Whitecap™ 2 Wireless Network Protocol White Paper

EXECUTIVE SUMMARY

Today's home networking applications and services require a wireless protocol that enables multimedia-capable, easy to use, and reliable home networking products. Factors driving the requirement for multimedia include the proliferation of digital appliances and multimedia content (e.g. digital video recorders, digital set-top boxes, MP3 players), the deployment of integrated broadband services (e.g. high-speed Internet access, video on-demand, voice over IP), and evolving personal computer applications (e.g. multiplayer gaming, personal videoconferencing). In fact, the catalyst to driving mainstream home networking penetration and adoption is a home network that includes the ability to support entertainment- and communications-oriented (i.e. multimedia) content.

Many of the technologies being used for home networking have simply migrated from the data-centric enterprise world. However, home users (i.e. consumers) have a different set of requirements than enterprise users, and products originally designed for the enterprise environment do not satisfy these requirements. These requirements fall into three key areas that serve to characterize the "goodness" of a wireless home networking solution:

- Multimedia and Quality of Service (QoS) Support-for distributing high-fidelity content (e.g. streaming audio, video, etc.)
- Ease of Use-for setting up and operating the network
- Reliability-for sustained operation and resistance to adverse environmental conditions and household interferers (e.g. microwave ovens, cordless phones)

The Whitecap™ protocol was designed by Cirrus Logic specifically to enable home networks that support these requirements. The protocol efficiently manages data transmissions on a network of heterogeneous digital devices and content. Devices include PCs, TVs, DVD players, web pads, broadband modems, residential gateways, digital set-top boxes, digital video recorders and other emerging information appliances and servers. Whitecap is particularly well-suited to extending the broadband experience and preserving the quality of service delivered by broadband service providers. Furthermore, Whitecap can handle bursty data communication traffic while simultaneously streaming multimedia content (video and audio).

As part of Cirrus Logic's "embrace and extend" model, our core Whitecap technology has evolved into a second generation offering, called Whitecap™2. Whitecap2 "embraces" IEEE 802.11 wireless industry standards-for Wi-Fi (802.11b) compliance and interoperability-and also "extends" 802.11 to address the unique requirements of the home-multimedia and QoS support, ease of use, and reliability. In fact, significant elements of Whitecap2 have been incorporated in the latest IEEE 802.11e specification, which adds multimedia and QoS support to the 802.11 standards. Whitecap2 is the industry's first embodiment of core 802.11e technology, and, as 802.11e moves toward a fully ratified standard, Whitecap2 provides the best migration platform towards this standard.

The following table summarizes Whitecap2's current features and benefits, which are detailed in this document.

Feature	**Implication**	**Benefit**
Wi-Fi Compliance	Certification of interoperability with all Wi-Fi (802.11b) products	Provides interoperability in environments where Wi-Fi is installed
Dynamic Stream Support	Contention-free access for deterministic behavior and predictable latency, unlike collision-based access mechanisms Support for multiple simultaneous streams Dynamic allocation of resources to streams	Provides mechanism to deliver multimedia content (including video, audio, voice, and data) through a wireless network Delivers higher sustained usable throughput Maximizes utilization of available bandwidth Provides foundation for Parameterized QoS
Parameterized QoS	Resource allocation for each stream based on bandwidth, latency, and jitter requirements Deterministic allocation of resources, unlike priority-based QoS	Allows differentiation for different types of content and services Supports multiple content streams with consistent, predictable results Preserves quality of broadband stream entering home
Peer-to-Peer (Mesh) Topology	Direct communication between devices even when central node or access point exists	Maximizes utilization of available bandwidth Maintains multimedia and QoS performance
Delayed Acks	Maximizes payload efficiency by deferring acknowledgement packets Minimizes overhead for network access and housekeeping	Delivers higher usable throughput
Coordinator Redundancy	Coordinator responsibility automatically assigned and handed off to alternate nodes	Ease of use Improves reliability and eliminates single point of failure
Open Enrollment	Allows wireless nodes to grant network access to standalone wireless devices Permits standalone wireless devices to obtain updates on-air	Ease of use for adding and maintaining standalone devices Avoids complex configuration
Protocol/Firmware Update	Ability to update nodes with latest protocol revisions and new features	Scalable to add new features Allows forward/backward compatibility Provides migration path as standards evolve
Forward Error Corrections (FEC)	Corrects corrupted content “on the fly”	Improves multimedia performance Provides interference immunity Increases the operating range
Channel Agility	Network automatically operates on channel with least interference	Avoids interference without user intervention Improves reliability Ease of use

Security Network and device authentication 40-bit WEP encryption	Nodes must be authenticated before granted access 40-bit encryption provides privacy equivalent to wired networks	Provides privacy and security

NEEDS OF HOME NETWORKING APPLICATIONS

Today's home networking applications are driving the need for a high performance, wireless network protocol with high usable speed (high network throughput) and isochronous, multimedia-capable services. These requirements are not addressed by existing contention-based networking technologies found in the enterprise today.

1. Home Networks Incorporate Multimedia

A primary driver for multimedia support in home networks is the proliferation of new digital consumer electronic devices. These devices include digital set-top boxes, digital video recorders (DVRs), DVD players, digital audio/MP3 players and jukeboxes, DBS systems, digital TVs and flat-panel displays, web pad, sand multimedia PCs. For example, the worldwide installed base of digital set-tops is projected to increase from 68 million units in 2000 to 337 million by 2005. Similarly, the installed base of DVRs is expected to expand from under 1000 units in 2000 to over 42 million by 2005.

Another key driver of this requirement is the deployment of digital multimedia content. The home network (Figure 1) will have to support all types of digital content, including both local content (e.g., DVD/DVR video, MP3 audio) and integrated broadband services (e.g. video on-demand, IP telephony, streaming media). This content is multimedia in nature, encompassing video, audio, voice, and data. Internet multimedia broadcasting is already prevalent. By the end of 2004, more than 48 million U.S. households are projected to pay for access to multimedia broadband service. Over this same time frame, the number of cable telephony subscribers is expected to exceed 20 million, and the number of video on-demand subscribers will exceed 30 million.

The ability to support multimedia is the "killer app" that will drive the mass adoption of home networks. Therefore, a home network must support the co-existence of batch data (print jobs, file transfers) and isochronous content (video, voice, audio). Consumers need to choose products today that will provide the foundation for multimedia network services.

2. The Need to Preserve High-Speed Broadband Internet Access

The desire for faster Internet access is driving the mass deployment of high-speed broadband access, such as cable, xDSL and satellite.

Broadband service providers are targeting and delivering bandwidth speeds in excess of 6 Mbps. Consumers need a high performance, wireless network to preserve, and not bottleneck, high-speed broadband Internet access among devices. As noted above, moving forward in the future, these high-speed connections will deliver integrated services encompassing video, audio and voice in addition to high-speed data, creating even more of a requirement for a high bandwidth, multimedia-capable home network infrastructure.

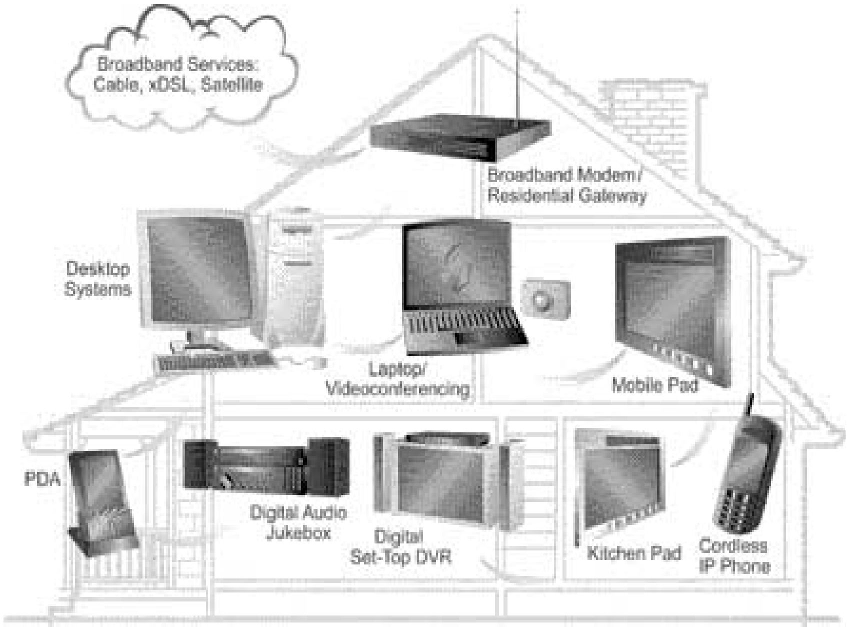


Figure 1. Multimedia-Capable Home Network

3. Networking Perspectives: Home vs. Enterprise

Home networking differs from enterprise networking in a variety of ways that influence the ultimate success of provided solutions. These differences include:

- Technical Expertise-Networking knowledge in the home is minimal, as opposed to a dedicated network administrator in the enterprise environment.
- Application Usage Model-Enterprise networking has typically focused on printer and file sharing among PC's, while applications driving the need for networking in the home are more entertainment-focused and more likely tied to service provider offerings-multimedia content distribution, broadband connection sharing, gaming, etc.
- Cost Sensitivity-There is more cost sensitivity in the home environment with both home users as well as consumer electronics companies and broadband service and equipment providers.
- Device Support-The enterprise environment consists of PCs and printers while the home environment is being bombarded with an assortment of digital devices that could potentially enjoy the benefits of a network: PCs, TVs, set-top boxes, web pads, DVRs, etc.
- Structural Variables-A standard home typically sits on a ¼ acre lot, with wallboard walls, wooden frames, and multiple smaller rooms, while the enterprise typically consists of much larger structures, more open spaces, roaming over wider areas, and mandated locations for electronic equipment. The home is an "unmanaged" environment in the sense that there is no control over equipment location in the home. Deployment in an enterprise environment is planned for best performance.
- Environmental Factors-Specifically regarding wireless transmissions, the home can be a much harsher environment with appliances such as cordless phones, microwaves, and metal ceiling fans that are much less common in the enterprise environment.

WHITECAP2: DESIGNED FOR HOME NETWORKING NEEDS

Two wireless networking technologies with the same raw speed can have very different performance and operating characteristics due to MAC (medium access controller) differences. Whitecap2 is specifically tailored for the home with the following features:

1. Complete Multimedia Support

- Whitecap2 provides superior throughput to support distribution of high-fidelity content, such as high bit-rate MPEG-2 (used in DVD titles and DVR video). Whitecap2 manages the transmission of such content at a higher bit-rate threshold and with higher quality due to the Dynamic Stream Support and Contention-Free Access architecture, while transmission in a data-oriented network (802.11b) faces pervasive skips and pauses. Dynamic Stream Support utilizes available bandwidth more efficiently than traditional 802.11 networks and provides for dynamic bandwidth allocation/management in an efficient manner. In a Contention-Free Access implementation there are no collisions as in a CSMA network, and each stream receives its required bandwidth-no more, no less. This allows multiple simultaneous streams and combinations of video and data streams from multiple nodes to coexist-something a traditional CSMA (collision based) 802.11b network cannot support.
- Whitecap2 is QoS infrastructure-enabled, which means that it allows Parameterized QoS support. Allocation of network resources for each stream is based on bandwidth, latency, and jitter requirements. This approach offers significant improvement over priority-based QoS mechanisms that do not provide deterministic allocation of resources. However, prioritized QoS can also be supported in a parameterized QoS implementation.
- A Peer-to-Peer (Mesh) Topology creates a network where devices communicate directly with each other. Even when a central node or access point exists in the network, payload traffic is not forced to transit through that device, which would reduce the total effective throughput.
- Delayed Acknowledgements improves the payload efficiency and minimizes overhead for network access and housekeeping by deferring acknowledgement packets, thus increasing the bandwidth available for multimedia transport.

2. Ease of Use

- The Coordinator Redundancy function allows continued operation even if the coordinator node within the network fails or is turned off. Whitecap2 identifies alternate coordinators on the network and automatically transfers the coordination function to one of those nodes.
- Open Enrollment allows "faceless" devices with no input mechanism, such as Ethernet bridges or access points, to be authenticated over the air from any authorized node on the network. The user can chose to grant or deny access based on the device.
- Wi-Fi Interoperability with 802.11b devices is an important feature of Whitecap2. It allows Whitecap2-based products to access Wi-Fi compliant devices deployed in public spaces such as airports, schools, hotels, conference centers, libraries, etc. Another key benefit is the ability for users to bring home their laptops from work and interoperate with their home network.
- Firmware Update is available for Whitecap nodes and allows users to install future firmware enhance-

ments and upgrades. Upgrades ensure scalability with new services and reduce device obsolescence. For "faceless" devices, firmware updates can be done over the air.

3. Reliable Wireless Delivery

- Non-delay sensitive streams such as video and audio cannot be retransmitted since a few dropped frames can severely diminish the quality and user experience. Forward Error Correction (FEC) recovers data "on the fly" and effectively increases the usable throughput. In unpredictable environments such as homes, this ensures consistent, quality performance and increased operating range.
- Whitecap2's Channel Agility feature can identify and switch network operation to the channel with the lowest packet error rate. If the connection between the coordinator and client(s) is broken, or the coordinator redundancy deems the bit error rate to be too high, the network will change channels.
- Security is also key in the home network. To avoid unauthorized access, the Whitecap2 protocol follows a strict authentication procedure before a connection is granted. Each Whitecap2 network is identified by a unique 16-bit subnet ID. The subnet ID is a field in the Whitecap2 protocol header and is unique to a specific network. Packets with the incorrect subnet ID authentication are dropped and denied access to all devices on the network. The Whitecap2 protocol subnet ID provides reliable security by exercising security on a packet-by-packet basis. WEP encryption algorithm extends the security to each frame transmitted over the air.

Whitecap2 provides the foundation to preserve QoS for service providers and a smooth migration platform towards the 802.11e implementation. Overall, Cirrus Logic's technology provides the performance to support current and emerging digital content types. Whitecap2 is not restricted to the 2.4 GHz operating frequency and can be easily implemented along with the 802.11a (at 5GHz frequency) PHY.

HOME NETWORK INFRASTRUCTURE REQUIREMENT

Given the unique characteristics of home networking outlined above, it is not realistic to expect an enterprise solution to fill the needs of the home network. In order to meet the needs of the home, a home network solution must address the following requirements:

Multimedia/Quality of Service Support

- High net throughput for supporting high-fidelity content, such as video transmission
- Efficient bandwidth allocation/usage to support multiple simultaneous content streams (also known as Traffic Category in the IEEE 802.11 Specifications)
- Support for isochronous streams (video, audio, voice)
- Predictable latencies to allow bandwidth allocation to be managed effectively
- Peer-to-peer communication-any device should be able to send and receive from any other at full performance levels

Ease of Use, Reliability, Robustness

- Easy installation with minimal user intervention
- Avoidance of in-band interferers

- Uncorrupted transmissions (no retransmitting content) to support isochronous streams
- Security to prevent unauthorized access and protect content
- Network coverage throughout all parts of the home

Scalability

- Firmware upgrade to support new network features and/or services
- Consistently high performance as additional devices are added
- Price/performance value for the consumer

Standards Compliance

- Wi-Fi (802.11b) compliant-interoperability with other Wi-Fi devices/networks
- Forward interoperability path for compliance with 802.11e

WHITECAP2 PROTOCOL KEY FEATURES

Cirrus Logic's first generation network protocol, referred to here as Whitecap1, addressed the immediate home networking needs for multimedia support, ease of use, and reliability. Our latest version, Whitecap2, adds Wi-Fi (802.11b) interoperability, while maintaining support for core Whitecap's home-oriented features. Whitecap2 also offers full backwards compatibility with Whitecap1-based devices.

As indicated previously, Whitecap2 encompasses the Wi-Fi protocol and Cirrus Logic's innovative multimedia and quality of service (QoS) extensions. Each Station (STA) in an Independent Basic Service Set (IBSS) can operate in either the Wi-Fi Mode or Multimedia (MM) Mode.

1. Wi-Fi Compliance

The Wi-Fi networking protocol that is part of Whitecap2 is Wi-Fi 2001 compliant. It is implemented upon the IEEE 802.11b standard and supports functionality as both a station and an access point. The features provided for Wi-Fi operation are listed below. (Please refer to the IEEE 802.11b Specification and the Wi-Fi System Interoperability Test Plan for additional details.)

- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) with random back-off
- 2.4 GHz, Direct Sequence Spread Spectrum (DSSS)
- Multiple rate support of 1, 2, 5.5, and 11 Mbps
- Support for channels 1-11 in the 2.4GHz band
- Sub-net identification, SSID (Service Set ID)
- Device authentication
- Support for open system authentication
- 40-bit WEP (Wired Equivalent Privacy) key security
- Roaming support
- CRC error detection

- Support for power management
- MAC-level acknowledgements
- RTS/CTS support
- NAV (Network Allocation Vector) Management
- Fragmentation and de-fragmentation
- Active and passive scanning
- Duplicate detection and rejection
- Support for broadcast and multicast frames
- Timestamp synchronization
- DCF (Distributed Coordinator Function)
- CF-aware (Wi-Fi 2001-aware of communications in the PCF time domain)
- Support for both infrastructure and ad-hoc mode (Wi-Fi 2001-ad-hoc interoperability)
- Beacon generation in ad-hoc mode

2. Multimedia and QoS Extensions

The Multimedia Mode in Whitecap2 was designed to enable home networks that address the consumer's need for multimedia support, ease of use, and reliability. Unlike other wireless networking protocols, Whitecap2 was designed from the ground up to accommodate and transmit all forms of multimedia content-including video, audio, voice, and data-in a noisy home environment (Figure 2 on page 9).

Whitecap2 is designed to work with leading edge, wireless digital radio technology to deliver the highest network utilization. The network architecture, services, and packet structure in Whitecap2 have been streamlined to minimize overhead and enable greater efficiency for multimedia transmission. Whitecap2 is designed to easily support various types of network devices, including desktop and mobile PCs, as well as non-PC devices such as wireless bridges, digital set-top boxes, digital video recorders, residential gateways, Internet phones, mobile web pads, and digital audio servers.

Whitecap2's key features enable high performance, wireless multimedia transmission that meets the needs of today's home environment. Current features in Whitecap2 include:

3. Peer-to-Peer (Mesh) Topology

Cirrus Logic's Whitecap2 protocol has a peer-to-peer (or mesh) topology that allows devices to communicate directly with each other-devices don't need to talk through a single device or server even if a central device (e.g. bridge/access point) exists in the network, as is the case with standard 802.11 networks. The network architecture based on a master-client relationship is enhanced to support peer-to-peer communications between the different clients on the network. This is achieved through the shadow-client mode. A shadow client is defined as a client with exactly the same data input as any of the currently online client but with its own separate command channel.

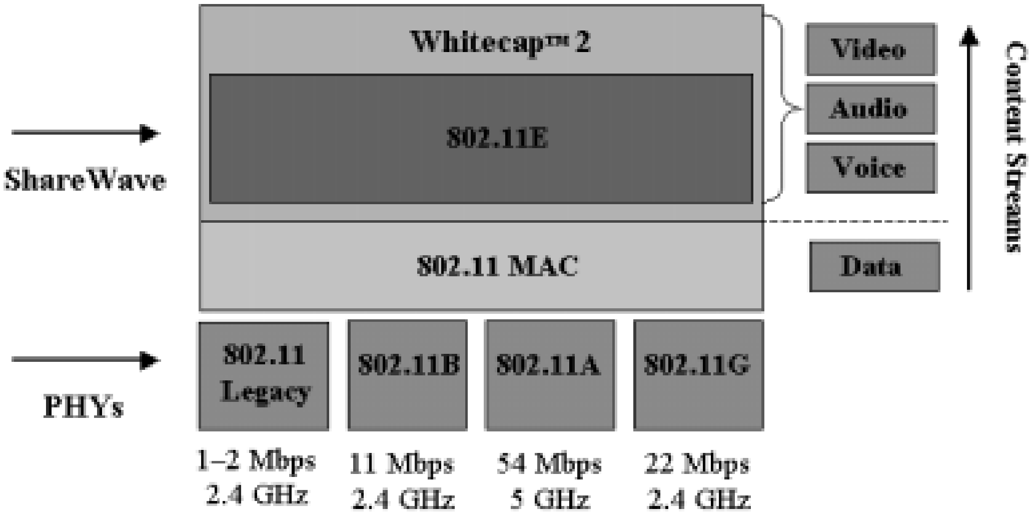


Figure 2. Whitecap Content and PHY Support

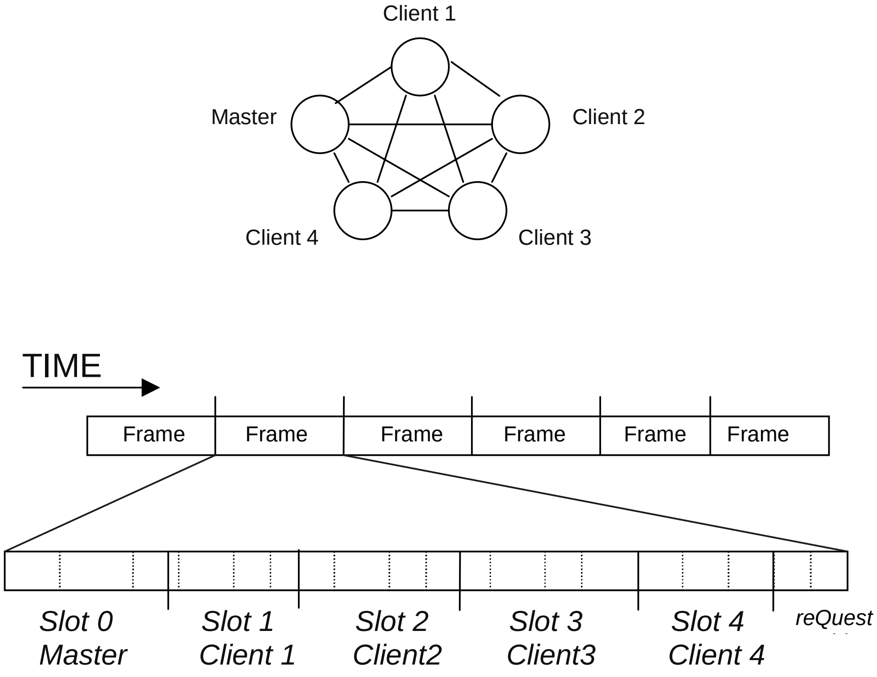


Figure 3. Slotted Access Architecture

4. Dynamic Stream Support / Contention-Free Access

Unlike contention-oriented protocols, such as CSMA, the Multimedia Mode extension is a connection-oriented network protocol that utilizes a Contention-Free Access mechanism enabled by a Point Coordination Function (PCF). Network bandwidth is slotted and shared among the multiple streams of network traffic. Each slot corresponds to each of the devices on the network. The Whitecap2 network assigns a coordinator function to a node that is responsible for transmitting periodic beacons (time reference) to synchronize clients. The coordinator also allocates bandwidth and polices traffic when devices transmit on the network.

Each node that needs to transmit is assigned a particular slot within a network frame. A network frame is defined as the duration between two transmissions from the coordinator device. The PCF assigns and dynamically adjusts slots based on the bandwidth needs of each node on the network (Figure 3 on page 9).

The contention-free access architecture preserves packet sequence and also provides the foundation for advanced QoS features such as priority services and parameterized QoS. Note that, as already mentioned in section 2.4, prioritized services are a subset of the parameterized, complete set of service differentiation.

Transmitted data has a four-layered hierarchy (Figure 4). Network frames are transmitted at even time intervals. The coordinator, depending on the number of clients and their bandwidth requirements, divides a network frame into the appropriate slot sizes. Each slot is capable of supporting one or more streams (audio, video, and data streams) that can be directed to any node in the network.

Parameters such as network frame size, wait time (time after beacon before client can transmit), transmission slot duration, etc., are provided to the client from the coordinator to maintain synchronization.

The first stream in a slot is dedicated as the command channel, which is primarily used to communicate client bandwidth requirements to the coordinator. Consequently, the network slot duration and the duration of each stream can be dynamically adjusted in real-time to ensure the best possible bandwidth utilization. This can happen when a new client comes online or a new application is launched at a client. Bandwidth requirements of the coordinator are treated the same as any other device.

Variable-length packets transmit the data that compose each stream, making the protocol very well suited for Real-Time Polling Services (rtPS) such as Audio/Video Streaming. Whitecap packets have 3 main parts: the header, the payload, and the ECC (Error Correction Code) bits. The header includes information such as Subnet ID, packet position in the stream, packet type, etc. The packet body contains the actual information (video, audio, data) for the related stream type or commands in a command packet. The CRC/ECC field contains the error correction information.

Note that only the Command (Signaling) frames include a CRC field and an ECC field. Payload frames contain only ECC bits; CRC is not applied while operating in Multimedia Mode.

The "reQuest" slot is reserved to allow new clients to automatically join, or "hot insert" themselves without impacting the performance of existing nodes. The new clients can insert a request packet to login to the network. If the coordinator does not respond to a client's requests, the client times out and switches channels. Upon reception of a connection request from a client device, the coordinator can authenticate the device and allocate a session ID. The coordinator node then adds the client to the online service table.

The coordinator device maintains the online service table consisting of all client device ID's and the bandwidth allocations. This information is used in deciding connection to a new client. As stated, the major responsibilities of a coordinator are for client authentication, bandwidth allocation, network frame synchronization, and selection of a quality channel for operation. Any device that has access to this and has the appropriate processing power can be a coordinator redundancy device. Parameters that the coordinator can determine include network frame size, number of online connections, transmission duration of each device, etc.

Dynamic Stream Support provides several benefits, including:

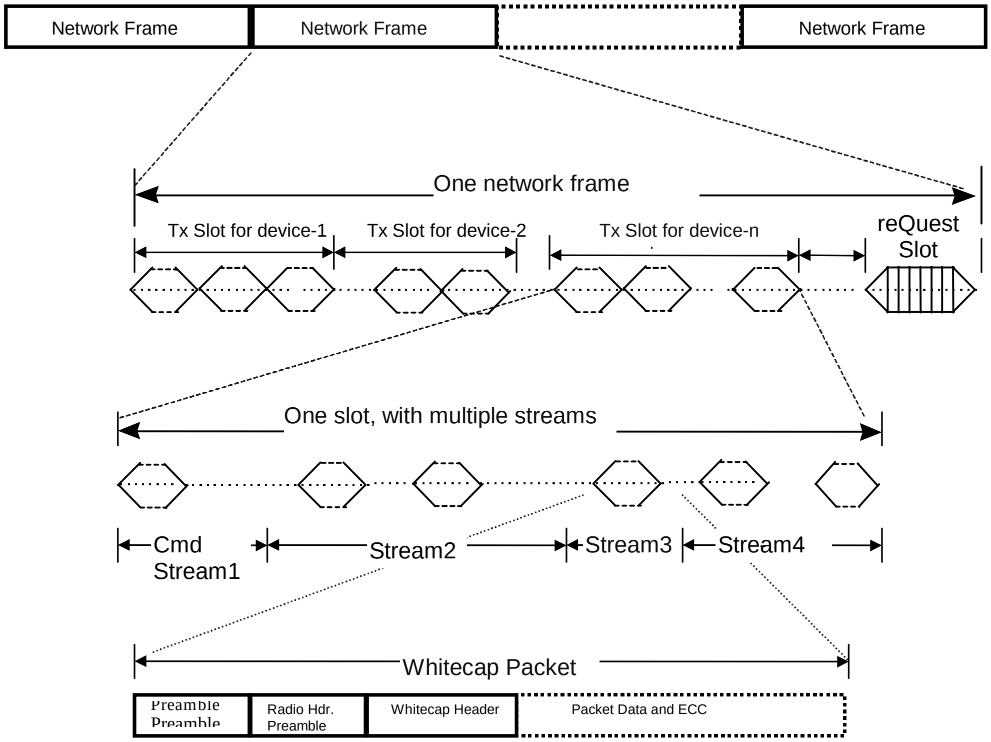


Figure 4. Dynamic Stream Support data structure hierarchy

High network performance and efficiency (high usable network throughput)
While operating in Multimedia Mode, Dynamic Stream Support assigns to each network node only the bandwidth it needs. This minimizes wasted bandwidth and preserves overall bandwidth for other network nodes and applications. More usable throughput means higher performance for all home network applications (i.e. higher video quality, faster file transfer times).

Eliminates unexpected delays and provides synchronization for multimedia content
Delays and unpredictable latency are unacceptable when transmitting isochronous content (video, audio, and voice). Dynamic Stream Support avoids unpredictable and long delays by eliminating collisions and the capture effect caused by carrier sense multiple access (CSMA) mechanisms. In CSMA access, shared bandwidth is not governed and network nodes are allowed to transmit at the same time. When network nodes realize they are transmitting simultaneously with other nodes, all nodes must back off and attempt to transmit later. This will result in unexpected and potentially long delays in multiple node networks. Networks may also experience the "capture effect" where one node transmitting a long sequence of data can monopolize the entire bandwidth while other nodes must wait-particularly problematic for time-sensitive multimedia content.

Whitecap2's Dynamic Stream Support architecture enables predictable latencies and provides the synchronization crucial for transmitting isochronous multimedia content (i.e. video, audio, and voice). The Dynamic Stream Support architecture provides the foundation and ability to support parameterized QoS features to enable high-quality video, audio, and voice transmission simultaneously with batch data.

Supports home network growth and expandability (adding more nodes)

As more and more nodes are added in a CSMA network, collisions become more frequent and the total usable throughput of the network degrades rapidly. In Whitecap2, as network nodes are added, additional bandwidth is simply reallocated and the overall available throughput is gracefully maintained.

- Key benefits delivered:
  - High Usable Throughput
  - Efficient Bandwidth Utilization/Allocation/Management
  - Multimedia Support
  - Parameterized QoS Foundation

5. Delayed Acknowledgements

The acknowledgements are grouped and transmitted as a command packet in the STAs slot in a network frame. The source always retransmits the negatively acknowledged packets first before transmitting any new packets.

In the case no acknowledgements are received (either positive or negative) before its next transmit slot, no retransmissions are done in the next transmit slot. The assumption here is that all the packets sent in the previous slot have been received by the remote STA; however, the buffers will be freed up only based on the next acknowledgement packet from the remote.

Delayed Acknowledgements are part of the retransmission scheme (ARQ), which is more complex and incorporates algorithmic procedures for the cases where:

1) The round trip delay between the transmitter STA and the receiver STA is superior to a network frame

2) Retransmission timer expires without an acknowledgement is received

3) The buffer in the receiver STA overflows

This innovative scheme was introduced in order to minimize the overhead and use the available bandwidth in a more efficient way.

6. Ten Nodes Supported at 11 Mbps

11 Mbps is available on each of 3 non-overlapping channels. Each non-overlapping channel allows the full bandwidth to be utilized. Up to ten wireless nodes can exist per subnet on a Whitecap2 network. Each node has a corresponding small network overhead reducing the available bandwidth per node as each new node is added. This is a predictable linear degradation due to the collision-free slotted architecture allowing for superior bandwidth management and scalability. By contrast, a CSMA-based network will experience the "capture" effect, where one or two nodes will occupy the entire bandwidth and deny access to resources to all remaining nodes.

7. Channel Protection (ARQ/FEC)

Different network applications and content drive different requirements of delivery quality and error correction. For instance, every packet of a bank statement is mission-critical data and needs to be retransmitted until the data is received correctly. On the other hand, CD-quality audio would sound terrible if packets were retransmitted, causing unexpected delays. Video also cannot tolerate delays, but missing packets may cause poor image and viewing quality. Whitecap2's forward error correction (FEC) offers several classes of delivery qualities to apply according to the type of media stream to deliver the highest possible performance and quality.

- Key benefits delivered
    - FEC can correct corrupted packets
    - Interference Immunity
    - Non-delay sensitive stream support

8. Auto Repeat reQuest (ARQ)

Whitecap2 supports selectable retransmissions of lossless streams with Auto Repeat reQuest (ARQ). Packets that are not received correctly are retransmitted until they are properly received. The number of retransmissions is application dependent, as these parameters can be changed from a default value during stream setup. ARQ can accommodate asochronous data and interoperate with less delivery-oriented upper network protocols such as UDP. ARQ does not guarantee "on time" delivery, therefore it is best applied to bulk and mission-critical data.

9. Forward Error Correction (FEC)

Packets in time sensitive applications are not retransmitted, but high-quality delivery is achieved through Forward Error Correction (FEC) coding. FEC recovers data "on the fly" while other correction mechanisms, such as CRC (Cyclic Redundancy Check), filters and drops corrupt data requiring retransmission. Consequently, FEC actually increases the available usable throughput. FEC can be used by either non-delivery-oriented or delivery-oriented applications; however, FEC is essential for video that is not retransmitted because even just a few dropped frames can cause poor image quality. Whitecap2 supports both FEC and CRC mechanisms.

CRC is computed using a standardized generator polynomial. The CRC is computed using the following standard generator polynomial of degree 32:

$G(x) = x^{32}+ x^{26}+ x^{23}+ x^{22}+ x^{16}+ x^{12}+ x^{11}+ x^{10}+ x^{8}+ x^{7}+ x^{5}+ x^{4}+ x^{2}+ x+1$

The CRC is the ONEs compliment of the sum (module 2) of the following:

a. The remainder of $xk*(x^{31}+ x^{30}+ x^{29}+ \ldots.+ x^{2}+ x+1)$ *divided (modulo 2) by G(x), where k is the number of bits in the calculation fields, and*

b. The remainder after multiplication of the contents (treated as a polynomial) of the calculation fields by x^{32} *and then division by G(x).*

The FEC scheme is based on Reed-Solomon coding. Reed-Solomon codes are block-based error correcting codes. The encoder takes a block of digital data and adds extra "redundancy" bits. The decoder process each block and attempts to correct errors and recover the original data. The number and type of errors that can be corrected depends on the characteristics of the Reed-Solomon code used.

Whitecap2 uses (n, k) Reed-Solomon coder over Galois Field (28). The 'n' and 'k', values are predefined and fixed. Each packet (including the header) is split into blocks of 'k' symbols (each symbol is a byte) and encoding is performed to form 'n' byte blocks. If number of bytes in a data packet is not integer multiple of 239 (k = 239), then the last block is sent with truncated encoding using virtual zeros technique. In this technique, the encoded bytes are computed as if the data is padded with zero bytes to complete a block, but the pad bytes are not transmitted. Instead, at the receiver, the pad bytes are added and then the data is decoded. For future products, it may be possible to add new types of encoding types through negotiations during stream connection establishment if the benefits prove to be significant. Note that the size of the blocks in every packet is always fixed to RS(255, 239).

10. Channel Agility

Whitecap2 allows operation across several independent non-overlapping channels. Each channel is capable of transmitting the full network bandwidth. Channel agility is the ability of the network to dynamically change channels in the event the current channel becomes severely degraded or unusable. This is done automatically, with no user intervention required. This allows the network to avoid in-band interferers, such as microwave ovens and cordless phones.

- Key benefits delivered
    - Network robustness-utilizes adequate channel to ensure high performance in the face of in-band interferers (cordless phones, microwaves)
    - Interference immunity
    - Ease of use-user does not have to find cleanest channel and set each node individually to the cleanest channel

Nodes change (switch) channels under the following conditions:

1) Nodes can change based on channel quality statistics (degraded channel)

2) Nodes can change when no connection to any other node after predetermined time

The coordinator node monitors channel system performance by evaluating its own packet rate and the packet rates communicated from client devices. The coordinator node then selects a better performance channel accordingly and instructs all clients to change channels.

11. Coordinator Redundancy

The Coordinator Redundancy feature protects against the possibility of a coordinator device failure bringing the whole network down. This feature eliminates a single point of failure and improves network reliability. Coordinator Redundancy also allows users to power down a coordinator node in a Whitecap2 network without disabling the entire network. Ease of use is improved because the user does not have to treat the coordinator node differently than the clients.

A Whitecap2 network must have a coordinator to operate (see section 1.1). Whitecap2's Coordinator Redundancy mechanism hands over the responsibilities of the coordinator device to an alternate coordinator device in the event the original coordinator fails or is taken off the network. The coordinator responsibility is not restricted to a particular type of device (i.e. access point). The role of the coordinator is invisible to the user.

- Key benefits delivered

- Network reliability-eliminates single point of failure
- Ease of use-network automatically adjusts to conditions without imposing any special configuration of nodes by end user

When establishing a network:
A network node(s) boots up as a client. One of the following three activities then takes place:

1) If a coordinator is found, node joins the network as a client
2) If no coordinator is found but an alternative coordinator exists, the nodes negotiate for coordinator role and the coordinator identity is established in the network
3) If no coordinator is found, the node becomes an alternate coordinator

On an established network:
If a coordinator is shut down, the coordinator role is handed off to one of the clients

In Whitecap2, "faceless" devices (no direct input mechanism), such as a 10BT bridge, will not have coordinator capability. This capability will come in a later Whitecap version.

12. Remote Firmware Update Support

Remote firmware updating allows users to install future product enhancements and upgrades. Upgrades ensure scalability of Whitecap2 with new home networking applications and services.

Software updates can be accomplished by installing the latest release. This can be done over a Whitecap2 network (within the subnet). Remote software updates are required for "faceless" devices such as the 10BT bridge.

From a binary file residing on the hard disk of any online PC, the host network manager downloads over the air to a device such as the 10BT bridge. The embedded network manager on the bridge receives the software update, and the node is then restarted.

- Key benefits delivered
  - No separate interface required to update "faceless" devices
  - Protection from obsolescence
  - Upgradeable to new features and services

13. Security and Privacy

Subnet ID Authentication

Unlike wired networks, wireless networks cannot be secured or contained physically. E-commerce over the Internet, copyrighted multimedia content (e.g. CDs, DVDs), and personal or financial information in the home require a high need for privacy. Whitecap2 employs several security mechanisms that prevent unauthorized access to data. Whitecap2 privacy and security exists in three different layers of the network stack (Figure 5).

Physical layer
Direct sequence spread spectrum (DSSS) radio transmission offers isolation at the physical layer. The im-

plementation of DSSS is difficult to intercept and decode. Radios must also be tuned to the correct frequencies to receive data. The original data stream is essentially encoded through chipping and scrambling.

Data link layer

To avoid unauthorized access, Whitecap2 follows a strict authentication procedure before a connection is granted. Each node in the network is identified by a unique 16-bit subnet ID. Whitecap2 addresses each node by its unique subnet ID-it is a field in the Whitecap2 header and is unique to a specific network. Packets with the incorrect subnet ID authentication are dropped and denied access to all devices on the network. Whitecap2 subnet ID provides reliable security by exercising security on a packet-by-packet basis. The subnet ID is assigned either through Open Enrollment (see section 4.2.10) or via user input.

Network layer

Whitecap2 does not inhibit encryption or security mechanisms employed by higher-level network applications or protocols. For instance, encryption employed by the IP protocol (e.g. SSL) to IP data is preserved by Whitecap2 and decrypted by the IP protocol at the receiving end. Internet or Web transaction encrypted data will be transmitted through Whitecap2 and decrypted by the Web browser at the receiving end.

- Key benefits delivered
    - Network security

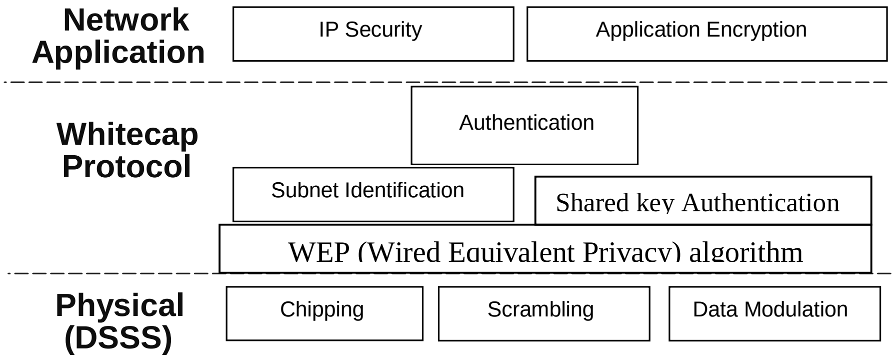


Figure 5. Privacy and security layers

Shared Key Authentication

The shared key authentication feature is available when the Station (STA) operates in either Wi-Fi or Multimedia Mode. It allows a STA to join the network by providing a secret shared key when requested by another STA in the network. The secret key is presumed to have been delivered to a STA via a secure channel, independent of the IEEE 802.11. It is contained in a write-only MIB attribute via the MAC management path. The shared key authentication feature is only available if the WEP option is implemented at the STA.

Wired Equivalent Privacy (WEP) algorithm

WEP is defined as protecting authorized users of a wireless LAN from casual eavesdropping. After being passed to the MAC layer, the digital content is encrypted using the steps described in this section. This approach denies access to information being passed from one device to another, unless the authentication key is known by the receiving STA.

The encryption algorithm can be summarized in the following steps:

1) The shared secret key (of length 40 bits), in conjunction with an Initialization Vector (IV), generates a 64 bit-long sequence, called the Seed.
2) The Seed is then input into a WEP Pseudo-Random Number Generator (PRNG), which will output a Key Sequence.
3) The payload data bits (MPDU) and the Key Sequence is input bit wise into a XOR. The resulting MPDU is a WEP encrypted frame.

This algorithm is available in both modes (Wi-Fi and Multimedia) and has the following advantages:

- Strength-it is very difficult to discover the secret key which can be frequently changed, along with the IV
- Self-synchronizing-critical property for a data-link level encryption algorithm
- Efficient-can be implemented in either hardware or software
- It is optional-WEP is not mandatory for 802.11

14. Open Enrollment and Device ID Authentication

There are two ways of installing a new device on a Whitecap2 network: through "open enrollment" or through user intervention.

Open Enrollment
Allows devices without an input mechanism to easily be added to a network in a secure fashion.

New nodes are considered in "open enrollment" state when executing the Cirrus Logic software/firmware, but the RAM has not yet been updated with an appropriate subnet id that would identify the device as a member of a given network. This is the case, for example, when adding an Ethernet bridge to the network.

The new node hops channels, transmitting requests to join a network. When one is found, the new node sends its device ID (MAC address), and waits for authentication from the existing network coordinator redundancy. This may or may not be granted, subject to user discretion.

If confirmed, the new node's RAM will be updated with the subnet id of the given network. The new client information will also be added to the coordinator's online table.

User Intervention
New nodes with an input mechanism (PCs) allow for the subnet id to be entered by the user during installation, thereby permitting the node to join the network (and the online table updated with the MAC address of the new node).

FUTURE FEATURES AND POTENTIAL FOLLOW-ON ENHANCEMENTS

Whitecap2 establishes the infrastructure that addresses the unique home networking needs centered on multimedia and QoS support, ease of use, and reliability. This infrastructure provides the foundation for managing bandwidth and resources in a predictable fashion that can be enhanced with more advanced QoS features such as parameterization of streams and guaranteed bandwidth of streams. Again, existing contention-based schemes are unable to provide the predictability needed to support these types of features, which are deemed crucial to service providers as they deliver integrated multimedia services (video, audio, voice, and data) to the home.

Effective bandwidth management and a slotted architecture are key components for providing future services that support multiple media streams in the home. A few of these are listed below:

- Parameterized QoS Services-Isochronous traffic (video, voice) is differentiated from best-effort traffic (file transfers, print jobs, internet browsing) by assigning a different set of parameters (bandwidth, delay, delay jitter) to each supported application.
- Guaranteed Bandwidth Reservation-Bandwidth negotiation allows for isochronous (e.g. MPEG-2 video) content that has very stringent bandwidth requirements to be maintained per the requirements, regardless of other asochronous traffic.
- Multicast-Reduces the required bandwidth to support sharing media streams by allowing traffic to be sent only once to the clients receiving the media stream (rather than to each individually).
- Co-location-Closely located subnets on the same channel can gracefully share the available bandwidth if they must operate on the same channel.

1. Advanced Quality of Service (QoS) Features

Whitecap2 has already in place the "hooks" necessary to support an 802.11e implementation with respect to multimedia content. The IEEE 802.11e draft specification allows for the implementation of a minimum of 4 and up to 8 physical queues. These queues will be used to differentiate Traffic Classes (TCs) with different bandwidth, delay, delay jitter and Packet (or Bit) Error Rate requirements.

Guaranteed bandwidth reservation

Whitecap2 is capable of reserving bandwidth for multimedia isochronous content that has extremely stringent bandwidth and latency requirements (e.g. DVD MPEG video). Embedded in Whitecap2 is the synchronization, time stamping, and sequencing necessary for isochronous communication. The amount of bandwidth required for a particular isochronous stream is negotiated between the coordinator redundancy and client through the command stream channel. The required amount of bandwidth is then reserved in the appropriate slot. Traffic is queued and buffered by the transmitting node and then transmitted on to the network (Figure 6). This ensures that a specific media stream will get the bandwidth the stream requires, regardless of other non-isochronous traffic.

Priority Service

Whitecap2 can provide a best-effort priority service. Priority services are applied to transmit traffic at each network node. High-priority traffic is differentiated from low-priority batch data (e.g. print jobs, file transfers) by decoding packet fields such as IP precedence bits and RTP payload. Differentiated packets are separated and buffered into three queues of high, medium, and low priority (Figure 6). After differentiating network traffic, time-sensitive, high-priority traffic is transmitted first. Priority service is applied as packets are transmitted out of the three queues in a Weighted Fair Queuing (WFQ) arbitration mechanism into the remaining bandwidth of each node's corresponding slot. WFQ arbitration transmits a higher ratio of higher-priority packets than lower-priority packets during the given slot time.

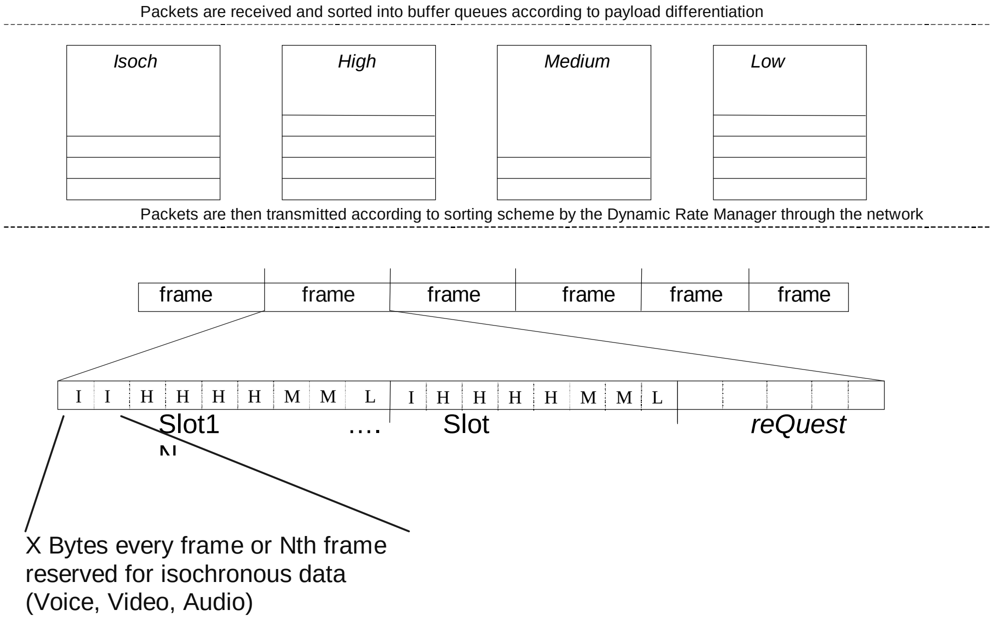

Packets are received and sorted into buffer queues according to payload differentiation
Isoch
High
Medium
Low
Packets are then transmitted according to sorting scheme by the Dynamic Rate Manager through the network
frame
frame
frame
frame
frame
frame
I I H H H H M M L I H H H H M M L
Slot1
….
Slot
reQuest
X Bytes every frame or Nth frame
reserved for isochronous data
(Voice, Video, Audio)

Figure 6. Whitecap2 protocol QoS

The benefits of advanced QoS include:

Simultaneous multimedia (video, voice, audio) and batch data (print jobs, file sharing) transmission
The ability to support simultaneous multimedia and batch data transmission without compromising multimedia quality is mandatory in a home network. For example, the quality of a MPEG-2 stream generated by a DVR or DVD player must be maintained when the home user is simultaneously printing a file to a remote printer or transferring a file between two PCs.

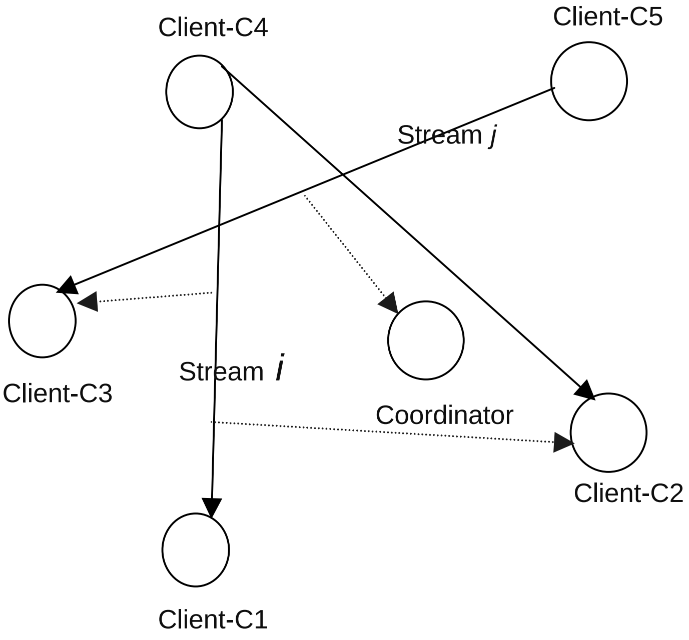
Whitecap2's guaranteed bandwidth reservation preserves high-quality isochronous data transmission even in high-batch data traffic environments. By prioritizing network traffic and delivering time-sensitive traffic first, priority services allow low rate data (email, print jobs) to coexist with multimedia content without any degradation in the user experience.

Preserves QoS of broadband Internet and digital multimedia content
Internet applications, services, and multimedia content distribution such as video on-demand, VoIP, and streaming audio need end-to-end quality of service to operate properly. Internet QoS initiatives including Resource Reservation Setup Protocol (RSVP), the audiovisual data transmission standard H.323, Real-time Transport Protocol (RTP), and priority services implemented in head-end routers, provide high-quality content distribution to the house. The network distributing content within the home must preserve QoS to utilize Internet content throughout the home in its intended form.

2. Multicast Addressing with Shadow Clients

Shadow clients in a Whitecap2 network allow support of multiple media streams. Viewing the same multimedia content at different locations is a common requirement for the home. Popular multicast protocols such as IP multicast and IGMP are being deployed by the Internet to deliver multiple media (video, audio, voice) streams to the home. Shadow clients reduce the required bandwidth to support sharing media streams by allowing traffic to be sent only once versus individually to each client receiving the media stream.

Shadow clients enable multicasting of multimedia content and data. A shadow client is a client that has been given permission from the coordinator to decode and receive traffic destined for another client (Figure 7). Unlimited shadow groups can be created within a Whitecap network. A multicast (shadow) group can consist of up to as many clients as are on the network. The coordinator node also provides information on the media stream to the shadow client device. This includes the data type, bandwidth requirements, decryption key, and the primary client's identification. Data is then received at the shadow client(s) with no additional bandwidth requirements to the network. Whitecap2's shadow-client capability easily interfaces to popular Internet IP multicast technologies such as IGMP. The conversion of IP multicast addresses to shadow clients is seamlessly handled by the Whitecap2 data link layer interface.



Stream *i*

- Client C4 is the source
- Client C1 is the primary destination device
- Clients C2 and C3 are shadow clients with permission to read stream *i* meant for Client C1

Stream *j*

- Client C5 is the source
- Client C3 is the primary destination device
- Coordinator device is a shadow client with permission to read stream *j* meant for Client C3

*** Dotted lines show the shadow client connections**

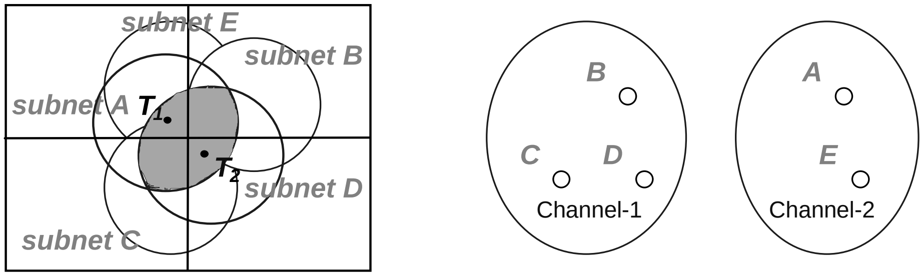
Figure 7. Shadow clients

3. Co-Location

Co-location enables the deployment of Whitecap2 networks in closely located homes and apartment complexes. Ideally, the distribution of wireless subnets should be non-overlapping to avoid interference with each other. Realistically, closely located homes and dense apartment complexes may make overlapping subnets commonplace to wireless home networks. Co-location and channel selection features allow overlapping networks to operate without degrading performance.

Overlapping subnets first utilize channel selection to find and change network operation to an available open channel, allowing both overlapping networks to transmit at full bandwidth. In the scenario where there are more overlapping subnets than available channels, the Whitecap2 co-location feature is enabled. The operation of non-overlapping networks in the same channel is achieved by sharing the available channel bandwidth through appropriate negotiations between overlapping subnet coordinators (Figure 8).

Coordinators of different subnets report bandwidth requirements to each other to efficiently use the entire available network throughput. The coordinators polices the transmissions of each network, thus avoiding interference. In the event that the coordinator cannot "see" each other (are out of each other's transmission range), a client that can "see" either coordinator is deemed a "proxy coordinator " and forwards coordinator communication traffic. The subnet ID in the Whitecap2 packet header is used to track packets of different subnets in the same channel.



(a) Physical location: Subnets A, B, C, D, and E are overlapping.

(b) Logical location: Subnets B, C and D share Channel-1 and Subnet A and E share Channel-2

Figure 8. Co-location example

CONCLUSION

The Whitecap2 network protocol is a key element of Cirrus Logic's technology and is optimally suited to serve as the foundation for wireless home networking products. Whitecap2 is designed specifically to address home networking requirements for multimedia support, ease of use, and reliability-to enable exciting new applications for the home. It incorporates Cirrus Logic's multimedia and QoS extensions for transmitting the full range of high-fidelity multimedia content (video, audio, voice, and data) wirelessly throughout the home, while preserving interoperability with other Wi-Fi (802.11b) products. Whitecap2 facilitates the deployment of high performance wireless home networks, which extend the digital broadband experience to multiple computers and electronic devices anywhere in the home.

Unlike other wireless networking protocols, Whitecap2 can accommodate and seamlessly transmit high-fidelity multimedia content-including MPEG-2 video and CD-quality audio-wirelessly throughout the home. Whitecap2 achieves this functionality as a result of its pioneering feature set, which includes:

- Contention-Free Access
- Dynamic Stream Support
- Parameterized QoS Infrastructure
- Peer-to-Peer (Mesh) Topology
- Forward Error Correction (FEC)
- Channel Agility
- Open Enrollment
- Coordinator Redundancy
- Delayed Acknowledgements

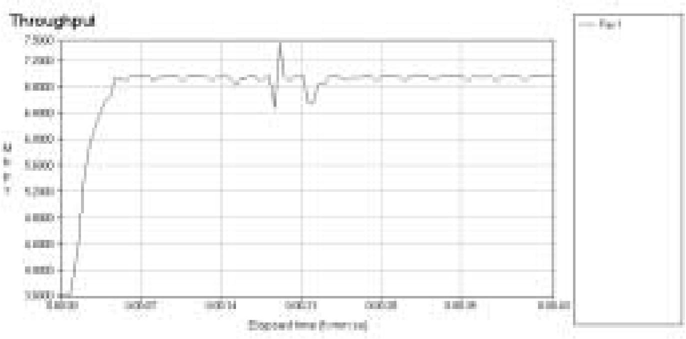
More advanced QoS features, such as parameterization of streams and guaranteed bandwidth, will be implemented in follow-on releases.

In addition, Whitecap2 is designed to work with leading edge wireless digital radio technology to deliver the highest network utilization. The network architecture, services, and packet structure in Whitecap2 have been streamlined to enable greater efficiency for multimedia transmission. Whitecap2 will easily support various types of network devices including desktop or mobile PC's, and non-PC devices.

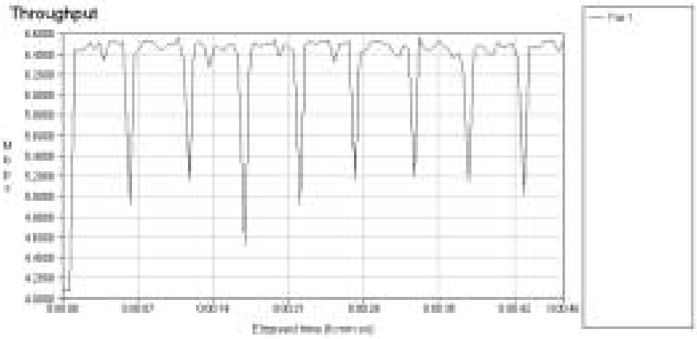
Finally, Whitecap2 is designed as an open, standards-based network protocol. Whitecap2 embraces Wi-Fi (EEE 802.11b), and is fully compliant with this standard.

ANNEX 1: PERFORMANCE COMPARISON BETWEEN MM AND WI-FI MODES

The following charts show a performance comparison of a Whitecap2-based product while operating in MM and in Wi-Fi modes. Note that the encryption is not activated in any of these modes. In case WEP encryption is active, the raw throughput is expected to decrease slightly in both modes of operation.

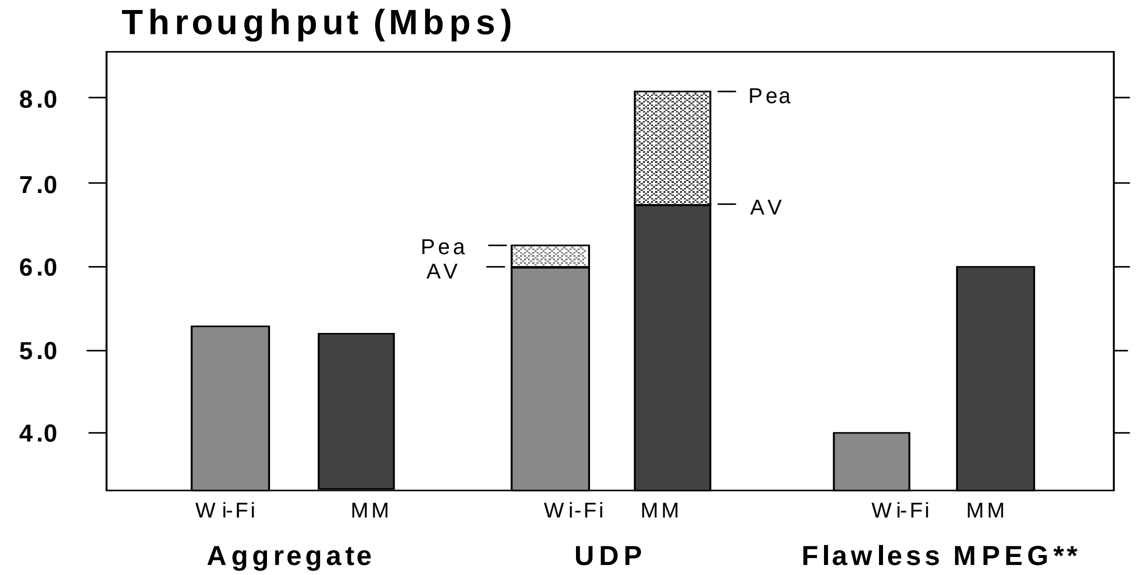


Slotted architecture (Dynamic Stream Support) provides superior usable throughput (~7Mbps) and lower overhead vs. Wi-Fi (both ad hoc and AP)



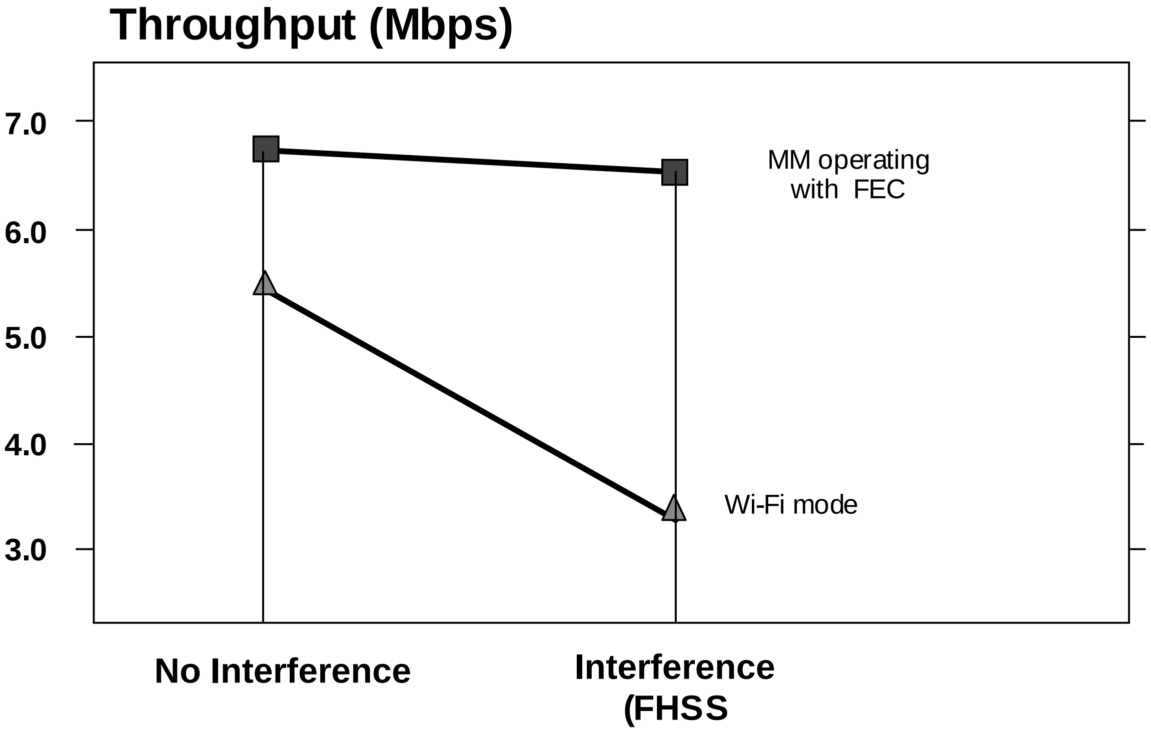
Average Wi-Fi mode throughput is ~6Mbps in ad hoc mode, and degrades by ~50% when in AP mode

The following figure shows the usable throughput advantage of the MM mode over the Wi-Fi mode in a Windows environment using UDP packets encapsulating the application payload blocks.



Notes: * Throughput measured between Windows 98 PC's using Ganymede Chariot Test Suite
** Flawless MPEG is maximum single stream that will play without stutter or pauses

Next chart shows the advantage of using FEC in the presence of an interferer.


Throughput (Mbps)
MM operating with FEC
Wi-Fi mode
No Interference
Interference (FHSS