AT&T Enhanced Push-to-Talk

Requirements and best practices for enabling Enhanced PTT over Wi-Fi networks

May 28, 2013
AT&T Enhanced PTT and Wi-Fi

• The Enhanced PTT 2.0 upgrade enables PTT calling over WiFi when connected to a compatible WLAN network + Internet access

• Device requirements
  • A device with Wi-Fi capability and Wi-Fi turned on
  • Compatible Enhanced PTT software on the user’s device
    • May require a software update through app store or eptt.mobi website (Windows Mobile 6.5)
    • Enhanced PTT 2.0 software upgrades will be available first for Android devices; iPhone, BlackBerry and Windows Mobile devices will be available later

• Network requirements
  • To use Enhanced PTT over Wi-Fi, the user must be connected to a WLAN network that provides certain minimum quality levels, configuration and Internet access to the Enhanced PTT servers
  • Networks can be public or private, as long as the user has ability to authenticate to that network (if secured)

• The following guide is intended for users of Enhanced PTT to ensure that their WiFi networks meet minimum requirements for connectivity, as well as providing recommendations for optimum performance of PTT over Wi-Fi
Minimum Requirements For PTT Over Wi-Fi

- Internet connectivity
  - Network to which the APs connect should provide access to the public Internet
  - This includes DHCP allocation of IP addresses, DNS servers and default gateways that provide full access to all Enhanced PTT server IP addresses / Fully Qualified Domain Names

- Firewall requirements
  - Wi-Fi network should allow devices to access standard TLS port (443) on Enhanced PTT server IP addresses: 198.24.14.0/24, 8.12.75.0/24, 69.44.221.64/27, 174.46.134.160/27 (full subnet specified with network mask specified)

- Wi-Fi access point capability
  - Access points should support either 802.11n or 802.11g

<table>
<thead>
<tr>
<th>Network Parameter</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Round Trip Time (RTT) between device connected to WiFi network and the EPTT Server/Internet</td>
<td>200 ms</td>
</tr>
<tr>
<td>Maximum Jitter between the packets</td>
<td>60ms or less</td>
</tr>
<tr>
<td>Maximum Packet Loss Rate</td>
<td>0.5 %</td>
</tr>
<tr>
<td>Minimum Bandwidth per Talker Leg</td>
<td>Uplink*: 50 kbps Downlink**: 15 kbps</td>
</tr>
<tr>
<td>Minimum Bandwidth per listener Leg</td>
<td>Uplink*: 20 kbps Downlink**: 50 kbps</td>
</tr>
<tr>
<td>Minimum Wifi signal strength</td>
<td>-69dbm</td>
</tr>
</tbody>
</table>

* Uplink: From WLAN network to Internet ** Downlink: From Internet to WLAN network
Best Practices For Wi-Fi Network Planning with EPTT

• For customers seeking an optimum Enhanced PTT + Wi-Fi experience, additional recommendations are made for supporting:
  • Large numbers of simultaneous Enhanced PTT calls within Wi-Fi networks with full quality
  • Protect Enhanced PTT Service traffic from other types of IP network traffic
  • Seamless roaming across the coverage area

• Best practices guidelines are provided for the following:
  • Access Point site planning
  • Access Point/network configuration
  • Firewalls and end-to-end QoS
  • Access Point-to-Access Point roaming
Access Point Site Planning

• Scalability to support large number of devices
  • Multiple access points independently connected to the backend network
  • Number of access points required depends on the number of devices that can be
    connected to each access point

• Wi-Fi access point setup
  • All access points must have the same SSID, use same security mechanism and pre-
    shared key (Wi-Fi password)
  • Access points with overlapping signals must use different channels to minimize
    interference
  • All access points are recommended to belong to the same subnet
  • Access points should support dual band with both 802.11g and 802.11n to support
    wider variety of devices

• Signal strength requirements
  • A minimum Signal to Noise Ratio (SNR) of 25 dB = -92 dBm noise level with -67 dBm
    signal should be maintained
Access Point/Network Configuration

• Wi-Fi Security
  • Recommended use of WPA/WPA2 PSK to prevent unauthorized traffic on AT&T’s Enhanced PTT service network

• Access points should support “Wi-Fi Power Saving Mode” – This allows the Enhanced PTT Devices to receive call even while Enhanced PTT devices are sleeping.
  • Enable U-APSD
    • U-APSD(Unscheduled Automatic Power Save Delivery) is an enhanced power-save mode for IEEE 802.11e networks. If you Enabled the UAPSD, the wireless client is allowed to enter Power Save mode.
  • DTIM period of 200ms (typical default)
  • The DTIM period indicates how often clients serviced by the access point should check for buffered data awaiting pickup on the access point.
Firewall/QoS Considerations

• Wi-Fi Radio Upstream/Downstream
  • Enforce WMM QoS use for all devices
  • WMM classification as Voice
  • Packet loss rate lower than 0.01% on Wi-Fi access network

• Network Upstream/Downstream
  • Estimated Bandwidth reservation
  • Based on estimated simultaneous calls
  • Expected roaming between access points

• IP DSCP mapping to Wi-Fi WMM Classification and vice versa
  • Mark the priority for the IP packets to/from the Enhanced PTT Server

• Firewall requirements
  • Firewall timeout for TCP transport must be at least 5 minutes, but 30 minutes is preferable
Access Point-to-Access Point Roaming

- Device IP address unchanged
- Roaming across Wireless Controller and Access Points should be seamless for large area coverage
- Access Point-to-Access Point Roaming latency less than 100ms
  - Optimization on handover between Access Points
- No packet loss while transitioning between Access Points