

IEEE802.11
Wireless Access Method and Physical Layer Specifications

**THE USE OF TERMS FOR EXPRESSING
 THE CONCEPTS OF "ROAMING", "HAND-OFF"
 "REGISTRATION" AND "IDENTIFICATION"
 IN WLAN SYSTEMS**

1. Issues Addressed(not necessarily resolved)

...and other related to issues.

- 10.2 - What are the events that cause switching between multiple CF's ?
 - do multiple CF's need to be specified?
- 10.4 - What are the requirements concerning service area ?
- 13.1 - What control and observation features are needed for network management support ?
- 13.2 - What is the architecture of the network management services ?
 - within the layer ?
 - separate layer ?
- 16.1 - Will the standard support roaming for both Asynchronous, and time-bonded services?
- 16.2 - What is roaming?
 - what is hand-off ?
- 16.3 - is anything required from IEEE 802.1 regarding roaming ?
- 16.6 - if 1.2/1.3/1.4 are supported, then does the standard need to support seamless "handover"?
- 16.7 - What does seamless mean ?
- 16.8 - how will the standard address the ability for the MAC to support hand-off between service areas?
- 16.9 - What are the requirements of the following functions related to station mobility?
 - coordination in ESS
 - security
 - management
 - location

2. Introduction

In order to minimize confusion in the discussions of these concepts, it is my intention to offer a set of definitions which (although open to editing and refinement) will allow each of us to communicate technical issues with a minimum of confusion.

3. Analogies

REGISTRATION

In the Cellular telephone industry , the term registration is used to describe the process which a customer of a cellular network goes through when first subscribing to that network. In this process the telephone-set is "programmed" with an internal identification issued by the company operating the network. The reason for registration is to allow the company operating the network to identify and bill the subscriber each time the telephone-set is used.

A given telephone-set may have multiple internal identification numbers for the purpose of registering to more than one cellular system (in the USA and most other countries there is more than one network providers for any given area - usually two.) This allows the user of the telephone-set to select or switch between network providers, provided he is registered with each.

It should be remembered that the registration function is a semi-permanent operation and last as long as the subscriber and the network operator have a business relationship.

ROAMING

For telephone-set users/owner who have the requirement to use their telephone-sets while traveling, the network providers offer a temporary form of registration which can be turn on and off easily by placing a telephone call to the business offices of the network provider. This feature called roaming is identical to registration except that the billing for calls made on networks where he might visit are billed to his "home" network provider.

While roaming the subscriber is given a temporary number which he can be reached at by callers from inside or outside the network he is operating in.

Roaming is a convenience feature and to be useful must be turned on and off easily from the telephone itself or via dial line. Billing must be automatic and integrated with the "home" networks billing. The major draw back is that the temporary telephone number is not the same as the "home" network number., and that the caller trying to reach a cellular telephone-set must know the temporary number. Although some networks offer a call-forwarding feature which would allow the subscriber to program a call-forward service from his home network to the temporary number of the network where he is "roaming", this requires multiple steps for the subscriber.

In its IDEAL form, roaming would be transparent to the subscriber and to the anyone wishing to call him. It should be invisible to the user how the infrastructure management accomplishes the temporary registration, validation of home network credit and billing. It should also be possible to automatically allow the home network to route incoming calls to the telephone-set while it is "roamed" on another network.

HAND-OFF

"Roaming", should not be confused with the process of handing-off of users as they transit cells within the same network while "off hook" and engaged in a conversation. Some of the functions of roaming may be involved if this transit of cells occurs between adjacent networks. In concept it should be possible to make a call in San Francisco and drive to LA before the call is finished, necessitating the "hand-off" of the call, not just from cell-to-cell but also from one network provider to another.

The process of handing-off a subscriber who transits from one cell's coverage to another while maintaining the subscribers call in an uninterrupted manner is one of the essential features of the cellular network. The mechanics of this process are not trivial and require a significant amount of signaling between the cells and changing of frequencies at the telephone-set. How this process works is not important but the fact that the user is unaware of it (or should be unaware) is important. Hand-off should appear to be "seamless", a term which means "invisible to the user."

ANALOGIES TO WIRELESS LANS

WLAN's could be of two forms; public, and private. These networks could offer a number of service types, like connection oriented (circuit switched), and connectionless (packet switched), each of these could be synchronous, asynchronous or isochronous (time bounded). They may be simplex, half duplex or full duplex (as seen by the STA). The network must also be able to cater to the needs of the mobile (or nomadic) user and mobile devices¹. These networks may offer subscribers access points to other LANs or WANs.

Controlling access to the WLAN is more complex than it is with the wired counterpart, and as with a cellular telephone, the subscriber to a public WLAN may wish to use other public WLANs in a "roaming" mode. It is also conceivable that private WLANs would allow access to their resources for selected users on a temporary basis. More likely than not, as with cellular networks, the WLANs in any given area may overlap their coverage and a STA may be a registered subscriber to more than one of these overlapping WLANs. In any case a mechanism similar to the "registration" and "roaming" features of cellular telephone would be necessary. If the WLAN architecture is cellular in topology then there may also be the necessity of a cell-to-cell hand-off, and if the

¹note: the network cannot assume that the STA is attended by a human.

architecture allows for mobility between network providers during sessions then some of the features of roaming must also be incorporated in the hand-off process between networks.

WLANS however, may have more services and resources available which they may wish to limit access to, by casual "roaming" subscribers. It is clear that public network providers will require a billing function, and even private network providers will want accountability and statistics regarding network users and resource access. How WLANS will address this, or how they will verify the account of the "roaming" subscriber are issues for architecture and implementation.

It is clear that "registration", "roaming", "identification/authorization" are network administrative issues and have little to do with the MAC/PHY of the 802.11. However it must be noted and allowed for in the network sign-on/sign-off process, and protocol - it cannot be left to the upper layers or to individual implementations, not if, the WLAN is to be a universal standard for wireless infrastructures. Without these administrative function the mobile stations and their user will be greatly limited, and the network infrastructure provider, whether public or private, will be reluctant to offer access to services or resources which cannot be rationalized or where cost cannot be allocated on a per-use basis.

Cell-to-cell hand-off (in 802.11 terms, service area - to - service area transitions with open sessions) will be particularly important because of the coverage area constraints imposed by the power and frequency requirements which 802.11 must live within. It will also be important when operating in environments where building sizes are large and the equipment and /or people accessing the infrastructure are mobile over a wide area. examples; a tether-less robotic transport which must traverse the length of a warehouse or factory, the automated mail delivery robots which may move from floor- to-floor, not to mention equipment being transported by people where it is necessary to maintain constant communication while the individual moves over wide areas, such as patient monitoring in a health care environment.

The management of these transition must be part of the 802 standard, and may well be appropriately architected at or within the MAC /PHY layers, while providing information to layers above for use by other 802.x services.

TERMS

While it is easy to understand the terms of roaming, registration, identification, authorization and hand-off in the broad context of a cellular telephone analogy, it is when we try to state these concepts without pre-conceptions for the purposes of a definition, usable in the requirements document, we find the need to define a number of other ideas with new terms. One of the important terms will be the one which describes the agent which will implement some of these mobility services. Here the term ADMINISTRATOR will be used to differentiate it from the 802.1 network management functions, and DOMAIN to indicate that there is a composite of network segments which may be ADMINISTERED by an agent (somewhat analogous to the network provider). ADMINISTRATION differs from 802.1 network MANAGEMENT in two ways; one, it is mandatory; two, it must operate over the DS and directly manage the PHY in real-time (perhaps managing frequencies or code sequences, power levels, antenna switching or other PHY related service area functions.). STA states which are of concern to the ADMINISTRATOR are;

- mobility within a service area after sign-on but before a session is started
- mobility within a service area while a session is on-going
- inter service area mobility for both of the above cases
- mobility between services areas covered by different management(administrative) domains - again; in the cases above
- sign-off requirements and defaults

We could adopt new terms, SUCH AS:

- RANGING to mean transiting BSA- to-BSA while in session and
- ROVING to mean transiting management or administrative domains while in session., and
- LOITERING to mean mobile but remaining within a single (basic or extended) SA.
- STATIONARY to mean stations which do not have mobility as one of their attributes.

We could also describe the state of a MOBILE STA as being REGISTERED NOT SIGNED-ON, REGISTERED SIGNED-ON not in session, or SIGNED-ON in session. The "in session" term means the CF function is managing transmitter functions for the STA and is cognizant of the STA's need to maintain continuity while moving². The SIGNED-ON term would mean that a STA with a given 802 address³ is known to the CF of the BSA and that it has been identified as being a REGISTERED STA with AUTHORITY to operate in this ADMINISTRATIVE DOMAIN, therefore it is also a member of a BSS or ESS.

The term DOMAIN ADMINISTRATOR would indicate that the CF has a higher authority to interact with in terms of IDENTIFICATION of the STAs wishing to operate within the SA, this function could be an 802.1 service invoked at SIGN-ON by the CF. This DOMAIN ADMINISTRATOR, as contrasted with the network management of 802.1, would coordinate inter-service area HAND-OFF (caused when a MOBILE STA RANGES) and inter-domain HAND-OFFs (when a MOBILE STA ROVES). Unlike the 802.1 manager the DOMAIN ADMINISTRATOR would be a mandatory element of the infrastructure. The DOMAIN ADMINISTRATOR would use the DS to signal adjacent SA's during HAND-OFF. If the PHY is a radio-PHY the DOMAIN ADMINISTRATOR may well be responsible for frequency/code sequence assignments, power management, and antenna switching. It may also be required to keep track of connection oriented (circuit switched) services which operate independently of the CF controlling the connectionless services (contention type packet switched "channel").

Monitoring of LOITERING STAs would be the exclusive responsibility of the CF of the BSS. This responsibility may also necessitate the ability to locate, and track (with the eye to predicting the need to signal HAND-OFF coordination to the DOMAIN ADMINISTRATOR.)

recap;

- REGISTRATION would mean the process of recording the STA address with the DOMAIN ADMINISTRATOR.
- ROAMING would be a form of temporary REGISTRATION to all "visiting" STAs needing access to the CF.
- IDENTIFICATION is the function performed by the CF with the DOMAIN ADMINISTRATOR to determine if a STA should be AUTHORIZED to use the CF.
- AUTHORIZATION is the granting of permission by the DOMAIN ADMINISTRATOR for a STA to become a member of a BSS or ES
- SIGN- ON would be the process a STA uses to inform the CF that it wishes to use the CF's services, i.e. to join a BSS or ESS,
- SIGN-OFF would be the process where the STA notifies the CF that it is no longer active (transmissions and reception will cease).
- ADMINISTRATIVE Domain and Function refer to the entire realm of BSS's and ESS's and their CF's (whether or not they are interconnected), that make up a network wholly owned and managed by one entity whether public or private.
- DOMAIN ADMINISTRATOR is the agent which implements the ADMINISTRATIVE FUNCTIONS

There would also be inter-domain signaling to set up services for ROAMING and ROVING and to provide the cross-domain identification of the ROAMER and ROVER, again this would occur over the DS and a common carrier.

If you consider these twist to the architecture it becomes apparent that the infrastructure is more akin to a cellular DATA-PCS, than a simile of wired ethernet, however to require it to be less would be to assure incompatible proprietary infrastructures operating under the label of "802 standard." We must therefore place these function in the requirements document, along with adequate definitions constructed without too many preconceptions from our various industry orientations. Although it may be argued that these terms imply a specific architecture it is hoped that they will allow the architecture discussion to proceed with more common understanding.

²note: although session connotes connection oriented services or upper layer functions it is important to realize that in connectionless service bands the difference between the state of a STA which is attached to the network and idle, and a STA which is active, whether or not the activity is an upper layer "session", is important.

³note: it may also be necessary to have an additional "internal identifier" similar to the one used in the cellular telephone to provide an affinity to each of the STAs' possible registered networks, if they overlap in their coverage.

Regulatory and conformance testing will probably impose the additional demand that the device or station carry an external SERIAL NUMBER, MODEL NUMBER and MANUFACTURE IDENTIFICATION. There could be a need to manage the transmitting station within an enterprises premises by the external serial number. This may necessitate 802.1 services not now available.

4. Proposed definitions

- REGISTRATION - A process by which a STA 's ADDRESS is logged with the domain ADMINISTRATOR to allow it to be IDENTIFIED when SIGNING-ON.
- ROAMING - A form of REGISTRATION used for MOBILE STA's which will use a network on a temporary basis.
- ROVING - the act of a MOBILE STA of transiting from one ADMINISTRATIVE domain to another while SIGNED-ON and in session .
- RANGING - the act of a MOBILE STA which is transiting from one Service Area to another within an ADMINISTRATIVE domain while SIGNED-ON and in session .
- LOITERING - the presence of a MOBILE STA within a BSS or ESS while signed on and in session.
- STATIONARY STATION - a STA which does not have the attribute of mobility.
- MOBILE STATION - a STA which has the attribute of mobility .
- MOBILITY ATTRIBUTE - an indicator passed by the STA to the domain ADMINISTRATOR during REGISTRATION to indicate that the STA will be operated as a MOBILE STA.
- ADMINISTRATIVE DOMAIN - the realm of BSS's and ESS's which are wholly owned and managed as a single entity, whether public or private.
- -DOMAIN ADMINISTRATOR - the agent which manages the ADMINISTRATIVE FUNCTION of the AD.
- -ADMINISTRATIVE FUNCTION(s) - the set of functions which are the responsibility of the DA.
- HAND-OFF - the process of passing control of the MOBILE STA's activities from one CF to another, whether or not the CF's are members of the same ADMINISTRATIVE DOMAIN or not.
- SIGN-ON - the process a STA goes through to IDENTIFY itself to the CF, for the purposes of joining a BSS or ESS.
- SIGN-OFF - the process a STA goes through when notifying a CF that it is no longer active.
- IDENTIFICATION - the ADMINISTRATIVE FUNCTION which a CF uses to determine from the DOMAIN ADMINISTRATOR that a STA is REGISTERED.
- AUTHORIZATION - the ADMINISTRATIVE FUNCTION which the DOMAIN ADMINISTRATOR uses to notify the CF that a STA is REGISTERED.
- LOCATION FUNCTION - an ADMINISTRATIVE FUNCTION used find a STA which is SIGNED-ON.
- TRACKING FUNCTION - an ADMINISTRATIVE FUNCTION used by the CF to determine if a MOBIL STA is about to transit its Service Area.

- **INTER-DOMAIN FUNCTIONS** - are the set of functions use by the **DOMAIN ADMINISTRATOR** to coordinate the **IDENTIFICATION, AUTHORIZATION** and **HAND-OFF** function across **ADMINISTRATIVE DOMAINS**.
- **INTRA-DOMAIN FUNCTIONS** - are the set of functions used by the **DOMAIN ADMINISTRATOR** to coordinate the **IDENTIFICATION, AUTHORIZATION** and **HAND-OFF** functions across **Service Areas** within an **ADMINISTRATIVE DOMAIN**.
- **PUBLIC ACCESS INFRASTRUCTURES** - an 802..11 compliant **ADMINISTRATIVE DOMAIN** operated for public use.
- **PRIVATE ACCESS INFRASTRUCTURES** - an 802.11 compliant **ADMINISTRATIVE DOMAIN** operated for private use.

5. New Issues

The discussion above points up some new issues related to the infrastructure management of the 802.11 WLAN. These are:

- where will the intelligence for the **ADMINISTRATIVE** functions reside(i.e.; a server, in the "HUB", at the **ACCESS POINT**)?
- what is the nature of the "agent" needed to implement these functions (hand-off, roaming, etc.)
- what is the implication for ad-hoc networks, and can they co-exist in the presence of a public or private infrastructure.