Streaming Video and Throughput Uplink and Downlink
IPTV

- IPTV - Digital TV delivered using technologies used for computer network.
- Internet Protocols (HTTP, RTP, RTSP, IGMP)
Why IPTV over wireless

- Two-way data flow (video on demand)
- Greater personalization / tailored advertising
- Use existing infrastructure
IPTV Protocols

- **SDP/HTTP**
  - (hyper-text-transfer-protocol)
  - Request
  - Response

- **RTSP**
  - (real time streaming protocol)
  - play
  - pause
  - record

- **RTP+IGMP**
  - (internet group management protocol)
  - connecting to multicast stream (TV channel)
  - changing from one channel to another

© BBC 2008
Video on Demand

• Select and watch video content (usually over a network)
• Either content is streamed or downloaded with/to the application
• Apps have a subset of VCR functionality including RWD, Pause, FFWD etc.
Codecs

- H.264
- MPEG4
- MPEG2
- WMV9
• PSIA - Physical Security Interoperability Alliance
  – Video streaming codecs H.264, MPEG4, JPEG
  – Streaming protocols RTP over UDP, RTP over RTSP over TCP, HTTP, HTTP snapshot (JPEG)
• ONVIF - Open Network Video Interface Forum
  – Video streaming codecs H.264, MPEG4, JPEG
  – Audio in G.711, G.726 16kbit, G.726 24kbit, G.726 32kbit, G.726 40kbit
  – Streaming protocols RTP over UDP, RTP over RTSP over TCP, HTTP, HTTP snapshot (JPEG)
  – Joystick PTZ
H.264

- Up to 50% in bit rate savings: Compared to H.263v2 (H.263+) or MPEG-4 Simple Profile, **H.264** permits a reduction in bit rate by up to 50% for a similar degree of encoder optimization at most bit rates.

- High quality video: **H.264** offers consistently good video quality at high and low bit rates.

- Error resilience: **H.264** provides the tools necessary to deal with packet loss in packet networks and bit errors in error-prone wireless networks.

- Network friendliness: Through the Network Adaptation Layer, **H.264** bit streams can be easily transported over different networks.
Multicast vs Unicast

- **Bandwidth Requirements**
  - Communication model is server – client communication.
  - Specific networks have UNICAST or MULTICAST communications
  - Unicast is ONE to ONE: In a system that only has one client that needs the video stream, where there is only one control room monitoring all the cameras, then unicast communication is sufficient.
  - Multicast is ONE to MANY: if a system possesses multiple clients, where the control room and two other remote sites are monitoring the cameras, then multicast communications is a superior solution.
  - Determine the right traffic type for your network based on the number of video streams required in order to minimize device load and bandwidth requirements.

Copyright 2014 Cambium Networks, Ltd. All rights reserved.
IPTV challenges in wireless

• Main challenge is RTP
  – In most cases uses UDP as transport and multicast delivery

• Problems in wireless network
  – Errors caused by interference or low signal level
  – Bandwidth congestion leading to dropped packets
  – Latency/Jitter
QOS & IPTV Advantage
Key Features for IPTV

- Distance & Capacity : Up to 40 Miles & 230 Mbps aggregate throughput (40MHz) per AP
- Reliability : Supports consistent throughput and advanced modulation to maintain zero packet loss in highly congested areas
- QoS : MIR, TDD frame control & traffic prioritization
- Ease of deployment : Cambium ePMP CCTV kit simplifies the setup of a CCTV wireless network in combination with Axis HD cameras.
- Security : Advanced Encryption Standard to encrypt all the data on the fly
Air Fairness Adaptive Scheduler

- Air Fairness” Scheduler Prevents a few “Bad” SMs from dragging down the entire Access Point
- Scheduler makes sure the Bad SM’s gets the consistent throughput to make sure the video is more stable
- Resource Allocations based on Time, not Throughput
Rate Adapt Algorithm

- According to ITU-R recommendations video streaming should have packet loss less than 3%.

- For the video compression picture, the I-frame packet loss has more impact to video than the B and P-frame. (single B-frame IP packet loss is only impact 1 frame. But single I-frame packet loss will affect 14 frames.)

- ePMP provides consistent high throughput with advanced rate adapt mechanism that is targeted to keep zero packet loss even in highly congested areas.

- eFortify capability in ePMP maintains high performance constantly by handling external interference.

- ePMP advanced rate adapt mechanism with reduced packet loss is best in class for video with compression.
QoS over-air priorities

Packet scheduling algorithm is Weighted fair queuing with fixed weights

<table>
<thead>
<tr>
<th>Priority Level</th>
<th>ePMP Traffic Priority Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>Highest Priority (Served first)</td>
<td>VOIP (only utilized when VOIP Enable is set to Enabled)</td>
</tr>
<tr>
<td>Medium Priority (Served once highest priority traffic is sent)</td>
<td>High</td>
</tr>
<tr>
<td>Lowest Priority (Serviced once Highest and Medium priority traffic is sent)*</td>
<td>Low</td>
</tr>
</tbody>
</table>

*default, all traffic passed over the air interface is low priority
Quality of Service (QoS)

- Unicast Traffic assigned to a priority level by L2/L3 packet markings
- Broadcast/Multicast Traffic can be configured to be High or Low Priority
- Data is scheduled for OTA Transmission according to its priority

Prioritization Can be Altered by **SM Priority**

**SM Priority**
- **Normal** - No Change to Data Priority
- **High** - All non-Voice Ingress (Uplink) Traffic Treated as **High** Priority
- **Low** - All non-Voice Ingress (Uplink) Traffic Treated as **Low** Priority
Automatic QoS rules

• Multicast detection
  – When enabled, all multicast data is going to High priority queue.
## Custom QoS rules

<table>
<thead>
<tr>
<th>Rule Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoS</td>
<td>Class of Service; traffic prioritization is based on the 3-bit header present in the 802.1Q VLAN-tagged Ethernet frame header in the packet ingressing the AP’s Ethernet port.</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>Traffic prioritization is based on the VLAN ID of the packet ingressing the AP’s Ethernet port.</td>
</tr>
<tr>
<td>EtherType</td>
<td>Traffic prioritization is based on the two octet Ethertype field in the Ethernet frame ingressing the AP’s Ethernet port. The Ethertype is used to identify the protocol of the data in the payload of the Ethernet frame.</td>
</tr>
</tbody>
</table>
# Custom QoS rules

<table>
<thead>
<tr>
<th>Rule Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>Traffic prioritization is based on the source and (or) destination IP address of the packet ingressing the AP’s Ethernet port. A subnet mask may be included to define a range of IP addresses to match.</td>
</tr>
<tr>
<td>MAC</td>
<td>Traffic prioritization is based on the source and (or) destination MAC address of the packet ingressing the AP’s Ethernet port. A mask may be included to define a range of MAC addresses to match. MAC address is combined with the mask to define the range of allowed MAC addresses.</td>
</tr>
</tbody>
</table>
Quality of Service (QoS)

- SM Priority: Normal, High, Low
- L2 Markings: VLAN, CoS, EtherType, MAC
- L3 Markings: IP, DSCP
Reliable multicast with ePMP
IPTV on ePMP

- ePMP Solution provides so much consistent performance that operators are planning IPTV deployments over wireless!
- New ePMP Feature provides for reliable Multicast over wireless:
  - AP & SM perform IGMP Snooping and restrict multicast transmission only to air links that require them
  - Saves RF Resources
cnPilot helps with IPTV
## Configuring WAN Access

The following table shows the configuration details for the WAN connection:

<table>
<thead>
<tr>
<th><strong>Config</strong></th>
<th><strong>Value</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect Name</td>
<td>1_TR069_VOICE_INTERNET_R_VID_</td>
</tr>
<tr>
<td>Service</td>
<td>TR069_VOICE_INTERNET</td>
</tr>
<tr>
<td>IP Protocol Version</td>
<td>IPv4</td>
</tr>
<tr>
<td>WAN IP Mode</td>
<td>Static</td>
</tr>
<tr>
<td>NAT Enable</td>
<td>Enable</td>
</tr>
<tr>
<td>VLAN Mode</td>
<td>Disable</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>1 (1-4094)</td>
</tr>
<tr>
<td>Static IP Address</td>
<td>10.140.134.135</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>10.140.134.254</td>
</tr>
<tr>
<td>DNS Mode</td>
<td>Manual</td>
</tr>
<tr>
<td>Primary DNS Address</td>
<td>10.120.12.30</td>
</tr>
<tr>
<td>Secondary DNS Address</td>
<td>10.120.12.31</td>
</tr>
</tbody>
</table>
Multi-WAN connection

- Split out traffic
  - Internet
  - (Remote) Management
  - Voice
  - Other
  - Or a combo of above
- Use multiple VLANs on the WAN side
- Data for each connection can be
  - Bridged
  - Routed over PPPoE
  - NAT’ed
- Internet and ‘other’ can be bound to specific ports and SSIDs