802.11 Best Practices on the 70 Series and CK3R/X Devices Using the TI Radio

Introduction

This paper describes the default configuration and behaviors of the 802.11 radio on the 70 Series and CK3R/CK3X devices. It mainly covers behaviors that are different than previous CK3 devices. It provides some explanation on these default behaviors. It also provides some guidance on modifying them. It covers the area of dynamic roaming, radar channel roaming, connection thresholds, connection intervals, power management, Quality of Service (QoS), and 802.11d. For the 70 series running OS build older than BP12-1, some of the description is not applicable.

Dynamic Roaming

On the CK3R/X, dynamic roaming threshold is enabled by default. The roaming threshold is dynamically adjusted based on the operating environment. When the Received Signal Strength Indicator (RSSI) is below the roaming threshold, the radio would start scanning to look for a better AP. If no better AP is found, then the roaming threshold is lowered. When the RSSI stays well above the roaming threshold, then the threshold is raised. Using this algorithm, it allows our device to roam well in different RF coverage deployment automatically, especially ones with non-uniform RF coverage. This default roaming configuration should work well for most of our customers. However, it is still possible to configure our device to use static roaming parameters. When considering static roaming parameters, one should take into account the following:

1) Is the deployment RF coverage relatively uniform such that an appropriate roaming threshold can be used to roam well in all coverage area?
2) The customers are not too concerned about the device is always connected to the best AP as the device roams around the deployment area. They are more concerned about maintaining a usable connection.
3) The customers would like to reduce the amount scanning the radio performs as the device is moved around.

Here are the driver registries for configuring static roaming parameters:

HKEY_LOCAL_MACHINE\Comm\TIWLN1\Parms (radio driver path)

“DynamicScanThreshold”=”0”; Setting it to 0 disables dynamic roaming and uses static roaming instead.

“RoamLowRssiThreshold”=”-70”; Roaming threshold

“RoamRssiDeltaThreshold”=”7”; Roaming delta. Setting it to less than 7 might cause undesirable “ping-pong” effect between AP’s with similar RSSI levels.

When using the device in a Cisco infrastructure, the static roaming parameters that get pushed down by the AP would get ignored by our devices when dynamic roaming is enabled. However, with static roaming, they would overwrite the radio’s default static parameters. To ensure that the device’s configured static parameters get used, one would need to set the following radio driver registry:

```
"CcxUseRFParameters"="0"
```

Radar Channel Roaming

Radar channels, also as known as Dynamic Frequency Selection (DFS) channels, are channels on the 5 GHz band. They are shared with civilian radar applications such as weather radar. Specifically, they are channels 52 thru 64 and 100 thru 140. Their actual availability depends on the current operating regulatory domain.

When operating in these channels, there is a significant amount of overhead. Before initial operation, the AP has to perform clear channel assessment to make sure that the selected channel is clear of radar activity. Once it is in operation, periodically the AP must enforce a quiet period where no 802.11 RF activities are allowed so that it can check for radar activity. During the Quiet Period, the device will not able to send/receive any packets. If radar activity is detected on the channel, the AP will perform a Channel Switch operation. Due to this overhead and these limitations, we recommend our customers avoid using the radar channels if at all possible.

By default, the CK3R/X doesn't support soft roaming to AP's on the radar channels, i.e., it would not discover roaming AP candidates operating on radar channels. As a result, it would just hang onto the current connection until it loses the link. It is possible to configure the radio to use passive scanning to support soft roaming. With passive scanning, it means that the SSID has to be broadcasted in order for it to work properly. There are other things to consider such as beacon intervals, the actual radar channels used in order to configure optimal values for a good roaming experience. If there is a real need to support soft roaming for a customer, please contact Product Support for assistance so we can provide an optimal configuration for their deployment environment.

Connection Thresholds

There are minimum RSSI connection thresholds for both the initial connection and roaming on the 70 series and CK3R/X. The default values are -77 dBm. This means that the radio will not make an attempt to connect to an AP if the RSSI is less than the default values for initial connection and roaming. This is designed to reduce RF thrashing in fringe RF coverage areas, avoid getting into AP-Client out-of-sync connection states and prevent other potential connection issues. Once the connection is established, it will try to maintain the connection even after the RSSI falls below the connection threshold (and there is no better AP that meets the roaming threshold requirement). In general, customers just need to be aware of these thresholds and don't need to do anything. These thresholds can be adjusted through the driver registry. Things to consider when adjusting them:

1. The deployment RF environment. With a very clean RF environment and a very sparse AP coverage, one can lower these thresholds to improve initial connection and roaming experience. Conversely, if the RF is very noisy, one can raise the thresholds.

2. Security option. Enterprise security options such as TLS would require more frames to complete the authentication process than a simple PSK option. Lengthy authentication would more likely to run into timeout issue in fringe RF coverage.

3. BT Coexistence. If a customer uses the Bluetooth link simultaneously with 802.11 all the time, it would place more stress on the 802.11 link and would require a higher connection threshold as a result.

Here are the driver registries for adjusting the connection thresholds (same radio driver path as earlier):

```
"SmeAssocMinRssi"=”-77” ; Initial connection threshold
“RoamApQualityThreshold”=”-77”; roaming threshold
```

Connection Intervals

When using the default Intermec Supplicant, it has default back-off connection attempt intervals. When the device is out of coverage area, the time it waits to make another connection is incremented to be increasingly larger over time. It is intended to save battery when out of connection range for an extended period. Consequently, it can take up to one minute before the radio attempts to make a connection after it has gone out of range for a few minutes or longer and then comes back in range. If a customer needs to have 802.11 connectivity within a few seconds of coming into connection range, the Intermec Supplicant back-off connection intervals can be modified through a registry. Since the radio driver also has its own back-off interval once the connection profile is pushed down to the radio driver, it is not necessary nor recommended to set it shorter than 16 seconds. Otherwise, it would cause unnecessary churn in the system when it is out of range.

Here is the registry for controlling it:

```
HKEY_CURRENT_USER\software\intermec\80211conf\profiles
```

```
"WaitAssociationDelays"=hex:80,3e,00,00  ; 16,000 ms in little endian format
```

Every 4 bytes (in little endian format) represents one time interval. If there is no need to have different time intervals for connection attempt, one interval is sufficient.

Power Management

Power Management on the TI radio is designed for more aggressive power saving than previous products such as the CK3 and CN3. When retrieving buffered packets from an AP, there is a configurable timeout value while waiting for the AP to respond with the buffered packet after sending out the PS-Poll. The default value is 80 ms. With some of slower consumer graded AP’s, it can take more than 80 ms for them to respond. When this happens, packets can get dropped. The best way to diagnose this problem is to use a wireless sniffer. Take a look at the time difference between the PS-Poll packet and the responded packet from the AP. If it is more than 80 ms, then that is the reason packets are dropped. Increase the wait time to match the slower AP by adjusting the following radio driver registry:

```
“QOS_rxTimeoutPsPoll”=”90”  ; in ms
```

When increasing the timeout value, one also needs to pay attention to the AP’s beacon interval. It doesn’t make sense to have a timeout value greater than the beacon interval. For example, if the AP’s beacon interval is 100 ms and the wireless trace indicates that the AP is taking 130 ms to respond to a PS-Poll, then setting QOS_rxTimeoutPsPoll to greater than 130 ms would not be sufficient. In addition, one should increase the beacon interval on the AP side to match operating condition.

Quality of Service

Quality of Service (QoS) is used to meet latency requirement and guaranteed minimum service through packet categorization and admission control. There have been some reported interoperability issues in the field where connection related problems seemed to have been resolved by disabling QoS.

A notable side effect with disabling QoS is that it also disables 11n functionality causing the device to behave like an 802.11(a)bg device. Here is the radio driver registry for disabling QoS:

```
“WME_Enable”=”0” ;
```

If you find a situation where disabling QoS resolves a problem, please contact the WLAN Engineering team for a debug driver for evaluation of the issue. Helping us to collect data will help us to eliminate this issue for current and future devices.

802.11d

802.11d allows us to use a single device configuration to be deployed in different regulatory domains, significantly reducing the number of configurations that Intermec has to offer. However, this feature requires 802.11d be enabled on the AP side for it to work optimally. There is hardly any overhead on enabling 802.11d in the infrastructure as it only adds a tiny Country Information Element in beacons and probe responses to allow potential clients to determine the current operating regulatory domain. Without 802.11d being enabled on the AP side, all the a-band channels are treated like radar channels, and there is limited support on Channels 12 – 14. If for some reason, the customer cannot enable 802.11d on the AP side, it is possible to disable the worldwide mode on the device and locks it down to a single regulatory domain. This can be done through the Configuration Store and it can only be done officially by the Service Department due to regulatory restriction.

Final Notes

When changing these registry settings to modify the default behaviors, one would need to reboot the device for the new settings to take effect. If the modified settings work better for a customer, the best way to deploy the settings consistently at a customer site is to contact Product Support to create an official Service Release with the desired settings.