Coverage Hole Detection and Mitigation Algorithm

The coverage hole detection and Mitigation algorithm is responsible for four things.

1. Coverage Hole Detection
2. Validation of the Coverage Hole
3. Mitigation if Prudent

The first order of business is to detect coverage holes, and second to mitigate them (if possible and wise) by increasing power/coverage. CHDM runs independent of RRM and the RF Group leader. In order to facilitate making decisions at a local level, it runs on every controller. Each individual controller performs coverage hole detection monitoring all associated AP's and thus monitoring every attached client and their received signal levels. Mitigation involves increasing the power on an AP, or group of AP's to improve coverage levels to a certain area where client signals fall below a customer selectable threshold.

The coverage hole algorithm was designed initially as a way for admins to evaluate coverage requirements as the network grows and changes. By monitoring coverage hole alerts an administrator can effectively track and identify areas of the network that might require additional AP's or the re-assignment of existing inventory. Given the dynamic nature of network growth, this is a good thing. Coverage hole correction was envisioned as a way to address short term lapses in coverage by temporarily increasing coverage where needed by extending the reach of existing assets. It had an added benefit in that it could be relied upon, in a properly designed and sufficiently dense network, of providing fault tolerance in the event of an AP failure.

Coverage Hole Detection (CHD)

Coverage hole detection is based on a 5 second (CHD measurement period) histogram of each Clients Received RSSI values maintained by the AP. Values between -90 dBm and -60 dBm are collected in a histogram in 1 dB increments. A client falling below the configured RSSI thresholds for 5 seconds is marked as a pre-coverage hole event. Pre coverage holes are immediately reported to the WLC and tracked upstream by Prime. At Prime an administrator can review pre coverage hole alarms, and with a location appliance can locate the pre coverage hole on the map.

No Mitigation action is performed on a pre-coverage hole. Pre coverage holes are tracked at the WLC in a 90 second cumulative histogram. A pre coverage hole becomes a coverage hole when it continues to operate below threshold for the entire 90 seconds.

Coverage Hole Detection is based on upstream RSSI metrics observed by the AP. Configurable values are:

- Data RSSI (-60 to -90 dBm) Default -80
- Voice RSSI (-60 to -90 dBm) Default -75
- Min Failed Client Count per AP (1-75) Default 3
- Coverage Exception Level per AP (1-100%) Default 25%

The RSSI value sets the minimum receive threshold for both voice and data separately. Minimum failed client count per AP determines the minimum number of clients that must be in a coverage hole before mitigation can be considered Coverage Exception level sets a percentage of the overall clients that must be in a coverage hole in order for mitigation to be considered. Both conditions Min failed Clients and Coverage Exception level must be satisfied for a coverage hole to be considered for mitigation.

(Failed Client Count > or = 3) AND (% failed Clients > or = 25%) = Mitigation

It's important when a coverage hole is detected to validate it as best we can and ensure that it's not a false positive. False positives can come from a client that just simply has poor roaming logic and is refusing to move to a better AP option, known as a sticky client.

Additional granularity exists for configuring the thresholds of an individual client as well. What is being tracked at the AP is the overall number of packets that fall below the RSSI thresholds established by the algorithm. Two values are passed from the WLC to the AP for evaluating failed packets against the threshold.

- Num_Failed_Packets–the number of packets received in a 5 second CHD measurement period that where below the RSSI threshold for the associated voice or data client type
- %_failed_Packets–the percentage of total packets received during the CHD measurement period that where below threshold

Both of these conditions must be true in order for a client to be considered in pre coverage hole alarm state. These values are configurable from the CLI only, and the default values should be used unless there is a directed reason to change them.

Notice first that both Voice and data clients are tracked separately based on the WMM UP (user priority). Each received packet from a client is evaluated. This is done through additional configuration values available through the CLI.

At the AP, the 5 second results are collected in a cumulative 90 second histogram, and once every 90 seconds this information is sent in an IAPP message to the WLC and the histogram is re-set. If the client remains in a pre-alarm condition for 90 seconds - it is then considered a coverage hole at the WLC. The WLC will next determine if this coverage hole can and should be mitigated by first determining if the client has a roaming option that it just isn't using. It checks this by determining the location of the client and evaluating its RSSI at other AP's that can hear it. If Other AP's can hear the client above the threshold - the report is marked false and the alarm is re-set.

Coverage Hole Mitigation

Coverage hole mitigation is a fairly simple process once the decision to mitigate is made. If a coverage hole exists AND it meets the criteria (minimum number of clients AND minimum percentage) for mitigation, the AP will increase power by one step. CHDM will then continue to run, and if additional mitigation is called for will re-qualify and power will again be increased by 1 step. This prevents wild and unstable swings in power. Coverage hole mitigation, while operating independent of RRM's DCA and TPC, can have a profound effect on surrounding AP's and the balance of the RF in an environment. Part of the decision to mitigate is to evaluate if mitigation could be successful. Increasing the power of a given AP independently of the RF Group metrics stands a pretty good chance of negatively impacting surrounding AP's. So mitigation is applied very judiciously. The combination of the new detection metrics and the power limits included in mitigation make this a very stable algorithm.

Optimized Roaming

Optimized Roaming was introduced in version 8.0 of the code and without going into detail on the feature (see HDX High Density Experience deployment guide) , borrows the Data RSSI threshold setting from CHDM to set the optimized roaming threshold at which a client will be gracefully dis-associated from the current AP radio. Enabling Optimized Roaming, disables Data RSSI Coverage Hole Detection.