

Mesh Software Operational Description

March 9, 2017

National Technical Systems
41039 Boyce Road
Fremont, CA 94538

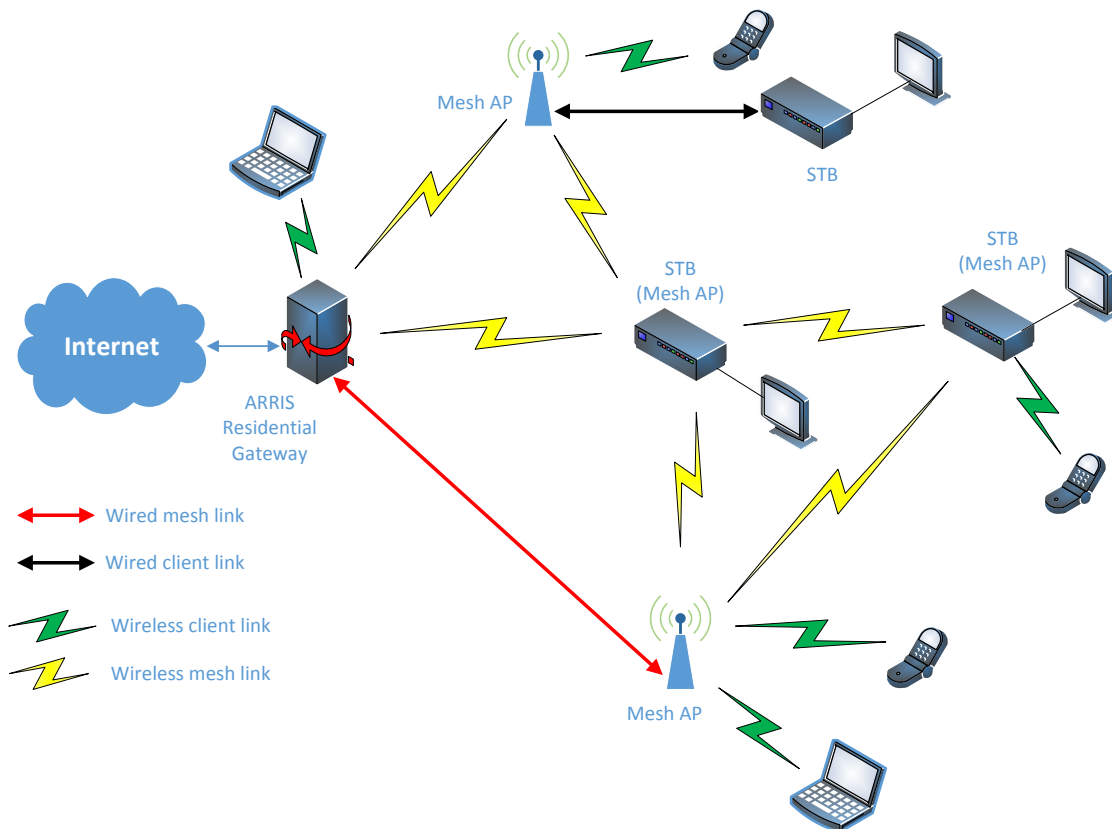
FCC ID: PGRBGW210
SOFTWARE VERSION: 9.2.04d30 (ARRIS) / 1.0.27 (AT&T)

1 Overview

The purpose of this document is to describe the operational description of the Wireless Distribution System (“WDS”) and the role of the ARRIS DSL wireless residential gateway in the Network. Any mesh node supported with this software implementation becomes part of the mesh network, which becomes the backhaul network for the clients connecting to the mesh AP nodes or the ARRIS DSL wireless residential gateway. Through the mesh network, optimal connections to the Internet as well as direct connections between peers can be established. No specific software is required to run on wireless clients (such as laptops, smart phones or tablets) in order to access to the wireless mesh network.

Since all mesh nodes in the network need to be in communication with each other, all of them need to operate on the same 5 GHz channel and all support DFS detection.

Below is an example a mesh network showing different types of mesh nodes including the ARRIS uDSL wireless residential gateway:



2 Mesh Software specifications

2.1 Mesh Routing

Mesh Routing features allows mesh nodes to act as smart access points that establish mesh links to each other and relay traffic between them on 5Ghz band and to function as an access point to the Ethernet wired and wireless clients that are associated with them.

Mesh links are established using Wireless Distribution System (“WDS”). Four-address frame format is used for addressing between mesh nodes. For security, WPA2 encryption is established between the links.

The Mesh Routing feature maintains route tables and finds the best end-to-end route among these links for each packet from a client to another one on the network. Although the ARRIS Residential Gateway will always persist as an AP/Master device in the mesh network the decision making for best route is distributed and there is no “master” AP in the network for this decision. As network conditions change (interference, topology change due to node shutdown or node addition), the route tables are updated for best routes for any client.

A maximum of 16 mesh APs (including the gateway node) is allowed to exist in a mesh network. The number of mesh links that can be established from each mesh AP may be limited by the wireless device driver on the supported node.

The maximum number of wireless clients that can connect to the mesh network is 128. The number of clients connected to each mesh AP may be limited by the wireless device driver on the supported node.

2.2 Push Button Setup and Automatic Configuration Sharing

The addition of a new mesh node into the mesh network is accomplished by the Push Button Setup which is based on the WPS protocol. The new Mesh node connects to the ARRIS Residential Gateway as a station device and gets the network credentials via WPS. After successful completion of WPS session, the new node switches to a Mesh AP mode, establishes WDS link to the Residential Gateway with WPA2 encryption, and starts broadcasting the SSID. As part of this exchange, a PIN is generated and exchanged to use when re-connecting upon credential change.

At that point additional mesh nodes only need to connect to one other mesh AP in the network using the same WPS mechanism, not necessarily to the Residential Gateway.

This setup will allow all the devices in the mesh network to have the same SSID and wireless security and allow clients to roam within the network. All devices in the same mesh network share a unique mesh ID that is used to identify a mesh network from another.

Any changes to the wireless configuration that are triggered from the Residential Gateway by the user via UI or from a central configuration server over TR-069 will be automatically propagated to the other mesh nodes by the Automatic Configuration Sharing feature over mesh links. It is assumed configuration changes are not triggered from any other AP mesh node than the gateway node.

The 5 GHz SSID and security configurations are propagated to all the mesh nodes in the network. Upon receiving the configuration change message, a mesh AP node reverts to station mode and scans for its peer. If the SSID is changed, it re-connects using the new SSID which it has received. If the password is changed, then it re-connects using the previously exchanged WPS PIN. After re-connection, the mesh node switches to AP mode and link process continues as described above.

If the operating channel is changed, then the mesh AP’s revert to station mode and scan for its peer and re-connects when it finds it again and then switches back to an AP mode.

2.3 Forming a Mesh Network

The ARRIS Residential Gateway is responsible for channel selection at startup to establish the wireless mesh network. When a mesh network is formed, the gateway selects the channel to operate on (using the Auto or User channel selection settings) and performs the CAC if a DFS channel was selected. In this network configuration all other mesh nodes always start up in STA (client) mode with passive scanning. Once the gateway is up and running, the other mesh nodes start their association with the gateway as described above using the WPS process. Once associated with the gateway the mesh STA (client) automatically switches to an AP mesh mode of operation using the associated channel and SSID from the gateway and performs a CAC before transmitting. Distance mesh nodes or client devices which do not see the gateway follow the same process to associate to the mesh AP node (which is now associated to the gateway) to form the mesh network.

2.3.1 Radar Avoidance

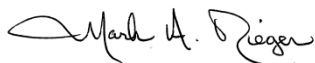
Adding the mesh software functionality to the Residential Gateway does not modify or change the radar detection and channel selection mechanism originally approved under the DFS grants for non-Mesh modes.

All mesh nodes, in addition to the Residential Gateway, in an active mesh network operating on a DFS channel actively monitor for radar and can detect radar. Since this implementation requires all of the mesh nodes in the mesh network to operate on the same channel, when radar detection occurs coordination is required between all nodes in the network to change to a non-DFS channel. When a mesh node detects radar, it selects a non-DFS channel, and sends a Channel Switch Announcement (CSA) frame (as defined in the 802.11h standard) to all of its clients and mesh peers, immediately stops transmitting on the channel, and switches to the non-DFS channel broadcasted in the CSA. Any node in the mesh network detecting radar retains the blacklisted channels (except when power cycle) for the 30 minute non-occupancy period.

Mesh APs that receive the CSA also forward the CSA message and immediately stops transmitting and switch to the channel designated in the CSA frame. If for any reason (i.e. lack of receiving CSA frame) any of the Mesh AP's that do not switch to the same channel will lose the connectivity to its peers and will revert back to a STA (client) mode after a pre-defined timeout and start scanning for its peers to re-connect on the new channel the mesh network as moved to.

If for any reason the Residential Gateway does not switch to the same non-DFS channel but switches to another one of its choice (user interaction), all mesh AP nodes will revert back to a STA (client) mode and passively scan for their peers and re-connect as described above.

If the Residential Gateway does not get the CSA message sent by a distance Mesh AP node which detected the radar, the mesh node that detected radar will black list the channel and move to the designated non-DFS channel. However, it and its clients will be locked out of the mesh network for the non-occupancy period as required in the DFS standard operating procedure.



Mark Rieger
Principal Hardware Engineer
Regulatory compliance and conformance

ARRIS
310 Providence Mine Road, Ste. 200, Nevada City, CA 95959 USA

o: +1 530-274-5440
c: +1 530-575-6010
e: mark.rieger@arris.com