Issue Identification: 4.4 (Topic: Network Types).

- Does the 802.11 standard will support geographic coexistence of multiple overlapping 802.11 networks?

Alternatives:

1) - Yes
2) - No

References:

1) - P802.11-93/40 - The Wireless Hybrid Asynchronous Time-bounded MAC Protocol

Arguments:

General:

1) - Method to accomplish this is not implied by decision to support it
2) - The issue cannot be equated to non-interference
3) Support cannot be constrained to mean guarantee

Pro:

1.1) - The WHAT protocol (see Reference #1) operates effectively even when there is no channel isolation for overlapping or adjacent BSAs. When traffic from different BSS is present on the same channel, STAs in the overlapping area behave as if their network is the union of the overlapping BSS. The result is that stations in overlapping areas perceive that their network is more congested that those in a single BSA. Of course this congestion can be reduced or eliminated if the PHY layer can provide channel isolation of adjacent BSAs.

Con:

Related Issue Identification:

Issue Originator:

Issue History:

January 1993: Date first opened.
March 1993: Alternatives #1 and 2 - Reference #1 - Argument_general #1 to 3 - Argument_pro #1.1 - Closure of the Issue (4.4) by endorsing Alternative #1; results: yes-23, no-0, abstain-0.

Issue Status: Close

Issue Identification: 4.5 (Topic: Network Types).

- Can a station be a member of an ad-hoc and non-ad-hoc network at the same time?

Alternatives:
1) - Yes
2) - No

References:
1) - P802.11-93/40 - The Wireless Hybrid Asynchronous Time-bounded MAC Protocol

Arguments:

Pro:

1.1) - There is a need for the standard to support this alternative.
2.1) - Multiple association has security impacts.
2.2) - At any point in time a STA is a member of one, and only one, BSS. A STA may be within range of both types of networks, but will participate in one or the other.

Con:

Related Issue Identification:
1) - 4.1 (Network Types)
2) - 4.3 (Network Types)

Issue Originator: Dave Bagby

Issue History:
January 1993: Date first opened.
March 1993: Alternatives #1 and 2 - Reference #1 - Argument_pro # 1.1, 2.1 and 2.2 - Attempt to close the Issue; failed in MAC group; result: yes-9, no-8, abstain-0.

Issue Status: Open

Issue Identification: 5.4 (Topic: Distribution Systems).

~~-Is the interface of the Distribution System is performed at:~~
- In which layer entity the interface of the distribution system is performed?

Alternatives:
1) - the MAC Layer
2) - the PHY Layer
3) - both MAC and PHY

References:
1) - P802.11-93/40 - The Wireless Hybrid Asynchronous Time-bounded MAC Protocol

Arguments:

Pro:
1.1) - There is no relation between the wireless PHY and the Distribution System (DS).

Con:

Related Issue Identification:
- 12.2 (Topic: Interfaces)

Issue Originator: John Corey

Issue History:
May 1992: Date first opened
March 1993: Reference #1 - Argument_pro #1.1 - Closing the Issue (5.4) by endorsing Alternative #1; result: yes-25, no-0, abstain-2.

Issue Status: Close

Issue Identification: 5.6 (Topic: Distribution Systems).

- What is the direction for the Association Service transaction?

Alternatives:

1) - From Station (STA) to Access Point (AP)
2) - From AP to STA
3) - Bidirectional

References:

1) - P802.11-93/9 - 802.11 DS Service Transactions
2) - P802.11-93/40 - The Wireless Hybrid Asynchronous Time-bounded MAC Protocol

Arguments:

Pro:

1.1) - Needed when Station (STA) is first powered on

1.2) - There is no need for a bi-directional service. If the Access Point (AP) causes a Disassociation, the Station can sign on with a different Access Point and cause a new Association. Only the Station knows which Access Point is the best one to choose for the new Association, so it does not make sense for an Access Point to cause an Association on behalf of a Station. If we require the Access Points to know about the real time signal strength of every Associated Station in relation to every Access Point; and communicate this information through the Distribution System in a timely manner, then we are making too many assumptions about the performance of the Distribution System. We cannot define the Distribution System; it already exists.

2.1) - See 'Re-association' in Reference #1

3.1) - Implied if association AP to STA decided to be necessary.

Con:

3.1) - See Alternative_pro #1.2

2.1) - See Alternative_pro #1.2

Related Issue Identification:

Issue Originator: Dave Bagby

Issue History:

January 1993: Date first opened - Alternatives #1 to 3 - Reference #1 - Argument-pro #1.1, 2.1 and 3.1.
March 1993: Reference #2 - Argument_pro #1.2 - Argument_con #3.1 and 2.1

Issue Status: Open

Issue Identification: 5.9 (Topic: Distribution Systems).

- How to determine that Access Points (APs) are present?

Alternatives:

1) - Discover:
   - Listen (APs beacon) - hard for ad-hoc networks
   - Ask (talk then listen) - may cause unnecessary traffic.
2) - Pre-configured knowledge
   - Disadvantages from installation and configuration viewpoints.

References:

1) - P802.11-93/9 - 802.11 DS Service Transactions
2) - P802.11-93/40 - The Wireless Hybrid Asynchronous Time-bounded MAC Protocol

Arguments:

General:

1) - The WHAT Protocol (see Reference #2) handle this in two ways:

a) Each MPDU that is transmitted by an Access Point is marked with a bit that indicates it was transmitted or relayed by an Access Point. A Station observing a Basic Service Set (BSS) that includes an Access Point will very quickly learn that the Access Point is present; and can attempt to sign on using a broadcast with the appropriate NETID.

b) When the network is idle, Access Points send out periodic Announce frames. Announce frames are also marked with the AP bit, so a receiving Station can distinguish an ad-hoc Basic Service Set from one that includes an Access Point.

Pro:

1.1) - Discover, Listen, if nothing is heard, then ask.

Con:

Related Issue Identification:

Issue Originator: Dave Bagby

Issue History:

January 1993: Date first opened - Alternatives #1 and 2 - Reference #1.
March 1993: Reference #2 - Argument_general #1 - Argument_pro #1.1

Issue Status: Open

Issue Identification: 6.2 (Topic: Security).

- Does the PHY layer performs or supports the security functions?

Editor's note: Ref: 78 (92/58R1)

Alternatives:

1) - Yes
2) - No

References:

1) - P802.11-93/28 - IEEE 802.10 Standard for Interoperable LAN & MAN Security

Arguments:

Pro:

2.1) - Multiple PHYs would most likely required multiple security implementations.
2.2) - Application of IEEE 802.10b would result in a media independent solution.
2.3) - IEEE 802.10b is an approved standard and allows for flexibility regarding Security functions (i.e. private to open system can share the same media (BSA).
2.4) - IEEE 802.10b permits interoperability with other 802 LANs employing it.

Con:

1.1) - See Aternative_pro #2.1 and 2.4.

Related Issue Identification:

Issue Originator:

Issue History:

May 1992: Date first opened
March 1993: Alternatives #1 and 2 - Argument_pro #2.1 to 2.4 - Argument_con #1.1 - Closure of the Issue (6.2) by endorsing Alternative #2; result: yes-22, no-0, abstain-2.

Issue Status: Close

Issue Identification: 6.3 (Topic: Security).

- How does unauthorized network access impact MAC throughput?

Editor's note: Ref: 1 (91/138) - Re-phrased 'Unauthorized network access impact on throughput' statement.

Alternatives:

1) - No direct impact

References:

1) - P802.11-93/28 - IEEE 802.10 Standard for Interoperable LAN & MAN Security

Arguments:

General:

1) - IEEE 802.10 protects against the ISO 7498-2 1988 threats of:
- Masquerade
- Replay
- Modification of messages.

Does not protect against the threats of :
- Denial of service; either intentional or unintentional (e.g. co-channel use, interference, lack of etiquette).

Pro:

1.1) - Unauthorized (failure of authentication) stations cannot access the network, therefore no direct impact on throughput.

Con:

Related Issue Identification:

1) - Issue 9.6 (Performance)

Issue Originator:

Issue History:

May 1992: Date first opened
March 1993: Alternative #1 - Reference #1 - Argument_general #1 - Argument_pro #1.1 - Closure of the Issue (6.3) by endorsing the alternative and transfer the issue to the 'Performance' (Topic 9) section of this document.

Issue Status: Close

Issue Identification: 6.4 (Topic: Security).

- How will Authentication and Registration be specified in the 802.11 Standard ?

Alternatives:

1) - Submission P802.11-93/8 (see Reference #1) provides an initial high level frame work for addressing wireless network security in general which includes Authentication and Registration.

2) - Submission P802.11-93/2 (see Reference #2) proposes a high level scenario of the Registration procedure taking place between an Access Point (AP) and a Station (STA). Security features such as Authentication, access control and data masking key exchange are addressed.

3) - Authentication and Registration procedures using 802.10b could be provided as an annex to 802.11. Possible implementation might use RSA, DSS, IS-54 or something else. Request submissions by interested parties on actual implementations consistent with 802.10b SDE.

References:

1) - P802.11-93/8 - Wireless Network Security
2) - P802.11-93/2 - Registration Scenarios for Wireless LAN MAC Protocol.
3) - P802.11-93/28 - IEEE 802.10 Standard for Interoperable LAN & MAN Security

Arguments:

Pro:

3.1) - Strong feeling within the committee that 802.10 will be adequate to address 802.11 Security issues.

Con:

Related Issue Identification:

1) - 6.1 (Security)
2) - 6.5 (Security)

Issue Originator: Larry Van Der Jag

Issue History:

July 1992: Date first opened
January 1993: Alternatives #1 and 2 - References #1 and 2.
March 1993: Alternative #3 - Reference #3 - Argument_pro #3.1

Issue Status: Open

Issue Identification: 6.6 (Topic: Security).

- Is there any additional work on Security that needs to be done by 802.11 in addition to the work that is done by 802.10 ?

Alternatives:
1) - Yes
2) - no

References:
1) - P802.11-93/28 - IEEE 802.10 Standard for Interoperable LAN & MAN Security

Arguments:

Pro:

2.1) - It is believed that document P802.11-93/28 (Reference #3) has answered that question, no, to majority of threats, but denial of services from Issue 6.3 still needs to be addressed, or this issue belongs somewhere else.

Con:

Related Issue Identification:
1) - 6.1 (Security)
2) - 6.5 (Security)
3) - 6.3 (Security)
4) - 6.4 (Security)

Issue Originator: Robert Crowder

Issue History:
July 1992: Date first opened
March 1993: Alternative #1 and 2 - Reference #1 - Argument_pro #2.1

Issue Status: Open

Issue Identification: 6.7 (Topic: Security).

- How does Re-association interact with Authentication?

Alternatives:

1) - Via third party Authentication service.
2) - IEEE 802.10 standard provides this interaction

References:

1) - P802.11-93/9 - 802.11 DS Service Transactions
2) - P802.11-93/28 - IEEE 802.10 Standard for Interoperable LAN & MAN Security

Arguments:

Pro:

1.1) - The standard should support the ability for a Station (STA) to ask the Distribution System (DS) to establish Authentication for itself to a requested set of Access Points (APs).

2.1) - The use of Security Associations set up in the Security Management Information Base, (SMIB) of 802.110 could provide for a way to effectively and efficiently handle re-associations for both authentication and privacy.

Con:

Related Issue Identification:

1) - 6.8 (Security)

Issue Originator: Dave Bagby

Issue History:

January 1993: First Opened - Alternative #1 - Reference #1 - Argument-pro #1.1.
March 1993: Alternative #2 - Reference #2 - Argument_pro #2.1

Issue Status: Open

Issue Identification: 6.8 (Topic: Security).

- How does Re-association interact with Privacy?

Alternatives:

1) - IEEE 802.10 standard provides this interaction

References:

1) - P802.11-93/9 - 802.11 DS Service Transactions
2) - P802.11-93/28 - IEEE 802.10 Standard for Interoperable LAN & MAN Security

Arguments:

General:

1) - Because the Privacy level can change dynamically, there is no gain by trying to pre-determine the Privacy level at the same time than third party Authentication.

2) - If a Re-association transaction includes the current Privacy level, it is very cheap to check that the new Access Point (AP) supports this privacy level.

Pro:

1.1) - The use of Security Associations set up in the Security Management Information Base, (SMIB) of 802.110 could provide for a way to effectively and efficiently handle re-associations for both authentication and privacy.

Con:

Related Issue Identification:

1) - 6.7 (Security)

Issue Originator: Dave Bagby

Issue History:

January 1993: First Opened - Reference #1 - Arguments-general #1 and 2.
March 1993: Alternative #1 - Reference #2 - Argument_pro #1.1

Issue Status: Open

Issue Identification: 6.9 (Topic: Security).

- Shall the 802.11 standard specify one or more publicly available privacy algorithms which all stations shall be required to support?

Alternatives:

1) - Yes
2) - No

References:

Arguments:

General:

1) - While support of 'all' privacy algorithms is ok, all stations are required to support a public algorithm.

2) - If (1) above is true, which algorithm (s) is the default? - possibly a 'null' security algorithm (see Argument_pro #1).

Pro:

1.1) - One privacy option shall be 'null'.

Con:

Related Issue Identification:

Issue Originator: Bob Crowder

Issue History:

March 1993: Date first opened - Alternatives #1 and 2 - Argument_general #1 and 2 - Argument_pro #1.1.

Issue Status: Open

Issue Identification: 9.1 (Topic: Performance).

- How will the standard address:
  a) - MAC throughput?
  b) - throughput probability?

Editor's note: Ref: 3 (91/138) - Re-phrase from 'Issues of throughput' statement and 'Other Functional Requirements Issues' list and 92/40 - re-phrase from 'Throughput probabilities' statement.

Alternatives:

1) - The throughput performance may be addressed via a an optional Data Compression function.

References:

1)- P802.11-92/123 - "Mathematica" Based Integrated MAC/PHY Performance Simulation Framework Including Capture Effect.
2) - P802.11-93/1 - Application of "Mathematica" Based Simulation Template to Demand Assigned MAC Described in IEEE P802.11-92/39 ("The IBM MAC Proposal").
3) - P802.11-93/29 - Wireless LAN MAC Protocol: Data Compression as a MAC Option to Improve Effective Throughput.

Arguments:

Pro:

1.1) - The function (compression) would be optional, at the MAC Layer, because it may be performed by higher layers.
1.2) - Any compression function will increase the [MAC] performance.

Con:

1.1) - Compression on a packet basis may not provide a very useful compression ratio.

Related Issue Identification:

1) - 29.1 (Simulation)
2) - 9.1 (Performance)

Issue Originator:

Issue History:

<u>May 1992:</u> First opened
<u>November 1992:</u> Reference and Related Issue.
<u>January 1993:</u> Reference #2
<u>March 1993:</u> Alternative #1 - Reference #3 - Argument_pro #1.1 and 1.2 - Argument_con #1.1.

Issue Status: Open

Issue Identification: 9.5 (Topic: Performance).

- Shall the 802.11 standard requires optional data compression at the MAC layer level?

Alternatives:

1) - Yes

References:

- 1) P802/11-93/29 - Wireless LAN MAC Protocol: Data Compression as a MAC Option to Improve Effective Trhoughput

Arguments:

General:

1) - If the function is good enough to warrant an option, why not be provided all the time? - the effect of compression on compressed data can become data 'expansion' - this is not an option but a feature which can be 'turned on/off'.

2) - If performed 'before' MAC in data flow, why is it a MAC option? - compression must be symmetrical and because of different vendor options, the compression function need to be in the MAC.

3) - Compression performed above MAC works with a larger data stream and thus more efficient.

4) - Requirement for public compression as first choice.

5) - Miscellaneous questions:

- impact of compression on transfer delay.
- interaction of compression and privacy - compression first, then cypher.
- compression imply the requirement for fragmentation facilities - do not know how much the data will compress.

Pro:

Con:

Related Issue Identification:

1) - 9.1 (Performance)

Issue Originator:

Issue History:

March 1993: Date first opened - Alternative #1 - Reference #1 - Argument_general #1 to 5

Issue Status: Open

Issue Identification: 9.6 (Topic: Performance).

- How does 'interference' impact MAC throughput?

Alternatives:

References:

Arguments:

General:

Pro:

Con:

Related Issue Identification:

Issue Originator: MAC Group

Issue History:

March 1993: Date first opened

Issue Status: Open

Issue Identification: 10.1 (Topic: Coordination).

~~- What is a Coordination Function (CF) ?~~

Editor's note: Ref: 17 (92/58R1)

- What Coordination Function (CF) will be specified in the standard?

Alternatives:

1) - A Distributed Coordination Function (DCF).

References:

1) - P802.11-93/40 - The Wireless Hybrid Asynchronous Time Bounded MAC Protocol.

Arguments:

Pro:

1.1) - A Distributed Coordination Function (DCF) should be specified as the default mode of operation. A DCF is simple to implement, sufficient for asynchronous service, and well suited to ad-hoc networks. A Point Coordination Function should be added as an optional extension when Time-bounded service is required. The WHAT protocol (see reference #1) is an example of this approach.

Con:

Related Issue Identification:

Issue Originator: Larry Van Der Jagt

Issue History:

May 1992: First opened
July 1992: Rephrase the Issue
March 1993: Alternative #1 - Reference #1 - Argument_pro # 1.1

Issue Status: Open

Issue Identification: 12.3 (Topic: Interfaces).

- What is the intelligence level at the MAC/PHY interface ?
Editor's note: Ref: 51 and 84 (92/58R1)

Alternatives:
1) Dumb interface
2) Smart interface
3) Half-dumb interface
4) Simple

References:
1) - P802.11-93/40 - The Wireless Hybrid Asynchronous Time-bounded MAC Protocol

Arguments:
Pro:
1.1) - Dumb is simple, easy to implement, assumed cheap.
1.2) - Dumb must, at least, detect Service Request type
1.3) - [Dumb] is desirable to have the PHY 'blind' to the type of data that passes thru it. - PHY must not be required to understand the meaning of bits that passe thru it.
1.4) - Minimum needs:
- Received signal quality
- Transmit level
- Handshake
- Desire to minimize DC power consumption

2.1) - Smart is flexible
2.2) - Smart may be required if the interface has options
2.3) - Smart may be required for one MAC for multiple PHY requirement
2.4) - Real time constraints motivate more smarts in the PHY
4.1) - A few generic primitives with parameters to control specific PHYs.

Con:
3.1) 'Half-dumb' should not be considered - 'Dumb is Dumb'

Related Issue Identification:

Issue Originator:

Issue History:

May 1992: First opened
November 1992: Alternatives #1 to #3, Arguments #1.1 to #1.4 and #2.1 to #2.4 and Argument #3.1.
March 1993: Alternative #4 - Reference #1 - Argument_pro #4.1.

Issue Status: Open

Issue Identification: 12.8 (Topic: Interfaces).

- Does a PHY independence layer need to be specify in the MAC ?

Editor's note: Ref: 52 (92/58R1)

Alternatives:

1) - Yes
2) - No

References:

1) - P802.11-93/40 - The Wireless Hybrid Asynchronous Time-bounded MAC Protocol

Arguments:

Pro:

Con:

Related Issue Identification:

- Issue 12.1 (Interfaces)

Issue Originator:

Issue History:

May 1992: First opened
November 1992: Related Issue ID.
March 1993: Alternatives #1 and 2 - Reference #1.

Issue Status: Open

Issue Identification: 17.3 (Topic: Addressing).

- What is the extent of Multicast ? ~~(Basic Service Set (BSS), Extended Service Set (ESS)).~~

Editor's note: Ref: 15 (92/58R1)

Alternatives:

1) - Basic Service Set (BSS)
2) - Extended Service Set (ESS)
3) - Both BSS and ESS

References:

1) - P802.11-93/40 - The Wireless Hybrid Asynchronous Time-bounded MAC Protocol

Arguments:

Pro:

3.1) - A Station should be explicitly control the scope of multicasts. The WHAT protocol (see Reference #1) provides this capability with the 'hierarchical' bit.

Con:

Related Issue Identification:

Issue Originator:

Issue History:

May 1992: First opened
March 1993: Alternative #3 - Reference #1 - Argument_pro #3.1.

Issue Status: Open

Issue Identification: 17.5 (Topic: Addressing).

- What is meant by addressing?
  ~~- Size ?~~
  ~~- Is IEEE 802 addressing ok ?~~

Editor's note: Ref: 66 (92/58R1)

Alternatives:
1) - Size
2) - IEEE 802

References:
1) - P802.11-93/40 - The Wireless Hybrid Asynchronous Time-bounded MAC Protocol
2) - P802.11-93/22 - Further Exploration of Transactions and Name Spaces

Arguments:

Pro:

2.1) - Wireless Stations should be identified by 48 bit unique IDs that are compatible with other IEEE 802 standards. All asynchronous service MPDUs carry the full 48 bit address in the WHAT protocol (see Reference #1). Time-bounded MPDUs use a short local identifier. However, the Call Setup message for Time-bounded connections contains the full 48 bit addresses of the source and destination.

Con:

Related Issue Identification:

Issue Originator:

Issue History:
May 1992: First opened
March 1993: Reference #1 and 2 - Argument_pro #2.1

Issue Status: Open

Issue Identification: 19.2 (Topic: Reliability).

19.2-A - Will the IEEE 802.11 MAC look like all other IEEE 802 MACs regarding delivery reliability?
19.2-B - How does Multicast affect this decision ?
Editor's note: Ref: 64 (92/58R1).

Alternatives:

19.2-A:

1) - Yes
2) - No

References:

1) - P802.11-93/40 - The Wireless Hybrid Asynchronous Time-bounded MAC Protocol

Arguments:

General:

19.2-A:

1) - Bit Error Rate (BER) explicitly defined in the PAR.
2) - BER is not delivery reliability.
3) - Undetected BER must be low; detected BER could be higher that other 802 MACs.

Pro:

19.2-A:

1.1) - It must provide comparable level of service to client software.
1.2) - Related to 1.1 above - must be good enough to not 'upset' the upper layer clients.

Con:

Related Issue Identification:

Issue Originator:

Issue History:

May 1992: First opened
March 1993: Alternative (19.2-A) # 1 and 2 - Reference #1 - Argument_general (19.2-A) #1 to 3 - Argument_pro (19.2-A) #1.1 and 1.2.

Issue Status: Open

Issue Identification: 19.5 (Topic: Reliability).

- What kind of error recovery mechanisms are to be incorporated into the MAC ?

Editor's note: Ref: 95 (92/58R1).

Alternatives:

1) - Positive ACK with low retries.

References:

1) - P802.11-93/40 - The Wireless Hybrid Asynchronous Time-bounded MAC Protocol

Arguments:

Pro:

1.1) - The 802.11 MAC should include a positive acknowledgement protocol with low level retries. This mechanism helps the MAC present approximately the same level of MSDU delivery reliability as other IEEE 802 protocols.

Con:

Related Issue Identification:

Issue Originator:

Issue History:

May 1992: First opened
March 1993: Alternative #1 - Reference #1 - Argument_pro #1.1.

Issue Status: Open

Issue Identification: 24.3 (Topic: PHY Types).

- How multiple PHY support for the MAC be specified ?

Editor's note: Ref: 28 (92/58R1).

Alternatives:

1) - In the MAC Layer

References:

1) - P802.11-93/40 - The Wireless Hybrid Asynchronous Time-bounded MAC Protocol.

Arguments:

Pro:

1.1) - The intelligence should be in the MAC layer. There should be a PHY specific sub-layer in the MAC to accommodate different wireless PHYs. One way to parameterize the interface is to provide a field in the MAC header that is used to pass PHY specific information across the MAC/PHY interface, and from MAC to MAC. The WHAT protocol (see Reference #1) follows this approach.

Con:

Related Issue Identification:

- 12.1 (Topic: Interfaces)

Issue Originator:

Issue History:

May 1992: First opened
March 1993: Alternative #1 - Reference #1 - Argument_pro #1.1.

Issue Status: Open

Issue Identification: 24.7 (Topic: PHY Types).

- Will the MAC standard specify the support of multiple PHYs transparently ?

Editor's note: Ref: 7 (91/138) - Re-phrase from the 'Support of multiple PHYs transparently' statement.

Alternatives:

1) - Yes
2) - No

References:

1) - P802.11-93/30 - Wireless LAN MAC Protocol: PHY Layer Transparency.

Arguments:

Pro:

1.1) - P802.11-93/30 describes how the MAC Protocol (described in P802.11-92/39) can be adapted in a straight forward manner to address several PHY layer types:

- Infra-red
- Spread Spectrum Direct Sequence
- Spread Spectrum Frequency Hopping
- Multi-channel Spectrum

Con:

Related Issue Identification:

- 24.3 (Topic PHY Types)

Issue Originator:

Issue History:

May 1992: First opened
March 1993: Alternatives #1 and 2 - Reference #1 - Argument_pro #1.1.

Issue Status: Open

Issue Identification: 24.10 (Topic: PHY Types).

- What modulation scheme will be used for Slow Frequency Hopping (SFH) PHY?

Alternatives:

Arguments:
Pro:

Con:

Related Issue Identification:

Issue Originator: PHY Group

Issue History:
March 1993: Date first opened

Issue Status: Open

Issue Identification: 25.1 (Topic: Channel).

- Will the standard provide a procedure to reserve medium channel capacity ?

Editor's note: Ref: 53 (92/58R1).

Alternatives:

1) - Yes

2) - No

References:

1) - P802.11-93/40 - The Wireless Hybrid Asynchronous Time-bounded MAC Protocol.

Arguments:

Pro:

1.1) - The standard should provide the ability to reserve the medium. The WHAT protocol (see reference #1) uses this technique to allow Time-bounded MPDUs to have higher priority media access than asynchronous MPDUs.

Con:

Related Issue Identification:

Issue Originator:

Issue History:

May 1992: First opened

March 1993: Alternatives #1 and 2 - Reference #1 - Argument_pro #1.1.

Issue Status: Open