.

Keywords: Architecture, Benefit Cost Analysis, Communications, Electronic Ticketing, Fiber Optics, Policy, Privacy, Radio, Safety, Standards, WiMAX, WiFi

Executive Summary

Wireless Internet service will allow customers to conduct business or connect to websites for leisure, personal, or entertainment purposes. It will also permit train operators to leverage the infrastructure and Internet access to improve ticket collection, public safety, and security, to bundle value-added services and to implement other services for improving operational efficiencies.

The project team include the principal investigator, the director of the California Center for Innovative Transportation (CCIT) – an organization of the University of California, Berkeley Institute of Transportation Study, the CCIT project manager , University of California researchers and students, managers from the Capitol Corridor Joint Power Authority (CCJPA) and Caltrans, a visiting scholar from Central Japan Railway company, a visiting scholar from Institut National de Recherche sur les Transports et leur Sécurité (INRETS) in France, and a subcontractor.

The project team researched world-wide deployment of general wireless-based services and Internet access on trains. It also conducted a survey on the trains managed by CCJPA for wireless Internet usage and various price points in addition to researching the business model options, technology options, and industry technology trends.

Many business model options and technology landscapes and market adoptions were researched and explored. Two business and technology model options were recommended: conservative and maximized market. The conservative model option requires less low capital investment. It, however, has low revenue potential and requires relatively high running cost. The maximized market model option has high revenue potential and requires relatively low running cost. It however requires high initial capital investment. In either option, a WiFi network is used in cars of train for train riders to connect their end user devices to the on-train gateway.

For the conservative model option, the on-train gateway is connected to the Internet using satellite for downloads and cellular for upload. The initial capital expenditure can be as low as $40K per train. The annual cost of ownership, however, can be in range of $100K – $150K depending on the number of users. This option can support up to 20 users per train based on the total bandwidth of 1-2Mbps satellite downlink and a bandwidth consuming rate of 100Kbps per user. The break-even point can be achieved in 1 – 2 years. However, the number of users it can support is limited, thus the revenue potential is limited. There is little chance of offering value-added services due to the limited communication bandwidth. To support more users or offer value-added services, it requires more initial capital expenditure and much higher running cost, and the break-even point can be achieved in 5 – 7 years depending on the business strategy, the bandwidth needed and revenue/cost sharing partnerships.

For the maximized market model, the on-train gateway is connected to the Internet via a high-bandwidth trackside wireless infrastructure connected to Internet via fibre-optical connection. The communication beacon infrastructure can be spaced from one kilometer

to 3km each and can support up to 160 users per train even if only half of the communication capacity is used for Internet service. The rest of the capacity can be used for administrative, homeland security, train operation and other value-added applications. Since the initial capital investment can be as high as $4M - $9M, the break-even point can't be achieved if there is no cost sharing through partnerships. If the 50% of the initial cost for initial capital expenditure can be shared with other partners or is supported by fund for homeland security mandate, the break-even point can be achieved in 7 years, and the profit potential can be quite high after the break-even point, especially if some value-added services can be deployed.

The characteristics of train riders affecting the usage and pricing point of the Internet access on train for determining the business model options are trip frequency, duration of trip, and pricing points of various charging types. There are two types of target user for the Internet access service on train: business trip; other. The business-trip riders have the characteristics of high frequency and medium travel duration. The other type of target user has characteristics of low frequency and long travel duration.

For business-trip traveler, the proposed price is $39.99 per month. It is determined based on the following factors: preferred price point for monthly charge type; number of year needed to break even; preferred price point for daily charge type. This pricing point is equivalent to $2.04 per trip, and is at 0.6 standard deviation lower than the mean of the per-trip plan in survey. For the non-business-trip riders, the best price point is $3.4/hour.

To support these business model options, the technical team assessed the wireless technology options and trend; researched the US legal requirement and federal regulation; examined wireless standard and capacity; designed the simulation environments and conducted test using moving vehicle and roadside mobile connectivity equipments to research the hidden issues and the technical merit of the emerging mobile IP technology. The objective of the technical research is to devise the technology infrastructure which will stay on the technology grow path and with open standards.

The researched and selected technology options are summarized as follows:

- WiMAX can reduce the Trackside Infrastructure cost and make it better over 10 years
- Options to be considered are Direct WiMAX to the train or DSRC-like technologies, and
- Satellite communication is desirable for backup and emergency operations.

Table of Contents

Acknowledgement iii
Abstract v
Glossary xv
Chapter 1 Introduction 1
Chapter 2 Project Overview 3
  Project Objective 3
  Related Project 3
  Tasks 3
Chapter 3 Business Modeling 4
  Methodology 4
  Revenue Forecast 5
    Research and Survey Service Deployment on Internet Access via Wireless Technologies 5
    Research Historical Ridership Data on Trains of Intercity Rail 7
    Survey WiFi Users at SFO Airport 9
    Survey Wireless Service Deployment in Transportation Environments 9
    Conduct User Survey on Low-bandwidth Internet Access on Train 13
    Business Model Derived from Survey Data 13
    Research State of High-Speed Internet Access on Train 15
  Business Modelling 16
    Concept of Operation 16
    Business Strategy and Market Growth 19
    Business Model Options 21
Chapter 4 Regulatory and Legal Requirement 27
  FCC Trends in Unlicensed Spread Spectrum Devices 27
  Wireless Specifications 27
    IEEE 802.11b 27
    IEEE 802.11a 28
    IEEE 802.11g 28
    IEEE 802.11i 28
    IEEE 802.16 Wi-Max 28
  Enforcement 29
  Power Limits 29
  Equipment Limitations and Certification 30
    Interference 31
  Laws on Antennas and Towers 33
    Height Limitations 33
Chapter 5 Technical Options and Technology Trends 35
  What is the Reference Architecture? 35
    Mobile Internet for Train Commuters and Enterprise Network Architecture 35
  Open Standard Radio Technologies 36
  Connectivity to the Train 37
  Components of Network Architecture 38

Strategy 40
Wireless Security Suite 41
Key Policies In-Train 41
Advanced Security and Networking Services for Secure In-Train Rail Environment and Enterprise Network 42
Chapter 6 Conclusion 43
Summary of Problem 43
Approach 43
Recommendations for Future Research 44

Glossary

Caltrans – California Department of Transportation

CCJPA – Capital Corridor Joint Power Authority

WiFi – Wireless Fidelity

WiMAX – Worldwide Interoperability for Microwave Access

WISP – Wireless Internet service provider

SMER - Statistical Multiplexing Effect Rate is an estimate (ratio) of the effective bits transmitted during a period. For example, if the SMER is 20 % during an hour of connection, the actual time for transmitting data during an hour of connection is only 12 minutes.

Chapter 1 Introduction

Internet access service is now spreading everywhere. The number of Internet access points (Hot Spots) has been steadily increasing over the last years in various locations such as hotels, airports, rail stations, etc. There are today over 60,000 Hot Spots worldwide [i] of which one third are in the United States. Mobile internet becomes now the next challenge for many service providers. Ships, planes and trains are becoming connected to the outside world. For example, major airlines like Lufthansa, Singapore airlines, All Nippon Airways are now providing Internet access to passengers. The railroad sector is also catching up with this new effort to bring more productivity and entertainment possibilities to train travelers by offering Internet access while traveling. During the next five to 10 years, most rail system riders in North America and Europe are expected to have onboard wireless Internet access, according to some industry estimates [ii]. Currently, there are many applications in these regions mostly in the pilot stages. A few services are offered on a commercial basis: in the U.K, GNER (Great North East Railway), Virgin Trains from London to Birmingham, Manchester and Glasgow, and Southern Brighton Express; in Northern Europe countries and also between Paris and Brussels on the Thalys high speed trains. In India the service is offered by Railtel on the Delhi-Amritsar and Delhi-Bhopal train routes [iii]. Similar services are used by train riders in Canada and in the U.S. There is also a relatively new on-going research effort led by academic and industrial consortia. In Italy, Alenia Spazio and Eutelsat are implementing a system along the Rome-Florence line with the support of the European commission funding within the FIFTH (Fast Internet for Fast Train Hosts) program. Europe is also supporting a consortium of European industry led by the Alcatel group within the MOWGLY R&D project (MObile Wideband GLobal Link sYstem). The business side of these activities is still at infancy stage because the level of willingness to pay for the services is still unknown and the current business models for Internet access at home or at work are not directly applicable to mobile situations. Nevertheless, the potential benefit of mobile Internet service is too huge to be ignored.

Business riders have expressed a need to use their time more productively and efficiently during their commute by staying connected to their office network. Some of them may be able to get work credit for the time they spend working while commuting on train. Leisure travelers have also expressed interest in using online services. One way for passengers on trains to stay connected to their offices is to use Internet connectivity on the train. The Internet connectivity can also provide train operators the additional benefits: increased efficiency; improved safety increased train ridership.

[i] Dankberg A. (2005). Existing Wi-Fi systems and networks, *draft report*, Institute of Transportation Studies, California Center for Innovative Transportation, Berkeley.
[ii] BWCS ltd. (2003) Railway WI-Lan services, *report*.
[iii] http://newswww.bbc.net.uk/1/hi/business/3835525.stm

Offering Internet connectivity on the train, however, presents unique challenges. There is no existing commercial provider offering train riders with high-speed Internet access services. Thus, no service data are available for researching the revenue potential and cost structure. Furthermore, existing wireless technologies can only offer low-bandwidth infrastructure as a viable communication option. To accelerate users' adoption of the Internet connectivity service on train, the service needs to be offered based on an infrastructure with higher bandwidth and a secure operational environment.

Chapter 2 Project Overview

Project Objective

The objective of this project is to assist the Capital Corridor Joint Power Authority and the California Department of Transportation to assemble a decision framework for selecting wireless Internet access on behalf of customers riding the three California State sponsored Intercity Rail services. Wireless Internet access services will allow customers to conduct business or connect to the web for leisure, personal, or entertainment purposes. Wireless Internet access will also permit train operators to utilize the Internet to improve ticket collection, public safety, and implement other capabilities to improve operational efficiencies.

Related Project

This PATH project is complementary to another CCIT project, Task Order #12 – WiFi on Trains Deployment Support, currently being performed, and related projects being conducted in France as part of the CCIT CalFrance effort and the Central Japan Railway Company (CJRC).

Tasks

The planned tasks of this project were as follows:

1. Survey customers on the three California Intercity Rail services for wireless Internet usage and various price points:
    a. Survey Capitol Corridor customers who used any trial wireless services on the trains.
    b. Survey other customers who have not yet used wireless Internet connectivity on the train.
    c. Analyze survey results and develop an understanding of the demand/price points for wireless Internet market.
2. Research business model options.
3. Research technology options and industry technology trends.

Chapter 3 Business Modeling

Methodology

To formulate business model options, we surveyed and researched (1) the interest of train riders who are willing to pay; (2) the cost of infrastructure needed to support the business volume; (3) the potential value chain created by the deployed service. The potential value chain includes companies with functions in hotspot leadership, network provision, authentication and security, accounting and billing, roaming, content provision, marketing, customer service, content creation, distribution and aggregation.

The volume of interest and acceptable service price for end users were compared to the timeframe and cost of such a system implementation, and business directions for service were given to maximize value creation and customer valuation. The description of business models explains the cost and the revenue structure to expect according to the value chain. Since the value chain depends on the technological, regulatory, cultural and economical environments, comparing Californian, French and Japanese experiments could be useful to understand how the markets may experience take-off and growth. The challenges to implement such services and technologies in other countries are based on the experience obtained in all locations and experiment sites.

To develop a valid business model and options, we used the approach consisting of the following processes:

- Assemble the project team. The following team members were assembled:
  - Dan Lovegren, Caltrans manager.
  - Jim Allison, CCJPA manager
  - Professor Kanafani Principal Investiagtor and his students
  - Hamed Benouar, Project Director
  - Bensen Chiou, Project Manager
  - Jean-Luc Ignace, Visiting Scholar , INRETS
  - Kazuhiro Yamada, Visiting Scholar, Central Japan Railway Company.
  - Glocol, a subcontractor specialized in wireless technologies.
- Assess state of existing wireless services. The service can be WiFi hotspot, fix WiMAX deployment, satellite-based or cellular network-based services.
- Assess the pricing structures and wireless strategies used by various service providers.
- Examine available historical service data such as train ridership to gauge the market potential.
- Perform survey on users of wireless service, such as WiFi hotspot at major airport.
- Perform survey on train riders on trial service of low-bandwidth Internet access on the train.
- Formulate viable business model options.

Revenue Forecast

Offering Internet access on train will very likely increase the train ridership. The infrastructure and service will also enable many value added services. As a result, the revenue will be increased. The revenue forecast in this report doesn't include these potential revenue sources.

A multitude of business models for the provision of wireless Internet can be implemented which incorporate numerous revenue sources. Potential revenue lies in areas such as per use or time charges, subscription fees, advertising, sponsorship, or merely an increase in train ridership generated by the wireless service. Additional revenue, either through an increase in duration of wireless use or an increase in users, is possible through traditional, non-mobile provision of wireless capabilities in Capital Corridor stations. A seamless integration between the mobile and non-mobile aspects would increase use of the on-train services. In addition, a wireless system may decrease the operational cost or increase operational efficiency in such areas as security, ticketing, and marketing. The revenue source that lends itself most easily to forecasting is user fees. The benefits of a wireless Internet system may outweigh the costs even without the inclusion of user charges. If the increase in ridership, efficiency, or security is significant enough, user charges may not be necessary or wanted. This report merely forecasts what revenues may be generated by user charges.

Research and Survey Service Deployment on Internet Access via Wireless Technologies

The number of locations providing public wireless Internet access has increased very rapidly in the early part of the 21st century. There are nearly 60,000 of these hotspots. The types of locations have become increasingly diverse. Nearly 17,000 are in hotels, 10,000 in restaurants, 10,000 in cafes, and 1,000 at airports.

There are also an increasing number in train stations and bus stations, with improving technology allowing for access on plans, trains, and vehicles worldwide, of which over one-third are in the United States. Tens of thousands of these WiFi hotspots are owned by major wireless service providers (WISP) such as iPass, Boingo, T-Mobile, and SBC.

Since wireless Internet technology is relatively new, especially for public commercial use, it is quickly evolving in wide-ranging industry. There is no universally accepted method of providing connectivity or common business plan, even for a use as specific as on-train access. The industry has yet to consolidate, resulting in a wide range of pricing options and providers. To best determine the appropriate business model for a new wireless location, it is helpful to examine business models used at other existing locations. Such analysis can determine what prices the market will bear, unique ways of funding the service, as well as what level of service the customer is expecting or desires.

The focus of this project is to provide mobile wireless Internet access to trains. Within the wireless on trains industry, technology varies from two-way on-board satellite systems to those with track-side routers communicating with a speeding vehicle. Since there are very few operational on-board wireless Internet systems, access locations on other transportation vehicles, such as busses and planes are examined. An on-train wireless system is part of a broader competition among transportation modes, and therefore must provide similar or better access and prices to increase ridership.

As mobile wireless technology is still in its infancy, the Wireless Fidelity (Wi-Fi) systems at transportation terminals are examined as well. These terminal locations are frequently a precursor to on-board systems and can be used for assessing and developing customer interest. With the inevitable industry consolidation, all of the wireless access points may be connected to a handful of Wireless Internet Service Provider (WISP) networks or aggregators, with similar structured pricing plans. This would give the consumer the greatest accessibility since signing up for numerous access accounts, and facing charges from numerous providers, will not be required. Once the technology is better developed, mobile wireless systems will likely join these large networks and be governed by their pricing structure. To some extent, this has already happened with the Connexion system, available on several commercial flights. Therefore, the project team also examines WISP pricing structures and determines access fees and existing access locations.

The last part of this activity integrates all of the material covered in an attempt to guide the creation of a business model for an on-train wireless system. The technologies used on trains and the companies developing those technologies are examined in greater detail. The business models used on transportation systems, at transportation terminals, and on wireless hotspot networks are summarized and compared. To compare pricing plans, sample usage patterns were developed, and the results are charted to provide a picture of existing access options and prices. Some trial and operational usage data are given as well, as a tool for determining the assimilation of mobile wireless systems.

We examined the following WiFi services on trains:

- United Kingdom on-train wireless system operated by Icomera AB.
- Linx trains running between Sweden and Denmark operated by Icomera AB.
- Wireless Internet trials on VIA trains between Montreal and Toronto operated by a joint venture of Bell Canada, Intel and PointShot Wireless.
- Wireless on ACE trains, running from Stockton to San Jose operated by PointShot Wireless.
- Wireless access in Stockholm, Sweden powered by Fujitsu-Siemens systems.
- Internet access on trains from London to Brighton designed by Nomad Digital.

There are several WiFi services on train under development:

- Icomera will install a 3G/satellite system on 85 trains in SJ- Scandinavia
- Broachreach and PointShot is implementing Internet access on Virgin Train in UK.

- The India government-operated rail and telecommunications company is installing trackside devices that will provide Internet access to passing trains as part of a nationwide connectivity project.
- Eurostar is installing wireless Internet capabilities using some form of satellite/cellular system. Thalys is pursuing the same goal on its Paris to Brussels high speed train route
- Alenia Spazio and Eutelsat are implementing a system on the Rome-Florence line to have Wi-Fi enabled trains by 2008-09.
- The Seattle Monorail Authority issued an RFQ in early 2004 for Internet service on its line.

On airplanes, the following WiFi services are available:

- Boeing Connexion has roaming agreements with iPass, InfoNet, NTT DoCoMo, T-Systems, Starhub, NTT Communications and Singtel, allowing users of each of those networks to use Connexion with their existing plans.
- Verizon Airfone offers low bandwidth Internet connectivity for email and instance messaging.
- Alitalia is testing a system to provide email coverage to airline routes flying between America, Europe and the Middle East.

In surface transportation, the following WiFi services are available or under developments:

- RaySat's SpeedRay offers Internet, digital TV and music access via a two-way satellite connection.
- Appear Networks and Cisco installed a wireless Internet system that was developed for a bus route in Paris.
- LimoLiner in New York City and Boston provides wireless Internet access on its vehicle.
- The Hampton Jitney provides Internet access on the bus from the Hamptons to New York City.

Other wireless services:

- WiFi service on ships, ferryboat, cruise lines, transportation terminal, highway rest stop, train station.
- Stationary WiMAX based services.
- Wireless service based on wide area network and city-wide network.

For the detail information, please see Appendix A – Worldwide WiFi System and Network

Research Historical Ridership Data on Trains of Intercity Rail

To forecast the revenue stream, historical ridership data were obtained from CCJPA. The period primarily analyzed was from September 1, 2004 to March 31, 2005.

Number of Riders

A few trends are noteworthy in the data. Weekday ridership is significantly higher than weekend ridership. With exceptions for holidays, weekday ridership generally ranged from 3,000 to 5,000 trips per day. Weekend ridership ranges from approximately 1,500 to 2,500 trips per day. Over that period, weekday ridership trended upward by 0.8 trips compared to 0.5 trips downward for weekend ridership. Revenue forecasts based on the historical ridership are conservative in that they do not attempt to predict how many people will switch from their cars to the train as a result of the increased service.

Travel time

The duration of the travel time of train riders is likely a major factor that riders use to decide to use Internet service on the train. A user traveling two hours will gain more benefit from being productive during that period than a user traveling for 30 minutes who barely has time to start his/her computer. Therefore the ridership data were analyzed based on travel time and are disaggregated by origin and destination (O-D). The average weekday and weekend-day origin-destination (O-D) ridership was determined. The train scheduled is analyzed to determine the time that a user will be onboard and therefore would have access to the wireless services.

Travel frequency

The distribution of the riders' trip frequency is important in determining what type of pricing plans to offer and therefore the impacts on the total revenue projection. It is expected that daily commuters will prefer a monthly plan and will wish to only pay a flat fee for a month's worth of use, while the occasional traveler will pay a per hour price. Those that ride everyday will gain more from Internet access because they may be able to reduce their in-office time by billing time spent on the train. In addition, they will gain tens of hours of productivity time over the course of a month or even week. The occasional vacationer or business traveler may only gain a short amount of productivity time or enhanced leisure, which likely has less value. To determine the type of rider currently on Capital Corridor trains, passenger survey data were obtained from the CCJPA. In particular, questions regarding the type of trip, the frequency of the trips, and the origin and destination of the trip were examined. Just over 50% of riders who travel over 20 times a year (barely more than one trip a month) are on their daily commute to or from work. It is likely that this 50.2% of riders will be the primary users of the services. An additional 27.5% of riders traveling 20 or more times are on their commute to or from work, but they don't use the train on a daily basis. Of all riders, 14% travel 300 or more times per year, 11.8% travel 151-300 times per year, 5.2% travel 101-150 times per year, 20.2% travel 20-100 times per year, and 48.8% travel less than 20 times per year.

Survey WiFi Users at SFO Airport

To understand the state of the WiFi usage and awareness of the general traveling public, a survey (1,100 forms distributed, 1092 forms collected) was performed at San Francisco Airport. Based on the results, we observed the following characteristics:

- 202 traveling correspondents had their laptops with them.
- 60% of travelers knew of WiFi, used WiFi for office, e-mail and internet surfing.
- Users would use WiFi more than 1.6 hours than they used now, if it was cheaper.
- Additional likely uses for WiFi were streaming video and games.
- Of those surveyed, the Internet service used at home was based on DSL or cable.
- The survey respondents expressed needs for high speed connectivity.

Survey Wireless Service Deployment in Transportation Environments

We also researched and examined the service deployments and related pricing strategies in transportation systems, transportation terminals and hotspot network providers.

Transportation Systems

There are very few examples of mobile on-board Internet access pricing structures. The majority of on-board wireless systems are in a trial phase and as a result are free. Several systems bundle access with a first class ticket. Companies offering bundled access include PointShot, Icomera, and Zealconnect. The Northern California ACE rail line provides free access through corporate support. The only systems currently offering subscription plans are on-automobile two-way satellite providers. These plans start at $60 per month, but they aren't comparable to on-bus or on-train systems because they provide only stationary access and aren't designed for commercial distribution of bandwidth. There are a few time-based purchase options. Two of these, WiFirst and Meteor provide access along an RATP bus line. On-airplane systems generally charge by use or by flight segment. Such systems include Connexion, Netvigator and Tenzing. There are too few existing pricing structures for in-motion on-vehicle devices to develop some sort of clear picture of the user's willingness to pay. In each case, a unique factor such as the lengthy user capture on a cruise line, the generally higher European rates, or the lengthier duration of an international air trip prevent application of these price structures to use on Amtrak trains in the U.S. The Nomad Digital system being installed on UK trains is groundbreaking in that it is the first mobile system aligned with a Wireless Internet Service Provider (WISP) network, in this case T-Mobile. It is seamlessly integrated into the T-Mobile network and is charging the same rates as all other T-Mobile UK hotspots. This will likely be more common for mobile systems in the future since it provides the most convenient access to the passenger.
the commercial usage was supposed to be launch in July 2005 but the service is still in testing mode

A 2004 data survey, published by BWCS Ltd.[ii] – a telecom consulting firm, forecasted that rail passengers will spend $420 million per year on mobile Wi-Fi services by 2008. The survey, conducted with 1600 UK rail passengers, yielded the following results [iv]:

- 78% of business travelers are interested in using Wi-Fi on the train;
- 72% would be persuaded to take trips via train rather than by auto or plane;
- Users are willing to pay $9.27 per hour on a per minute basis or a flat fee of between $9.27 and $14.82 for trips under two hours and between $12.97 and $22.24 for trips over two hours;
- Users are willing to pay between $27.80 and $46.33 per month for unlimited access; and
- 65% expect to pay via credit card or their existing WISP, and 28% expect it to be bundled in the price of a ticket.

The results of the survey, given in British Pounds, were converted to American Dollars. One must keep in mind the generally higher Wi-Fi access fees and train ticket costs in the United Kingdom and Europe before applying these results to train systems in the United States. Also notable is that the survey was conducted with commuters already using rail.

In an unrelated poll of air passengers, 80% indicated that the availability of Wi-Fi connectivity could affect their decision on which carrier to fly. Only 18% of the respondents are willing to pay more than $10 for the service, while 41% expect it to be free.

Transportation Terminals

Transportation terminals can provide more examples of public wireless Internet access pricing structures. A few airlines bundle access into their first class lounge fees. Several airports and rest stop operators provide free access as an informational feature or use generator. Monthly subscription plans are available from a few companies. These plans range in price from $19.95 to $29.95. The most common consumer purchase option is the 24 hours of continuous access plan. Airport wireless providers such as Concourse Communications, Massport and HMS Host, as well as road-side providers Flying J and Freedom Net, give this purchase option to their customers. One-day continuous access costs between $4.95 and $7.95. Thirty-day continuous access is also available from marina operator iDock and a few roadside operators at a price range of $24.95 to $49.95. Several hotspot network operators, such as AT&T, Bell Canada, Boingo, BT Openzone, ICOA, iPass, Kubi Wireless, and Orange have hotspots at several transportation terminals. Access fees charged at these locations are the same as at other hotspots on their network. Therefore their fees will be analyzed in the next section.

[iv] http://www.wirelessdevnet.com/news/2003/aug/29/news1.html

Hotspot Network Providers

In most cases, various hotspot locations provide the same level of service, whether it is in a coffee shop, a McDonalds or an airport lounge. Therefore, one would expect their prices to be similar. A market research study of European hotspots determined that prices in an area are uncorrelated with density of hotspot providers in the area. A few of the operators charge per minute or megabyte, or offer scalable packages. Therefore the plan chosen by the user and the fees incurred depend on the frequency and duration of usage. In addition, while most operators offer a per-hour or per-day purchase option, those are certainly not the only access options a user may face. The fees charged by 45 different hotspot operators were catalogued and plotted. All of the available subscription and time plans were listed.

The most common type of time duration access option was the monthly subscription, provided by 29 of the 45 operators. Only 7 of the 25 North American operators did not have a monthly option. The second-most common option is the 24-hour continuous usage plan, offered by 27 operators. Eighteen have a per-hour fee, and 12 have a year-long subscription option. Other time duration options provided by several operators include per minute, per 15 minutes, per 30 minutes, per 120 minutes, and per week.

Indiscriminate of the type of usage pattern, North American wireless providers charged far less than their international counterparts. The average price for one hour of continuous service worldwide is $7.77, and only $4.02 in North America. A BroadGroup study of 122 European providers determined that 50% offered the one-hour pricing option, with an average price of $7.33, close to the average calculated in this study. They noted that the average price for one hour of Wi-Fi access in Europe fell 11% in 2004. The average price for 24 hours of continuous service from the providers in this study is $19.27, but only $8.28 for the 25 North American providers analyzed. The BroadGroup study calculated that 58% of those studied offered the 24-hour pricing option, with an average price of $19.25, also very close to the average calculated here. The average month-to-month subscription in this study is $45.85, but only $32.49 in North America. The average monthly or pre-paid year-long subscription is $584.23 ($48.69 per month), and in North America is $306.91 ($25.58 per month). The per-minute rates were similar ($0.24 worldwide and $0.23 in North America), but that is likely due to the small number of operators providing that option. To show this contrast, as well as to allow the North American prices to be easily separated, the North American and non North-American prices were plotted in different shades. The non-North American prices are plotted in a lighter shade of the same color as the North American prices.

In Figure 1, of Appendix A, the time in minutes is plotted against the fee for that period, both on a logarithmic scale. In this case, the usage pattern determines actual fees incurred for those plans with variable pricing dependent on mega-bytes of data transferred or minutes in the session. The plans were converted into the number of minutes that a user could theoretically use the plan, for example the minutes available for a year-long plan is the number of minutes in a year. One can see that there are a few outliers, but for most time durations, North American operators were exclusively cheaper than their international counterparts. This is especially noticeable in the 24-hour and year-long plans. Those time durations only offered by one or two providers, including 10 minutes, 4 hours, and 6 months, were not plotted on the charts.

Since users won't actually use the wireless Internet every minute of a 24-hour period, let alone every minute of the month, the price per minute of use for each of the plans was analyzed. This is the rate at which a user will pay per minute of actual Internet usage. Four different usage patterns were used in this analysis, and they are plotted in Figures 1-4, see Appendix A:

- A frequent, short duration user who mainly checks their e-mail15 minutes per use,
    - 5 uses per week for a total of 300 minutes and 10 MB per month;
- A frequent, medium duration user such as a train rider
    - 60 minutes per use, 5 uses per week for a total of 1200 minutes and 20 MB per month;
- An occasional, long duration user such as an airport user;
    - 120 minutes per use, 0.5 uses per week, for a total of 240 minutes and 10 MB per month;
- An occasional, very long duration user such as one who may use Wi-Fi for business
    - 240 minutes per use, 2 uses per week, for a total of 1920 minutes and 40 MB per month.

The fee for each time period was divided by the amount of time the user would use the Internet, according to these usage patterns, to come up with the fee per minute. For the frequent, short duration user, the cheapest option is the year-long plan, which costs an average of $0.16 per minute ($0.09 in N. America). The most expensive is the day-long plan, which costs an average of $1.31 per minute ($0.54 in N. America). While there is a large discrepancy between the rates of North American and international providers, the type of plan that is cheapest to the user is similar. For the frequent, medium duration user, the cheapest is the year-long plan at an average of $0.04 per minute ($0.02 in N. America). The most expensive is the day-long plan, which costs an average of $0.33 per minute ($0.14 in N. America). For the occasional, long duration user, the cheapest is the per hour plan at an average of $0.13 per minute ($0.06 in N. America). The most expensive is the per week plan, which costs an average of $0.38 per minute ($0.18 in N. America). For the occasional, very long duration user, the cheapest is the per-year plan at $0.03 per minute ($0.01 in N. America), and the most expensive is the per-minute plan at $0.24 ($0.23 in N. America).

In summary on researching and assessing the world-wide deployment, historical data shows:

- There are two distinct groups of user:
    - A. occasional and long-duration trip;
    - B. frequent and medium-duration trip
- Cheapest pricing for type A user: Per-hour plan ($0.13/minute world-wide, $0.06/minute for North America)

- Most expensive pricing for type A user: Per-week plan ($0.38/minute world-wide, $0.18/minute for North America)
- Cheapest pricing for Type B use: year-long plan ($0.04/minute world-wide, $0.02/minute for North America)
- Most expensive pricing for Type B use: day-long plan ($0.33/minute world-wide, $0.14/minute for North America)

Conduct User Survey on Low-bandwidth Internet Access on Train

There are many potential markets for the service of Internet access on train. For example, existing train riders may increase their travel by train or pay the service. Offering service of Internet access on train may also potentially attract those travelers who currently do not travel by train. As a result, the train ridership may likely increase. The potential market of the non-train riders can be assessed by performing a carefully designed survey on the population in towns and cities along the route at least one hour away from major destinations of train ride. Due to the limited resource, the assessment of this potential market is out of the scope of this project. This assessment may be performed by future follow-up activity. This section only covers the survey on the train riders.

During the project period, PointShot Wireless, Inc., a Canadian company, conducted a trial wireless Internet service on Capitol Corridor trains. To help better define service implementation options and make it easier for the state to select a business model and vendor for the service, the project team performed the following survey activities:

1. Designed a survey form as the Appendix D – Wireless Internet (WiFi) Survey.
2. Conducted the survey on the three state InterCity Rail service. Over 1,100 survey forms were distributed to users in different time of the day and at different origin and destination. There were 1,092 responses.
3. Data entry and cleansing. The result of focus group survey is depicted in Appendix E – Data Analysis on Survey Data.
4. Extract the survey result and refine the business model.

Business Model Derived from Survey Data

Type of traveler

Of those who completed and returned in the survey form, 67% were business users, and 33% were non-business user.

Willingness to pay for service in business and non-business traveler

This number has to be compared to the number of riders traveling with a wi-fi equipped laptop computer

Of the business users,

- 44% expressed willingness to pay for the service
- 56% expressed interest to use the service if it is free.

Of the non-business users,

- 20% expressed willingness to pay for the service
- 80% expressed interest to use the service if it is free.

Effect of travel time on business users' willingness to pay for service

The travel time of the train rider plays an important role in users' willingness to pay or not for the service.

- Of those business users who travel for less than 80 minutes,
  - 26% expressed the willingness to pay for the service
  - 74% expressed interest to use the service if it is free.
- Of those business users who travel between 80 and 185 minutes,
  - 51% are willing to pay to use the service.
  - 49% expressed interest to use the service if it is free.
- Of those business users who travel for more than 185 minutes,
  - 54% expressed willingness to pay to use the service.
  - 46% expressed interest to use the service if it is free.

Pricing Structure

To research the best pricing structure, several strategies are investigated: by hour, by trip, by day, by month.

Charge by hour

For the option of charging service by hour, the average hourly rate for those who are willing to pay for the service is $2.80.

- Those who travel for less than 60 minutes one way, the mean hourly rate is $3.40.
- Those who travel between 60 and 312 minutes are willing to pay $2.60.
- Those who travel more than 312 minutes one way are willing to pay $1.90 hourly.

Charge by trip

For the option of charging service by trip, the average amount the train riders are willing to pay is $4.40 a trip.

- Those who travel less than or equal to 99 times a year, the average amount is $5.40 a trip. Within this sub-group,
  - Those who travel for over 100 minutes are willing to pay for $6.50 a trip.
  - Those who travel less than or equal to 100 minutes are willing to pay $5.00 a trip.
- Those who travel more than 99 times a year are willing to pay $3.20 a trip.

Charge by day

For the option charging service by day, the average maximum service charge users are willing to pay per day is $6.40.

- For those who travel for less than and equal to 20 time a year, it is $8.80 a day.
- For those who travel between 20 and 80 times a year, it is $7.20 a day.
- For those travel more than 80 times a year, it is $5.00.

Charge by month

For the option of charging service by month, the average amount the train riders are willing to pay is $20.30 a month.

For the detailed analysis on the data collected from survey, see the Appendix E – Data Analysis on Survey Data.

In summary on the result of survey, the analysis of survey data shows:

- The average maximum price per hour is $2.84. It's $3.42 for occasional travelers and $1.92 for frequent travelers.
- The average maximum price per month is $20.32. It's $18.33 for occasional travelers and $26.34 for frequent travelers.
- The average maximum price per trip is $4.44. It's $5.42 for occasional travelers and $3.18 for frequent travelers.
- The average maximum price per day is $6.41. It's $7.2 for occasional travelers and $5.02 for frequent travelers.

Research State of High-Speed Internet Access on Train

The existing WiFi-on-trains services or those under development are mostly based on the low initial cost-low bandwidth infrastructure. To formulate a viable business model and the infrastructure supporting the projected growth of usage, the project team also researched the state of service deployments based on high-speed Internet access on trains.

T-Mobile recently announced that the world's first genuine broadband Wi-Fi service on trains is available to passengers on the London to Brighton rail route. Passengers on Southern's express rail service between London and Brighton - one of the busiest railway routes for business people traveling to and from London - are able to send and receive emails or surf the Internet securely all while traveling on the train.

The service is made possible through a partnership with Southern (who provides access to the trains and station locations where the service is offered), Nomad Digital (who provides the technology) and T-Mobile (who offers the Wi-Fi service to customers).

Since this is the first broadband Internet access on the train, we have researched its service and any issues it encountered and contacted the network vendor designing and maintaining the trackside wireless infrastructure. We also invited the technology vendor to present the inner knowledge of its infrastructure and, to some extent, the organizational relationships among all the players.

The information on this service will be used for further refining the business model and technical design created in this project.

Business Modelling

The project team has utilized all the information gathered and the available data collected and cleansed them to formulate the concept of operation and the business model.

Concept of Operation

To aid the design and development of the infrastructure, the project team has discussed and developed the Concept of Operations to depict and guide the design of the service. There are two modes of operation: Configuration and Operation.

Configuration Mode

The operations in the Configuration mode are those needed to install, configure, and manage the infrastructure, and to provide the user with service.

The type of user performing the tasks in the Configuration Mode are Transit Administration staff (IT, infrastructure engineering or service supervisor), the administrator of the service provider, and the security officers handling infrastructure protection or other homeland security applications. The operations and the users in the Configuration mode are depicted below:

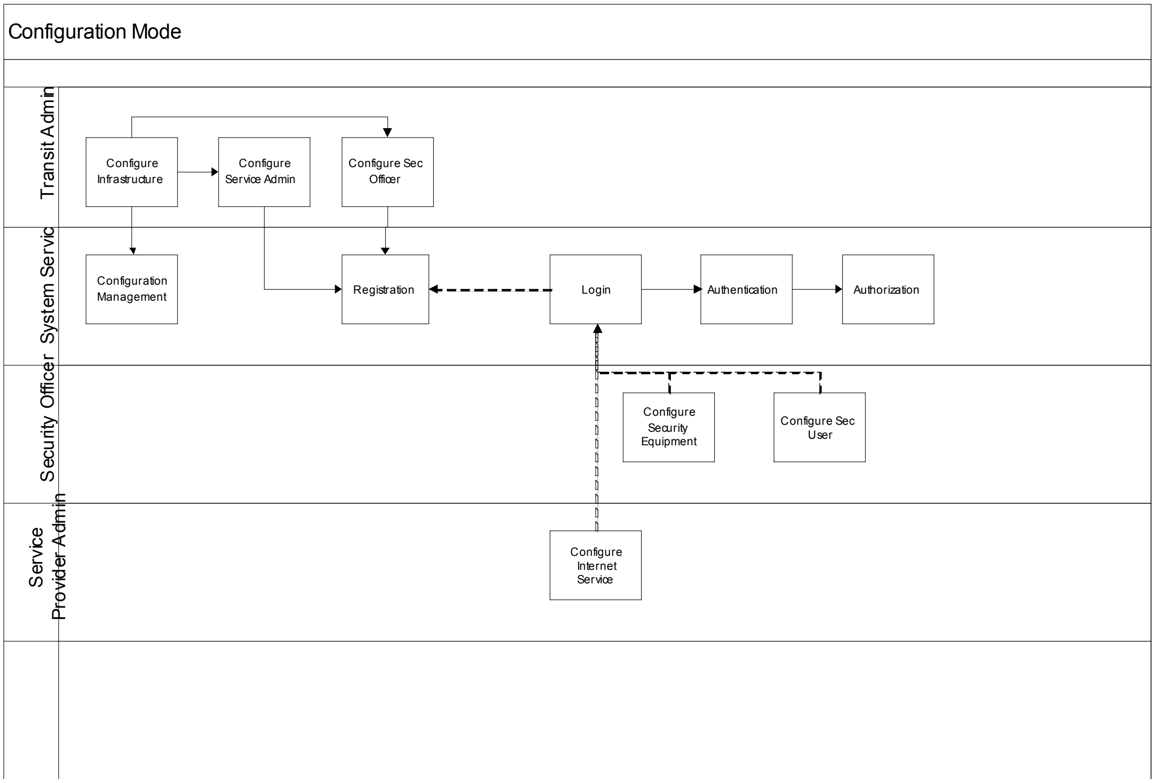


Figure 1 : Configuration mode operation

Operation Mode

The operation mode consists of operations mainly for end users to use the service, the service provider's administrator to monitor service use or for security officers to perform the security related tasks. The operations and the users in the Configuration mode are depicted below:

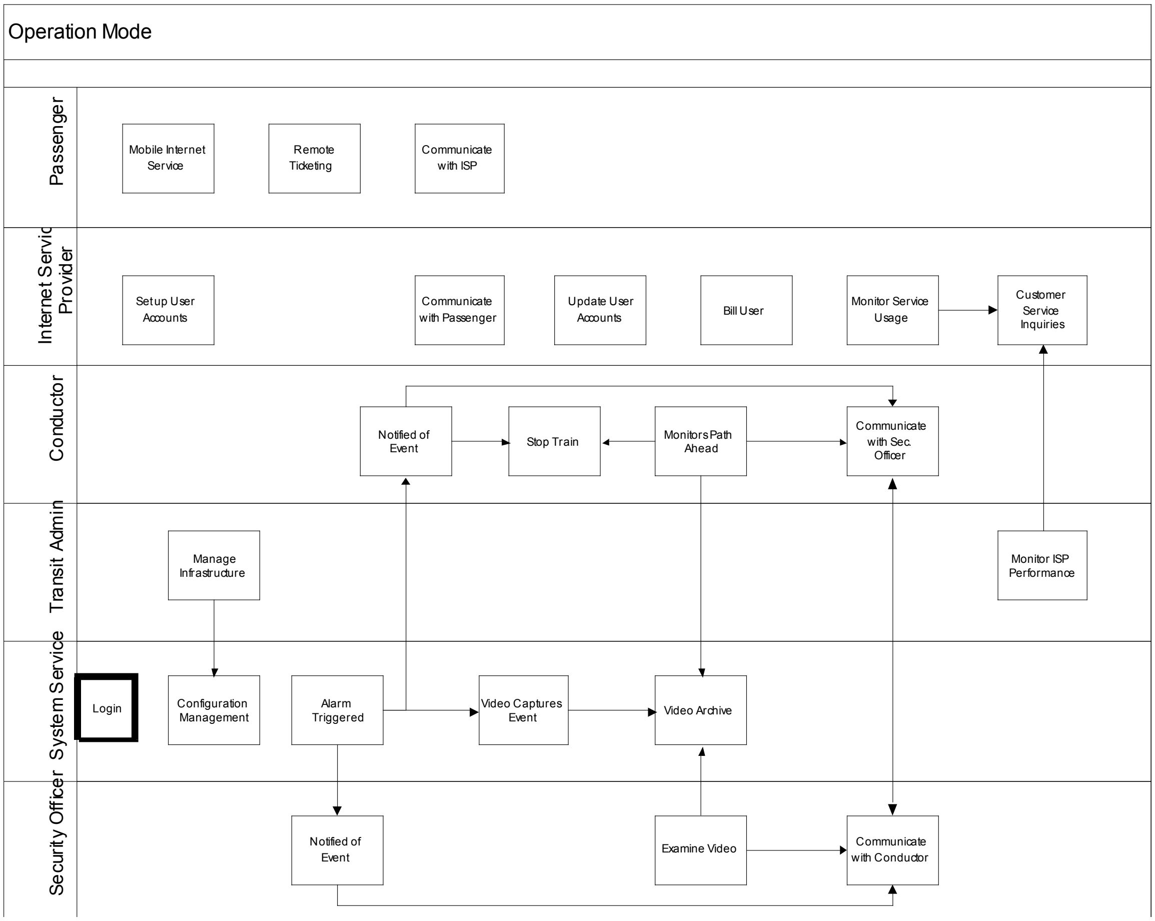


Figure 2 Operational Mode Operation

Business Strategy and Market Growth

After thoroughly assessing the worldwide WiFi deployment, examining train ridership, and surveying the train riders on the trains of the three State InterCity Rail services, the project team has developed two viable business model and technology options: conservative and maximized market. The conservative model option requires low initial cost with relatively high running cost and low revenue potential. The maximized market model option has high revenue potential, potential value-added services and low running cost. It however requires high initial capital cost.

Conservative - Low initial cost/high running cost – low revenue

The amount of cost depends on the subscribed bandwidth. It is low with low bandwidth; it is higher with higher bandwidth. The target population (the number of expected customers) is also an important parameter influencing the cost for deploying the technological solution. In other words, the bandwidth needed is directly linked to the number of customers using the service.

This model option is aimed at capturing the business of mobile Internet services on trains in a conservative strategy. It utilizes the communication model of the combined satellite and cellular networks. In two cars of each train, there are WiFi hotspots connected to the outside world by satellite transponder for downlink and cellular using single carrier, radio transmission technology for uplink. We have estimated the bandwidth needed to support the usage volume, and thus the costs needed for the equipment and leased communication lines.

Maximized Market - High initial cost/low running cost – high revenue

This model option is aimed at capturing the business of mobile Internet services on the train as much as the market grows. It requires a communication model with high-bandwidth infrastructure consisting of an on-board WiFi network and trackside infrastructure based on Worldwide Interoperability for Microwave Access (WiMAX), mobile IP technology and fiber-optics. This model can support a large number of users and additional value-added services such as homeland security due to the much higher bandwidth it provides.

Market growth

It is very difficult to project the growth of the market since there are no available service data to support the valid projection on the type of target deployment environments similar to the service routes of State Intercity Rail. The project team has researched many appropriate ways to project market growth and finalized on the following two strategies:

- Derive a projected market growth rate based on the assessment of the worldwide deployment of WiFi and other wireless services.
- Derive a projected market growth rate based on the results of the survey of individuals riding the trains containing cars equipped with infrastructure for providing the Internet access service with low bandwidth communication infrastructure.

Market growth based on worldwide WiFi service deployment

We have performed the research and assessment of the service deployments in various countries such as US, UK, Sweden, etc. and the evaluation conducted by TGV in France (Paris-Lyon) and the Shinansen in Japan (Tokyo-Osaka). Based on the assumption of 5% of travellers who would pay for the WiFi connection on the train and are willing to pay $5 on average per trip (the average effective connection time would be 36 minutes on average, with a Statistical Multiplexing Effect Rate (SMER) of 20% (effective transmission ratio), and the market would grow 2% a year. The revenues and cost projections are shown in Figure 3 and Figure 5.

Market growth based on user survey

Based on the results of the user survey conducted by the project team in July 2005 on trains of State Intercity rail, 17% of users who usually travel with WiFi equipped laptop are willing to use and pay the service. The revenues and cost projections are shown in Figure 4 and Figure 6.

There are two distinct subgroups of users in terms of the users' perception of the service and willingness to pay for the service: those who already used the trial service and those who have not used the trial service.

Users already used the trial service

The results of survey indicate that, for those who have already used the trial Internet access on the train are willing to pay $3.50 on average per trip (average 82 minutes of effective connection –survey results with a 20% SMER). The cost per trip is calculated as an average value obtained from the different mode of payments (per hour, per trip, per day, or per month) as stated in the survey.

Users not used the service yet

The results of survey indicate that, for those who have not used any Internet access on the train are willing to pay $5.30 on average per trip for average of 82 minutes of effective connection. The cost per trip is calculated as an average value obtained from the different mode of payments (per hour, per trip, per day, or per month) as stated in the survey.

Analysis of difference between those who tried the service and those who has not

The service fee that train riders are willing to pay is $3.50 for those who already used the trial service vs. $5.30 for those who haven't used the trial service. The difference is very likely caused by the poor quality of the trial service due to the limited service availability and low bandwidth of infrastructure supporting the service.

Since there are only two cars in trains at specific times, and the deployed trial service is based on the low-initial-cost/high-running-cost with low-revenue-potential, the quality of trial service may damper the willingness of users to pay for the service. Besides, the train schedule of which one or two cars are equipped with the service is not fixed or unpredictable, thus that may further erode the train riders' willingness to pay for the currently deployed service. We believed that if the service is offered with good quality, a predictable schedule, high bandwidth and service ubiquity, the users' willingness to use and the amount to pay for the service will very likely be increased.

Business Model Options

There are four possible business model options depending on the revenue potential and the projected market growth with a 10-year deployment timeframe: low revenue based on service assessment, low revenue based on user survey, high revenue based on service assessment, high revenue based on user survey.

Low Revenue based on service assessment

The plotted lines of revenue and cost, numbered according to the order of lines at year 10 are as follows:

1. Revenue $5 per session, 5% users, 2% net increase per year
2. Revenue $3 per session, 5% users, 2% net increase per year
3. Cost for low simultaneous usage with 85 kps downlink, 21 kbps uplink, SMER 20%
4. Cost for high simultaneous usage with 266 kps downlink, 66 kbps uplink, SMER 20%

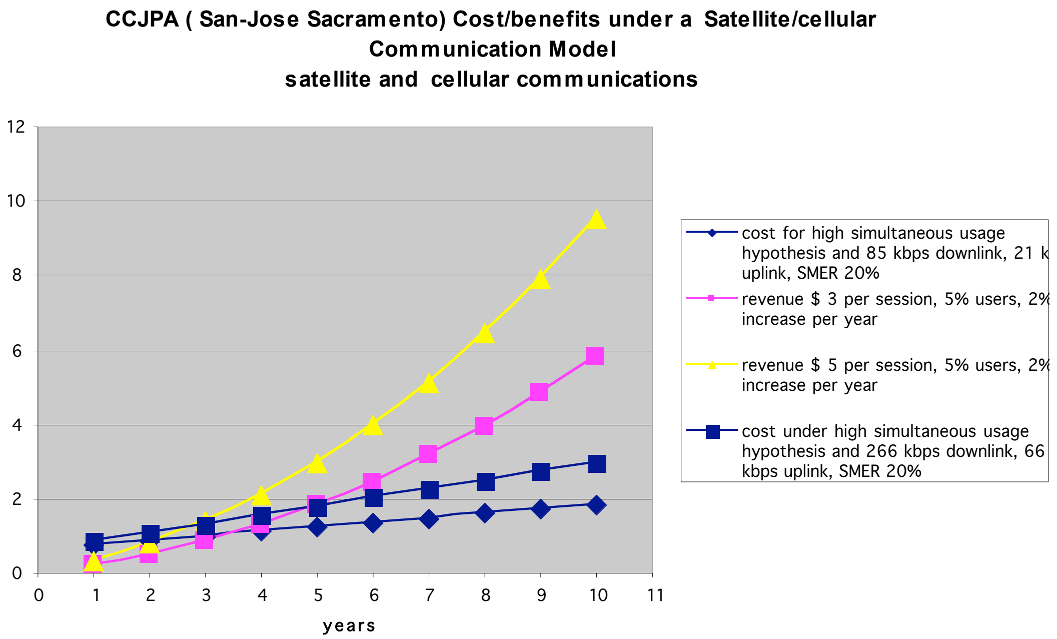


Figure 3: Revenue/cost using higher satellite downlink and cellular uplink bandwidth

Low revenue based on user survey

The plotted lines of revenue and cost, numbered according to the order of lines at year 10 are as follows:

1. Revenue $5.3 per session (upper limit), 17% users, 2% net increase per year
2. Cost for high simultaneous usage hypothesis and 266 kbps, downlink, 66 kbps uplink, SMER 20%, 82 min average connection time
3. Revenue $3.5 per session (lower limit) , 17% users, 2% net increase per year.
4. Cost for high simultaneous usage hypothesis and 85 kbps downlink, 21 kbps uplink, SMER 20%, 82 min average connection time.

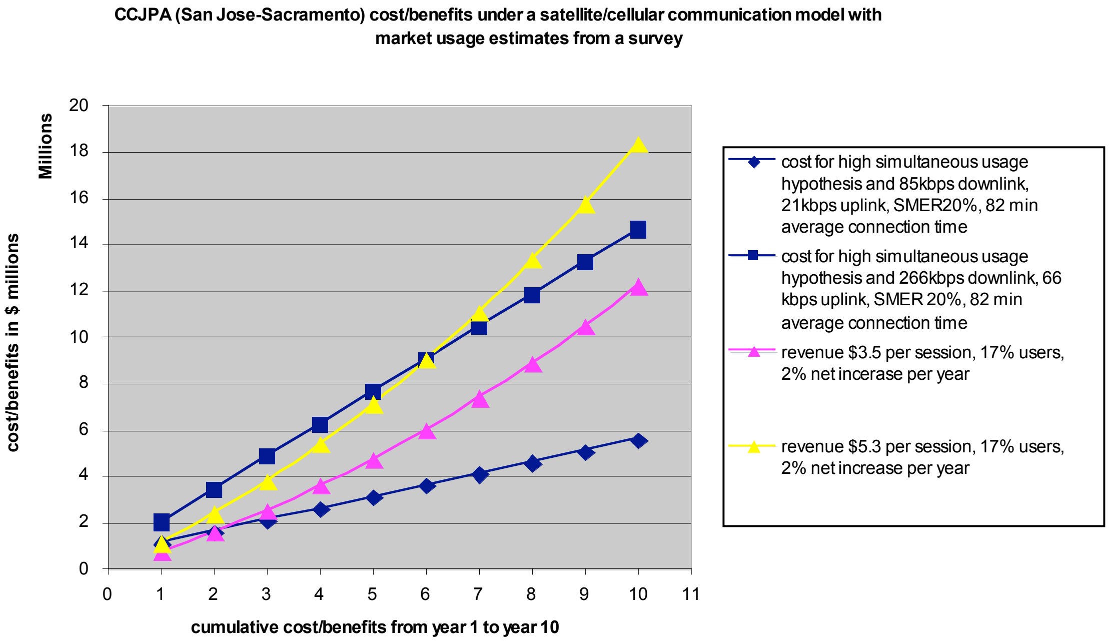


Figure 4: Benefit/cost using lower satellite downlink and cellular uplink bandwidth

High revenue based on service assessment

This model utilizes the dedicated communication network along the tracks with 4 mega kbps (uplink and downlink). The plotted lines of revenue and cost, numbered according to the order of lines at year 10 are as follows:

1. CCJPA cumulative investments including installation cost.
2. Revenue based on $5 per trip.
3. CCJPA cumulative cost if 50% cost sharing with other partners.
4. Revenue projection based on $3 per trip.

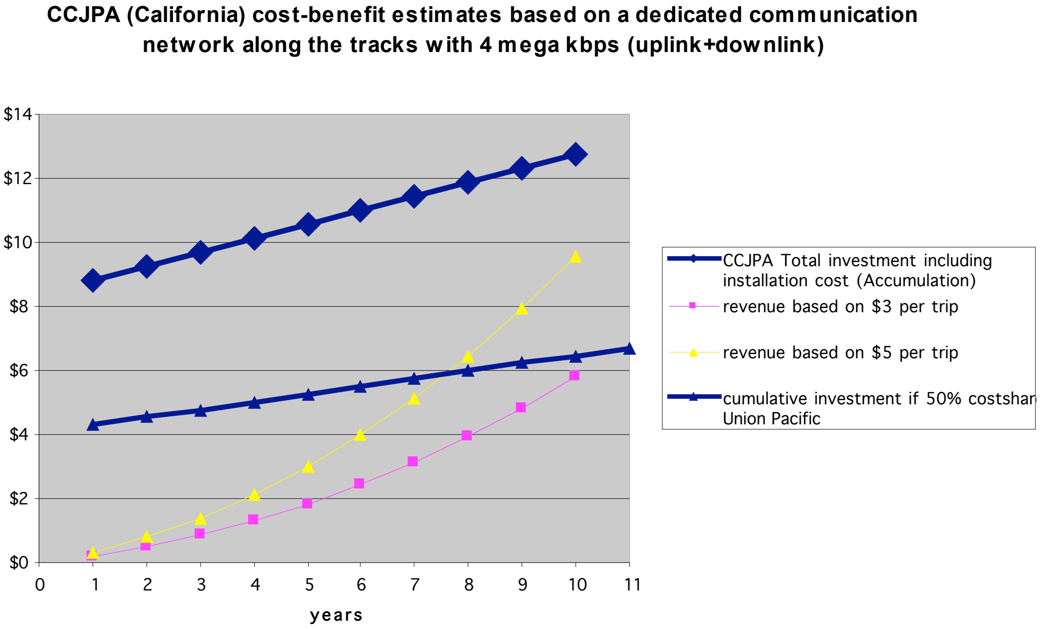


Figure 5: Benefit/Cost using trackside infrastructure w/o cost sharing

High revenue based on user survey

This model utilizes the dedicated communication network along the tracks with 4 mega kbps (uplink and downlink). The plotted lines of revenue and cost, numbered according to the order of lines at year 10 are as follows:

1. Revenue based on $5 per trip.
2. CCJPA total cumulative investment including installation cost.
3. Revenue based on $3 per trip.
4. CCJPA total cumulative investment if 50% cost shared with other partners.

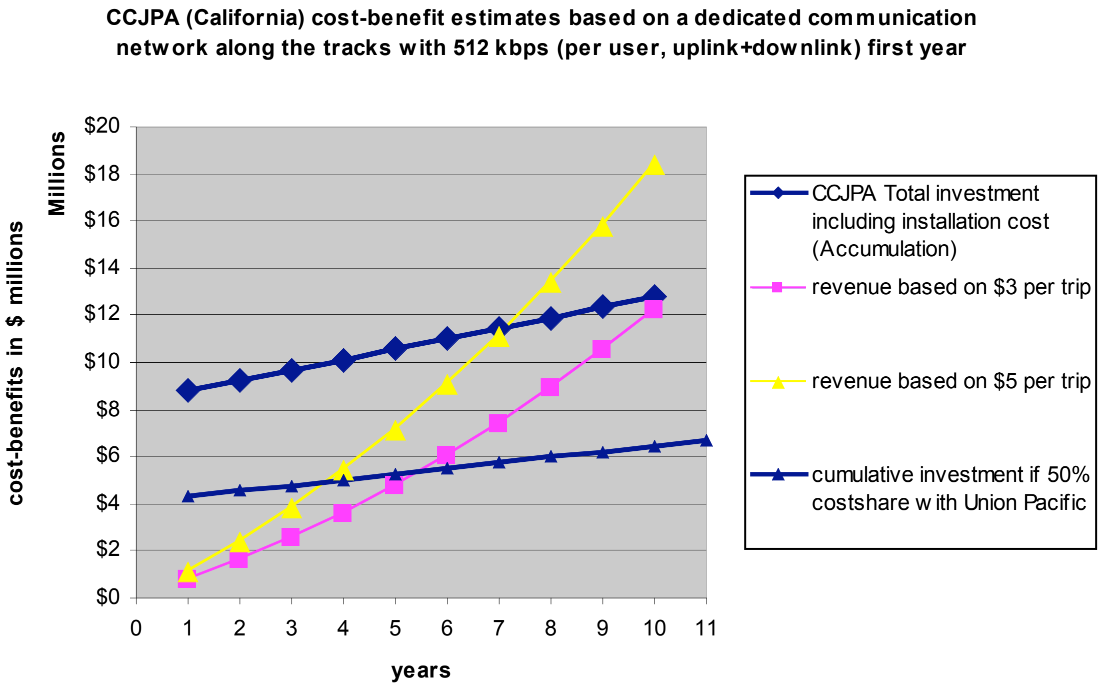


Figure 6: Benefit/Cost using trackside infrastructure with 50% cost sharing

For detail information on the Business Model Options, please see Appendix C – WiFi on Train- A Cost and Revenue Analysis.

For more information on the business model options, please see the following appendices:

- Existing WiFi System and Network Report
- Wireless Internet on Capitol Corridor Trains Revenue Forecasting Procedure
- WiFi on Train – A Cost and Revenue Analysis
- WiFi Survey
- CCJPA Best Explaining Variables
- Evaluation of the Willingness to Use and to Pay for internet Connection on-board CCJPA.

Chapter 4 Regulatory and Legal Requirement

Enabling wireless Internet services on the trains required design, installation, and operation of an environment consisting of wireless infrastructure in addition to the wired Internet. This chapter describes the regulatory and legal requirement specific to the wireless environment.

FCC Trends in Unlicensed Spread Spectrum Devices

Regulatory Principles of FCC

According to the FCC the provisions for unlicensed spread spectrum devices were first introduced in 1985. The provisions are based on simple principles. There are minimal rules to control for interferences and at the same time encourage innovation through flexibility. The FCC adjusts the rules periodically in response to technology advances and other developments. The FCC develops broad rules as a framework and leaves it to the private sector to develop detailed standards. The 802.11 is a family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE).

Wireless Specifications

IEEE 802.11b

- Developed by industry standards group – widespread support and explosive growth
- Also known as “Wi-Fi”
- Key Features:
  - Direct Sequence Spread Spectrum
  - Operates in the ISM band at 2.4 GHz in 5 MHz steps
  - Low power < 100mW; range < 100m
  - Designed for network operations
  - Bandwidth: 22 MHz; data rates up to 11 Mb/s
- Applications:
  - Wireless access points
  - Wireless bridge to Ethernet backbone
  - Community networks
  - Access points at public gathering places

IEEE 802.11a

5.7 GHz; up to 54 Mb/s

- An extension to 802.11
- Applies to wireless LANs
- Provides up to 54 Mbps in the 5GHz band
- Most commonly, communications takes place at 6 Mbps, 12 Mbps, or 24 Mbps.
- Orthogonal frequency division multiplexing encoding scheme NOT FHSS or DSSS.
- The specification applies to wireless ATM systems and is used in access hubs.

IEEE 802.11g

2.4 GHz; up to 54 Mb/s

- Applies to wireless LANs
- Provides 20+ Mbps in the 2.4 GHz band.
- Most recently approved standard
- Wireless transmission over relatively short distances at up to 54 megabits per second (Mbps) compared with the 11 megabits per second of the 802.11b standard.
- Operates in the 2.4 GHz range and is compatible with 802.11b, 802.11g.

IEEE 802.11i

- adds the Advanced Encryption Standard (AES) security protocol to the 802.11 standard for wireless LANs.
- Security has been a primary concern for IT managers reluctant to deploy wireless networks, but AES is a stronger level of security than found in the current Wi-Fi Protected Access security standard. (From NetworkWorldFusion)

IEEE 802.16 Wi-Max

- Introduction of new alternative digital technologies : OFDM
- Growing interest in 5.8 GHz Unlicensed National Information Infrastructure Devices

Enforcement

- The Commission has authority to investigate any user of the band and can come on site and inspect the operation of the equipment.
    - *15.29 (a) Any equipment or device subject to the provisions of this part, together with any certificate, notice of registration or any technical data required to be kept on file by the operator, supplier or party responsible for compliance of the device shall be made available for inspection by a Commission representative upon reasonable request.*
- The FCC has very limited resources for enforcement at the moment, as the trend for the last couple of decades is deregulation.
- The National Telecommunication and Information Administration (NTIA) and the Interdepartmental Radio Advisory Committee (IRAC) manage federal usage of the spectrum.

Power Limits

- FCC rules require suppression of the signal outside the band to prevent interference.
- *FCC 15.247 (2) Field strength limits are specified at a distance of 3 meters.*
- *FCC 15.249 ©(2)(e)For digitally modulated systems, the power spectral density conducted from the intentional radiator to the antenna shall not be greater than 8 dBm in any 3 kHz band during any time interval of continuous transmission.*
- Must ensure that the public is not exposed to radio frequency energy levels in excess of the Commission's guidelines.
    - FCC 1.1307 (b)(1)
        - FCC 1.1310 Table 1 - Limits for maximum permissible exposure (MPE)
        - FCC 2.1093 Table 1 – Transmitters, Facilities, and Operations subject to routine environmental evaluation.
- *FCC 15.247 (3) As an alternative to a peak power measurement, compliance with the one Watt limit can be based on a measurement of the maximum conducted output power. Maximum Conducted Output Power is defined as the total transmit power delivered to all antennas and antenna elements averaged across all symbols in the signaling alphabet when the transmitter is operating at its maximum power control level.*
    - *FCC 15.247 (4) The conducted output power limit specified in paragraph (b) of this section is based on the use of antennas with directional gains that do not exceed 6 dBi.*
- FCC 15.247 – 802.11(b) : 2.4 GHz band
    - Point to multi-point:
        - Minimum 6 dB bandwidth at least 500 kHz
        - Allow up to 1 watt of Transmitter Power Output (TPO) with a 6 dBi antenna **OR**
        - 36 dBm **OR**

        - 4 watts of Effective Radiated Power over an isotropic antenna (EIRP)
        - TPO needs to be reduced 1dB for every dB of antenna gain over 6dBi.
    - Point to point:
        - FCC encourages directional antennas to minimize interference to other users.
        - More lenient w/ point-to-point links
            - TPO reduced by 1/3 of a dB instead of a full dB for point-to-multi point.
- FCC 15.407 – 802.11(a) :
    - Point to multi-point:
        - “low” band 5.15GHz -5.25 GHz
        - IN- BUILDING ONLY
            - Max Power of 50 mW (TPO)
            - *15.407 (d) Any U-NII device that operates in the 5.15-5.25 GHz band shall use a transmitting antenna that is an integral part of the device*
            - *15.407 (e) Within the 5.15-5.25 GHz band, U-NII devices will be restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.*
        - “middle” band 5.25 GHz – 5.35 GHz
            - Max Power 250 mW
        - “high” band 5.725 GHz – 5.825 GHz
            - Max Power 1 watt
            - Antenna gain of 6 dBi**,** 36 dBm **or** 4 watts EIRP
        - Point to point:
            - 15.407 (a)(3) TPO of 1 watt and up to 23 dBi gain antenna w/o reducing the TPO 1 dB of gain over 23 dBi
            - 15.247 (b)(3)(ii) Allow the use of any gain antenna for point to point operations w/o having to reduce the TPO for the 5.725 GHz to 5.825 GHz
                - LOOK AT EQUIP CERTIFICATION FOR EIRP RESTRICTIONS

Equipment Limitations and Certification

- FCC Part 15 devices:
    - *15.203 An intentional radiator shall be designed to ensure that no antenna other than that furnished by the responsible party shall be used with the device.*
    - *15.204 © Only the antenna with which an intentional radiator is authorized may be used with the intentional radiator.*
- FCC basics of certification 2.901 – 2.1093
- FCC requirements for Part 15 devices 15.201

- *15.204(b) A transmission system consisting of an intentional radiator, an external radio frequency power amplifier, and an antenna, may be authorized, marketed and used under this part.* ***However, when a transmission system is authorized as a system, it must always be marketed as a complete system and must always be used in the configuration in which it was authorized. An external radio frequency power amplifier shall be marketed only in the system configuration with which the amplifier is authorized and shall not be marketed as a separate product.***
    - Recertification of equipment okay.

- Temporary options to certification
  - Experimental licenses (Part 5)
    - Used for temporary experimentation
    - Up to 2 year limit
  - Special temporary authorities (STA) (Parts 15.7 and 5.61)
    - Used for urgent requests for use of the spectrum where you cannot go through the traditional paperwork process imposed by the FCC to get your equipment license.
    - Must be used for specific purposes i.e., Educational research
    - 6 month limit
    - Lower priority for interference than experimental licenses but for Part 15 devices it's not of concern.

Interference

- The device may not cause harmful interference.
- The device must accept any interference received, including interference that may cause undesired operation.
- Harmful interference
  - FCC Part 2.1 © - Interference which endangers the functioning of a radio-navigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radio-communication service operating in accordance with regulations.
  - FCC Part 15 .3(m) – Any emission, radiation or indication that endangers the functioning of a radio navigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radio communications service operating in accordance with this chapter.
  - The 2.4 GHz band is a bit more congested than the 5.8 GHz both have interference issues.
- Devices that fall into Part 15 of the ISM band (2400-2483 MHz)
  - Include: unlicensed telecommunications devices
    - Cordless phones, home spy cameras, FHSS, and DSSS LAN transceivers.
  - *FCC 15.5 (b) Operation of an intentional, unintentional, or incidental radiator is subject to the conditions that no harmful interference is caused and that interference must be accepted that may be caused by the*

    operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific, and medical (ISM) equipment, or by an incidental radiator.
  - *FCC 15.5 © The operator of a radio frequency device shall be required to cease operating the device upon notification by a Commission representative that the device is causing harmful interference. Operations shall not resume until the condition causing the harmful interference has been corrected*
    - Note: A Commission representative as well as operators of other licensed and non-licensed devices can inform you of interference and require that you terminate operation.
  - Using 802.11b channels 1,6,11 don't interfere with each other
- Devices that fall into the U-NII band
  - No overlapping channels
  - Lower 200 MHz – 8: 20 MHz wide channels can be used w/o interfering w/ channels w/in earshot
- ISM Part 18
  - Also an unlicensed service
  - Radio frequency should be contained within the devices but other users must accept interference from these devices
  - Part 18 frequencies that could effect 802.11 devices are 2.400 to 2.500 GHz and 5.725 GHz to 5.875 GHz
- Satellite Communications – Part 25
  - Uplink or downlink of data, video etc, to/from satellites in Earth orbit.
  - U-NII band is reserved for Earth-to-space communications at 5.091-5.25 GHz
    - Also allocated to the fixed satellite service (earth-to-space) for non-geostationary satellites on a primary basis
    - FCC is trying to decommission this band for "feeder" use to satellites as "after January 1, 2010, the fixed –satellite service will become secondary to the aeronautical radio navigation service." Part 87
- Broadcast Auxiliary – Part74
  - Electronic news Gathering (ENG) video links can cause interference to 802.11 gear such as access points deployed with omni-directional antennas servicing an area.
  - Wireless providers should consider contacting a local frequency coordinator for Part 74 frequencies that would be affected. Society of Broadcast Engineers www.sbe.org
  - ENG frequencies that overlap 802.11 devices are 2.450 to 2.467 GHz (channel A08) and 2.467-2.4835 GHz (channel A09) (Part 74.602)
- Unlikely you will interfere with them but they can interfere with you
  - Stations in the Maritime Service
    - 2.4 -9.6 GHz used for radio determination RADAR
  - Aviation Services – Part 87

- 470 MHz to 2.450 GHz to overlap the channels used by 802.11b and 2.450 to 10.500 GHz to overlap the channels used by 802.11a.
- Land Mobile Radio Services – Part 90
  - 2.450 to 2.835 GHz for commercial activity
  - can only license 2.450 to 2.483 GHz (90.35(a)(3)).
- Amateur Radio – Part 97
  - 2.390 -2.450 GHz overlap 802.11b
  - 5.650 -5.925 GHz overlap 802.11a
    - Primary from 2.402 to 2.417 GHz
    - Secondary at 2.400 to 2.402 GHz
      - There is a Notice of Proposed Rule Making (NPRM) for the FCC to change the 2.400 to 2.402 to primary.
- Fixed Microwave Services –Part 101
  - 2.450 to 2.500 GHz band used to transport video
  - Used by Local Television Transmission Service (LTTS) and Private Operational Fixed Point-to-Point Microwave Service (POFS).
- Federal Usage (NTIA/IRAC)
  - For 802.11b
    - FCC 15.247(h) Spread spectrum systems are sharing these bands on a noninterference basis with systems supporting critical government requirements that have been allocated the usage of these bands. Secondary only to ISM equipment operated under the provisions of Part 18 of this chapter. Many of these government systems are airborne radiolocation systems that emit a high EIRP that can cause interference to other users.
  - For 802.11a
    - FCC 15.407 Commission strongly recommends that parties employing U-NII devices to provide critical communications services should determine if there are any nearby government radar systems that could affect their operation.

Laws on Antennas and Towers

- FCC has overruled local ordinances and homeowner agreements that would prevent installations.
  - *FCC 1.4000(a)(2) "fixed wireless signals" means any commercial non-broadcast communications signals transmitted via wireless technology to and/or from a fixed customer location.*

Height Limitations

- Cities regulation the construction of towers
  - Max height
  - Zoning of antenna/tower
  - Construction
  - Aesthetic.
- FAA and FCC tower registration.

        - FCC 17.7 (a) Any construction or alteration of more than 60.96 meters (200 feet) in height above ground level at its site.

- New Standards to help:
    - IEEE group (802.11h) development of transmission power control (TPC) and dynamic frequency selection (DFS).
        - These protocols will use the band more efficiently and be required for European deployment.

Chapter 5 Technical Options and Technology Trends

This chapter describes high-level view of the Reference Architecture created by the project team. For detail Reference Architecture, see Appendix G – Technical Reference Architecture.

What is the Reference Architecture?

The reference architecture of CCJPA-Caltrans Request for Qualifications (RFQ) is a key ingredient to providing information quickly and effectively to people. The desire is to have a wireless technology architecture that supports WiFi for commuters on Capitol Corridor Inter-City Trains between Auburn and San Jose, California, while being consistent, manageable, non-redundant and comprehensive.

The Reference Architecture is the basic foundation for the CCJPA WiFi on Trains and Caltrans business functions. It is on the critical path to enable future Wireless Applications projects.

The focus of the Reference Architecture is to provide CCJPA and Caltrans with an enterprise-wide blueprint for the future technical architecture. The Reference Architecture is one of the essential pieces that allow business and technical teams to develop applications to support CCJPA and Caltrans.

The topics addressed in this document include:

- Mobile Internet for Train Commuters and Enterprise Network Architecture
- Information Security Architecture
- Reliability & Fault Tolerance.

Mobile Internet for Train Commuters and Enterprise Network Architecture

The Mobile Internet and Enterprise Network Architecture is the foundation of the overall architecture. All other components rely upon the availability and capabilities of the network. The ingenuity of this reference architecture is to explore how technologies utilizing high gain antennas, Wi-Fi meshed networks and WiMAX together with Mobile IP-based Mobile Networks can be combined to provide a total last-mile access solution now and in the future.

There are many different wireless technology usage segments. Each wireless technology is designed to serve a specific usage segment and component of the architecture:

- Commuter Personal Usage - Personal area networks (PANs)
- In-Car Train - Local area networks (LANs)
- Train-to-Trackside - Metropolitan area networks (MANs)
- Trackside-to-Internet - Wide area networks (WANs).

The requirements for each usage segment are based on a variety of variables, including:

- Bandwidth needs
- Distance needs
- Power
- User location
- Services offered
- Network ownership.

Open Standard Radio Technologies

The adoption of open standard for radio technologies—including 802.11, 802.16 and future standards – speeds up the explosive growth of service based on wireless technologies. Wireless Fidelity (Wi-Fi) revolutionized the market for unlicensed client-access radios in a wide variety of applications. Starting in 2005, Worldwide Interoperability for Microwave Access (WiMAX) certification of the IEEE 802.16-2004 standard for fixed-position radios will do the same for point-to-point (P2P) and point-to-multi-point (P2MP) wireless broadband equipment in both the licensed and unlicensed bands.

In 2006, the WiMAX standard, i.e., IEEE 802.16e, for portable operation is expected to be ratified, thus standardizing client radios in unlicensed and licensed bands. This certification will provide users with an alternative and allow service providers the benefit of additional tier services. It provides up to 50-kilometers of service area, allows users to get broadband connectivity without the need of direct line-of-sight to the base station, and provides total data rates up to 75 Mbps — enough bandwidth to simultaneously support hundreds of businesses and homes with a single base station.

All Internet Connectivity for commuters in the rail car must comply with IEEE 802.11g standards and specifications. Inside the cars of train, one or more access point (AP) can be used for aggregating and connecting end users' device such as notebook computers.

Connectivity to the Train

There are three possible independent modes for providing connectivity to the train:

1. Satellite Communication
2. Existing Cellular Networks
3. WiFi/WiMax Bridge Network.

Model #3 is the preferred mode for high-volume deployment. Mode 1 and 2 can be used for the low initial cost – low volume business case or for the backup communication channel of mode 3.

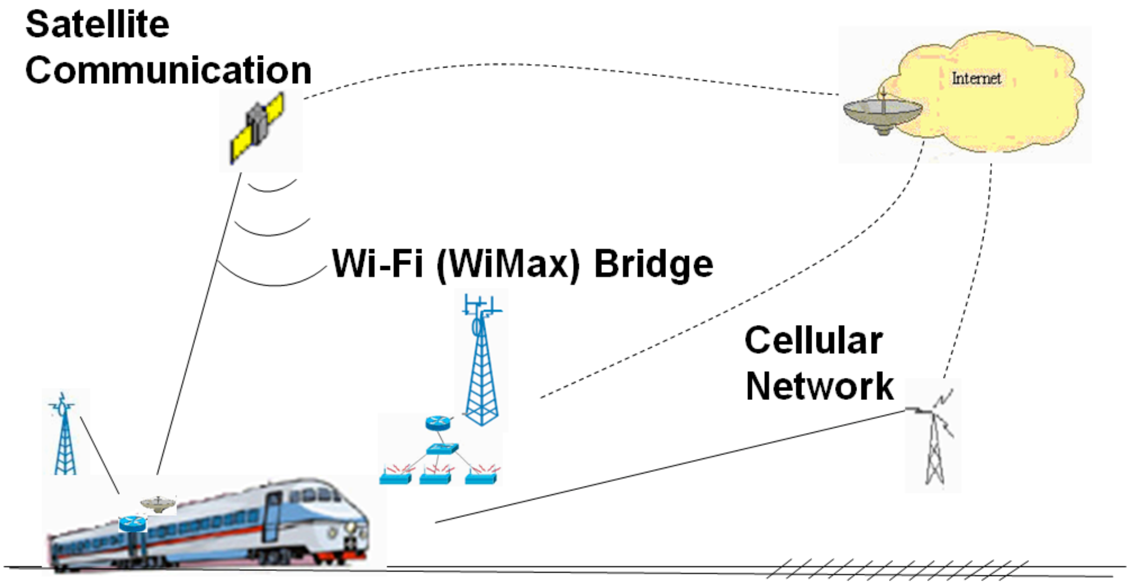


Figure 7: Conceptual Diagram of Internet Connectivity on Train

Components of Network Architecture

The different types of network architecture components are as follows:

- Command and control centers including the following:
  - Mobile Internet service center performing the configuration management and user service provision. It includes user interface, database management system, client authentication server, etc.
  - Homeland security service center configuring the access control to the homeland security-related infrastructure & capability, and operating the homeland security subsystems. It includes the user interface, database management system, security officer provisioning system, security violation incident processing and database.
- In-Train Architecture components – components on-train supporting the mobile Internet service and homeland security service. These are network equipments, e.g., WiFi access router, on car(s) of train to which the train riders' devices, e.g., notebook computer, connect to.
- Train to Back-Haul Architecture component – infrastructure used to enable the communication for the on-train data traffic between train and back-haul component such as fiber-optics cable along the train track.
- Trackside communication system connecting all the trackside wireless infrastructures to the data gateway on which the data are routed to different service centers.
- Homeland security surveillance system alerting security violation, capturing incident scene, and sending processed incidents to security service center.
- Data gateway dispatching data to various service centers, and the deployed wireless infrastructure and security system.
- Data network connecting data switch to various service centers.
- Interface to emergency response system for integrating the train operation with the emergency response systems of communities along the track, state or federal government agencies.
- Interface to law enforcement systems for integrating the train operation with the law enforcement agencies.
- Interface to existing or future homeland security infrastructure for more coherent safety measures.

The following diagram depicts how these network components works together.

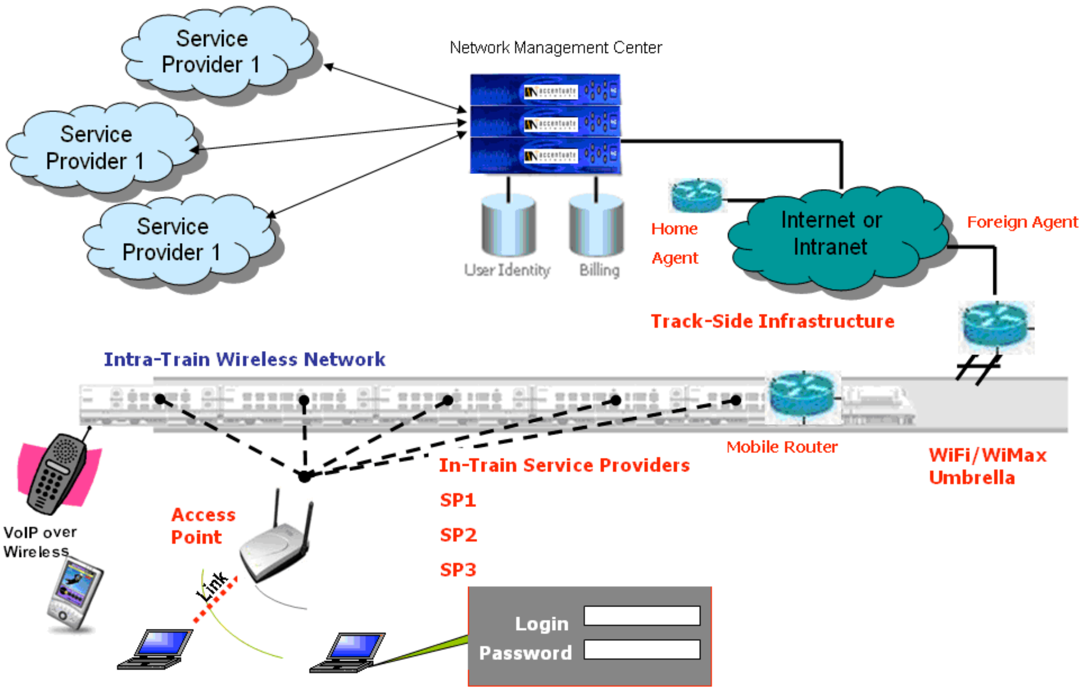


Figure 8: Network components

In addition, there are data networks connecting the data aggregation switch to various service centers. And more importantly, a subsystem such as mobile IP router/bridge is needed to maintain the Internet connectivity while the train passes through different trackside infrastructure.

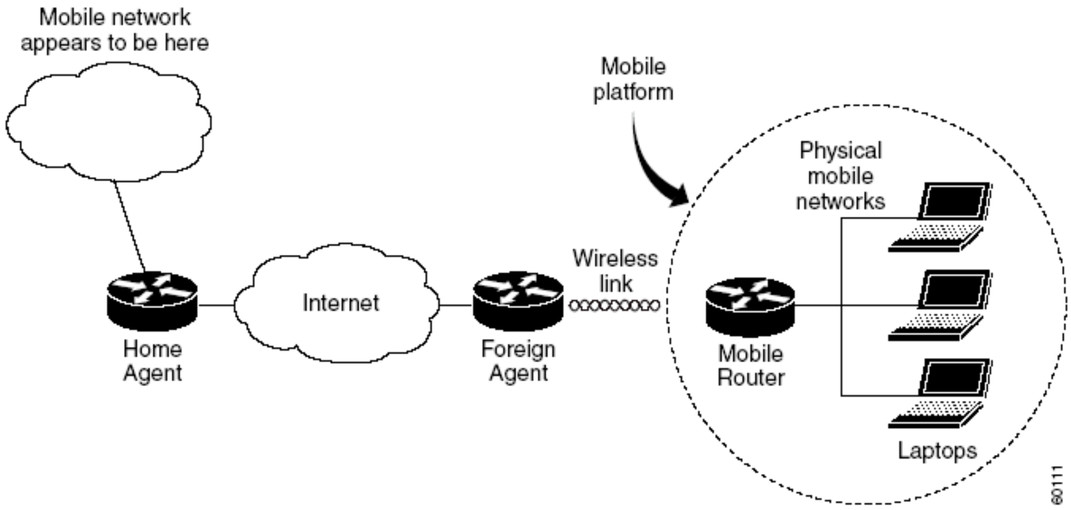


Figure 9: A Typical Mobile Network (Courtesy Cisco Systems)

In the train setup, the foreign agent is placed along the trackside and connected through wired media or the Internet to the home agent. The mobile router on the other hand is placed on board the train. The mobile router may be used to provide the in-car network connectivity, in which case a Mobile Router is required in each car supporting wireless access. On the other hand it can be placed in one car, constituting an infrastructure network while other cars are infrastructure less and connect to the main car via an ad-hoc network.

Information Security Architecture

Strategy

The architecture should support the following security requirements:

- Data integrity,
- Data privacy,
- Audit trail of the homeland security related events,
- Access control to the homeland security related capabilities,
- Access control to mobile Internet service is managed by service provider, and
- Provide robust wireless security services that closely parallel the security available in a wired LAN.

Wireless Security Suite

The network must be secure with a scalable and manageable system featuring a well-built Wireless Security Suite, an enterprise-ready, standards-based, WLAN security solution that gives network administrators confidence that their data will remain private and secure.

The solution must provide the following benefits:

- Support Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) providing access control via per-user, per-session mutual authentication and data privacy via strong dynamic encryption.
- Only legitimate clients will be allowed to associate with legitimate and authorized network RADIUS servers via authorized access points.
- Stronger encryption to be provided by WPA with Temporal Key Integrity Protocol (TKIP) enhancements such as message integrity check (MIC), per-packet keys via initialization vector hashing, and broadcast key rotation and by WPA2 with Advanced Encryption Standard (AES) encryption enhancements to help ensure that data will remain private and secure.
- A variety of IEEE 802.1X extensible authentication protocol (EAP) types can be supported, Cisco LEAP, Protected EAP-Generic Token Card (PEAP-GTC), PEAP-Microsoft Challenge Authentication Protocol Version 2 (PEAP-MSCHAPv2), EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled TLS (EAP-TTLS), EAP-Subscriber Identity Module (EAP-SIM), and EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
- Support LEAP for mutual authentication and both TKIP and WPA TKIP algorithms.
- A wide selection of RADIUS servers, such as the Cisco Secure Access Control Server (ACS), can be used for enterprise-class centralized user management. RADIUS accounting records for all authentication attempts are supported.

Key Policies In-Train

Key policies relevant for in-train wireless network and the service vendors comprise:

- ✓ include strong authentication and encryption for network access;
- ✓ mitigate denial of service and other disruptive attacks;
- ✓ implement capabilities to assess the risks and vulnerabilities associated with 802.11 networks and devices;
- ✓ develop defensive actions necessary to detect, deter, and defeat unauthorized 802.11 activity;
- ✓ include intrusion detection methodologies for the 802.11 wireless systems; and
- ✓ share 802.11 security knowledge - such as historical forensics - to improve overall security processes.

Appendix A

Existing Wi-Fi Systems and Networks

Adam Dankberg
Institute for Transportation Studies
California Center for Innovative Transportation

March 9, 2005

INTRODUCTION **1**

TRANSPORTATION LOCATIONS **3**

EXISTING WI-FI SERVICES ON TRAINS 3
WI-FI SERVICES ON TRAINS UNDER DEVELOPMENT 5
WI-FI ON AIRPLANES 8
WI-FI ON VEHICLES 11
Moving Vehicles *11*
Stationary Vehicles *13*
WI-FI ON SHIPS 14
Cruise Ship *14*
Ferryboats *15*

WI-FI IN TRANSPORTATION TERMINALS **15**

AIRPORT 15
HIGHWAY REST STOPS 17
TRAIN STATION 18
MARINAS 18
GAS STATIONS/PARKING LOTS 19

NON-TRANSPORTATION LOCATIONS **19**

WIMAX 19
WIDE-AREA NETWORK & OTHER CITY-WIDE SYSTEMS 20
RESTAURANTS/COFFEE SHOPS 22
OTHER LOCATIONS 24
FUTURE TECHNOLOGY 24

WIRELESS PROVIDERS **25**

TRAIN PROVIDERS **30**

CURRENT MARKET COMPETITORS 30
COMPETITORS WITH TECHNOLOGY IN-DEVELOPMENT OR TESTING 31
COMPANIES WITH SUSPENDED PRODUCTS 33

BUSINESS MODELS **33**

TRANSPORTATION SYSTEMS 33
TRANSPORTATION TERMINALS 35
HOTSPOT NETWORK PROVIDERS 35

FIGURES **39**

Introduction

The number of locations providing public wireless Internet access has increased very rapidly in the early part of the 21st century. There are nearly 60,000 of these hotspots worldwide of which over one-third are in the United States. London alone has over 1,200 public locations. The leading American city, New York, has over 800. There were only about 2,000 locations worldwide in early 2003. At the time, it was predicted that there would be 40,000 hotspots in 2006. Projections for 2008, forecast 200,000 hotspots, although it appears that number will be surpassed well before then. Just as the number of hotspots has exploded, the types of locations have become increasingly diverse. Nearly 17,000 are in hotels, 10,000 in restaurants, 10,000 in cafes, and 1,000 at airports. There are also an increasing number in train stations and bus stations, with improving technology allowing for access on planes, trains, and vehicles. Over 4,500 of the worldwide hotspots are free. The rest are offered by a large number of wireless Internet providers (WISPs). There are hundreds of these companies, from Access Anyplace to ZRNet. The largest, including iPass, Boingo, T-Mobile, and SBC, have thousands or even tens of thousands of these hotspots on their network.

Since wireless Internet technology is relatively new, especially for public commercial use, it is a quickly evolving and wide-ranging industry. There is no universally accepted method of providing connectivity or common business plan, even for a use as specific as on-train access. The industry has yet to consolidate, resulting in a wide range of pricing options and providers. To best determine the appropriate business model for a new wireless location, it is helpful to examine business models used at other existing locations. Such analysis can determine what prices the market will bear, unique ways of funding service, as well as what level of service the customer is expecting or desires.

This appendix examines a large number of existing and proposed wireless systems, listing each location's pricing, technology and any other relevant data. The focus is on mobile wireless systems, specifically trains. Within the wireless access on trains industry, technology varies from two-way on-board satellite systems to those with track-side routers communicating with the speeding vehicle. Since there are very few operational on-board wireless Internet systems, access locations on other transportation vehicles, such as busses and planes are examined. An on-train wireless system is part of a broader competition among transportation modes and therefore must provide similar or better access and prices in order to increase ridership. As mobile wireless technology is still in its infancy, the Wireless Fidelity (Wi-Fi) systems at transportation terminals are examined as well. These terminal locations are frequently a precursor to on-board systems and can assess, and develop, customer interest. With the inevitable industry consolidation, all of the wireless access points may be connected to a handful of WISP networks or aggregators, with similar structured pricing plans. This would give the consumer the greatest accessibility since signing up for numerous access accounts, and facing charges from numerous providers, will not be required. Once the technology is better developed, mobile wireless systems will likely join these large networks and be governed by their pricing structure. To some extent, this has already happened with the Connexion system, available on several commercial flights. Therefore, this appendix also looks at WISP pricing structures, determining access fees and existing access locations.

The last part of this appendix integrates all of the material covered in an attempt to guide the creation of a business model for an on-train wireless system. The technologies used on trains and the companies developing those technologies are examined in greater detail. The business models used on transportation systems, at transportation terminals, and on wireless hotspot networks are summarized and compared. To compare pricing plans, sample usage patterns were developed, and the results are charted to provide a picture of existing access options and prices. Some trial and operational usage data are given as well, as a tool for determining the assimilation of mobile wireless systems.

Transportation Locations

Existing Wi-Fi Services on Trains

GNER – UK

Icomera AB was chosen to operate what became the first operational United Kingdom on-train wireless system. It began as a free trial, but it now has a pricing structure of 30 minutes for £2.95 ($5.57), 60 minutes for £4.95 ($9.35), 120 minutes for £7.95 ($15.01), and 180 minutes for £9.95 ($18.29). The access periods are continuous. First class passengers have free use of the system. The Icomera system uses a satellite download/cellular upload architecture and is testing a 3G/satellite system. Users download at approximately 500 Kbps, with a slower upload rate. Service is being expanded for use on 10 Mallard trains, at a total cost of approximately 1 million pounds. On September 20, 2004, GNER, Icomera, and BWCS released a report on wireless Internet usage during the trial. They stated that people were upgrading to first class in order to have free access to the wireless Internet. The report stated: "Just over 70 per cent of people using the GNER Wi-Fi service have been checking and sending email, while 42 percent have been accessing corporate networks and 30 percent have been checking GNER's online travel information." Usage was growing quickly, increasing 77% per week and had increased from an average of 45 minutes per session to 70 minutes per session over the first few months of service. Sixty-seven percent said they would definitely use it again and 88% said they would recommend it to others. Twenty-five percent said they would travel more if it was available on all trains.

Linx – Sweden, Denmark

Icomera AB operates a system on Linx trains running between Sweden and Denmark. The system uses a satellite downlink/GPRS uplink and achieves a maximum speed of about 400 Kbps for downloads. Access costs SEK 50 ($6.77) for 40 minutes and SEK 80 ($10.84) for the entire journey. Access can be purchased either on the train's deli car or with ticket booking for business class customers. Linx uses the system to provide paper-free ticketing.

VIA Rail – Canada

A joint venture by Bell Canada, Intel and PointShot Wireless has implemented a wireless Internet trial on VIA trains between Montreal and Toronto. The service is available for free and only in first class cars. It uses Bell satellites for download and Bell's wireless network for upload. Funding is provided by Bell Canada's Accelerator Fund. The network also consists of wireless access in station lounges in Montreal, Dorval and Toronto. For a short time, beginning in February 2004, an additional trial was run by Spotnik, TELUS, PalmOne, and Cisco on the Montreal-Quebec City line. It was available in first class only. The technology used was a satellite download/cellular upload. Station lounges in Montreal and Quebec City were equipped as well. PalmOne's involvement provided for a program where passengers could borrow a handheld device for use on the train. A Kinetic Strategies report showed that Canada has a 22% broadband penetration, compared to 10% in the U.S. This indicates that Canadian train passengers may be more likely to expect and utilize onboard wireless Internet services and may be more demanding of those services.

Altamont Commuter Express – Northern California

PointShot's RailPoint system was installed on ACE trains, which run from Stockton to San Jose. The system is free for users courtesy of the sponsorship of the University of Phoenix, which offers online classes. Wireless Internet is available only on one vehicle. Similar to other PointShot systems, it is a satellite download/cellular upload. The system achieves a maximum transfer rate of 1-2 Mbps for downloads. The system serves 45-60 users per day over the course of three trips. Operators claim if the system generates 10 additional riders per day it justifies its costs.

SNCF – France

The SNCF Wi-Fi initiative, Click TGV, restricts users to sending e-mails without attachments only and limited Internet connectivity. It uses GSM/GPRS for both downloads and uploads. Tourist info, news and games will be provided on the system. Access is free during the trial and laptops can be rented for €8 per trip. The system is on two first class cars and one second class car on the Paris-Bordeaux-Pau line, a line traditionally more popular with tourists. The system cost €100,000 per car to install. The access code required to use the system must be obtained at the stations. This experiment was an attempt to provide an Internet service and that SNCF is looking now at a better technology to provide a real commercial service in the near future.

Stockholm Public Transit Authority – Stockholm, Sweden

A Fujitsu-Siemens system is providing access for Stockholm Public Transit Authority employees in Stockholm subway stations. An overlaying Appear Networks system allows location-based, real-time data content including subway operations. This is designed to allow employees to provide customer support and report problems. Employees are using handheld devices to connect to the system. In the future it will expand to allow public access, but it is currently restricted to transit employees.

Wi-Fi Services on Trains under Development

SJ- Scandinavia

In January of 2005, Icomera AB announced an €11 million contract with SJ, the leading Scandinavian train operator. The rail network carries over 70,000 people per day. Icomera will install a 3G/satellite system on 85 trains, with service expected to start in the summer of 2005. Icomera provides an end-to-end service for the train operator. It will be the first major rollout of a 3G/satellite system.

Southern – UK

In early March 2005, Nomad Digital, with help from Redline Communications, will rollout a pre-WiMax mobile Internet solution on Southern's London to Brighton line. The 90 kilometer line will have pre-WiMax equipment running along the track every three kilometers. On-board Wi-Fi access points will communicate with the WiMax devices and allow users to connect to the Internet via their laptop Wi-Fi network cards. The providers are expecting the system to provide a bandwidth up to 32 Mbps. The system should allow service at all times during the trip, including when the train is in tunnels. The free trial is scheduled to run from early March to the end of April. After that period, the system will join the T-Mobile UK network. Users will be required to signup with T-Mobile to gain access. In conjunction with this installation, T-Mobile is adding hotspots at 16 of the train stations along the London to Brighton line.

Virgin Trains – UK

A joint venture between Broachreach and PointShot is implementing a 3-step approach to providing Internet access to Virgin Trains customers. Step 1, currently being implemented, is to bring wireless access to all Virgin Trains stations. Step 2 is to place enlarged hotspots at these locations using directional antennas that will cover several miles of track. Step 3 is to provide access over the entire route.

DSB – Denmark

Zealconnect's Pulz8express system is being installed on DSB trains and is scheduled to be in use by the end of 2005. It will be free for First Class passengers and available to other riders for a fee. A study concluded that users would be willing to pay $1.65 to $3.30 per session for access on the route.

RailTel – India

The government-operated rail and telecommunications company is installing trackside devices that will provide Internet access to passing trains as part of a nationwide connectivity project. In total, about 600 of these trackside devices will be used throughout the country. The system is expected to provide 2 Mbps of bandwidth. The service will be free initially and installed on two routes. It will only be available on air conditioned cars because the service doesn't work with open doors or windows. Luxury cars will carry a kiosk with two computers and will allow laptop access.

SBB – Switzerland

Swisscom is installing wireless Internet service on 75 cars for use on the Rorschach-Geneva line. It will be operational by September 2005, and may be expanded to all cars by 2007.

Eurostar – Cross-Channel

Eurostar is refurbishing its 27 train-fleet and is installing wireless Internet capabilities. It will use some form of satellite/cellular system but won't be able to provide access while the train is in the Chunnel. They are also installing hotspots in terminals in Paris, London, and Brussels.

Trenitalia – Italy

Alenia Spazio and Eutelsat are implementing a system on the Rome-Florence line with monetary support from the European Commission covering the 4.6 million euro trial cost. If successful, the service, called FIFTH, will expand to other lines. The goal is to have 250 Wi-Fi enabled trains by 2008-09. The system is satellite-based and will include TV programming. In addition, base stations that can broadcast delayed TV will be utilized in tunnels, which make up 7% of network.

Seattle, Washington

The Seattle Monorail Authority issued an RFQ in early 2004 for Internet service on its line, but no recent developments have been publicized.

La Defense Subway Station – Paris, France

A very similar Appear Networks system is also in use at La Defense, a major transportation hub outside of Paris that handles 480,000 passengers per day. In fact, La Defense is one of the ten largest transportation hubs in Europe. Employees can connect via PDA's and receive "context-aware" information including vehicle schedules and passenger movements. The system is aware of each employee's location and job function and can provide necessary time and location-based information. Subway passengers have Internet-only access on the same network courtesy of Cisco infrastructure. Appear hopes to expand the system to other Paris subway stations.

Wi-Fi on Airplanes

Connexion by Boeing

Several airlines are installing Boeing's Connexion system. It achieves transfer rates of 5 Mbps for downloads and 1 Mbps for uploads using a two-way satellite system. The system costs $1 million per plane to install and requires the aircraft to be grounded for some time for installation. Boeing has roaming agreements with iPass, InfoNet, NTT DoCoMo, T-Systems, Starhub, NTT Communications and Singtel, allowing users of each of those networks to use Connexion with their existing plans. An agreement with Boingo will allow customers to charge the Connexion fees to their Boingo account. Connexion has agreements with 220 corporate customers to provide simplified billing and account management for their employees. Some user data are available from trials completed on Lufthansa flights. Approximately 30% of passengers were using the service on trials.

Boeing marketing has estimated that 20% of passengers (60-80) on large planes will sign up for the service. Where the service is past the trial phase, service costs $14.95 for flights less than 3 hours, $19.95 for flights between 3-6 hours and $29.95 for flights longer than 6 hours. These plans have no time or megabyte (MB) restrictions. In addition 30 minutes of use may be purchased for either $7.95 or $9.95.

Table 1: Connexion Locations

Singapore Airlines	Installing the system in 2005. Will include four channels of international news.
Lufthansa	Currently on some flights in and out of Munich, Frankfurt, and 13 North American cities. It will be on the rest of their planes sometime in 2005. Free weather and news is provided on the portal.
ANA	On the Tokyo-Shanghai route
Japan Airlines	On the Tokyo-London route
Scandinavian Airlines	On some Copenhagen routes and all international flights in and out of Seattle
China Airlines	Was available on North American flights in April 2005
Asiana Airlines	Installing on fleet of 777s by July of 2005
El Al Israel Airline	Installation on El Al's fleet will be completed by 2007

Korean Air also signed up for the service. British Air was an initial supporter, but due to cost concerns will only provide short message service (SMS), not Internet capability.

Verizon Airfone/Tenzing

The Tenzing service is a cheaper alternative to Connexion. In most cases planes don't have to be taken out of operation to install the equipment. It replaced the JetConnect service on United, US Air and Continental Boeing 767s. The service is limited strictly to e-mail and instant messenging due to low bandwith capabilities. Currently the service is estimated to provide 128 Kbps, although that is being upgraded to 1.7 Mbps by 2006. It is currently on 900 aircraft, including those operated by United, Emirates, and Iberia. Ethernet connections are provided at the seat, as opposed to cabin-wide wireless access. The service costs $15.98 per flight plus $0.10 per kilobyte on United and $10 for e-mail and $5 for instant messaging on Iberia. It is noteworthy that this price is only slightly less than the Connexion service, despite significantly less service capability. The replaced JetConnect service cost $5.99 per flight but could not send e-mail.

Other Services

Cathay Pacific is using a system on all flights developed jointly by PCCW Netvigator and Tenzing that provides e-mail capability only. Connectivity is also restricted to only first class and the first few rows of coach, via Ethernet connections at the seats. Two service plans are available: 1) $9.95 plus $0.60 per KB on both e-mails and attachments; and 2) $19.95, which includes up to 2 KB per e-mail with attachments still costing $0.60 per KB.

Alaska Airlines, Ryanair and 5 other regional operators are utilizing an APS-developed system. The APS device, called the digEplayer, is distributed by flight attendants. The unit has 64 movies, some TV shows and music and has a battery usage time of 10 hours, but it does not have Internet capability. The system cost $10 in coach and is free for first class customers.

Alitalia is testing an AirTV system that will have e-mail only through a direct satellite connection. The cost has not been publicized but will be a flat fee. AirTV is the provider for JetBlue’s DirectTV access in the United States. They hope to increase their customer base while eventually providing “60+ channels of live television and 40Mbps of Internet, e-mail, and data services to aircraft worldwide.” This service will be launched in 2007 over the North Atlantic, which will provide coverage to airline routes flying between America, Europe and the Middle East.

ARINC’s SKYLink system allows for Wi-Fi access in-cabin at a download rate of 5 Mbps and an upload rate of 256 Kbps, using two-way satellite connectivity. ARINC began coverage in April 2004 over North America. Its current customer base is business jets, but ARINC hopes to provide service on Virgin Atlantic in the future.

Wi-Fi on Vehicles

Moving Vehicles

RaySat

RaySat’s SpeedRay, announced in January 2005, is the only product available that provides in-motion Internet capability to personal vehicles. It consists of a 5” antennae that is attached to the roof of the vehicle. A two-way satellite connection is used to provide Internet, digital TV, and music access. Connection speeds are approximately 2 Mbps for downloads and 128 Kbps for uploads. The hardware costs $3,495, with installation running from $200 to $500. The user must also purchase satellite receivers for TV or Internet reception, allowing the system to be used with either DISH network or DirectTV or any satellite Internet provider. In addition, the user must pay for whatever Internet or TV subscription they choose. The product will start shipping in the third quarter of 2005.

RATP – Paris

A wireless Internet system was developed for the Public Transport Exhibition 2004 in Paris by Appear Networks and Cisco. Its use was demonstrated on a bus during the conference, held in June 2004. Using Wi-Fi, if near a hotspot, or GPRS, the system provided information to the user dependent on the location of the bus and time of day. Such information included schedules for nearby transit systems, local business information and conference information. In addition, bus drivers would have the ability to notify the command center if a parked vehicle was impeding their route. Appear Networks provided the value-added services on top of the Cisco router. This exhibit was a part of an in-progress trial along RATP bus line 38 in Paris. The system is operated by Wixos, a conglomeration of companies including RATP (the Paris metro operator), Cap Gemini Ernst Young, and Cisco. Eight different companies pay Wixos fees to use the system and then provide service and charge fees to the general public. These companies include hotspot providers Wifirst, Wifispot, and Meteor. The providers charge the same rate for use of these locations as they do their other wireless locations. The system consists of antennaes placed along the 38 bus line, which runs from Gare du Nord to the Porte d'Orleans. The service may be expanded to include antennas placed outside of all 372 metro stations. During the free trial, run from April until June 2003, only 604 users signed up the first month and 1,700 in the 3 months of the trial, disappointing the RATP. Forty percent of those 1,700 only used the service once, 16% connected more than once per week, and 3% used it several times of day. Twenty-five percent of users logged on via a PDA, 19% via a Macintosh, and the rest via PC. Ninety percent of those polled said they intended to use the network in the future.

LimoLiner – New York City to Boston

The LimoLiner, a luxury bus that travels between New York and Boston, provides wireless Internet access on its vehicle. The service is bundled in the price of a ticket, which is $69 each way. In addition, the service includes two channels of live TV.

Hampton Jitney – The Hamptons to New York City

The Hampton Jitney is a luxury bus that travels from the Hamptons to New York City. Its wireless system was developed by Wi-RAN and AT&T. The Internet service transfers data at 100 Kbps and costs either $8 per trip or $40 per month. It uses the AT&T Wireless network for data transfer and is installed on four of the company's busses.

ETH, Zurich Public Transport – Zurich

A system developed by sunrise, ETH World, and Zurich Public Transport provides Internet access on a shuttle bus running between two campuses of the Swiss Federal Institute of Technology in Zurich. The service is free and operates at 48 Kbps.

TxDOT - San Antonio

LifeLink, a TxDOT project, is using a TransGuide system to provide wireless connectivity between ambulances on the move and nearby hospitals in San Antonio, Texas. It uses line-of-sight wireless to allow patient data, video and communications between the vehicle and the hospital. This will allow doctors to prepare for and help treat patients en route to the hospital. Fifty-nine antennas have been setup throughout the city to provide connectivity for the system. It cost $20,000 to outfit each of ten ambulances.

Stationary Vehicles

Several companies make satellite dish systems for stationary vehicles. These products require the purchase of hardware and a monthly service fee. StarBand, iNetVu and MotoSat sell products that use a two-way satellite, mounted on the vehicle roof. KVH's TracNet 2.0 uses a cellular uplink with its satellite downlink and provides TV capability. These systems provide approximately 400-500 Kbps download with 56-90 Kbps upload. They cost anywhere from $1,000 to $6,995 to install in addition to a monthly fee of $60 to $99. Additional, more expensive, monthly plans providing more bandwidth, higher upload/download speeds or more storage space are available with the KVH and StarBand systems. The StarBand and MotoSat systems only work in the United States, the iNetVu system works everywhere except Asia, and the KVH system works in North America and Europe, and functions on boats as well.

Wi-Fi on Ships

Cruise Ship

Maritime Telecommunications Network

Holland America Line, Norwegian Cruise Line, and Carnival Cruise Line use a Maritime Telecommunications Network system. It is available only in some public areas, not private cabins. The service costs $100 for 250 minutes of access time, $55 for 100 minutes, and $25 for 33 minutes. Laptops are available for rent at $20 per day and a wireless card is available for $10 per day. These prices are extremely high compared to other transportation wireless systems, but due to the length of most cruises and the captive nature of the ship, there are no Internet access alternatives for passengers. Holland America provides in-room dial-up service for $0.50 per minute at 56 Kbps. A passenger can also use the Internet café, which has a similar pricing structure plus additional fees of $3.95 for activation and $3.95 for each sent e-mail. Norwegian Cruises provides a similar service, but their in-room dialup costs $0.75 per minute. In February 2005, Carnival announced a new ship, the Carnival Valor, with complete Wi-Fi access from "bow to stern".

Others

Seabourn Cruise Line uses a Wi-Fi Zone system that costs $0.50 per minute. It uses a satellite communications system and is available shipwide. Minutes can be purchased in bulk, which can lower the rate to as little as $0.25 per minute. Princess Cruise Line uses a V-Link Solutions system that costs $10.50 per 30 minutes. It is installed on 14 Princess vessels.

Ferryboats

Chantry Networks, Mobilisa – Washington

In August 2004, the Washington State Ferry system initiated wireless Internet service on the Port Townsend-Keystone route, with plans to extend it to three others by the end of the year. Over 75,000 Pugent Sound residents use the ferry system each day, corresponding to a potential market of 12 million passengers per year. The system is capable of handling between 300 and 400 simultaneous users per ferry. The service will be free during the trial, courtesy of a million dollar Federal Transportation Administration grant. Mobilisa developed a Wireless over Water technical solution to overcome the difficulties presented by wireless connectivity over open water. The system uses radios on the ferry and on shore to provide access. It has now expanded to the Bainbridge-Seattle ferry, which carries 6.5 million per year. A University of Washington study concluded that users would pay $19 to $39 per month for service.

The Harbor Bay Ferry between San Francisco and Alameda also may provide access, through an Enterprise Network Solutions system, but no additional information was available on this service.

Wi-Fi in Transportation Terminals

Airport

The number of airports with publicly accessible wireless Internet systems is increasing very rapidly. Three hundred seventy nine American airports were equipped at the end of 2004 with wireless Internet, up from 178 in 2003. This may pass 1,000 by 2008. These systems provide opportunities both for travelers and the airlines themselves, aiding in ticketing and customer service procedures. These systems aren’t very different from the typical coffee shop hotspot, except they generally cover a greater area and permit more users. In some cases the airport selects a customized system and has an integral role in system operations. In other cases, companies such as SBC or Wayport are contracted to install infrastructure and manage billing and all other aspects of the system. For example, access is provided by Wayport in at least six airports, ICOA in several small regional airports, Tata Indicomm in Indian airports, SBC in Cleveland, and Sprint in Kansas City. San Francisco International Airport has a non-exclusive contract with T-Mobile to provide access in portions of the terminal in exchange for a base monthly rent or a portion of revenues. In addition, many airport wireless systems have roaming agreements, providing access to Boingo, iPass or other aggregators' customers. Concourse Communications provides access at numerous airports, customizing the system to each airport's specifications. At locations such as Minneapolis-St. Paul, Nashville, and Detroit Metro, this access costs $6.95 for 24 consecutive hours. Users of Sprint or SBC can pay for usage at Concourse locations through those companies. Some airports, including Ft.Lauderdale/Hollywood and Portland, are free.

In addition, some airlines, particularly JetBlue, provide access for customers in their terminals or at their gates. JetBlue provides free access in its JFK terminal in New York and with a consortium of technology and advertising partners in the Long Beach airport. More commonly, airlines provide wireless access in their business lounges. These lounges restrict access and usually require either a first class ticket or an executive membership to gain entrance. American, Delta, United, and US Air partnered with the T-Mobile network to provide access. Lounge users must signup with T-Mobile or use their existing T-Mobile accounts to gain access, in addition to paying their executive club fees. Continental, Alaska Airlines, and America West provide free access for their lounge members. To gain one-time access to an America West lounge, one can pay $35. Northwest charges $6.95 per day for its lounge members.

In most cases, these systems provide value-added content, specialized for each airport. Flight information and airport information is frequently provided free of charge, even for those without wireless subscription plans. OnAir Entertainment provides eight channels of live satellite TV to users in the Museum of Modern Art, Universal City Walk, and Austin Airport. They do not provide the Internet access, but merely the content that adds value to the Internet connection. Additional features will be provided in the near future. Concourse Communications plans to allow users to wirelessly print in their airports and will integrate voice-over Wi-Fi, allowing users to make calls from their laptops. Wayport is testing live-TV over Wi-Fi and will eventually offer music and movies.

Highway Rest Stops

Placing wireless Internet accessibility at highway rest stops entails some hurdles not faced by typical retail hotspot locations. They are often in rural or uninhabited areas without nearby supporting infrastructure. But in the last few months, several states have instituted rest stop wireless or kiosk programs. TxDOT provided both wireless and kiosk service for free and hopes to be in 102 rest areas by October 2005. This program is designed to get tired drivers to pull over and take breaks. Iowa DOT contracted the I Spot Network to provide free wireless Internet at several rest stops. The infrastructure and operating costs are covered by advertising that is placed on the portal. Advertisements cost $20 and up. It is currently in eight rest stops, but the state recently announced plans to extend service to 40 rest stops. They cited 111,000 uses in the system’s first seven months of operation. Two aspects of value-added content both provide funding and encourage use. The state distributes traffic, tourist and weather info, and I Spot compiles exit guides that include lodging, gas, and food information and promotions in the local area. The Maryland Office of Tourism contracted Net-Stand LLC to place a system at two rest stops. The system is free for the first ten minutes and then costs $4 per hour. Net-Stand is supplying the hardware for free and is purchasing broadband service. The state is seeking to earn money from this program. The State of Michigan contracted SBC to place Wi-Fi at ten rest stops, state parks and docks. The system costs $7.95 for 24 hours of continuous use but provides free access to michigan.gov. Each site has a 150-foot signal range. Flying J truck stops provide access at 285 locations. siriCOMM has placed slow speed (48 Kbps) connections at 250 Pilot Travel Centers in 38 different states.

Train Station

A large number of train stations have installed wireless access capability. In many cases, train operators are building a customer base for wireless connectivity before expanding service on board the rail car. Train station systems are very similar to airport systems. They are high-use broadband hotspots and provide some train service information, usually free of charge. Virgin, using Broadreach, has installed wireless service in first class lounges in 370 of its UK train stations, calling the service Carriage Connect. Roaming agreements with BTopenworld, Virgin.net, and iPass allow some users to avoid paying a separate fee for use of the system. Urban Hot Spots, among others, has installed service in Penn Station in NY. It is available for a fee of $6 per day or $30 per month. AT&T is providing service in six Northeast Corridor Amtrak stations, including New York, Baltimore, Providence, Wilmington, Philadelphia, and Boston. It costs $9.99 for non-AT&T Wireless customers for 24 hours of service. Swisscom provides service at seven SBB stations in Switzerland. Cegetel is installing a system at 50 SNCF stations in France, requiring users to sign up for Cegetel wireless service. InSite Wireless won a 15-year contract from the Massachusetts Bay Transportation Authority to install wireless antennas at 4 downtown Boston subway stations. The system was operational in fall 2005. InSite promised the city at least $4 million in exchange for the exclusive rights over the life of the contract.

Marinas

iDockUSA.com, a division of ICOA, provides access at 36 different marinas, primarily in California. It uses the broadband connection at the marina and broadcasts it out to the slips. Each account is allowed 3 users, and the system provides a bandwidth of 200 Kbps.

Gas Stations/Parking Lots

A few providers are targeting gas stations for wireless service. E-Plus has placed hotspots at Agip gas stations in Europe. Users choose between monthly plans and purchasing time on a per minute basis, with a minimum 30 minutes purchase. The monthly plans are scalable depending on how many MB the user downloads. E-Plus provides discounts for corporate customers. Mapesbury Communications has installed hotspots at Texaco gas stations in the United Kingdom. These hotspots are on the T-Mobile network. FreedomNet has employed its Mobility service in 9 parking areas in Michigan. Users parking in the areas can access the Internet from laptops inside their vehicle. FreedomNet charges $4.95 for 24 hours, $9.95 for a week and $19.95 per month. There are also more expensive monthly plans for higher bandwidth priority.

Non-Transportation Locations

Wireless technologies in use at non-transportation locations may eventually be applicable to a mobile on-board environment. Two of these technologies, WiMax and WAN, will be addressed. Additionally, business models utilized at non-transportation locations may be applicable to transportation systems and will be analyzed here as well. These systems can also provide usage data that allows a better understanding of the wireless user.

WiMax

WiMax is as of yet not a certified technology, meaning its systems aren’t interoperable and, there exists no common set of standards. It is still in development, and there is much debate regarding its future role in the wireless world. Some have deployed pre-WiMax systems, while others say that no true WiMax system has been developed. Many in the industry believe by the time WiMax is operable and certified, it will be surpassed in speed and range by 3G and Wi-Fi (802.11) systems. Nonetheless, an increasing number of communities are either installing or plan to install pre-WiMax. WiMax, known as 802.16e, is distinct in its long-range capabilities. Instead of signal strength tapering off at a 90 meters, its signal can reach up to 48 kilometers. In addition, it supports data transmission speeds up to 70 Mbps, as opposed to 802.11b's 11 Mbps or 802.11g's 64 Mbps. Mobile WiMax is not currently in use, meaning that the user must be stationary in order to be connected. This may change soon, as a mobile WiMax system is being installed by Nomad Digital on Southern UK trains. If mobile WiMax is successful, it could be the dominant future technology for wireless access on trains and vehicles since a small number of towers could cover an entire line without a break in service and at a high bandwidth. It may also prove very useful for rural, sprawling cities, allowing for long-range wireless connectivity instead of laying expensive wires. Skelleftea, Sweden has installed a system that reaches 31 miles to cover the city's 71,000 residents, with a bandwidth of 25 Mbps. The WiMax system was developed by MobileCity, a consortium of companies, universities and governments. The project is funded by the European Union. Mid-Uusimaa, Finland, has installed a Radionet/Wi-Lan WiMax system funded by Mäntsälän Sähkö, an energy company. It covers an area of 800 square kilometers and 60,000 residents. Irish Broadband Internet Services Ltd. is conducting a similar trial in Dublin. Houston County, Georgia, working with Intel, has proposed a system of two towers, each covering a 30-mile radius. The system will cost $2 million, which will be recouped by charging residents $15 to $30, plus $25 for a PC Card. They have yet to find an ISP, financing, or a supplier.

Wide-Area Network & Other City-Wide Systems

Tropos Networks

Tropos Networks' MetroMesh wireless systems provide connectivity for large municipal areas including Las Vegas, Los Angeles, and Tokyo. Their customers include 40 resellers and 125 municipalities. The company's product allows customers to deploy systems covering a very large area with minimal infrastructure. For example, the reseller developing the Las Vegas location expects to cover 100-square miles with the system. Transfer rates range from about 512 Kbps to over 1 Mbps. Three months after installation in Chaska, MN, 20% of the households in the 16-square mile city are paying

Tropos' $15.99 per month access fee. New Orleans law enforcement is using the system to provide video surveillance of high crime areas.

Sacramento Area - Surewest

Surewest has installed a system in the 916, 530, 209 area codes in the Sacramento, CA area. It requires users to have a Sierra Wireless Air Card to get service and is available anywhere in those area codes. The service costs $29.95 per month for a one-year contract, with a $25 activation fee. The speed of the service is limited to 40-60 Kbps.

Philadelphia

The City of Philadelphia's decision to install a city-wide wireless system has been much publicized and led to a public debate regarding the role of cities in providing technology. Successful phone-company lobbying resulted in a Pennsylvania state law banning cities from deploying city-wide wireless networks, although Philadelphia received an exemption. They have yet to choose a provider, but have promised that the system will be free in public areas and to households and businesses in need of assistance. It will cover 135-square miles, serving 1.5 million people from transmitters placed on light poles. The system will cost $10 million and will be funded through investments and run by a separate management company.

Athens, GA – UGA New Media Institute

Athens, Georgia, home of the University of Georgia, has installed an expansive Wide-Area Network. Funding is provided by the Georgia Research Alliance and the system is designed by the UGA New Media Institute. It is free to use and serves a role as an educational tool for college students. It only works outdoors and is designed for PDAs, so that it doesn't compete with local Internet Service Providers (ISPs). The network, covering 24 blocks of downtown Athens, allows students to develop add-on programs.

One such program allows you to see if any of your friends are also downtown. They hope to include local merchants into the program.

Others

A 512 Kbps system has been installed in Singapore by SingTel using 150 hotspots throughout the city. It costs $0.20 per minute for existing SingTel customers. SatXpro and Eutelsat installed a system in Valley of Esere during the International Show of the 4x4 in August 2003. Due to the remote nature of the conference site it required a two-way satellite connection, provided by Eutelsat. Eutelsat developed a similar system with France Telecom for use at the resort Alpe d'Huez during the Tour de France. The two-way satellite system provided 2 Mbps for downloads and 512 Kbps for uploads. France Telecom installed the hotspots that utilized the satellite connection and made it accessible to guests. The city of Taipei in Taiwan is installing a system that will be operational by the end of 2005. Developed by Q-Ware, the system will have 15,000 to 20,000 access points in the city and should handle the needs of the city's 2.6 million residents. Q-Ware spent $70 million on infrastructure and will recoup costs by charging users. Downtown Long Beach is expanding an existing system to include all of downtown. Funding is provided by several sponsors and suppliers, including Vernier, Color Broadband, Intermec, Development Tech, and G-site. As a result, it is free for users. Walnut Creek, CA, has a system developed by WCWiFi that costs $3.95 per hour, $6.95 per day, $14.95 per week, and $24.95 per month. Several other public areas, such as Union Square in San Francisco and the James L. Knight Center & Miami Convention Center in Miami, FL, have existing public access wireless systems as well. The Union Square location is free, provided by the city in an effort to encourage more shoppers. The Miami locations were developed by RoomLinX and charge for use.

Restaurants/Coffee Shops

Starbucks has probably been the most successful at increasing public awareness of hotspots due to its widespread rollout and the complementary nature of a coffee break and the Internet. Starbucks locations are on the T-Mobile system. All users are required to sign up for T-Mobile service, whether by subscription or on a prepaid time basis. Studies have shown that T-Mobile subscribers visit Starbucks more often- an average of 8 times per month- and spend more time in the stores. The average connection lasts one hour. Nearly 90% of T-Mobile HotSpot accesses are during off-peak store hours or after 9 AM.

McDonalds, after a trial program with multiple vendors, chose Wayport to provide wireless access in many of their United States restaurants. McDonalds tested several pricing methods, including bundling the service with Big Macs, but with Wayport selected a charge of $2.95 for two hours of access. It also allows Wayport users to sign on using their Wayport account. McDonalds pays Wayport on a per-store basis as well as a share of the walk-up access. They receive from Wayport a portion of the strategic roaming partner payments above a certain amount.

Schlotzsky's, a national deli-chain, provides free wireless Internet at 38 Cool Deli Schlotzsky's. Forty percent of their customers say that free Wi-Fi or the free use of in-store computers are factors in choosing the deli. Six percent say that free Wi-Fi is the key reason they went to a Schlotzsky's that day. The system extends up to ¼ mile outside the restaurant as well.

United Restaurant Development provides free Wi-Fi access at 15 of their sites in the United Arab Emirates, including Cinnabon and Seattle's Best Coffee locations. HMS Host, an airport concessionaire, provides Wi-Fi access at a cost of $7.95 per day at various locations in Anchorage, La Guardia, San Diego, Miami, and Palm Beach airport locations. The Panera Bread Company provides free access, using an ICOA system, at over 600 locations throughout the US.

Other Locations

Two major ballparks have wireless connectivity available for their fans. SBC Park in San Francisco uses a Nortel system, sponsored by the San Francisco Giants and SBC. One hundred twenty one access points are used to provide stadium-wide access. It was free for the 2004 baseball season. Access included the Giants Digital Dugout, which is comprised of statistics, highlights and other in-game information. Possible future uses include the ability to order food, watch replays or keep score electronically. The system provided a bandwidth of 2 to 5 Mbps. An average of 200 fans used the service per game. Minute Maid Park in Houston, using a Cisco and Wide Area Management Services system, is the other major ballpark location. The project is run by Time Warner Cable-Houston. They charge users $3.95 for four hours of access. In October, when the Houston Astros were in the playoffs, they had a total of 613 users, for 1500 hours of total connection time.

Jukeboxes in 2,700 restaurants and bars in all 50 states are slated to provide wireless Internet courtesy of ecast and Pronto Networks. Pricing and details of the rollout were not available.

Car rental companies Hertz and Avis are implementing public wireless Internet access at their rental counters, with eventual rollout to their vehicles. Hertz recently became a Wayport strategic partner. Users with a Wayport account can access the Internet in Hertz's waiting areas and parking lots. In a unique partnership, Wayport hotspot locations will show up on Hertz' NeverLost in-car navigation system, allowing drivers to get directions to the nearing hotspot. Hertz's competitor, Avis, contracted SBC to add 88 Avis locations to its FreedomLink network in 2005.

Future Technology

The CAPANINA project, involving 14 corporations, universities, and research institutions, is developing "wireless and optical broadband technologies for use on High

Altitude Platforms (HAPs)." These HAPs are floating airships that reside at an altitude above airplane flight paths, but within the atmosphere. They hope to use these HAPs to provide broadband communications over a very large area under the airship. They pledge data transmission rates of up to 120 Mbps, with mobile connectivity. The CAPANINA project hopes to deliver broadband access within 3 to 5 years, with mobile access two years later. The projected cost is one-tenth that of satellites, while serving 1,000 times more users than a satellite within its coverage area.

Wireless Providers

Several hundred wireless Internet service providers (WISPs) and wireless aggregators operate hotspots in 96 countries worldwide. Some, such as T-Mobile, SBC and Swisscom stretch across national borders, while others such as FreedomNet, Kubi Wireless, and Meteor have a smaller geographic base. Aggregators, such as iPass and Boingo, integrate the hotspots run by numerous WISPs into their billing and authentication program, allowing subscribers to seamlessly access far more hotspots than those operated by just one company. They develop roaming or partnership agreements with each WISP to allow the sharing of customer account information. This allows them to have very large hotspot footprints. Through roaming agreements, Boingo has 13,000 hotspots, iPass has over 20,000 in 150 countries, BT Openzone has 7,000 and Wayport has over 4,700. Roaming agreements in some cases allow users of either of the partner companies to access the other's systems. For example, T-Mobile and BT Openzone customers can access either company's hotspots, although for an additional fee. In iPass's case, they don't operate any hotspots, but merely aggregate others, so their partners do not gain additional hotspots through the partnerships.

Each WISP and aggregator offers a different pricing structure, complicating the marketplace. For example, the price to use Connexion by Boeing is different depending on whether you are a customer of iPass, NTT DoCoMo, Singtel or none of the above. In addition, some do not provide access to individuals, or do not advertise their rates, except at each hotspot location. For example, iPass only deals directly with business customers, with wireless charges customized for each account. For some companies, roaming capabilities are included in the basic account, while others charge users additional fees or have different plans for roaming. AirRover is on the Airpath network, but access to those additional locations costs an additional $20 per month. SBC charges users $20 more per month as well to access partner locations such as those operated by Concourse Communications and WeRoam.

The pricing structure of 45 different wireless providers was examined. To allow comparison, all prices were converted into dollars. As exchange rates fluctuate constantly, these prices are not precise in today's dollars, but are approximately accurate. The most common form of access one can purchase is either in a 24-hour continuous increment or a monthly subscription. Other access types included per minute, per 10 minutes, per 15 minutes, per 30 minutes, per hour, per 2 hours, per 4 hours, per week, per 6 months and per year. In addition to their time-based charges, some companies charge an additional fee based on megabytes transferred. Per connection fees are also somewhat common. Many of the larger providers offer existing cellular or long-distance customers significant discounts. For example, SBC offers SBC Yahoo! DSL users the option to pay just $1.99 per month for hotspot access with a yearlong subscription. Another provider, SingTel waives its $10.50 subscription fee for existing customers.

A few of the larger providers and those with unique pricing strategies are discussed in more detail below.

Boingo

Boingo has over 13,000 hotspots at a wide variety of locations in 39 countries. Boingo's 186 airport locations include LAX, DFW, LGA and MIA. There are 1,981 hotspots in restaurants and cafes, 2,702 in hotels, 255 in retail stores and 50 in convention centers. These numbers increase almost daily. Boingo pays hotspot operators $1 to $2 per connect day and $20 to $50 for new customers. It allows VoIP, the ability to use the telephone over the Internet, through an agreement with Vonage. Boingo charges users $7.95 for two 24-hour connections at the same location, or one can pay a monthly $21.95

subscription fee. Partners include Concourse Communications, ADP Telecom, TelMex, Earthlink, and Fiberlink.

iPass

iPass has over 20,000 locations throughout the world. It sells directly only to corporate customers and does not post its fees on its website. An individual user may gain access by purchasing the service from one of iPass's resellers. A search of their website yielded a list of 10 such resellers in the United States. One reseller, Net-roamer, charges $0.15 per minute, with a daily maximum of $20.50 for North American users. Another reseller, EZRoam, charges $0.12 per minute, with a daily maximum of $16.20 at each location. A third, Central House, charges a $10 account setup fee, $8.95 per month, and $0.12 per minute. Additional plans offered include a flat $58 per month payment and $540 per year payment. iPass has agreements with seemingly every hotspot provider. Provider partners include Kubi Wireless, Airpath Wireless, Concourse Communications, FatPort, Wayport, Monzoon Networks, Swisscom, Connexion, and T-Mobile. iPass customers using T-Mobile locations pay a flat $9.99 per day fee.

GoRemote

GoRemote is very similar in its operations to iPass. It has 7,800 Wi-Fi hotspots in 45 countries. 3,792 are in cafes/restaurants, 2,478 in hotels, 37 in convention centers, and the rest are in other locations. They also provide Ethernet access in over 250,000 hotel rooms and provide over 48,000 access points, including dial-up numbers. Wi-Fi providers with agreements with GoRemote include Wayport, STSN, Connexion, and at least 50 others. They also do not sell directly to the general public. In the United States, one can purchase service through six different resellers. One such, Roadpost, charges $19.95 per month, plus $0.12 per minute at most Wi-Fi locations. Dial-up and Ethernet access has different pricing rates. Another, Dialer.net, charges $0.199 per minute, or $20 for 24 hours of continuous access, with no monthly fee. They also have special corporate rates. In early 2005, GoRemote announced roaming agreements with SBC Communications and Connexion by Boeing.

SBC FreedomLink

SBC has over 6,000 hotspot locations, including at Barnes & Noble bookstores, The Coffee Bean coffee shops, Avis car rental counters, SBC Park, and Michigan and California State Parks. They are also the cheapest hotspot provider for those using SBC Yahoo! DSL. With a year-long commitment and the DSL service, customers can get a $1.99 per month subscription that gives them access to all SBC locations. Those who are not prior customers can pay $19.95 per month for access to SBC locations plus $4 per use of a roaming partner's site or $39.95 per month for use of all partner locations. Both monthly plans require a year-long subscription. Partners include Concourse Communications, Wayport, Telmex, iPass, GoRemote, and Syniverse. In addition, SBC allows the user to pay per connection. Three connections cost $25, eight cost $50, and 20 cost $100.

T-Mobile

There are over 11,500 T-Mobile hotspots, including at Borders, Starbucks, Hyatt Regency's, Kinkos, and several airline lounges. T-Mobile USA and T-Mobile UK charge their users different rates, although international roaming is allowed. T-Mobile hotspot users have a variety of payment options. American users can purchase one hour of use for $6, one day of use for $9.99, sign up on a month-to-month basis for $39.99 per month, or sign up for a year-long subscription for $29.99 per month. These pricing plans are available at virtually all T-Mobile locations. T-Mobile cellular customers get 50% off these rates. T-Mobile has roaming agreements with BT Openzone, Comcast, AT&T Wireless, Concourse Communications, and iPass. T-Mobile UK customers will have seamless access to the wireless internet system being installed on Southern's London to Brighton line.

Wayport

Wayport has over 6,300 hotspot locations, including at least six airports, McDonalds, Hertz car rental counters, and several Oakwood corporate housing properties. Wayport logged over 5 million Internet sessions in 2004. They recently completed partnerships with Zinio and Newsstand to provide digital magazines and newspapers for their customers. Wayport charges $9.95 per connection for hotel users, $6.95 per connection for airport users and for all others. Three connections cost $25, eight cost $50, and 20 cost $100. In addition, monthly plans cost $49.95 on a month-to-month basis and $29.95 with a year-long commitment. Corporations can get reduced rates with 50 or more users. Wayport reached an agreement with SBC, allowing SBC customers to roam at any location on the Wayport network. They also have agreements with Sprint and Boingo, but they do not apply in hotels or McDonalds locations. These partners pay $32 per month, per Wi-Fi World Site providing access to their customers. Wayport locations will be listed in the Hertz NeverLost in-car navigation system, allowing Hertz customers to easily locate Wayport hotspot locations.

DotSpot Wireless

DotSpot Wireless only has one location so far, The Car Spa in Southern California, but it is unique in that it provides access for free. It uses the DotSpot Wireless Ad Server to bring advertisements to users. The ad revenue pays for the service. These ads show up every five minutes, with flash ads every thirty minutes, but there are no pop-up ads. DotSpot provides the equipment and technology for an initial fee to the service provider. The service provider also gets free advertising on the network. The willingness of the consumer to tolerate advertisements will be the determining factor in the success of this business model. They are initially focusing on the automotive service sector, followed by the medical industry.

Transnet Wireless

Transnet Wireless uses private distributors or individuals to deliver its service to the public. They sell the machine and the network access to a distributor. The distributor then receives the fees charged to the user of the machine, giving a percentage back to the provider. Each ATM-style unit costs $11,995 and provides wireless access at a range up to 300 feet. These systems will be installed in Illinois parks. Roaming agreements are in place with Spring, iPath, GRIC, Airpath, BT, Picopoint, FatPort, and Kubi Wireless.

Train Providers

There are numerous players in the on-train wireless Internet market. Some competitors already have products in operation, such as Icomera AB and PointShot. Others are just in the testing phase, and yet others have just announced products and are further from reaching the marketplace. Some companies have developed a since discontinued product.

Current Market Competitors

PointShot, based in Ottawa, operates a system called RailPoint utilizing a satellite download and GPRS or 3G upload. It is currently in operation on train lines in Canada, Northern California and is planned to provide service in the United Kingdom. PointShot systems achieve an on-train transfer rate of 400 Kbps. PointShot Wireless determined that 30% of train passengers in their free trials accessed the Internet wirelessly, with an average of 45 minutes per session. Broadreach, based in London, reached an agreement with PointShot to use their technology in European markets. Currently, Broadreach is in 370 United Kingdom train stations, under the ReadyToSurf name. They hope to have most of the United Kingdom’s rolling stock Wi-Fi capable within two years. Of those participating in a Broadreach survey, 42% would be very interested in using Wi-Fi on a train. Thirty percent in the same study predicted an average log-on time of between 30 and 60 minutes. PointShot also has an agreement with Appear Networks, based in

Stockholm, to develop time, location, and user-dependent information systems. Appear Networks currently provides services for networks in Paris and Sweden.

Icomera AB, based in Sweden, developed a very similar system, called Wireless Onboard Internet. It uses a combination of GSM and satellite technologies. Icomera systems are also capable of receiving digital TV. They have systems currently in operation in the UK and Sweden/Denmark. Their systems also achieve an operational transfer rate of 400 Kbps.

Competitors with Technology In-Development or Testing

21Net, based in the UK, has developed a system allowing a two-way onboard satellite connection. It uses a satellite connection for downloads and a combination of satellite, GPRS, and 3G for uploads. In testing, it reached a transfer rate of 700 Kbps. Due to the faster upload capabilities, it will be able to provide video conferencing, in addition to TV reception and Internet access.

Wi-Lan, based in Canada, and Wellink, based in South Korea, has developed Mobilis, which they label the first commercially available two-way broadband wireless product designed for a high-speed mobile environment. Suggested applications include real-time video surveillance, streaming advertising and Internet access. They claim that Mobilis has a bandwidth of up to 32 Mbps, which would allow for streaming video. The product has been tested at speeds up to 110 km/hr. Instead of using satellites, Mobilis uses track-side access units that are connected to a land-based backbone and handles service via their Sequential Soft Fast Handoff. In addition, it places a mobile unit on the train car to exchange information with the track-side devices. An antenna instead of a satellite dish is needed for this communication, allowing for a smaller on-vehicle device. They have not announced deployment on any rail lines.

ZealConnect is installing its Pulz8Express service on Denmark trains in 2005. It uses track-side base stations to provide access to train passengers. It claims a transfer speed that will be better than asymmetric DSL (ADSL). ADSL has a 1.5 to 9 Mbps downstream rate and a 16 to 640 Kbps upstream rate.

RailTel, a state-owned communications company, is placing track-side base stations along rail lines in India. These track-side devices should provide transfer rates up to 2 Mbps. They will only work with cars with closed doors and windows.

New Jersey-based Lucent, Vancouver-based In Motion, and Beijing-based Top Global are developing a system called Wi-Fi on the Move that focuses on 3G technology. It has a maximum speed of 300-500 Kbps and is not deployment ready.

RaySat, based in McLean, Virginia, has two products that are capable of providing on-train Internet access. One, called Torpedo Ray, is in use on European trains. It uses a satellite download with a cellular upload. The system includes TV, Internet, and a rear-seat entertainment system. The second product, announced at the end of 2004, called EagleRay, uses a two-way satellite connection via a 5.5" tall antenna mounted on the vehicle.

Nomad Digital, a UK company, has developed a pre-WiMax mobile system for use on Southern trains on its London to Brighton line. It has the potential to provide the fastest data transfer speeds as a result of the placement of WiMax devices trackside every 3 kilometers. The system, developed with Redline Communications, will potentially provide up to 32 Mbps of bandwidth.

Mesh Networks, based in Florida, is adapting mesh network technology for use on rail. This uses several track-side routers that communicate with each other to provide continuous service. Mesh Networks was purchased by Motorola in November 2004.

Companies with Suspended Products

NRoute Communications developed one of the first on-board Internet systems for use on Amtrak's Keystone Corridor in late 2002. Amtrak installed touch-screens on the back of each seat, allowing users to watch movies and TV as well as access the Internet. They planned to add laptop access capabilities as well as pay-per-view movies. It used satellite, GPS and a local caching server to provide access. The project was funded by a $155,000 grant from PennDOT.

Compaq and Yahoo! developed a program for use on Amtrak Acela, Capital and Hiawatha trains in 2002. Compaq Pocket PCs were mounted on one car on each train, with wireless connectivity provided by Yahoo! Users could surf the Internet for free.

Spotnik, a branch of TELUS, developed a satellite download/cellular upload system for trial use on the VIA Montreal to Quebec City route. The system reportedly achieved speeds of 1-2 Mbps during its trial, which began in February 2004. Station lounges in Montreal and Quebec City were incorporated into the program as well. Users could borrow a palmOne handheld for use on the train as part of the program.

Business Models

Transportation Systems

There are very few examples of mobile on-board Internet access pricing structures. The majority of on-board wireless systems are in a trial phase, and as a result are free. Several systems bundle access with a first class ticket. Companies offering bundled access include PointShot, Icomera, and Zealconnect. The Northern California ACE rail line provides free access through corporate support. The only systems currently offering subscription plans are on-automobile two-way satellite providers. These plans start at $60 per month, but they aren't comparable to on-bus or on-train systems because they provide only stationary access and aren't designed for commercial distribution of bandwith. There are a few time-based purchase options. Two of these, WiFirst and Meteor, provide access along an RATP bus line. On-airplane systems generally charge by use, or by flight segment. Such systems include Connexion, Netvigator and Tenzing. There are too few existing pricing structures for in-motion on-vehicle devices to develop some sort of clear picture of the user's willingness to pay. In each case, a unique factor such as the lengthy user capture on a cruise line, the generally higher European rates, or the lengthier duration of an international air trip prevent application of these price structures to use on Amtrak trains in the U.S. The Nomad Digital system being installed on UK trains will be groundbreaking in that it will be the first mobile system aligned with a WISP network, in this case T-Mobile. It will be seamlessly integrated into the T-Mobile network and is scheduled to charge the same rates as all other T-Mobile UK hotspots. This will likely be more common for mobile systems in the future since it provides the most convenient access to the passenger.

A 2004 BWCS data survey forecasted that rail passengers will spend $420 million per year on mobile Wi-Fi services by 2008. The survey conducted with 1600 UK rail passengers, yielded the following results:

- 78% of business travelers are interested in using Wi-Fi on the train;
- 72% would be persuaded to take trips via train rather than by auto or plane;
- Users are willing to pay $9.27 per hour on a per minute basis, or a flat fee of between $9.27 and $14.82 for trips under two hours and between $12.97 and $22.24 for trips over two hours;
- Users are willing to pay between $27.80 and $46.33 per month for unlimited access;
- 65% expect to pay via credit card or their existing WISP, and 28% expect it to be bundled in the price of a ticket.

The results of the survey, given in British Pounds, were converted to American Dollars. One must keep in mind the generally higher Wi-Fi access fees in the United Kingdom and Europe before applying these results to train systems in the United States. Also notable is that the survey was conducted with commuters already using rail.

In an unstrung poll of air passengers, 80% indicated that the availability of Wi-Fi connectivity could affect their decision on which carrier to fly. Only 18% of the respondents are willing to pay more than $10 for the service, while 41% expect it to be free.

Transportation Terminals

Transportation terminals can provide more examples of public wireless Internet access pricing structures. A few airlines bundle access into their first class lounge fees. Several airports and rest stop providers provide free access as an informational feature or use generator. Monthly subscription plans are available from a few companies. These plans range in price from $19.95 to $29.95. The most common consumer purchase option is the 24 hours of continuous access plan. Airport wireless providers such as Concourse Communications, Massport and HMS Host, as well as road-side providers Flying J and Freedom Net, give this purchase option to their customers. One-day continuous access costs between $4.95 and $7.95. Thirty-day continuous access is also available from marina operator iDock and a few roadside operators at a price range of $24.95 to $49.95. Several hotspot network operators, such as AT&T, Bell Canada, Boingo, BT Openzone, ICOA, iPass, Kubi Wireless, and Orange have hotspots at several transportation terminals. Access fees charged at these locations are the same as at other hotspots on their network. Therefore their fees will be analyzed in the next section.

Hotspot Network Providers

In most cases, various hotspot locations provide the same level of service, whether it’s in a coffee shop, a McDonalds or in an airport lounge. Therefore, one would expect their prices to be similar. A Research and Markets study of European hotspots determined that prices in an area are uncorrelated with density of hotspot providers in the area. A few of the operators charge per minute or megabyte, or offer scalable packages. Therefore the plan chosen by the user and the fees incurred depend on the frequency and duration of use. In addition, while most operators offer a per-hour or per-day purchase option, those are certainly not the only access options a user may face. The fees charged by 45 different hotspot operators were catalogued and plotted. All of the available subscription and time plans were listed. It was assumed that the wireless user did not have a pre-existing subscription with the operator that would earn them a discount, for example SBC's fee of $1.99 per month for existing DSL subscribers.

The most common type of time duration access option was the monthly subscription, provided by 29 of the 45 operators. Only 7 of the 25 North American operators did not have a monthly option. The second-most common option is the 24-hour continuous usage plan, offered by 27 operators. 18 have a per-hour fee and 12 have a year-long subscription option. Other time duration options provided by several operators include per minute, per 15 minutes, per 30 minutes, per 120 minutes, and per week.

Indiscriminate of the type of usage pattern, North American wireless providers charged far less than their international counterparts. The average price for one hour of continuous service worldwide is $7.77, and only $4.02 in North America. A BroadGroup study of 122 European providers determined that 50% offered the one-hour pricing option, with an average price of $7.33, close to the average calculated in this study. They noted that the average price for one-hour of Wi-Fi access in Europe fell 11% in 2004. The average price for 24-hours of continuous service from the providers in this study is $19.27, but only $8.28 for the 25 North American providers analyzed. The BroadGroup study calculated that 58% of those studied offered the 24-hour pricing option, with an average price of $19.25, also very close to the average calculated here. The average month-to-month subscription in this study is $45.85, but only $32.49 in North America. The average monthly or pre-paid year-long subscription is $584.23 ($48.69 per month), and in North America is $306.91 ($25.58 per month). The per-minute rates were similar ($0.24 worldwide and $0.23 in North America), but that is likely due to the small number of operators providing that option. To show this contrast, as well as to allow the North

American prices to be easily separated, the North American and non North-American prices were plotted in different shades. The non-North American prices are plotted in a lighter shade of the same color as the North American prices.

In the first figure, Figure 1, the time in minutes is plotted against the fee for that period, both on a logarithmic scale. In this case, the usage pattern determines actual fees incurred for those plans with variable pricing dependent on MB transferred or minutes in the session. The plans were converted into the number of minutes that a user could theoretically use the plan, for example the minutes available for a year-long plan is the number of minutes in a year. One can see that there are a few outliers, but for most time durations, North American operators were exclusively cheaper than their international counterparts. This is especially noticeable in the 24-hour and year-long plans. Those time durations only offered by one or two providers, including 10 minutes, 4 hours, and 6 months, were not plotted on the charts.

Since users won't actually use the wireless Internet every minute of a 24-hour period, let alone every minute of the month, to determine the rates facing the user and the plan they will most likely select, the price per minute of use for each of the plans was analyzed. This is the rate at which a user will pay per minute of actual Internet usage. Four different usage patterns were used in this analysis and are plotted in Figures 2-5:

- A frequent, short duration user who mainly checks their e-mail
    - 15 minutes per use, 5 uses per week for a total of 300 minutes and 10 MB per month;
- A frequent, medium duration user such as a train rider
    - 60 minutes per use, 5 uses per week for a total of 1200 minutes and 20 MB per month;
- An occasional, long duration user such as an airport user
    - 120 minutes per use, 0.5 uses per week, for a total of 240 minutes and 10 MB per month;

- An occasional, very long duration user such as one who may use Wi-Fi for business
    - 240 minutes per use, 2 uses per week, for a total of 1920 minutes and 40 MB per month.

The fee for each time period was divided by the amount of time the user would use the Internet, according to these usage patterns, to come up with the fee per minute. For the frequent, short duration user, the cheapest option is the year-long plan, which costs an average of $0.16 per minute ($0.09 in N. America). The most expensive is the day-long plan, which costs an average of $1.31 per minute ($0.54 in N. America). While there is a large discrepancy between the rates of North American and international providers, the type of plan that is cheapest to the user is similar. For the frequent, medium duration user, the cheapest is the year-long plan at an average of $0.04 per minute ($0.02 in N. America). The most expensive is the day-long plan, which costs an average of $0.33 per minute ($0.14 in N. America). For the occasional, long duration user, the cheapest is the per hour plan at an average of $0.13 per minute ($0.06 in N. America). The most expensive is the per week plan, which costs an average of $0.38 per minute ($0.18 in N. America). For the occasional, very long duration user, the cheapest is the per-year plan at $0.03 per minute ($0.01 in N. America) and the most expensive is the per-minute plan at $0.24 ($0.23 in N. America).

Figures

Figure 1
Price vs Time Period
15 mins/use, 5 uses/wk, 300 mins/mth, 10 MB/mth

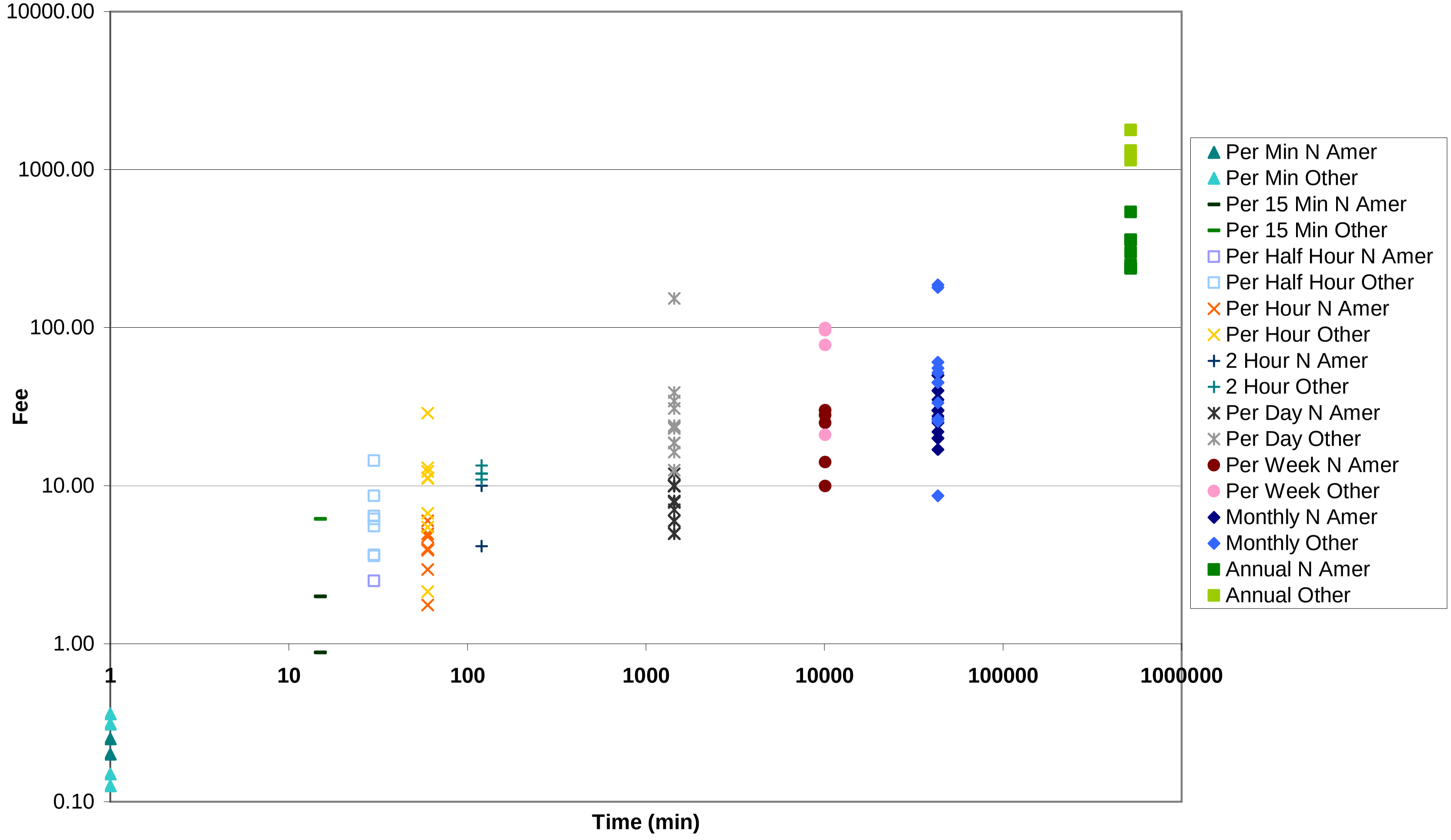


Figure 2
Price/Time vs Time Period
15 mins/use, 5 uses/wk, 300 mins/mth, 10 MB/mth

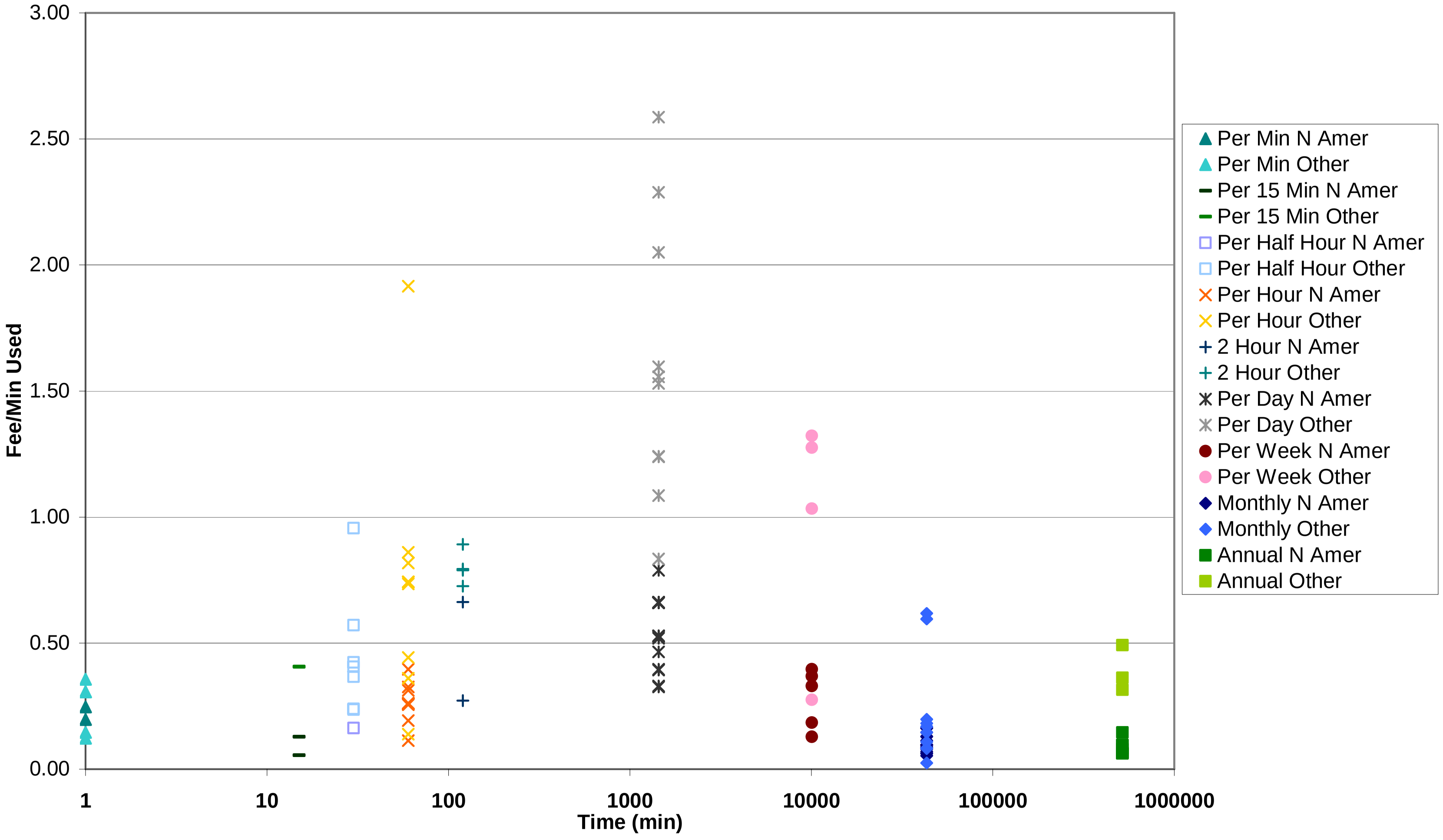


Figure 3
Price/Time vs Time Period
60 mins/use, 5 uses/wk, 1200 mins/mth, 20 MB/mth

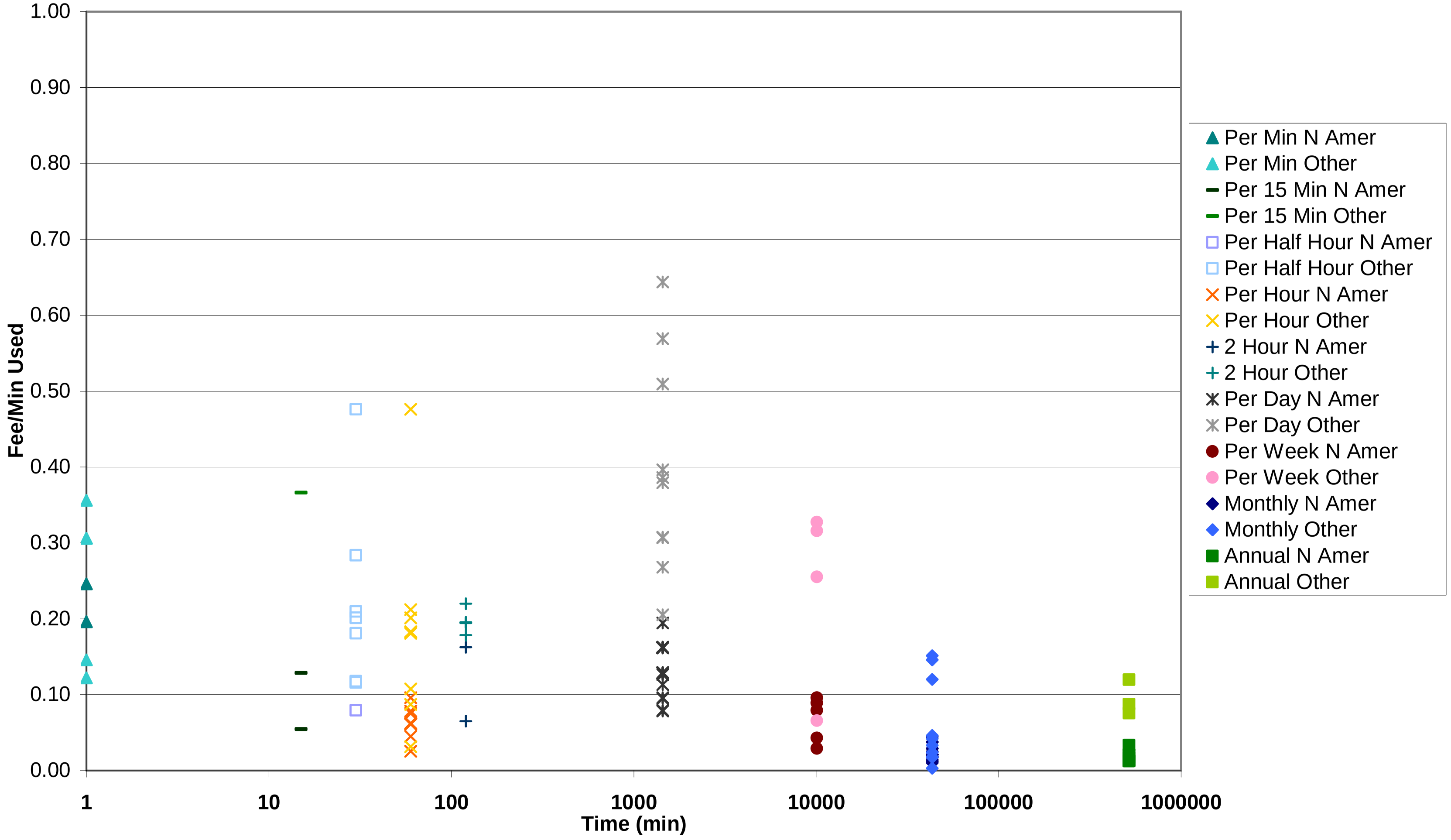


Figure 4
Price/Time vs Time Period
120 mins/use, 0.5 use/wk, 240 mins/mth, 10 MB/mth

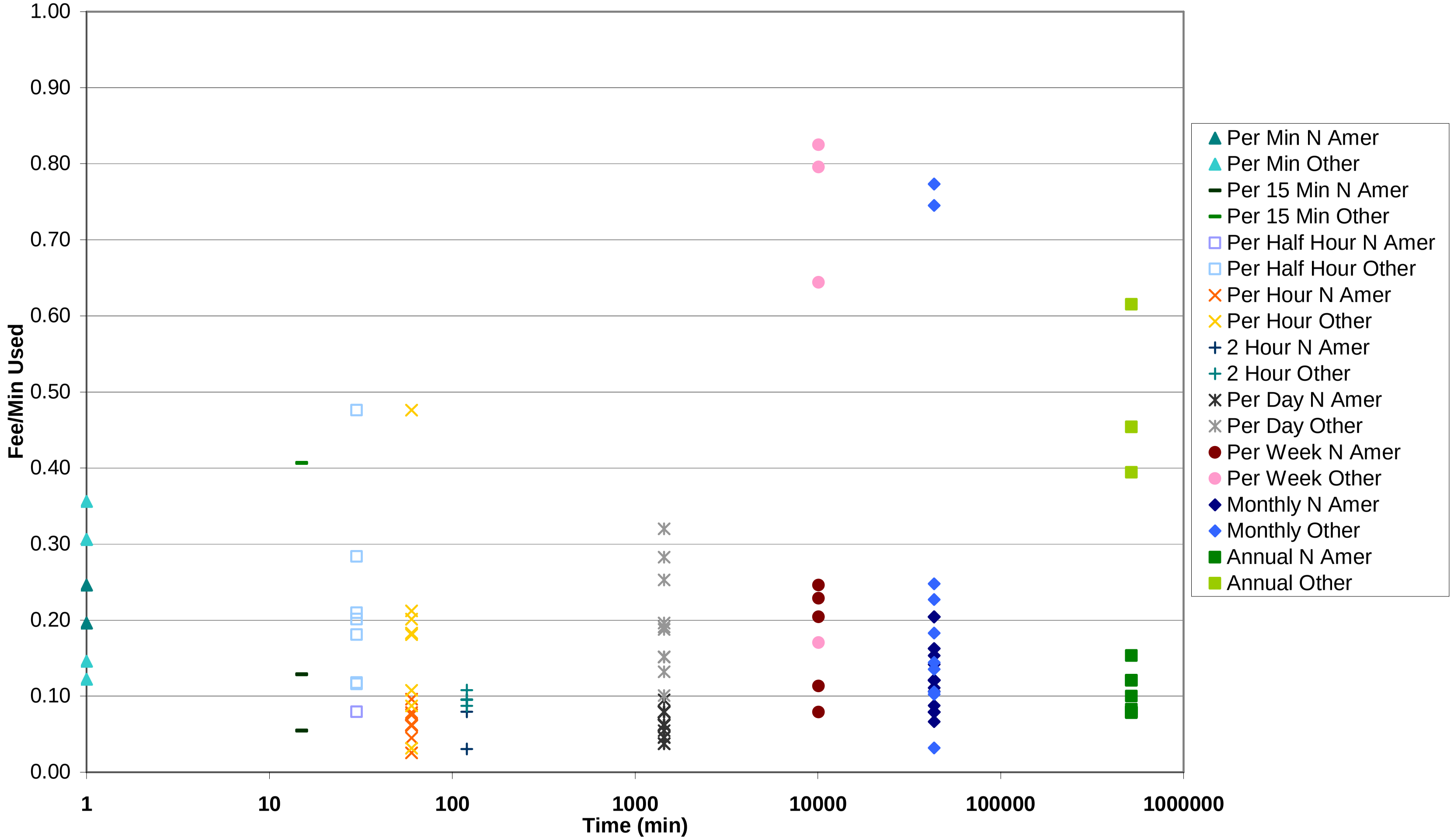
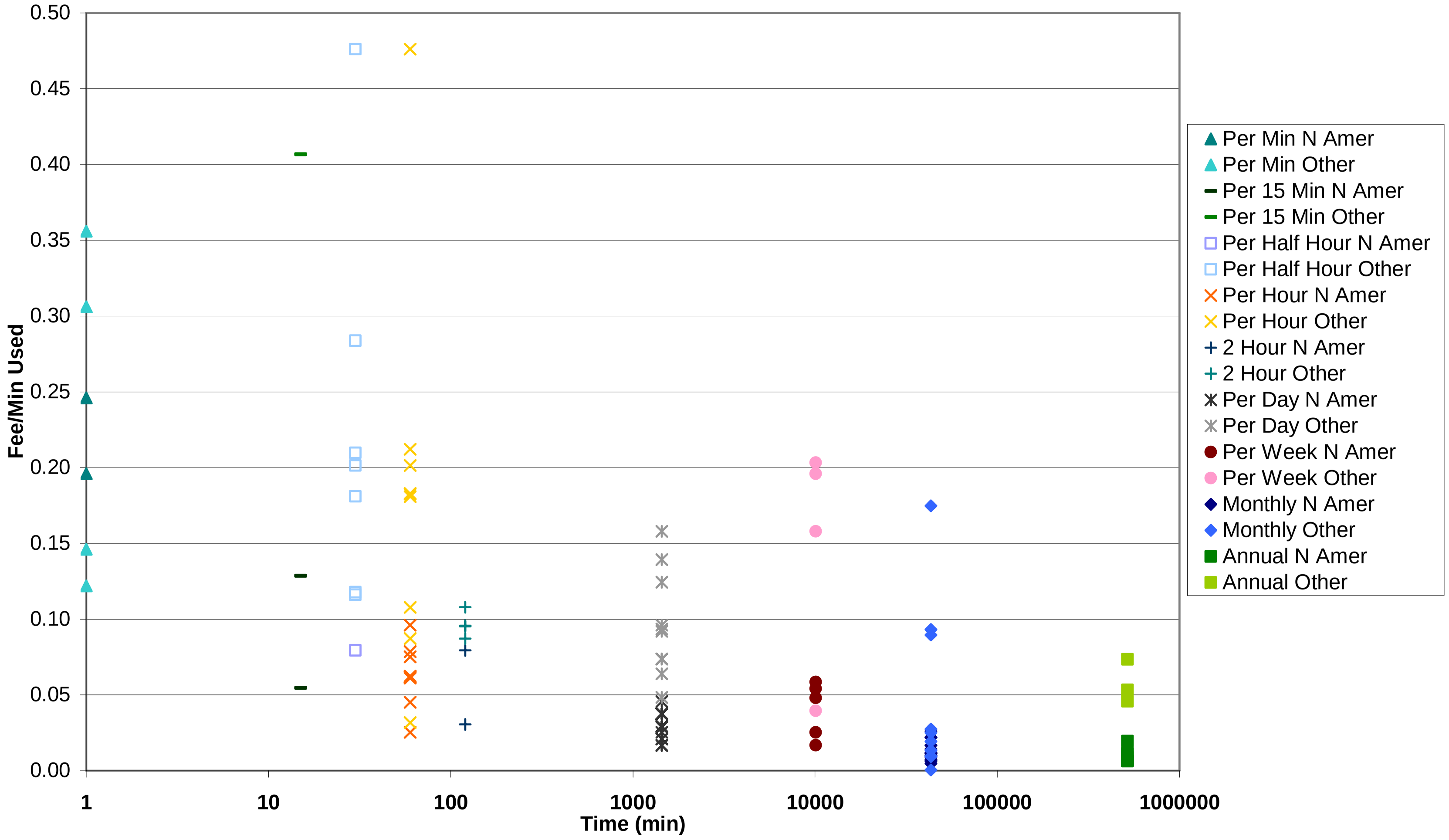


Figure 5
Price/Time vs Time Period
240 mins/use, 2 uses/wk, 1920 mins/mth, 40 MB/mth



Appendix B

Wireless Internet on Capital Corridor Trains

Revenue Forecasting Procedure

Adam Dankberg
California Center for Innovative Transportation
Institute of Transportation Studies
UC Berkeley

June 14, 2005

Table of Contents

Introduction.. 1
Capital Corridor Ridership Data 1
Number of Riders.. 1
Travel Time... 2
Travel Frequency 3
Revenue Projection 4
Survey 4
Revenue Projection Methods 6
Method 1 6
Method 2 6
Sample Projection 7
Other Revenue Sources.. 8
Conclusion 8

Introduction

This appendix outlines a process for which the revenue potential of wireless Internet on Capital Corridor Amtrak trains can be calculated. A multitude of business models for the provision of wireless Internet can be implemented that incorporate numerous revenue sources. Potential revenue lies in areas such as per use or time charges, subscription fees, advertising, sponsorship, or merely in additional ridership generated by the service. Additional revenue, either through an increase in duration of wireless use or an increase in users, is possible through traditional, non-mobile provision of wireless capabilities in Capital Corridor stations. A seamless integration between the mobile and non-mobile aspects would increase use of the in-station services. In addition, a wireless system may decrease cost or increase efficiency in such areas as security, ticketing, and marketing. The revenue source that lends itself most easily to forecasting is user fees. The benefits of a wireless Internet system may outweigh the costs even without the inclusion of user charges. If the increase in ridership, efficiency, or security is significant enough user charges may not be necessary or wanted. This report merely forecasts what revenues may be generated by user charges if such a business model is chosen. The revenue forecasting methodology is based on the Capitol Corridor Ridership data and the possible pricing models derived from the weekday and weekend train riders.

Capital Corridor Ridership Data

Number of Riders

The number of riders is derived from the historical train ridership data obtained from CCJPA. The period primarily analyzed was from September 1, 2004 to March 31, 2005. A few trends are noteworthy in the data. Weekday ridership is significantly higher than weekend ridership. With exceptions for holidays, weekday ridership generally ranged from 3,000 to 5,000 trips per day. Weekend ridership ranges from approximately 1,500 to 2,500 trips per day. Over that period, ridership trended upward by 0.8 trips per day on weekdays. On weekends it trended downward by 0.5 trips per day. When data dating back to October 1, 2000, is included these trends are less significant, as ridership only increased by 0.1 trips per weekday and by 0.3 trips per weekend-day over the 4.25 year span. From this data it is apparent that weekdays will generate the vast majority of revenue from users. An analysis of weekday-only revenue will likely capture a large portion of the revenue potential of the service.

This forecast is conservative in that it does not attempt to predict how many people will switch from their cars to the train as a result of the increased service. Therefore the pool of potential users analyzed is only those making up the current ridership, assumed in this study to be the average daily ridership during the September to March period. It is expected that usage patterns will be different on weekdays and weekends as a result of the difference in ridership composition. Therefore, weekday and weekend data were separated and should be analyzed separately.

Travel Time

If fees are applied based on usage time, then a rider with a short trip will generate less revenue than a rider with a longer trip. It is also expected that the percentage of usage will differ based on trip length. A user traveling two hours will gain more utility from being productive during that period than a user traveling for 30 minutes who barely has time to start their computer. Therefore the data were further disaggregated by origin and destination. The total ridership between each of the 15 stations over the September-March period was calculated by summing the ridership between each origin-destination (O-D) pair for each day. This period has 130 weekdays and 51 weekend-days. From this information, the average weekday and weekend-day O-D ridership was determined.

To determine the time that a user will be onboard and therefore would have access to the wireless services, the train service schedule was analyzed. The time between each station was obtained from the online Capital Corridor schedule. In some cases different trains have different times between stations – in each of these cases the average travel time was used. There are slight differences between the weekend and weekday travel times, so the two periods were analyzed separately. From the schedule, an O-D travel time table was created. See Appendix for table. The travel times range from 7 minutes between Berkeley and Emeryville to 257 minutes from San Jose to Rocklin.

These data are presented below as a cumulative distribution function. It indicates both the percentage and total number of riders with a trip length shorter than a given amount. For example, 27% of weekday riders are on the train less than 60 minutes and will probably have a lower wireless internet usage rate. Ten percent of weekday riders are on the train longer than two hours and will likely have a very high demand for Internet services. The average weekend travel time is longer, likely because there are fewer work commuters and more vacationers. Only 10% are on the train for less than 60 minutes and 21% are on the train longer than two hours. Thus while demand is expected to be lower on the weekend since ridership is made up of fewer workers, this is somewhat mitigated by a longer trip length and therefore more time to use the services.

Travel Frequency

The distribution of the riders' trip frequency is important in determining what type of pricing plans to offer and therefore impacts the total revenue projection. Survey data are expected to indicate different demand rates among the different traveler types. It is expected that daily commuters will prefer a monthly plan and will wish to only pay a flat fee for a month's worth of use, while the occasional traveler will pay a per hour price. Those that ride everyday will gain more from internet access because they may be able to reduce their in-office time by billing time spent on the train. In addition, they will gain tens of hours of productivity time over the course of a month, or even week. The occasional vacationer or business traveler may only gain a short amount of productivity time or enhanced leisure, which likely has less value. To determine the type of rider currently on Capital Corridor trains, passenger survey data were obtained from the CCJPA. In particular, the questions regarding the type of trip, the frequency of trip, and the origin and destination of the trip were examined. Just over 50% of riders who travel over 20 times a year (barely more than one trip a month) are on their daily commute to or from work. It is likely that this 50.2% of riders will be the primary users of the services. An additional 27.5% of riders traveling 20 or more times are on their commute to or from work, but don’t use the train on a daily basis. Of all riders, 14% travel 300 or more times per year, 11.8% travel 151-300 times per year, 5.2% travel 101-150 times per year, 20.2% travel 20-100 times per year, and 48.8% travel less than 20 times per year.

Revenue Projection

These information sources: the ridership data, the schedule and the CCJPA survey, were used to calculate the average number of riders per day by travel time and frequency. It is apparent that the weekday and weekend have different ridership patterns and will also likely have different Wi-Fi service demands. It is also notable that the vast majority of riders have a travel time between one and two hours and that half of these riders use the train less than 20 times per year.

Survey

The revenue projection is dependent on the number of users, the price of each of the service packages offered and the distribution of user demand between each of these packages. To guide projections of user demand and user willingness to pay, a survey was conducted on Capital Corridor trains in the summer of 2005 once trial service was implemented. This survey is attached in the appendix. The results of the survey were not available at the time the draft was written.

The number of wireless users is determined from current ridership, analyzed with respect to travel time and travel frequency, and forthcoming survey data. Specifically, the percentage of survey respondents indicating they would be willing to pay for services multiplied by the number of existing riders will produce an expected user base. The survey additionally asks the frequency of train ridership and the origin/destination of that trip, allowing for segregation of the data by travel time and travel frequency. Since the survey will likely not properly capture the distribution of trip frequency and travel distance, and usage patterns will depend on these characteristics, this disaggregation should increase the accuracy of the analysis. As an approximation, riders who wish to use the service are assumed to use the Internet on each of their trips. The total number of uses in each entry in the travel time x travel frequency matrix is the number of users multiplied by the median number of trips in each frequency bin. The specific frequency distribution of existing riders was not available from the CCJPA, so the data can only be analyzed with respect to these frequency bins. Through this multiplication and a summing of each cell in the matrix, the total number of annual uses can be determined.

Similar surveys have been conducted on other systems to determine rider interest in wireless Internet. While the rider makeup varies, especially between Europe and the United States, these results should at least provide some expectations for the Capital Corridor survey. A BWCS survey [i], completed with the help of 1600 UK rail passengers, indicated that 78% of business travelers would want to use Wi-Fi on the train. Another survey indicated that only 18% of air travelers would be willing to spend more than $10 on wireless internet.

The on-board wireless survey also asked the maximum amount that the respondent would be willing to pay per hour, per trip, or per month. The mean of these responses should give an indication as to a fair and efficient price. If anything, the mean price from the survey will be lower than the actual efficient price since people will know they are affecting the future price with their responses. To determine the applicability of the survey results, the survey results should be compared with both existing wireless Internet network rates and existing on-board mobile wireless internet rates. The network rates should be equal to or below the rates charged on-board since the technology required for fixed wireless services is substantially less expensive. Currently, most for-fee on-board wireless services are offered in Europe, which in general has significantly higher wireless fees. Therefore the fees charged for the services in these cases, notably GNER and Linx trains, will be higher than what the market will bear in the United States. To provide a range of revenue potential depending on the price structure chosen, the mean and each of the quartiles of the price distribution should be analyzed.

[i] BWCS ltd. (2003) Railway WI-Lan services, *report*.

Revenue Projection Methods

Method 1

Two different methods of projecting revenue are utilized. Question #10 of the wireless on-board survey asks users whether they would prefer a per-month, per-trip or per-hour fee. The responses to this question are only relevant for those who expressed interest in the service in question #7. Optimally, the analysis would provide the answers to these questions based on each respondent's origin and destination (and therefore trip time). To create a much less time consuming, and as a result a slightly rougher projection, it is assumed that the preference of payment plan is independent of trip time. To maintain the study's applicability, the percentage preferring each type of plan needs to be broken down by trip frequency. The payment plan preference will almost certainly depend on the number of trips per month the rider takes. A daily commuter will not want to purchase service every trip on every day, but he/she will know that a monthly subscription will be cheaper and more convenient.

Those on trips lasting 2 hours or more are assumed to purchase two hours of service, all other riders are assumed to purchase 1 hour of service. For example, if X% of those taking under 20 trips per year prefer the hourly plan, then X% of those riders with a trip time of under 120 minutes will purchase one hour of an hourly plan and X% of those riders with a trip time of over 120 minutes will purchase two hours on the hourly plan. The total revenue for each plan [percentage of respondents preferring that plan x the number of trips per year (or riders for the monthly plan) x plan fee] is summed to forecast the total annual expected revenue.

Method 2

An inherent error in the above analysis is that people do not know the rates they will be charged for each of the plans before answering the survey question. They are assumed to minimize cost and will therefore choose the plan with the lowest cost, which they do not know at the time the survey is issued. Therefore, the responses to the survey may not provide an indication to the actual distribution of payment plans chosen. It may be more accurate to make the revenue forecast while minimizing cost for the user based on the results of the survey’s fee question. Those who ride the train more frequently will prefer a monthly plan, while those who will use the service only occasionally will pay per use. Since only 10% of weekday riders ride the train for more than two hours, and not all will purchase usage for multiple hours, it is assumed that the per trip and per hour rate preferences will be similar. Detailed ridership frequency data was not made available, but users were separated by large frequency ranges (<20, 20-100, 101-150, 151-300, >300). On existing wireless systems the monthly rate is approximately 8 times the hourly rate. This is for non-mobile systems, but it is expected that as technology improves, mobile wireless pricing will eventually approach or become uniform with non-mobile rates. Therefore it is assumed that users who will ride the train more than 8 times per month (96 per year) will choose the monthly payment plan. Therefore the users who take 101 or more trips per year are assumed to purchase the monthly plan. Those who ride the train less than 101 times per year are expected to pay per use. The responses to question #7 (would you pay for service) can be broken down by time and frequency, as mentioned above. Thus the total revenue is the percentage of respondents in each consumer segment (grouped by frequency and travel time) that are interested in wireless internet x the number of riders (or trips) in each category x the price of the plan.

This provides a forecast of revenue approximately only for weekday usage. Weekend usage is only captured in the above process through weekend trips taken by those who were surveyed during the week. Weekend-only riders will not have their usage captured by this analysis. A survey conducted on the weekend would capture this data. While there aren’t plans to conduct the survey on the weekend at this time, if a need arises in the future the analysis will be similar to the one outlined above.

Sample Projection

To provide a general benchmark for expected revenue, survey results were projected. If, independent of trip time and frequency, 10% of all riders are interested in wireless Internet, and the existing network providers service rates are implemented revenue generated by use of the service will be between $63,000 and $125,000. It is expected that the market will bear greater fees than those charged on competitive non-mobile networks and that rider demand will vary based on travel time and trip frequency.

Other Revenue Sources

Additional revenue sources are possible. Even without wireless internet, train ridership is increasing by approximately a rider a day. Of course as the number of riders increase, the number of users and therefore revenue increase. The service will hopefully directly lead to an increase in train ridership, especially for longer trips. Thus the new riders will lead to additional revenue, especially since the new riders generated by the service will have a usage rate of nearly 100%. Additional advertising possibilities may present themselves as well.

Conclusion

This paper presents a method for which the potential revenue generated by an on-board wireless internet service may be estimated. Since survey data on passenger demand and acceptable service fees is not available at this time, this appendix only outlines the process and does not produce an actual revenue projection. With this analysis, it is possible to input the survey results and quickly obtain a rough revenue estimate. A more precise estimate can be obtained through further disaggregation of the data by rider frequency and trip length, as well as other rider characteristics not included. These characteristics include trip purpose, laptop ownership, and familiarity with wireless technology. Service attributes will also affect revenue potential, including bandwidth, technical support, and reliability. Revenue potential will likely increase in the future as wireless technology improves and further infiltrates society. Thus while wireless service on-board may appear to be unprofitable in the near-term, the outlook could change as the result of numerous factors.

Appendix C

WI-Fi on Trains
A Cost-Revenue Analysis

Jean-Luc Ygnace

CCIT

U.C. Berkeley

July 2005

SUMMARY

The objective of this research is to give a business perspective according to technology and usage studies for the service trials. The output will be an overall business model for deploying Wi-Fi on trains. The volume of interest, “acceptable service price for end users (consumers, professionals, machines…)” will be compared to the timeframe and cost of such a system implementation, and “business” directions for service will be given to maximize value creation and customer valuation. The description of business models explains the cost structure and the revenue structure to expect according to the value chain. Since the value chain depends on the technological, regulatory, cultural and economical environments, comparing Californian, French and Japanese experiments could be useful to understand how the markets may experiment take-off and growth. The challenges to implement such services and technologies in other countries are based on the experience obtained in all locations and experiment sites.

STATEMENT OF THE WORK

After work places and homes, internet access is spreading now everywhere. The number of Internet access points (Hot Spots) has been steadily increasing over the last years in various locations as hotels, airports, rail stations, etc. There are today over 60 000 Hot Spots worldwide [[1]] of which one third are in the United States. Mobile internet becomes now the next challenge for many service providers. Ships, planes and trains are becoming connected to the outside world. For example major airlines like Lufthansa, Singapore airlines, All Nippon Airways to just cite a few of them are now providing Internet access to in bound passengers. The railroad sector is also catching up with this new effort to bring more productivity and entertainment possibilities to train travelers by offering new possibilities to connect to high speed internet while traveling. During the next five to 10 years, most rail system riders in North America and Europe are expected to have onboard wireless Internet access (Wi-Fi), according to some industry estimates [[2]]. Currently, there are many applications in these regions, mostly in the pilot stages. A few services are offered on a commercial basis in the U.K, - GNER (Great North East Railway), Virgin Trains from London to Birmingham, Manchester and Glasgow, and Southern Brighton Express, in Northern Europe countries and also between Paris and Brussels on the Thalys high speed trains. In India the service is also offered by Railtel on the Delhi-Amritsar and Delhi-Bhopal train routes [[3]]. Similar services are used by train riders in Canada and in the U.S. There is also a relatively new on-going research effort led by academic and industrial consortia. In Italy Alenia Spazio and Eutelsat are implementing a system along the Rome-Florence line with the support of the European commission funding within the FIFTH (Fast Internet for Fast Train Hosts) program. Europe is also supporting a consortium of European industry leaded by the Alcatel group within the MOWGLY R&D project (MObile Wideband GLobal Link sYstem). In the U.S, the California Center for Innovative Transportation at U.C Berkeley is also pursuing a similar goal with the “train connected project” [[4]] in partnership with the Railroad operator Capital Corridor from the San Francisco Bay Area. Nevertheless, the business side of these activities is still at infancy stage because the level of willingness to pay for the services is still unknown and the current business models for internet access at home or at work are not directly applicable to mobile situations.

A NEED FOR COST/REVENUE EVALUATIONS

On one hand the traditional business models for Wi-Fi deployment are generally evaluating the willingness to pay for connectivity services and on the other hand to evaluate the potential role of all the players involved in the value chain like the billing, roaming, content providing, roaming, security, marketing and customer relationship managements. All these aspects are being priced together at $4 on average per hour of communication. In the case of trains we do not know yet the willingness to pay for the service. The cost of a ride varying enormously from one country to one another it is more difficult to evaluate a fixed cost of the service because we can suspect a statistical correlation between the price of the ticket and the willingness to pay for a connection fee during that ride. This aspect is less important in the case of long-haul air trips where prices per class are more similar among different airlines. The value of time during a train ride may also vary very much depending on the socio economic profile of the user. Finally, the rail transportation is usually subsidized by the public sector and the decision process to implement new technologies in a train is always determined by a complex association of public policies requirements as well as by private business modes of action.

A lot of variables are still uncertain to design a formal business model. Our approach would consider a financial framework of cost/revenues scenarios in order to give reasonable boundaries to the definition of viable business models to deploy internet connection and services into trains.

Case studies analysis in France, California and Japan

We have considered three very distinct railroad networks representing the 270 km San-Jose Sacramento California Capital Corridor, the 505 km Paris-Lyon French high speed TGV and the 515km Tokyo-Osaka high speed Shinkansen lines. The ridership is also very different for the three cases. The California operator is serving around 1.3 millions riders a year, the French figure is almost 7 millions per year and the Shinkansen line hits 108 millions passengers per year.

We developed models to evaluate the cost-revenues ratios for Wi-Fi services on these trains on a ten year cumulative basis.

On the cost side, we evaluate the deployment of two possible competing technologies for connecting the trains to the outside world: satellite and/or cellular links on one hand and dedicated infrastructure along tracks (WI-MAX type) on the other hand. The model is based on assumptions concerning the required equipment based on an evaluation of the bandwidth needed to satisfy the demand based on the potential number of connected passengers (5% per train during the first year) and the total number of trains circulating both ways at the same time on the entire network. We assume that each train is fully equipped except in the California case where we only equip two cars of each of the 7 trains. The cost of equipment of the train with Wi-Fi Hot Spots, wiring, immobilization cost and manpower is fixed and therefore is independent of the technology for communicating with the outside. The presence or absence of satellite antenna is the only difference. In the case of satellite we calculate the lease line cost (average market price of $65per kbps per year on a long term transponder lease), and $12 per kbps per year for 1xRTT cellular type of communication. All equipment costs assume a 15% fee per year for maintenance (5%) and for renewal over the ten year period (10%). In the case of the dedicated infrastructure technology along the rail side (WIMAX type), we assume a total cost for beacons and pole equipment and installation. The model allows a beacon every 1km in Japan, every 3 km in California and every 5 km in France.

The revenue model is based on the following assumptions and is similar for each geographic area:

1) At least 5% of train riders are willing to have internet access while traveling (This figure is consistent with published results in the U.K and in the U.S. An article in the Wi- Fi netnews [5] claimed that the Altamont Commuter Express in California had between 3% and 4% of passengers who connected to the in-board Wi-Fi network just after the launch of the service)
2) We take into account the national projections for the train ridership increase over the 10 years
3) the WI-FI market growth is evaluated at 2% per year. In the French case we assume a growth of 2% for coach class travelers and 3% for 1st class travelers
4) We assume that the Wi-Fi access can increase the train ridership by 0.2% per year. (50% of the ticket revenues are allocated to the Wi-Fi revenue model for these passengers)
5) We evaluate two pricing options: $3 and $5 per session (currency exchange rate change basis: 1.3 USD per euro and 100 yens per USD). We estimate that an average session lasts two hours. The $5 and $3 values correspond to an average estimate. It means that we do not take into account the different billing possibilities by trip or monthly. Whatever the discount for multi usage or the increase for one way usage is, the total revenue we estimate remains constant. Our model estimates a global envelope
6) We take into account various levels of bandwidth availability per user
7) The total bandwidth allocated is the result of the number of connected passengers per train, the total number and the usage behavior. We assume that the users will transmit data (uplink and downlink) during 30% of the session time (the average time of a session is evaluated at two hours) we also take into account two different mode of connection: 1) 75 % (high simultaneous usage) of the users connect at the same time, for example at the departure of the train, 2) 60 % (low simultaneous usage) will adopt this mode. This parameter simulates a theoretical peak hour demand for bandwidth. In all cases we estimate a Statistical Multiplexing Effect Rate of 20%.

Option 1: Two way communication satellite solutions

- The French TGV case

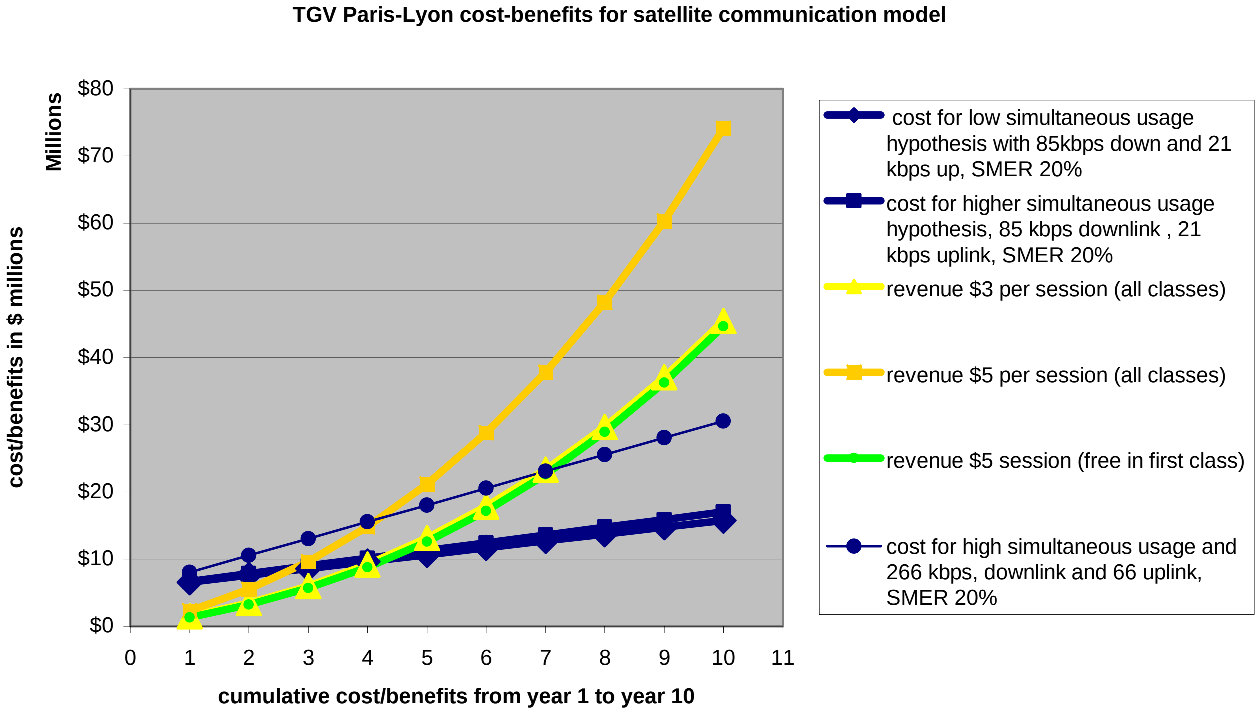


Figure 1: Cost-revenue model for the French TGV case

Depending on the assumptions for session pricing and the throughput offered per passenger, the breaking point goes from three years to seven years, Figure 1.

- Capital Corridor trains

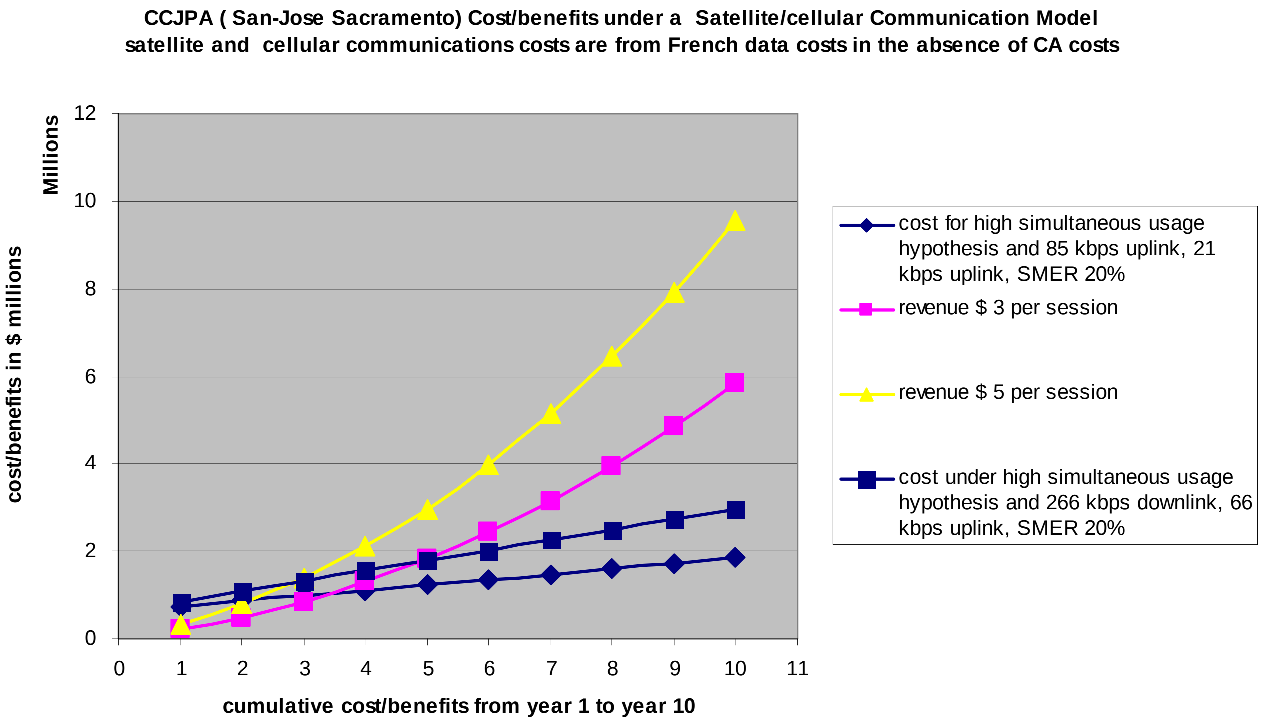


Figure 2:Cost-revenue Model for the California Capital Corridor Case

The breaking points are between two years and five years,
Figure **2**. Our simulation is equipping only two cars per train and the up link communication is using 1xRTT type of cellular communication. Due to the low number of passengers we do not think that a two way satellite communication would be appropriate. If several trains operators would like to provide a common service over the state of California, the issue could be re-assessed.

- The Japanese Shinkansen

In this case the satellite technology cannot be used alone because 20% of the network cannot be reached by satellite signal due to the presence of tunnels and high rise buildings. The cost assumptions include the development of wimax beacons along the portions of the tracks not reachable by satellite. The breaking points are between three years and five years,
Figure **3**. The EV-DO cellular solution seems financially unrealistic.

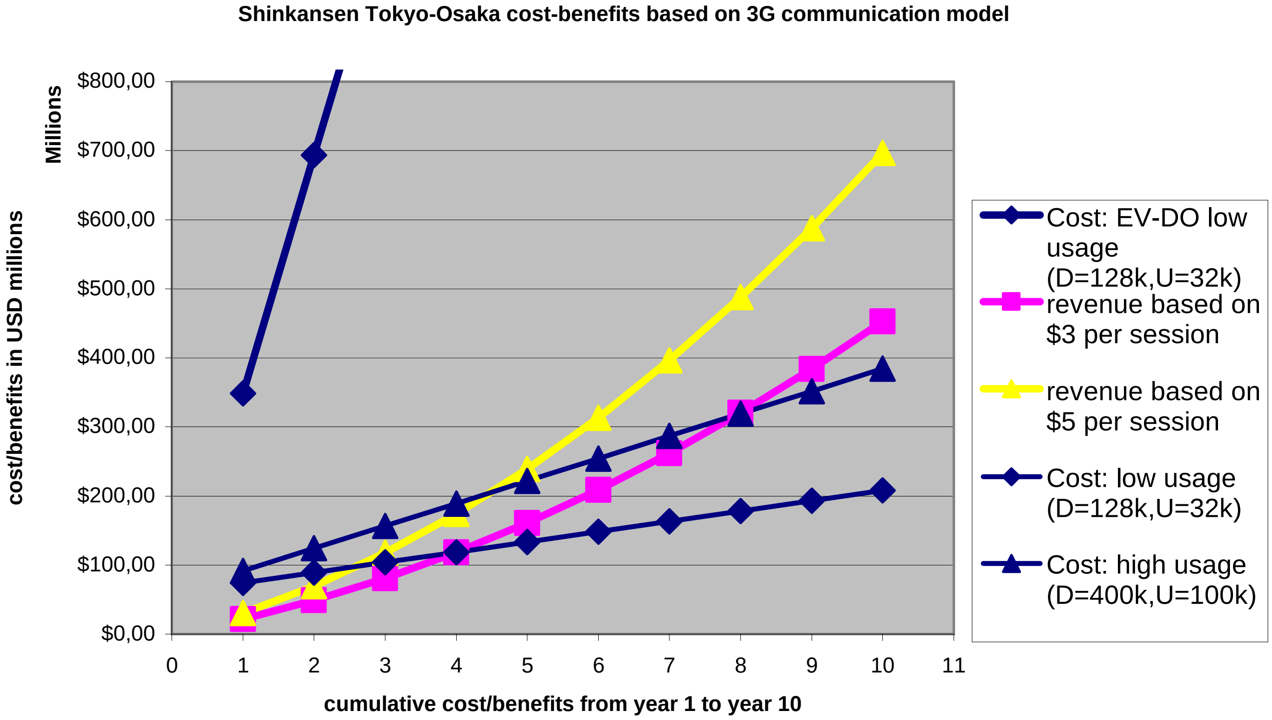


Figure 3:Cost-revenue Model for the Shinkansen Case

The models show a relatively constant period of time to reach the breaking points. The main differences are concerning the total cumulated benefits that could be provided over the ten year period. These benefits are a direct function of the ridership. The benefits can rise from $6 for the California train to $500 millions for the Shinkanen over ten years. This is to emphasis that any business operator willing to offer such services has to take into account the need to serve large markets, not to cover the costs but to reach meaningful benefits.

Option2: Dedicated communication technologies (WIMAX) along the tracks

This option would request the installation of WIMAX beacons mounted on poles along the tracks to maintain connectivity between the train and the outside world. The beacons have also to be connected to land line cables. The option is usually more expensive than the satellite option, although it provides much more available bandwidth per passenger. It also allows the implementation of various services for rail operators' management purposes. For example the beacons can also communicate and transfer data of video cameras disposed at strategic railroad crossings to offer real time information within the train and also at the train management center to increase the safety and security of the trains. The wimax option can also be partially deployed in cooperation with other satellite/cellular networks.

Following the charging model ($3 or $5 per session) the breaking points are between four and six years, Figure 4. For the same bandwidth it appears that the Wimax solution would be more profitable on the long term but necessitates a bigger investment in the short term.

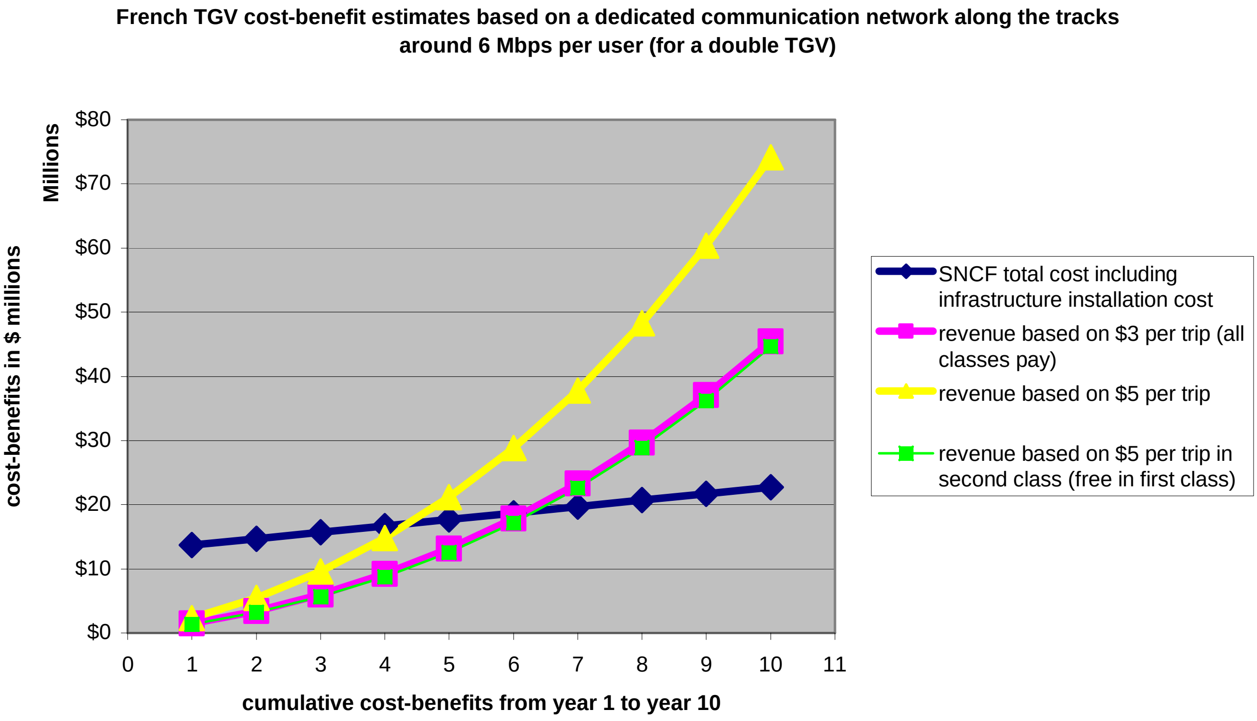


Figure 4 : Trackside Infrastructure Cost-revenue Model for the French TGV

- The Shinkansen case

The trackside infrastructure option remains by far the most competitive option in that case, Figure 5. The breaking points are between three and four years.

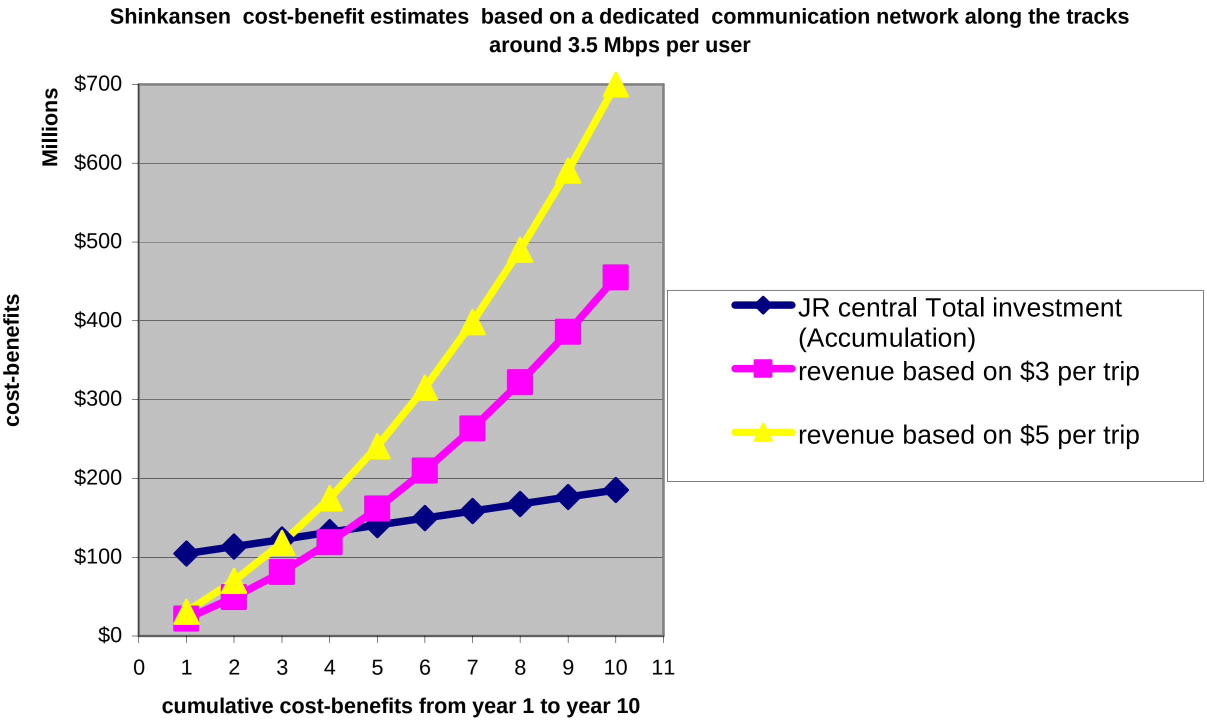


Figure 5 : Trackside Cost-revenue for the Shinkansen

- The Capital Corridor case

This option is very out of range in the absence of any cost sharing from a third partner, like Union Pacific or any other one, Figure 6.

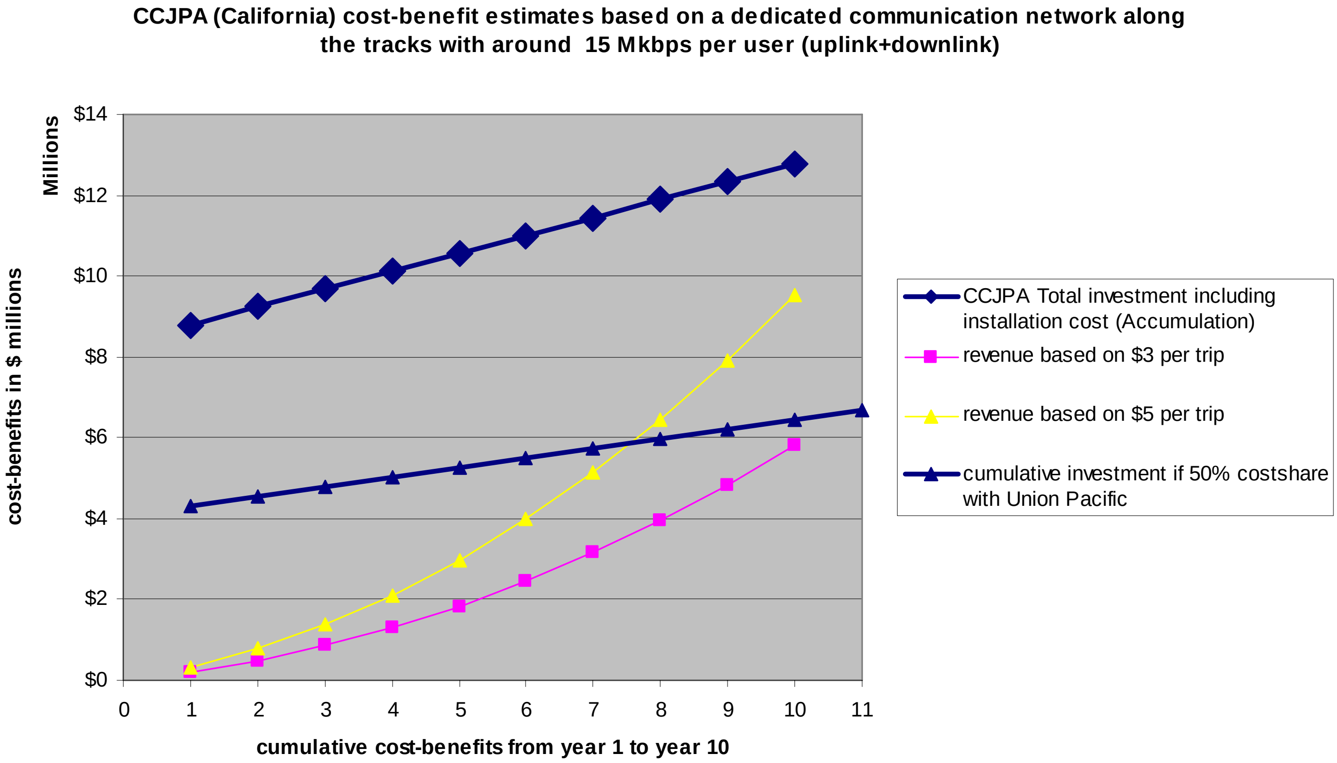


Figure 6: Trackside Cost-revenue Option for the Capital Corridor Case

CONCLUSIONS

The financial shell that we have defined for our revenue model represents $ 15 to $ 25 per hundred train riders. We assume a fixed price of $3 to $5 per session. This envelope remaining constant or at least no decreasing implies that any business model based on various charging methods i.e. by hour, by trip, or monthly passes have to equilibrate the final output. If we are charging per monthly subscription for frequent travelers let's say in the range from $30 per month, the price of single connections for other passengers will have to be increased to compensate. The business models and the value chain definitions will have to take this factor into account. The case studies that we have selected were necessary to show the viability of the solutions. From the survey, train rider are willing to pay $3.18 per trip, $2.6 per hour, $5.02 per day, or $26.35 per month depending on the payment method. The result of surveys will help us to define more accurate values for the willingness to pay and the needs for bandwidth from the passengers. We still do not know with precision the behavior of the train riders as they use internet in trains and how much bandwidth they need.

Another major aspect of the revenue model would have to evaluate the monetary benefits of the deployment of these technologies considering for example the value of time of the work being possible when riding a train. Also a potential increase in ridership due to the Wi-Fi attractiveness and consequently the impact of this modal shift on a lower usage of the road bring new needs for research. The economic evaluation of potential services for rail operator's management purposes is also needed.

The trial and surveys planned on the Capital Corridor trains in July 2005 will give us a better understanding of the viable scenarios for internet deployment.

Revenue projections for 100 riders (5% users on first year on average)	WI-FI trip cards Pricing solution Among by trip CCJPA tickets holders	WI-FI 10 ride-cards Pricing solution Among10-ride CCJPA tickets holders	WI-FI 20 ride-cards Pricing solution Among monthly CCJPA tickets holders
$25	5$ 5% of users	50 $ 5% of users	100$ 5% of users
$15	3$ 5% users	30 $ 5%users	60 $ 5$ users
$25	8$ 3.3% needed	40$ 4.4%	60$ 9.4%
$15	5$ 2.7% needed	25$ 5.2%	40$ 10.1%

Table 1 : Pricing Models on CCJPA Trains

Following our basic assumptions of a $5 or $3 charge per session to cover the deployment costs, the pricing solutions (per session, per 10 tickets or monthly), would have to be adequate with the revenue expectations, Table 1.

The survey will help us to validate the model and to know if the theoretical percentages that we have modeled are compatible with the answers given by the train riders.
Our models are also assuming a minimum bandwidth required by the users. A recent article [6] shows that the of data bits transferred by the 450000 users of the T-Mobile Hot Spots in the U.S. are 45kbits on average per second of connection over 1 millions sessions in one month. One of our models for CCJPA is evaluating the needs at 330 kbps per train. This is very consistent with the values observed at the T-mobile hot-spots, although we have here a lower limit. There is no reason to think that the expectations of train riders would be different from those of the Hot spots customers, e.g. at Starbucks or anywhere else. The analysis of user comments in the Capital Corridor guestbook [7], shows that a lot of them are not satisfied by the actual bandwidth they experiment on the trains, especially if they had to pay for such a service. More research is needed to evaluate the means to provide a better service at a reasonable cost:

SAM

2005-06-22

Ride date: 06-22-2005
Train number: 522

“It is nice to have wifi on the Capitol trains but I agree with the others that it is not worth paying extra for since service is spotty and extremely slow. I would rather see an across the board 40 or 50 cents train ticket price increase and then have the service offered free of charge for all users on all trains. Since I am not willing to pay to sign up for the service, posting my comments on this forum and looking through the Capitol Corridor website is about all I can do onboard now. Too bad. »

Terri

2005-06-21

Ride date: 6/21/05
Train number: 522

“I'm on line now and while I can do simple Google searches, the speed is not sufficient for me to use my company's remote access, nor even to check my personal email on line. According to my laptop, the speed is 11mbps - 1/5 the speed of dialup. Nice idea needs much more speed -the equivalent of DSL to be useful”.

Thomas

2005-06-21

Ride date: Daily
Train number: 545 & 547

“I have been commuting daily on the Capital Corridor for the last year and while the thought of Wi-Fi is fantastic on a train it needs to be implemented better. First...the $6.95 daily fee that Opti-Fi charges is way too steep for the relatively short time on the train or the quality. Using various download speed testers shows the performance varies wildly from slower than dial-up speeds to something less than broadband. It needs to be a more consistent speed to argue that the service is successful and thus worth charging money. Yes there is a $35 monthly option but without Wi-Fi available on all cars and trains it really is not worth it. I love the train and it's employees. But the way Wi-Fi is being implemented? It could be done a lot better”.

High speed seamless internet connections are possible through the installation of Wi-Max stations along the rail track as stated in our model. The cost of this solution is not realistic for a rail company carrying 4000 riders per day along a 170 miles corridor. The implementation of such beacons would have to cover other usages like urban Wi-Max coverage for residents who live in a two or three miles radius from the tracks. T-Mobile and the Southern commuters

express line are the only example to experiment today a similar solution between London and Brighton in the United Kingdom. The service will be commercially available in July 2005 and is tested on several trains everyday, see trial schedule on the daily basis, Table 2.
High speed internet for trains is a real challenge. Business models and technology solutions have to be improved.

Trains with Wi-fi access today

DATE: 27.06.05

Brighton	*Croydon*	*Victoria*	*Victoria*	*Croydon*	*Brighton*
07:16	08:04	08:23	08:36	08:52	09:28
07:33	08:24	LB	10:06	10:22	10:58
09:49	10:25	10:41	11:06	11:22	11:58
11:19	11:55	12:11	12:36	12:52	13:28
12:19	12:55	13:11	13:36	13:52	14:28
13:49	14:25	14:41	15:06	15:22	15:58
14:49	15:25	15:41	16:06	16:22	16:58
16:19	16:55	17:11	18:07	18:24	19:13
17:19	17:55	18:11	19:06	19:24	20:02

Table 2 : Daily WI-Max trial conducted on British Trains

The Capital corridor case remains under uncertainty as long as more global solutions are not assessed. If the main communication link is supported by satellite communication, it is important to organize a state consortium with all train operators able to lease one or two dedicated satellite transponders of 33Mbps each in order to cover the entire California fleet at the same time with decent bandwidth. This is a solution to obtain a reasonably priced solution.

On the other hand, the infrastructure solution can be viable on certain rail links if it is bundled with rail safety/security issues and also with residential (or business) areas coverage for internet access or VOIP businesses. This is the cornerstone to bring service providers in that business.

Of course, all intermediates solutions can be viable. We do not think we can rely on Pointshot/Parsons business plan only.

REFERENCES

[1] Dankberg A. (2005). Existing Wi-Fi systems and networks, *draft report*, Institute of Transportation Studies, California Center for Innovative Transportation, Berkeley.

[2] BWCS Ltd. (2003) Railway WI-Lan services, *report*.
[3] http://newswww.bbc.net.uk/1/hi/business/3835525.stm

[4] Verma, H, Ygnace, J.L., Benouar, H, (2004). "Trains Connected Project", *ITS World Congress at Nagoya Japan*.

[5] http://wifinetnews.com/archives/2004_07.html

[6] http://www.informationweek.smallbizpipeline.com/infrastructure/164302525

[7] http://www.amtrakcapitols.com/aboard_the_train/wi-fi_guestbook.php

Appendix D

Wireless Internet (Wi-Fi) Survey

Date_______________ Time_________________

Train Information:

Name: Capitol Corridor Train Number:___________

Passenger Information:

At what station did you board the train:________________

At what station will you leave the train:_____________

Normal travel time between these two stations:___________

Home Zip code:_______________

Work Zip code:_______________

---

1. What is the purpose of today's trip? ____Business ____Other

2. How often do you travel on Capitol Corridor Trains per year?.

3. Do you ever make similar trips by car? Yes / No

4. Do you ever have occasion to ride the following trains:

San Joaquin: (In the San Joaquin Valley from Bakersfield to Sacramento and into the Bay Area, terminating in Oakland). Yes / No

Pacific Surfliner: (Southern California from San Diego to Los Angeles, Santa Barbara and San Luis Obispo). Yes / No

5. Do you usually carry a portable computer when you travel by train? Yes / No

If Yes, is it Wi-Fi equipped? Yes / No

6. Do you carry any other Wi-Fi equipped electronic device when you travel by train? Yes / No

7. If it were possible to connect to the internet aboard the train would you use the service?

____Yes, but only if it was free

____Yes, and I would be willing to pay something for the service

____No

(PLEASE COMPLETE OTHER SIDE)

.

.

8. If you were to use the service, what would you use it for (Check all that apply)?

___ Connect to office

___ Download/upload files

___ Email

___ Internet surfing

___ Other (Please list):____

9. How much time would you expect to spend connected to the internet per trip if cost was not a factor,?

_____Hours _____Minutes

10. If there is a fee for high-speed wireless internet service, how would you prefer to be charged:

___ Total time connected, billed monthly

___ Flat fee per trip

___ Flat fee per day

___ Flat fee for month

11. Given that if people responding to this survey indicate their unwillingness to pay or would pay very little, the service may not be provided, what is the maximum amount you would be willing to pay for high speed internet service: **(Please answer for all four payment plans)**

Hourly (cumulative time billed monthly): $0 $1 $2 $3 $4 $5 $6 $7 $8

Per trip: $0 $2 $3 $4 $5 $6 $7 $8 $9 $10

Per day: $0 $4 $5 $6 $7 $8 $9 $10 $11 $12

Monthly: $0 $10 $15 $20 $25 $30 $35 $40

12. How would the availability of internet service affect the trips you make by train?

___ Increase the number of trips I would make

___ Change the timing of my trips

___ Other _____________________________

___ No effect

13. Some trains in the Capitol Corridor have already been equipped with Wi-Fi. Have you ever used this service? Yes / No

14. Do you currently have internet service at home? Yes / No

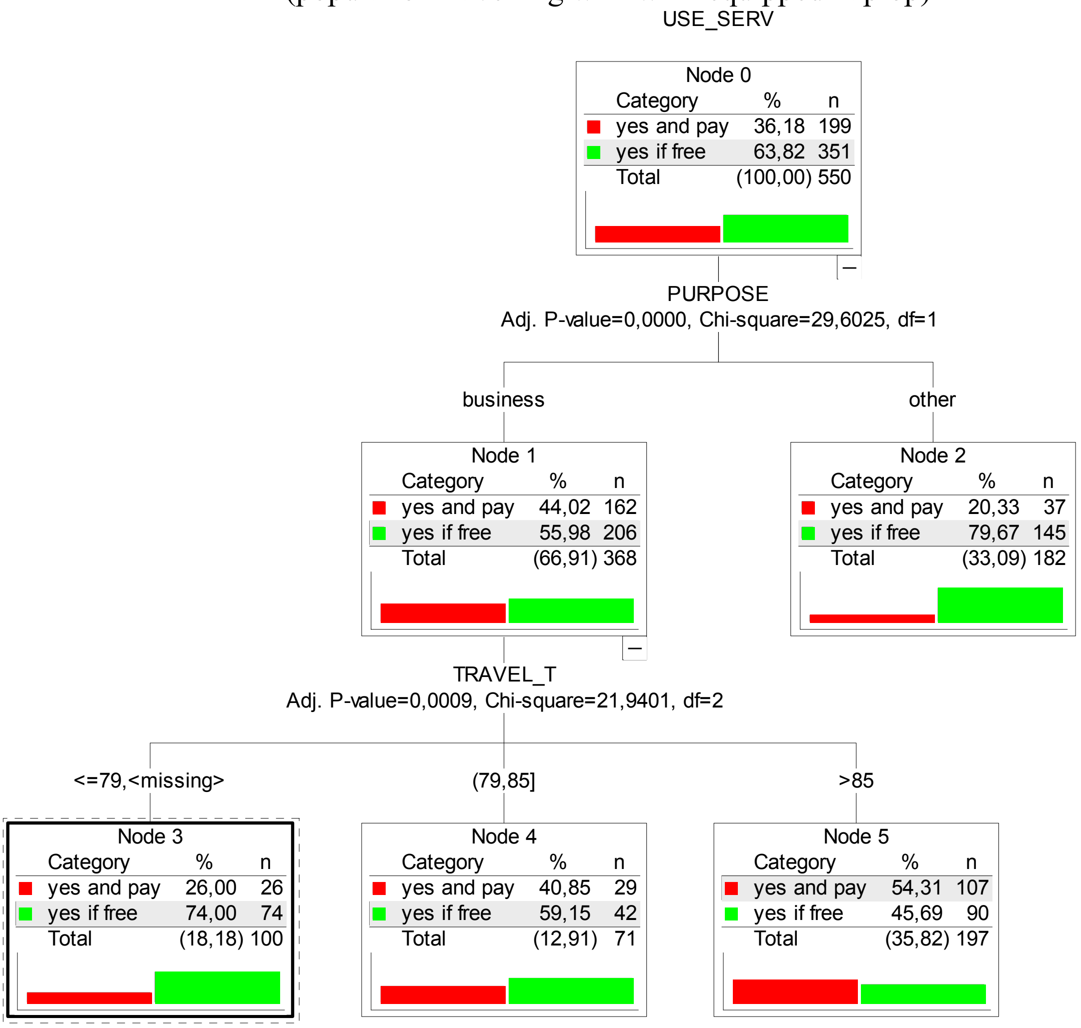
If Yes, what type is it? ____Dial-up ____DSL ____Cable

Who is your service provider? ____________________________

Appendix E

Analysis on the WiFi Survey Data

Best explaining variables for the willingness to use the service
(population travelling with wi-fi equipped laptop)


USE_SERV
PURPOSE
Adj. P-value=0,0000, Chi-square=29,6025, df=1
business
other
TRAVEL_T
Adj. P-value=0,0009, Chi-square=21,9401, df=2
<=79,<missing>
(79,85]
>85

Node 0

	Category	%	n
🟥	yes and pay	36,18	199
🟩	yes if free	63,82	351
	Total	(100,00)	550

Node 1

	Category	%	n
🟥	yes and pay	44,02	162
🟩	yes if free	55,98	206
	Total	(66,91)	368

Node 2

	Category	%	n
🟥	yes and pay	20,33	37
🟩	yes if free	79,67	145
	Total	(33,09)	182

Node 3

	Category	%	n
🟥	yes and pay	26,00	26
🟩	yes if free	74,00	74
	Total	(18,18)	100

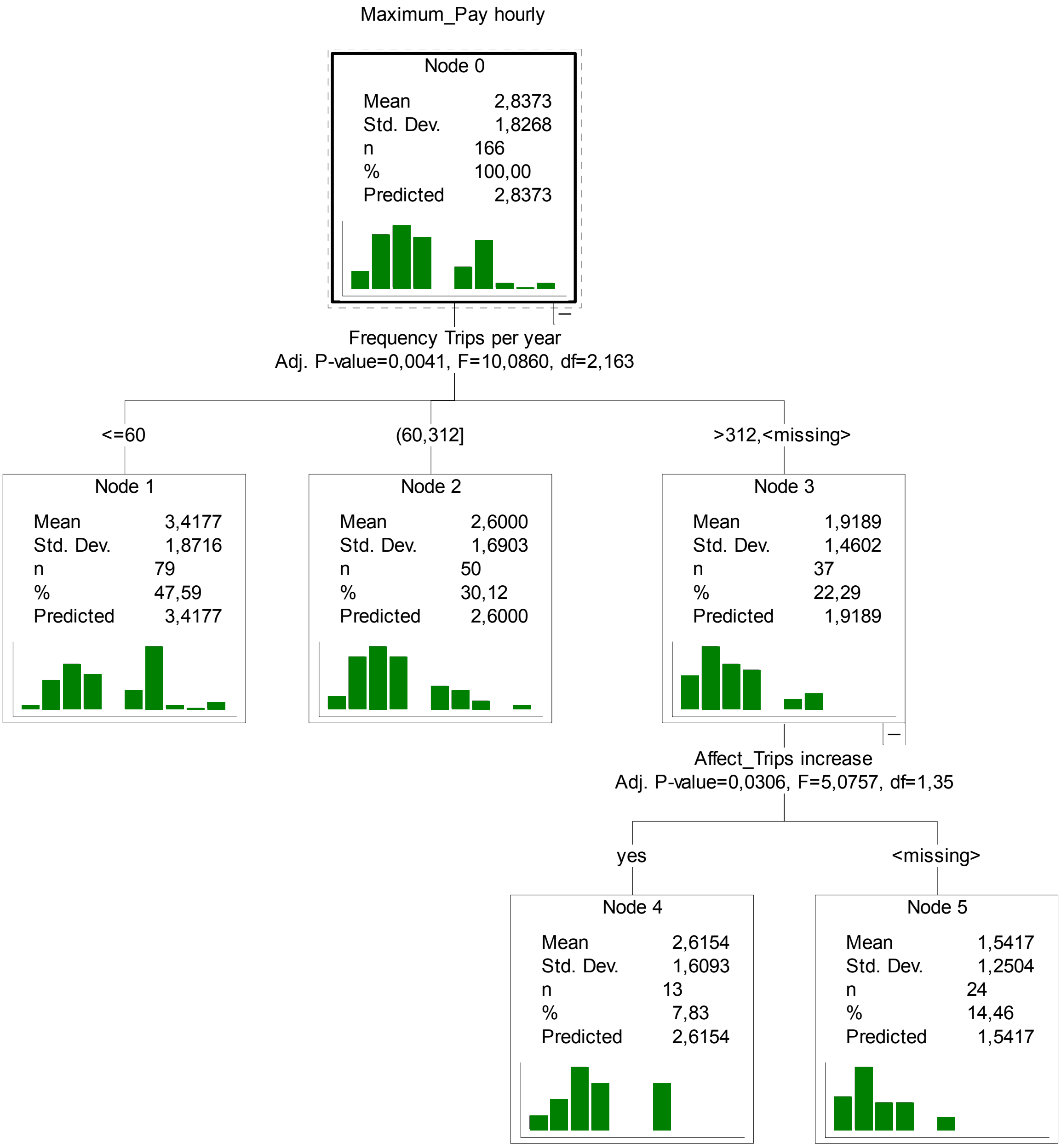
Node 4

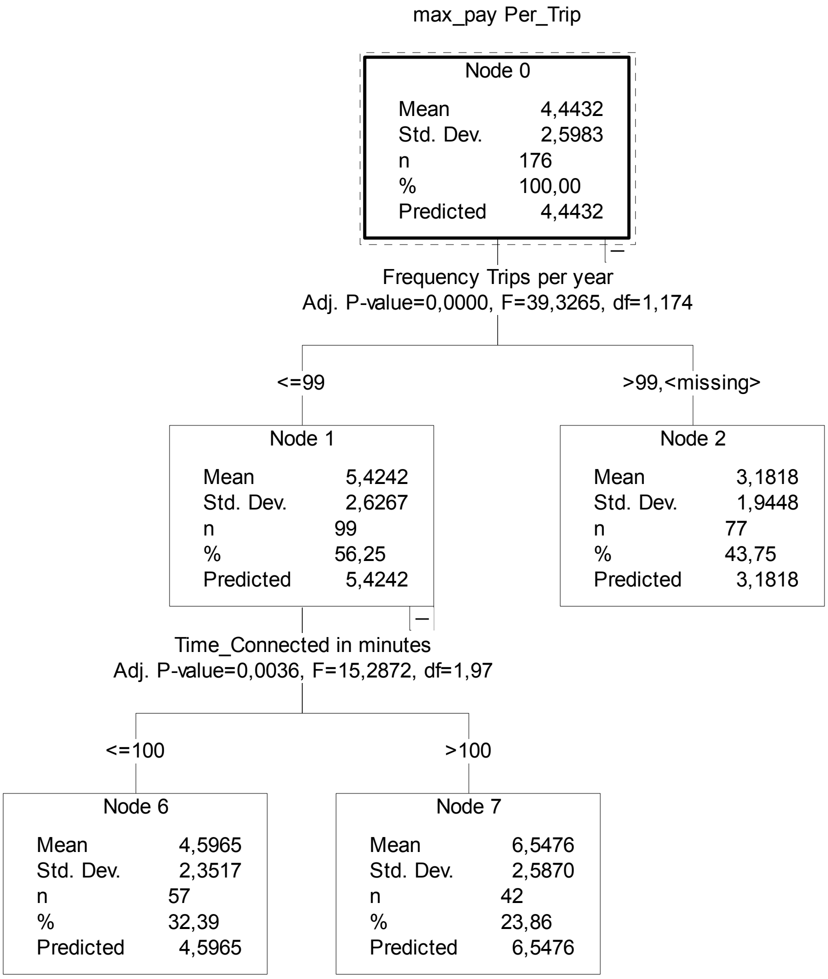
	Category	%	n
🟥	yes and pay	40,85	29
🟩	yes if free	59,15	42
	Total	(12,91)	71

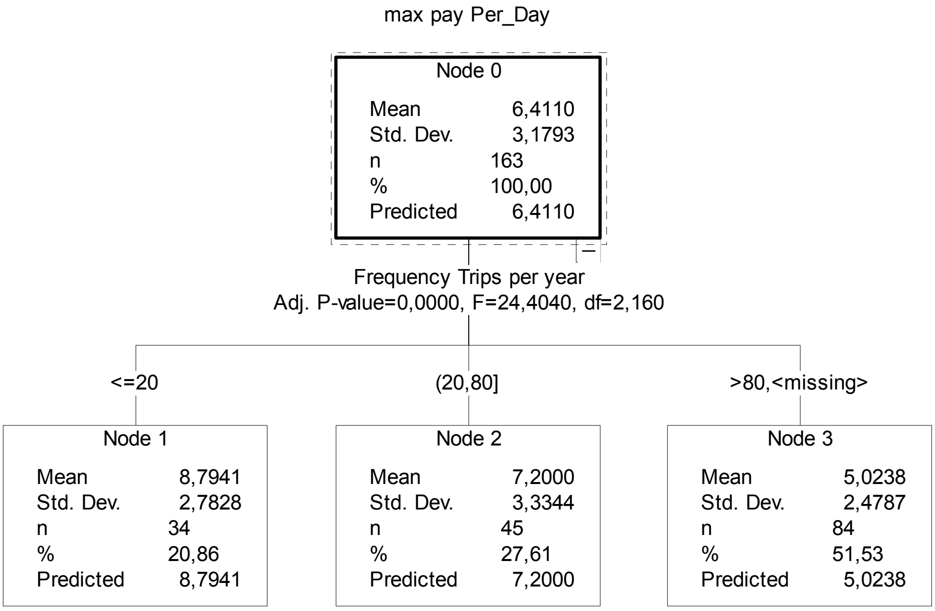
Node 5

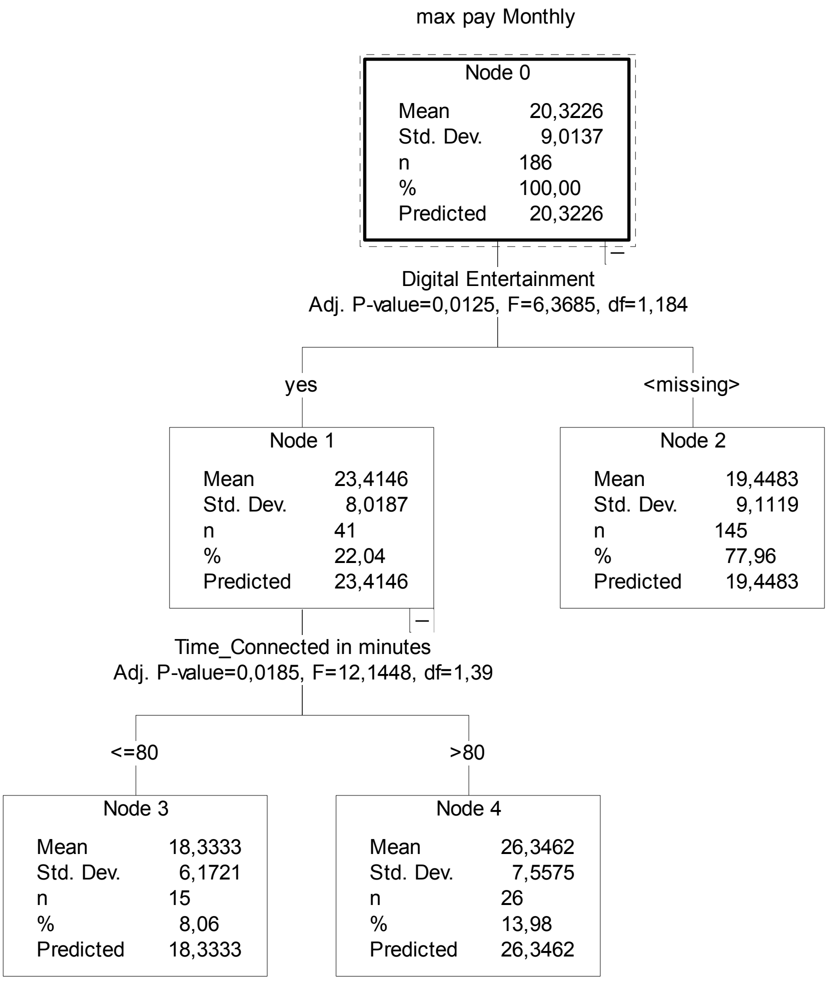
	Category	%	n
🟥	yes and pay	54,31	107
🟩	yes if free	45,69	90
	Total	(35,82)	197

Best explaining variables of the willingness to pay in dollars (by mode of payment)
(population travelling with a wi-fi equipped laptop and willing to pay to use the service)




max_pay Per_Trip
Node 0
Mean 4,4432
Std. Dev. 2,5983
n 176
% 100,00
Predicted 4,4432
Frequency Trips per year
Adj. P-value=0,0000, F=39,3265, df=1,174
<=99
>99,<missing>
Node 1
Mean 5,4242
Std. Dev. 2,6267
n 99
% 56,25
Predicted 5,4242
Node 2
Mean 3,1818
Std. Dev. 1,9448
n 77
% 43,75
Predicted 3,1818
Time_Connected in minutes
Adj. P-value=0,0036, F=15,2872, df=1,97
<=100
>100
Node 6
Mean 4,5965
Std. Dev. 2,3517
n 57
% 32,39
Predicted 4,5965
Node 7
Mean 6,5476
Std. Dev. 2,5870
n 42
% 23,86
Predicted 6,5476


max pay Per_Day
Node 0
Mean 6,4110
Std. Dev. 3,1793
n 163
% 100,00
Predicted 6,4110
Frequency Trips per year
Adj. P-value=0,0000, F=24,4040, df=2,160
<=20
(20,80]
>80,<missing>
Node 1
Mean 8,7941
Std. Dev. 2,7828
n 34
% 20,86
Predicted 8,7941
Node 2
Mean 7,2000
Std. Dev. 3,3344
n 45
% 27,61
Predicted 7,2000
Node 3
Mean 5,0238
Std. Dev. 2,4787
n 84
% 51,53
Predicted 5,0238


max pay Monthly
Node 0
Mean 20,3226
Std. Dev. 9,0137
n 186
% 100,00
Predicted 20,3226
Digital Entertainment
Adj. P-value=0,0125, F=6,3685, df=1,184
yes
<missing>
Node 1
Mean 23,4146
Std. Dev. 8,0187
n 41
% 22,04
Predicted 23,4146
Node 2
Mean 19,4483
Std. Dev. 9,1119
n 145
% 77,96
Predicted 19,4483
Time_Connected in minutes
Adj. P-value=0,0185, F=12,1448, df=1,39
<=80
>80
Node 3
Mean 18,3333
Std. Dev. 6,1721
n 15
% 8,06
Predicted 18,3333
Node 4
Mean 26,3462
Std. Dev. 7,5575
n 26
% 13,98
Predicted 26,3462

Appendix F

Evaluation of the Willingness to Use and to Pay for internet Connection on-board CCJPA Trains Based on Survey Results

By

Jean-Luc Ygnace

INRETS/CCIT U.C. Berkeley

October 2005

The survey was conducted on trains of the three InterCity Rail service routes during the week of July 11th 2005. One thousand and one hundred questionnaires were distributed to the train riders and thousand ninety-two questionnaires were completed and constitute the frame of the analysis. The aim of the survey is to evaluate the willingness to use high speed Internet on trains as it relates to travel train travel behavior and other factors that may affect the use of the technology.

I Train usage and Internet connection needs

I.1 Ridership Factors

Fifty-three point three percent of the surveyed population is traveling for business purposes and the rest for other purposes which were not précised within the survey questionnaire, Figure 1.

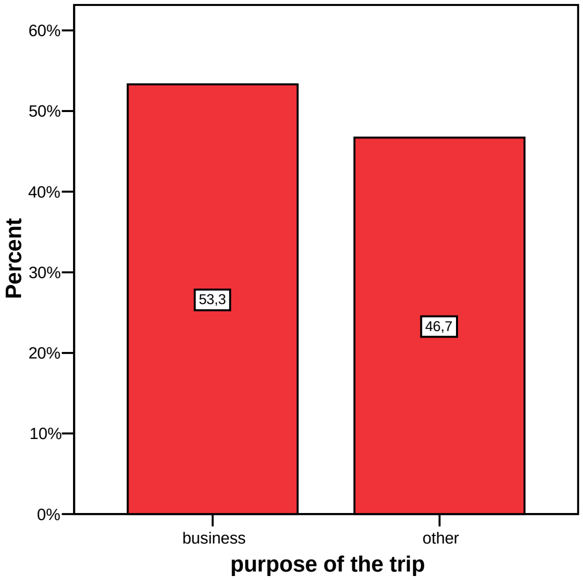
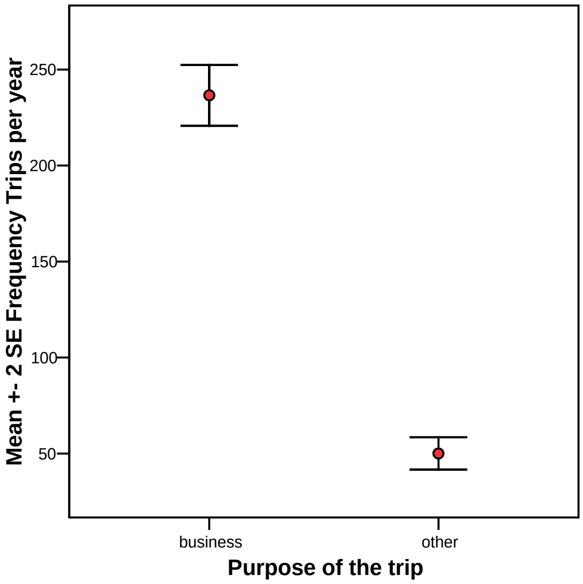


Figure 1: Purpose of the trip

The average travel time is 99 minutes (minimum 15minutes, maximum 256, standard deviation 37 minutes), the average number of trips per year is 150 (minimum 1, maximum 720, s.d 178). More precisely, 50 % of the population travels more than 94 times a year and 50 % of the population travels more than 50 minutes per trip. Trips related to business are on average more frequent: Figure 2, and shorter in time: Figure 3.



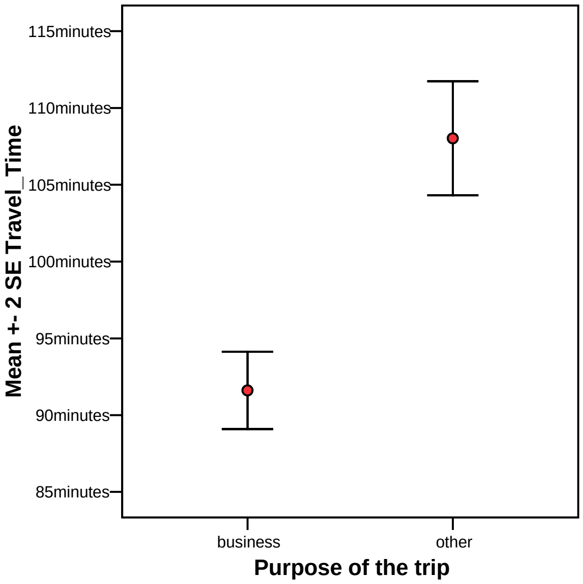


Figure 2: Average trip frequency by purpose **Figure 3: Average trip time by purpose**

In both cases, for business or for other purpose, travelers are also making the same trips by car in almost equal proportion, Figure 4.

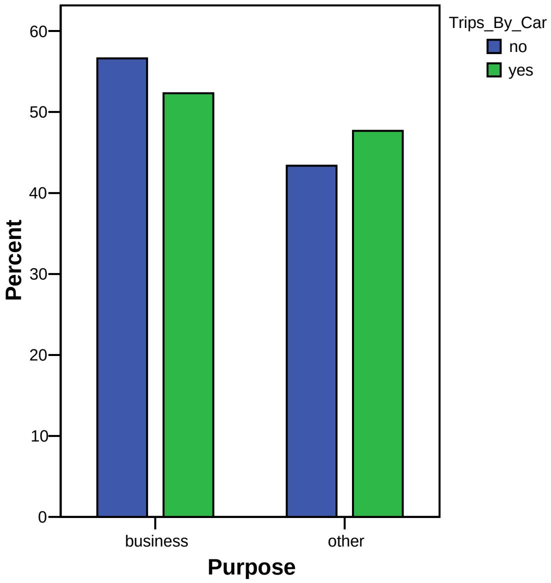


Figure 4: Distribution of trip by mode and purpose

I.2 Internet Access While Traveling

Within the scope of our work, the target population for any marketing effort to provide internet to train users is basically based on those carrying a device equipped with the communication wi-fi protocol.

Fifty-seven percent of the travelers surveyed declare they usually travel with a laptop computer, Figure 5, and 89.7% of those computers have a wi-fi communication protocol on their computer.

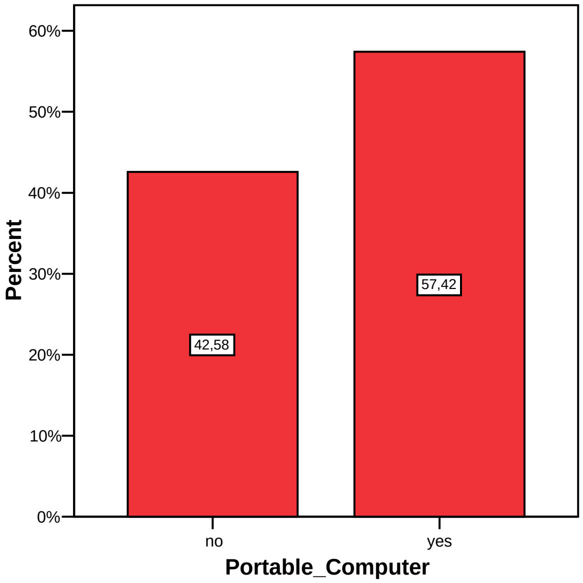


Figure5: computer availability during train ride

The proportion varies depending on the purpose of the trip: 67.1% of the travelers with a laptop are traveling for business, 65.4 of travelers without a laptop are traveling for other purposes than business, Figure 6.

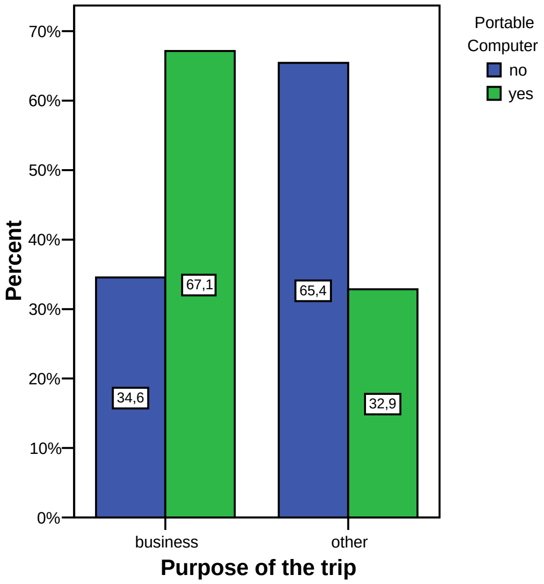


Figure 6: Computer availability and trip purpose

I.2.1 Willingness to Use the Service

The willingness to use the service is very high among the population. Without considering the availability of a laptop among the population, 65.2 % are willing to use the service if it is free and 26.2% would pay for it, Figure 7.

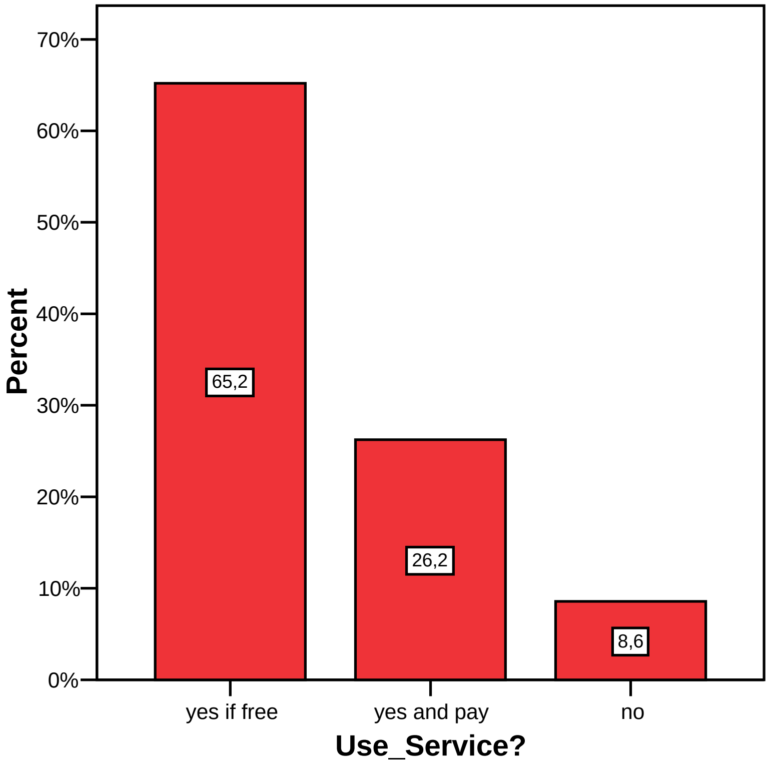


Figure 7: Willingness to use and to pay for the internet connection among the total population

The business travelers are showing a higher willingness to pay for the service, Figure 8.

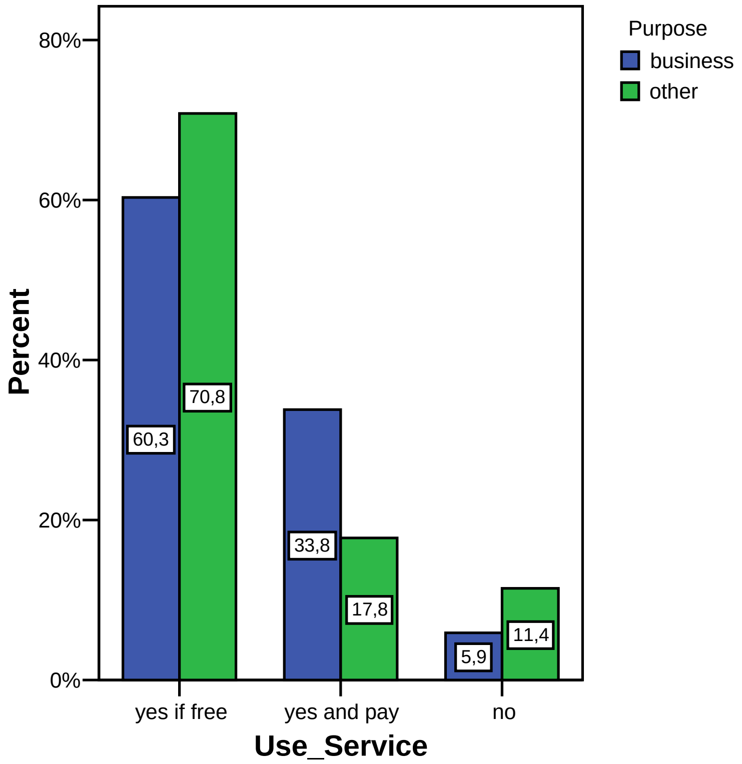


Figure 8: Willingness to use and to pay for the internet connection among depending on the purpose of the trip

When considering the target population only, i.e. those traveling with a wi-fi equipped computer or any other wi-fi equipped device, 391 travelers would use the internet if it was free **(35.8% of the total population)** and 215 riders would pay for the service **(19.7% of the total)**.

We can assume that more users would travel with a laptop if the service was available on a large scale. For the time being it is more reasonable to select the part of the population who is already traveling with a wi-fi equipped laptop to try to evaluate the potential market.

I.2.2 Internet Usage Among Wi-fi Equipped Riders

The riders are planning multiple usages of Internet while connected in the trains. 97 % are willing to use internet for e-mail purposes, 77% for internet surfing and 61% to connect to the office, Table 1. There are some differences among the users who are willing to pay and the users who would use internet if it was free. 70 % of the paying users would use internet to connect to the office, while only 55 % of the “free” users would connect to the office. This information is quite important as the bandwidth necessary to connect to the office (VPN) would have to be larger to satisfy the paying users. 54% of the paying users would also use the internet connections to download/upload files.

type of usage		yes if free	yes and pay	
connect to office	count of user in each pay type	217	150	total count of usage: 367
	pay type pct in this usage	59.1	40.9	usage pct of total population: 61
	usage pct given pay type	55.8	70.4	
	pay type pct in total population	36.0	24.9	
download/upload file	count of user in each pay type	173	115	total count of usage: 288
	pay type pct in this usage	60.1	39.9	usage pct in total population: 47.8
	usage pct given pay type	44.5	54	
	pay type pct in total population	28.7	19.1	
email	count of user in each pay type	375	209	total count of usage: 584
	pay type pct in this usage	64.2	35.8	usage pct in total population: 97
	usage pct given pay type	96.4	98.1	
	pay type pct in total population	62.3	34.7	
Internet surfing	count of user in each pay type	299	165	total count of usage: 464
	pay type pct in this usage	64.4	35.6	usage pct in total population: 77.1
	usage pct given pay type	76.9	77.5	
	pay type pct in total population	49.7	27.4	
Digital Entertainment	count of user in each pay type	121	47	total count of usage: 168
	pay type pct in this usage	72.0	28.0	usage pct in total population: 27.9
	usage pct given pay type	31.1	22.1	
	pay type pct in total population	20.1	7.8	
Other use	count of user in each pay type	38	13	total count of usage: 51
	pay type pct in this usage	74.5	25.5	usage pct in total population: 8.5
	usage pct given pay type	9.8	6.1	
	pay type pct in total population	6.3	2.2	
column total		389	213	total count: 602
Total		64.6	35.4	pct: 100

```
Percents and totals based on respondents

602 valid cases;14 missing cases
```

Table 1: type of internet usage by willingness to pay or to use the services for free

Fifty-two point three percent of the potential users declare that the availability of internet would not have any effect on the mobility while 36.1 % declare they would increase the number of trips by train. 46% of the riders who would pay for the service declare they would increase their number of trips by train, Table 2.

Service effect		Yes if free	Yes and pay	
Trip increase	count of user in each pay type	119	97	total count of effect: 216
	pay type pct in this effect	55.1	44.9	effect pct of total population: 36.1
	effect pct given pay type	30.7	46.0	
	pay type pct in total population	19.9	16.2	
Change_Timing	count of user in each pay type	27	28	total count of effect: 55
	pay type pct in this effect	49.1	50.9	effect pct of total population: 9.2
	effect pct given pay type	7.0	13.3	
	pay type pct in total population	4.5	4.7	
Other effect	count of user in each pay type	31	15	total count of effect: 46
	pay type pct in this effect	67.4	32.6	effect pct of total population: 7.7
	effect pct given pay type	8.0	7.1	
	pay type pct in total population	5.2	2.5	
No Effect	count of user in each pay type	231	82	total count of effect: 313
	pay type pct in this effect	73.8	26.2	effect pct of total population: 52.3
	effect pct given pay type	59.7	38.9	
	pay type pct in total population	38.6	13.7	
Column total		387	211	total count: 598
Total		64.7	35.3	pct: 100

```
Percents and totals based on respondents

598 valid cases;18 missing cases
```

Table 2: **How internet usage affects the trips by willingness to pay or to use the services for free**

II Monetary Aspects of the Service Usage for the Target Population

II.1 Mode of Payment

The purpose of the trip explains the differences among the repartition of the preferred mode of payments, by hour, by trip, by day or by month. Business travelers do not particularly favor any mode of payment, as potential users traveling for other purposes indicated they would mostly pay by trip, Figure 9.

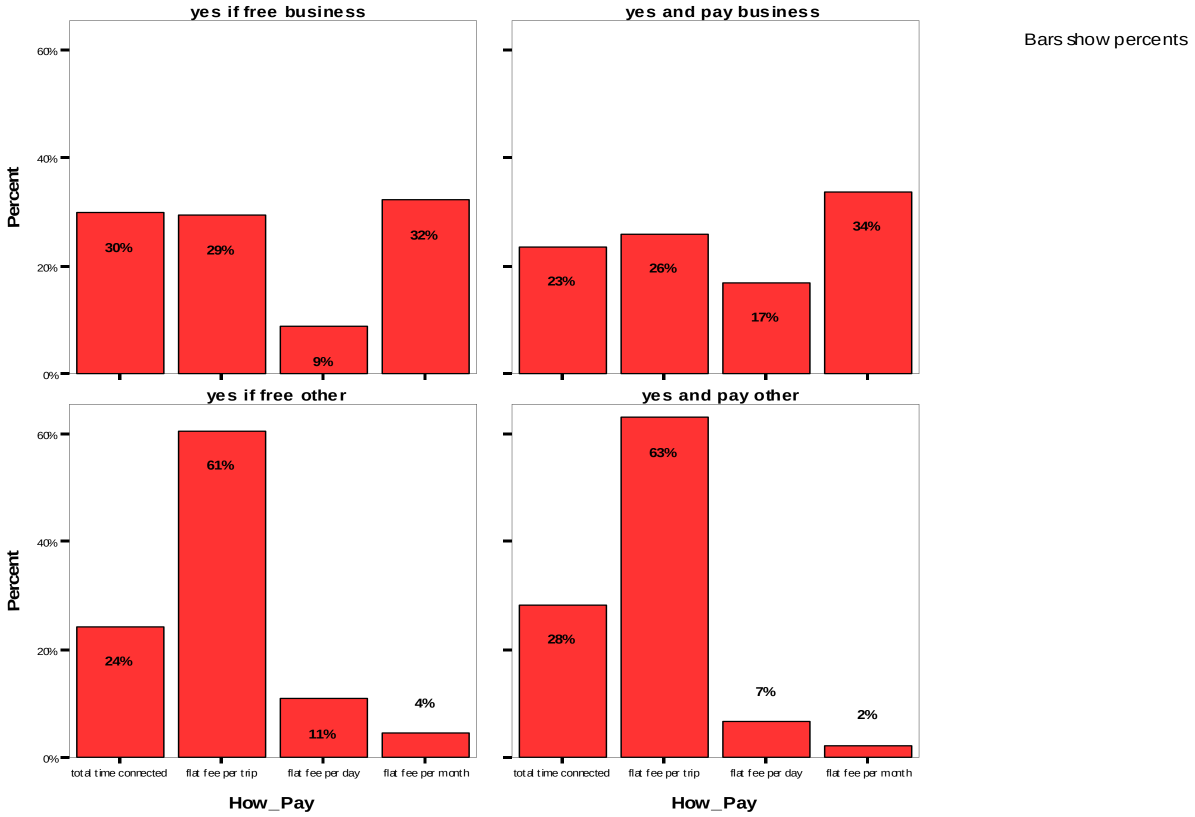


Figure 9: Preferred mode of payment depending on trip purpose and willingness to use the service

The rating of the mode of payment is quite independent of the stated preference to use the service for free or to pay for it.

II.2 Willingness to Use and Previous Usage of Wi-fii on Board CCJPA

Previous users of the wi-fi service on board CCJPA trains show a significant higher interest to pay for the service in the future, Table 3. (Pearson chi square: 8.962, df: 2, sig: .01)

Use_Service * Used WiFi Crosstabulation

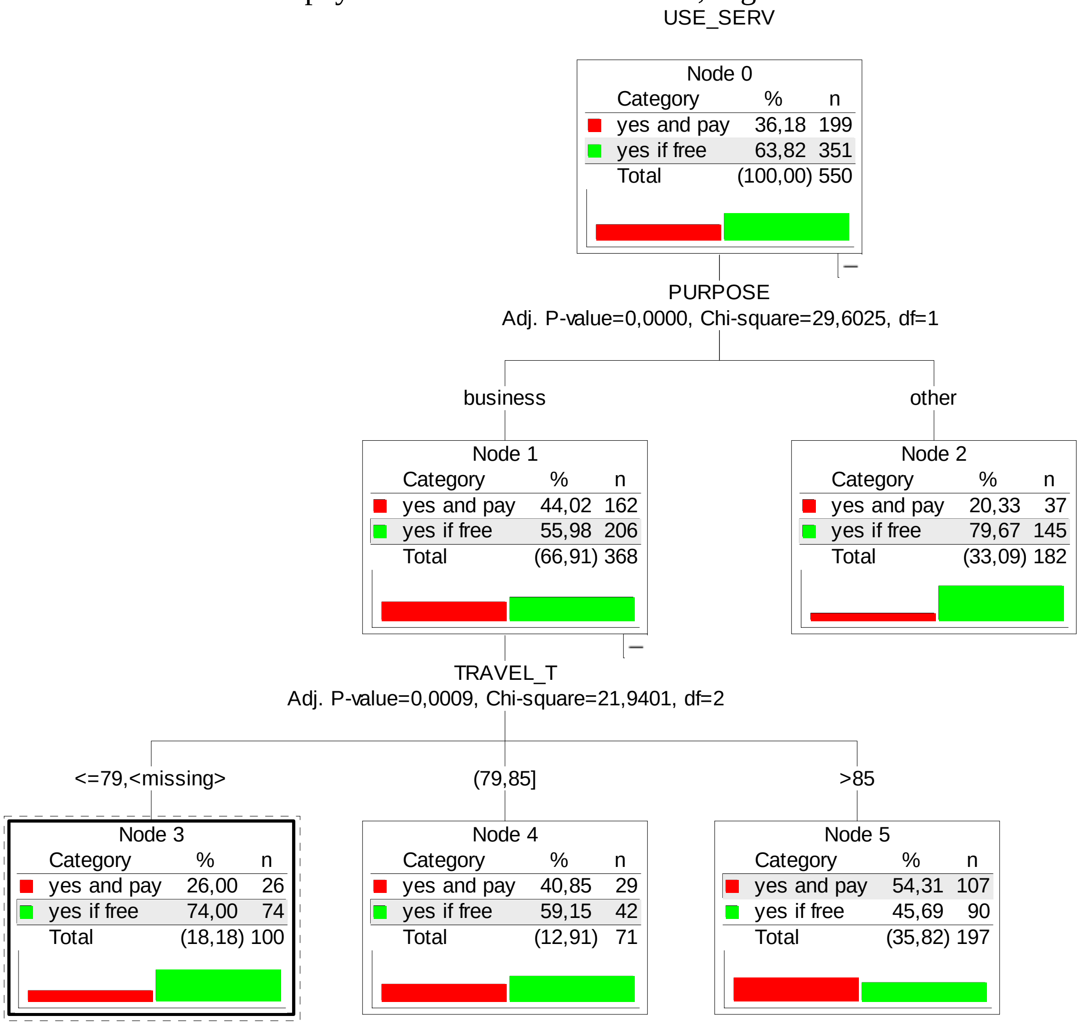
			Used WiFi		Total
			no	yes	
Use_Service	yes if free	Count	267	116	383
		% within Use_Service	69,7%	30,3%	100,0%
		% within Used WiFi	**67,8%**	**56,6%**	**63,9%**
		% of Total	44,6%	19,4%	63,9%
	yes and pay	Count	122	88	210
		% within Use_Service	58,1%	41,9%	100,0%
		% within Used WiFi	**31,0%**	**42,9%**	**35,1%**
		% of Total	20,4%	14,7%	35,1%
	no	Count	5	1	6
		% within Use_Service	83,3%	16,7%	100,0%
		% within Used WiFi	1,3%	,5%	1,0%
		% of Total	,8%	,2%	1,0%
Total		Count	394	205	599
		% within Use_Service	65,8%	34,2%	100,0%
		% within Used WiFi	100,0%	100,0%	100,0%
		% of Total	65,8%	34,2%	100,0%

Table 3: Previous usage of wi-fi on CCJPA and willingness to use for free or to pay

Thirty-five point one percent of the target population (traveling with a wi-fi equipped laptop) would pay for the service. They are 42.9% among the ones who already used the service and 31% among the ones who never used it before.

II.3 Explaining Variables

The use of the answertree^{tm} software statistical package allows to find key variables to identify group (willingness to use for free or to pay) membership. The method that we use is based on Chi-squared Automatic Interaction Detection to identify optimal splits. The tree shows that the business travelers are probably going to be willing to pay more often for the service than the other travelers. Among the business travelers, travel time is the best predictor to explain the willingness to pay. 26% of those traveling less than 79 minutes would pay for the service, 40% of those traveling between 79 minutes and 85 minutes would pay, and 54% of those traveling more than 85 minutes would pay for the internet connection, Figure 10


USE_SERV
PURPOSE
Adj. P-value=0,0000, Chi-square=29,6025, df=1
business
other
TRAVEL_T
Adj. P-value=0,0009, Chi-square=21,9401, df=2
<=79,<missing>
(79,85]
>85

Node 0

Category	%	n
🟥 yes and pay	36,18	199
🟩 yes if free	63,82	351
Total	(100,00)	550

Node 1

Category	%	n
🟥 yes and pay	44,02	162
🟩 yes if free	55,98	206
Total	(66,91)	368

Node 2

Category	%	n
🟥 yes and pay	20,33	37
🟩 yes if free	79,67	145
Total	(33,09)	182

Node 3

Category	%	n
🟥 yes and pay	26,00	26
🟩 yes if free	74,00	74
Total	(18,18)	100

Node 4

Category	%	n
🟥 yes and pay	40,85	29
🟩 yes if free	59,15	42
Total	(12,91)	71

Node 5

Category	%	n
🟥 yes and pay	54,31	107
🟩 yes if free	45,69	90
Total	(35,82)	197

Figure 10: Classification tree to explain the willingness to pay for the Internet service

II.4 Pricing Value of the Internet Service

One hundred ninety-six riders who are traveling with a wi-fi-equipped computer or any other wi-fi device are willing to pay for a service and are able to give a monetary value to their preferred mode of payment.

When summing the value of the total revenue from the 196 trips with internet connections, the result value is $4.5 per trip on average, i.e. $885.82 in total. The value per trip with a connection is inferred from the mode of payment. For example when the rider declares a preferred mode of payment per month, we calculate the dollar value of the trip of the survey based on the average number of trips per month

Two main subpopulations are considered to give upper and lower values of the willingness to pay: we make a difference between the riders who already experienced the internet connection on-board CCJPA trains (the given average value per trip connection is $ 5.3) and the ones who did not experience the service yet (the given average value is $3.5). Seventeen perecent of the total population can be divided into the two subgroups. The cost/revenue evaluation will be based on the assumptions that at least **17%** of he traveling population will be the initial customers of the service. The choice of mode of payment and the value of the internet connection within the mode is mainly explained by the travel conditions of the user, i.e. trip frequency, travel time, etc.

II.4.1 Payment by the Hour

The classification tree, Figure 11, shows that the dollar value of the service is higher when the number of trips per year s is shorter. The dollar value per hour of connection is $ 3.4 when the average number of trips per year is lower or equal to 60; the value is %2.6 when the trip frequency is between 60 and 312, and $ 1.9 for more than 312 trips per year. Among the ones traveling more than 312 times per year the perception of the effect of the internet connection is a also a good explaining factor. The ones who perceived then internet connection as a way factor to justify a rider ship increase arte willing to pay more than the ones who do no answer to this question. ($ 2.6 instead of $1.5 per trip hour of connection)

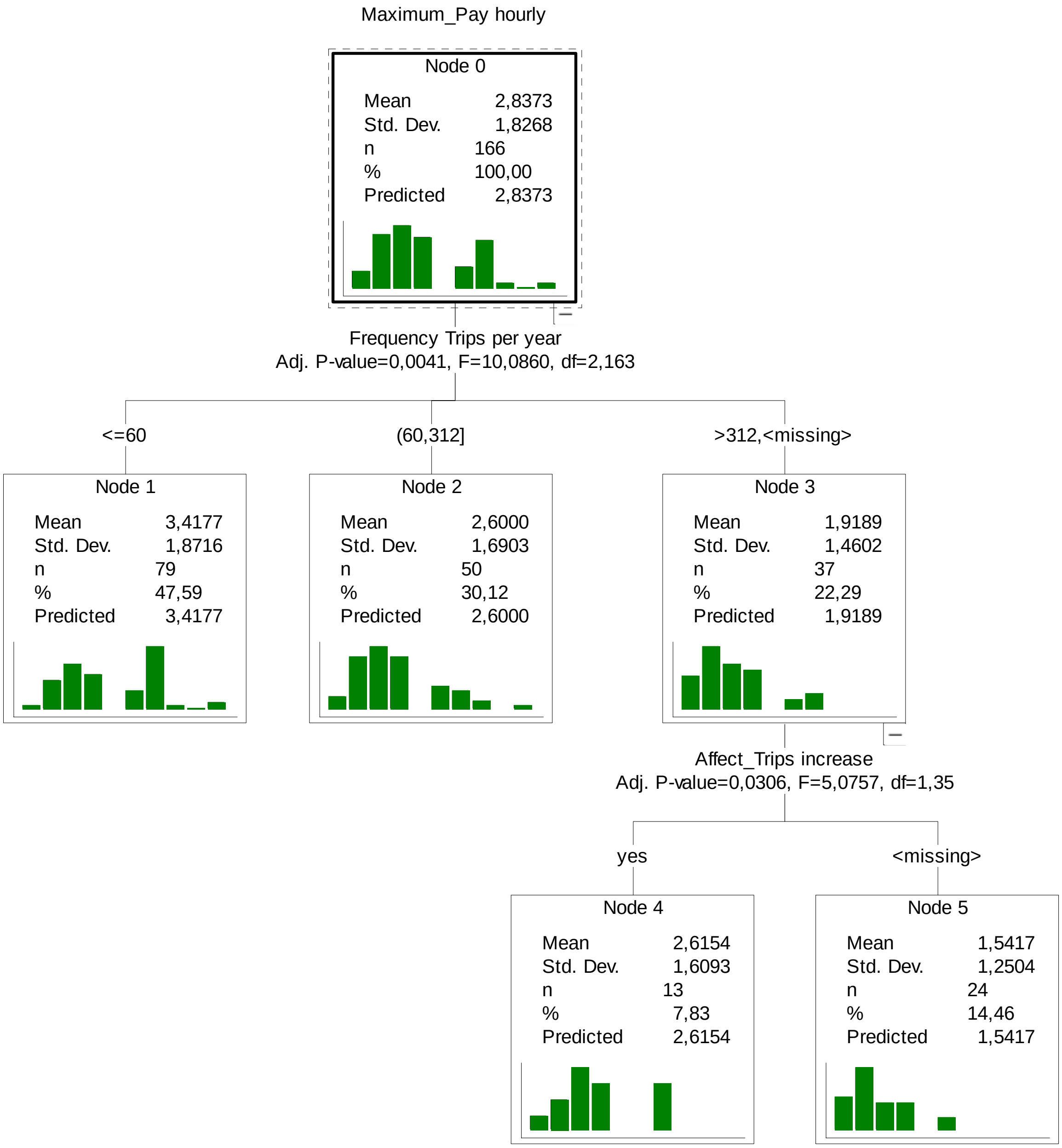


Figure 11: Classification tree to explain the willingness to pay for the Internet service by the hour

II.4.2 payment by trip

The trip frequency remains the best explaining variable of the willingness to pay, figure 12. The payment by trip/connection would be $5.4 when traveling less than 99 trips per year and $3.1 when traveling more than 99 times per year.

Among the ones traveling less than 99 times per year, the connection time is also a good indicator. The lower they would use the connection, the lower value they would pay per trip. $ 4.5 when the connection is lower than 100 minutes, and $6.5 when the planned connection would be more than 100 minutes per trip.

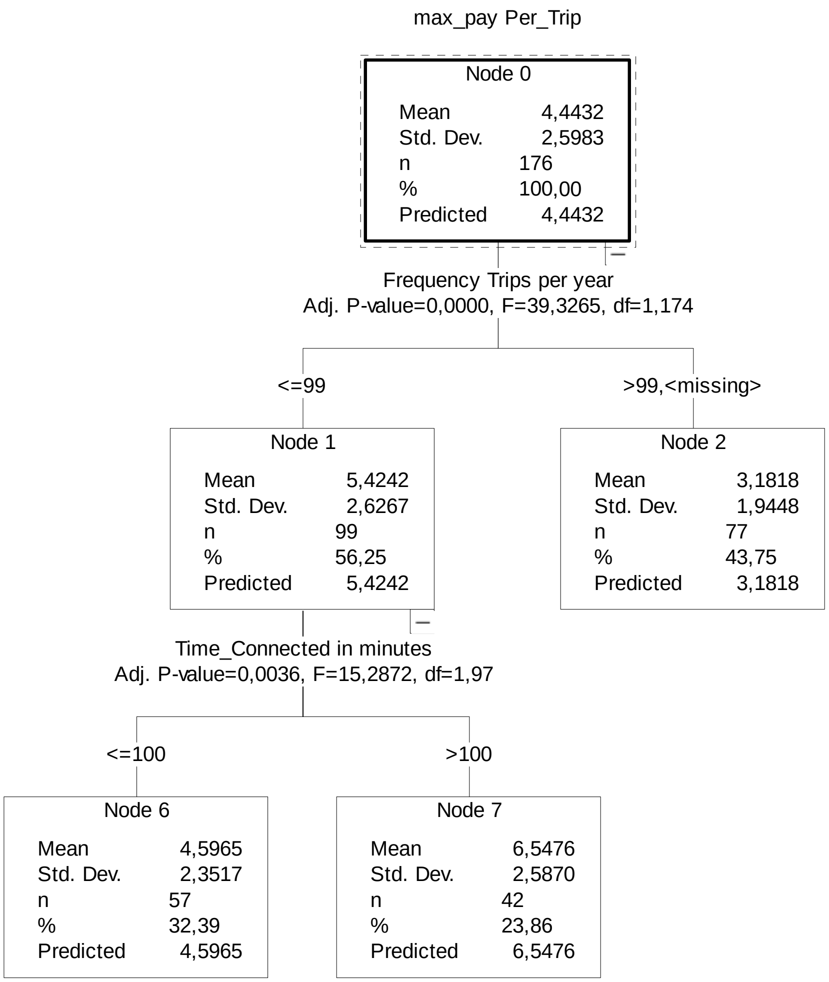


Figure 12: Classification tree to explain the willingness to pay for the Internet service by trip

II.4.3 Payment per Day

The dollar value of the connection is also explained by the trip frequency, Figure 13.

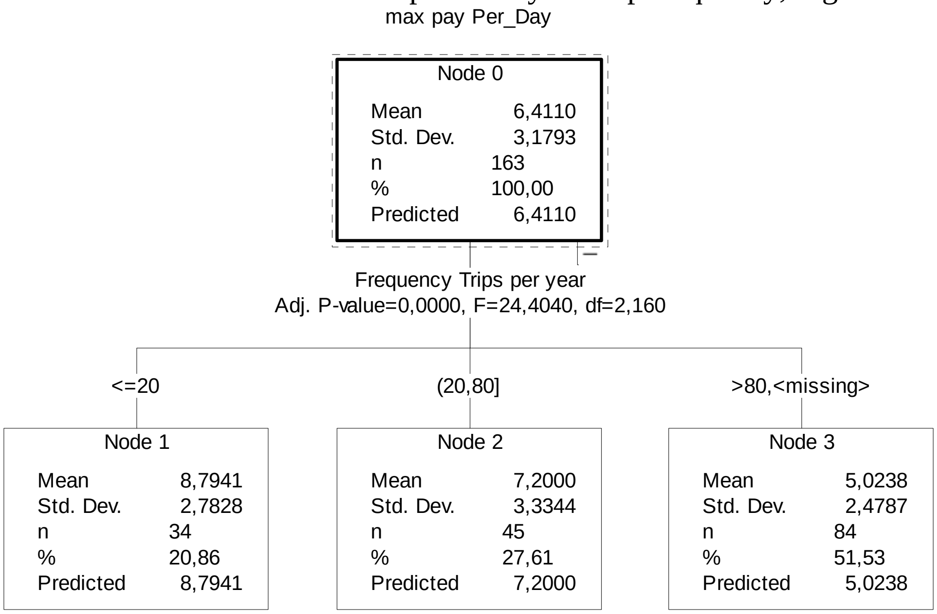


Figure 13: Classification tree to explain the willingness to pay for the Internet service by day

The dollar value is decreasing when the average number of trips per year is increasing.

II.4.4 Payment per Month

In that case the dollar value of the monthly payment is explained by willingness to use digital entertainment services, figure 14. The average monthly payment for internet connection would be $23.4 for the population willing to use digital entertainment on-board trains. The connection value would be $19.4 for the ones who do not select the service. The connection, time is the best explaining variable of the willingness to pay higher price for the digital entertainment users. The ones who intend to connect les than 80 minutes would pay $18.3 on average per month and the ones planning to connect more than 80 minutes would pay $ 26.3 per month for the internet connection on-board trains.

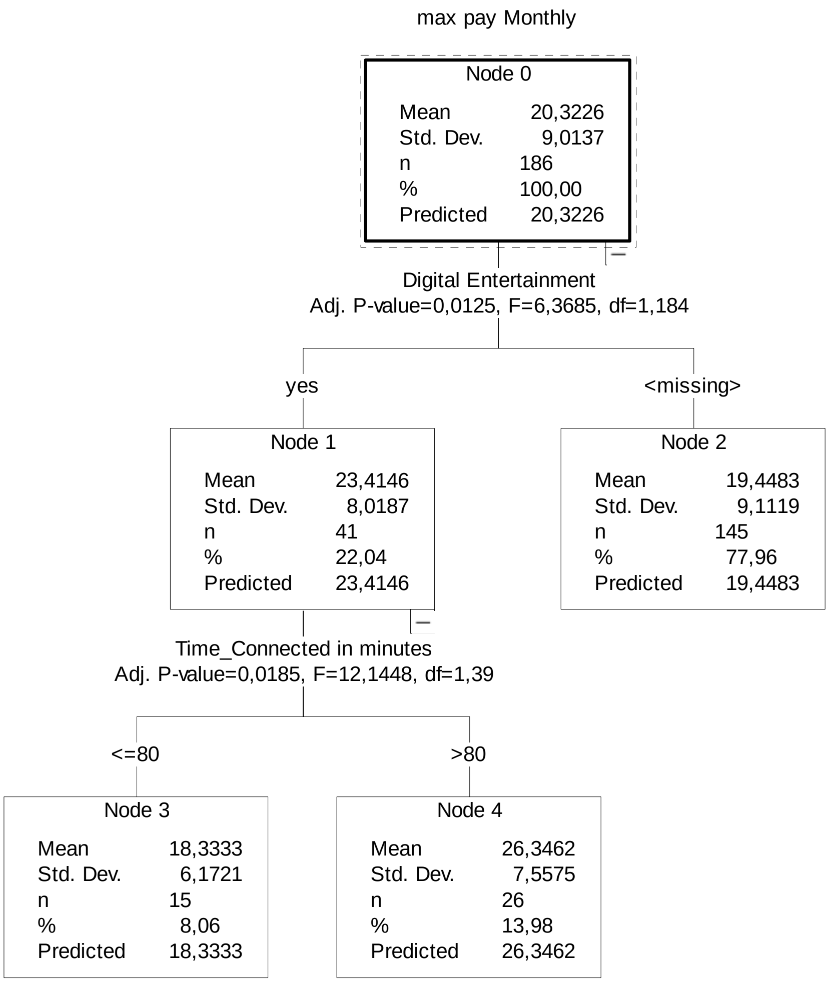


Figure 14: Classification tree to explain the willingness to pay for the Internet service by month

III Cost Revenue Models Based on Survey Results

The deployment cost/revenue models are based on two different technology choices and different scenarios of market growth.

Technologies (10 years deployment timeframe):

1) Option 1: Wi-fi hot-spots in two cars of each train (we get two cars to be sure that they would be enough seats for all wi-fi customers) the hot spot are connected to the outside world by satellite transponder (downlink) and cellular XRTT type (uplink)
We have estimated the needed bandwidth (see legends inside the figures), for the equipment and for lease lines communication costs. (All the data are explained in the attached excel spreadsheets)
This option is for high speed internet access only

2) Option 2: wi-max option, with wi-fi inside the cars and wi-max beacons along the tracks
This option is for high speed internet access and home land security services

Market growth (10 years deployment timeframe):

1) Option A: we assume that 5% of travellers who would pay for a wi-fi connection in the train, willing to pay $5 on average per trip (the average effective connection time would be 36 minutes on average, with a SMER of 20 % (effective transmission ratio). The market growth would be 2 % per year.

The figures are assessed from what we know from the market deployments in different countries (UK, Sweden, etc, see Adam's report). We conducted the same evaluation for the TGV in France (Paris-Lyon) and the Shinkansen in Japan (Tokyo-Osaka).

2) Option B: based on the estimates form the survey conducted by Doug at U.C Berkeley in July 2005.

Option B is considering a market share of 17 % of users who are usually travelling with wi-fi equipped laptop, who are willing to use the service and who are willing to pay for the service, and who are able to give a monetary value to their willingness to pay as well as a preferred mode of payment.

We selected two values:

a) $3.5 on average per trip (average 82 minutes of effective connection –survey results with a 20% SMER) and 17 % users (we assume of 2% per year theoretical market growth). *The value of $3.5 is based on the (survey) estimates from the sub population who already used the service on-board and are willing to use and pay for it in the future. . The cost per trip is calculated as an average value obtained from the different mode of payments (per hour, per trip, per day, or per month) as stated in the survey.*

b) $5.3 on average per trip (average 82 minutes of effective connection –survey results) and 17 % users (we assume of 2% theoretical market growth). *The value of $5.3 is based on the (survey) estimates from the sub population who never used the service on-board but are willing to use it and pay for it. The cost per trip is calculated as an average value obtained from the different mode of payments (per hour, per trip, per day, or per month) as stated in the survey.*
We can assume that the "true" value is between the two boundaries.

Figure 15: option1*+ option A
Figure 16: option 2* + option A

Figure 17: option1* + option B
Figure 18: option 2*+ option B

* The deployment cost of the technologies is also based on the estimated theoretical bandwidth needed to serve the total potential demand for high speed internet connection (with an acceptable quality of service. A recent article [i] shows that the of data bits transferred by the 450000 users of the T-Mobile Hot Spots in the U.S. are 45kbits on average per second of connection over 1 million sessions in one month. We think that the bandwidth available for train users should be at least equivalent to what the paying users of T-mobile use at the hot-spots in the U.S., without considering that any possibility to offer VPN connections would increase the bandwidth needed).

Figure 15: CCJPA (San-Jose Sacramento) Cost/benefits under a Satellite/cellular Communication Model
satellite and cellular communications

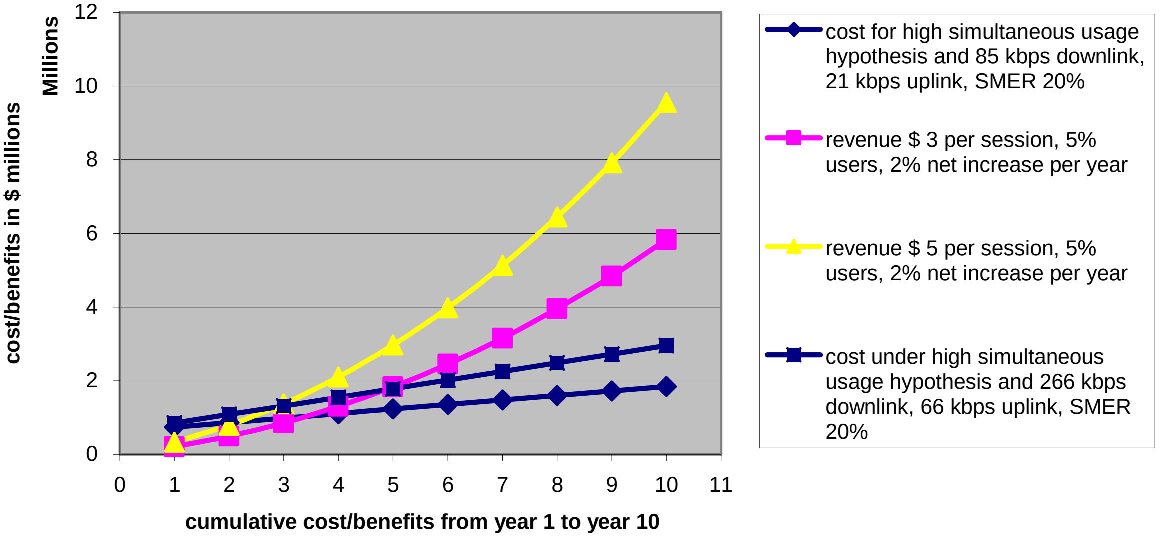


Figure 16: CCJPA (California) cost-benefit estimates based on a dedicated communication network along the tracks with 4 mega kbps (uplink+downlink)

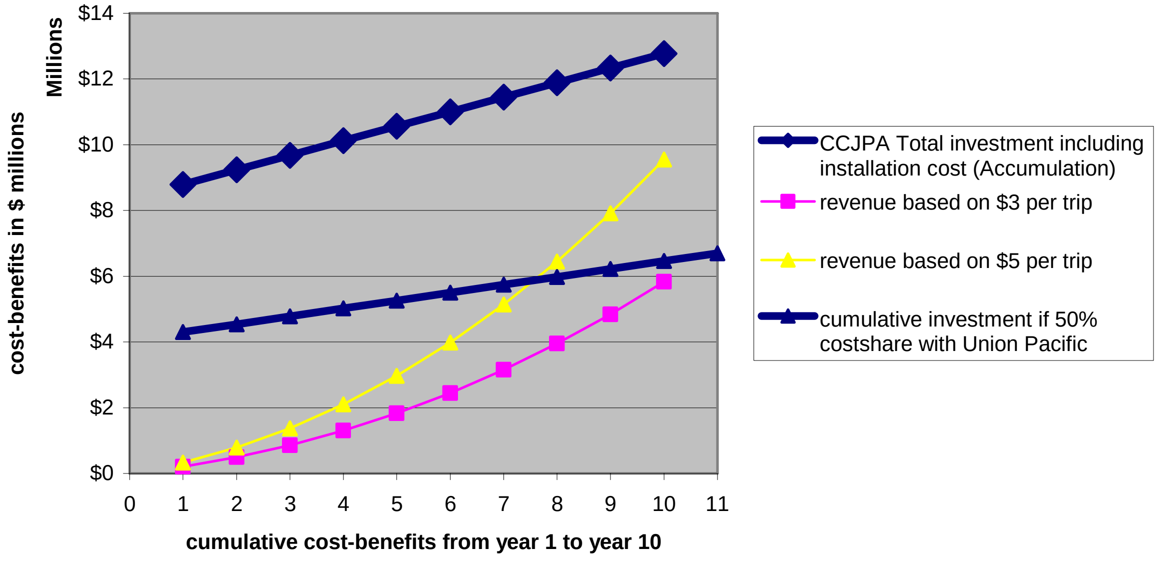


Figure 17: CCJPA (San Jose-Sacramento) cost/benefits under a satellite/cellular communication model with market usage estimates from a survey

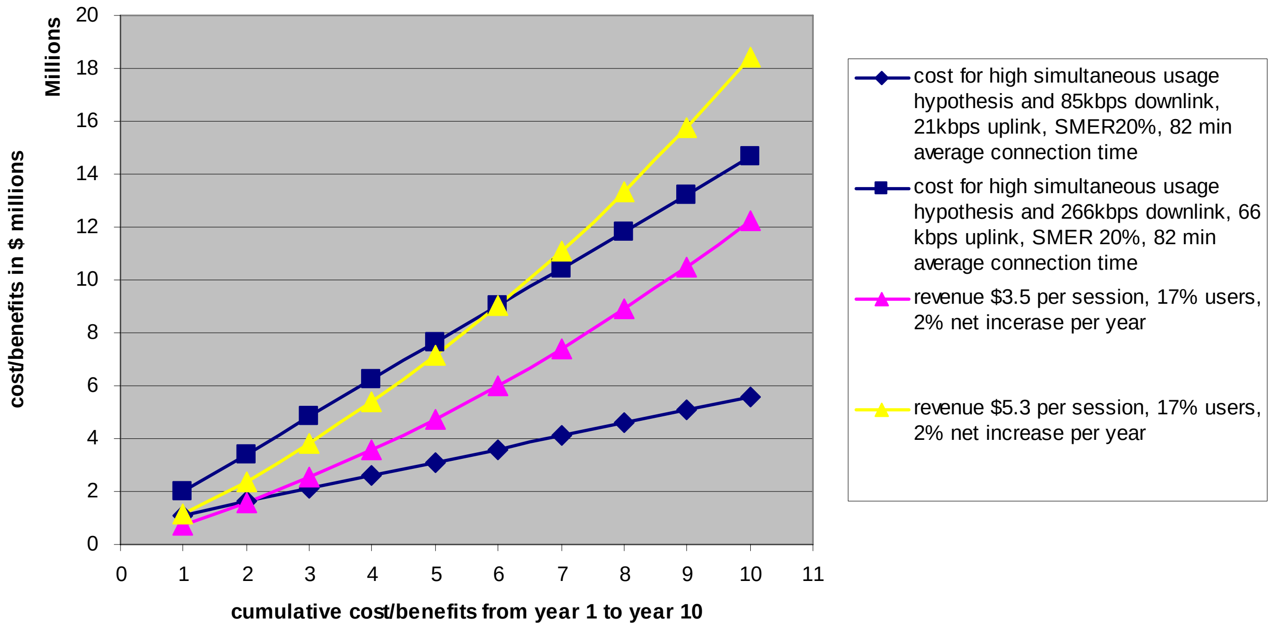
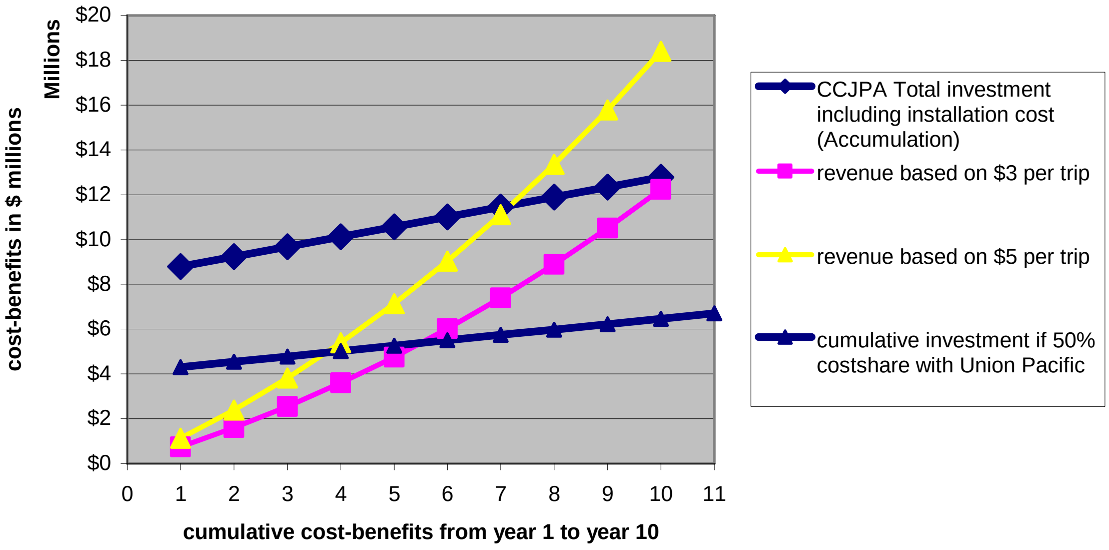


Figure 18:CCJPA (California) cost-benefit estimates based on a dedicated communication network along the tracks with 512 kbps (per user, uplink+downlink) first year



[i] http://www.informationweek.smallbizpipeline.com/infrastructure/164302525

Appendix G

Technical Reference Architecture

By

Bensen Chiou
Dr. Harsh Verma, Glocol Inc.
Dr. Jean-Luc Ygnace, INRETS, France
Kazuhiro Yamada, Central Japan Rail Company

Table of Contents

Table of Contents 3
1.1 The Reference Architecture: A Living Document 1
1.2 What is the Reference Architecture? 1
1.2.1 Architecture 1
1.2.2 Infrastructure 2
1.2.3 Strategy 2
1.3 Scope of the Reference Architecture 3
1.4 Benefits of the Reference Architecture 3
CHAPTER 2: MOBILE INTERNET AND ENTERPRISE NETWORK ARCHITECTURE 4
2.1 Strategy 4
2.1.1 Wireless Technology Usage Segments 4
2.1.2 Challenges 5
2.2 Wireless Specifications 7
2.3 Wireline Specifications 7
2.4 Network Extension 8
2.5 Redundancy in Network 8
2.6 Enhanced Network Security 8
Hot Standby 8
Load Balancing 8
2.7 The Capitol Corridor Route 9
2.8 Conceptual Diagram of the Mobile Internet and Enterprise Network 10
Connectivity to the Train 10
Cellular Internet 14
CHAPTER 3: COMPONENTS OF THE NETWORK ARCHITECTURE 15
3.1 Summary of the Network Architecture Components 15
3.1.1 Mobile Networks: 15
3.2 In-Train Architecture Components 19
3.3 Train to Back-Haul Architecture Components 22
3.3.1 What is the Back Haul? 22
3.3.2 Homeland Security/Monitoring Requirement 23
3.4 Homeland Security/Monitoring Architecture Components 23
3.5 Wireless Networks 24
Wireless LAN Architecture 24
3.6 Emerging Technologies 25
10GB Ethernet 25
IEEE 802.11n 25

CHAPTER 4: WIRELESS BROADBAND AND STANDARDS....................................27
4.1 Overview of Radio Spectrum..27
4.2 Strategy 29
4.2.1 The WiMAX Spectrum Picture 29
4.3 Protocols 34
4.4 Strategy 35
4.4.1 Overview..35
4.4.2 Radio Transmission Techniques...38
4.5 Infrastructure..41
4.5.1 Strategy 41
4.5.2 Trackside Infrastructure for Intelligent Grade Crossings 41
4.6 Issues..44
4.7 Security 45
4.7.1 Strategy 45
4.7.2 In-Train 46
4.7.3 Back-Haul to Train 54
4.7.4 Homeland Security/Monitoring 55
4.7.5 Back-Haul to Train - FCC and DHS Collaboration..........................55
4.7.6 Homeland Security/Monitoring Architecture Components and National ITS Architecture...57
4.8 Applications Required To Be Supported 73
4.8.1 Homeland Security..73
CHAPTER 5: BANDWIDTH REQUIREMENTS...76
5.1 Strategy 76
5.2 Applications and Bandwidth Requirement 76
CHAPTER 6: APPENDIX 81
6.1 Standards..81
6.1.1 Overview..81
6.1.2 Reliability and Availability...82
6.1.3 Approvals and Compliance..82
6.1.4 Wireless Standards..83
6.2 Performance Specifications 84

CHAPTER 1: INTRODUCTION

1.1 The Reference Architecture: A Living Document

The Reference Architecture document is a living document and is meant to be updated periodically to incorporate changes in technology and business requirements.

1.2 What is the Reference Architecture?

The reference architecture of CCJPA-Caltrans RFQ is a key ingredient to providing information quickly and effectively to people. The desire is to have a wireless technology architecture that supports WiFi for commuters on Capitol Corridor Inter-City Trains between Auburn and San Jose, California, while being consistent, manageable, non-redundant, comprehensive, and easily integrated with the Homeland Security Requirements for Rail Transportation Infrastructure.

The user group requiring information is no longer just individuals within CCJPA. Individuals and organizations outside of CCJPA need access to Security and Safety related information located throughout Caltrans and Transportation Security Administration of Homeland Security. The technical architecture provides the base upon which applications are built that support these needs.

An architecture is a blueprint rather than a facility. It is often compared to the city plan that lays out major highways, sets zoning ordinances, and defines locations and utilities. It does not describe the details of houses, though it may impose standards of size, construction, and safety. The architecture is not intended to limit the solutions or creativity of the individuals involved with the business enterprise. The purpose of the architecture is to provide guidelines that promote and facilitate the integration of systems and development of an infrastructure that is consistent, manageable, scaleable, and easily integrated.

Within the Information Technology profession, two terms, architecture and infrastructure, are used interchangeably; however, each has a very different meaning. For this reason, clarifying these terms initially should reduce the potential for any misunderstanding.

1.2.1 Architecture

Architecture defines the guiding principles that will create the framework from which the infrastructure can be defined. It is the general direction that the operating systems, hardware, and networks will take.

Architecture refers to the logical view of the data, processes, applications, technology, and standards required to support the business from an information and technology perspective. The architecture also defines the standards, policies, and procedures for implementing an environment. Architecture addresses the structure and interconnection between information processing and technology as well as the logical information and technology architecture required to support business systems.

1.2.2 Infrastructure

Infrastructure defines the specific components that make up the wireless local area network (WLAN), wide area network (WAN), back-haul network and backbone hardware, operating systems, mobile environment applications, identity management and relational database management system (RDBMS). The infrastructure is defined based on the recommendations of the architecture. The architecture provides guiding principles; whereas, the infrastructure defines the specific components that are required.

Recommendations Leading to the Reference Architecture

Information technology architecture is a series of principles, guidelines, or rules used by an organization to direct the process of acquiring, building, modifying, and interfacing with IT resources throughout the enterprise. These resources can include equipment, software, communications protocols, application development methodologies, database systems, modeling tools, IT organizational structures, and more. The benefit of an integrated architecture is a more efficient business providing greater service to the end user and promoting a greater sense of collaboration that will contribute to the best use of available resources.

The following objectives may be kept in mind:

- Provide an integrated, scaleable, and supportable technology architecture
- Coordinate solutions and information flows for technology architecture development
- Include appropriate controls and access for commuters as well as support for security operations, wireless business area, workgroup, and employee operations computing
- Ensure effective development, maintenance, and integration of the data, application, and technology architectures
- Involve stakeholders throughout the Department in definition and evolution of the technology architecture
- Include a “configuration management” process by which existing data, applications, and technology components can be managed and migrated toward the defined architecture.

The Reference Architecture is the basic foundation for the CCJPA WiFi on Train and Homeland Security Processes and Caltrans business functions. It is on the critical path to enable future Wireless Applications projects.

The focus of the Reference Architecture is to provide CCJPA and Caltrans with an enterprise-wide blueprint for the future technical architecture. The Reference Architecture is one of the essential pieces that allows business and technical teams to develop applications to support CCJPA and Caltrans.

The topics addressed in this document include:

- Mobile Internet for Train Commuters and Enterprise Network Architecture
- Information Security Architecture
- Hardware Architecture
- Operating Systems
- Applications Platform Architecture
- Relational Database Management System (RDBMS)
- Enterprise Systems Management
- Reliability & Fault Tolerance

1.2.3 Strategy

CCJPA commuters demanded Wi-Fi and it is being analyzed that Wi-Fi may be helpful in increasing train commute by as much as 71% (ref: BBC News Item)

It was important to do trial evaluations in making decisions and in allocating resources. In order to ensure that these decisions and allocations are made with the highest quality data, sound management practices are essential.

By using sound management practices, Caltrans and CCJPA WiFi on Trains project is gradually being moved from a somewhat "experimental trials" state toward a more "integrated" state. This is a long-term process.

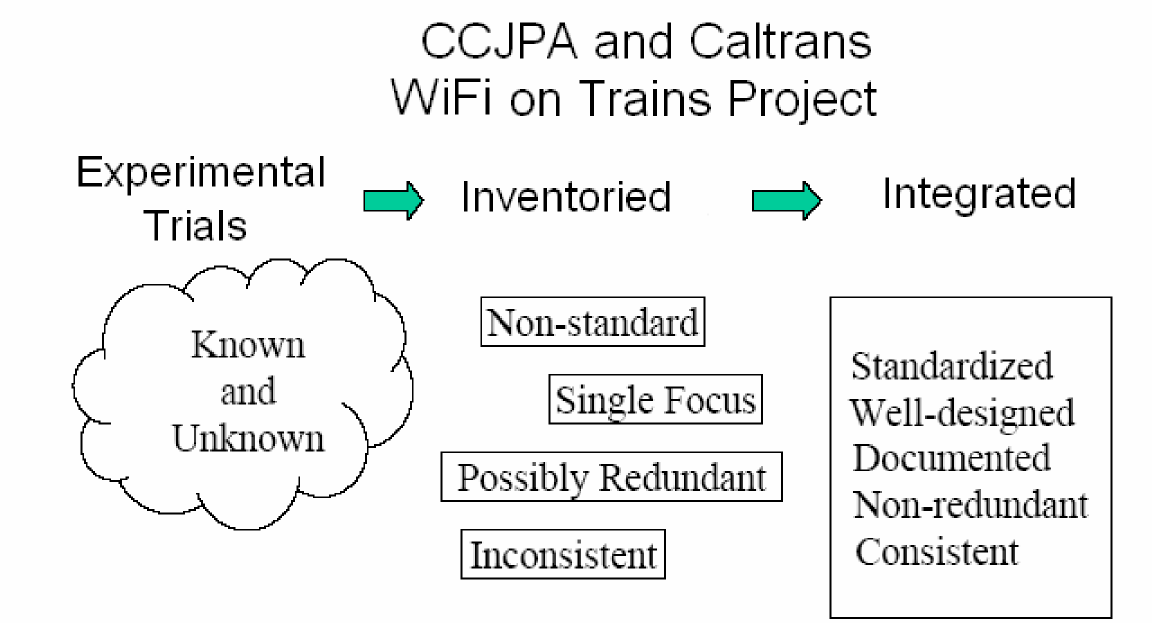


Figure 1: WiFi on Trains Project

1.3 Scope of the Reference Architecture

The focus of the Reference Architecture is to provide CCJPA with an enterprise-wide blueprint for WiFi design. For software project development teams, working with existing applications or developing new applications, the Reference Architecture is essential. Topics addressed in this document include:

- Architecture standards
- Wireless Standards
- Protocols
- Radio Frequency Spectrum.

1.4 Benefits of the Reference Architecture

Applying components of the CCJPA Reference Architecture when creating or modifying wireless-based applications will:

- Provide an environment that promotes better communication and more informed decision-making for both internal and external stakeholders
- Promote a common understanding of the components
- Promote the sharing of data across organizational boundaries
- Reduce redundancy
- Reduce loss of knowledge due to turnover and retirement.

Applying the Reference Architecture will produce benefits to CCJPA. Non-compliance, in favor of quick implementation, will almost certainly result in eventual increased costs.

CHAPTER 2: MOBILE INTERNET AND ENTERPRISE NETWORK ARCHITECTURE

2.1 Strategy

The Mobile Internet and Enterprise Network Architecture is the foundation of the overall architecture. All other components rely upon the availability and capabilities of the network. This is summarized as follows:

The ingenuity of this reference architecture is to explore how technologies utilizing high gain antennas, Wi-Fi meshed networks and WiMAX together with Mobile IP based Mobile Networks can be combined to provide a total last-mile access solution now and in the future.

For the first time, joint government, academia and industry-wide support and innovation are driving broadband wireless networking technologies and network operators, service providers and users would benefit from a wide array of high-performance, feature-rich and cost effective products and services.

2.1.1 Wireless Technology Usage Segments

Different characteristics behind wireless components for the Enterprise Architecture are as diverse as the wireless technologies being offered today. Each wireless technology is designed to serve a specific usage segment and component of the architecture:

- Commuter Personal Usage - Personal area networks (PANs)
- In-Car Train - Local area networks (LANs)
- Train-to-Trackside - Metropolitan area networks (MANs)
- Trackside-to-Internet - Wide area networks (WANs)

The requirements for each usage segment are based on a variety of variables, including:

- Bandwidth needs
- Distance needs
- Power
- User location
- Services offered
- Network ownership

The three key deployment types that make up the wireless access for above train usage access are:

- Backhaul,
- Last-mile and
- Coverage (referred to as hot zones).

Wireless last-mile coverage typically uses the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard with high-gain antennas, while hot zones use modified IEEE 802.11 equipment in a mesh deployment.

IEEE 802.16 features can resolve many of the difficulties in last-mile implementations which will have a considerable impact in the evaluation of terrestrial networks for train connectivity.

Open standard radio technologies—including 802.11, 802.16 and future standards—offer advantages to WISPs and users.

Wireless Fidelity (Wi-Fi) revolutionized the market for unlicensed client-access radios in a wide variety of applications. Starting in 2005, Worldwide Interoperability for Microwave Access (WiMAX) certification of the IEEE 802.16-2004 standard for fixed-position radios will do the same for point-to-point (P2P) and point-to-multi-point (P2MP) wireless broadband equipment in both the licensed and unlicensed bands.

In 2006, the IEEE 802.16e standard for portable operation is expected to be ratified, thus standardizing client radios in unlicensed and licensed bands. This certification will provide users with an alternative and allow service providers the benefit of additional tier services.

The cost and limited flexibility of wired backhaul limits wireless access growth. Wired backhaul solutions can be too expensive for establishing widespread wireless access and because a standard means for deploying IEEE 802.11 into the last mile or within a hot zone has not emerged, each WISP implements long-distance IEEE 802.11 solutions differently.

WiMAX is a wireless metropolitan-area network technology that provides interoperable broadband wireless connectivity to fixed, portable and nomadic users. It provides up to 50-kilometers of service area, allows users to get broadband connectivity without the need of direct line-of-sight to the base station, and provides total data rates up to 70 Mbps — enough bandwidth to simultaneously support hundreds of businesses and homes with a single base station.

2.1.2 Challenges

Typical modified IEEE 802.11 network topologies associated with last-mile and hot-zone coverage use either directional antennas or a mesh-network topology. Wi-Fi provides the certification for IEEE 802.11 client-to-access point (AP) communications. However, implementations of AP-to-AP and AP-to-service providers (that is, backhaul applications) that are typically needed for wireless last-mile and hot-zone coverage are still proprietary, thus providing little or no interoperability.

Because the IEEE 802.11 standards were designed for unwiring the local area network (LAN), metro-access applications are facing the following challenges:

• *Non-standard Wireless inter-AP communication*
Today, wireless links used to connect 802.11 APs for inter-AP communication in mesh networking are vendor-specific. The proposed IEEE 802.11s standard, estimated to be ratified in 2007, will standardize Wi-Fi mesh networking.

• *Providing Quality of Service (QoS)*
QoS refers to the ability of the network to provide better service to selected network traffic over various technologies. The goal of QoS technologies is to provide priority (including dedicated bandwidth to control jitter and latency) that is required by some real-time and interactive traffic, while making sure that in so doing the traffic on the other paths does not fail. In general, unlicensed bands can be subject to QoS issues because deployment is open to anyone. Advances in the associated standards and related technologies, however, help mitigate problems with unlicensed bands, such as multi-path interference. The proposed IEEE 802.11e standard, which is projected to be ratified in 2006, will standardize Wi-Fi mesh-network topology.

• *Expensive Backhaul Costs*
Backhaul refers both to the connection from the AP back to the provider and to the connection from the provider to the core network. To extend wireless access nodes, providers still rely on wires for long distance coverage. Some providers find wiring large areas too expensive.

• *Limited Services*
Without QoS, applications such as voice over Internet protocol (VoIP) may reduce a call’s quality, thus limiting the provider’s ability to tier services and obtain additional revenue streams. Current Wi-Fi last-mile and large-coverage solutions offer excellent data transfers. Some vendors offer proprietary QoS.

Despite the challenges, an integrated solution could resolve the main issues for the following reasons:

- Wireless metro-access solutions available today, if deployed in a cost-sharing mode jointly with a city, using mesh networking implementations, can be more cost-effective and flexible than their wired counterparts.
- Such a solution can provide a standards-based connection from AP-to-mobile users for hot-zone coverage.
- WISPs can offer broadband services to geographically challenged areas (such as rural towns near the **Richmond** or **Suisun-Fairfield** area).
- Local governments can provide free access for businesses or emergency services (such as police and fire fighters).
- Homeland Security Control Management Center can communicate through this network and monitor activities in near real time.

• *Transmission Control Protocol / Internet Protocol (TCP/IP)*

With the growth of the Internet and networks, TCP/IP has become the primary protocol for connectivity. In order to address the needs of commuters and future client/server and intranet technologies, Mobile Internet with TCP/IP protocol should be available.

2.2 Wireless Specifications

All Internet Connectivity for commuters in the rail car must comply with IEEE 802.11g standards and specifications. IEEE 802.11g (Wireless-G) is the upcoming 54Mbps wireless networking standard that's almost five times faster than the widely deployed Wireless-B (802.11b) products found in homes, businesses, and public wireless hotspots around the country - but since they share the same 2.4GHz radio band, Wireless-G devices can also work with existing 11Mbps Wireless-B equipment.

- Standards Compliant - comply with the IEEE802.11g (DSSS) specifications for Wireless LANs
- Supports both 802.11b and 802.11g Wireless Stations - The 802.11g standard provides for full backward compatibility with the 802.11b standard, so both 802.11b and 802.11g Wireless stations can be used simultaneously.
- Speeds of min 54Mbps - Speeds up to the 802.11g standards of 54Mbps
- Encryption as it relates to Wireless Networking

2.3 Wireline Specifications

All data wiring in any part of CCJPA Rail Cars shall comply with the EIA/TIA 568 standards and use unshielded twisted pair (UTP) category six (6) or better wire.

Copper

- Category 6 Cabling With (568-B.2-1) with a maximum distance of 100m or 295 feet
- Maximum attenuation of Cable = 19.8 db, Connector = 0.2 db, and channel = 21.3 db
- Category 6 Cabling must be plenum rated
- Speeds up to 1000 Mbps

Fibre-optics

- 1000 Base FX to provide speeds matching the Catagory 6 Cabling
- Fiber Optics should be Multimode

2.4 Network Extension

The system must provision for any extension to any Homeland Security Interface office and specifically be.

i. Interoperable with existing security surveillance system in place
ii. Interoperable with existing emergency response system.
iii. Provide additional security surveillance system intelligently reducing needs of high bandwidth communication system.

2.5 Redundancy in Network

The system must provision for redundant connectivity where required for Homeland Security Needs. This will provide a more robust fault-tolerant network, which is required for a successful implementation of client/server and intranet technologies for Homeland Security Requirement.

One of the options for providing redundancy is to ensure that all wireless access stations are supplied by two different network providers. Backup power supplies and generators may also be utilized to ensure continuity at wireless access stations.

Outside monitoring may be utilized to ensure network uptime. Network monitoring can be handled by a centralized Network Operations Facility or it may be outsourced to a network security company. This mechanism will also be used to measure bandwidth availability and performance of the network. Such testing will allow for proactive network upgrades to continually provide superior service to the end users.

2.6 Enhanced Network Security

Hot Standby

- Support failover to a standby device, thus increasing network uptime.
- Automatically routed by routing protocol inherent in networking equipment
- Provides for greater network redundancy for network continuity and traffic management

Load Balancing

- Distribute user connections across available access points to optimize aggregate throughput.
- Greater network performance during peak usage
- Assists in network continuity during equipment outages

2.7 The Capitol Corridor Route

The route of the Capitol Corridor between Auburn and San Jose, California is shown below. The diverse geographical characteristics and areas including the curves and bends of the track must be kept in mind for providing the best and most cost-effective Internet coverage on the route.

There are a total number of 15 stops between Auburn and San Jose and 3 motor coach routes from Sacramento, Emeryville and Oakland on certain trains and certain times. It is not the intention to provide Internet services on the motor coaches connecting the train to the points of destination.

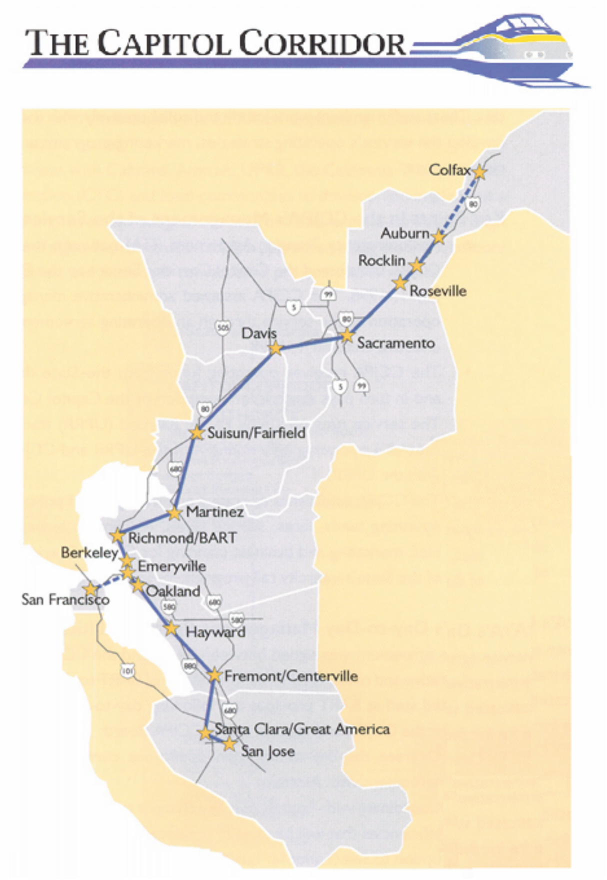


Figure 2: The Capital Corridor Route

2.8 Conceptual Diagram of the Mobile Internet and Enterprise Network

Connectivity to the Train

There are three possible independent modes for providing connectivity to the train:

1. Satellite Communication
2. Existing Cellular Networks
3. WiFi/WiMax Bridge Network

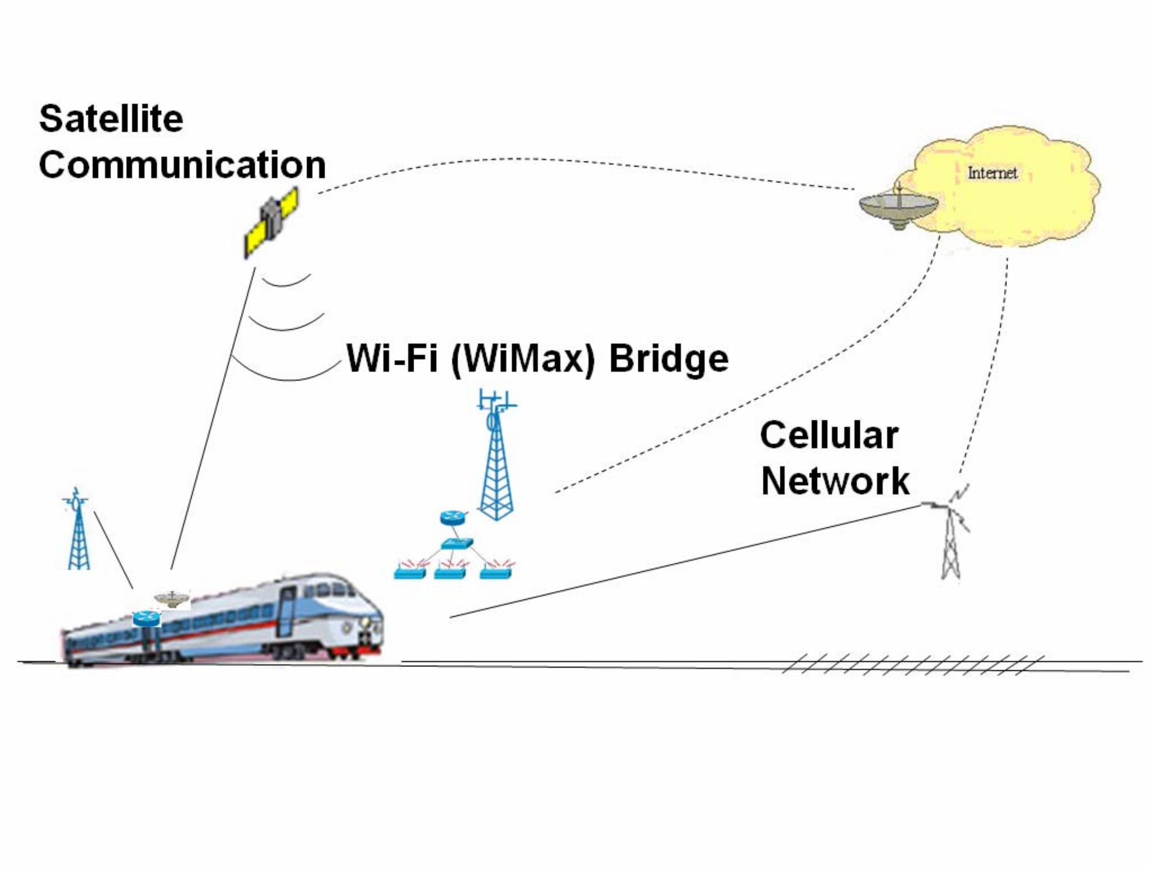


Figure 3: Conceptual Diagram to show connectivity to the train

CCJPA and Caltrans trials presently run two types of wireless components thru the OptiFi Trials

- Satellite for Download
- Cellular for Upload

Satellite Communications

Satellite communications technology is critical to understanding the future direction that the deployment for WiFi and Homeland Security could take. Often new applications will stimulate technical innovations, and in some cases -- for example, that of frequency congestion. It is quite obvious that the development of new satellite technology should be consistent with the market need and opportunity, however a prime reason for using satellite communications is to provide a Backup or fall-up mechanism if trackside infrastructure or cellular network is out of service, let us say, because of an earthquake, as happened in the case of Hurricane Katrina, when the only communication channel available was Satellite.

The advantage of Satellite communications is that it covers remote areas where Trackside DSL, cable access or cellular is unavailable. Satellite communication services utilize telecommunications satellites in Earth orbit to provide Internet access to for the Backhaul. However, Satellite offers relatively less network bandwidth. In addition, the long delays required to transmit data between the satellite and the ground stations tend to create high network **latency**, causing a sluggish performance experience in some cases. Network applications like **VPN** and online gaming may not function properly over satellite Internet connections due to these latency issues.

Older residential satellite Internet services support only "one-way" downloads over the satellite link, requiring cellular connectivity for uploading. All newer satellite services support full "two-way" satellite links.

Two-way satellite Internet consists of:

- Approximately a two-foot by three-foot dish
- Two modems (uplink and downlink)
- Coaxial cables between dish and modem

A typical satellite based system comprises of:

- On Roof Antenna System
- Antenna Controller
- Satellite Modem
- In-train Wi-Fi distribution system

The service can be managed remotely by the back-office system located at the Network Control Center.

The fourth-generation of satellites doesn’t cover huge areas by default. Instead, they can beam 492 Kbps signals to areas that range from the size of a city to the size of a small region.

Such communication will have to rely on bi-directional satellite link to make the Wi-Fi more of a business service, and to serve as a backup for infrastructure fallout. Also if passing through a tunnel, a train link using satellite communication should be capable of being restored within a couple of seconds and the system should allow users to maintain their link to a local server onboard the train.

The current trial uses one-way satellite for downlink and cellular 1xRTT for uplink. The bandwidth is a limitation limiting to a maximum of 10 users.

Recently 21Net, a company based out of Spain, deployed satellite communication to support a high speed service. During trials, four laptops on a train were reported to be connected at 700 Kbps each. 21Net reports a fast uplink to the Internet using satellite connection than GPRS or 3G to send data from the train to the Internet.

21Net's system claims to support business applications such as video conferencing and the sending of large emails, and being comparable to ADSL. Trials took place in late June 2005 and late July at undisclosed locations in Europe. Hyde-Thomson said that during one trial four laptops were able to each get a connection speed of 700Kbps simultaneously on a train moving over 300 kilometers per hour.

Current Satellite Internet services for use on trains provide a capability of multimedia, broadband internet and intranet access, however it will be key to be able to provide VPN access in addition to access to Internet and email and download and upload capability. In addition there is a perceived need for a variety of entertainment that may be provided from on board servers to passengers with wireless equipped laptops. These users' needs have been established by market research and by various similar services that have been offered on some trains (such as DVD player rental on Eurostar trains seatback video screens in D Bahn ICE, etc).

Satellite system architectures are typically based on two-way Ku-band satellite transmission to provide connectivity between the internet backbone and a master server on the train. Direct reception of satellite television channels on the same satellite is also possible.

A hub earth station provides the connection from the backbone (and from the network operations centre) via the satellite directly to a low-profile tracking antenna on the train. GPRS and Wi-Fi access between the train and available networks (e.g. in stations and in tunnels) may also be provided.

Key Issues

The key issues to be addressed for Satellite Communication are:

- Availability of low-profile two-way Ku-band tracking antennas at an appropriate cost
- Meeting stringent safety requirements of high speed train operators.

Benefits

The benefit of 21Net's solution is the provision of a business-class broadband internet access to customers in a reliable and cost effective manner. The emphasis is on providing a quality service rather than the intermittent, low bandwidth service that a GPRS-enabled laptop user might suffer today.

In particular, the use of two-way Ku-band satellite transmission enables high bandwidth (2MBit/s by 512kBit/s) un-contended connectivity to the train which will be shared by (say) 50 simultaneous users.

Based on tests by 21Net, it is reasonable to expect satellite link with the train at 4MBit/s downlink and 2MBit/s uplink, with 10 users using the system via Wi-Fi enabled laptops (downloading large files, streaming videos, etc).

The Thalys train operating on the line between Brussels and Paris is said to provide service to as many as 100 users per train using the 21Net satellite broadband infrastructure.

The equipment must interface with a wide range of radio backhaul networks and WLAN authentication, authorization, and accounting (AAA) systems. The mobile networks using Mobile Router, must intelligently and seamlessly manage a combination of satellite, cellular and 802.11/802.16 connectivity to the Internet to ensure maximum uptime for commuters. Requests would be transmitted from the customer's client device, such as a laptop or handheld computer, to the wireless LAN aboard the train and then to the Network Control Centre.

The need for Homeland Security requirements is to provide seamless access to mission-critical voice, video and data communications for emergency purposes.

In addition to connection management functions, the mobile networks must contain an integrated caching and scheduling engine that enhances the user experience by storing frequently used and custom content for rapid onboard access without tying up external radio connections. Multiple methods of content provisioning, including cached content and direct download could be used. The customer on board the train experiences improved speed and service performance, while the cache ensures that valuable external bandwidth is left available for other customers and uses.

Cellular Internet

Cell phones have existed for decades, but only recently have cellular networks evolved to become a mainstream form of wireless Internet service. By cabling a cell phone to a router in the train and installing a cellular network adapter and a wi-fi hot spot, Internet connectivity can be maintained and provided within any area with cell tower coverage.

EDGE (Enhanced Data rate for Global Evolution) provides data speeds up to 384 Kbps for TDMA and GSM networks;

GPRS (General Packet Radio Service) 171.2 Kbps speeds on GSM networks; and

1XRTT provides speeds up to 144 Kbps in CDMA networks.

Older cellular communication protocols allowed for only very low speed networking. Newer "3G" cell technologies like **EV-DO** and UMTS promise to deliver network speeds competitive with those of DSL and other wired networks.

Many cellular providers sell Internet subscription plans separate from their voice network contracts. Generally speaking, cellular Internet will not function without having an Internet subscription n place.

EVDO is a high-speed network protocol used for wireless Internet data communications. EVDO supports up to 2.4 Mbps bandwidth using a set of radio frequency channels. The EVDO protocol supports asymmetric communications, allocating a majority of this bandwidth for downloads. Like cable modem and other broadband Internet technologies, EV-DO is an "always-on" service that does not require establishing dialup network connections. Some CDMA cell phones support EVDO.

The focus of this research is to evaluate trackside Wi-Fi or terrestrial networks using terrestrial radio and mobile network technologies.

CHAPTER 3: COMPONENTS OF THE NETWORK ARCHITECTURE

3.1 Summary of the Network Architecture Components.

There are different types of network architecture components as follows:

- Command and control centers including the following:
    - Mobile Internet service center performing the configuration management and user provisioning. It includes user interface, database management system, client authentication server, etc
    - Homeland security service center configuring the access control to the homeland security related infrastructure & capability, and operating the homeland security subsystems. It includes the user interface, database management system, security officer provisioning system, security violation incident processing and database.
- In-Train Architecture components – components on-train supporting the mobile Internet service and homeland security service
- Train to Back-Haul Architecture component
- Trackside communication system connecting all the trackside wireless infrastructures to the data gateway on which the data is routed to different service centers.
- Homeland security surveillance system alerting security violation, capturing incident scene, and sending processed incidents to security service center.
- Data gateway dispatching data to various service centers, and the deployed wireless infrastructure and security system.
- Data network connecting data switch to various service centers
- Interface to emergency response system
- Interface to law enforcement systems
- Interface to existing homeland security infrastructure

In addition, there are data networks connecting the data aggregation switch to various service centers.

3.1.1 Mobile Networks:

The main aim of this research is to evaluate trackside infrastructure to provide the rail authorities with hi-speed wireless access at high throughputs and fast connections. Previous projects have used cellular uplink/ satellite downlink to provide this on board connectivity. Trackside Infrastructure has the potential of providing high connectivity via WiFi (or WiMAX) which will allow higher throughputs. With geo-stationary satellites, for example, a signal has a round trip time of approximately 0.5 seconds. 3G cellular networks generally offer throughputs only up to 2Mbps.

Mobile IP:

Providing constant WiFi access on board a moving train is possible because of Mobile IP. Mobile IP is an open standard defined by the Internet Engineering Task Force (IETF) RFC 3220. It allows a client to maintain the same IP address as it roams between different networks. This is essential in order to maintain a continuous uninterrupted connection while moving between networks, as is the case on board a train. Mobile IP operates at the network layer and is based on IP, and thus is supported by any media which supports IP.

Mobile Network Components:

A mobile network generally consists of mobile nodes or a mobile router, a home agent, and a foreign agent.

Mobile Node: A mobile node (MN) is a device which appears to be connected to its home network (maintaining the same IP address), while it roams between networks.

Mobile Router: A mobile router (MR) works similarly to a mobile node, except that it allows entire networks to roam. The Cisco 3200 Mobile Access Router includes a WMIC (Wireless Mobile Interface Card) which acts as an access point as well.

Home Agent: A home agent (HA) is a router at the home network through which a mobile router receives authentication and authorization, and which directs traffic destined to a node on the mobile network, to the mobile router by maintaining an association between the latter’s home IP address and care-of address. In order to do this, the HA creates an entry for the mobile network in its routing table.

Foreign Agent: A foreign agent (FA) is a router at the foreign network which helps the mobile router inform its home agent of its care-of address, and delivers packets from the home agent to the mobile router. The FA is a fixed router.

Care-of Address: The current location of a mobile router on a foreign network.

The MR, HA, and FA are generally connected in the following manner:

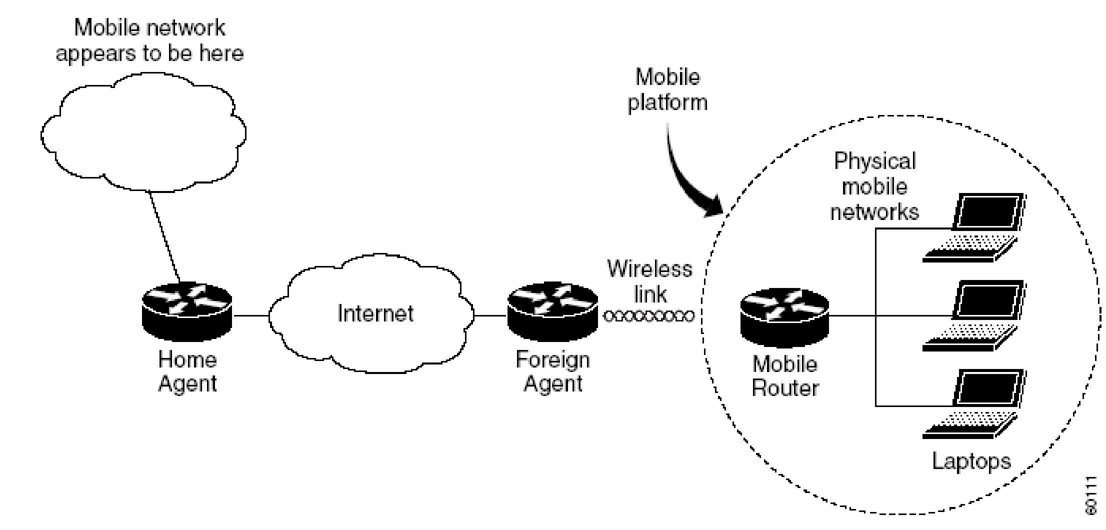


Figure 4: A Typical Mobile Network (Courtesy Cisco Systems)

In the train setup, the foreign agent is placed along the trackside and connected through wired media or the internet to the home agent. The mobile router on the other hand is placed on board the train. The mobile router may be used to provide the in-car network connectivity, in which case a MR is required in each car supporting wireless access. On the other hand it can be placed in one car, constituting an infrastructure network while other cars are infrastructure less and connect to the main car via an ad-hoc network.

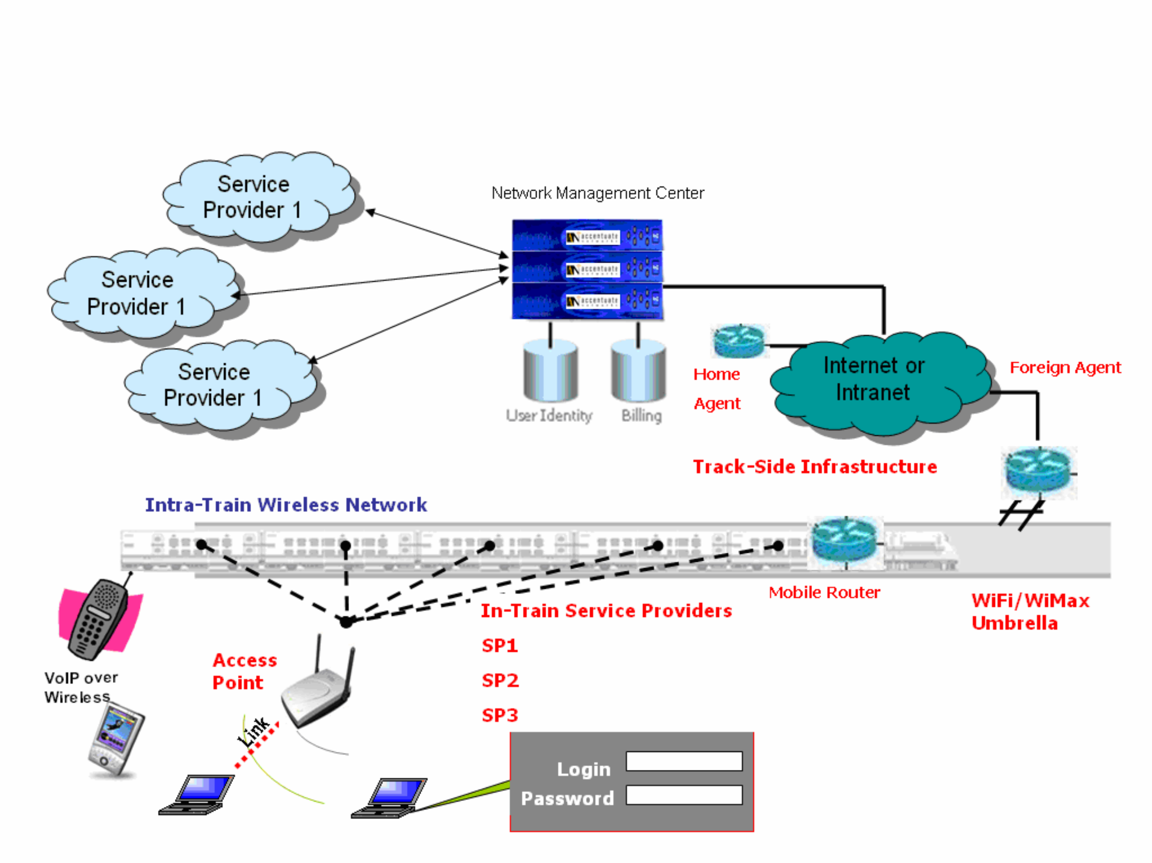


Figure 5: Hi-Level Architectural Framework

3.2 In-Train Architecture Components

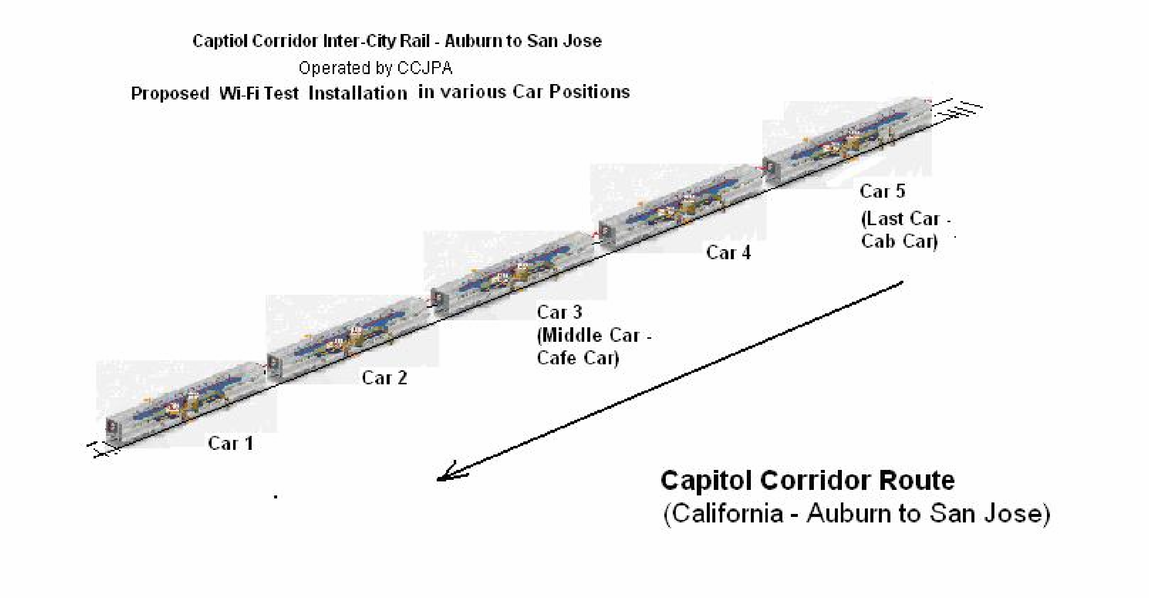

Captiol Corridor Inter-City Rail - Auburn to San Jose
Operated by CCJPA
Proposed Wi-Fi Test Installation in various Car Positions
Car 5
(Last Car - Cab Car)
Car 4
Car 3
(Middle Car - Cafe Car)
Car 2
Car 1
Capitol Corridor Route
(California - Auburn to San Jose)

Figure 6: Proposed Installation

In-Train Access would require at least the following components:

- On Roof Antenna System
- Antenna Controller
- Satellite / Wi-Fi / Wi-Max / Cellular Modems and Routers
- Wi-Fi in-train distribution system
- Onboard Server
- WLAN access points

Value-Chain of Hardware, Identity Management and Services In-train

The diagram below describes the Value-Chain of Hardware, Hotspot, Network Provisioning, Authentication and Security for Identity Management, Accounting and Billing, Roaming, Content Provisioning, Marketing and Customer Services, Content and Aggregation which would be required In-Train.

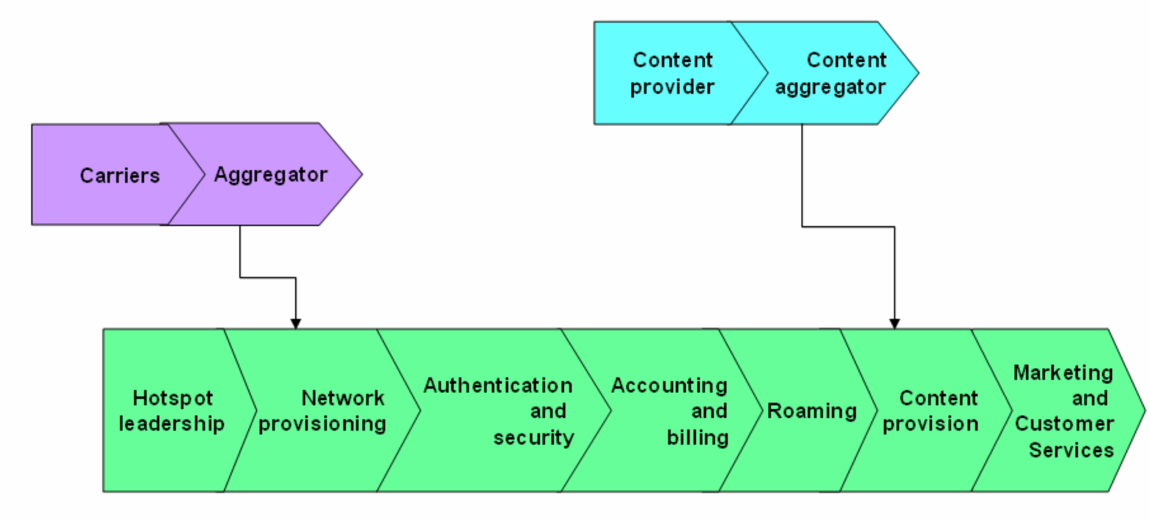


Figure 7: Value-Chain

Table 1: Value Chain Description

Activity	Functions	Critical Resources
"Hotspot" leadership	- Define hotspot strategy and negotiate with suppliers and partners	- Venue ownership - Relationships with partners
Network Provisioning	- Design, install and maintain infrastructure, - Negotiate with subcontractors and partners - Ensure access provision and interoperability with roaming agents	- Technical capabilities - Knowledge of inter-city rail activities - Relationship with venue owner
Authentication and Security	- Ensure authentication of users - Ensure security of communications - Provide integration with other networks	- Network ownership - Technical capabilities
Billing and Roaming	- Provide technical and billing interconnection with other hotspot and mobile operators - Manage data for billing purpose	- Network ownership - Technical capabilities - Ability to negotiate roaming agreements
Content provision	- Provision of content services - Aggregation of content from various sources	- Content ownership - Ability to relate content and customer expectations
Marketing and Customer Service	- Definition of offer with partners - Promotion and sales of access and services - Management of customer relationships	- Sales network - Customer ownership - Brand image

Alternate schemes of possible In-Train Layouts of Access Points and Bridges for connecting adjacent cars and providing intra and inter-coach connectivity including possible usage of CAT 5 cabling between the cars is possible.

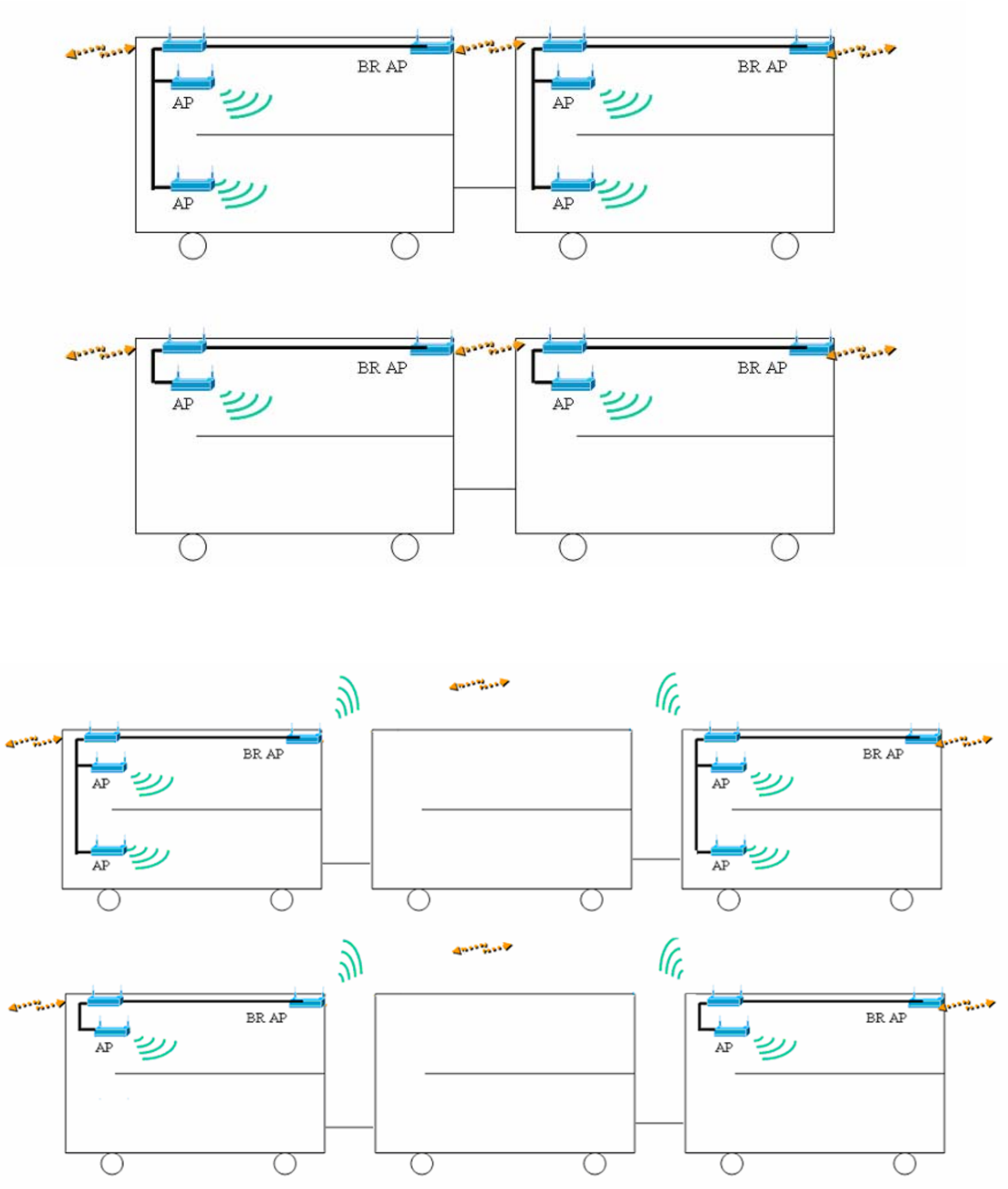
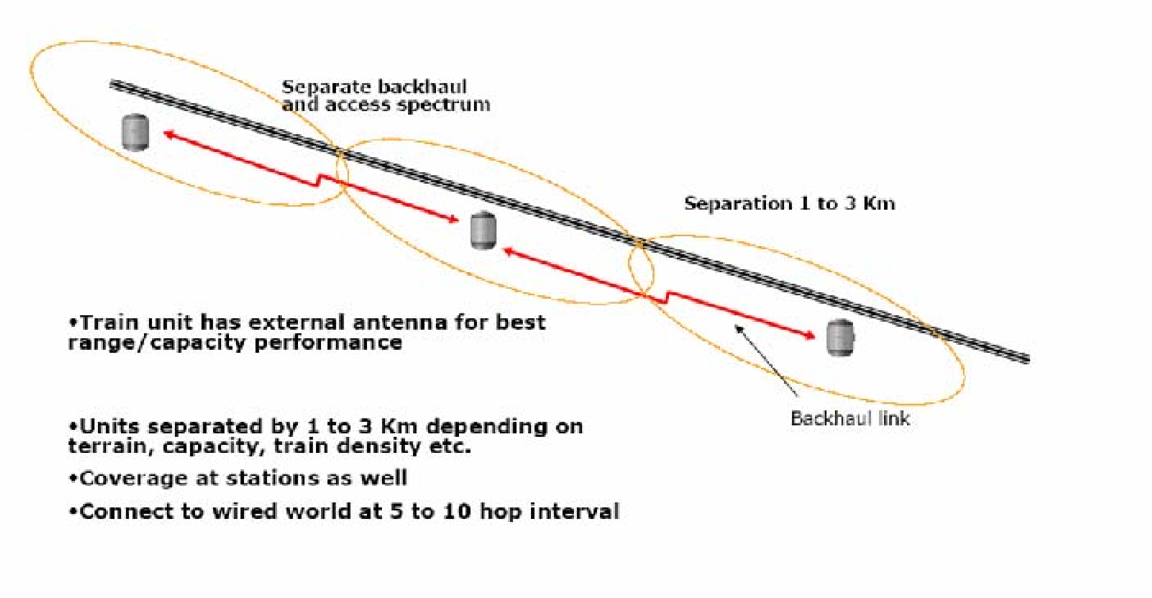


Figure 8: Examples of possible In-Train Layouts of Access Points and Bridges for connecting adjacent cars – Intra and Inter-Coach Connectivity.

3.3 Train to Back-Haul Architecture Components

3.3.1 What is the Back Haul?



- Train unit has external antenna for best range/capacity performance

- Units separated by 1 to 3 Km depending on terrain, capacity, train density etc.
- Coverage at stations as well
- Connect to wired world at 5 to 10 hop interval

Figure 9: Backhaul Components

3.3.2 Homeland Security/Monitoring Requirement

The Homeland Security/Monitoring should meet the following requirements:

- The system should allow security officers to remotely assess/verify the scene of violation by remotely controlling the security cameras to zoom in/out, change direction of the camera, and to dynamically adjust the video capture policy based on the assessment of violation scene, or to start capturing the video frames.
- The system should notify the security officers of the security violation as fast as possible with sufficient amount of information, and yet the information load can be supported by the available communication mechanism.
- System should be interoperable with Homeland Security repository database for checking/correlating suspected intruder against those images in database.
- The user interface of security officer should be friendly and effective. System should issue audible alert, configurable by security officers, along with blinking indicator of the scene. System shouldn’t require security officers to stare at surveillance monitor all the time.
- The system should enable efficient and effective integrate the alarm with the first responders and/or law enforcement.
- Captured video frame can be annotated and replayed for post-incident processing.
- The health of communication path between intrusion sensor and the system used by the security officer should be monitored and maintained.

3.4 Homeland Security/Monitoring Architecture Components

The architecture for the homeland security/Monitoring includes the following components:

- On-site subsystems to sense the security violation and alert the video surveillance system.
- On-site video surveillance systems, if alerted, to direct surveillance camera to the scene of security violation and starts capturing of the incident scenes.
- On-site processing systems to aggregate the on-site surveillance systems and intelligently communicate to the homeland security service center (see below). It can also fall back to text only message if the available bandwidth of the communication system falls below the configurable threshold.
- Communication system among security center, security surveillance system, and on-board conductor.
- Homeland security center
    - Authentication and authorization

    - Automatic incident processing and dispatching
    - Security officer command and control interface
- On-board conductor user interface
- Interface to emergency response system
- Interface to law enforcement system

3.5 Wireless Networks

Wireless technology allows laptops of commuters and workstations to be connected to the LAN without having to put in place a wiring infrastructure that connects each laptop to the network. A base transceiver that connects to only one port in the wiring infrastructure and wireless adapter cards in the workstations provide a method to rapidly connect workstations to the network.

Wireless broadband networks that use unlicensed devices for point-to-multipoint transmissions of distances of fewer than 300 feet, or for point-to-point Internet connectivity using networks that span greater distances (*e.g.*, distances that can reach a few miles) can be described as Wireless Local Area Networks (WLANs). These networks generally involve equipment manufactured in accordance with the IEEE 802.11 family of standards for unlicensed wireless devices, commonly known as "Wi-Fi" (an abbreviation for Wireless Fidelity). These networks have met with tremendous success, and increasingly have been used by Wireless Internet Service Providers (WISPs) – which may number as many as 8,000 providers – to provide a facilities-based alternative to wireline (*e.g.*, DSL) and cable services to millions of Americans over networks that may range in size from small communities, to multiple counties, to multi-regional geographic areas or even larger. Over the last several years, the number of wireless "hot spots" using Wi-Fi technologies have grown exponentially and may number as many as 150,000 by the end of 2005. In addition, several mobile service providers recently have begun using Wi-Fi hot spots to complement their licensed mobile cellular services. Significant advances are expected in the IEEE 802.11 family of standards, thus enabling further improvements in the broadband data rates, coverage, and performance.

Wireless LAN Architecture

There are two types of wireless networks: ad hoc and infrastructure networks.

Ad hoc networks are computer-to-computer network i.e. wireless stations connect to each other directly.

Infrastructure networks typically consists of wireless nodes such as laptops or personal digital assistants, connected to wireless access points. The access points (APs) in turn are connected to the distribution system (network backbone). Each mobile station must associate with an AP in order to gain access to the network. This is done with a series of exchanged frames between the station and the AP. Each network has a Service Set Identifier (SSID). Wireless devices communicating with each other must have the same SSID.

Signal strengths for the AP vary from one location to the other within the AP's coverage area. This can be due to physical obstacles such as walls, doors, etc… Moreover, an AP may become congested with traffic especially as more and more stations associate with that AP.

3.6 Emerging Technologies

The adoption of the network strategies listed above will be a dynamic process. It is already evident that newer technologies are being developed that offer advantages to future CCJPA-Caltrans wireless network design. Some examples include:

10GB Ethernet

10GB Ethernet is an extension of the IEEE 802.3 ethernet standard. It provides a high speed internal backbone for local area networks.

IEEE 802.11n

This new wireless standard is backward compatible with 802.11b/g and will provide data rates between 100Mbps and 500 Mbps.

The CCJPA-Caltrans Network will continue to evolve into a more open and serviceable platform to meet future commuter and homeland security/business requirements.

Wireless broadband networks that involve point-to-point or point-to-multipoint networks with individual network links that can provide last mile connectivity in metropolitan environments or can span distances of up to 30 miles are often referenced as Wireless Metropolitan Area Networks (WMANs). Devices deployed in these networks are manufactured in accordance with vendor-specific proprietary equipment (*e.g.,* Canopy, BreezeMAX) or with the IEEE 802.16 family of standards. The IEEE 802.16 standard, first developed in 2001 for fixed wireless systems (*e.g.*, backhaul) operating in the 11-16 GHz frequency range of licensed "upper" bands, continues to evolve. In 2003, IEEE 802.16a – commonly referred to as Wi-Max – was developed for operations in lower frequencies in the 2-11 GHz range, including licensed bands as well as bands that permit use of unlicensed wireless devices. More recently, the IEEE 802.16a standard has been extended to include 802.16d, which is also for fixed wireless broadband applications. In addition, the IEEE currently is working to finalize the 802.16e standard, a mobile wireless extension. In sum, the evolving 802.16 standard holds great promise for future developments in wireless broadband because it can be used for applications in both licensed and unlicensed spectrum, allows communications without the need for line-of-site connections, enables interoperability with different equipment using the same standard, and, in the near future, will encompass both fixed and mobile wireless applications.

Over the past sixteen months, wireless carriers have begun to deploy broadband technologies on their mobile cellular networks operating on licensed spectrum, and many have announced plans to launch or expand these technologies in the near future. Using new technologies – such as CDMA 1x EV-DO (EV-DO), Wideband CDMA (WCDMA) (also known as UMTS), UMTS/HSDPA (High Speed Downlink Packet Access), and Flash-OFDM (Orthogonal Frequency Division Multiplexing) – carriers are now, or later this year will be, providing wireless broadband services to millions of Americans at speeds ranging from 300 kbps to close to one Mbps. It is expected, for instance, that networks using EV-DO technologies will cover as many as 150 million Americans by the end of 2005.

CHAPTER 4: WIRELESS BROADBAND AND STANDARDS

4.1 Overview of Radio Spectrum

The radio spectrum is divided into different frequency bands, with each band supporting different applications.

The radio frequency spectrum chart is given below:

The FCC allocates these frequency bands:

The Very Low Frequency Band (VLF) extends from 10 to 30 KHz (power line carrier systems).

The Low Frequency Band (LF) extends from 30 to 300 KHz (power line carrier systems, air traffic control).

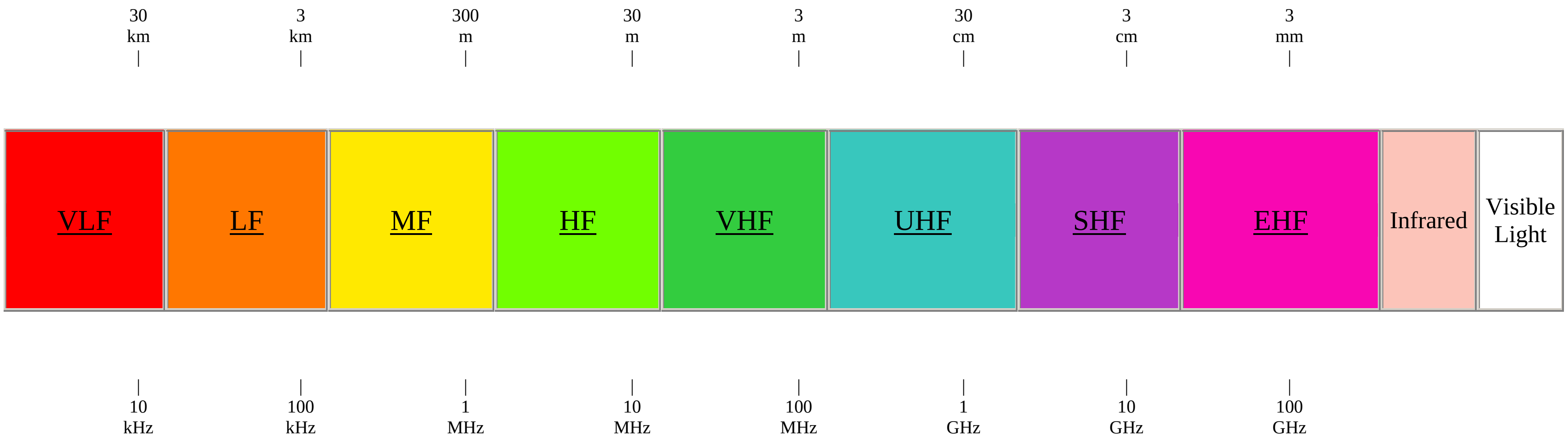
The Medium Frequency Band (MF) extends from 300 KHz to 3 MHz (AM broadcast radio, air traffic control).

The High Frequency Band (HF) extends from 3 to 30 MHz (flight test stations).
The Very High Frequency Band (VHF) extends from 30 to 328.6 MHz. (TV channels, FM Broadcast radio…)

The Ultra High Frequency Band (UHF) extends from 328.6 MHz to 2.9 GHz. (TV channels, cellular radio, microwave, ISM, wireless LAN…)

The Super High Frequency Band (SHF) extends from 2.9 to 30 GHz (ISM, microwave, wireless LAN…).

The Extremely High Frequency Band (EHF) extends from 30 GHz and above (microwave, wireless service…).



Frequency Spectrum (http://www.jneuhaus.com/fccindex/spectrum.html)

4.2 Strategy

The Wireless Broadband Access Task Force of the Federal Communications Commission, February 2005, appears to recommend and apply a pro-competitive, deregulatory framework – one that imposes the fewest regulatory barriers at both the federal and state level – to wireless broadband services to maximize innovation and consumer benefits.

With a background of FCC's deregulatory framework, the reference architecture proposes to:

- Consider classifying wireless broadband as an "information service" – consistent with FCC's determination regarding broadband services offered over cable networks and its tentative conclusion regarding broadband offered over wireline – in order to minimize potential regulatory hurdles at both the federal and state level;
- Consider examining whether wireless broadband constitutes an "interstate service" so as to minimize potential regulatory hurdles;
- Alternatively, consider applying the deregulatory principles applicable to Commercial Mobile Radio Services which lay the foundation for rapid deployment of mobile voice and data services over the past decade – to wireless broadband; and
- Similarly, consider clarifying the scope of state authority in setting terms and conditions relating to wireless broadband services to ensure that there are consistent and minimal state regulatory barriers to nationwide wireless broadband deployment.

The recommendations may also further facilitate secondary market arrangements that provide wireless broadband service providers with easy access to licensed spectrum, in places and amounts that they need, and enhance opportunities for more efficient and "dynamic" sharing of the same spectrum among different users and uses made increasingly possible by current and future technologies.

4.2.1 The WiMAX Spectrum Picture

Wireless broadband is clearly at a crossroads. Convergence is taking place between the technology road maps of WiMAX/802.16 and advanced 3GPP, 3.5G-4G cellular systems. These technologies are on a collision course and will provide similar bandwidth and significant market overlap in the coming years.

The evolution of spectrum availability and overall regulation will greatly impact the future of mobile broadband wireless networks and systems for Wi-Fi on the train.

Using results from directly surveying regulators in the fifty largest economies in the world to make an in-depth study of BWA/WiMAX spectrum and the impact that spectrum availability and services regulation will have on the success of Broadband Wireless and WiMAX, this seeks to provide the most up to date information on spectrum allocation, assignment, and licensing rules.

Fixed Broadband Wireless Spectrum

3.5GHz Band - The 3.5GHz band is the most widely available band allocated for broadband wireless access worldwide, except for the United States despite recent opening at 3650MHz. Covering 300MHz of bandwidth, from 3.3 to 3.6GHz and in some case up to 3.8GHz, this band offers great potential for fixed applications whether backhaul or last mile access.

3.5GHz remains a band allocated mostly for fixed only services in 77% of the countries surveyed. However the regulators are starting to revise their positions to allow portable services in a first step towards allowing full mobility at 3.5GHz. 13% of countries surveyed have loosened up their requirements for fixed only services at 3.5GHz. Regulators recognize that the line distinguishing BWA and 3G is blurring and may converge in the future.

4.9 GHz – Public Safety - In April 2003, in the 4.9 GHz proceeding, the Federal Communications Commission took action to ensure that spectrum suitable for wireless broadband applications was made available in support of public safety. The Commission limited eligibility in the band to those entities that would be operating in support of public safety, and then adopted innovative approaches to allow broadband technologies to develop in the band[1]. For example, instead of only assigning narrow channels to licensees, the Commission granted licensees the authority to use the entire 50 megahertz block of spectrum. This will allow manufacturers to develop, and licensees to utilize, a variety of new broadband applications employing varying bandwidths. These applications could include high-speed digital technologies and wireless local area networks for incident scene management, dispatch operations, and vehicular operations that are both temporary and permanent in nature.

[1] *See* The 4.9 GHz Band Transferred from Federal Government Use, *Second Report and Order and Further Notice of Proposed Rule Making*, 17 FCC Rcd 3955 (2002); The 4.9 GHz Band Transferred from Federal Government Use, *Memorandum Opinion and Order and Third Report and Order*, 18 FCC Rcd 9152 (2003); *see also* The 4.9 GHz Band Transferred from Federal Government Use, *Memorandum Opinion and Order*, 19 FCC Rcd 22325 (2004).

5GHz U-NII & WRC Bands - The Unlicensed National Information Infrastructure (U-NII) bands have three major frequency bands: low and mild U-NII bands (5150 - 5350) (802.11a), WRC (new) (5470 - 5725), and upper U-NII / ISM band (5725 - 5850). Wi-Fi exists in the lower and middle U-NII bands, which have demonstrated viability for BWA. Many overlapping 5GHz frequency bands earmarked for BWA growth exist around the world. The newly allocated World Radio Conference (WRC) 5470 to 5725MHz band adds significant license-exempt bandwidth. Most metropolitan deployments are in the upper U-NII 5725 to 5850 band because there is less interference there, i.e. Wi-Fi and the outdoor power allowance are in the higher 2 to 4W range as compared to only 1W in the lower and middle U-NII bands.

5.9 GHz DSRC - The newly-formed ITS band or Dedicated Short Range Communications (DSRC) systems, operate in the 5.850-5.925 GHz. There is a petition for Reconsideration by the National Public Safety Telecommunications Council (NPSTC) as per Amendment of the FCC's Rules regarding DSRC Services in the 5.850-5.925 GHz band (5.9 GHz band), *Report and Order*, 19 FCC Rcd 2458 (2004). Some examples of public safety short-range DSRC applications include: intersection collision avoidance, lane merge, work zone warnings, road condition warnings, vehicle stopped or slowing, vehicle/vehicle collision avoidance, imminent collision warning, rollover warning, and electronic toll collection.

MMDS - The Multi-channel Multipoint Distribution Service (MMDS) spectrum includes 31 channels of 6MHz spacing in the 2500 to 2690MHz range and includes the Instructional Television Fixed Service (ITFS) in the US. This spectrum has been significantly under-utilized for its original instructional TV purpose, and has been allocated for BWA service in a few countries including the United States, Brazil, Mexico and Canada.

Spectrum such as:

- License-exempt sharing of television broadcast spectrum
- 700 MHz
- 902-928 MHz (US and Canada)
- 2.40 - 2.4835 GHz
- 5.250 - 5.350 GHz (mid-UNII band)
- 5.470 - 5.725 GHz (proposed additional 255 MHz in US)
- 24 GHz
- 60 GHz
- 70-80-90 GHz

are not (yet) addressed by WiMAX's plans to focus system profiles to use OFDM modulation, operating in the 3.5 GHz licensed (non-US), 5.8 GHz license-exempt, and 2.5 GHz licensed bands, in that order.

Future Spectrum for BWA/WiMAX

Additional bands are being considered today by different regions around the world for the deployment of WiMAX and other similar broadband wireless access services. In Japan the 4.9GHz - 5.0GHz band will be used after 2007 while the 5.47GHz - 5.725GHz band is also being considered for future use. The first one will require a license for BS deployment and will support 5MHz, 10MHz and 20MHz bandwidths, while the second one will possibly not require a license and would support 20MHz bandwidths. In the US, the 700MHz is slowly being freed by broadcasters to allow BWA services and the 450MHz is seeing renewed interest for mobile WiMAX due to its great propagation characteristics

3.6 -4.2 GHz:

US will finalize allocation of 3650-3700 MHz
Some manufacturers & service providers starting to look at 3.6-4.2 GHz for 4 G
UK already has some FWA licenses in 3.6-3.8 GHz
CEPT (Europe) and France issued 3.4-3.8 GHz consultation in Q4'04
Malaysia issued 3.4-4.2 GHz consultation in 2004

Block Sizes

The situation varies form region to region and form countries within the same region. In Europe, many blocks assigned are 20/25//28MHz/ or 14MHz wide. Some countries like Norway assigned narrower blocks (2X 3.5MHz). The largest blocks we have found were in Sweden with 2X70MHz. In Asia 10.5Mhz blocks in duplex are common (China, Honk Kong). In CALA, most blocks assigned are in the 25MHz range.

We believe the trend among regulators will be "technology neutral" to provide the flexibility to operators to deploy the solutions they need.

Spectrum availability for WiMAX Mobility

Regulators recognize that the line distinguishing BWA and 3G is blurring and may converge in future. However, regulators must honor their commitment made in the 3G auctions, to not allocate spectrum for 3G mobile communication services before a determined period of time around 2006-2007. Numerous regulators have adopted from the International Telecommunication Union (ITU) definition of "pedestrian mobility speed" for 3G technologies to differentiate between the two.

To be specific, this means that wireless broadband operators may only offer fixed or pedestrian mobile services. Operators are not allowed to provide mobile services at vehicular speeds for now. This restriction will be lifted once the 3G moratorium ends.

More liberal countries where full mobility is allowed include USA (2.5GHz), Canada (3.5 and 2.5GHz), Australia, Korea (2.3GHz WiBro).

While most of Europe the band 2.5-2.69 GHz is exclusively reserved for UMTS mobile services and is therefore not available to BWA/WiMAX service providers. In other parts of the world, initiatives such as the ITU WP8F, are pushing to allow interoperability bodies between UMTS and OFDM in these mobile services.

The ITU is organized into three main sectors. Each sector is broken up into study groups that carry out the majority of the technical work. All ITU guidelines are developed according to a formal process. The study groups address particular technical "questions," which are technology areas that warrant further research. Once a topic has been sufficiently researched and a decision has been made about how to proceed, the group submits a formal "recommendation." This recommendation is then shared with all of the external ITU partners and national governments.

Two groups within the ITU specifically engage in helping to define the next generation of mobile wireless include:

Working Party 8F (WP8F) in section ITU-R
Special Study Group (SSG) "IMT 2000 and Beyond" in section ITU-T

WP8F is focused on the overall radio-system aspects of 4G, such as radio interfaces, radio-access networks (RANs), spectrum issues, service and traffic characteristics, and market estimations.

The SSG "IMT-2000 and Beyond" is primarily responsible for the network or wireline aspects of future wireless systems including wireless Internet, convergence of mobile and fixed networks, mobility management, internetworking, and interoperability.

Beyond the regulation constraints, WiMAX needs lower bands to economically deploy networks that will provide full mobility. **Higher than 3GHz bands are not suitable for mobile networks as proper coverage would require too many base stations compared to sub 1GHz bands.**

The WiMAX regulatory group is working towards influencing the regulatory bodies worldwide to open up bands for WiMAX mobility. Those bands could include the 700 MHz and 450 MHz. The regulatory working group is also working to create an environment to support eventual global roaming for nomadic & mobile WiMAX devices

4.3 Protocols

WiFi (Wireless Fidelity) is a set of product compatibility standards for wireless local area networks (WLAN). It is based on the IEEE 802.11 standards.

The Open Systems Interconnect Reference Model (OSI model) is the standard method of describing computer network communications and protocols. It is a layered model where each layer depends on the functions of the layers below it and each layer gives additional functionality to layers above it. The OSI model consists of 7 layers (from lowest to highest): Physical Layer (Layer 1), Data Link Layer (Layer 2), Network (Layer 3), Transport Layer (Layer 4), Session Layer (Layer 5), Presentation Layer (Layer 6), and Application Layer (Layer 7). Layers 4-7 describe how applications present data and how they initiate and maintain connections. Layers 1-4 describe the physical transmission media and the format of transmissions. For the scope of our project, Layers 1-3 are the most important.

Layer 1 is the Physical Layer and it describes the transmission media. On a wireless network, radio waves are the transmission medium. On a wireless card, the PHY handles transmitting packets onto the airwaves. Because the transmission medium is radio waves, all stations on the network share it; there is no way for multiple stations to transmit simultaneously. If multiple stations do try to transmit at the same time, a collision occurs and both transmissions are corrupted. For this reason, 802.11 networks employ a Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) scheme. 802.11 networks employ Collision Avoidance instead of Collision Detection because bandwidth is not plentiful enough to be wasted with collisions. CSMA/CA is implemented in the Data Link Layer.

Layer 2 is the Data Link Layer and determines when the medium is available for transmission and implements CSMA/CA. The Data Link Layer is implemented through the Media Access Controller (MAC). The MAC will only pass data to the PHY when it senses that the medium is available for transmission. It can determine availability in two ways: first, the MAC is alerted when a the PHY receives a transmission; second, stations can set a Network Allocation Vector (NAV), which is a timer that signifies how long the medium will be in use. By using these two mechanisms to control media access, the 802.11 MAC can avoid many collisions and conserve bandwidth. The MAC also determines whether a transmission received by the PHY is destined for this computer. The MAC makes this determination through a unique 48bit address (MAC Address) that is assigned to each MAC at manufacture. If the destination MAC address in the frame matches the MAC address of the MAC, the transmission is destined for this computer and it is passed up to the Network Layer; otherwise it is discarded.

Layer 3 is the Network Layer and it provides the ability to transmit varying amounts of data over multiple networks. On the Internet, the Network Layer is implemented in the Internet Protocol (IP). IP uses a 32-bit address that identifies the specific computer and the network it is on. Routers process IP datagrams and forward packets based on the network address; routers pass the packet to the next closest router to the network. The IP address is what allows computers to be accessible over the Internet; in order to maintain a connection, the IP address must remain constant.

When wireless computers roam between different networks, they normally need to receive a new IP address. This causes the computers to lose any connections they previously had. This is undesirable for our project due to the interruptions that it would cause while using Video over IP, Voice over IP, VPN, SSH, or any other connection oriented application. The solution to this is to use Mobile IP.

4.4 Strategy

The following are the basic IEEE protocol standards for wireless networking which will have an important bearing to this project:

Table 2: Important IEEE Protocol Standards for Wireless Network

802.11	**Wireless LAN (WLAN)**
802.15	**Wireless Personal Area Network (WPAN)**
802.16	**Broadband Wireless Access (BWA)**
802.18	**Radio Regulatory Technical Advisory Group**
802.19	**Coexistence Technical Advisory Group**
802.20	**Mobile Broadband Wireless Access (MBWA)**

4.4.1 Overview

IEEE 802.11b:

This standard is an amendment to the IEEE 802.11 standard.
This standard uses a Direct Sequence Spread Spectrum system. It provides the four possible data rates: 1 Mbps, 2 Mbps, 5.5Mbps, and 11 Mbps, with the latter two rates provided by 8-bit chip complementary code keying (CCK).
In reality the data rates are lower than those specified, due to the need for acknowledgements (ACK) as well as the effect of collisions, resulting in an actual throughput of 6-7 Mbps. It operates in the 2.4 GHz ISM band, in 5 MHz steps. As this band is unlicensed, it is subject to interference from other systems.
The IEEE 802.11b physical layer uses a channel bandwidth of 22MHz.

It is limited to a 100 m range in a Line of Sight (LOS) environment. This is undesirable for the sake of our project, as it would require the installation of too many bridges on the trackside.

IEEE 802.11a:

IEEE 802.11a works in the 5 to 6 GHz band, and provides data rates up to 54 Mbps. Again the actual maximum throughput is about half of that value, due to MAC protocol overhead and other transmission issues. It is more affected by physical obstructions than 802.11b; however the 5 GHz band is less used than the 2.4 GHz band leading to less interference. Also the operating range of 802.11a is shorter than that of 802.11b. IEEE 802.11a uses OFDM.

The 5-GHz frequency band isn't as crowded as the 2.4-GHz frequency because it offers significantly more radio channels than the 802.11b and is used by fewer applications. It has a shorter range than 802.11g, is actually newer than 802.11b and isn't compatible with 802.11b.

IEEE 802.11e:

Recently ratified by the IEEE (?? Check date??), the 802.11e quality-of-service specification is designed to guarantee the quality of voice and video traffic. It will be particularly important for companies interested in using Wi-Fi phones.

IEEE 802.11g:

IEEE 802.11g works in the same frequency range as 802.11b, but provides data rates up to 54 Mbps, with an actual throughput of about 25 Mbps. It also uses OFDM.

IEEE 802.11i:

Also sometimes called Wi-Fi Protected Access 2 (WPA 2), 802.11i was ratified in June 2004. WPA 2 supports the 128-bit -and-above Advanced Encryption Standard, along with 802.1x authentication and key management features.

IEEE 802.11k:

Predicted for ratification in mid-2006, the 802.11k Radio Resource Management standard will provide measurement information for access points and switches to make wireless LANs run more efficiently. It may, for example, better distribute traffic loads across access points or allow dynamic adjustments of transmission power to minimize interference.

IEEE 802.11n:

This standard is yet to be ratified, but promises actual throughputs in the 100 Mbps range and a 10 fold increase in the operating ranges. This is accomplished with the use of multi antenna systems.

IEEE 802.11r:

Expected to be ratified in mid to late 2006, the 802.11r Fast Roaming standard will address maintaining connectivity as a user moves from one access point to another. This is especially important in applications that need low latency and high quality-of-service standards such as voice-over-WLAN.

IEEE 802.11s:

This standard will deal with mesh networking. It is predicted to be ratified in mid-2008.

WiMAX and IEEE 802.16:

WiMAX or Worldwide Interoperability for Microwave Access is a certification mark for products that conform to the 802.16 standard. It is faster than WiFi, and covers larger distances. WiMAX certified products will extend wireless access to metropolitan area networks (MAN). WiMAX products are designed to be compatible and interoperable with WiFi products.

This standard promises data rates of 72 Mbps in OFDM based systems. Products based on 802.16 can support distances of up to 50 Km and can operate in Obstructed Line of Sight (OLOS) and Non Line of Sight (NLOS) paths. The physical layer has 3 variants: single carrier, 256 carrier OFDM and 2048 carrier OFDM. IEEE 802.16 supports Time Division Duplex (TDD) and Frequency Division Duplex (FDD) and provides adaptive modulation which selects the highest data rate consistent with the lowest error rate.

It also provides high scalability, allowing it to support much more users than 802.11.

IEEE 802.16 operates in the 10-66 GHz band, while IEEE 802.16a specifies operation in the 2-11 GHz band.

MIMO

Multiple-Input Multiple-Output refers to using multiple antennas in a WiFi device to improve performance and throughput. The MIMO technology takes advantage of a characteristic called multi-path, which occurs when a radio transmission starts out at point A and then reflects off or passes through surfaces or objects before arriving, via multiple paths, at point B. MIMO technology uses multiple antennas to collect and organize signals arriving via these paths. The technology is expected to be used in the 802.11n standard.

RFID

Radio frequency identification uses low-powered radio transmitters to read data stored in a transponder (tag) at distances ranging from one inch to 100 feet. RFID tags are used to track assets, manage inventory and authorize payments, and they increasingly serve as electronic keys for everything from autos to secure facilities.

4.4.2 Radio Transmission Techniques

Spread Spectrum:

In Spread Spectrum (SS) systems, an information signal is sent using a much larger bandwidth than the minimum required bandwidth necessary to send the information. SS uses wide band, noise-like signals, making the sent information harder to detect, intercept, demodulate, and jam.

A function independent of the data being sent is used to determine the bandwidth of the transmitted information. At the receiver, the received signal is correlated with this same function or spreading signal, to recover the original data. The most widely used forms of SS are Direct Sequence (DSSS) and Frequency Hopping (FHSS).

DSSS:

Basic Operation of DSSS:

At the transmitter, a pseudo-noise sequence, pn_t, is generated at a chip rate R_c. This sequence is multiplied by the binary data input, d_t having a symbol rate R_s, causing the baseband bandwidth R_s to be spread to a baseband bandwidth R_c. The resulting signal is modulated using M-PSK, and transmitted over the channel.

At the receiver, the received signal is multiplied by a pseudo-noise sequence pn_r. If pn_r is identical to pn_t, the received signal is de-spread, yielding the original data input having bandwidth R_s.

If pn_r is not identical to pn_t, no de-spreading occurs, and the transmitted data can not be recovered.

Note that we can have a short code or a long code system. A short code system uses a pseudo-noise sequence of code length equal to a data symbol, while a long code system uses a sequence of code length much larger than a data symbol.

Resistance to interference:

Suppose the transmitted signal is subjected to some form of interference i, along the channel. At the receiver, i will be multiplied by the pseudo-noise sequence pn_r, causing it to be spread, thus increasing its bandwidth and decreasing its power spectral density. By applying the multiplied signal to a low pass filter, most of the interference component (which is now wideband) is filtered out.

Applications of DSSS:

A DSSS system is specified in the IEEE 802.11b standard. Using 8-bit Complementary Code Keying (CCK) as the modulation scheme allows the higher data rates 5.5 Mbps and 11Mbps. 1 and 2 Mbps use an 11-chip Barker code.

As DSSS signals are relatively wideband, if access points are set up in proximity to each other, channel overlap may occur, causing reduced performance. As such it is typical to use only 3 access points and thus 3 networks in close proximity as to avoid channel overlap. Usually channels 1 (centered at 2.412 GHz), 6 (2.437 GHz) and 11 (2.462 GHz) are used in the US, thus allowing frequency separations of about 25 MHz.

FHSS:

In FHSS, a pseudo-noise sequence pn_t is used to pseudo-randomly shift the carrier frequency to be used in the M-ary FSK modulation, at a hopping rate R_h. This causes the transmitted FSK signal to occupy a number of frequencies in time, with each frequency being occupied for a duration of $T_h = 1/R_h$, referred to as the dwell time.

In general DSSS provides slightly higher data rates and shorter delays than FHSS, as well as being more resistant to noise.

OFDM:

Orthogonal Frequency Division Multiplexing is a multi-carrier transmission technique, which uses multiple frequencies to simultaneously transmit multiple signals in parallel. The frequencies are chosen to be orthogonal to each other, allowing the spectra of sub-channels to overlap while not interfering with each other, thus providing spectral efficiency. This high spectral efficiency, along with OFDM’s resistance to multi-path, has led to its use in both WiMAX and WiFi. An OFDM signal can be demodulated with the use of Fast Fourier Transform (FFT) chips which are commercially available. Phase Shift Keying (PSK) or Quadrature Amplitude Modulation (QAM) can be used to increase the data throughput.

Adaptive Modulation:

Modulation is the process by which a carrier wave carries an analog or digital message signal across a channel. Three basic modulation schemes exist: phase, frequency, and amplitude shift keying. They extend from binary schemes to M-level modulation schemes (higher throughputs and spectral efficiencies). However, in order to use higher order modulation schemes, a higher SNR (and thus transmission power) is needed to overcome interference and bit error rates (BER).

This is where adaptive modulation comes into play. With adaptive modulation, the transmitter gathers information about the channel conditions and accordingly chooses which modulation scheme to use. This information can be gathered at the receiver and fed back to the transmitter. As the range increases (and thus interference increases), lower order modulation schemes are used. This provides the system with higher average throughputs while increasing the coverage distance.

4.5 Infrastructure

4.5.1 Strategy

The infrastructure consists of the following sub-systems:

- In-Train infrastructure
- Train-to-trackside infrastructure
- Trackside infrastructure
- Security surveillance system
- Data aggregation switch
- Trackside – switch communication system
- Homeland security service center
- Mobile Internet service center
- Infrastructure management center

4.5.2 Trackside Infrastructure for Intelligent Grade Crossings

Grade Crossings

Highway-railroad grade crossings are intersections where a highway crosses a railroad at-grade. They are also called level crossings in other countries such as Canada, Australia, and the United Kingdom.

To avoid collisions, traffic control devices are required at grade crossings just like intersecting roads need stop signs or traffic signals. Traffic control devices used to avoid collisions include warning signs, crossbucks (the familiar x-shaped signs), pavement markings, and, in some locations, bells, gates and flashing lights as described in the Manual of Uniform Traffic Control Devices (MUTCD).

Grade crossings may be public or private. Public grade crossings are where the roadway is under the jurisdiction of and maintained by a public authority. Private grade crossings are where the roadway is privately owned, such as on a farm or industrial area, and is intended for use by the owner or by the owner's licensees and invitees. A private crossing is not intended for public use and is not maintained by a public highway authority. In 2001, there were 154,084 public crossings and 98,430 private crossings.

Collisions between highway vehicles and trains have been, until recently, the greatest source of injuries and fatalities in the railroad industry. In the past several years, the number of trespassers killed and injured along the railroad's right-of-way has exceeded those killed and injured at the grade crossings. The Federal Railroad Administration's Office of Safety develops detailed statistics on the railroad industry's safety.

This section provides an overview of the research and development, policy, and Next Generation Program information on grade crossings available within the Federal Railroad Administration and links to the FRA Office of Safety. Some work has been done on grade crossing safety and research in other Federal and State government agencies, universities, the rail industry, and non-profit groups like Operation Lifesaver.

Intelligent Grade Crossings

ITS is the application of new communications, computer, and sensor technologies to highways and transit systems and the careful integration of system functions to provide more efficient and effective solutions to multimodal transportation problems. The goal of ITS is provide a seamless, multimodal, and nationwide transportation system. Development of a National Architecture, which is the framework that addresses all ITS user services, and defines the subsystems and data flows (i.e., information that must be shared between subsystems) required to make ITS work, has been the first step in achieving this vision. In particular, the technologies and operations needed for a transportation system that will satisfy the requirements of the 31 user services are defined in the architecture. Two user services deal directly with grade crossings: #30, Highway-Rail Intersections, and #31, Archived Data.

Highway-Rail Intersection (HRI) User Service #30 - The ITS Architecture provides for the integration of the railroad operating systems with the traffic management systems and was developed through a consensus process involving the AAR, ASLRRA, AASHTO, States, ITS America, FHWA, and FRA. The result is a system that would have the capability for getting advance warning of approaching trains through interconnected information systems that link the motorist to the traffic management and rail operations systems. It also allows for the capability of warning the locomotive engineer of obstacles or trapped vehicles at grade crossings, and potentially for trespassers along the right-of-way.

As the next step in the ITS Program, FRA and the ITS Joint Program Office have worked with Standards Development Organizations, including the Institute of Transportation Engineers, the Institute of Electrical and Electronic Engineers, AREMA, AASHTO, and others, to develop the standards necessary for implementing ITS at grade crossings nationwide. These standards will be the basis for projects that will tie grade crossing warning systems to local traffic management systems and will include communication to the PTC systems now being developed to increase safety for both motor vehicle users and rail passengers and crewmembers. These standards will also be turned into regulations by FHWA for the purpose of funding decisions. No Federal funds would go the HRI projects that do not meet the standards.

Archived Data User Service (ADUS) #31 - Real-time data from traffic and transit operations can be archived and used for purposes other than in ITS control strategies. By archiving the detailed data collected, more accurate analyses for planning, research, performance monitoring, and policy purposes can be conducted at much lower costs. ADUS was the latest User Service to be adopted into the National ITS Architecture in September 1999.

Standards development is underway for ADUS, and it will provide guidance in system design and promote the integration of ITS with traditional information systems and ensure consistent deployments of archives within regions as well as throughout the nation. To implement ADUS, a Strategic Plan for ADUS Standards was one of the first specific activities identified. Many of the other activities in the ADUS Program Plan will feed the standards efforts as more is learned from research and case studies. Standards will expedite national level analyses that rely on comparing conditions across the country in a consistent manner as well as allow historical comparisons and trend monitoring since data definitions will remain stable over time. They also will allow comparison of operations among various regions.

Intelligent Grade Crossings are those locations where ITS for roadways come together with Intelligent Railroad Systems, and in particular, Positive Train Control (PTC) systems. PTC systems, unlike traditional railroad signal systems, provide continuous information on train location and speed. FRA, working with the ITS Joint Program Office, intends to sponsor Intelligent Grade Crossing projects on railroad corridors in Michigan, Illinois, and Alaska where FRA-sponsored communication-based PTC systems are being implemented and demonstrated. Coordination will take place with the State highway departments so that these grade crossing projects are integrated with other projects that are underway. For example, warning to motor vehicles of oncoming trains, as well as advice on alternate routes to avoid blocked crossings, would be transmitted through the standardized ITS dedicated short-range communications system and displayed on standardized in-vehicle information displays and roadside variable-message signs.

Intelligent Railroad Systems

A theme cutting across virtually all the RD&D program elements is the use of sensors, computers, and digital communications to collect, process, and disseminate information to improve the safety, security, and operational effectiveness of railroads. Intelligent Transportation Systems (ITS) for highways and mass transit are based on these technologies, as are the new air traffic control and maritime vessel tracking systems. Military services, major parcel delivery companies, pipeline operators, and police, fire, and ambulance services also use these technologies. The Federal Railroad Administration and the railroad industry are working on the development of Intelligent Railroad Systems that would incorporate the new sensor, computer, and digital communications technologies into train control, braking systems, grade crossings, and defect detection, and into planning and scheduling systems as well.

The new Intelligent Railroad Systems are key to making railroad operations-freight, intercity passenger, and commuter-safer and more secure, reducing delays, reducing costs, raising effective capacity, improving customer satisfaction, improving energy utilization, reducing emissions, and becoming more economically viable. The systems can be implemented as independent systems, in which case their benefits will be limited, or they can be implemented as integrated systems, in which case the benefits will be compounded. FRA, through its Research, Development and Demonstration program elements, is encouraging the railroad industry to adopt the integrated approach when implementing these systems.

Positive Train Control Overview

FRA is supporting national deployments of advanced signal and train control technology to improve the safety, security, and efficiency of freight, intercity passenger, and commuter rail service through regulatory reform, technology development, infrastructure implementation, and financial assistance. Positive Train Control (PTC) refers to technology that is capable of preventing train collisions, over speed derailments, and casualties or injuries to roadway workers (e.g., maintenance-of-way workers, bridge workers, signal maintainers) operating within their limits of authority. Positive Train Control systems vary widely in complexity and sophistication based on the level of automation they implement and the degree of control they are capable of assuming. While PTC systems can be designed to independently operate, most of the developments focus in enhancing a previously existing method of rail operations. This technology has the potential capability to limit the consequences of events such as hijackings and runaways that are of special concern in an era of heightened security.

4.6 Issues

Range of Connectivity

The reach of public networks continues to be limited by the relatively short range of 802.11 in general, though the new 802.11g specification combines the speed of 802.11a and the range of 802.11b.

RF and Sporadic Connectivity

Sporadic connectivity because of weak RF signals requires creation of mobilized solutions which could provide at least the following features:

- locally caching data from back-end systems
- providing asynchronous messaging
- allowing session persistence through connection and disconnection cycles.

Small cell sizes

The small cell sizes of Wi-Fi LANs present many challenges to Rail, Road and Air travel environments where users cover large areas. Issues arise, for example, when multiple disconnected users need updates from each other.

Costs of Satellite Connectivity

While Wireless WAN technologies such as satellite connectivity and GPRS have been available, they have not been adopted by service providers as mainstream offerings, and their cost has made them unpopular among end-users; thus, their use has been limited.

Quality of Service

The lack of Quality of Service (QoS) features in existing 802.11 standards also has a negative impact on delay-sensitive applications such as streaming media and voice.

Low-Latency Vs Error-free Transmission

This describes the issue where a tradeoff on low-latency delay can be made with Error-free transmission of data. On one side are applications which need low-latency operation where errors can be tolerated (e.g., for VoIP or streaming video) while on the other end of the spectrum of applications are those which need error-free transmission where higher latency can be tolerated (e.g., for database synchronization). These can be typically depicted in our environment by Video Surveillance Applications Vs e-Ticketing Applications.

4.7 Security

4.7.1 Strategy

The architecture should support the following security requirements:

- Data integrity
- Data privacy
- Audit trail of the homeland security related events
- Access control to the homeland security related capabilities
- Access control to mobile Internet service is managed by service provider
- Provide robust wireless security services that closely parallel the security available in a wired LAN.

Wireless Security Suite

The network must be secure with a scalable and manageable system featuring a well-built Wireless Security Suite, an enterprise-ready, standards-based, WLAN security solution which gives network administrators confidence that their data will remain private and secure.

The solution must provide the following benefits:

- Support Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2) providing access control via per-user, per-session mutual authentication and data privacy via strong dynamic encryption.
- Only legitimate clients be allowed to associate with legitimate and authorized network RADIUS servers via authorized access points.
- Stronger encryption to be provided by WPA with Temporal Key Integrity Protocol (TKIP) enhancements such as message integrity check (MIC), per-packet keys via initialization vector hashing, and broadcast key rotation and by WPA2 with Advanced Encryption Standard (AES) encryption enhancements to help ensure that data will remain private and secure.
- A variety of IEEE 802.1X extensible authentication protocol (EAP) types be supported, Cisco LEAP, Protected EAP-Generic Token Card (PEAP-GTC), PEAP-Microsoft Challenge Authentication Protocol Version 2 (PEAP-MSCHAPv2), EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled TLS (EAP-TTLS), EAP-Subscriber Identity Module (EAP-SIM), and EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
- Support LEAP for mutual authentication and both TKIP and WPA TKIP algorithms.
- A wide selection of RADIUS servers, such as the Cisco Secure Access Control Server (ACS), can be used for enterprise-class centralized user management. RADIUS accounting records for all authentication attempts are supported

4.7.2 In-Train

Key policies relevant for In-train wireless network and the service vendors are comprised of the following:

- ✓ include strong authentication and encryption for network access;
- ✓ mitigate denial of service and other disruptive attacks;
- ✓ implement capabilities to assess the risks and vulnerabilities associated with 802.11 networks and devices;
- ✓ develop defensive actions necessary to detect, deter, and defeat unauthorized 802.11 activity;
- ✓ include intrusion detection methodologies for the 802.11 wireless systems;
- ✓ share 802.11 security knowledge - such as historical forensics - to improve overall security processes

Advanced security and networking services for Secure In-Train Rail Environment and Enterprise Network,

The proposed system for providing a secure Rail Environment and Enterprise Network should provide robust user and application policy enforcement, multi-vector attack protection, and secure connectivity services through a wide range of rich security and networking services, including:

- Advanced Application-Aware Firewall Services
- Voice-Over-IP and Multimedia Security
- Robust Site-to-Site and Remote Access IPSec VPN Connectivity
- Intelligent Networking
- Flexible Management Solutions

FIREWALL SERVICES for BUSINESS PROTECTION AND APPLICATION CONTROL

Application Layer Security

The proposed system should integrate a broad range of advanced firewall services to protect rail operations and allied operations, operators and businesses from the constant barrage of threats on the Internet in the wireless rail network environment.

The proposed system should provide rich firewall services, tracking the state of all network communications and preventing unauthorized network access.

Building upon those services, the proposed system should deliver strong application layer security through intelligent, application-aware inspection engines that examine network flows at Layers 4-7.

To defend networks from application layer attacks and to give businesses more control over applications and protocols used in their environment, these inspection engines should incorporate extensive application and protocol knowledge and employ security enforcement technologies that include protocol anomaly detection, application and protocol state tracking, Network Address Translation (NAT) services, and attack detection and mitigation techniques such as application/protocol command filtering, content verification, and URL de-obfuscation.

The proposed system inspection engines should also give businesses control over instant messaging, peer-to-peer file sharing, and tunneling applications, enabling businesses to enforce usage policies and protect network bandwidth for legitimate business applications.

Multi-Vector Attack Protection

The proposed system should incorporate multi-vector attack protection services to further defend businesses from many popular forms of attacks, including denial-of-service (DoS) attacks, fragmented attacks, replay attacks, and malformed packet attacks. Using a wealth of advanced attack protection features, including TCP stream reassembly, traffic normalization, DNSGuard, FloodGuard, FragGuard, MailGuard, IPVerify, and TCP intercept, the proposed system should identify and stop a wide range of attacks, and provide real-time alerts to rail security administrators.

Flexible Access Control and Flow-Based Policies

Rail Security Administrators may want to create custom security policies using flexible access control technologies which must be provided by the proposed system, including network and service object groups, user and group-based policies, and predefined applications and protocols. A Modular Policy Framework may be provided in the proposed system so that rail security administrators are able to easily define granular flow-based and class map-based policies, which can apply a set of customizable security services, such as Inspection Engine policies, Quality of Service (QoS) policies, connection timers, and more, to each administrator-specified traffic flow/class. By combining these flexible access control and per-flow/class security services, stateful inspection and application-aware firewall services, and the multi-vector attack protection services that the proposed system should deliver, businesses can enforce comprehensive security policies to protect themselves from attack.

VOIP SECURITY SERVICES and NEXT-GENERATION CONVERGED NETWORKS

The proposed system should provide protection for a wide range of voice-over-IP (VoIP) and other multimedia standards. This would allow businesses to securely take advantage of the many benefits that converged data, voice, and video networks provide, including improved productivity, lower operational costs, and increased competitive advantage. By combining VPN and Quality of Service (QoS) with the advanced protocol inspection services that the proposed system should provide for these converged networking standards, businesses would be able to securely extend voice and multimedia services and the benefits they deliver to remote offices, home offices, and mobile users.

ROBUST IPSEC VPN SERVICES and MOBILE USERS

The proposed system should provide full-featured VPN capabilities so that businesses can securely connect networks and mobile users worldwide across low-cost Internet connections. Solutions supported may range from standards-based site-to-site VPN using the Internet Key Exchange (IKE) and IP Security (IPSec) VPN standards, to newer innovative easy VPN remote access capabilities. The VPN must deliver a uniquely scalable, cost-effective, and easy-to-manage remote-access VPN architecture that eliminates the operational costs associated with maintaining the remote-device configurations that are typically required by traditional VPN solutions, and provide feature-rich remote access VPN services, including enforcing VPN client security posture requirements and performing automated software updates of VPN Clients, to deliver secure, easy-to-manage remote access to corporate networks. proposed system should encrypt data using 56-bit Data Encryption Standard (DES), 168-bit Triple DES (3DES), or up to 256-bit Advanced Encryption Standard (AES) encryption.

The proposed system should use either an Active/Standby failover design or a more advanced Active/Active failover design, which supports complex network environments that require asymmetric routing support.

Failover pairs continuously synchronize their connection state and device configuration data, thus providing an easy-to-manage high availability solution. Synchronization can optionally take place over a high-speed LAN connection, providing another layer of protection by enabling businesses to geographically separate the failover pair. In the event of a system or network failure, network sessions are automatically transitioned between appliances, with complete transparency to users.

INTELLIGENT NETWORKING SERVICES to ENABLE SIMPLIFIED DEPLOYMENT AND SEAMLESS wireless NETWORK INTEGRATION

The proposed system should deliver a wide-range of intelligent networking services for seamless integration into today's diverse network environments as follows:

- Provide Open Shortest Path First (OSPF) dynamic routing services to detect network outages and route around them.
- Mission-critical real-time enterprise applications, collaborative computing applications, and streaming multimedia services need to be securely delivered using the comprehensive PIM-Sparse Mode v2 and Bidirectional-PIM routing support
- Advanced IPv6 security services for securing deployments of next-generation IPv6 networks for businesses
- Simultaneously securing existing IPv4 environments with the same appliance during the transition period towards an IPv6 infrastructure

DoD Mandate for Security Directive
Issues – Wireless Infrastructure and Radio Engineering

The Department of Defense (DoD) Directive Number 8100.2 defines the security policies for the use of commercial wireless technologies in the DoD Global Information Grid (GIG). It is intended to protect the DoD computers and networks from the security vulnerabilities created by wireless networks and devices. The Directive calls for highly secure wireless networks and makes 802.11 intrusion detection methodologies a requirement for compliance.

What is the Scope of the DoD Directive?

The Directive applies to securing all commercial wireless devices, services or technologies, whether data or voice for non-classified information. The DoD directive explicitly prohibits wireless devices for transmission, storage or processing of classified information. However, areas covered by this no-wireless policy must still have an enforcement system in place.

Example of commercial wireless devices includes wireless enabled computers, PDAs, mobile phones and handheld scanners. Because commercial 802.11 wireless systems are increasingly deployed everywhere especially where infrastructure security is becoming highly important, much of the Directive is applicable to 802.11 technologies. The Directive is a policy intended to protect infrastructure from various vulnerabilities of wireless systems. But a policy is useless if it isn't monitored and enforced.

Summary of DoD Wireless Directive Compliance Requirements

The advantages of Wi-Fi on Train are high, but they come with a price. WLANs are inherently vulnerable to malicious attacks, due to the uncontrolled nature of the wireless medium and to the complexities with securing wireless LAN devices, networks, and configurations. Wireless signals spill out uncontrollably beyond physical walls and can leave a back door open to the rest of the network. A single mis-configured access point or laptop – or a single rogue access point – creates a potentially enormous security hole for hackers to walk right though making commercial Wi-Fi networks a common hacking target.

In light of this challenging network medium, a well designed security policy like the DoD Wireless Directive could be useful or even essential. But the Directive will only be as effective as the ability to monitor for vulnerabilities and attacks, accurately and instantly.

Table 3: Directive Requirements

Directive Requirement **For 802.11 Networks and Devices**	**Directive Sections**
Authentication and Encryption - use and verification measurements at both device and network level for strong authentication and FIPS 140-2 encryption.	4.1.1 4.1.2
RF Monitoring - actively screen for wireless devices, monitor for use in unauthorized areas or when connected directly to wired network.	4.3 4.5 4.7
Vulnerability Assessment - detect and assess the risks and vulnerabilities associated with wireless technologies.	5.2.3.1
RF Intrusion Detection - monitor for external attacks and accidental interference from friendly sources.	4.1.4 5.6.5.2
Network Management and Support - detect interference to aid in resolution.	5.1.7.3
Knowledge Reporting - sharing wireless expertise between agencies; develop and distribute threat mitigation information.	4.10
Cost-Effectiveness - ensure strategies and potential architectures that minimize costs of wireless systems.	5.1.4

Issue for Security is to possibly incorporate continuous RF-based monitoring, distributed across the entire area where such sensitive applications may be running in effect and it has to be cost-effective.

How should the service vendors participating in CCJPA RFQ comply to the Security Directive?

Authentication and Encryption
Look for automatic notification of policy violation to key security configurations, such as the authentication and encryption used by access points, VPN gateways, and client devices. For hackers to get through, it takes just one device to be mis-configured or altered. Define signature rules that report policy violations in real-time on a per access point or device basis.

RF Monitoring
Utilize some kind of distributed RF-based sensor technology to auto-discover all the 802.11 assets end-to-end. More than showing the APs connected to the network, the system should identify all active 802.11 devices using the airwaves and display their status in real-time, including traffic patterns. Particularly important if there are

eTicketing Hardware devices utilizing wireless for which unauthorized access is prohibited, The service vendor will need to immediately detect unauthorized devices and help to disable them before a hacker can exploit them.

Vulnerability Assessment
Provide proactive vulnerability assessment of 802.11 networks and devices. The vendor must identify mis-configurations, mis-implementations, and policy violations and also provide superior audit capabilities over handheld scanners to monitor 24x7 across the entire geography. Vulnerabilities may be summarized in both real-time displays and historical reports.

RF Intrusion Detection
Provide a sophisticated 802.11 intrusion detection system, capable of detecting wireless specific denial of service attacks, mapping operational measurements to determine whether the interference is accidental or malicious. The vendor may also scan for all types of suspicious activities, identifying active attacks and reconnaissance activities in progress.

Network Management and Support
Network management monitors Wi-Fi performance, enabling network operations to maximize network performance and reliability. The vendor may report of noise and interference from neighboring wireless networks, in-car and terrestrial, channel overlap, congested access points, network utilization, and station throughput. These tools are essential for isolating interference anomalies, whether it is from friendly sources or outside attacks.

Knowledge Reporting
Information Reports may be archived in a database for trend reporting, such as planning and forensic analysis, which may easily integrate with leading enterprise reporting applications.

Cost-Effectiveness
Vendor should avoid any cost-prohibitive deployment and provide methods of cost reduction and performance.

In summary, the proposed Service Vendors may need to automate the monitoring and compliance of the Secure Wireless Directive by providing:

1. Continuous, distributed RF-based views of wireless LAN security threats.
2. Real-time, second-by-second, 802.11 intrusion detection and protection (IDS/IPS).
3. Policy defining, monitoring, and enforcement
4. Detailed usage tracking and forensic analysis of attacks.
5. Purpose-built RF sensors for advanced diagnostics and operational support.
6. Easy integration with reporting tools for Directive adherence reports.
7. High scalability, over multiple locations and broad geographies.
8. Best overall value, with system costs about half of competitive alternatives.

CCJPA In-Train Wi-Fi Trials - What to Watch Out For
Wireless Network Vulnerabilities

Left unprotected, wireless LANs (WLANs) make easy targets for malicious intruders on the train - those seeking access to search, steal, or destroy. Some simply want a free ride on the Internet, but others want to take data or vandalize the network. It is important to keep the vital networked assets protected from airborne attacks. The first step is to implement ***"best practices"*** for safe-guarding the WLAN and CCJPA Service Trial Wi-Fi Network.

It is also needed to monitor and identify potential WLAN weaknesses that leave the system open to intrusion. Even if a WLAN is not, it would still be needed to monitor for unauthorized, rogue wireless use.

The following list describes the key WLAN vulnerabilities that must be guarded against:

Ad hoc networks - An ad-hoc network is created when two devices (such as laptop PCs) equipped with WLAN cards establish a direct peer-to-peer connection. They don't require the use of an access point (AP) and they don't require authentication. Therefore, it's easy for the hacker to get onto an ad-hoc network and compromise the other stations. An Ad hoc network can easily be created by the passengers in the rail car amongst themselves, if they so desire.

Accidental associations - Without taking steps, people in an adjacent rail car or even a trackside building can unintentionally link with the network. Such accidental associations develop when a strong 802.11 signal leaks beyond the closed doors and windows of the train. Neighboring users who use laptops can automatically and unknowingly connect with the network. It also works the other way around.

Rogue APs – Some people might want to bring their own AP to the train and benefit from the convenience of wireless. The trouble is, this kind of casual AP deployment provides another easy target for hackers, even with moderate security turned on. Though these people aren't aware they've created a security risk, others know better. Train Riders who intentionally deploy unauthorized APs can easily hide them from wired-side detection by simply duplicating the Medium Access Control (MAC) address of the station originally connected.

Rogue clients (bridges) - Wi-Fi devices in the form of audio bugs, video cameras, or Trojan Horses enable hackers to steal proprietary information and assets from the enterprise. These readily available devices can be small and unassuming, some even taking the form-factor of a power brick. Without radio frequency (RF)-based monitoring, detection is extremely difficult due to the fact that they may not be directly connected to the provider network.

Insecure network configuration - Without proper equipment configuration, the vendor's WLAN could be at serious risk. Inappropriate settings such as default passwords, open Service Set Identifiers (SSIDs) broadcasts, weak or no encryption, and lack of authentication leave the WiFi service in the train open to attack. Even after parameters have been altered to beef up security, commuters can accidentally change them to an insecure state or a power loss can reset them.

Weak encryption - No encryption method is foolproof. Hackers can easily crack the Wired Equivalency Protocol (WEP). Even enterprise-class security mechanisms that leverage authentication standards are vulnerable. Moreover, recent studies by the Institute of Electrical and Electronics Engineers (IEEE) show that even the latest authentication standards can be broken.

Fast Secure Roaming (Access-Point Role) - Fast Secure Roaming allows authenticated client devices to roam in-train securely from one car to another or one access point to another without any perceptible delay during re-association.

4.7.3 Back-Haul to Train

Security Directive
As the Wi-Fi capability is incorporated within the Capital Corridor Inter-City AMTRAK trains between Sacramento/Auburn and San Jose/Oakland and becomes available to commuters on commercial service terms, security becomes a prime concern for CCJPA.

Wireless networks and devices are inherently more vulnerable to hacker attacks than their wired counterparts. This is particularly true for 802.11 networks. Wireless LAN signals could extend out of one rail car or a railway station or even a trackside building with wireless Internet as the train slowly passes by and can't be controlled. Hackers, sometimes sitting in the next rail car or sometimes hundreds of feet away, can get access. Wireless LANs are also shared, meaning any device on the network can watch the communications of other devices on the network. Finally, the popularity of 802.11 networks has resulted in a plethora of sophisticated attack tools that can automate the steps to break the encryption and authentication used in most wireless networks. These tools are readily available on Internet and can be used by practically anyone.

4.7.4 Homeland Security/Monitoring

The infrastructure should support the following security related applications:

- Protection of critical transportation infrastructures
- Collision prevention of pedestrians or disabled vehicles at crossing intersection
- Enable security officers, transit operator and conductor to improve security mandate

4.7.5 Back-Haul to Train - FCC and DHS Collaboration

Federal Communication Commission (FCC) and Department of Homeland Security (DHS) collaboration.

The FCC's relationship with DHS also holds promise for increasing the deployment of wireless broadband technology in support of public safety missions around the country. The Commission heeded the public safety community's need for spectrum suitable for broadband applications when it adopted rules dedicating 50 megahertz of spectrum in the 4.9 GHz range in support of public safety services[2]. This broadband spectrum may be used for a diverse range of public safety services, but may be especially valuable for establishing WLANs at the scene of major incidents. There are a range of other applications, such as video transmission. In adopting the rules for the 4.9 GHz band, the Commission chose operating parameters that closely matched those of commercial and consumer equipment in nearby bands. In so doing, the Commission afforded the public safety community the benefits of economies of scale because equipment used in great quantity in these nearby bands is readily adaptable to the 4.9 GHz spectrum environment. The Homeland Security implications of the 4.9 GHz rules are significant because entities engaged in Homeland Security efforts will be able to integrate their operations with public safety by simply inserting a low-cost 4.9 GHz PCI card into a laptop computer and signing on to the LAN that has been established at the incident scene. We also note that there is no technical reason why 4.9 GHz technology need be limited to a specific incident scene and that, given the low-cost of the technology, there is no reason why public safety hot spots could not be established throughout a metropolitan area. Moreover, the 4.9 GHz rules have created a broadband "pipe" sufficiently flexible to accommodate Homeland Security applications that have not even yet appeared on the drawing board.

The FCC, through its participation as a partner with DHS in Project SAFECOM, has been able to craft rules in the 4.9 GHz band and other bands that address public safety needs that are also attuned to the evolving needs of Homeland Security. The Commission

[2] 4.9 GHz proceeding discussed in FCC WBA Task Force Report Section V.A, above.

participates in SAFECOM to "provide an effective forum for informed, innovative and on-going exchanges aimed at ensuring steady progress towards achievement of nationwide interoperability capability"[3] and effective public safety communications. Staff of the Wireless Telecommunications Bureau meets regularly with DHS representatives and participates in SAFECOM's Executive Board Committee meetings. The Task Force recommends that the Commission continue to take advantage of its relationship with DHS to bring Homeland Security issues to the forefront in the activities of such organizations as the National Public Safety Telecommunications Council and the Public Safety Regional Committees that the Commission has established to promote, among other things, interoperability in the 800 MHz band and the 700 MHz Public Safety band.

Emergency Management Needs Via Satellite Network

For Homeland Security needs, to set up an Emergency Management Information System (EMIS) at the Network Management Center for the Capitol Corridor, would require Satellite Connectivity as a backbone for communications backup in the event of a disaster. Through the Satellite Communications Network, the Capitol Corridor could rely on the EMIS network to connect to critical resources from medical, police, sheriff, fire and City Hall agencies in an emergency.

Designated operators could communicate through the satellite network when the Office of Emergency Management activates the system, in an emergency, for two-way communications with a dedicated hub server at the Network Management Center.

This would help to create a secure, emergency response intranet across the Capitol Corridor or across the entire State. A mirror site should be provided to serve as a backup hub for the network.

Even though the primary network could still be trackside infrastructure-based and terrestrial, with Wi-Max standards, the network operators for emergency management may need to us a satellite network when they have a dire need.

All the attributes of satellite communication make it a natural fit for emergency operations. Disasters often cut or create gaps in terrestrial service, but, by virtue of its wireless nature and wide area coverage, satellite networks are immune to interruptions on the ground.

[3] *See* John B. Muleta Testimony before the U.S House Government Reform Committee on National Security, Emerging Threats, and International Relations Subcommittee; First Responder Interoperability: Look Who's Talking Now (July 20, 2004).

4.7.6 Homeland Security/Monitoring Architecture Components and National ITS Architecture

Homeland Security Needs for Capitol Corridor Inter-City Rail of California may be evaluated in the context of the National and State ITS Architectures, which provide a framework at the national and state levels with the objective of protecting the rail transportation information and infrastructure. The focus of the security update to the National ITS Architecture is the security services or mechanisms that meet this high-level objective.

Security is represented in the National ITS Architecture in two ways:

1. **Securing ITS**: ITS is an information system in its own right that must be protected so that ITS applications are reliable and available when they are needed. This aspect of security applies to all the subsystems and architecture flows in the National ITS Architecture. "Securing ITS" is shown as the foundation since the ITS systems must be secure before ITS can reliably be used to improve the security of the surface transportation system.

2. **ITS Security Areas**: ITS can be used to enhance the security of the surface transportation system. Eight security areas define the ways that ITS can be used to detect, respond to, and recover from threats against the surface transportation system. These eight ITS security areas are shown at the top of the figure below, supported by the "Securing ITS" security services that make ITS secure. Specific subsystems, architecture flows, market packages, and supporting physical and logical architecture definitions have been defined for each ITS security area.

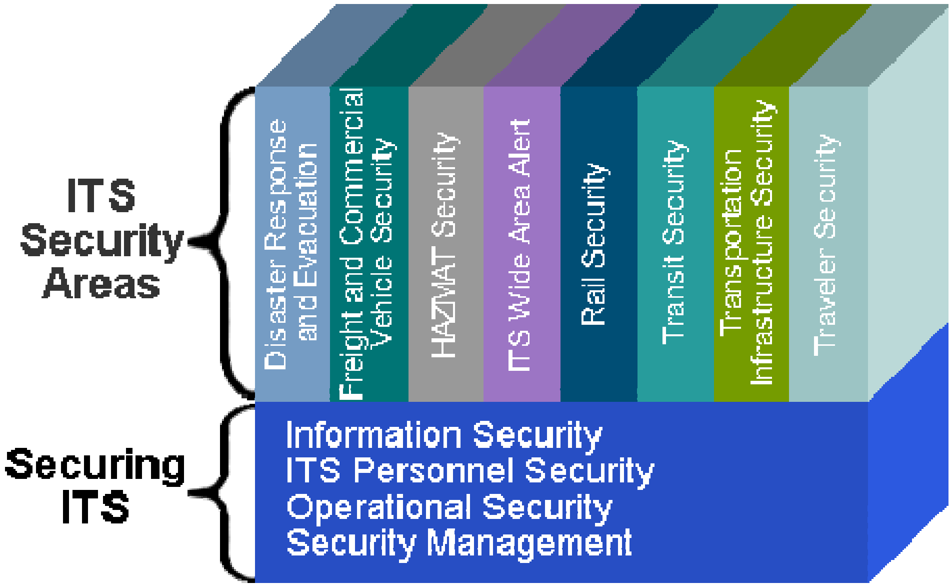


Figure 11: ITS Security Areas

Consider a transit surveillance system that includes CCTV cameras and a control center to illustrate these two views of security. From one perspective, we need to make sure that the cameras can only be controlled by the control center, that they can't easily be taken off-line, and that any sensitive images that may be collected are protected from unauthorized disclosure. These are all considerations associated with securing the transit surveillance system and are addressed as part of "Securing ITS". From another perspective, the transit surveillance system is an ITS system that provides both a deterrent and a response tool that improves the security of the transportation system. This view of the transit surveillance system is defined in one of the eight security areas ("Transit Security").

Securing ITS

ITS systems are subject to security threats like any other information technology system. This is true not only for systems that process personal or financial information (i.e., electronic toll collection systems), but also for many other types of ITS systems. Dynamic message signs are subject to tampering and unauthorized use, traffic signal control systems must operate flawlessly and fail in a safe manner when errors do occur, and many ITS operations centers may be called upon to play an important role in disaster response and recovery. ITS systems can only contribute to a disaster response if the ITS systems are robust and secure enough to operate reliably in crisis situations. Note from these examples that security is not only concerned with preventing unauthorized disclosure of sensitive information. Comprehensive security also addresses a broad range of threats that can disrupt or alter system operation.

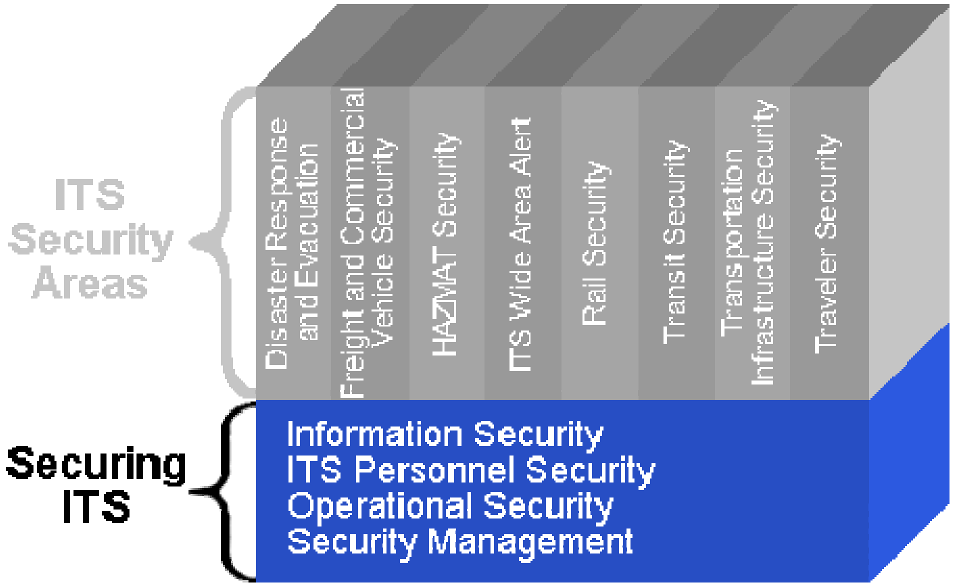


Figure 12: Securing ITS

Security Services

Security services are typical security mechanisms or countermeasures that provide for different aspects of security. Security services are driven by the security objectives and threats expected to adversely impact a system or communication between systems.

Information Security

Information Security deals with securing the origin, transmittal and destination of the information itself.

- Confidentiality - The system should prevent unauthorized disclosure of information deemed sensitive.
- Integrity - The system should ensure that information is protected from unauthorized intentional or unintentional modifications.
- Availability - The system should protect critical ITS services in order to prevent degradation or denial of the ITS services to users of the services. Single points of failure should be avoided.
- Accountability - The system should provide protection against a sender of an information transmission later denying that they sent the information. The system should provide protection against a receiver of an information transmission later denying that they received the information. This concept is known as Non-Repudiation or Accountability.
- Authentication - The system should verify the identity of a user and/or other system prior to granting access to a requested resource.
- Auditing - The system should have the capability to trace ITS subsystem and individual user actions and activities. The auditing function of the system places the actions and activities in an audit trail that is protected from unauthorized access and modification.
- Access Control - The system should limit access to the resources of a subsystem to only those users and other subsystems that are properly authorized. After authenticating an entity, the system should have the capability to limit system access to information or resources based on that entity’s access privileges. The system should limit software modifications and upgrades to users and other systems that have authorization.

Operational Security

Operational Security is responsible for protecting ITS assets against both physical and environmental threats. This area provides monitoring, access control, configuration control and security incident and materials management of critical ITS assets.

- Physical and Environmental Protection - The system should protect against adverse environmental conditions (e.g., temperature extremes, moisture and humidity, wind, dust). The system should provide capabilities to minimize the affects of power disruptions and surges. The system should protect against telecommunications failures. The system should provide capabilities like fire prevention, detection, and suppression.
- Physical Access Control - The system should prevent unauthorized physical access to critical ITS facilities, field equipment, and other ITS assets. The system should log all attempts to physically access ITS facilities, field equipment, and other assets. The system should notify operations staff when a breach of physical access is attempted.
- Security Monitoring - Critical ITS facilities, field equipment, and other ITS assets should be monitored. Manual and automated alarms should be provided.
- Security Incident Management - Security incidents should be actively managed via identification, operations, and recovery. The incident should be reviewed and analyzed to determine how to improve security to prevent future occurrences. Procedures should be deployed that manage these incidents, including the review and analysis processes. These procedures should be continually improved and updated to mitigate future occurrences of the same type of incident. This could include defining different types of security incidents, and the procedures in place for preventing future occurrences of each – these procedures may be different depending on the type of incident.
- Contingency Planning - Operational continuity and disaster recovery plans should be prepared and periodically tested and revised to ensure the integrity and continuity of operations and minimize the impact to the system from a disaster. The system should implement a comprehensive strategy for backup and restoration.
- System Maintenance - Only authorized software, hardware, and devices should be installed or used. System changes should be documented, authorized, and tested prior to deployment. Change management procedures should be used.
- Sensitive Materials Management - Sensitive information should be securely stored, protected, and properly disposed of.

Personnel Security
Personnel Security is responsible for ensuring that ITS personnel do not inadvertently or maliciously cause harm to ITS assets and have proper training in the event there is a security-related incident.

- Personnel Screening - ITS Personnel with access to sensitive information or in security-critical positions should be subject to pre-employment screening, including background checks when appropriate per the security policy in effect. ITS Personnel in these sensitive positions should be subject to periodic reinvestigation.
- Supervisory Controls - Supervisory practices should be followed that ensure that ITS Personnel roles and responsibilities are properly exercised.
- Awareness and Training - All critical ITS Personnel should be trained on relevant security policies, practices, and guidelines.
- Separation of Duties - Duties should be identified such that one person acting alone cannot compromise the security of critical ITS services. Job rotation should be used for sensitive ITS positions.
- Least Privilege - ITS Personnel should be granted the level of access needed to fulfill their role and no more.
- Accountability - ITS Personnel should understand their responsibility and be accountable for their actions. Audit trails and logs should be reviewed to detect improper access.
- Termination - The system should prevent unauthorized access by transferred or terminated employees.

Security Management
Manage Security provides the underpinnings for Information Security, Operational Security and ITS Personnel Security. The system is governed by and enforces the system security policy. A system security policy specifies the security procedures, roles and responsibilities, system configuration (both between subsystems and between subsystems and terminators), operational security needs, ITS personnel security and ITS asset security. Risks are identified and assessed to determine necessary safeguards. Critical data and assets should be identified.

- Security Management - The security management service connects all of the other security services together in order to provide security controls throughout ITS. Security Management ties in with the Information, Operational, and Personnel security aspects of securing ITS as well as the eight security areas. The security management service includes user and system assignment of appropriate access control, password management and a host of other security mechanisms. Security Management is often implemented by a combination of manual and automated controls. Security Management includes the definition, implementation, and enforcement of the following: security policies and procedures, roles and responsibilities, and system configuration. System configuration management provides the means for ensuring all aspects of the ITS deployment are configured to provide an effective, efficient, and secure operating environment. Interfaces between architecture entities should be designed and implemented such that each security-related specific interface has minimal and closely controlled functionality in providing system access.

Security Objectives

Security Objectives help form the basis for evaluating appropriate security services and levels of service that satisfy the security objectives. The security objectives have classifications of High, Medium, Low, and Minimal.

Availability
The availability objective ensures that systems and information are accessible and usable to authorized individuals and/or processes.

Confidentiality
The confidentiality security objective ensures information is not disclosed to unauthorized individuals, processes, or systems (e.g., protecting trucking company records). The objective of confidentiality is to prevent unauthorized disclosure of information deemed sensitive. This objective defines the level of restriction to sensitive information that is transmitted or stored within a system.

Integrity
The integrity security objective ensures the accuracy and reliability of information and systems. This objective defines the level that information is protected from unauthorized intentional or unintentional modifications. This objective is related to auditing accountability, authentication, and access control services for sensitive information.

Security Threats

Security Threats, along with Security Objectives, also provide the basis for evaluating appropriate security services. The security threats have classifications of High, Medium, Low, and Minimal.

Deception
A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.

Disclosure
A circumstance or event whereby an entity gains access to data for which the entity is not authorized.

Disruption
A circumstance or event that interrupts or prevents the correct operation of system services and functions.

Usurpation
A circumstance or event that results in control of system services or functions by an unauthorized entity.

Securing Architecture Flows

The focus of the ITS Standards program is for systems to be able to seamlessly exchange information. Protecting system interfaces is critical to securing ITS. The interfaces, or architecture flows, as defined in the National ITS Architecture have been analyzed to ascertain applicable security services importance. In order to keep the security considerations for architecture flows manageable, architecture flow groupings were created for architecture flows that share similar security objectives, threats and security services

Architecture flows have been placed into one of fifteen groups that are based on unique security considerations. In cases where an architecture flow could be allocated to multiple groups, the most appropriate security group was chosen. Each architecture flow group has been given typical security service, security objectives and security threat classifications of high, medium, low or minimal. Similar architecture flows are grouped together so that security services can be consistently applied. The security service classifications are based on the security objective and threat importance. For example, the combination of a high level of integrity (i.e., unauthorized modification of the information) and a high level for the threat of deception would necessitate, among other services, a high or great need for the Access Control security service.

The information content of the architecture flow coupled with its operational role was considered in the security service classifications. In some cases, the security service, objective or threat is not applicable and thus will not be in the corresponding table. The security service considerations are typical, it is incumbent on the user to tailor the security considerations as appropriate to the ITS application (e.g., sensitive archive data might require a higher classification than the nominal "Low" designation identified in the National ITS Architecture).

ITS Security Areas

The term "Security Area" represents area of ITS which can be used to enhance surface transportation security. The National ITS Architecture provides entities (subsystems and terminators), functions, and interfaces that cover aspects of eight ITS security areas in the figure below. For each ITS security area, this section discusses the scope of the area along with its architecture representation including appropriate market packages.

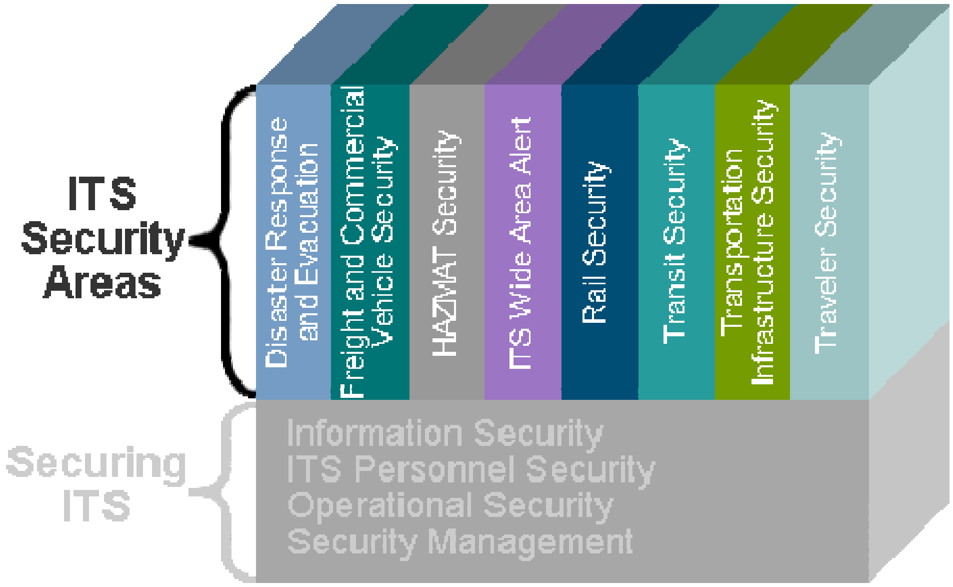


Figure 13: ITS Security Areas

Disaster Response and Evacuation

The Disaster Response and Evacuation (DRE) Security Area uses intelligent transportation systems to enhance the ability of the surface transportation system to respond to and recover from natural disasters, terrorist acts, and other catastrophic events. DRE improves access to the scene for response personnel and resources, provides better information about the transportation system in the vicinity of the disaster, supports resource coordination and sharing of current situation information, and provides more efficient, safer evacuation for the general public if needed.

All types of disasters are considered including natural disasters (hurricanes, earthquakes, floods, winter storms, tsunamis, etc.) and technological and man-made disasters (hazardous materials incidents, nuclear power plant accidents, and national security emergencies such as terrorism, nuclear, chemical, biological, and radiological weapons attacks terrorist acts.). Broad inter-agency coordination is critical in all disaster scenarios, with transportation professionals performing well-defined roles in the larger context of the multi-agency response to the disaster. DRE defines how ITS can be used to coordinate and integrate DRE activities within diverse organizations in order to improve the safety of the responders and the public at large, and improve the performance and effectiveness of the transportation system as a part of the overall disaster response.

In the physical architecture, DRE centers on the Emergency Management Subsystem, which represent the interface to local, county, state, and federal public safety, emergency management, and other allied response agencies. In DRE, this subsystem represents both the Emergency Operations Centers and the Incident Command Systems that are established when disaster strikes. DRE focuses on the interfaces between this subsystem and the subsystems that represent the transportation operators and information providers (Traffic Management Subsystem, Transit Management Subsystem, Information Service Provider, Maintenance and Construction Management, Rail Operations, etc.). DRE builds on existing Incident Management capabilities.

The Disaster Response and Evacuation security area centers on the Emergency Management subsystem and is best characterized in the National ITS Architecture by four market packages: Early Warning System (EM07), Disaster Response and Recovery (EM08), Evacuation and Reentry Management (EM09), and Disaster Traveler Information (EM10).

Freight and Commercial Vehicle Security

The area of freight and commercial vehicle security considers the awareness aspect of security through the surveillance of either commercial vehicles or freight equipment. Freight equipment includes containers (with or without chassis), the chassis, or trailers. In addition, the interface with inter-modal facilities is another aspect of this area. There are four major functions included as part of this security area.

The first functional area is tracking commercial vehicle or freight equipment locations to determine if an asset has deviated from its planned route. The carrier's operation center (FMS, Fleet and Freight Management Subsystem) would be responsible for monitoring the route. In addition, the commercial vehicle's on-board system can correlate its current location to the planned route and notify the operation center of a route deviation. If a route deviation exceeds the established limits, the operation center would be responsible for formulating a response plan, which could include notifying public safety agencies.

The second functional area is to monitor the identities of the driver, commercial vehicle and freight equipment for consistency with the planned assignment. The carrier's operation center (FMS) determines if an unauthorized change has occurred and is responsible for implementing a response plan, which could include notifying public safety agencies. In support of a seamless inter-modal system, assignment information is exchanged with inter-modal facilities and shippers.

The third functional area is to monitor freight equipment for a breach or tamper event. A breach or tamper event includes the nature of event, time, location, freight equipment identity, monitoring device status and environmental threat sensor readings (chemical, biological, etc.).

The fourth functional area is to monitor the commercial vehicle for a breach or tamper event. A breach or tamper event, in this instance, includes the nature of event, time, location, commercial vehicle identity, driver identity and monitoring device status.

The Freight and Commercial Vehicle Security area is largely comprised of four market packages. The Fleet Administration (CVO01) market package includes the capability to identify commercial vehicle route deviations. The location of the Commercial Vehicle can be monitored by the Fleet and Freight Management subsystem and route deviations exceeding the established limit are flagged. The Fleet and Freight Management subsystem is responsible for formulating a response plan, which could include notifying public safety agencies.

The Freight Administration (CVO02) market package includes the capability to identify route deviations, and breach and tamper events of freight equipment. The Fleet and Freight Management subsystem monitors the route by obtaining location information directly from the freight equipment or via the commercial vehicle. The Fleet and Freight Management subsystem monitors shipments to make sure that no tampering or breach of security occurs to the freight equipment. For security related incidents, the Fleet and Freight Management subsystem is responsible for formulating a response plan, which could include notifying public safety agencies.

The On-board CVO and Freight Safety & Security (CVO08) market package includes the capability for the Fleet and Freight Management subsystem to detect and respond to commercial vehicle breach and tamper events. In addition, both commercial vehicle and freight equipment breach or tamper events are made available to the Commercial Vehicle Check subsystem.

The Freight Assignment Tracking (CVO13) market package provides for the planning and tracking of three aspects of commercial vehicle shipments. For each shipment, the commercial vehicle, the freight equipment, and the commercial vehicle driver, are monitored for consistency with the planned assignment. The Fleet and Freight Management subsystem determines any unauthorized changes, and is responsible for formulating a response plan which could include notifying public safety agencies.

HAZMAT Security

The HAZMAT Security area’s purpose is to reduce the likelihood of a successful hijacking of security sensitive HAZMAT cargo and its subsequent use as a weapon.

The first major function is tracking security sensitive HAZMAT cargo carrying commercial vehicles and report unexpected and significant deviations or operations on restricted roadways to police. In order to protect business confidential operational information, the operational tracking and the determination of a significant route deviation requiring notification of public safety is done by a commercial carrier's operations center (FMS).

The second major function is detection of security sensitive HAZMAT cargoes on commercial vehicles by remote sensing and imaging from the roadside. By also reading electronic tag information (carrier ID, vehicle ID and driver ID) from a sensed commercial vehicle, any detected security sensitive hazmat can be correlated with existing credentials, to determine if the cargo being carried is a permitted operation. If not, the vehicle can be asked to pull-in, and public safety may be notified.

The third major function is authentication of drivers and notification to public safety if an unexpected driver attempts to operate a vehicle carrying security sensitive HAZMAT. As with tracking security sensitive HAZMAT cargo, the commercial fleet management center acts to validate and verify any discrepancies prior to notification of public safety.

The HAZMAT Security area is largely represented by four market packages. The Fleet Administration (CVO01) market package includes the capability to track commercial vehicles by a Fleet and Freight Management center. If the Fleet Management Center notices a significant discrepancy, it may notify police.

The CV Administrative Processes (CVO04) market package includes the distribution of usable and non-usable local and national HAZMAT routes with associated administrative restrictions by time and for specific classes of HAZMAT cargoes. This map information is distributed by public agencies to Information Service Providers, Fleet and Freight Management functions and map update providers.

The Roadside HAZMAT Security Detection and Mitigation (CVO11) market package is used to detect HAZMAT cargoes at the roadside, and correlate the detected operations with existing credentials to determine if a detected HAZMAT cargo is a permitted activity. If a non-permitted activity is detected, the Commercial Vehicle Check station may notify police.

The CV Driver Security Authentication (CVO12) market package authenticates a commercial vehicle driver based on information downloaded to the vehicle from the Fleet Management Center. If an unauthenticated driver is detected, a vehicle may be safely disabled by the Fleet Management Center, and the Fleet Management Center may notify police.

ITS Wide Area Alert

The ITS Wide Area Alert security area notifies the traveling public in emergency situations such as child abductions, severe weather watches and warnings, natural and human-caused disasters, military operations, and civil emergencies where lives and/or property are at stake. It utilizes ITS driver and traveler information technologies to immediately provide information and instructions to the traveling public, improving public safety and enlisting the public's help in some scenarios. The ITS technologies supplement and support other emergency and homeland security alert systems such as the Emergency Alert System (EAS).

When an emergency situation is reported and verified and the terms and conditions for system activation are satisfied, a designated agency broadcasts emergency information to traffic agencies, transit agencies, information service providers, the media, and other ITS systems that have driver or traveler information capabilities. The ITS systems, in turn, provide the alert information to the traveling public using ITS technologies such as Variable Message Signs, Highway Advisory Radios, in-vehicle displays, transit displays, 511 traveler information systems, and traveler information web sites. The service providers for this security area include the emergency management, homeland security, military and public safety agencies that issue the Wide Area Alert, the traffic, transit, and traveler information organizations that convey the information to the traveling public, and the traveling public itself.

In the physical architecture, the Emergency Management Subsystem represents the agency/system that broadcasts the emergency information to the ITS systems. This subsystem provides the alert information to the Traffic Management Subsystem, Transit Management Subsystem, Information Service Provider, Maintenance and Construction Management Subsystem, and Toll Administration Subsystem, which in turn provide the alert information to system operators and the traveling public.

The ITS Wide Area Alert security area centers around the Emergency Management subsystem and is best characterized in the National ITS Architecture by the Wide Area Alert (EM06) market package. The Wide Area Alert market package uses ITS driver and traveler information systems to alert the public in emergency situations such as child abductions, severe weather events, civil emergencies, and other situations that pose a threat to life and property. The alert includes information and instructions for transportation system operators and the traveling public, improving public safety and enlisting the public's help in some scenarios. The ITS technologies will supplement and support other emergency and homeland security alert systems such as the Emergency Alert System (EAS).

When an emergency situation is reported and verified and the terms and conditions for system activation are satisfied, a designated agency broadcasts emergency information to traffic agencies, transit agencies, information service providers, toll operators, and others that operate ITS systems. The ITS systems, in turn, provide the alert information to transportation system operators and the traveling public using ITS technologies such as dynamic message signs, highway advisory radios, in-vehicle displays, transit displays, 511 traveler information systems, and traveler information web sites.

Rail Security

The general area of Rail Security includes ITS functionality to monitor and secure trains, rail cars, fixed assets (track, wayside equipment and highway-rail intersections) and personnel. Rail Security focuses on freight rail (security aspects of passenger rail are covered under transit security). The current version of the National ITS Architecture addresses a subset of the overall area of rail security, specifically interfaces between rail entities and highway entities. These are the interfaces relating to highway rail intersections (HRI) and the interfaces from rail operations to traffic and emergency management functions of the architecture.

The primary security function associated with HRI is surveillance of the intersection, which is performed in the architecture by the Roadway subsystem. The market package that provides this function is ATMS14, Advanced Railroad Grade Crossing.

The interface between rail operations and the traffic management functions is expressed in the architecture as the interface between the Rail Operations terminator and the Traffic Management Subsystem and contains incident and advisory information. It is included in market packages ATMS13 (Standard Railroad Grade Crossing), ATMS14 (Advanced Railroad Grade Crossing), and ATMS15 (Railroad Operations Coordination).

The interface between rail operations and the emergency management function is expressed in the architecture as the interface between the Rail Operations terminator and the Emergency Management Subsystem. The market packages that address this interface are ATMS08 (Traffic Incident Management System), for normal incidents; EM08 (Disaster Response and Recovery), for disaster response; and EM09 (Evacuation and Reentry Management), for coordination during evacuations.

Transit Security

The area of transit security addresses passenger, facility, and asset security for passenger rail and bus transit systems. The area addresses surveillance and sensor monitoring of transit stations, stops, facilities, infrastructure, and vehicles. The surveillance includes both video and audio surveillance. The sensor monitoring includes threat sensors (e.g. chemical agent, toxic industrial chemical, biological, explosives, thermal, acoustic and radiological sensors), object detection sensors, motion or intrusion detection sensors, and infrastructure integrity sensors.

Transit-related systems also include analysis of sensor or surveillance outputs for possible threats and automatic notification of appropriate transit or public safety personnel to potential threats. The Transit Security area supports traveler or transit vehicle operator initiated alarms that are monitored by central dispatch or the local police. This area also includes a security management and control capability that not only provides detection, identification and notification of threats or incidents, but also allows the transit agency to take response measures such as remote vehicle disabling. In addition, this area also provides access control to transit vehicles, requiring positive operator identification before transit vehicles can be operated.

Another aspect of the Transit Security area of the National ITS Architecture is to provide emergency information to travelers using the transit system by visual (signs) or audio messages on-board the transit vehicle, at transit stops, or in transit facilities. Finally, the transit security area will interface with appropriate security agencies (e.g., the Transit Information Security Analysis Center) to assist in analysis of threats and to report threats.

The Transit Security area's key market package is Transit Security (APTS5). This market package includes six key interfaces. The first key interface is between the Transit Vehicle Subsystem and the Transit Management Subsystem for traveler or vehicle operator initiated alarms, vehicle disabling, and vehicle operator authentication.

The second key interface is between the Transit Vehicle Subsystem and Emergency Management Subsystem (representing either a public safety agency or the public safety aspects of a transit agency e.g., transit police) for traveler or vehicle operator initiated alarms, surveillance, and sensor monitoring.

The third key interface is between the Remote Traveler Support Subsystem (representing devices in public transit areas such as transit stations) and Emergency Management Subsystem for traveler initiated alarms, surveillance, and sensor monitoring.

The fourth key interface is between the Security Monitoring Subsystem (representing devices in non-public transit areas such as transit yards) and Emergency Management Subsystem for surveillance and sensor monitoring.

The fifth key interface is between the Transit Management Subsystem and Emergency Management Subsystem for sharing emergency information and coordinating incident response.

The sixth key interface is between the Emergency Management Subsystem (representing either a public safety agency or the public safety aspects of a transit agency e.g., transit police and the Alert and Advisory Systems terminator for sharing of threat information or threat data for analysis.

Transportation Infrastructure Security

Transportation infrastructure can be monitored and protected by a broad array of ITS technologies. Transportation infrastructure security includes the monitoring of transportation infrastructure (e.g., bridges, tunnels and management centers) for potential threats using sensors and surveillance equipment. Threats to infrastructure can result from acts of nature (e.g., hurricanes, earthquakes), terrorist attacks or other incidents causing damage to the infrastructure (e.g., stray barge hitting a bridge support). Barrier and safeguard systems are used to preclude an incident, control access during and after an incident or mitigate impact of an incident.

The Emergency Management Subsystem monitors the transportation infrastructure. Information on threats is shared primarily with the Other EM, TMS, and MCMS subsystems but can also be shared with other subsystems. The Traffic Management Subsystem controls the barrier and safeguard equipment although Emergency Management can request deployment. The security of transportation infrastructure is covered primarily in the Transportation Infrastructure Protection (EM05) market package.

Traveler Security

The Traveler Security area is responsible for increasing the safety and security of travelers in public areas including public transit facilities, bridges, tunnels, parking facilities and (major) intersections and other roadway features.

There are four key market packages that represent the Traveler Security area. The Transit Security (APTS5) market package provides for traveler security through surveillance and sensor monitoring to warn of hazardous situations as well as allowing travelers to report emergencies.

The Transportation Infrastructure Protection (EM05) market package includes the monitoring of transportation infrastructure (e.g., bridges, tunnels and management centers) for potential threats using sensors and surveillance equipment.

The Wide-Area Alert (EM06) market package uses ITS driver and traveler information systems to alert the public in emergency situations that pose a threat to life and property.

Finally, the Disaster Traveler Information (EM10) market package uses ITS to provide disaster-related traveler information to the general public, including evacuation and reentry information and other information (possibly responsive to specific traveler requests) concerning the operation of the transportation system during a disaster.

4.8 Applications Required To Be Supported

4.8.1 Homeland Security

Location-based information is crucial to homeland security. Rail operations supervisors at all levels of Caltrans Transportation Infrastructure Security and CCJPA must effectively collect analyze and share integrated data captured thru the wireless network systems along with spatial information which can be extended to managing and reducing the consequences of all forms of rail emergencies.

.

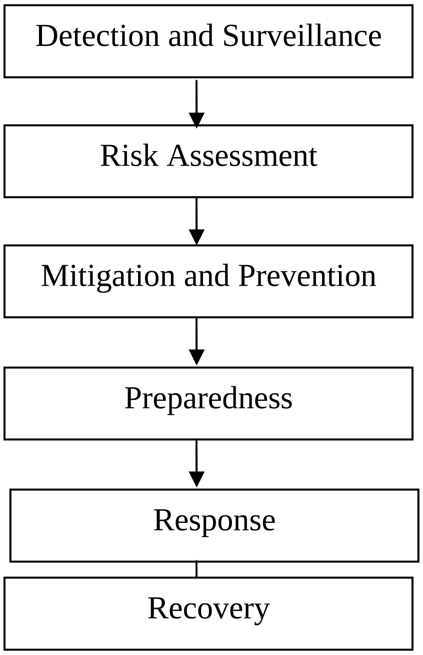


Figure 14: Security Flowchart

Proposed Application Framework

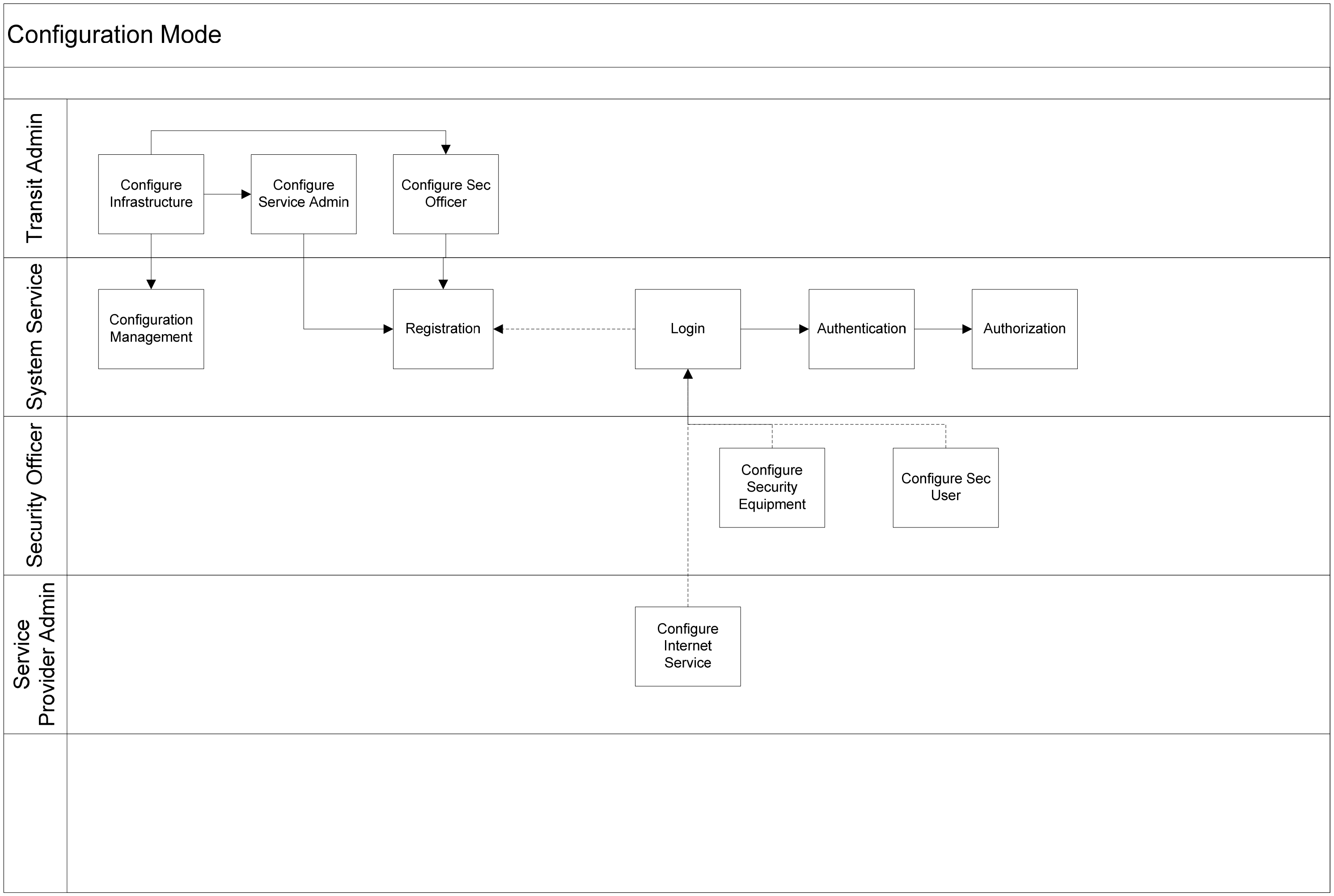


Figure 15: Proposed Application Framework

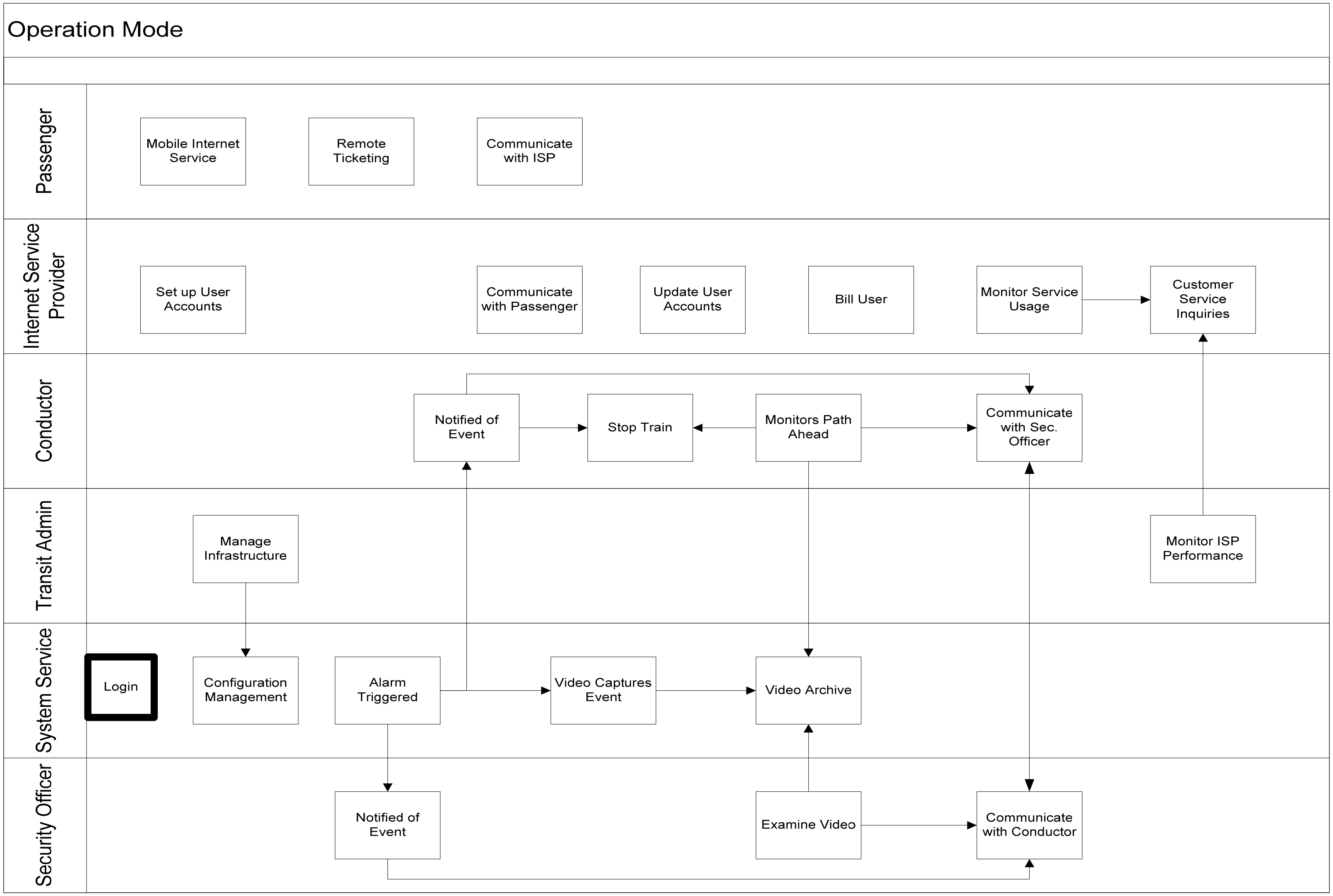


Figure 15: Continued

CHAPTER 5: BANDWIDTH REQUIREMENTS

5.1 Strategy

The Bandwidth requirements are identified below for Commercial Applications like E-Mail, VPN and Voice over IP as well as for Homeland Security Requirements and Video Entertainment such as Video over IP and Video Surveillance.

A lower and upper limit for Estimated No of Users has been set to justify initial requirements which could increase as the service becomes viable.

5.2 Applications and Bandwidth Requirement

Table 4: Bandwidth Requirements

Application	**Bandwidth Requirement Per User**	**Estimated No of Users – Lower Limit**	**Estimated No of Users –Upper Limit**	**Total Bandwidth Requirement**
Homeland Security				
Video Surveillance	384 Kbps	1	3	1152Kbps
e-Ticketing				
Commercial Applications for Commuters				
E-Mail	**1.24Kbps**	**5**	**100**	**124 Kbps**
VPN	**16 Kbps**	**5**	**100**	**1600 Kbps**
Voice over IP	**32 Kbps**	**5**	**50**	**1600 Kbps**

Grand Total 4476 Kbps

Table 5: Typical Commercial Off-The-Shelf Packages and Standard Bandwidth Usage

Commercial Off-The-Shelf Packages	**Type of Service**	**Potential User**	**Possible Merits, Issues or Problems**	**Estimated No of Users**		**Total Bandwidth Requirement**	**Typical Standard Costs Per Package**
				Lower Limit	**Upper Limit**		
Personal use - i. E-Mail ii. Web browsing iii. Instant Messaging iv. VPN for Tele-Commuting	ADSL /Cable for internet connection. Minimum of 1.5 MBPS of transfer capability in order for every user to be able to have usable bandwidth.	Daily Commuters		5	100	Min 1.5 Mbps	$50-$100 per month for DSL /Cable service
	For areas not live with DSL /Cable service, possibility is Fractional-T1 or Full-T1.			5	100	G77	$250-$1000/month for Fractional and Full-T1 service.

Table 5: Continued

Internet Gaming	ADSL /Cable for internet connection.	1. Daily Commuters 2. Gaming Company		5	100		$50-$100 per month for DSL /Cable service
	For areas not live with DSL /Cable service, possibility is Fractional-T1 or Full-T1.			5	100		$250-$1000 per month for Fractional and Full-T1 service.
Email Server (say, on the train)	Connectivity to the internet is vital. The In-Train Service Provider must have a connection that is reliable and cost effective, equivalent to Full-T1 service.	Possible Corporate Partners		5	100		Same as above

Table 5: Continued

In-Train Web Server/Web Host	Connectivity to the internet is vital. In-Train Web Server / Web Host must have a connection that will be reliable and cost effective. Depending on how much bandwidth will be utilized several solutions are possible: Single T1 (1.5 Mbps) Dual T1 (3.0 Mbps) Fractional DS3 (1.5 to 45 Mbps) Full DS3 (45 Mbps)	1. Service Provider or Vendor Partner from Bid 2. Rail Diagnostics Server 3. Internet Search Companies such as Google, Yahoo, etc				1.5 Mbps 3 Mbps 1.5 to 45 Mbps 45 Mbps	The price for full-T1 data lines ranges from $600 to $1000/month. Fractional DS3 lines range from $5000 to $10,000/month. Full DS3 lines range from $9,000 to $15,000/month.

Table 5: Continued

ISP Services	Solutions possible as above: Single T1 (1.5 Mbps - 27 simultaneous users) Dual T1 (3.0 Mbps - 54 simultaneous users) Fractional DS3 (1.5 to 45 Mbps - 27 to 804 simultaneous users) Full DS3 (45 Mbps - 804 simultaneous users)	1. Service Provider Vendor Partner from Bid 2. Service Providers like AOL	Features would be nice to know for setting up an SLA with the Vendor. Full DS3 capability may not be required as there would not be so many simultaneous users	25	800	1.5 Mbps 3 Mbps 1.5 to 45 Mbps 45 Mbps	As Above

CHAPTER 6: APPENDIX

6.1 Standards

6.1.1 Overview

Table 6: Standards' Overview

802.11	**Wireless LAN (WLAN)**
802.15	**Wireless Personal Area Network (WPAN)**
802.16	**Broadband Wireless Access (BBW)**
802.18	**Radio Regulatory Technical Advisory Group**
802.19	**Coexistence Technical Advisory Group**
802.20	**Mobile Wireless Access**

IEEE 1473

This standard defines the protocol for inter-car and intra-car serial data communications between subsystems aboard passenger trains. It sets forth the minimum acceptable parameters for a network that can simultaneously handle monitoring and control traffic from multiple systems. While the network itself is not vital, it is intended to be capable of carrying vital messages. This standard will be structured with respect to the OSI seven-layer model.

Table 7: Product Compatibility Required

Access-Point Compatibility	Compatible with any Wi-Fi certified WPA or WPA2 client device for basic capability
Workgroup-Bridge Compatibility	Support operations with standard access points and bridges
Wireless-Bridge Compatibility	Compatible with standard wireless bridges

6.1.2 Reliability and Availability

Table 8: Desired Reliability and Availability should be as follows:

	Access Points or Bridges	Power Injectors
Mean Time Between Failure (MTBF)	>= 132,000 hrs	>= 400,000 hrs

6.1.3 Approvals and Compliance

Table 9: Approvals and Compliance

Country Compliance	Vendors are responsible for verifying approval for use in the US and special requirements in California.	
	Access Points and Bridges	**Power Injectors**
Wi-Fi Certification	Wi Fi CERTIFIED In access-point role (WPA and WPA2)	-
Safety	• UL 60950 Third Ed. • CSA C22.2 No. 60950-00 • IEC 60950 Sec Ed, amendments 1-4 • EN 60950; 1992, amendments 1-4 • CSA 94/UL50-NEMA Rated	• UL 60950 Third Ed. • CSA C22.2 No. 60950-00 • IEC 60950 Sec Ed, amendments 1-4 • EN 60950; 1992, amendments 1-4 • UL2043
Radio Approvals	• FCC Part 15.247 • ARIB-STD-T66 v2.1 • FCC Bulletin OET-65CRSS-102 • Designed to EN60945	-
EMI and Susceptibility (Class B)	• FCC Part 15.107 and 15.109 Class B • EN 55022 Class B • EN 55024 • AS/NZS 3548 Class B • VCCI Class B • Designed to CISPR 25, ISO 11452-24, EN50121, EN60571 and SAEJ1113	• FCC Part 15.107 and 15.109 Class B • EN 55022 Class B • EN 55024 • AS/NZS 3548 Class B • VCCI Class B

6.1.4 Wireless Standards

Table 10: Wireless Standards

Air Interface Standard	IEEE 802.11b or IEEE 802.11g Note: Bridge mode has enhancements to the standard to allow longer- range bridging communications.
Frequency Band	• 2.412 to 2.462 GHz (FCC) • 2.412 to 2.472 GHz (ETSI) • 2.412 to 2.472 GHz (TELEC)
Wireless Modulation	**802.11b** • Direct Sequence Spread Spectrum (DSSS): –Differential Binary Phase Shift Keying (DBPSK) at 1 Mbps –Differential Quadrature Phase Shift Keying (DQPSK) at 2 Mbps –Complementary Code Keying (CCK) at 5.5 and 11 Mbps **802.11g** • Orthogonal Frequency Divisional Multiplexing (OFDM): –BPSK at 6 and 9 Mbps –QPSK at 12 and 18 Mbps –16-quadrature amplitude modulation (QAM) at 24 and 36 Mbps –64-QAM at 48 and 54 Mbps
Media Access Protocol	Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA)
Operating Channels	**802.11b/g** • Americas: 11
Non-Overlapping Channels	3

6.2 Performance Specifications

- Data rates of 54 Mbps in the 2.4 GHz band
- Range of 20 miles (32 kilometers [km]) at 11 Mbps
- Aggregate throughputs approaching 28 Mbps
- Maximum transmit power of 100 milli-watts (mW) for 802.11b and 30 mW for 802.11g
- For moving train-installed deployments, over 100 km per hour speeds at 12 and 24 Mbps
- Packet Error Rate (PER) at 1% or better for 128 byte packets
- Support for antenna diversity
- Multiple, configurable radio network roles for point-to-point and point-to-multipoint network architectures
- Wide DC power-input range allowing a variety of power-supply options such as solar power or vehicle power (+10 to +48 volts direct current [VDC])
- Wide operating temperature range of -22°F to 131°F (-30° to +55°C)
- Meet NEMA 4 and IP56 specifications for harsh environments
- Captured antenna for easy mounting and support for external antennas
- Support 3DES

- Be Compatible with Military and Command & Control Environments in public safety
- Be Compatible with Military and Command & Control Environments in public safety
- Provide advanced IP services
- Provide Security features including firewall protection and encrypted virtual private networks (VPNs) to keep data secure over a public WAN infrastructure.
- Provide Quality-of-service (QoS) features to enable simultaneous access to several applications over a single WAN connection and protect delay-sensitive traffic such as video
- Provide QoS to facilitate low-latency routing of delay-sensitive applications such as Voice over IP
- Enable QoS to allow the intelligent management of bandwidth by allowing operators to define which applications or users are given priority over others
- Provide compatibility with IETF industry standards
- Provide a simplified application development environment by supporting industry-standard TCP and UDP protocols
- Provide support for voice, video and data applications over IP
- Enable remote management and monitoring via Simple Network Management Protocol (SNMP), Telnet, or Hypertext Transfer Protocol (HTTP) and local management via console port
- Provide data and system integrity when using public networks by incorporating at least minimum Security features such as IP Security (IPSec), Triple Data Encryption Standard (3DES) and stateful firewalls and intrusion detection

- Provide a capability to provide real-time alerts to ensure perimeter security
- Provide an efficient broadcast of data or video for increased situational awareness, multi-user communications and surveillance applications for Homeland Security Requirements
- Provide control and configuration of secure access options by supporting per-user and per-session authentication using RADIUS authentication services
- Allow secure tunnels to be established to ensure data integrity
- Ensure interoperability between applications and IP-based networks
-

Security

Table 11; Security Issues

Security-Bridge Role	Wireless Security required: **Authentication** • 802.1X support including LEAP to yield mutual authentication and dynamic per-user, per-session encryption keys **Encryption** • TKIP or WPA TKIP; key hashing (per-packet keying), Message Integrity Check (MIC) and broadcast key rotation • AES (802.11i)
Security-Access-Point Role	Wireless Security supporting WPA and WPA2, including: **Authentication** • 802.1X support including LEAP, PEAP-GTC, PEAP-MSCHAPv2, EAP Message Digest 5 (EAP MD5), EAP-TLS, EAP-TTLS, EAP-SIM, and EAP-FAST to yield mutual authentication and dynamic per-user, per-session encryption keys **Encryption** • WPA: Cisco TKIP or WPA TKIP; key hashing (per-packet keying), MIC and broadcast key rotation • WPA2: AES (802.11i)
Security-Workgroup-Bridge Role	Cisco Wireless Security Suite, including: **Authentication** • 802.1X support including LEAP to yield mutual authentication and dynamic per-user, per-session encryption keys **Encryption** • TKIP or WPA TKIP; key hashing (per-packet keying), MIC and broadcast key rotation • AES (802.11i)
SNMP Compliance	Versions 1 and 2

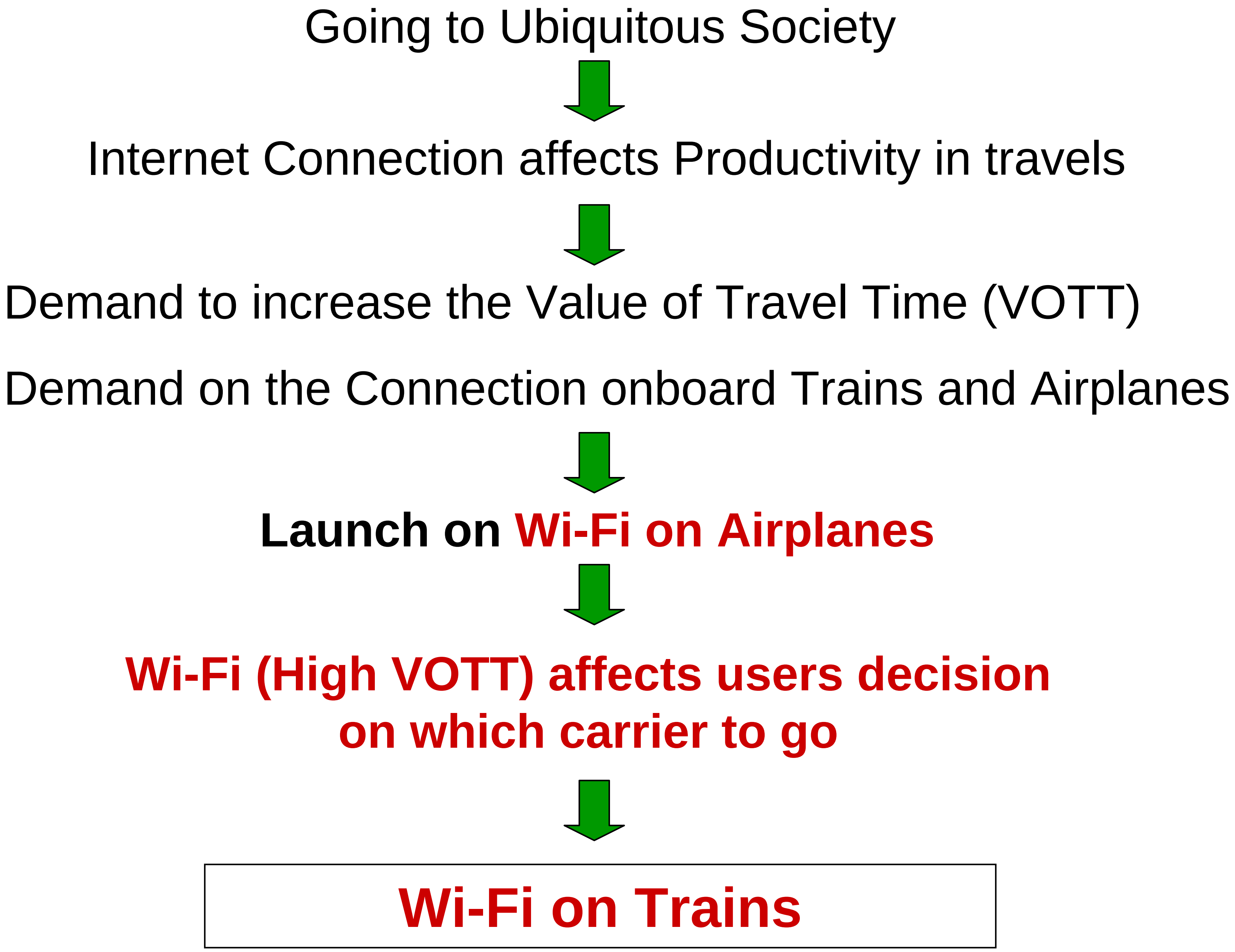
Appendix H

Technologies for Wi-Fi on Trains

May 31, 2005

Kazuhiro Yamada

Introduction & Objective



Going to Ubiquitous Society

Internet Connection affects Productivity in travels

Demand to increase the Value of Travel Time (VOTT)

Demand on the Connection onboard Trains and Airplanes

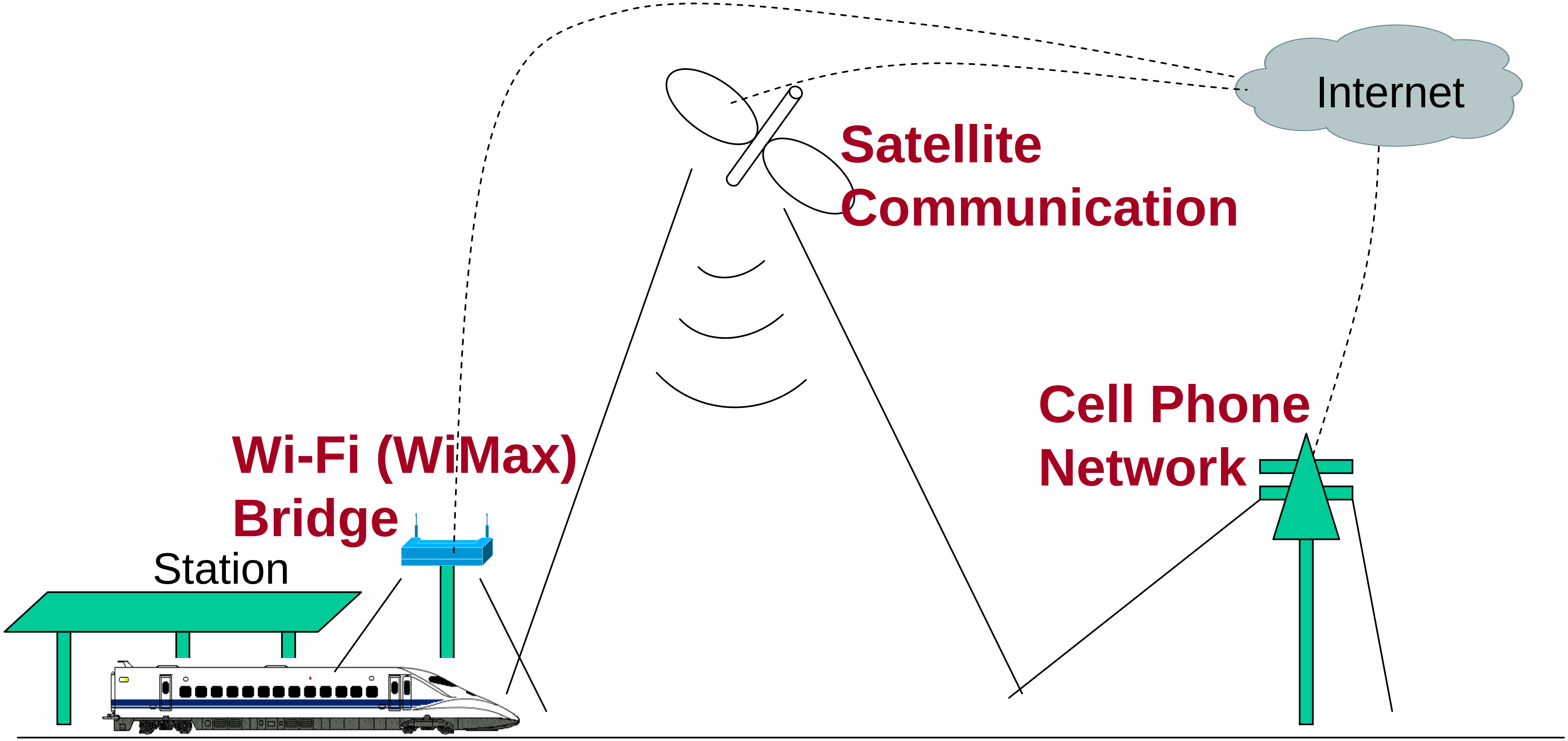
Launch on Wi-Fi on Airplanes

Wi-Fi (High VOTT) affects users decision on which carrier to go

Wi-Fi on Trains

Required Technologies for WiFi on Trains

Choices of the best technologies matching to places



STEP : 1. Survey the latest Radio communication technologies

What are pros and cons?

2. Develop the Seamless Handover using Mobile IP

Outline

1. Radio Technologies
   1. Satellite Communication
   2. Trackside Solutions

2. Network Technology

   Mobile IP

Radio Technologies

Satellite Communication

Features of Geostationary Satellite

+ Bandwidth : 500MHz or 1GHz in Ku Band (14MHz)

+ Number of Transponders : 24 in 500MHz, 48 in 1GHz

+ Connection Speed : 30Mbps on each transponder

Total 720Mbps in 500MHz, 1.44Gbps in 1GHz

+ Easy Receiving, Difficult Transmitting

Satellite receiving, Cell transmitting = CCJPA, VIA, Eurostar

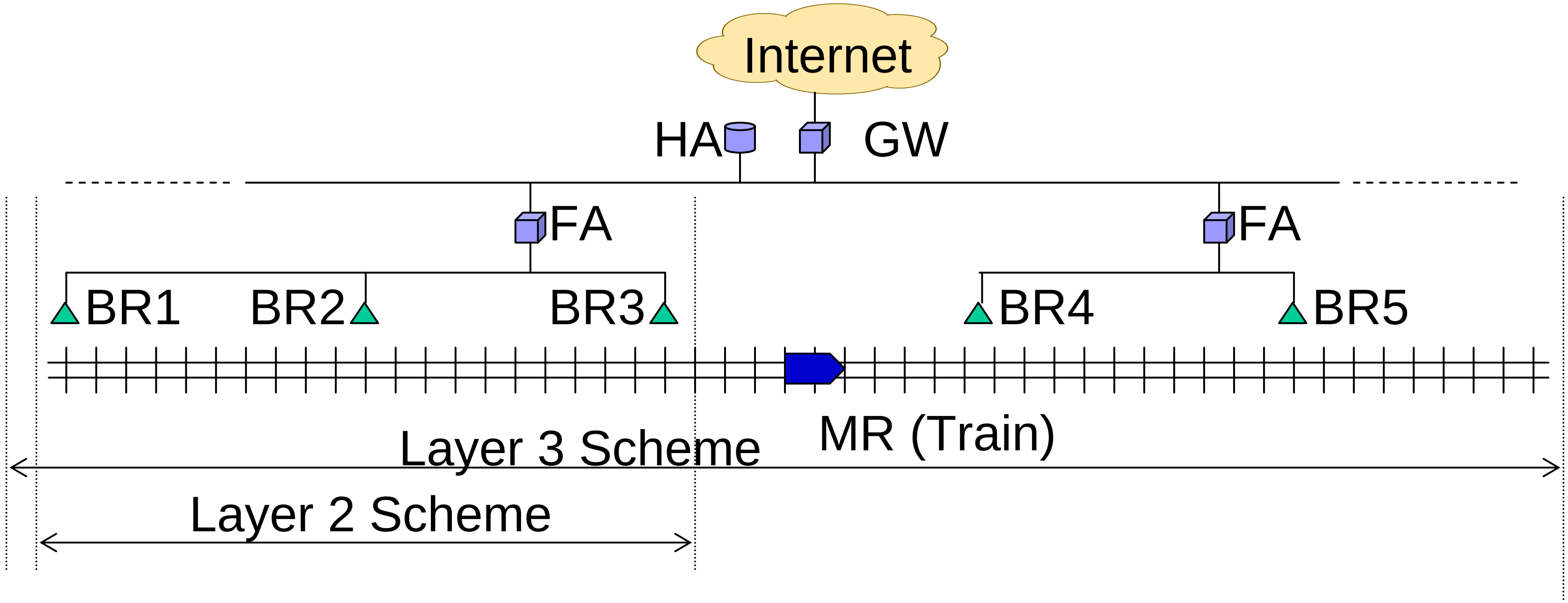
Satellite for both ways = TGV, RENFE

+ Not available all over the world (Need to check the coverage)

+ Connection Speed depends on the contract

+ The more high speed = the more high cost

Wi-Fi (WiMax) Bridge



- **Install BRs on trackside**
- **Connection Speed**

  IEEE802.11g (Wi-Fi) = 54Mbps

  IEEE802.16e (WiMax) = 32Mbps ? (not standardized)
- **Distance between two BRs**

  >> depends on the regulations in each country
- **WiMax Bandwidth lies mainly on 5GHz LICENCED band**

WiMax (IEEE802.16e) in the future ?

Standard	IEEE802.16d	**IEEE802.16e** (*2)	
Scene	Fixed	Mobile (L2H/O, up to 150km/h?)	
Modulation	64QAM (*1)	16QAM ? (**2/3** speed of 64QAM)	QPSK ? (**1/3** speed of 64QAM)
Bandwidth	~ 20MHz (*1)	~ 10MHz ? (**1/2** speed of 20MHz)	
Speed	~ 75Mbps (*1)	~ 32Mbps ?	~ 16Mbps ?
Range	(in general) ~ 5 or 6km (Ant is on the top of a tower) ~ 20km (*1)	(Directional) ~ 2.5km ? (Omni-directional) ~ 1.5km ?	(Directional) ~ 4km ? (Omni-directional) ~ 2.5km ?

(*1) Intel-conducted trial in Las Vegas in May 2005

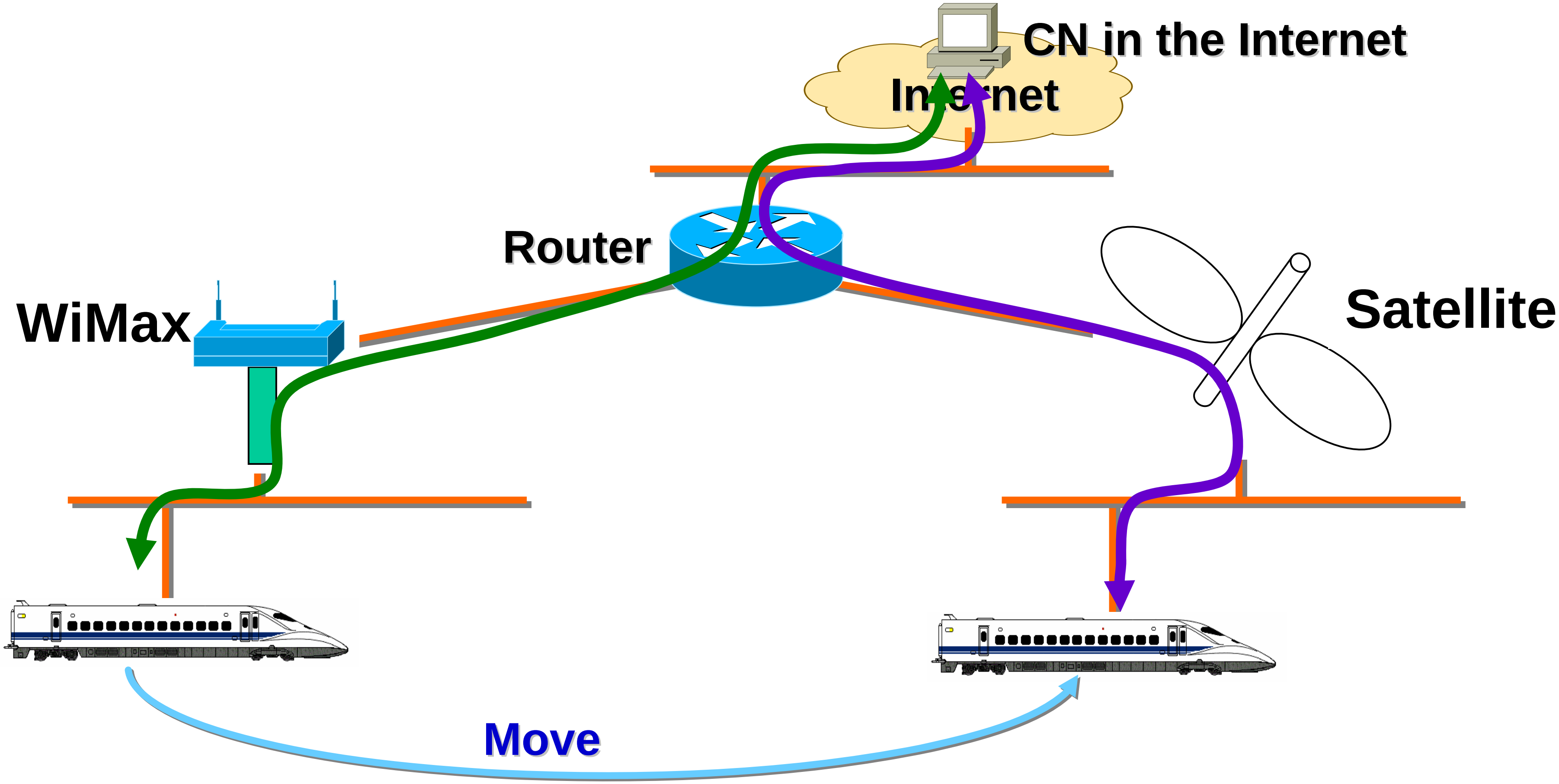
(*2) Based on WiLAN-conducted trial (Reported in Oct. 2004) This is not a standard.

Summary of Radio Technologies

	Satellite	Trackside
Connection Speed	Up to tens of Mbps per system	Tens of Mbps per BR
Installation Cost	Low	High
Running Cost	High	Low
Applicable to	**Small to Mid** Size system	**Large** size system

Network Technology

Why is Special(?) Network Tech needed?

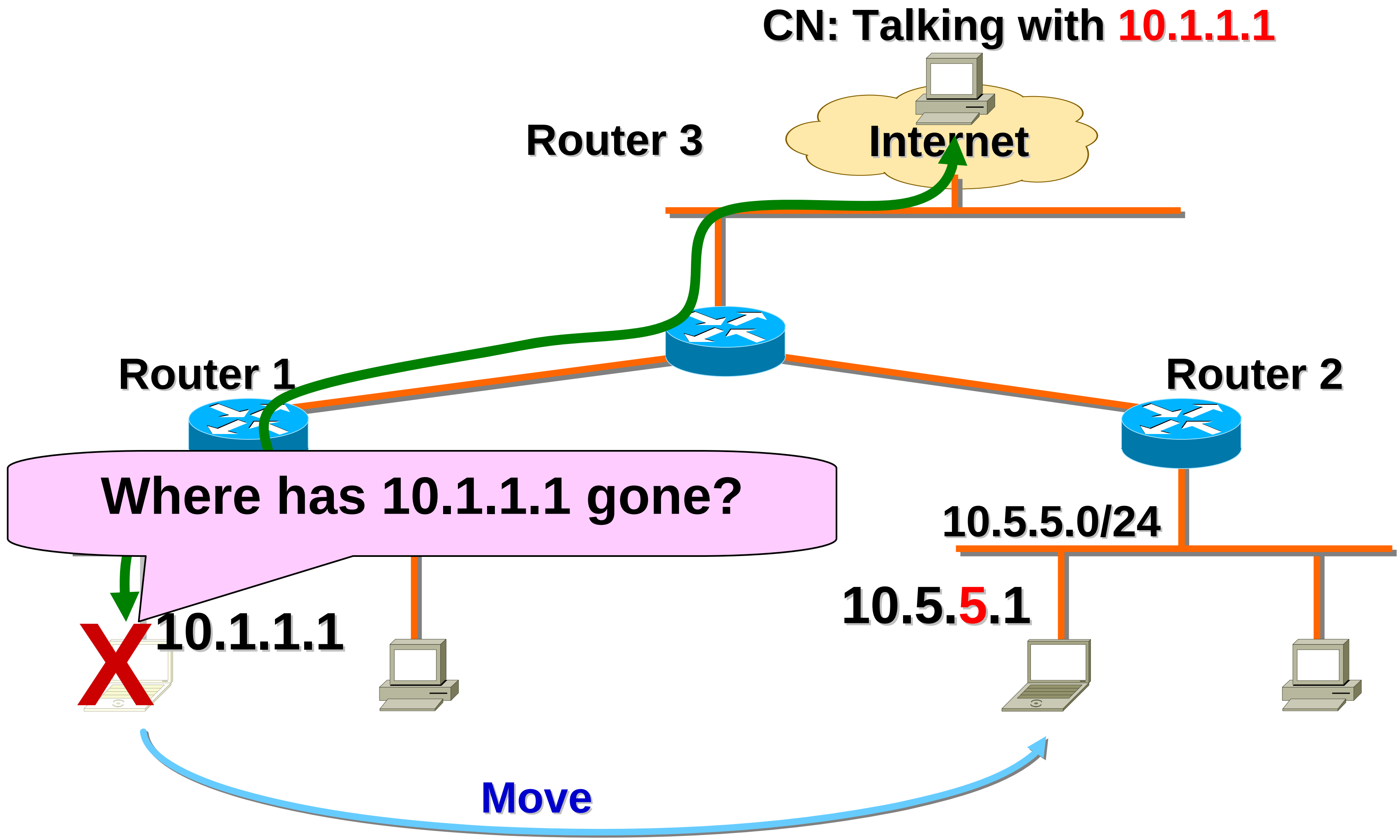


IP route is changed

↓

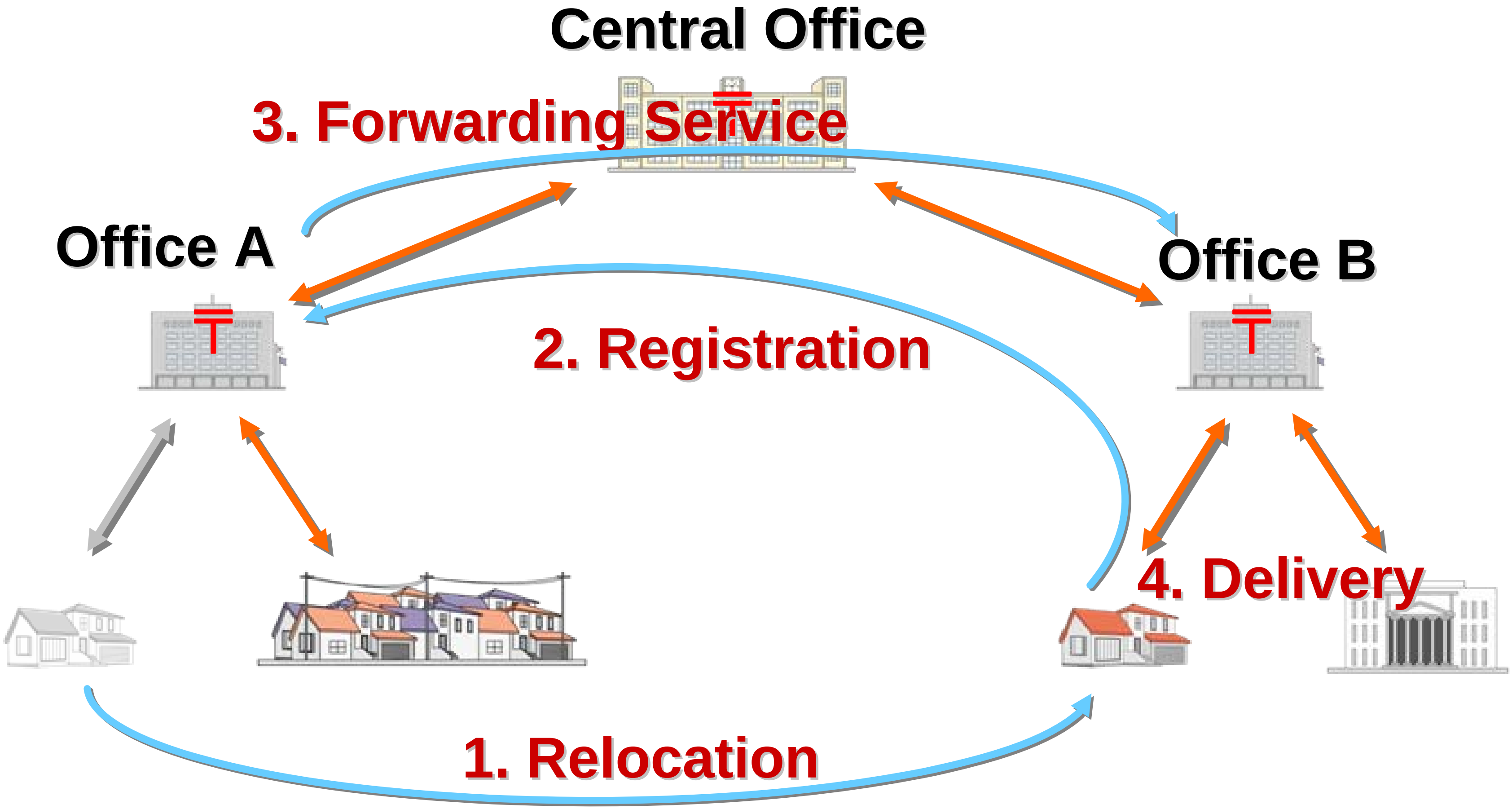
Supported by a Network Technology

Traditional IP Network

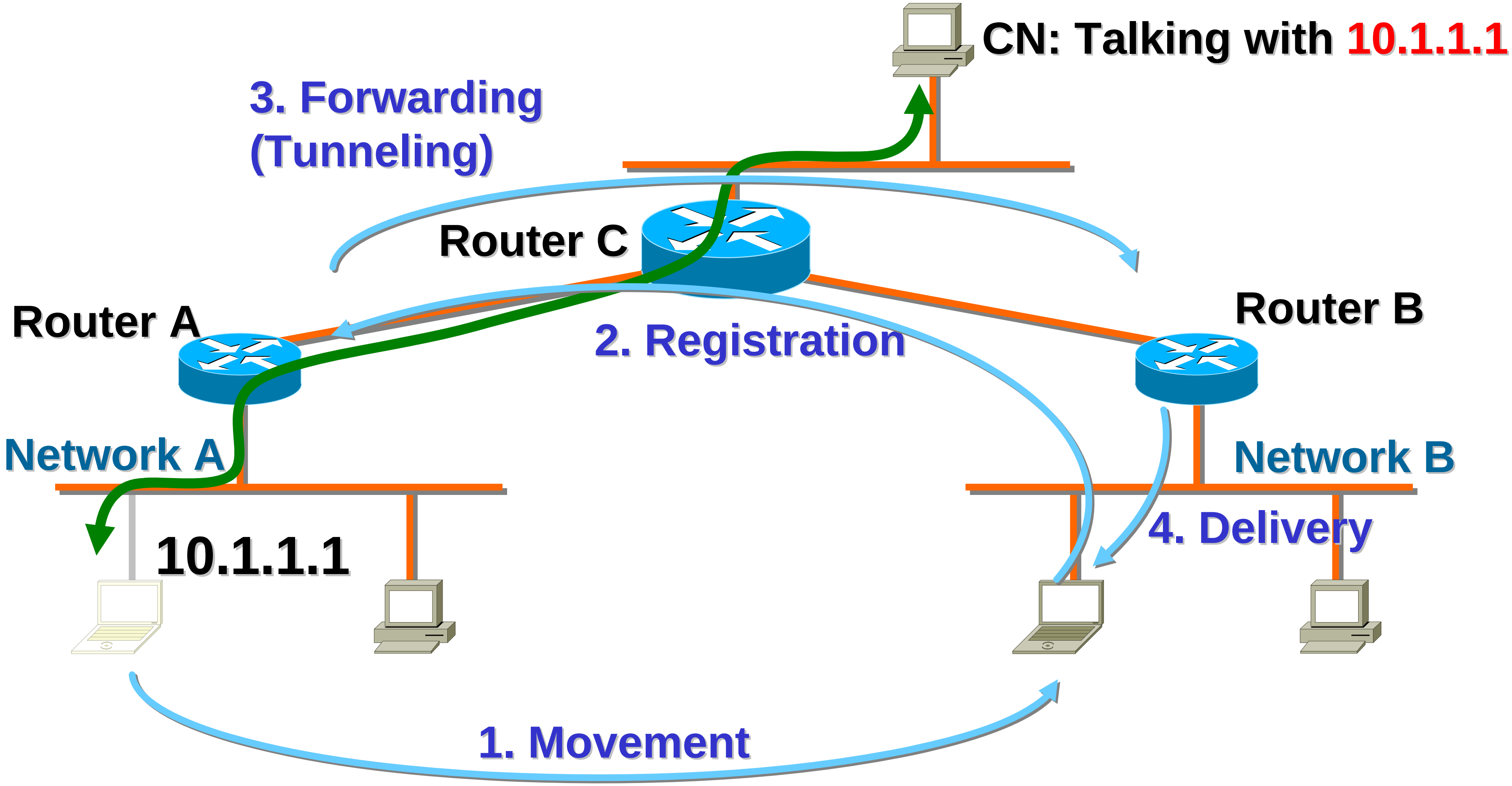


It is **Mobile IP** that supports the movement.

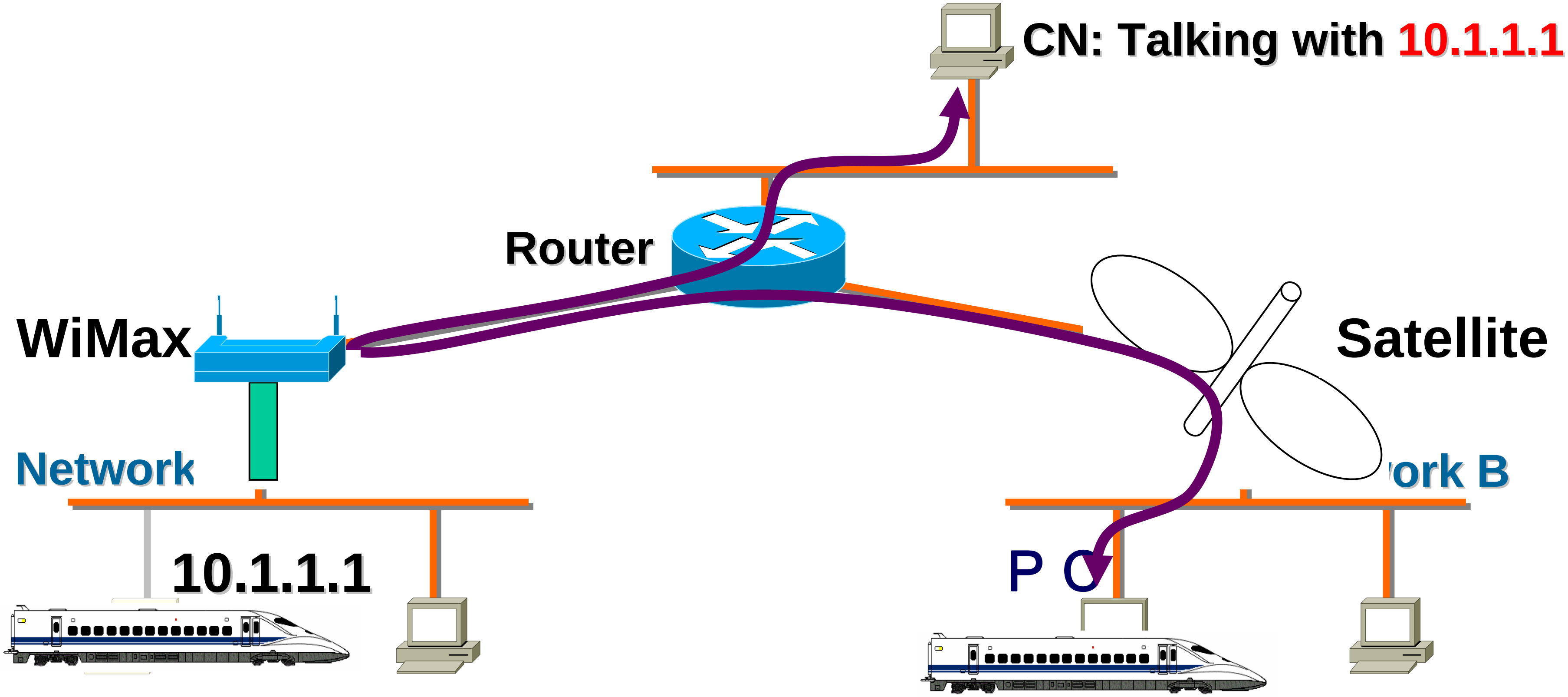
How Mobile IP works? (ex. Postal Service)



How Mobile IP works? (IETF standard = RFC3344)



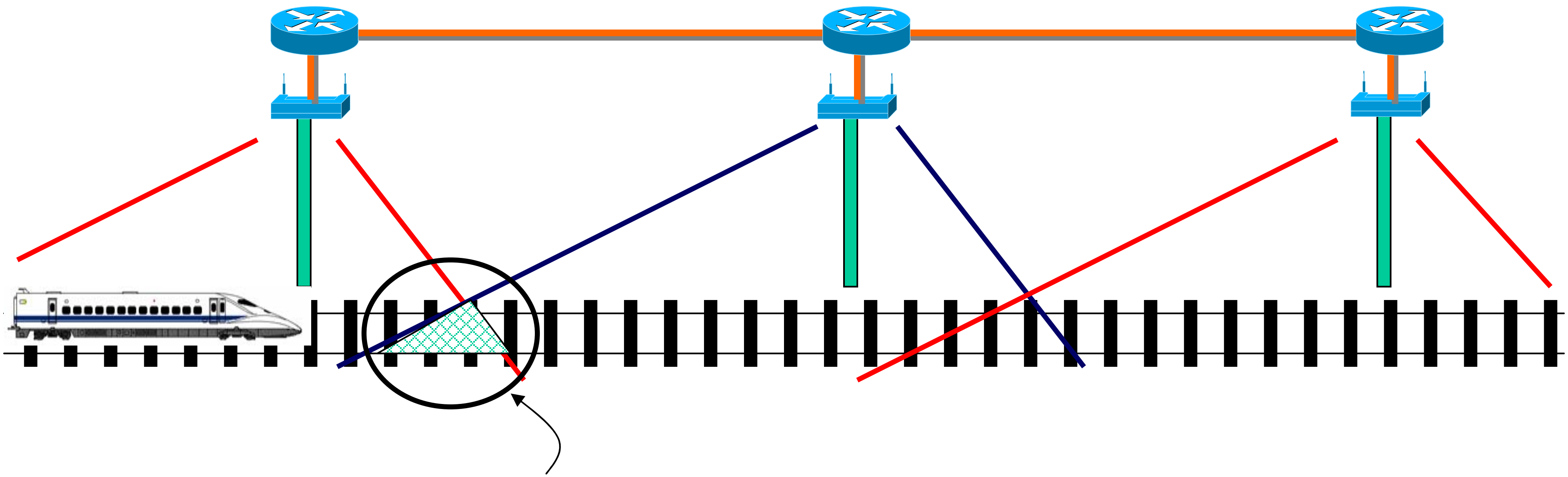
How Mobile IP works? (IETF standard = RFC3344)



It generally takes a few seconds to complete a Handover.

Is it acceptable?

Mobile IP for Wi-Fi (WiMax) Bridge



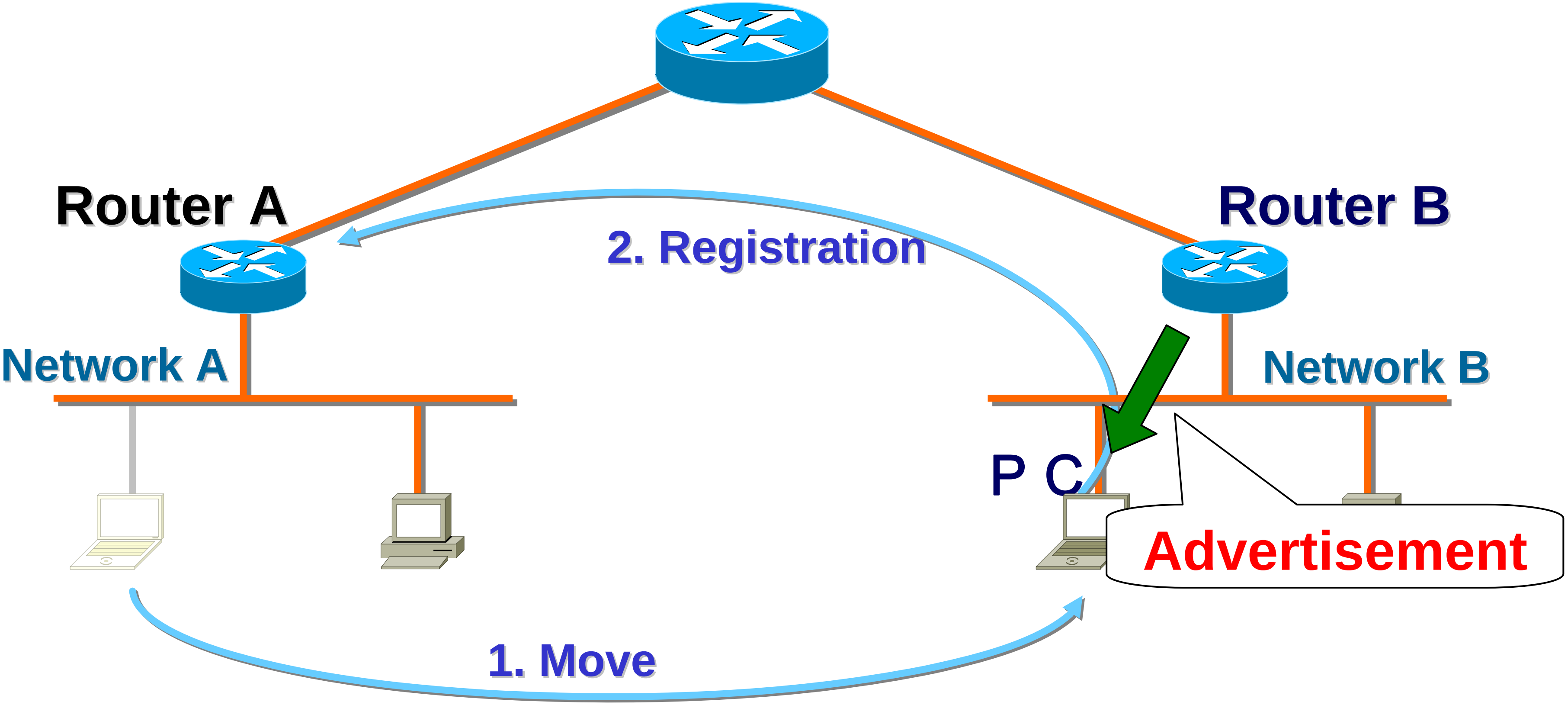
A few sec needed after receiving blue radio

A train passes within seconds, it loses the connection.

(To avoid disconnection)

1. Shorten the Mobile IP process time
2. Lengthen the overlap time (red and blue)

What is the MIP H/O process?



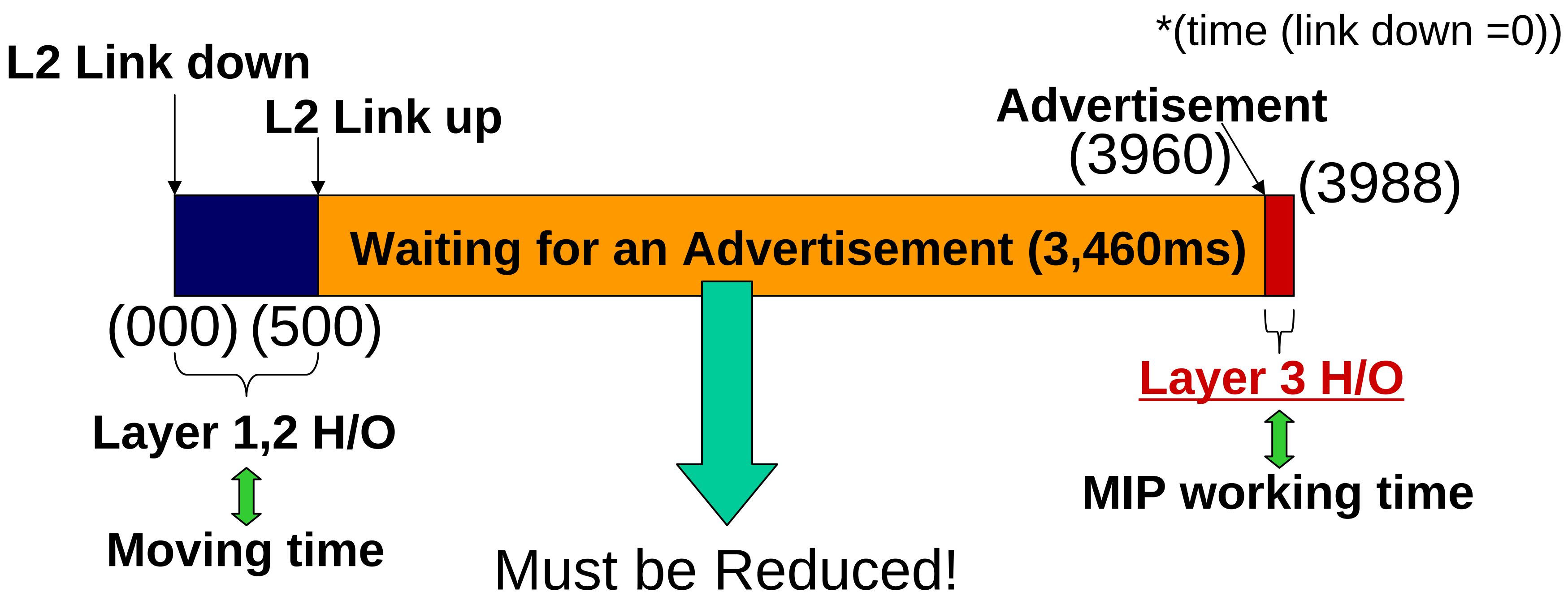
+ Move Detection

Waiting for an Advertisement from Router B

+ Advertisement Interval is variable

Shorter Interval = Higher load to the Network

MIP Process time



*(time (link down =0))

L2 Link down

L2 Link up

Advertisement

(3960)

(3988)

Waiting for an Advertisement (3,460ms)

(000) (500)

Layer 1,2 H/O

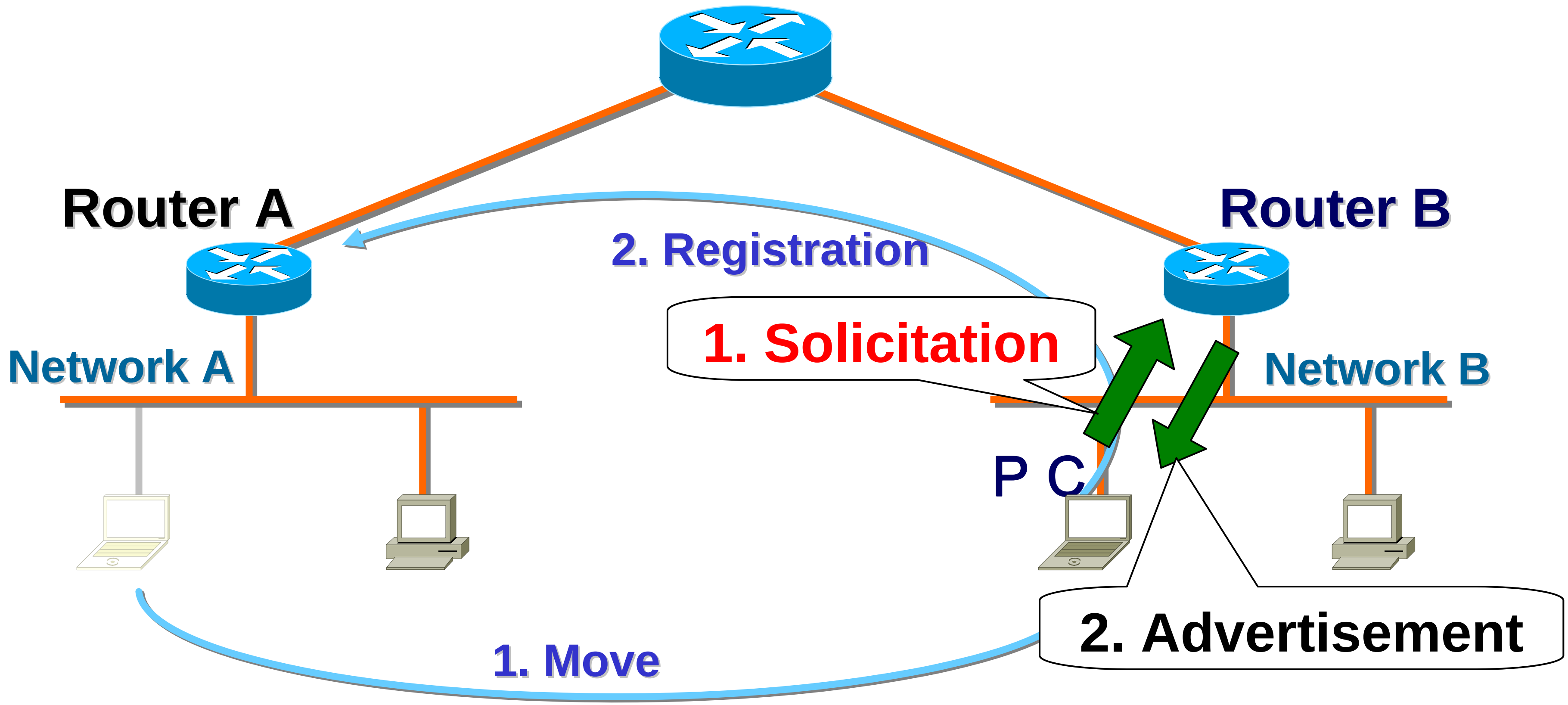
Moving time

Must be Reduced!

Layer 3 H/O

MIP working time

Shorten MIP Process Time with SNMP-trap



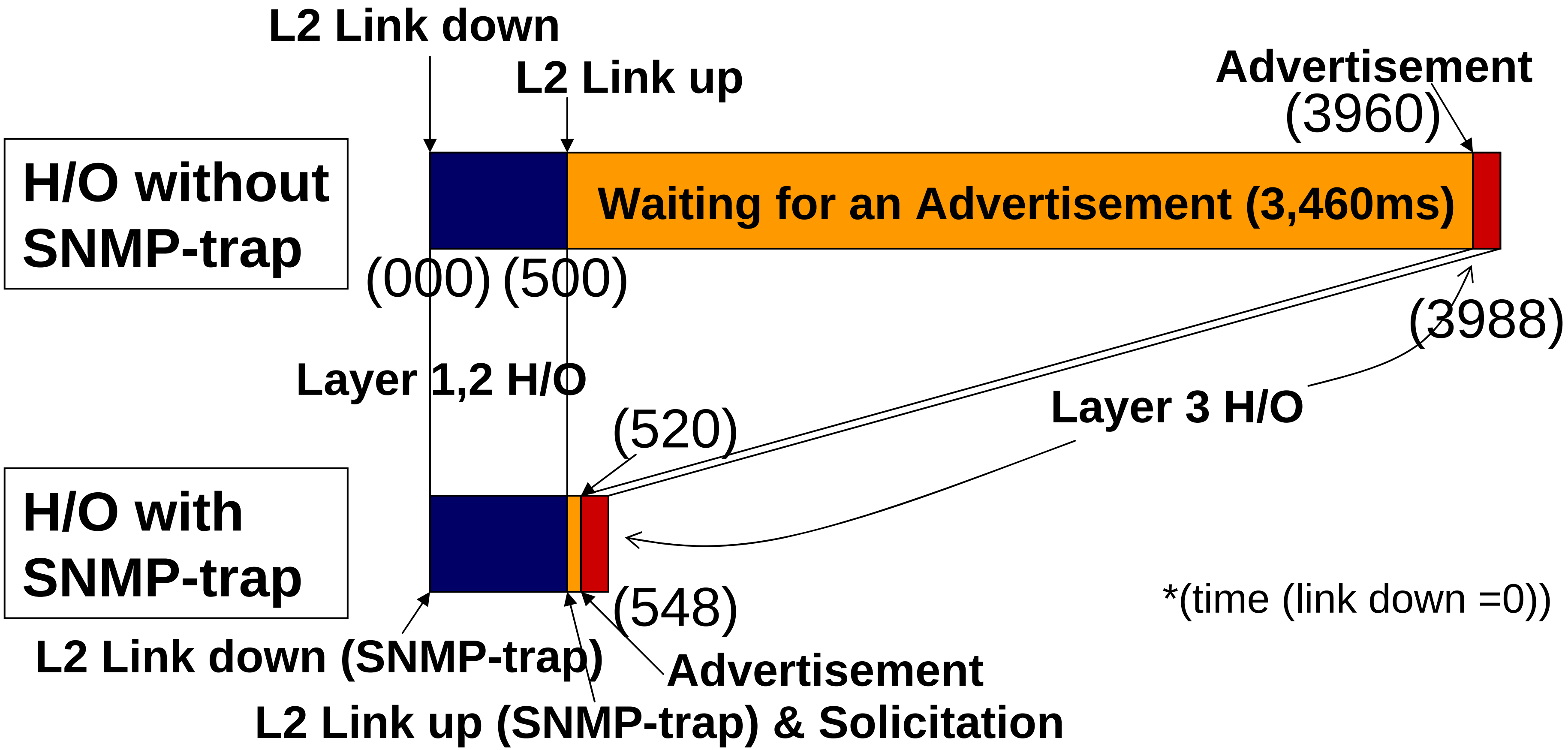
+ Move Detection

Watching the (wireless) Interface by SNMP-trap

Finds the interface change, informs MIP.

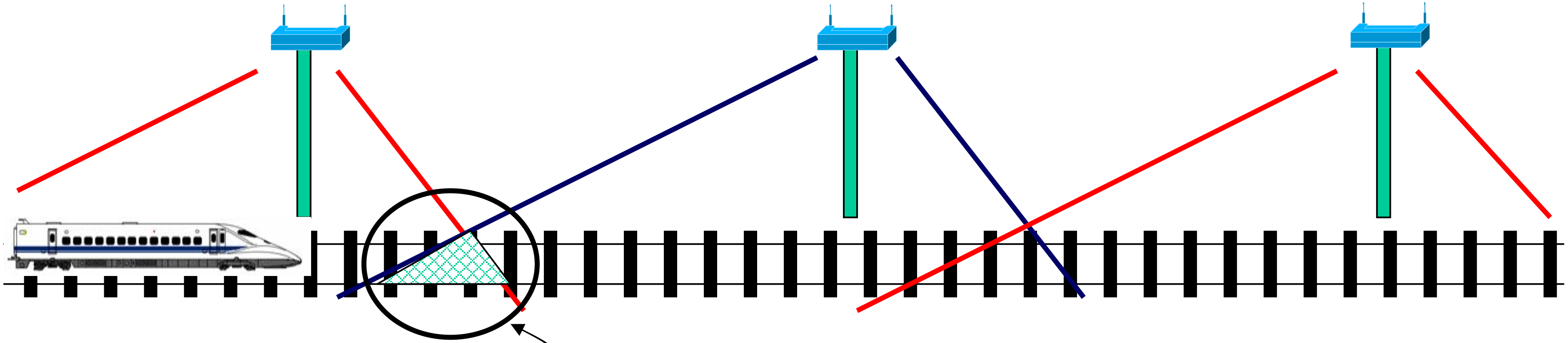
+ NO periodical Advertisement Needed

Result of Handover with SNMP-trap



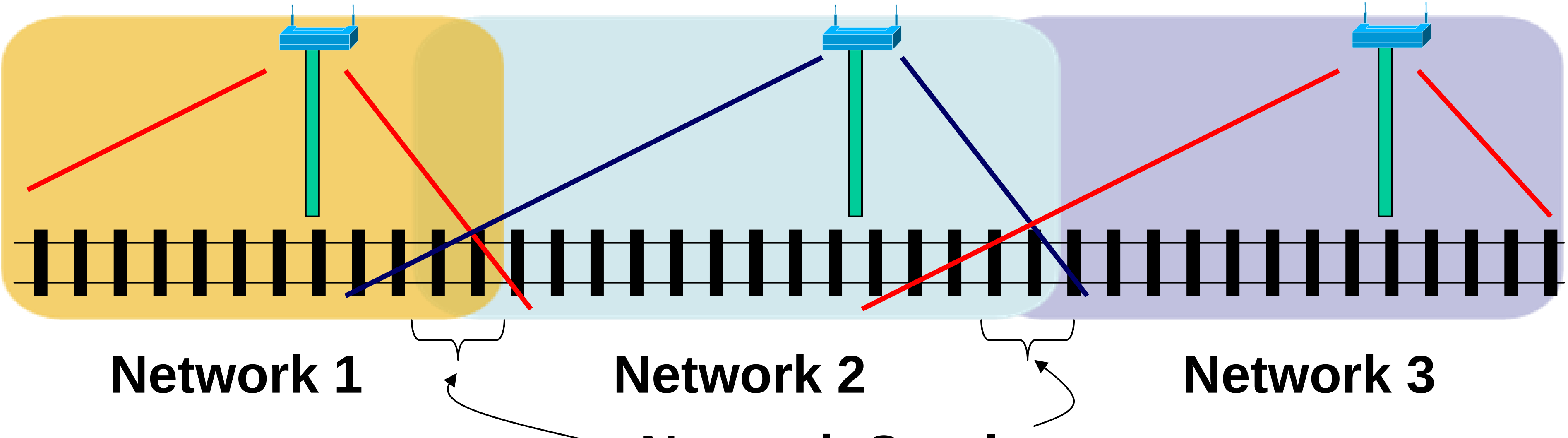
SNMP-trap reduces waiting time 3,440ms to 20ms.

Lengthen the overlap time



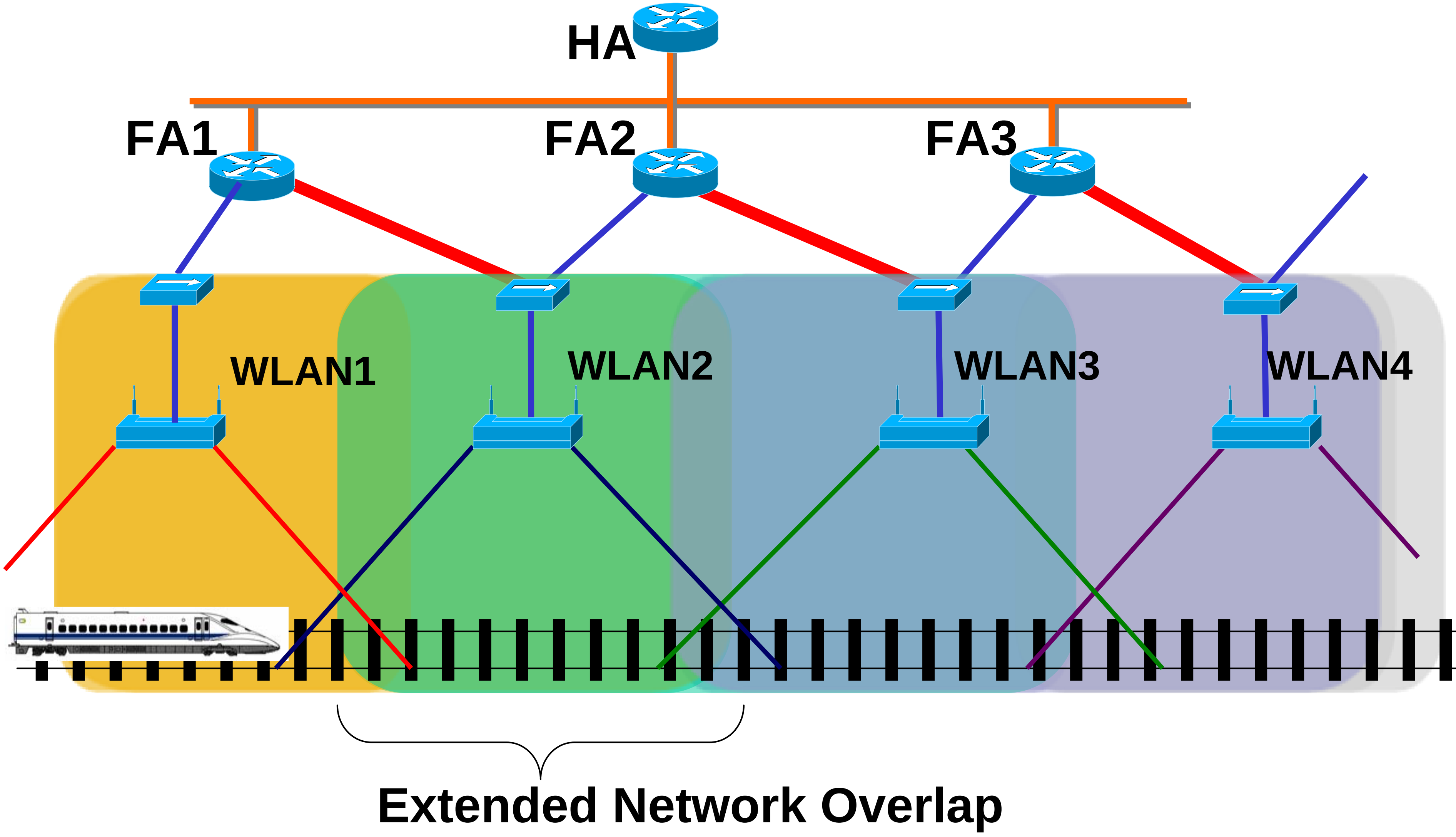
Physically Impossible to lengthen the time & distance

Logical Network is…

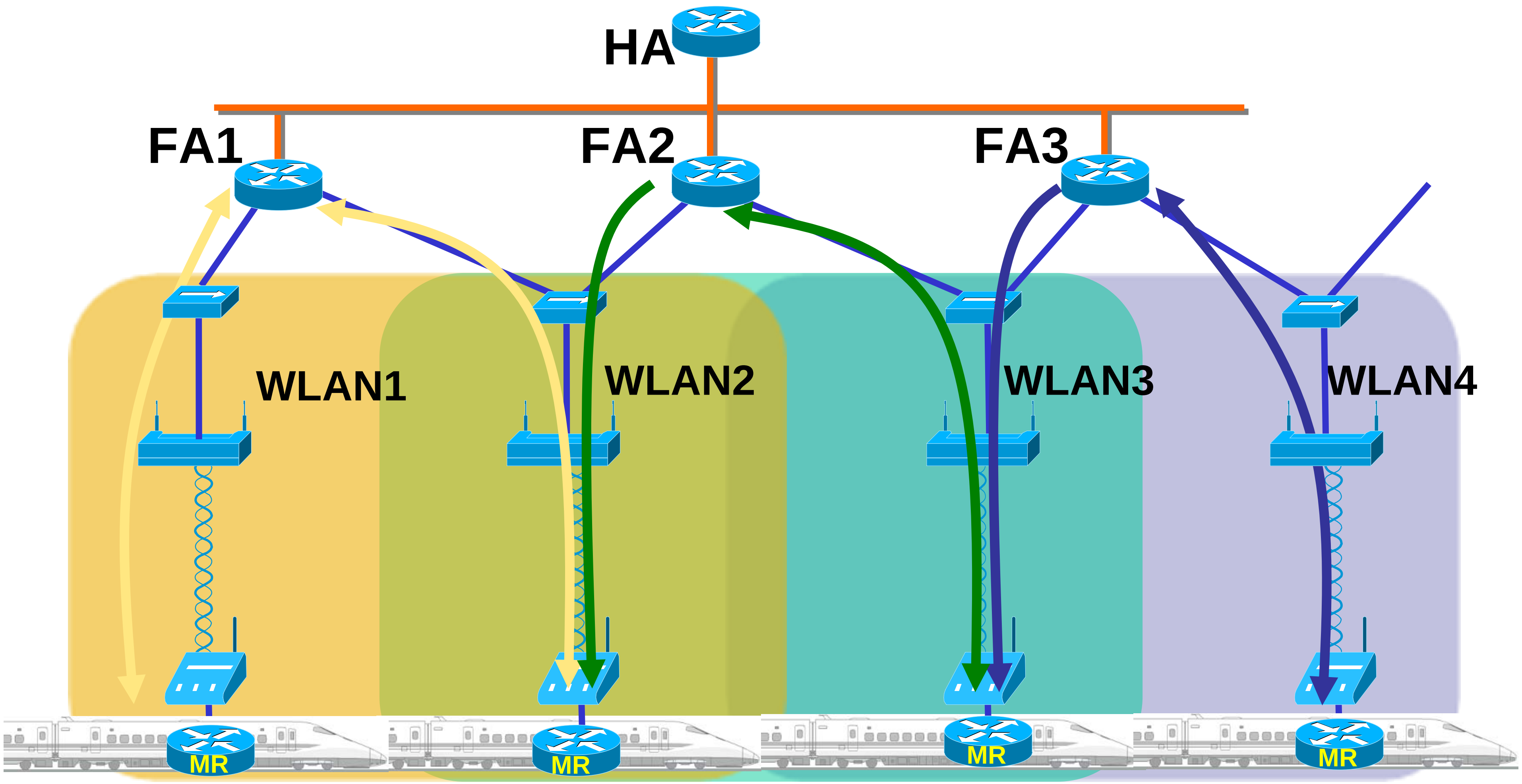


Network Overlap

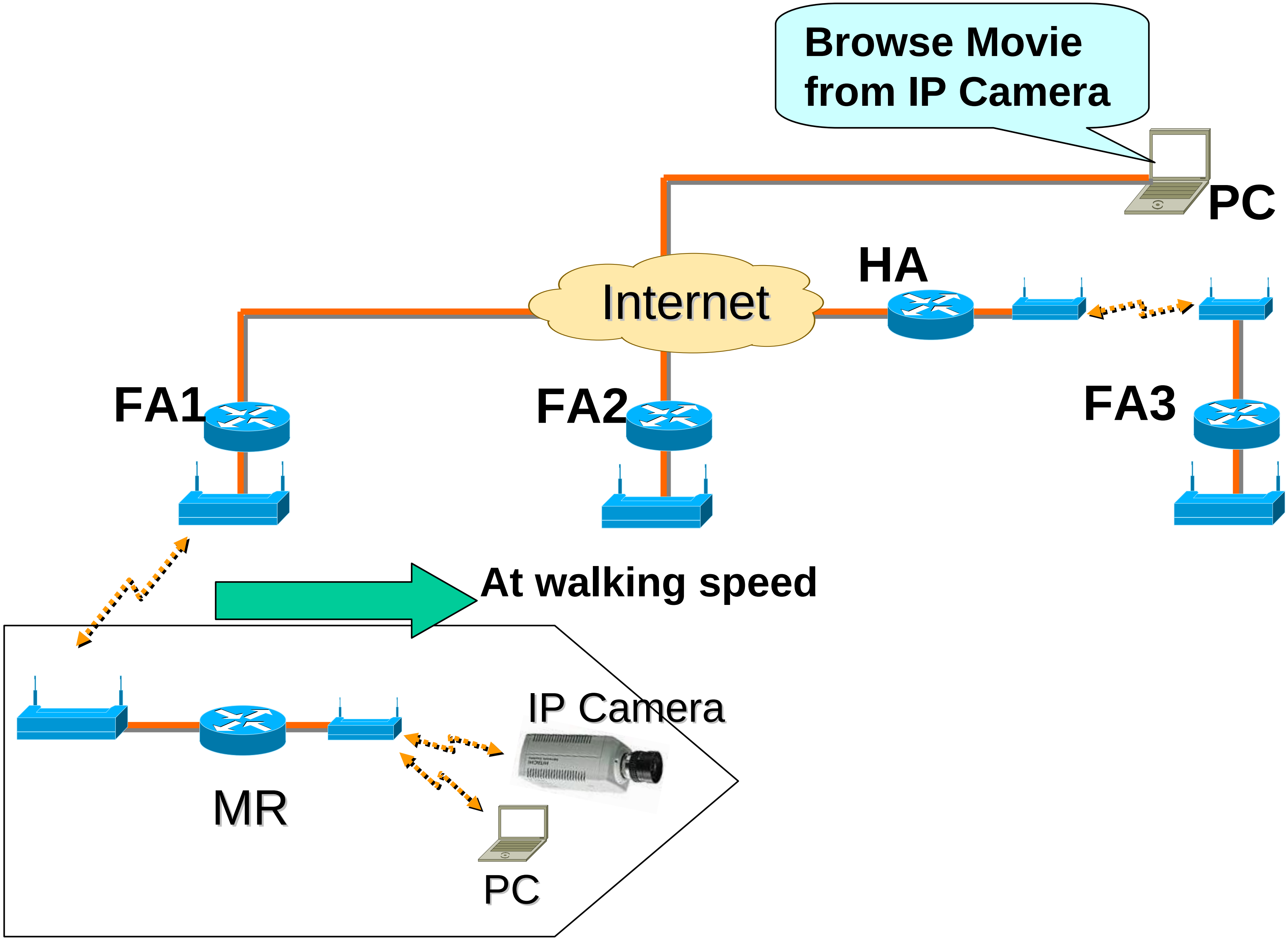
Lengthen the Network Overlap



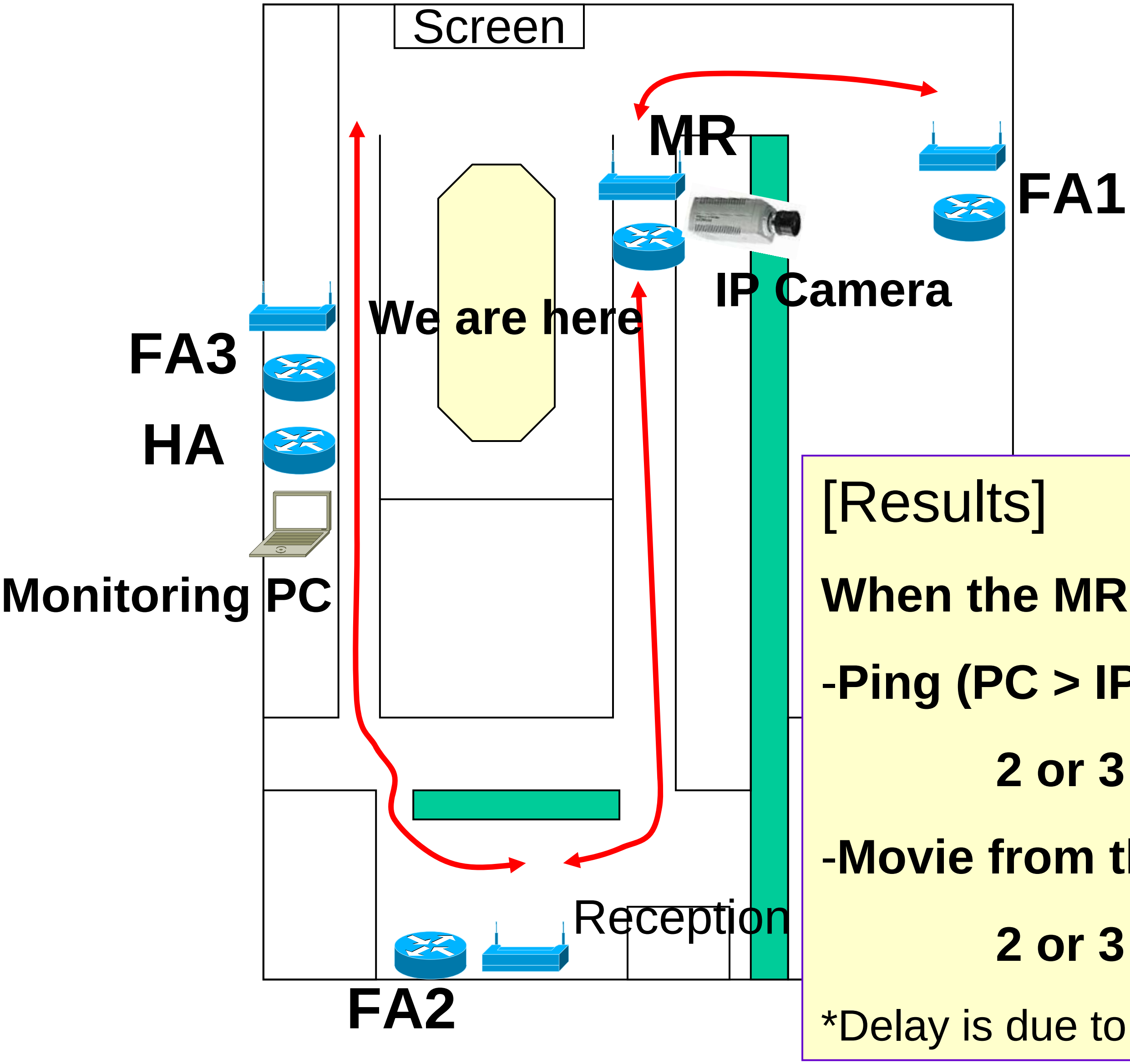
How do trains roam?



Lab Test (Application = Movie Streaming)



Lab Test (Application = Movie Streaming)



[Results]

When the MR roams,

-Ping (PC > IP Camera)

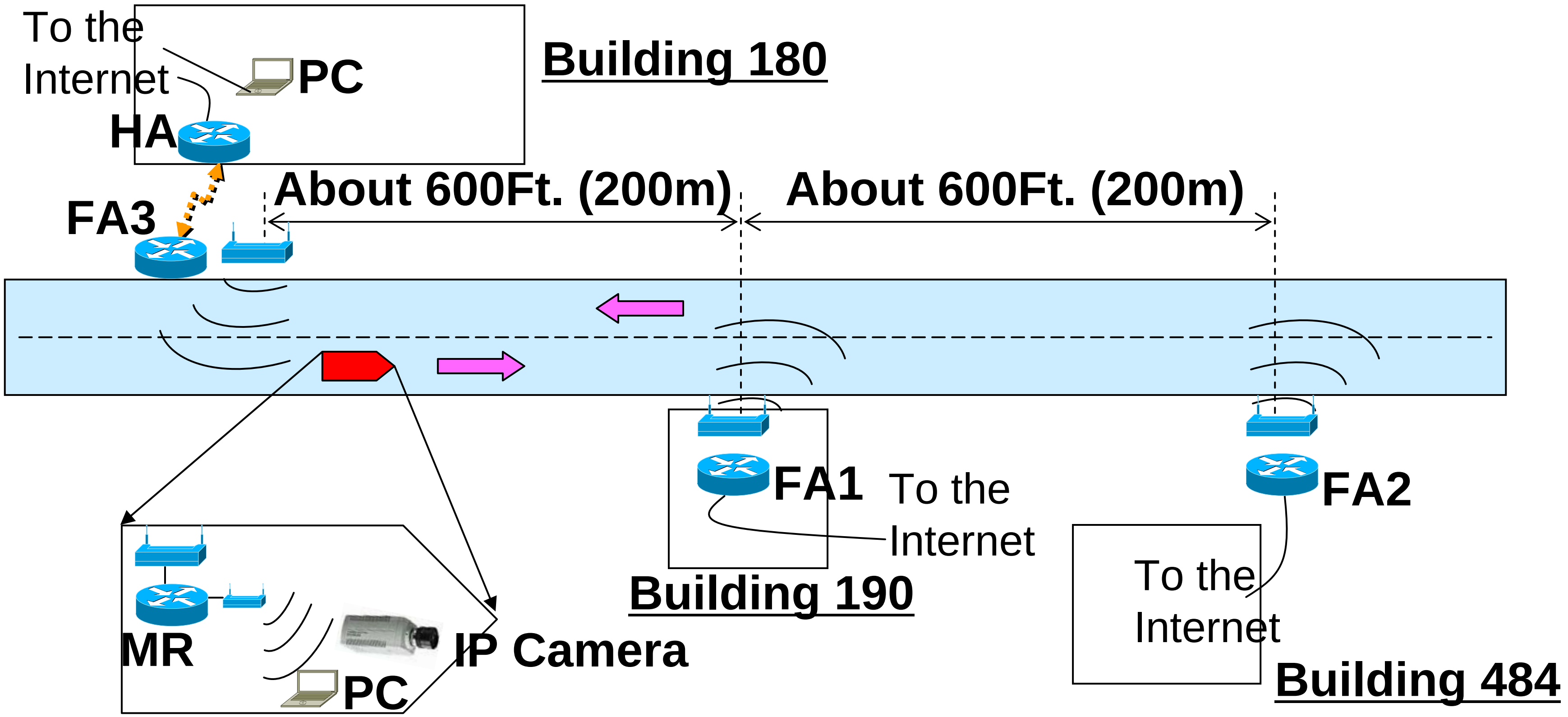
2 or 3 pings Lost

-Movie from the Camera

2 or 3 sec frozen time

*Delay is due to BR processes

Field Test at car speed



To the Internet

PC

HA

Building 180

FA3

About 600Ft. (200m)

About 600Ft. (200m)

FA1

To the Internet

Building 190

FA2

To the Internet

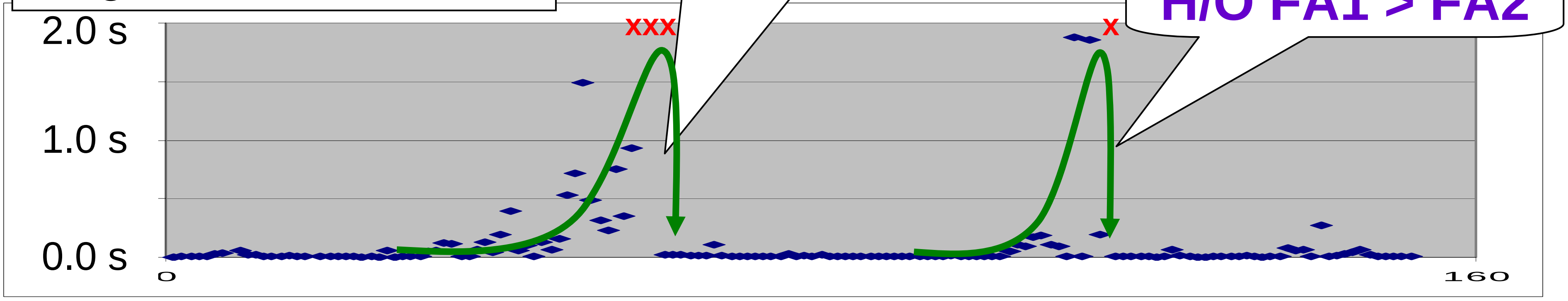
Building 484

MR

PC

IP Camera

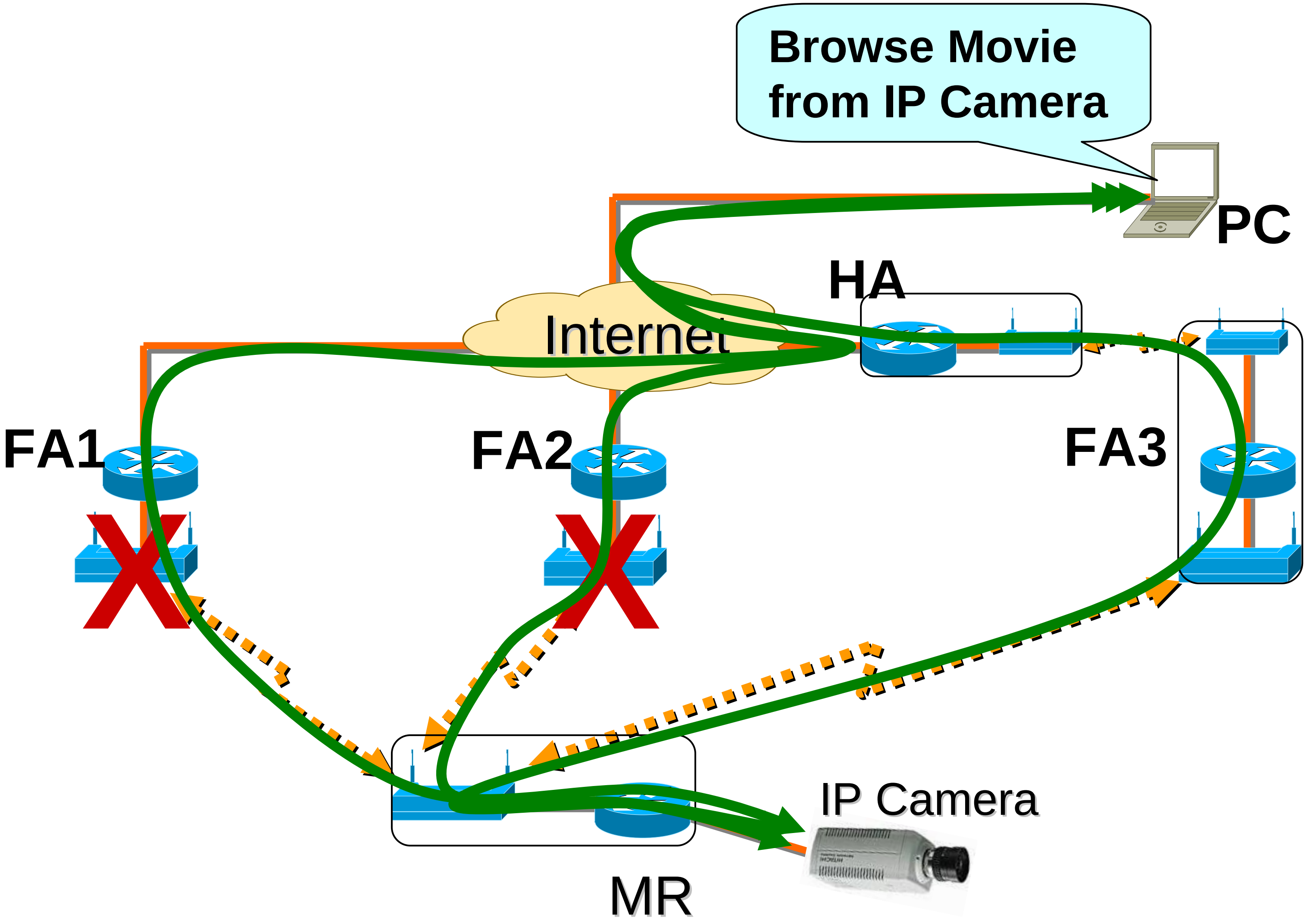
Ping Turn Around Time



H/O FA3 > FA1

H/O FA1 > FA2

Demonstration



Conclusion of Network Technology

What is the standard for mobile network?

Mobile IP

What are the requirements to apply to rail systems?

1. Reduction of the H/O process time

⇨ **SNMP-trap reduces 3,440ms to 20ms.**

2. Optimization of the network topology

Mobile IP Test Results

1. MIP works very well

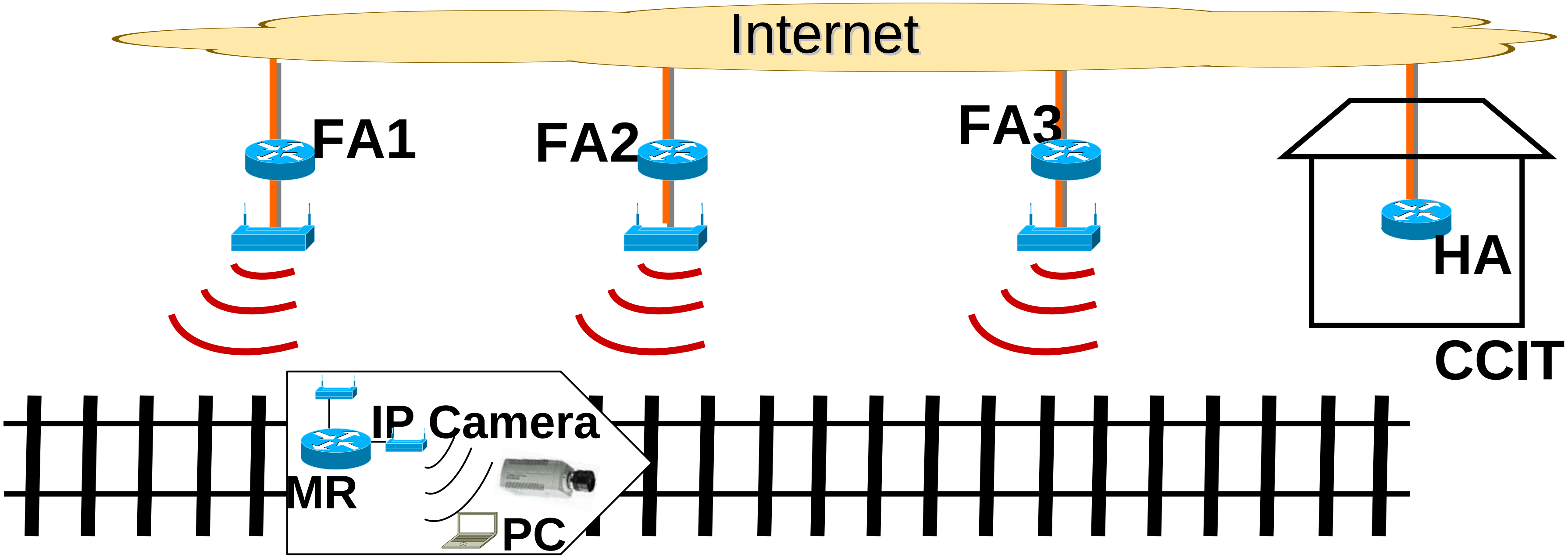
⇨ **Can be deployed to wi-fi on trains system**

2. Layer 2 takes 500ms in the H/O process

⇨ **Should be configured (Next Step)**

Next Step in Network Technology

1. Field Test on a train



2. Layer 2 H/O should be optimized.