Next Generation UC Clients and Endpoints
Agenda

• Next Generation Endpoints and Clients
• Call Control Enhancements
• Next Gen Design Considerations
  – Quality and Experience Control (Medianet, QoS & CAC)
  – Seamless Secure Access (Secure Connect)
  – Wireless LAN and Bluetooth
  – VXI Design
Next Generation Endpoints and Clients
Cisco UC Client Integration
Cisco Unified Client Services Framework (2nd Generation)
Cisco Jabber – CSF2G Capabilities

- Instant Messaging / Group Chat
- Rich Presence
- Contact Search
- Enterprise Call Control
- Business Video
- Web/Desktop Collaboration
- Conferencing
- Visual Voicemail
- App Integration (MS Office)
- Remote Access
- User Management & Authentication
- Rich Presence
- User Management & Authentication
- Contact Search
- User Management & Authentication
- App Integration (MS Office)
2nd Generation CSF (CSF2G)

- Operating System
  - Windows
  - OS X
  - iOS
  - Android

- Platform-Specific Implementation
  - Media A/V Engines
  - Media Device Interface
  - System Implementation
  - OS Abstraction

- Portable Libraries
  - APIs (C, C++)
  - Implementations
  - Call Control (SIP, CTI, DVO)
  - Media (A/V) Control
  - IM & Presence
  - Person Mngt (LDAP, AD, UDS)
  - Visual Voicemail (IMAP, REST)
  - Configuration (TFTP, CUP)
  - Remote Access (SSA)

- Products
  - User Interface, App Specific logic

- CSF2G
  - Jabber Phones
  - CUCI Integrations
  - Virtual Communicator
  - CUVA Mode

- Media A/V Engines
  - Media Device Interface
  - System Implementation
  - OS Abstraction
Extending CSF to New Next Gen Platforms

- Web Integrated - Quad
- Smartphones – Cius
Cisco Cius

802.11a/b/g/n, 3G/4G and Bluetooth
Wired to Wireless Transition
H.264 video standard
High-definition 720p video
Built-in Cameras
Dual Independent Displays
VDI Support – Vmware, Citrix, Wyse
Cisco AppHQ

Cisco Applications

Partner Applications

Market Applications

Android Mkt Place

Customer Applications

Home Depot Administrator

Home Depot User

“Admin Controlled Access “

USF Administrator

BoA User

#CiscoPlusCA
Cisco VXC Clients Brings together VDI And Collaboration (VXI)

New Desktop Virtualization Endpoints

- Integrated backpack 8900/9900 Phones — only requires monitor and keyboard
- Standalone VDI and integrated UC/VDI towers
- Desktop Virtualization UC Software

CIUS: 1st mobile converged tablet for voice, video, data apps and VDI

All endpoints support VMware View and Citrix XenDesktop
VXI with Cisco Cius

- VDI Support (Citrix, VMware, Wyse)
- HD media station
  - 3 USB ports
  - 10/100/1000-Gbps switch ports
  - Additional speaker for wideband hands-free
  - DisplayPort™ to connect display

Virtual Desktop

Cisco Cius

Video Out

HDMI/Display Port

USB/BT

Keyboard/ Mouse
Virtualization Experience Clients 2100/2200

- VDI Support ICA/RDP and PCoIP
- Power over Ethernet (POE)
- Supports 2 monitors
- Keyboard and Mouse
- Audio Mic and Speaker
- 4 USB ports

<table>
<thead>
<tr>
<th>VXC 2111</th>
<th>PCoIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>VXC 2112</td>
<td>ICA/RDP</td>
</tr>
<tr>
<td>VXC 2211</td>
<td>PCoIP</td>
</tr>
<tr>
<td>VXC 2212</td>
<td>ICA/RDP</td>
</tr>
</tbody>
</table>
Cisco VXC 4000

Enables UC voice capabilities for repurposed windows PCs used for virtual desktops

Eliminates the hairpin effect

Supports Citrix XenDesktop and VMware View

Endpoint support: WinXP, Win7
Cisco VXC 6215

- Thin client that unifies voice, video and VDI in one device
- Supports high quality, scalable voice and video, delivering optimal user experience
- Uses unique voice, video processing capabilities to eliminate the hairpin effect
- Linux based platform supports HDX/ICA, PCoIP/RDP
Cisco Jabber Mobile Clients
Cisco UC Mobility Architecture
Direct Connect Model

- Within Enterprise
- WiFi Access Point
- DMZ
- Cisco Adaptive Security Appliance or Integrated Services
- INTERNET (SSL VPN)
- Wireless Access Point
- PSTN Gateway
- PSTN Gateway
- Mobile Voice Network
- Roaming
- Unified IP Phones
- Communications Manager
- Microsoft AD and Exchange
- Unity Connection
- Uniject IM (cross-launch)
- WebEx (cross-launch)
- Unified Presence
- Enterprise and UC Applications
Cisco Precision Video Engine (CPVE) (CSF2G)

- **is** a standards-based high-definition and high-fidelity audio/video engine
- enables a revolutionary high-def and high-fidelity audio and video experience
- **is** responsible for handling all things related to audio & video processing
- **is** a wrapper for (former Tandberg) *Precision Media Engine* (PME) library
- CPVE **is** cross-platform and exposes a streamlined C++ API for easy integration
 BFCP (Binary Floor Control Protocol) (CUCM 8.6+)

BFCP enables **presentation sharing** between BFCP capable endpoints.

**Presentation Sharing** - ability to send a video stream such as a presentation from desktop in addition to the standard main video.

![Diagram showing BFCP connection between Jabber clients, Personal Telepresence systems, and Telepresence Rooms.](image)
Enhanced Call Control (ECC)

ECC is a single, cross-platform, Call Control API.

Integrates softphone, deskphone, BFCP, and P2P call control stacks with media, config retrieval, security, deskphone video, desktop share, SSA, MediaNet, Qos, etc.

<table>
<thead>
<tr>
<th>CC API</th>
<th>Config</th>
</tr>
</thead>
<tbody>
<tr>
<td>Softphone Call Control</td>
<td>MediaNet</td>
</tr>
<tr>
<td>Deskphone Call Control</td>
<td>SSA</td>
</tr>
<tr>
<td>BFCP Control</td>
<td>Secure Signalling</td>
</tr>
<tr>
<td>P2P Control</td>
<td>Serviceability</td>
</tr>
<tr>
<td>Media Termination</td>
<td>Win, Linux, Mac, iPad</td>
</tr>
<tr>
<td>CPVE / GIPS</td>
<td></td>
</tr>
</tbody>
</table>

ECC builds on and depends on the CSF2G Libraries

ECC clients just include the modules they need
<table>
<thead>
<tr>
<th>ECC Features</th>
<th>Jabber/ Win</th>
<th>VXC</th>
<th>Web Phone</th>
<th>CUCILync</th>
<th>Jabber/ Mac</th>
<th>Jabber for iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic call ctrl – make, receive, dtmf, transfer, conf, call forward, divert, multiple calls, QoS</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Advanced call ctrl – call park, shared line, SNR, URI dialing, call pickup, hunt group pickup, handoff to mobile</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>CTI Control/ Deskphone control</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>CTI Servitude</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>CPVE Video</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>GIPS Video</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Security – secure SIP, SSA</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Serviceability – failure &amp; recovery, network change, SRST, SSO, CTI load balancing</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>BFCP Desktop share</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>PC-to-PC voice &amp; Video</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Medianet support</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Poly-device registration – CSF, UPC, TCT, VXC</td>
<td>x</td>
<td></td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Windows support</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Linux Support</td>
<td>x</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mac support</td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iOS support</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>64-bit</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Medianet
Medianet?

Medianet is an end to end architecture for a media-optimized network.

Medianet allows the deployment, scalability and optimization of quality of experience of rich media solutions into the organization.

**Media Aware**: Detection and optimisation of different types of media and application.

**Endpoint aware**: Easy deployment. Automatic Detection and Configuration of endpoints.

**Network Aware**: Detect and respond to changes in devices, connection and service availability.
Medianet
Media Services Interface

A Software Development Kit (SDK) that resides on endpoints / applications that enables:

• Tight integration between applications and the network

• Endpoints take advantage of intelligent network services

Provides a set of APIs which abstracts and simplifies integration with the network:

• Endpoints do not need to be aware of network layer protocols

• Implementation is consistent across all endpoints to ensure intelligent services are reliably applied
**Metadata**

**Build Infrastructure**

**Expand Production**

**Expand Actions**

Network Readiness: ISRG2, Cat3k, Cat4k, ASR1k, Cat6k

MSI Based End points (WebEx, VXI, TP), MSP, NBAR

Video Monitoring, QoS, FNF, PBR, PfR

---

**Table:**

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Destination IP</th>
<th>Port 1</th>
<th>Port 2</th>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>10.1.1.1</td>
<td>2134</td>
<td>80</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td>10.76.109.45</td>
<td>10.76.109.51</td>
<td>1200</td>
<td>2000</td>
<td></td>
<td>WebEx Video</td>
</tr>
<tr>
<td>10.76.109.45</td>
<td>10.76.109.50</td>
<td>450</td>
<td>5060</td>
<td></td>
<td>SIP</td>
</tr>
<tr>
<td>30.1.1.1</td>
<td>135.1.1.1</td>
<td>1500</td>
<td>1600</td>
<td></td>
<td>WebEx Video</td>
</tr>
<tr>
<td>20.1.1.1</td>
<td>125.1.1.1</td>
<td>1500</td>
<td>1600</td>
<td></td>
<td>Surveillance</td>
</tr>
</tbody>
</table>

**Metadata Database**

**Video Monitoring**

**PIR/PBR**

**Netflow**

**QoS**

NBAR and MSP Producing Metadata

WebEx

VXI/VNA

TP/Tandberg
Quality of Service (QoS) Updates
Whole Sessions are composites of multiple application flows (Video, Voice, Data).

More & More apps are opaque (ex: video streams).

Increasing use of Encryption.

Per flow and stateful are key attribute of modern classification.
Application Awareness
Identification and Classification

PROBLEM
- What is going on in my network?
- Voice Traffic classification
- Video Traffic classification
- Critical applications

SOLUTIONS
- Implicit: MCQ, DPI (NBAR2, MSP)
- Explicit: Metadata
- Indirect: RSVP Agent, Media Services Proxy (MSP)
Application Awareness

Control

PROBLEM
• How do I optimize Voice & Video?
• How do I optimize my Network Resources?
• How do I manage video quality during congestion?

SOLUTIONS
• QoS
• Medianet
AutoQoS Updates

• Currently all switch platforms support AutoQoS-VoIP
  ▪ Best practice QoS designs for IP Telephony (only) deployments
• Catalyst 2K/3K now supports AutoQoS for Medianet
  ▪ AutoQoS SRND4
  ▪ Supports not only IP Phones, but also TelePresence & IPVS cameras and softphones
  ▪ Autoprovisions ingress trust, classification, marking & policing
  ▪ Autoprovisions ingress queuing (as applicable)
  ▪ Autoprovisions egress queuing

Two high-level approaches:

1. Local packet marking
2. Create identifiable traffic streams edge devices mark DSCP, either by sending media on specific port ranges, or via Medianet

Local Packet Marking (depends on OS platform)

**Windows 7**
Does not allow applications to mark DSCP (unless Network Config Ops group member)

**Windows XP**
Jabber will mark packets using an API from windows 2000
QoS and Trust with CSF Desktop Clients

- **Windows 7 QoS and Security Model**
  - Windows 7 user mode apps can't set QOS / DSCP markings.
  - Recommended to use the QOS Policy Engine via AD Group Policies

- Using Group Policy for CSF Clients (Jabber, CUCI-LYNC)
  media ports can individually be marked with correct DSCP value

- Alternative switch configuration

- CSF uses different port ranges for different types of media
  - Centrally administrated port range configuration from CUCM, lower half utilized for audio and upper half utilized for video streams
• How to enforce a consistent network policy when classification are not available along the path?
  – Eg: Rule: Prioritize Voice communication from Marylou to John?
• Endpoint can provide information not available or visible on the wire
Medianet Flow Metadata

1. Application or Client Creates Metadata

<table>
<thead>
<tr>
<th>IP Src</th>
<th>IP Dst</th>
<th>Prot</th>
<th>L4 Src</th>
<th>L4 Dst</th>
<th>Application</th>
<th>Vendor</th>
<th>Dial From</th>
<th>Dial To</th>
<th>Caller ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.1.2</td>
<td>20.1.1.2</td>
<td>UDP</td>
<td>2000</td>
<td>4000</td>
<td>Video-Conference (Audio)</td>
<td>Cisco</td>
<td>83922564</td>
<td>85268229</td>
<td>Albert Albatross</td>
</tr>
</tbody>
</table>

2. Metadata Announcement

3. Media Flow

QoS based on Metadata

Export of data to NMS
Metadata Integrating with QoS

<table>
<thead>
<tr>
<th>Metadata Database</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
</tr>
<tr>
<td>10.76.109.45</td>
</tr>
<tr>
<td>30.1.1.1</td>
</tr>
<tr>
<td>20.1.1.1</td>
</tr>
<tr>
<td>30.1.1.1</td>
</tr>
</tbody>
</table>

Policy-map Metadata

class audio-class-1
set dscp af41
!
class-map match-all audio-class-1
match application webex-audio
Call Admission Control (CAC)
Call Admission Control - Mandatory?

- Over-provisioning for Unified Communications media is extremely difficult
- UC media traffic cannot be “squeezed” or delayed (it is inelastic), so congestion control cannot be used
- Different policies need to be applied to different types of calls
Call Admission Control Approaches

- Works well for trivial topologies (hub-and-spoke)
- Easy to deploy
- Handles different policies (per media type, per calltype, per user)
- Unaware of network state

- Handles any network topology
- Support different policies / multiple applications and instances
- Optimal use of resources (accurate tracking of path and bandwidth, reacts to network failures/changes)
- Preserves user experience
## Admissions Control and QoS Synchronization

- CAC model needs to reflect QoS / Network reality
- Same-class application DBs must add up to or less than class bandwidth

<table>
<thead>
<tr>
<th>Application Class</th>
<th>PHB</th>
<th>Admission Control</th>
<th>Congestion Management &amp; Congestion Avoidance</th>
<th>Cisco Video Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>VoIP Telephony</td>
<td>EF</td>
<td>Required</td>
<td>Priority Queue (PQ)</td>
<td>IP Phone and Client Telephony</td>
</tr>
<tr>
<td>Real-Time Interactive</td>
<td>CS4</td>
<td>Required</td>
<td>(Optional) PQ</td>
<td>Cisco TelePresence and CIUS Video</td>
</tr>
<tr>
<td>Multimedia Conferencing</td>
<td>AF41</td>
<td>Required</td>
<td>BW Queue + DSCP WRED</td>
<td>Cisco CUPC / Video Telephony : EX : MXP</td>
</tr>
</tbody>
</table>
Admission Control Policy and Mediation

- **Remember**: Admission Control enables deterministic session experience.
- Simplest form of mediation is denying additional sessions.
- Advanced forms may force renegotiation of existing sessions to lower experience (lower bitrate, resolution, fps, no video etc.).
Session Level Bandwidth Modifier (CUCM 8.6+)

Specifies the max amount of bandwidth needed when all the media streams used. Typically this will be less than the sum of individual streams values (not all streams have their maximum at the same time).

There are 3 Session Level Bandwidth Modifier values:

- **b=TIAS:<bandwidth-value>**
  Transport Independent Application Specific Maximum (TIAS) bandwidth modifier is a bit-rate value. This value is the max needed by the application (SDP session level) or media stream (SDP media level) without headers.

- **b=AS <application Specific>**
  Application Specific maximum bandwidth is dependent on the application's notion of maximum bandwidth.

- **b=CT <conference Total>**
  Conference Total gives a maximum bandwidth that a conference session will use. Its purpose is to decide if this session can co-exist with any other sessions.
Adaptive Video and Call Admission Control

- Video application automatically adapts (adjusts bitrate) to available bandwidth
  - Used with admission control mediation
  - Video Escalation / De-escalation
- If used without admission control, place in best effort QoS class
  - Watch for fairness and other-traffic starvation
  - Keep business critical traffic separate

---

Soft client Video ad-hoc

ad-hoc VC

Room based TP ad-hoc

Scheduled Event

Room based TP Scheduled
CVPE Media Resilience – Bandwidth Adaptation

Packet loss reported by remote endpoint via RTCP Receiver Reports (RRs) and CPVE adjusts bitrate accordingly

Two types of Bandwidth Adaptation

1. **Static Network Adaptation** – pick best starting rate to transmit new call and best possible initial receive parameters to influence incoming bandwidth

2. **Dynamic Network Adaptation** - adjust the transmit rate during call to maximise bandwidth use when needed but avoid congestion

Reducing the configured sending rate:
There are 2 phases of Downward Adaptation

1. **Startup Phase** - The first 10 seconds since receiving the first RR
   - Minimum of 2 RRs received reports losses

2. **Steady State**
   - The network is classified as **Consistently Lossy** and
   - The most recent observation has significant packet loss (i.e. > 1%)
Media Resilience – Bandwidth Adaptation

Note for downspeed:
• Bitrate is never reduced if the network is classified as Burst Lossy or Lossless
• A new reduced bitrate is never lower than 128 kbps
• Subsequent bitrate reductions (if required) are spaced by minimum of 10 seconds

CPVE Increases the configured transmit rate if - and only if –
• The network is classified as Lossless
• The current configured sending rate is lower than the allowed maximum media bandwidth available for the session

If the above is satisfied, increase bitrate by MAX (15% of current send rate, 64 kbps)

Bitrate increases (if criteria met) are separated by 20 seconds minimum.
CPVE will also adjust the encoding video width and height that are supported by the current video capture device according to the newly adapted send rate.

Important Note: The above behavior assumes the following:
• The other endpoint supports RTCP and sending of RTCP RRs
• The other endpoint sends RTCP RRs every 5 seconds
If either of these are false, the timing and behavior of the above will be significantly different, and BW adaptation may not work at all
Seamless Secure Access (Secure Connect)
**Traditional VPN**

**Secure the Device**

- **Other apps gain access to enterprise network**
- **UC App uses any existing protocols**
- **VPN client is separate, platform-specific install**
- **User or UC App can trigger VPN connection**

**Diagram details:**
- Local Resources
- Internet
- Other App
- UC App
- VPN Client
- Encrypted connection
- ISR, ASA
- Unified Presence
- Unified Communications Manager
- Unified MeetingPlace
- Microsoft AD and Exchange
- Unified IP Phones

**UC App**
- Use any existing protocols
- Can trigger VPN connection

**Other App**
- Gain access to enterprise network

**VPN Client**
- Separate, platform-specific install
Other apps do not access the enterprise network

Jabber Secure connect feature
Secure the Jabber Application or Device

- Other apps
- Secure Connect
- Internet
- Local Resources
- ASR, ISR, ASA
- Unified Communications Manager
- Unified Presence
- TFTP
- Unified MeetingPlace
- Microsoft AD and Exchange

Jabber app uses existing protocols

Access to all enterprise services for Jabber app

Single app. Secure connection is a feature.

Works with existing Cisco secure remote access infrastructure

ASR, ISR, ASA

Internet

Local Resources

Jabber (CSF)

Other apps

Secure Connect

Unified MeetingPlace

Unified Presence

Unified Communications Manager

TFTP

Microsoft AD and Exchange

Jabber app uses existing protocols

Other apps do not access the enterprise network
Secure Connect
Common Remote Access Infrastructure

- Diverse Endpoint Support
- AnyConnect Mobile Client or Cisco Jabber
- Security Integrated into the network

Security
- Data Loss Prevention
- Threat Prevention
- Acceptable Use
- Access Control

Experience
- Outside Enterprise
- Access Granted
- Intranet
- Corporate File Sharing
- Always-on Intelligent Connection
Cisco Jabber Secure Connect Feature Details

- Secure connect is a built-in feature of Jabber CSF
  - No separate security app needed

- Secures the connection for Jabber application traffic and workloads to the enterprise, instead of securing the entire device

- Enterprise-grade encryption and authentication
  - Leverages Cisco ASA or Cisco ISR security solutions

- Seamless user experience as part of Jabber
  - Jabber app controls secure connect in the background
Wireless LAN and Bluetooth Updates
Wireless Recommendations for Voice/Video

- 802.11n
- Secure Roaming
- QoS and CAC
- Wireless Cell Design
- Bluetooth Implications
Wireless Security Recommendations

• 802.1x EAP Types
  EAP-FAST
  PEAP
  
• Authentication
  Open
  WPA/WPA2
  WPA/WPA2 PSK

• Encryption
  AES
  TKIP/MIC
  WEP

Note: CCKM (Cisco Centralized Key-Management) should be implemented for seamless roaming
Cisco Centralized Key Management (CCKM)

- With 802.1x authentication recommended to implement CCKM for fast secure roaming
- 802.1x introduces delay during roaming with requirement for full re-authentication
- CCKM centralizes the key management and reduces the number of key exchanges.
- With CCKM roaming times can be reduced from 400-500 ms to less than 100 ms, hence the transition time from one AP to another will be transparent to the user
- CCKM can be utilized with the following security combinations

<table>
<thead>
<tr>
<th>802.1x Type</th>
<th>Key Management</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP-FAST</td>
<td>WPA2, WPA</td>
<td>AES, TKIP</td>
</tr>
<tr>
<td>PEAP</td>
<td>WPA2, WPA</td>
<td>AES, TKIP</td>
</tr>
</tbody>
</table>
WLAN Admission Control and QoS

• Admission control grants clients access on per-WLAN (SSID)
• This is typically done in one of two ways
  – Load – number of calls based on channel load
  – TSpec – based on a host of additional parameters
• Wi-Fi Multimedia (WMM) 802.11e’s Traffic Specification (TSpec) takes much more than load into account
  – Clients request admission based on: traffic priority (access category), power save, mean data rate, frame sizes, min PHY data rate
Wi-Fi Multimedia (WMM)

• What is WMM?
  ▪ supplement to 802.11 MAC layer
  ▪ Allows Diff-Serv QoS by creating four queues, called Access Categories
  ▪ Access Categories access channel via EDCA (Enhanced Distributed Channel Access), an enhancement of the existing DCF (Distributed Coordination Function)

• What does WMM add?
  ▪ Uplink frames are marked with 802.1p CoS
  ▪ Prioritized access for uplink traffic
  ▪ ACM flag allows uplink access categories to be enabled/disabled
802.11e / WMM Media Access Classifications

- Separates traffic types into 4 QoS access categories (AC)
- Background, Best Effort, Video, Voice
- These 4 ACs also have unique delay and random back off characteristics for accessing the RF channel (EDCA)

![Diagram showing Applications categorized into Background, Best Effort, Video, and Voice with Internal Collision Resolution]
Quality of Service (QoS) with Wireless

To ensure proper queuing, use the following suggestions:

- Ensure WMM is enabled in SSID config.
- Enable network DSCP or configure QoS policy to set the DSCP values.
- Enable the “Platinum” QoS profile in the SSID configuration when using Cisco Unified Wireless LAN Controller technology.
- QoS policy needed for Cisco APs in autonomous (standalone) mode.

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>DSCP</th>
<th>802.1p</th>
<th>WMM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voice</td>
<td>EF (46)</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Video</td>
<td>AF41 (34)</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Call Control</td>
<td>CS3 (24)</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>
SIP Based QoS (WLC code stream 6.0)
Intercept and snoop SIP traffic (AP: Upstream, WLC: downstream) to determine voice session and set QoS
RFC 3261 compliant client

SIP Based CAC (WLC code stream 7.0)
Enable the network to roam voice session between APs based on available bandwidth
Feature is applicable to SIP phone w/o TSPEC
Bandwidth parameters are configured manually on per session basis
Cisco’s Application-Aware QoS (When Remarking is Required)

All QoS is Best Effort Unless Otherwise Remarked by the SIP Engine at the AP

Best Effort QoS

Assume all L3 Markings are Stripped off before entering the controller.

The SIP Snooping Engine will Reprioritize RTP Streams Identified in the SIP packet
Cisco’s End-to-End QoS Model

QoS Marking are Preserved and Translated into WMM Access Categories at AP

L3 Markings are set Correctly by the Servers and clients and Trusted Through The Network
Data Rate Config and Wifi Channel Utilization

To increase channel utilisation on WLAN, data rates in use need to be faster.
- To do this the lower data rates must be disabled thereby forcing the use of the faster data rates that are enabled for WLAN
- Recommended to disable rates below 12 Mbps for best results
  - 802.11b data rates should only be enabled if legacy clients exist in 2.4 GHz
  - Recommended use 5 GHz for CIUS / UC devices if legacy devices in 2.4 GHz

<table>
<thead>
<tr>
<th>802.11 Mode</th>
<th>Mandatory Data Rates</th>
<th>Supported Data Rates</th>
<th>Disabled Data Rates</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>12 Mbps</td>
<td>18 - 54 Mbps</td>
<td>6,9 Mbps</td>
</tr>
<tr>
<td>802.11g</td>
<td>12 Mbps</td>
<td>18 - 54 Mbps</td>
<td>1,2,5.5,6,9 Mbps</td>
</tr>
<tr>
<td>802.11a/n</td>
<td>12 Mbps</td>
<td>18 – 54 Mbps, MCS 0 – MCS 7 (MCS 8 – MCS 15)</td>
<td>6, 9 Mbps</td>
</tr>
<tr>
<td>802.11g/n</td>
<td>12 Mbps</td>
<td>18 – 54 Mbps, MCS 0 – MCS 7 (MCS 8 – MCS 15)</td>
<td>1,2,5.5,6,9 Mbps</td>
</tr>
</tbody>
</table>
WLAN Cell Design

- Cell edge should be -67 dBm, which is the minimal required signal strength for UC
- At least 15-20% overlap of adjacent cells
- Recommended to have dual APs available with adequate signal in critical use areas.
Call Capacity

- Ensure network is designed to accommodate desired call capacity
- Cisco APs can support up to 27 bi-directional voice streams for both 802.11a and 802.11g at 24 Mbps or higher
- Call capacity can be reduced if using Coexistence
- Coexistence = 802.11g/n + Bluetooth
- Use of 802.11b is NOT recommended
## Audio Only Call Capacity

- Audio only call capacity for 802.11a/g/n without Bluetooth is below
- Audio only call capacity when using 802.11n data rates to be determined

<table>
<thead>
<tr>
<th>Max # of Streams</th>
<th>802.11 Mode</th>
<th>802.11 Data Rate</th>
<th>Channel Width</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>802.11a or 802.11g + Bluetooth Disabled</td>
<td>12 Mbps</td>
<td>20 MHz</td>
</tr>
<tr>
<td>27</td>
<td>802.11a or 802.11g + Bluetooth Disabled</td>
<td>24 – 54 Mbps</td>
<td>20 MHz</td>
</tr>
<tr>
<td>27</td>
<td>802.11a/n or 802.11g/n + Bluetooth Disabled</td>
<td>MCS 0 – MCS 7</td>
<td>20 MHz &amp; 40 MHz</td>
</tr>
</tbody>
</table>
## Audio + Video Call Capacity

- Video call capacity for 802.11a/g/n without Bluetooth is below:
- Video call capacity when using 802.11n data rates and HD 720p TBD

<table>
<thead>
<tr>
<th>Max # of Streams</th>
<th>802.11 Mode</th>
<th>Video Rate</th>
<th>802.11 Data Rate</th>
<th>Channel Width</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 - 10</td>
<td>802.11a or 802.11g + Bluetooth Disabled</td>
<td>384 Kbps</td>
<td>12 – 54 Mbps</td>
<td>20 MHz</td>
</tr>
<tr>
<td>2 - 5</td>
<td>802.11a or 802.11g + Bluetooth Disabled</td>
<td>1 Mbps (VGA)</td>
<td>12 – 54 Mbps</td>
<td>20 MHz</td>
</tr>
<tr>
<td>2 - 5</td>
<td>802.11a or 802.11g + Bluetooth Disabled</td>
<td>720p (HD)</td>
<td>12 – 54 Mbps</td>
<td>20 MHz</td>
</tr>
<tr>
<td>5–13 (20Mhz) 8–16 (40Mhz)</td>
<td>802.11a/n or 802.11g/n + Bluetooth Disabled</td>
<td>384 Kbps</td>
<td>MCS 0 – MCS 7</td>
<td>20 MHz &amp; 40 MHz</td>
</tr>
<tr>
<td>2–8 (20Mhz) 3–11 (40Mhz)</td>
<td>802.11a/n or 802.11g/n + Bluetooth Disabled</td>
<td>1 Mbps (VGA)</td>
<td>MCS 0 – MCS 7</td>
<td>20 MHz &amp; 40 MHz</td>
</tr>
<tr>
<td>1–4 (20Mhz) 2–7 (40Mhz)</td>
<td>802.11a/n or 802.11g/n + Bluetooth Disabled</td>
<td>720p (HD)</td>
<td>MCS 0 – MCS 7</td>
<td>20 MHz &amp; 40 MHz</td>
</tr>
</tbody>
</table>
Bluetooth Headsets

Bluetooth headsets are available from the following vendors

**Aliph®**
- Jawbone Icon for Cisco
- Jawbone Icon

**Plantronics®**
- Discovery 655, 925, 975
- Explorer 360, 390, 395
- Voyager 510, 520, 855, Pro

**Jabra®**
- BT5020, BT8040, BT5010, T533
- JX10 Series 2

**Motorola®**
- H720, H780
Bluetooth Coexistence Audio Only Call Capacity

- When using Coexistence (802.11b/g/n + Bluetooth), call capacity is reduced to the following:
  - Recommend to deploy 802.11a/n (5 GHz) when using Bluetooth to avoid Coexistence limitations
  - Use of 802.11b is not recommended when using Coexistence.

<table>
<thead>
<tr>
<th>Max # of Streams</th>
<th>802.11 Mode</th>
<th>802.11 Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>802.11g + Bluetooth Enabled</td>
<td>12,(18 – 54) Mbps</td>
</tr>
<tr>
<td>TBD</td>
<td>802.11g/n + Bluetooth Enabled</td>
<td>12,(18 – 54 Mbps, MCS 0 – MCS 7)</td>
</tr>
</tbody>
</table>
The Impact of a Crowded Spectrum
Performance At Risk in Unprotected Networks

- Reduced network capacity and coverage
- Poor quality voice and video
- Potential complete link failure

<table>
<thead>
<tr>
<th>Interference Type</th>
<th>Near (6m)</th>
<th>Far (20m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4 or 5 GHz Cordless Phones</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Video Camera</td>
<td>100%</td>
<td>57%</td>
</tr>
<tr>
<td>Wi-Fi (busy neighbour)</td>
<td>90%</td>
<td>75%</td>
</tr>
<tr>
<td>Microwave Oven</td>
<td>63%</td>
<td>53%</td>
</tr>
<tr>
<td>Bluetooth Headset</td>
<td>20%</td>
<td>17%</td>
</tr>
<tr>
<td>DECT Phone</td>
<td>18%</td>
<td>10%</td>
</tr>
</tbody>
</table>

Source: FarPoint Group
Detect and Classify

CleanAir – Detect and Classify

Uniquely identify and track multiple interferers
Assess unique impact to Wi-Fi performance
Monitor AirQuality
Locate and Mitigate

High-resolution interference detection and classification logic built-in to Cisco’s 802.11n Wi-Fi chip design. Inline operation with no CPU or performance impact.
WLAN Bandwidth Management

With Video Now More Important Than Ever

- 11n Packet Aggregation Configuration for Dense Video/Voice
- Manage out all possible interferers
- Manage out all possible low data rates
- Use Band Select
- Use Call Admission Control
- Use Quality of Service
- Enable Windows XP and Windows 7 QoS
Virtual Experience Infrastructure (VXI)
Cisco Virtual Experience Infrastructure
Open Validated Architecture

Virtualised Data centre
- Collaboration Applications
- MS Office
- Desktop Virtualisation Software
  - citrix
  - VMware
- Hypervisor
  - Microsoft OS
  - VMware

Virtualisation-Aware Borderless Network
- Branch
  - VDS/CDN
  - Mobility
  - Clean Air
- Access switching w/PoE
  - WAAS

Virtualised Collaborative Workspace
- Cisco Clients
- Cius Business Tablets
- Cisco Virtualisation Experience Clients

Thin Client Ecosystem
- Thin Client Ecosystem
- [Logos]

End-to-End Security, Management and Automation
Cisco Innovation Solving VDI + Video + Voice

Avoiding the Hairpinning Problem

The Hairpinning Problem

- Real time media used for Voice and Video
- Forced through VDI display protocols
- Display protocols never intended for latency/jitter sensitive traffic
- Poor user UC experience when delivered through VDI
- Media flows back to Data Centre
- Latency / Jitter
Cisco Innovation Solving VDI + Video + Voice

Avoiding the Hairpinning Problem

VXI Solution

- VXC intelligence recognises real-time media session
- Redirects traffic outside of display protocol
- Facilitates direct connection to CUCM then b/w endpoints
- Media path never traverses display protocol

Benefits

- Bandwidth reduction
- Improved experience both for desktop and UC
- High quality voice and video
  - QoS, CAC
  - no hairpinned of media
Rich Media User Experience restored by VXC 2x00 & VXI

Media Flow
Outside of Display Protocol

VXC

Signalling

PCoIP, ICA/RDP

Desktop O/S

Desktop Virtualization S/W
VMWare/Citrix

Hypervisor
VMWare/Citrix

Connection Broker

VM

Data Center

Unified CM and Unified Presence Server
Rich Media restored by VXC 6215/4000 via Cisco VXI

- Video & Voice Support
- Linux based endpoint
- Monitors
  - Single: 2560x1600
  - Dual: 1920x1200
- No PoE

- Software Appliance on XP and Win 7
- Enables VXI Collaboration for refurbished PCs

End User

VXC 6215

VXC 4000

Media Flow outside of Display Protocol
Next Generation Endpoints and Clients