IEEE P802.11
Wireless LANs

TGe Requirements

Date:

July 5, 2000

Author:

Tim Godfrey
Intersil
Phone: 913-706-3777
Fax: 913-664-2545
e-Mail: tgodfrey@choicemicro.com

General Requirements

Any changes to the standard must be optional. This standard can not make a device conformant to the existing 802.11 standard non-conformant.

Any changes to the standard must remain compatible with legacy equipment (both APs and stations, and both DCF and PCF modes).

Association decisions must remain a policy decision of the AP or station and must not become requirements in the standard. IE, decisions to accept or reject association requests or admit association requests are outside the scope of the standard.

Changes to frame formats must be compatible with existing formats.

Capabilities must fit in remaining bits of CIF

Extensions to existing frames must use the information element data structure

New frame subtypes of existing types should be used in preference to the currently reserved fourth frame type.

New frame formats should be kept to the minimum required to meet the requirements.

Functional requirements must be fully specified

Requirements must be stated in measurable terms and units.

Minimum acceptable functionality, to be used as a gate for proposals.

Requirements for delivery of multimedia data streams must be related to known data types/rates and human perception of error/loss.

{we will generate a list of specific applications, performance numbers and source standards to be inserted here}

Support for direct STA to STA communication.

Provide a mechanism to mitigate the effects of interference between overlapping BSS's that are not a part of the same ESS, while not compromising security mechanisms.

Dynamic Frequency Selection (DFS) per CEPT.

Transmit Power Control (TPC) per CEPT.

Allows for migration and duplication of Distribution Services.

Minimal increase in complexity, while meeting other requirements.

External Requirements

Applications

Support for the traffic loads listed in the application scenarios specified in document 00/143.

{minimum gating application requirements, with values and sources}Higher Layers

The QoS definition should be higher layer agnostic.

Accept the indicates and requests of 802.3ac (VLANs), and add to it as appropriate for mobility and security and regulatory compliance.

Support the Inter Access Point Protocol recommended practices being developed by 802.11 Task Group F.

Support for terminal assisted handoff decisions (to insure media stream can be handled by new AP before disconnect).

Support for load balancing within the ESS.

Should adhere to existing or upcoming IETF standards.

IETF and 802.1 QoS support.

Do not duplicate functions provided by higher layer standards, except where the nature of the wireless medium breaks an assumption of the higher layer standard.

QoS Requirements

Corrections to the PCF, such as those identified by NWN and Philips, as well as those that may be identified during further design of the protocol to meet the QoS requirements must be incorporated. {refs to papers}

If the PCF as it is currently defined is used, the use of the isochronous extension enabled by 802.11b is preferred, adding an external scheduling mechanism and the minimal necessary connection/bandwidth negotiation management frames.

Extending the MAC Management SAP may be necessary to provide the needed indications and requests to support an external scheduler, i.e., something that is outside of the scope of the standard.

The current MAC data interface is sufficient to support the necessary data scheduling at both the AP and station.

Support for multiple priorities and classes of service.

Support for Class of Service three years in the future

Support for QoS Streams and bursty data concurrently.

Support for "toll quality" voice, audio, and video streaming.

Support for multiple simultaneous streams with differing priority and class requirements.

Support for interactive data streams.

Support for dynamic bandwidth allocation and/or reservation.

Support for classes of service where acknowledgement is not mandatory.

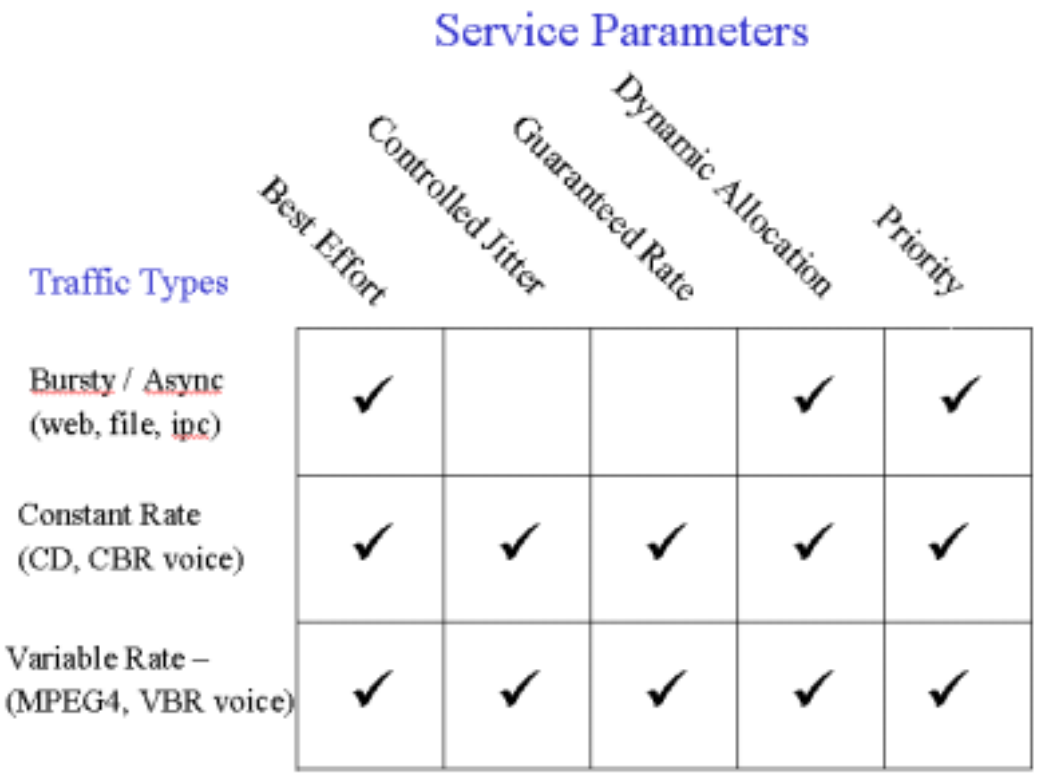

Figure 1 QoS Taxonomy

Security Requirements

General

All security extensions must be able to be used in both independent and infrastructure BSSs. {TBD Jesse Walker}

The standard must add at least one extension to the authentication algorithms that provides mutual authentication in both Infrastructure and Independent BSSs.

In the standard, security requirements are independent of QoS requirements. However, implementers should be aware of the potential interactions.

The extensions to the standard should not be constrained by QoS requirements.

It is an implementer decision as to which algorithms are to be used and whether that choice is compatible with QoS requirements.

Authentication

Security framework must prevent unauthorized authentication or re-authentication with an AP as those terms are defined within the 802.11 specification.

Security framework must be able to prevent unauthorized access by unauthenticated peers over the link.

Security framework must allow for mutual authentication of STA and AP.

Security framework authentication mechanisms must fit within the designated multi-media authentication and re-authentication time budget.

Security framework should make no assumption whether peer authentication is machine or user authentication, as different organizations will establish different policies regarding who or what is authenticated.

Privacy

Security framework must protect network traffic from eavesdropping to a reasonable level compatible with the state of the art.

Security framework must allow for authentication of the source of each packet, to prevent link hijacking or undetected insertion of rogue packets into the link.

Security framework must preserve the security characteristics of content streams.

The security extensions must not build in support for application layer protections mechanisms, i.e. SDMI, CSS, or other application content protection systems.

Keys

Security framework must allow key distribution or derivation of per-link or per-session keys

Security framework must strongly protect keys and passwords from recovery by eavesdropper

Extensibility, Compatibility, and Interoperability

Negotiation of authentication and privacy algorithms must be incorporated.

The following negotiations must be supported:

1. authentication algorithm

2. privacy algorithm

3. data integrity algorithm

4. key establishment algorithm

5. one way hash function for sub key derivation algorithm

6. key expiration

Negotiation must take place before authentication is complete.

Inability to complete negotiations must cause a failure to authenticate.

All extensions to the standard must use the current authentication frame format.

No additional fixed fields may be added to the frame format.

All extension to the frame format must be done using one or more information elements.

Modifications to the content or meaning of existing fixed fields must be compatible with legacy equipment.

A flexible mechanism for adding both authentication and privacy algorithms must be incorporated, so that the standard does not need to be revised to use new algorithms in the future.

Existing algorithm identifications from other standards should be used where applicable.

The standard should specify one set of algorithms as mandatory when security extensions are implemented.

Security framework must not compromise (i.e., break the security of) existing industry standard network user authentication methods and techniques used within the framework.

Security framework must coexist with existing industry standard network user authentication methods and techniques (e.g., RADIUS-based authentication).

Security framework must scale to:

Simple, "self-managing" or "unmanaged" environments (etc., home, SOHO)

Ad hoc wireless LANs

Enterprise environments (e.g., office campuses, factories)

Public environments (e.g., hotels, public services)

Implementation and Complexity

Security framework should cause minimal computational expense consistent with meeting other requirements.

Security framework should use public and/or standard algorithms to the greatest extent possible.

Security framework should minimize the number of mandatory cryptographic algorithms.