



Secure Wireless Architectures for Converged Applications



Stephen Orr

Consulting System Engineer CCIE #12126

Cisco Federal

sorr@cisco.com

Session Objectives

This session WILL cover:

- **WLAN Primer**
- **Needs of Converged Applications**
 - Wireless Quality of Service Principles
 - WLAN System-wide QoS Requirements
 - Where QoS Fits into the Wireless Network
- **Mobility Impact on Wireless Security and VoWLAN**

Anti-Session Objectives

This session WON'T cover:

- **Basic 802.11/WLAN topics and design**
- **RF cell planning and site surveying**
- **In-depth switching and routing QoS principles**

Key Takeaways

The Key Takeaways of this presentation are:

- **Understand when, where, and why QoS is necessary**
- **Appreciate the *end-to-end* requirements of QoS**
- **Understand where VoWLAN fits into the QoS discussion**
- **Apply QoS/VoWLAN while maintaining security**

802.11 WLAN Standards Activities

The “Alphabet Soup”

| <u>Standard</u> | <i>Develop Spec</i> | <i>Interoperability Testing</i> |
|-------------------------------|---------------------|---------------------------------|
| ▪ 5 GHz, 54 Mbps | IEEE 802.11a | Wi-Fi Alliance 802.11a |
| ▪ 2.4 GHz, 11 Mbps | 802.11b | 802.11b |
| ▪ Multiple Regulatory Domains | 802.11d | |
| ▪ Quality of Service (QoS) | 802.11e | WMM |
| ▪ Inter-Access Point Protocol | 802.11f | |
| ▪ 2.4 GHz, 54 Mbps | 802.11g | 802.11g |
| ▪ DFS & TPC | 802.11h | |
| ▪ Security | 802.11i | WPA, WPA2 |
| ▪ Japan 5 GHz Channels | 802.11j | |
| ▪ Measurement | 802.11k | |
| ▪ Maintenance | 802.11m | |
| ▪ High-Speed | 802.11n | |
| ▪ Fast Roaming | 802.11r | |
| ▪ Mesh Networking | 802.11s | |
| ▪ Management Frame Protection | 802.11w | |



Yellow – Over the air protocols
Orange – Key Wi-Fi standards
White – All other

Introduction to QoS Principles



First: Why QoS for WLAN?

- **Wireless is fundamentally different from wired**
 - Far more stringent bandwidth limitations
 - Limited spectrum (few non-overlapping channels)
 - Half-duplex medium
 - Every directed data and management frame is ACK'd
 - 'Listen Before Talk' contention model
- **This all makes WLAN highly susceptible to latency and jitter**
- **Can't really 'throw bandwidth' at the problem, either**

QoS Concepts

- **Latency**

 - Fixed Delay

 - Variable Delay

- **Jitter**

 - Delay Variance

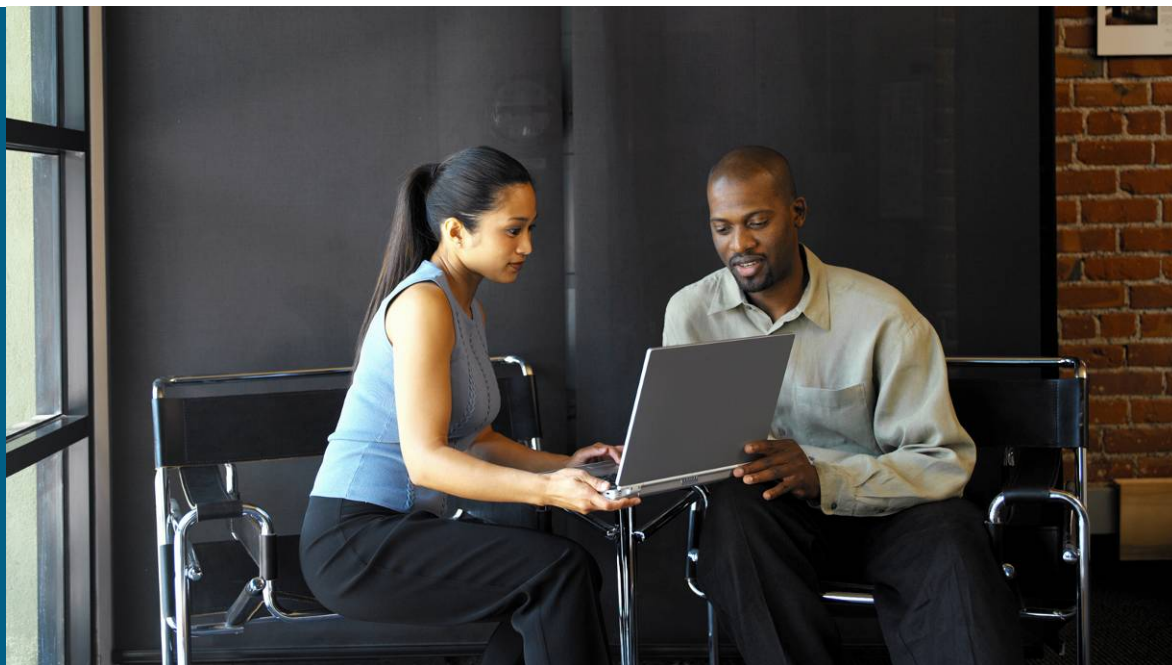
- **Loss**

 - Packet/Frame Loss

So, Where's the Need for QoS in WLAN?

- In the past, there hasn't been much QoS need
 - WLANs designed for coverage and basic data access
- Now, WLANs designed for mission-critical applications
 - Shift from coverage to capacity to allow for
 - More client devices
 - More requiring data apps (higher bandwidth needs)
 - Emergence of voice- and video-over-WLAN needs*
 - Proliferation of voice handsets (such as Cisco's 7920)*
 - Latency-sensitive applications (softphone applications, IPTV, etc)*

How Does QoS Work Today in 802.11?



Without 802.11e... It Doesn't

- **802.11 networks are completely egalitarian**

Every device, AP included, has equal access to transmit

No device has precedence over any other

Example: voice handsets abide by the same access rules as laptops

All transmissions for each individual device have the same access, transmitting in 'FIFO' fashion

No application has more transmit 'weight' than any other

Example: on a single laptop, a voice frame has the same right to transmit as any other frame, such as a web frame

802.11's Access Rules

- **Distributed Coordinated Function (DCF)**

Transmission rules followed by all clients

DCF is 802.11's rules of the road

- **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**

Responsible for mediating access to the air

CSMA/CA is 802.11's traffic lights

802.11's Access Rules

- **Distributed Coordinated Function (DCF)**

 - Transmission rules followed by all clients

 - Interframe spaces (IFS) are used to 'prioritize' traffic

 - IFS are very short delays before transmissions are allowed

 - The **Short Interframe Space (SIFS)** is used for transmission of management and control frames

 - The **DFS Interframe Space (DIFS)** is used before the transmission of data frames

- **CSMA/CA allows 'peaceful' coexistence of many devices trying to transmit simultaneously**

802.11's Access Mediation

- **Carrier Sense Multiple Access with Collision Avoidance**

 - CSMA/CA responsible for mediating access to the air

 - Reduces the likelihood of a transmission collision

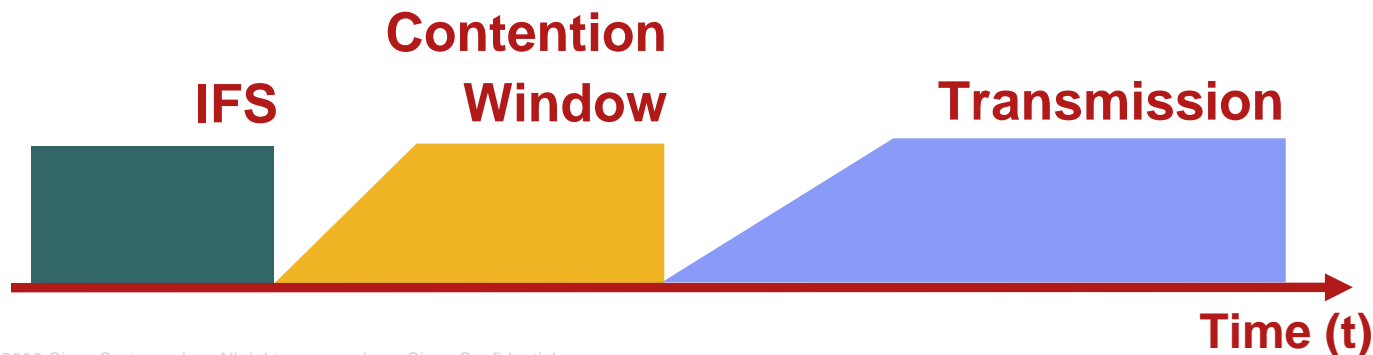
 - Provides probabilistically fair access to every device

- **CSMA/CA provides a framework clients follow before being allowed to transmit: *'Listen before talk'***

 - Wait the appropriate interframe space (SIFS or DIFS)

 - If medium is free, wait to make sure no one else is beginning to transmit (this is called the 'backoff')

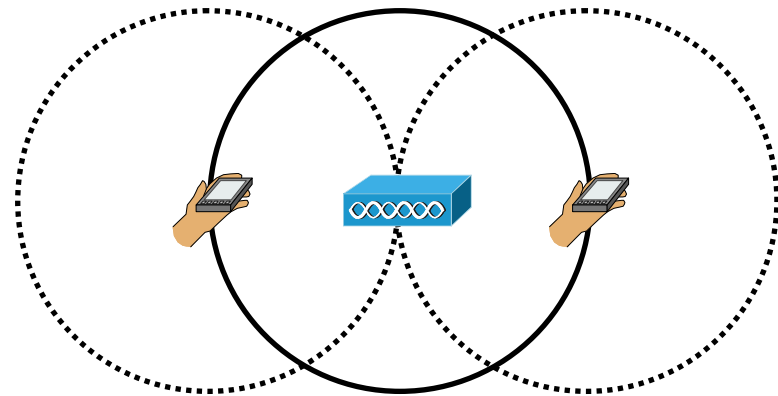
 - If medium is still free after 'backoff', then transmit



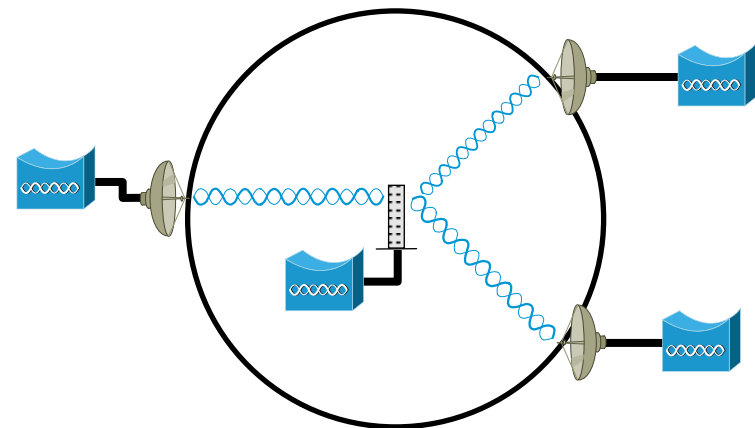
Hidden Nodes Are Also a QoS Issue

- If you can't hear a frame, you can't avoid colliding with it
- Only the AP can see and be seen by all nodes
- 11b and 11g coexistence creates a hidden node potential

CTS-to-self is typically used



Hidden Nodes Due to Range



Hidden Nodes Due to Directional Antennas

Retrofitting 802.11 with QoS

- Intelligent queuing at the AP allows the WLAN to realize downstream, over-the-air QoS

Upstream, from AP to controller QoS applied, as well

- Prioritization done per-WLAN

Additionally/alternatively, QoS can be assigned per user via Identity-based Networking Services (IBNS)

- DiffServ and 802.1p priority preserved upstream and downstream between AP and controller

--- To complete WLAN QoS, [add WMM/802.11e](#) ---

Introduction to 802.11e and Wireless Multimedia (WMM)



QoS with WMM/802.11e

- **IEEE TGe ratified 802.11e in late 2005**
- **11e outlines two modes of operation**
 - Enhanced Digital Channel Access (EDCA)**
 - Hybrid Coordinated Function Controlled Channel Access (HCCA)**
- **The Wi-Fi Alliance moved early with a subset of 11e called Wireless Multimedia (WMM), similar to the way they did with WPA/11i**
- **WMM specifies a subset of 11e functionality, called EDCA**
 - Very few vendors support HCCA**

EDCA

- **EDCA is similar to DCF's contention-based access model in that it is up to each individual device to determine when it is allowed to access the medium**

Prioritization is done by allowing differing traffic types varied access levels based on how long they wait to transmit

Prioritizing with EDCA Access Categories

- WMM/11e specifies four different classifications of traffic called ***access categories***, or ACs

Background

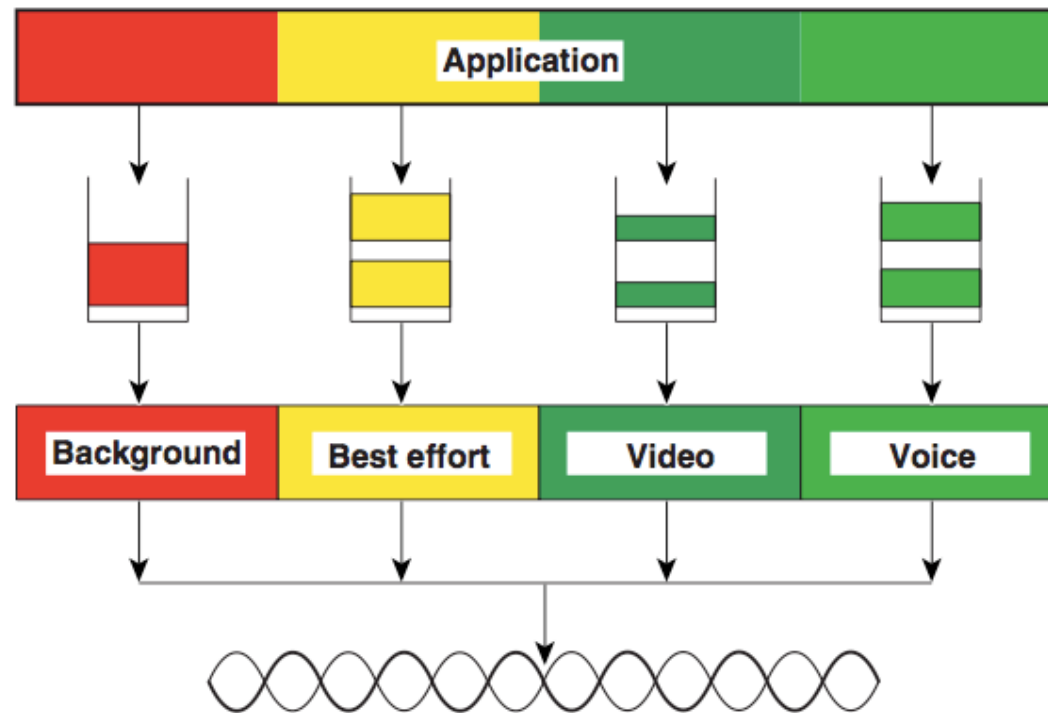
Best-effort

Video

Voice

From Application to Transmission

- Based on application tagging, frames are passed to the appropriate access categories, and then queued for transmission



QoS Frame Tagging

- Each category corresponds to an 802.1p/D classification and is tagged accordingly for upstream QoS preservation
- In the downstream, WMM/11e category and associated backoff interval is determined by frame/packet tagging

| Priority | 802.1 Priority (=User Priority) | 802.1p Designation | Access Category | WMM Designation |
|----------------|---------------------------------|-------------------------------------|-----------------|-----------------|
| Highest | 1 | BK Background | AC_BK | Background |
| | 2 | -Spare | | |
| Lowest | 0 | BE Best-effort | | |
| | 3 | EE Excellent Effort | AC_BE | Best-effort |
| | 4 | CL Control Load | | |
| | 5 | VI Video <100ms | AC_VI | Video |
| | 6 | VO Voice <10ms | AC_VO | Voice |
| | 7 | NC Network Control “must get there” | | |

11e and 802.1p/D to DSCP Tagging

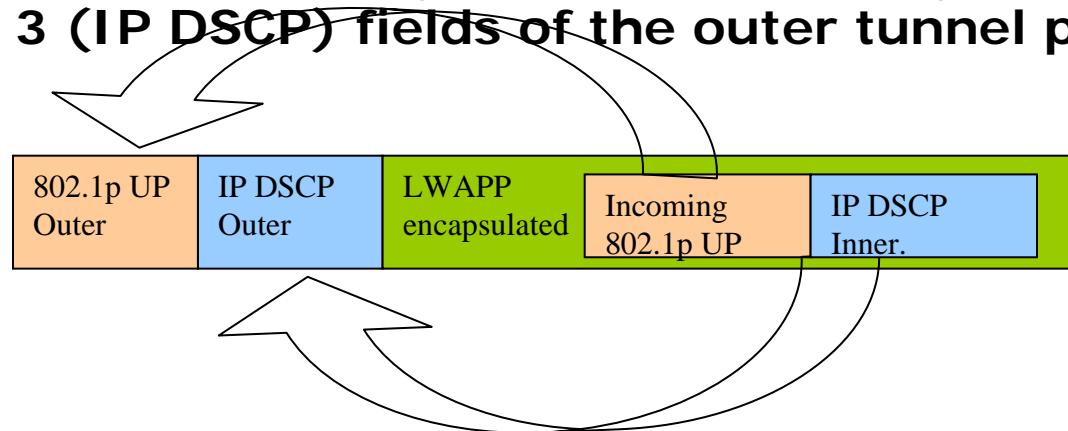
| 802.1p/D UP-based Traffic Type | DSCP UP | 11e UP |
|--|-----------|--------|
| Inter-network control (LWAPP, 802.11 mgmt) | 48 | 7 |
| Voice | 46 (EF) | 6 |
| Video | 34 (AF41) | 5 |
| Voice Control | 26 (AF31) | 4 |
| Background (Gold) | 18 (AF21) | 2 |
| Background (Gold) | 20 (AF22) | 2 |
| Background (Gold) | 22 (AF23) | 2 |
| Background (Silver) | 10 (AF11) | 1 |
| Background (Silver) | 12 (AF12) | 1 |
| Background (Silver) | 14 (AF13) | 1 |
| Best Effort | 0 (BE) | 0, 3 |
| Background | 2 | 1 |

End-to-End QoS Mapping 802.11e to Wired QoS

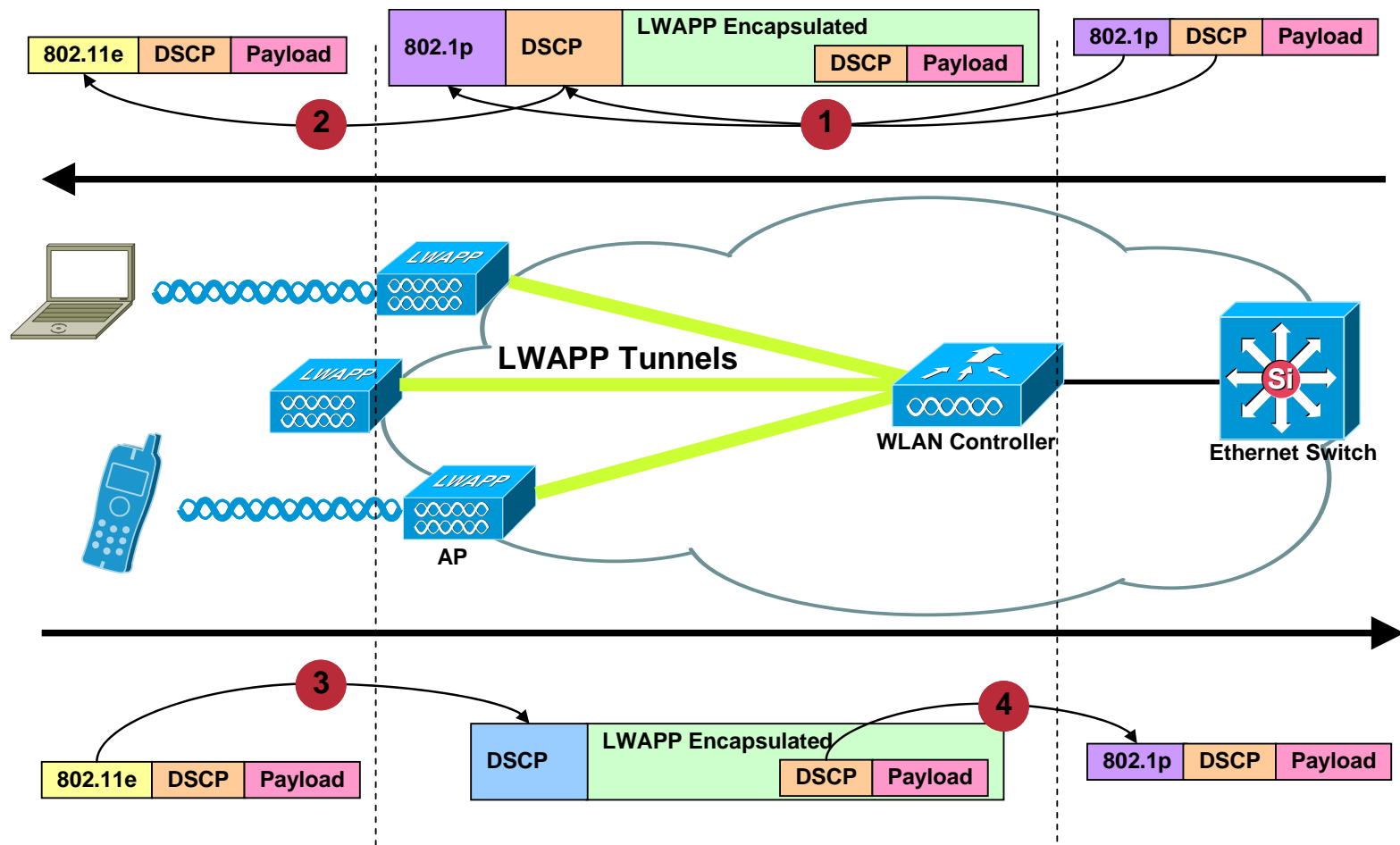


Problem Description

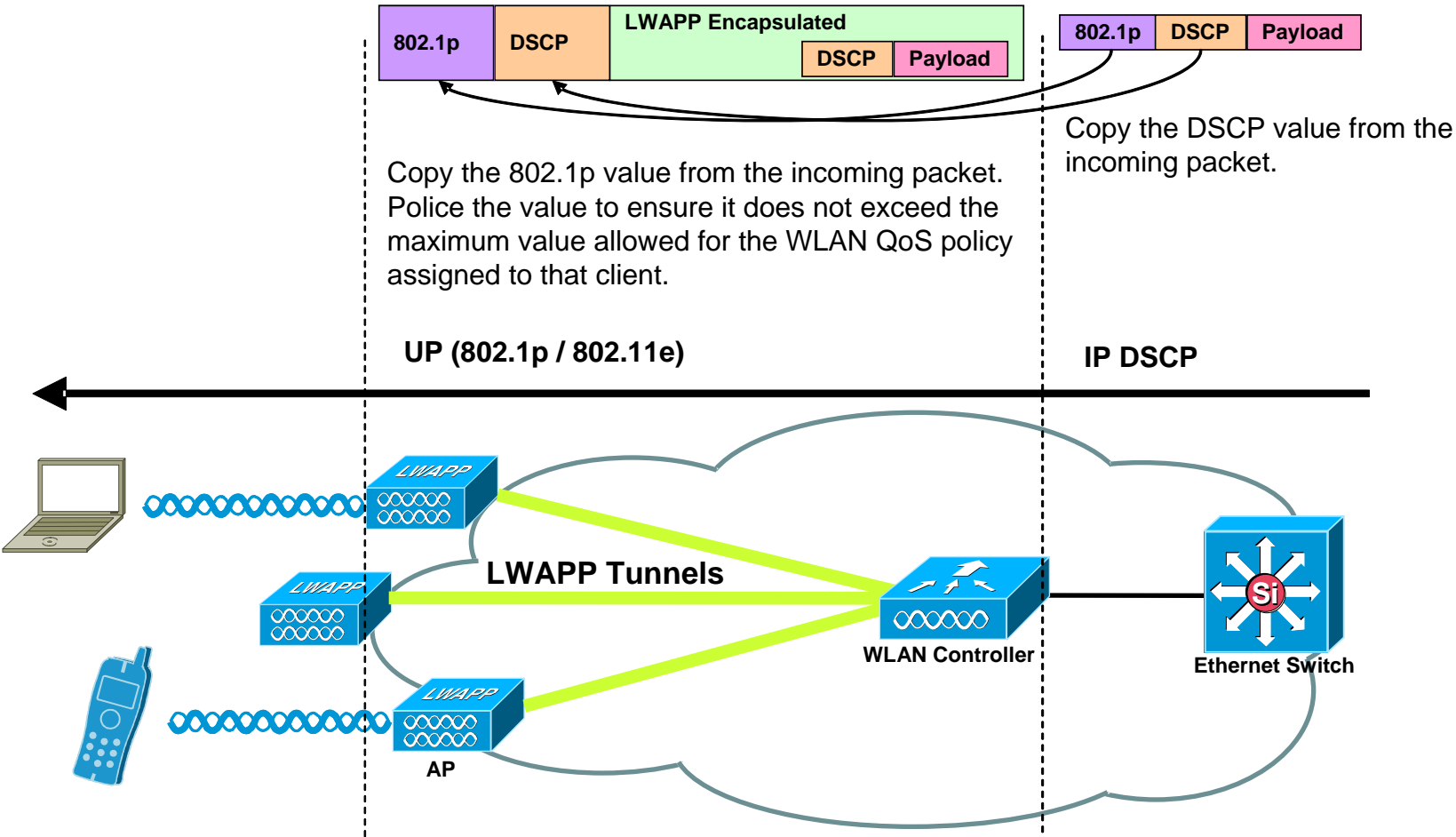
- Adds support for Layer 3 IP Differentiated Services Code Point (DSCP) marking of packets
- Enhances how Layer 3 information is used by APs to ensure packets receive correct over the air prioritization from the AP to the wireless client.
- WLAN data is tunneled between AP and WLAN controller via LWAPP
- To maintain the original QoS classification across this tunnel, the QoS settings of the encapsulated data packet must be appropriately mapped to the Layer 2 (802.1p) and Layer 3 (IP DSCP) fields of the outer tunnel packet.



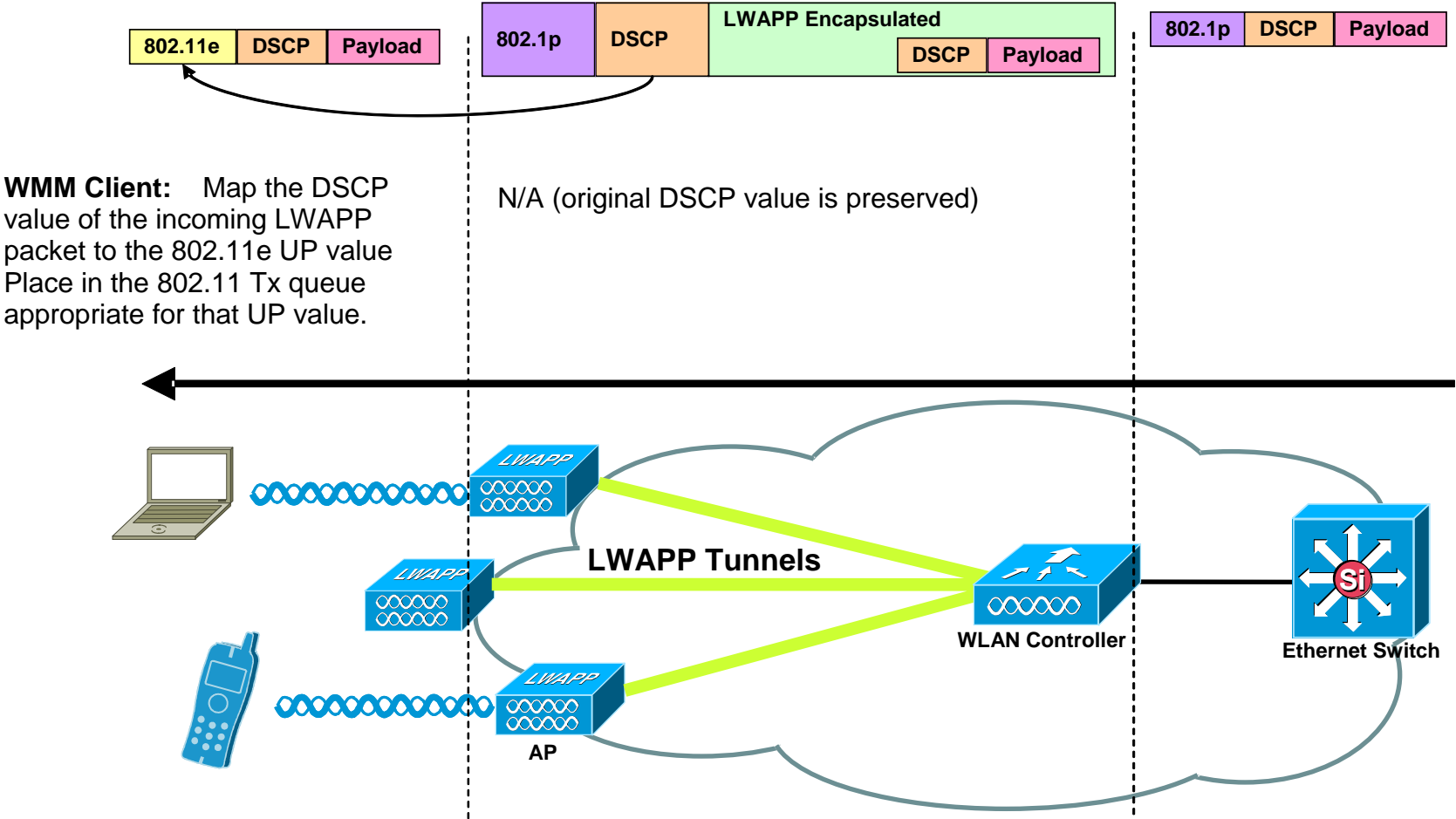
Feature: Description



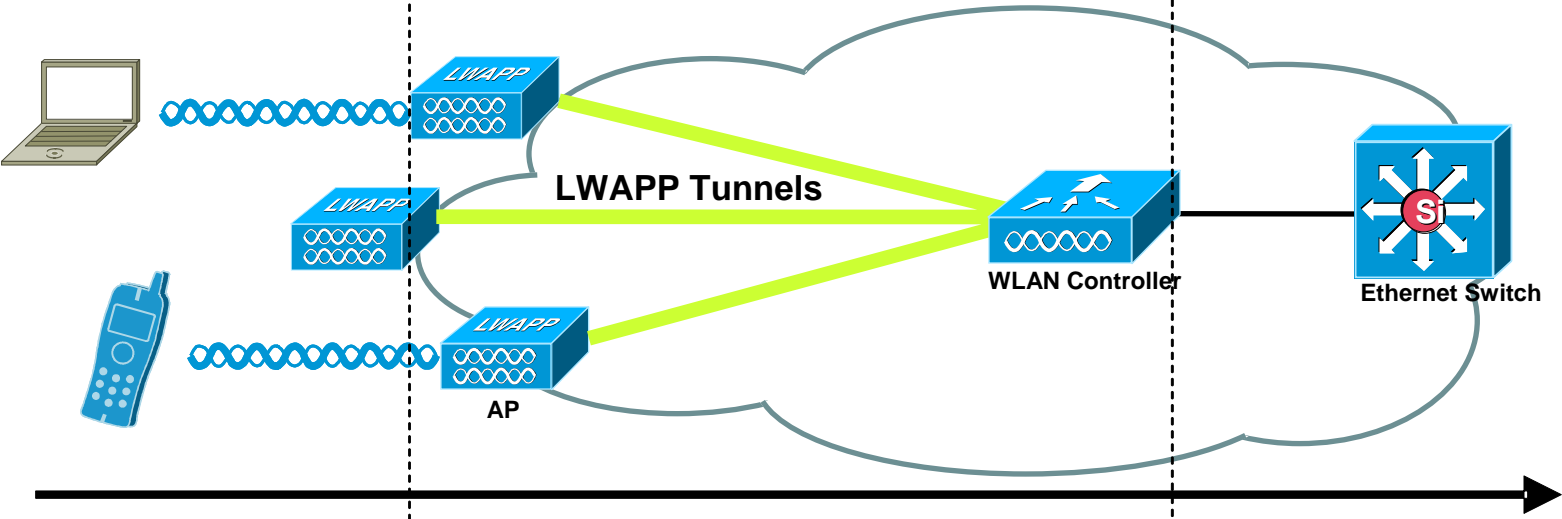
QoS From Controller to AP



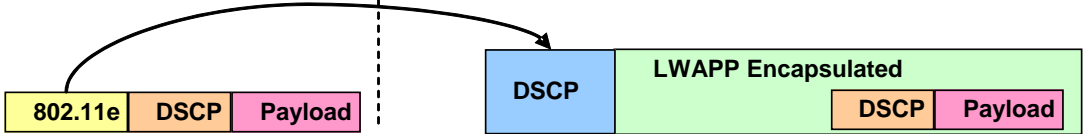
QoS From AP to Wireless MM Client



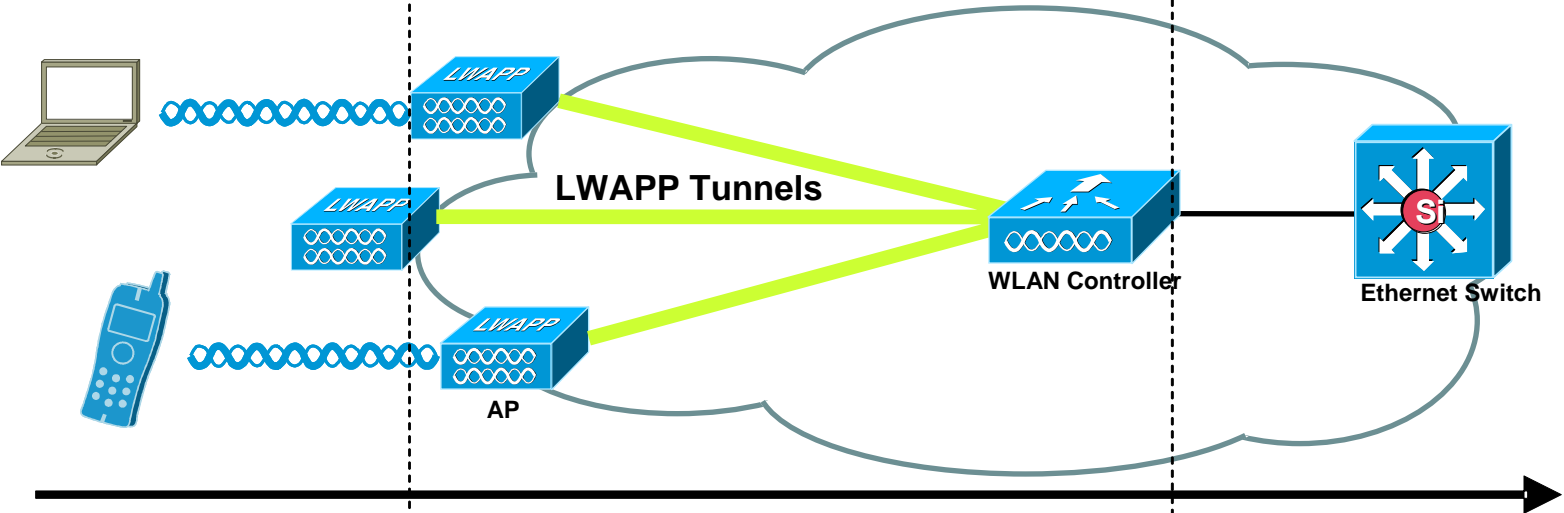
QoS From Wireless client to AP to Controller



WMM Client: Police the 802.11e UP value to ensure it does not exceed the maximum value allowed for the QoS policy assigned to that client; map the value to the DSCP value.

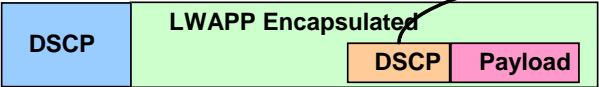


QoS From Controller to Ethernet switch

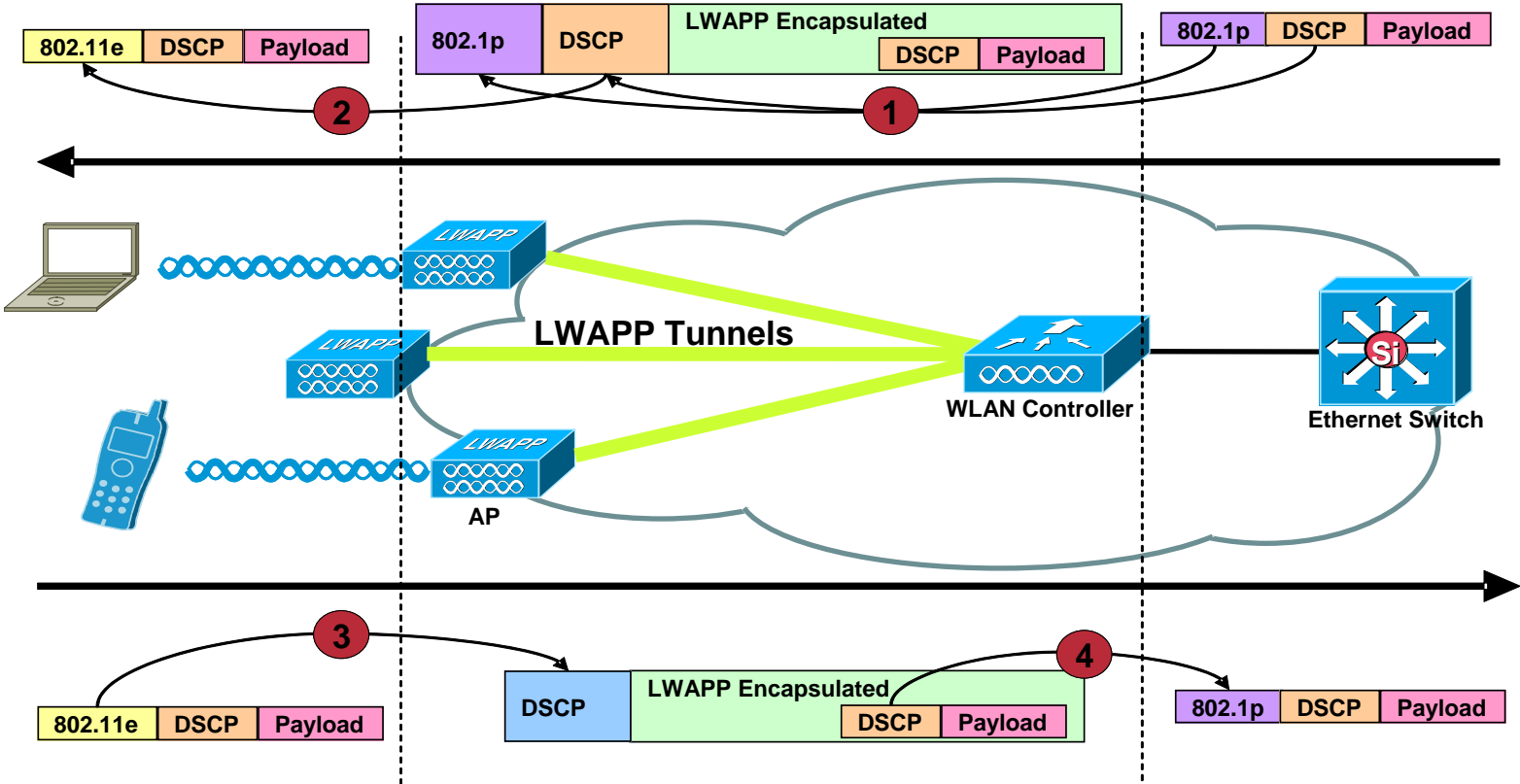


Map the DSCP value of the original packet to the 802.1p UP value.

N/A (original DSCP value is preserved)



WMM/11e, DSCP, Dot1p Relationship



Note: Over-the-air packets to the AP are policed allowing edge switches to trust the QoS marking of the packets from the AP

What about the Client??



Client-Side Trusted QoS

- **Whether using EDCA today or HCCA tomorrow, upstream QoS from the client isn't a possibility without the necessary client piece**
- **Not only does the client need to support WMM/11e QoS, but the client needs to know how to mark traffic to the appropriate access category**
- **Even with the necessary AC marking, this upstream marking needs to be trusted**

Without trusted QoS, DoS attacks may be sanctioned

Trusted Client-Side QoS Configuration

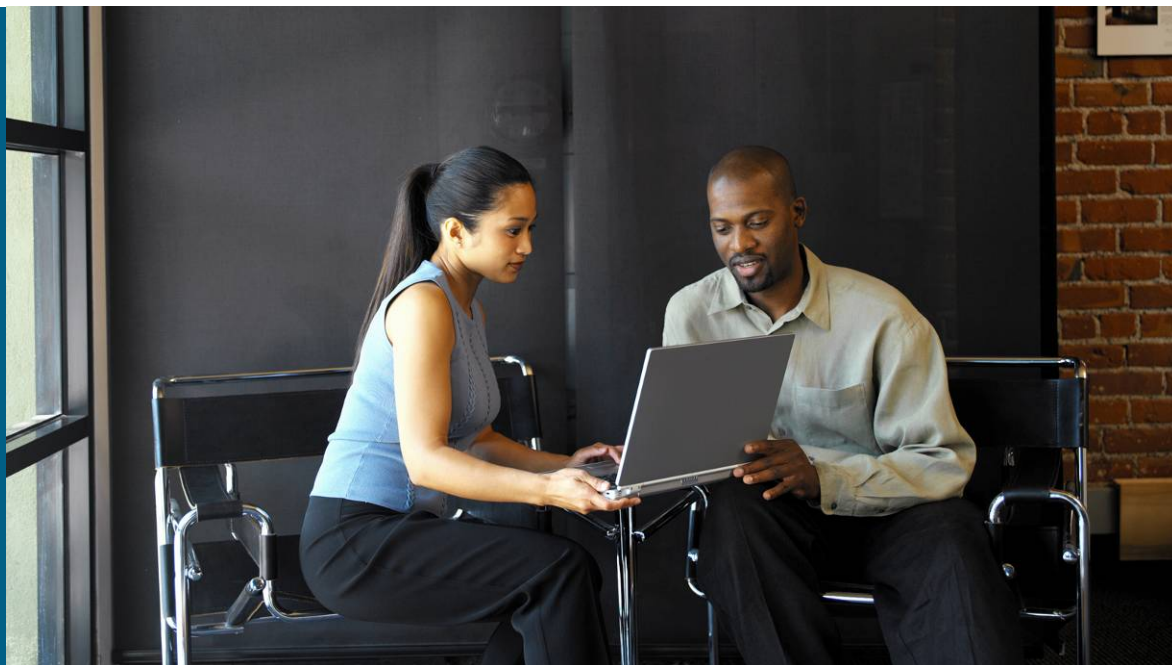
- **Cisco's Security Agent (CSA) allows centralized control of client-side QoS marking on a per-application basis**

The CSA Management Center (CSAMC) allows QoS rules to be securely passed to CSA client-side software

This not only allows applications' traffic to be properly applied to correct access categories, but it restricts users, and more likely, self-appraising applications, from overriding such classification

- **Such a client-side software piece isn't necessary for purpose-built devices such as Cisco's 7921**

Other QoS Topics



Call Capacity

- Ensure the network is designed to accommodate for desired capacity
- Can have up to 20 active RTP streams for both 802.11g and 802.11a @ 54mbps with minimal background traffic depending on initial channel utilization
- At 11mbps can have up to 10 active RTP streams with minimal background traffic



Admission Control

- **Admission control allows metered client access based on available resources at the AP**
- **Clients can intelligently select access points based on advertised load information**
- **Admission control is typically performed to optimize for voice, called call admission control (CAC)**

By indicating to a phone when too many AP resources are occupied, it may alternatively seek out a less-loaded access point

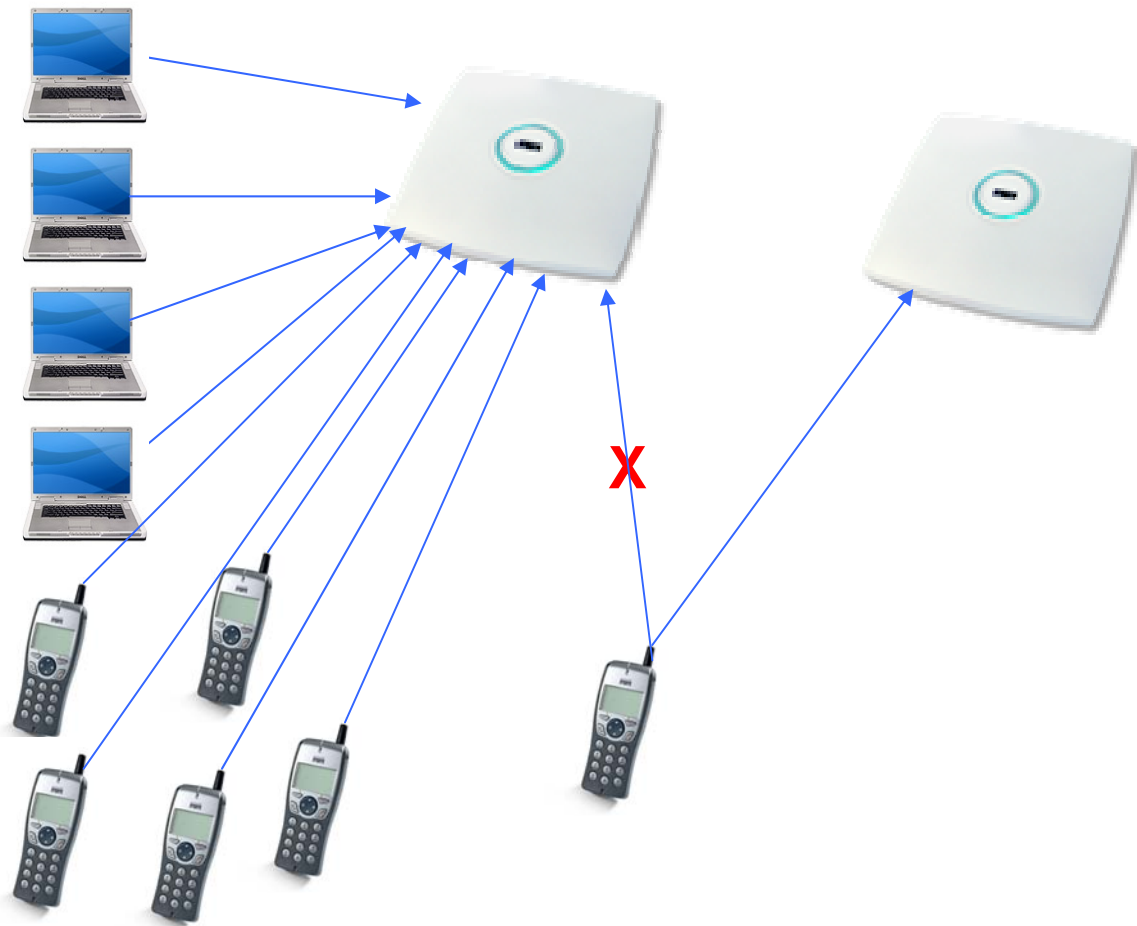
- **Admission control is performed in a couple of ways**

Approaches to Admission Control

- **Admission control grants clients access on a per-WLAN (SSID) basis**
- **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
- **WMM/11e's Traffic Specification (TSpec) takes much more into account**
 - Clients request admission based on: traffic priority (access category), power save, mean data rate, frame sizes, minimum PHY data rate, etcetera**

TSPEC-Based Call Admission Control (CAC)

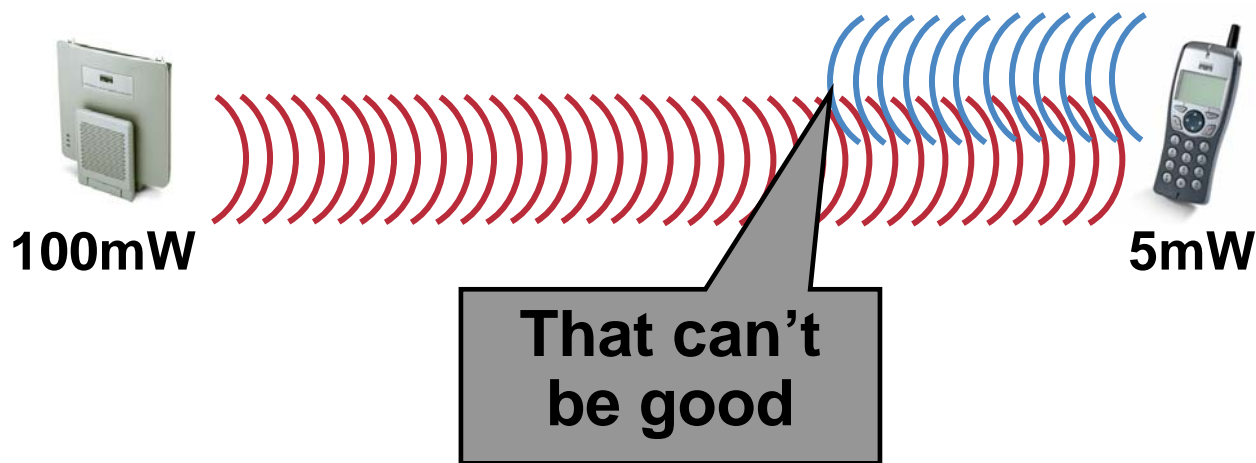
- Defined to the AP
- What percentage of traffic will be reserved for data and voice



Benefit: Ensures That the Number Of **Active Voice Calls Do Not Exceed The Configured Limits**

Dynamic Transmit Power Control (DTPC)

- Set the same transmit power on the AP and on the phones
- The Unified Controller advertises it's transmit power for the clients to learn
- Prevents one-way audio
i.e., RF traffic is only being heard in one direction



Roaming and Security



IEEE 802.11i (WLAN Security) Improvements

- 802.11i is the IEEE 802.11 subcommittee responsible for WLAN security improvements
- Key components of IEEE 802.11i standard are:
 - EAP/802.1x framework-based user authentication
 - TKIP: mitigate RC4 key scheduling vulnerability and active attack vulnerabilities (***not recommended unless client can't support AES***)
 - Key management: isolate encryption key management from user authentication
 - AES: Long-term replacement protocol for RC4 (WEP)
- WPAv2 is the Wi-Fi Alliance (WFA) inclusion of 802.11i security recommendations

Wi-Fi Protected Access



- What are WPA and WPA2?
 - Authentication and encryption standards for Wi-Fi clients and APs
 - 802.1x authentication
 - WPA uses TKIP encryption
 - WPA2 uses AES block cipher encryption
- Which should I use?
 - Gold, for supporting NIC/OSs
 - Silver, if you have legacy clients
 - Lead, if you absolutely have no other choice



Gold

WPA2/802.11i

- EAP Fast/TLS/PEAP
- AES



Silver

WPA

- EAP-Fast/TLS/PEAP
- TKIP



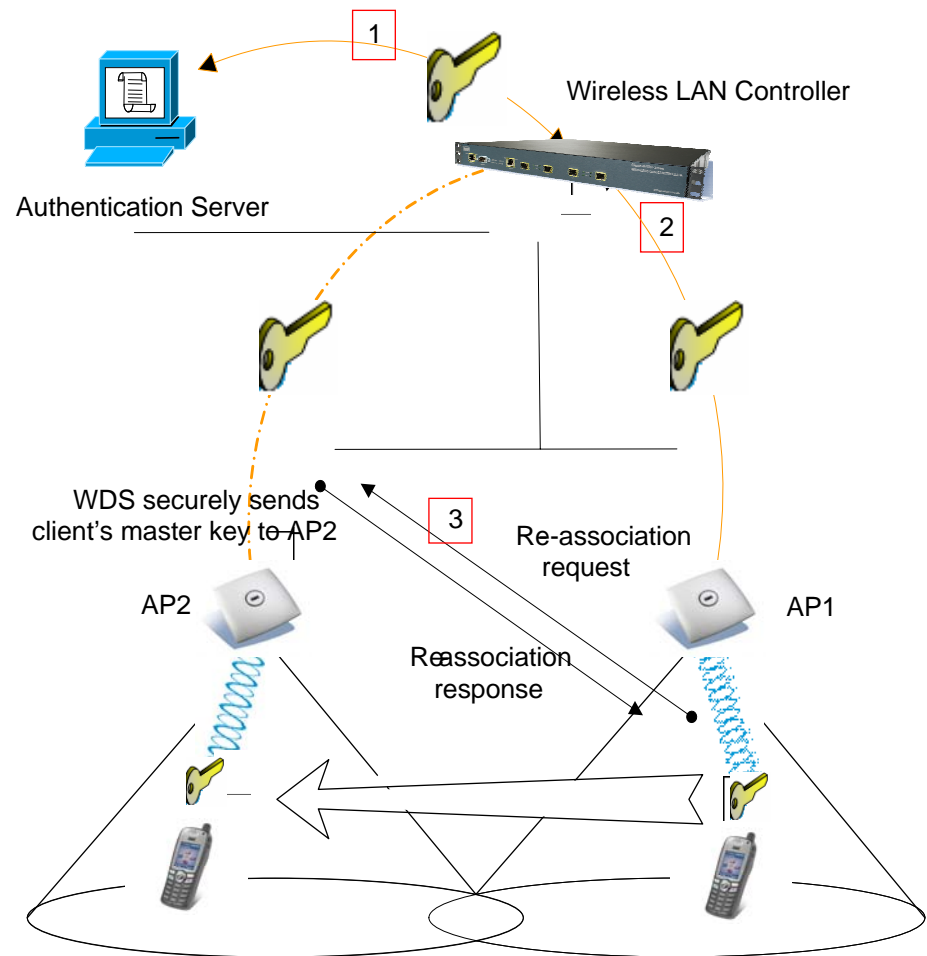
Lead

Dynamic WEP

- EAP-Fast/LEAP
- VLANs + ACLs

802.11i Fast Secure Roaming

- Client must Securely Roam in less than 150ms
- Wireless LAN Controller is the Authentication
- RADIUS Server delivers the client 802.11i Pairwise Master Key (PMK) to the WLC
- WLC delivers Session Key (Pairwise Transient Key) to AP1
- At re-association, AP2 receives new PTK from WLC
- Client authenticates with radius server only once.



- 1 Client authenticates with authentication server 2 Master key is cached on the WLC and PTK sent to the AP 3 Client roams to AP2 and new keys are generated

References and Further Reading

- **The IEEE 802.11 Handbook: A Designer's Companion by Bob O'Hara and Al Petrick (Second Edition)**
- **Cisco's Enterprise Mobility Design Guide (Version 3.0)**
<http://www.cisco.com/univercd/cc/td/doc/solution/embly30.pdf>
- **Cisco 7920 Phone Design and Deployment Guide**
http://www.cisco.com/en/US/products/ps6366/prod_technical_reference09186a00805e75a1.html
- **Wireless White papers**
http://www.cisco.com/en/US/products/ps6366/prod_white_papers_list.html

Q & A



