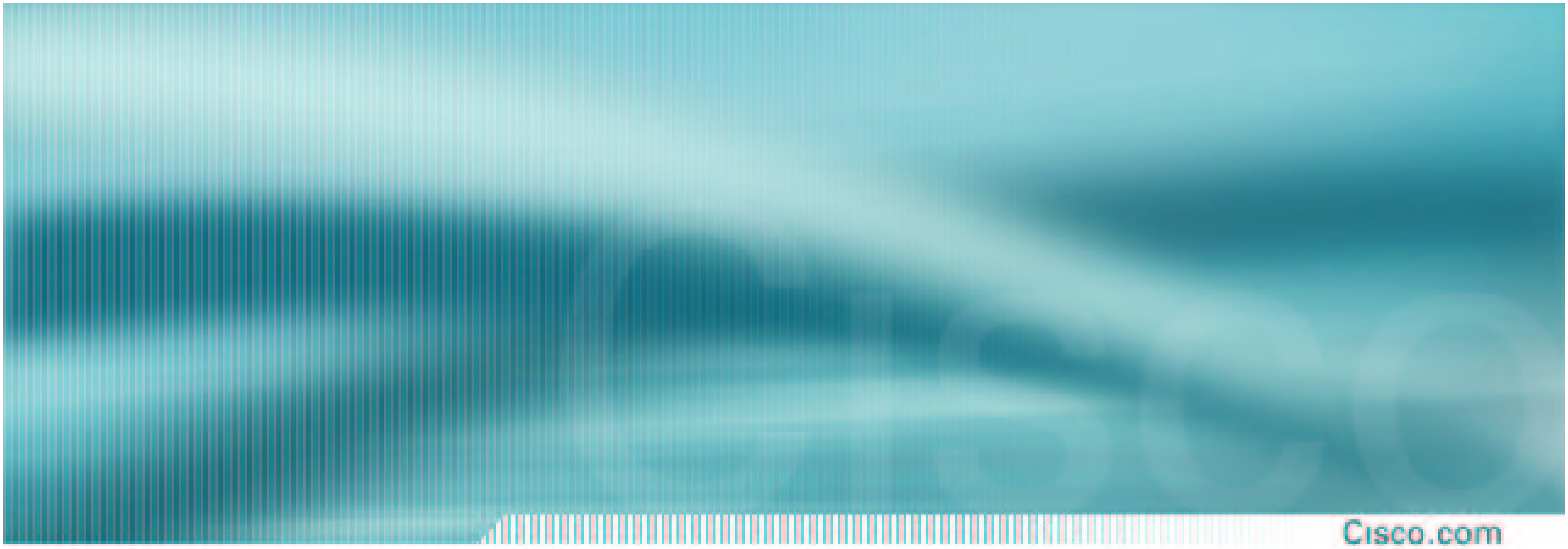


Wireless LAN Evolution

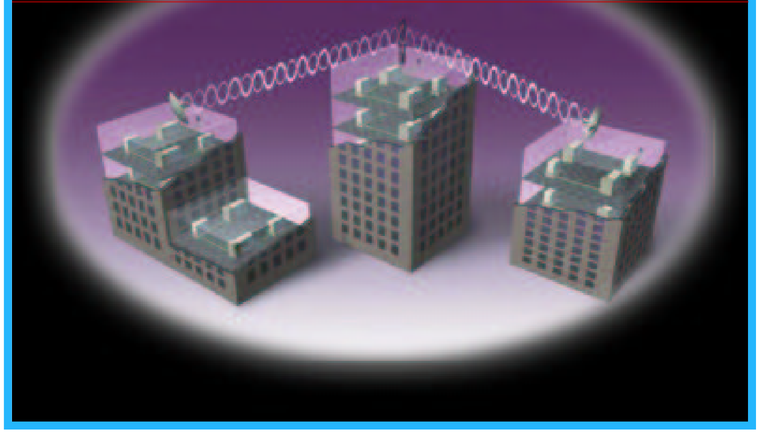
Frank Bartel

Internetworking Consultant

fbartel@cisco.com

Extended Connectivity with Wireless LAN

Point-to-Point/Multipoint Wireless



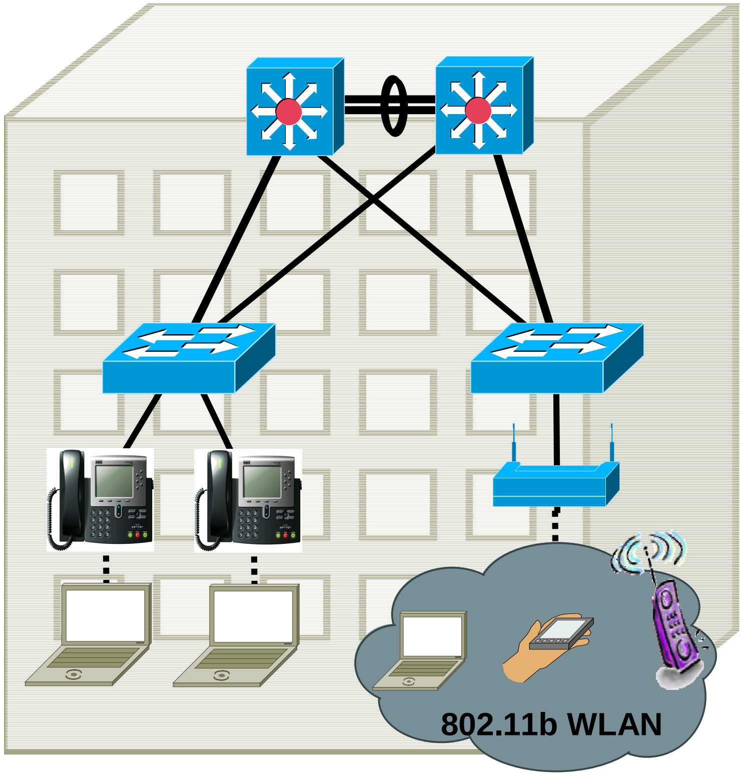
Building Wireless LAN

Public Access Hot Spot

At Home

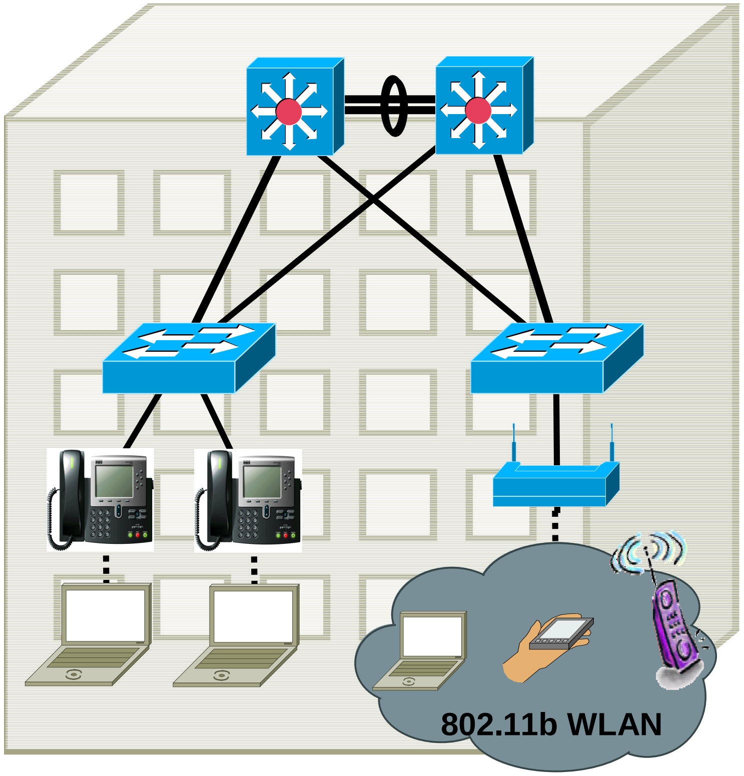
Campus WLAN Design

- .11b vs .11a
- Security
- VLANs
- QoS
- L2/L3 Roaming
- Voice
- Product Line

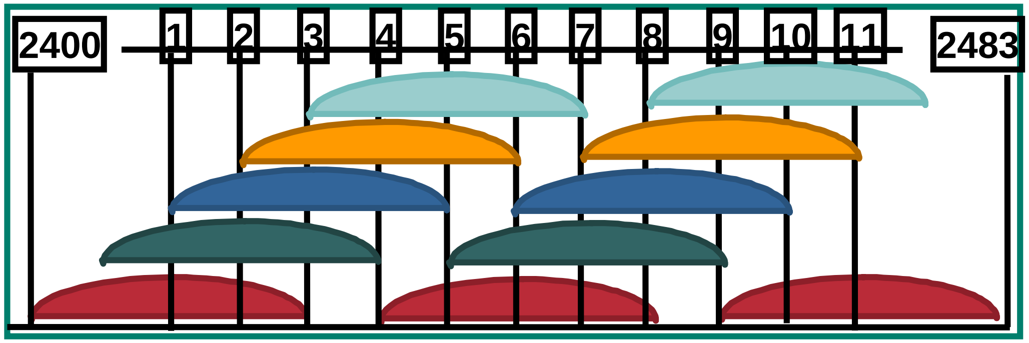


Campus WLAN Design

- .11b vs .11a
- Security
- VLANs
- QoS
- L2/L3 Roaming
- Voice
- Product Line



802.11b 11Mb 2.4GHz Direct Sequence



- Ratified as standard in Sept. 1999
- 11Mb 2.4GHz
- 11 US channels
- 13 ETSI channels
- 14 Japan channels
- Power levels of 36dBm EIRP-FCC 20dBm EIRP-ETSI
- Virtually approved for worldwide use

Characteristics of 802.11a

- Orthogonal Frequency Division Multiplexing (OFDM)

  Data rates supported: 54, 48, 36, 24, 12 and 6Mbps

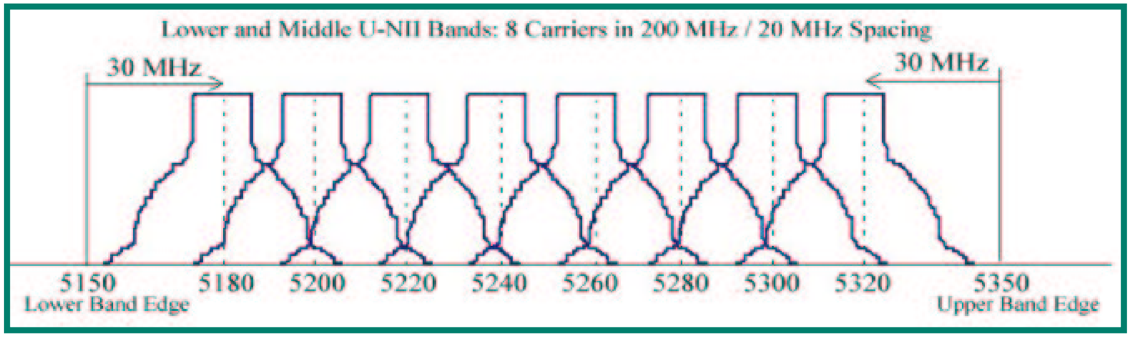
  Can “downshift” to lower data rates for longer range

- Compliant with FCC and Japanese regulations

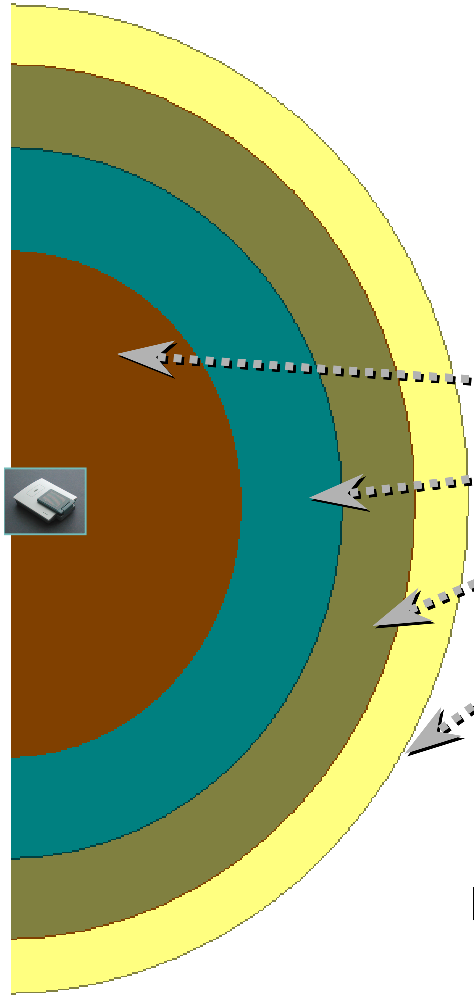
  Initial offering will not be available in EMEA and portions of Asia/Pacific

- 5GHz band has more channels than 2.4GHz band

  UNII-1 + UNII-2 = 8 non-overlapping channels
  (vs. 3 channels for 2.4GHz)



Range Comparisons



2.4Ghz/100mW

11 Mbps 140 Feet

5.5 Mbps 180 Feet

2 Mbps 250 Feet

1 Mbps 350 Feet

5Ghz/40mW

54 Mbps @40-60 Feet Radius

48 Mbps @ 70-90 Feet

36 Mbps @ 90-110 Feet

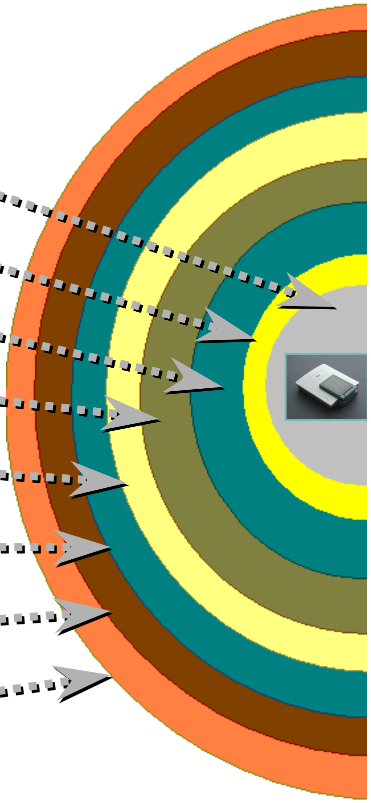
24 Mbps @ 110-125 Feet

18 Mbps @ 125-135 Feet

12 Mbps @ 135-145 Feet

9 Mbps @145–155 Feet

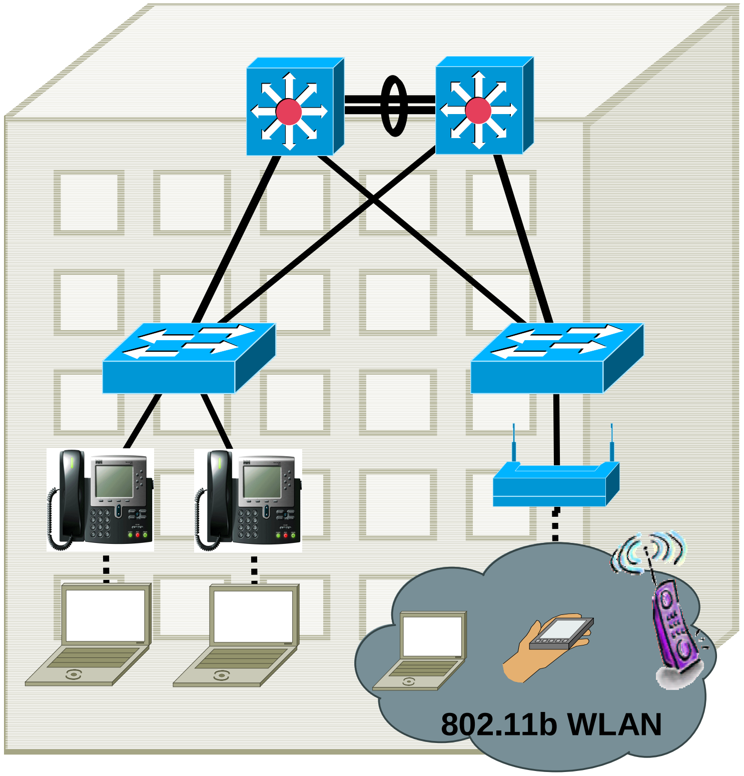
6 Mbps @ 155–165 Feet



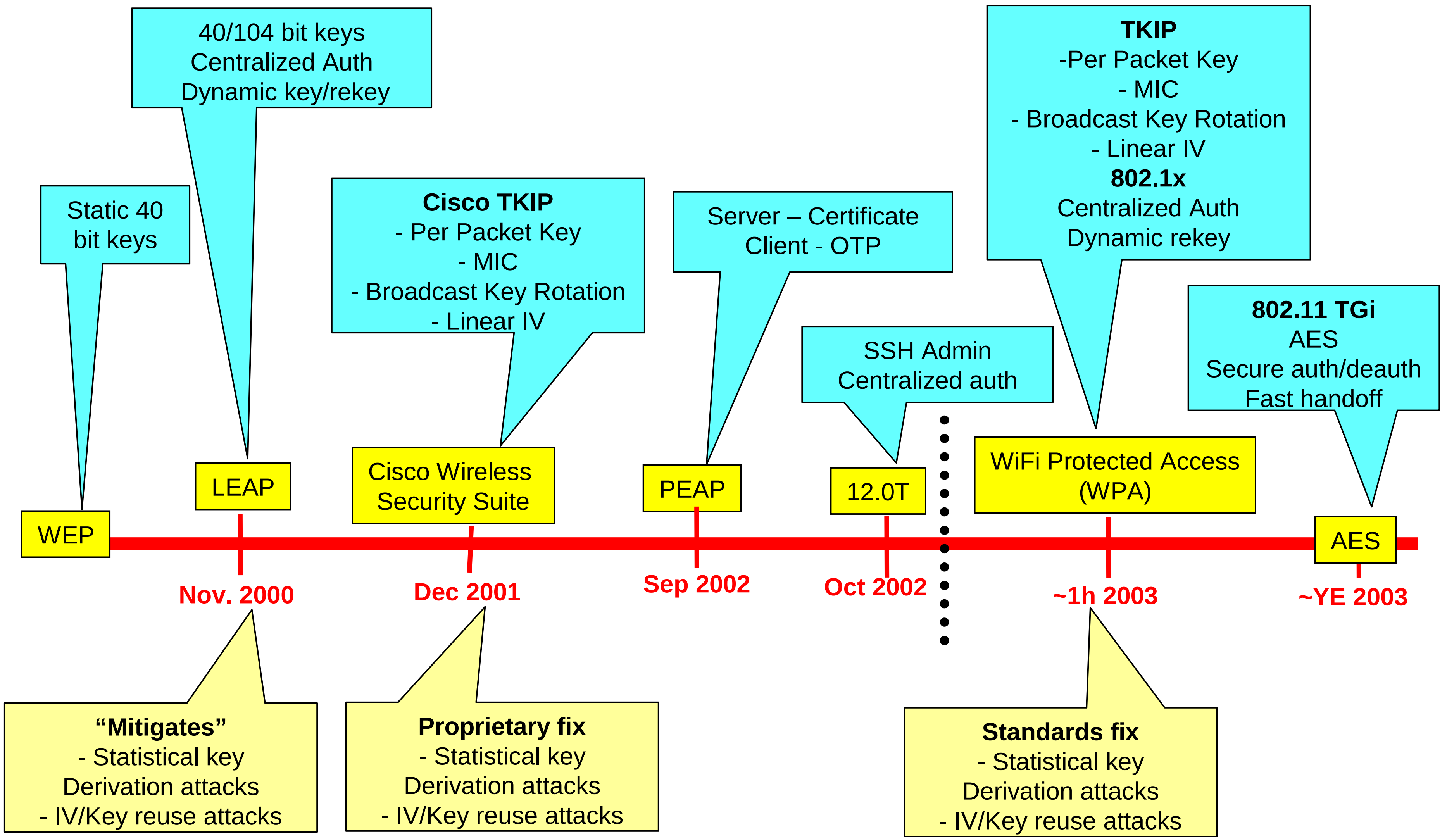
Ranges using 2.2dBi dipole antenna on AP, and Standard PC Card style radio

Campus WLAN Design

- .11b vs .11a
- Security
- VLANs
- QoS
- L2/L3 Roaming
- Voice
- Product Line



Cisco WLAN Security suite



WEP

Static 40 bit keys

LEAP

Nov. 2000

40/104 bit keys
Centralized Auth
Dynamic key/rekey

“Mitigates”
- Statistical key
Derivation attacks
- IV/Key reuse attacks

Cisco Wireless Security Suite

Dec 2001

Cisco TKIP
- Per Packet Key
- MIC
- Broadcast Key Rotation
- Linear IV

Proprietary fix
- Statistical key
Derivation attacks
- IV/Key reuse attacks

PEAP

Sep 2002

Server – Certificate
Client - OTP

12.0T

Oct 2002

SSH Admin
Centralized auth

WiFi Protected Access (WPA)

~1h 2003

TKIP
-Per Packet Key
- MIC
- Broadcast Key Rotation
- Linear IV
802.1x
Centralized Auth
Dynamic rekey

Standards fix
- Statistical key
Derivation attacks
- IV/Key reuse attacks

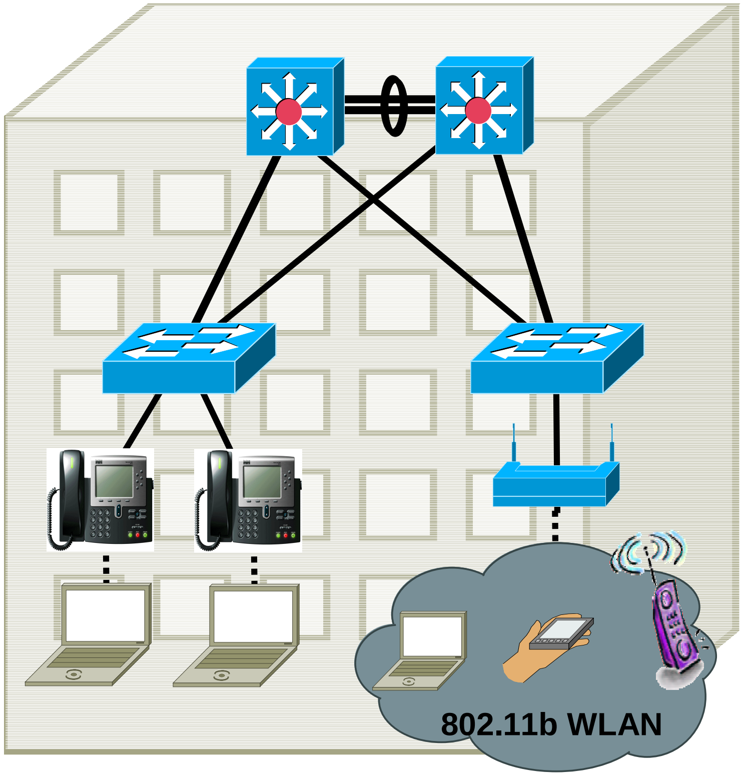
AES

~YE 2003

802.11 TGi
AES
Secure auth/deauth
Fast handoff

Campus WLAN Design

- .11b vs .11a
- Security
  - Identity based networking
- VLANs
- QoS
- L2/L3 Roaming
- Voice
- Product Line



History Repeats Itself

What happens when there is a technology that is relatively *simple* to deploy, can *dramatically improve* the way we work, but is not made *readily available* to employees?

Employees will "deploy their own" and Network *stability* and *security* can be compromised

15 Years Ago it was Desktop modems

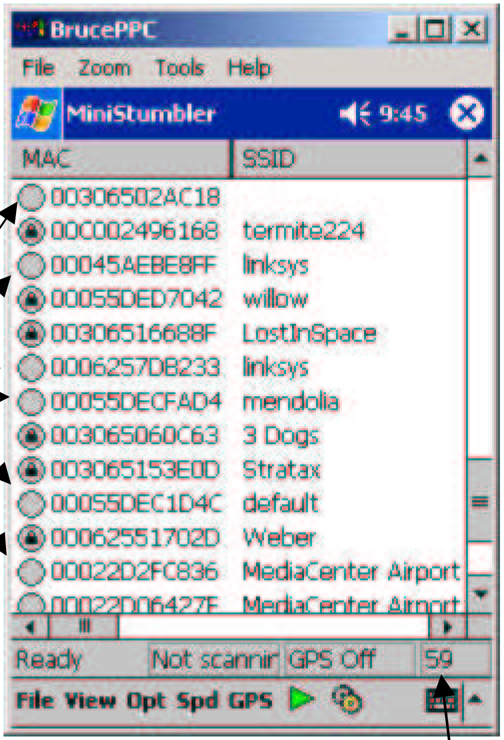
Today it is Wireless LAN

Please Mr. IT Guy, don't take my wireless
Hmm, or maybe I can just deploy my own

**Result:
Rogue AP's**

Prevalence of Rogue AP’s

Example: 59 APs in 7 miles in SJ Commute



	MAC	SSID
○	00306502AC18	
●	00C002496168	termite224
○	00045AEBE8FF	linksys
●	00055DED7042	willow
●	00306516688F	LostInSpace
○	0006257DB233	linksys
○	00055DECFAD4	mendolia
●	003065060C63	3 Dogs
●	003065153E0D	Stratax
○	00055DEC1D4C	default
●	00062551702D	Weber
○	00022D2FC836	MediaCenter Airport
○	00022D06427F	MediaCenter Airport

Insecure APs

59 APs found

- A daily drive to work taken within the car at normal speeds with an IPAQ running a freeware application (Mix of Residences and Enterprises)
- Insecure Enterprise Rogue AP’s are a result of:

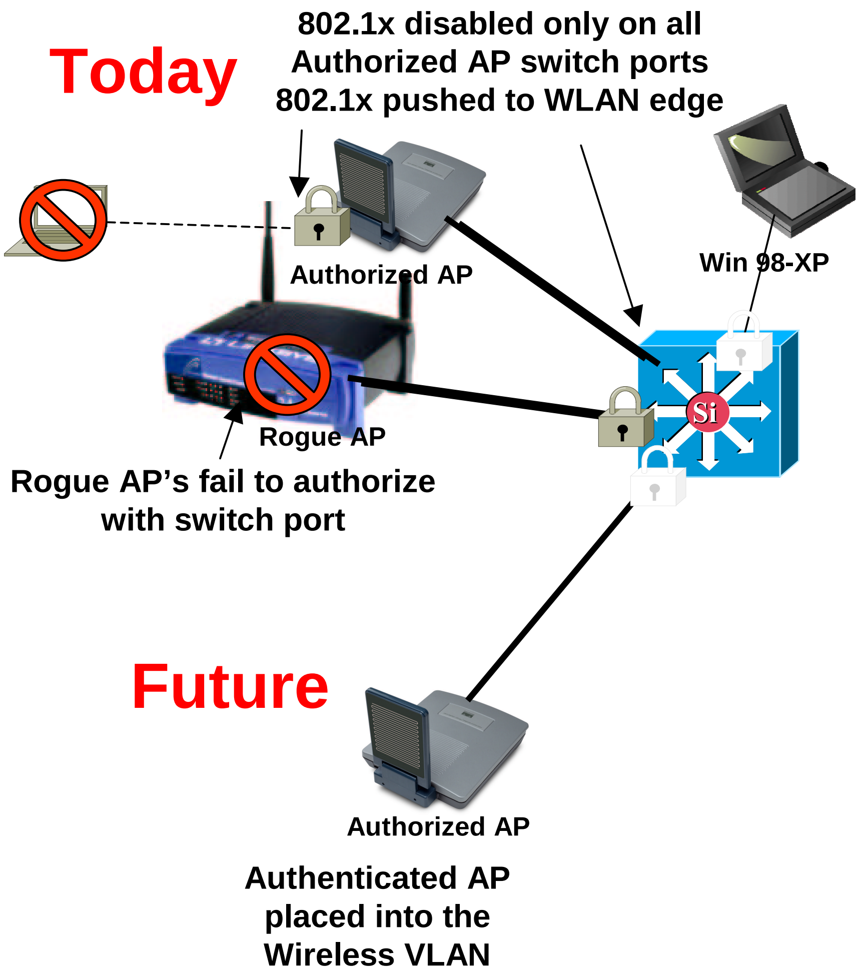
  Well intentioned self-install due to absence of sanctioned WLAN deployment

  An infrastructure that is not “Wireless Ready” to protect against Rogue APS

Campus Mobility – Rogue AP Detection/Denial

What can be done now/soon/future?

- You probably already have a WLAN deployment in your corporate network (whether you know it or not)
- An IT deployed and supported WLAN is the best way to prevent insiders from installing their own APs
- Use a combination of scripts and wireless analyzers to regularly audit for rogue APs


Today
802.1x disabled only on all Authorized AP switch ports
802.1x pushed to WLAN edge
Authorized AP
Win 98-XP
Si
Rogue AP
Rogue AP's fail to authorize with switch port
Future
Authorized AP
Authenticated AP placed into the Wireless VLAN

Why worry about 802.1x on switch ports?

802.1x on switch ports can;

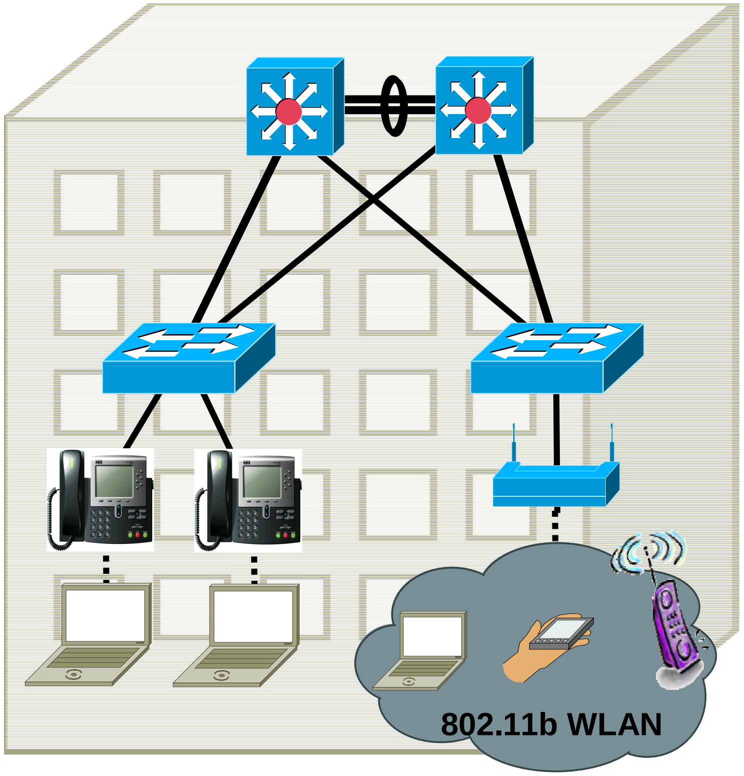
- Prevent rogue APs from connecting
- Prevent any unauthorized device from connecting
- Allow user-based policy to be dynamically applied to switched ports

Campus WLAN Design

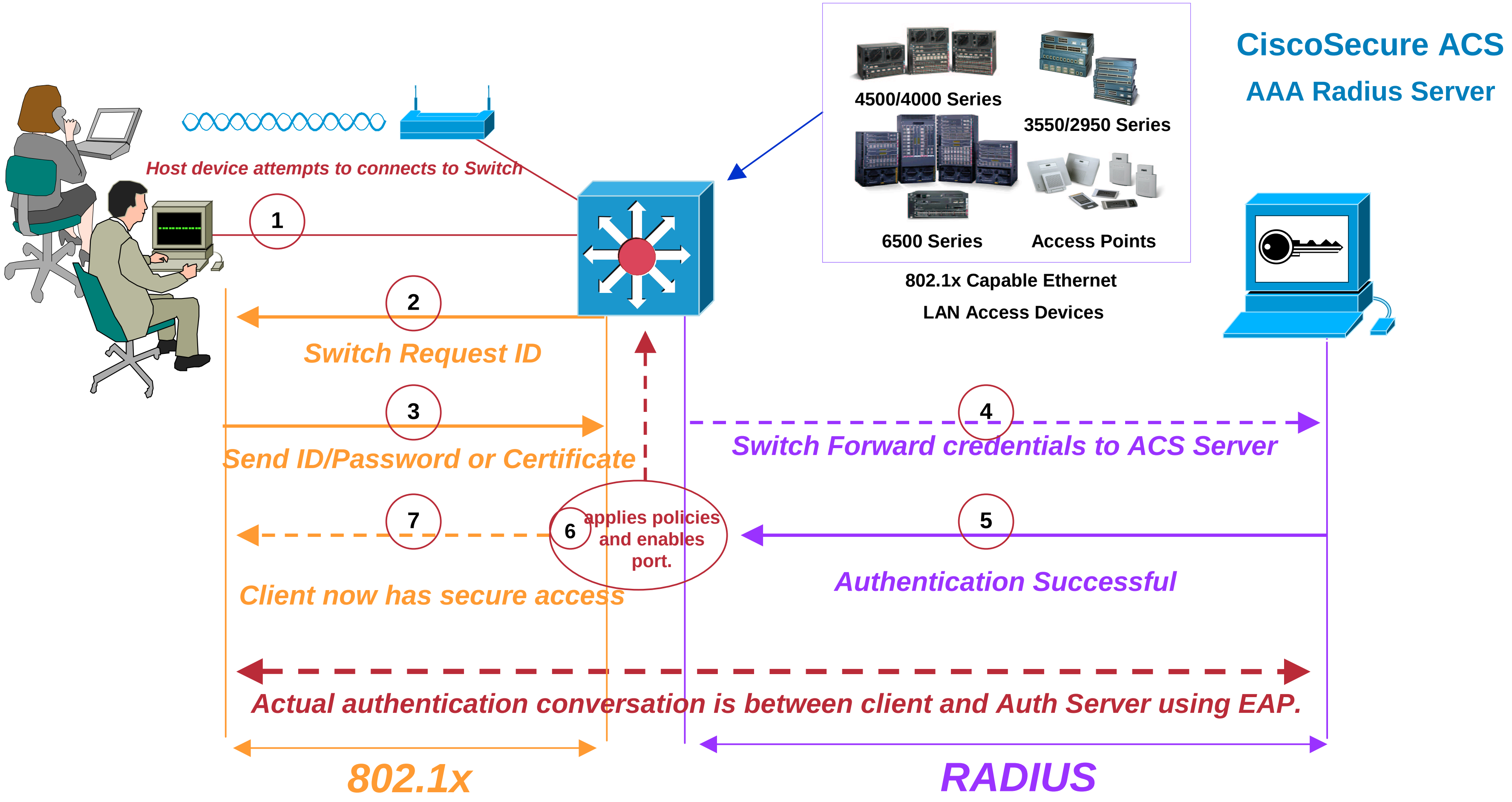
- .11b vs .11a
- Security

  Identity based networking

  - 802.1x wired/wireless
- VLANs
- QoS
- L2/L3 Roaming
- Voice
- Product Line



How Does Basic Port Based Network Access Work?



CiscoSecure ACS

AAA Radius Server

4500/4000 Series

3550/2950 Series

6500 Series

Access Points

802.1x Capable Ethernet

LAN Access Devices

Host device attempts to connects to Switch

1

2 Switch Request ID

3 Send ID/Password or Certificate

4 Switch Forward credentials to ACS Server

5 Authentication Successful

6 applies policies and enables port.

7 Client now has secure access

Actual authentication conversation is between client and Auth Server using EAP.

802.1x

RADIUS

The switch detects the 802.1x compatible client, forces authentication, then acts as a middleman during the authentication, Upon successful authentication the switch sets the port to forwarding, and applies the designated policies.

802.1x Configuration Options

Client OS	•WinXP (SP1)	•Apple OS X
	•Win2K (SP3)	•RedHat Linux
	•Win 98	•HP/UX
	•Win ME	•Sun Solaris
Supplicant	•OS Integrated	•ACU
	•MeetingHouse	
	•Open1x	
RADIUS Server	•MS Win2K IAS	•FreeRADIUS
	•CiscoSecure ACS	•SteelBelted RADIUS
	•MS .NET Server IAS	•MeetingHouse Aegis
Authentication Method	•EAP-TLS	•Cisco PEAP w/MSCHAPv2
	•EAP-MD5	•Cisco PEAP w/EAP-GTC
	•MS PEAP w/MSCHAPv2	•MS PEAP w/EAP-GTC
	•MS PEAP w/EAP-TLS	
PKI CA	•MS Win2K Certificate Server	•Verisign
	•OpenCA	
	•Entrust	
Authenticator	•Catalyst 6500	•Catalyst 3550
	•Catalyst 4500	•Aironet 350
	•Catalyst 2950	•Aironet 1100/1200

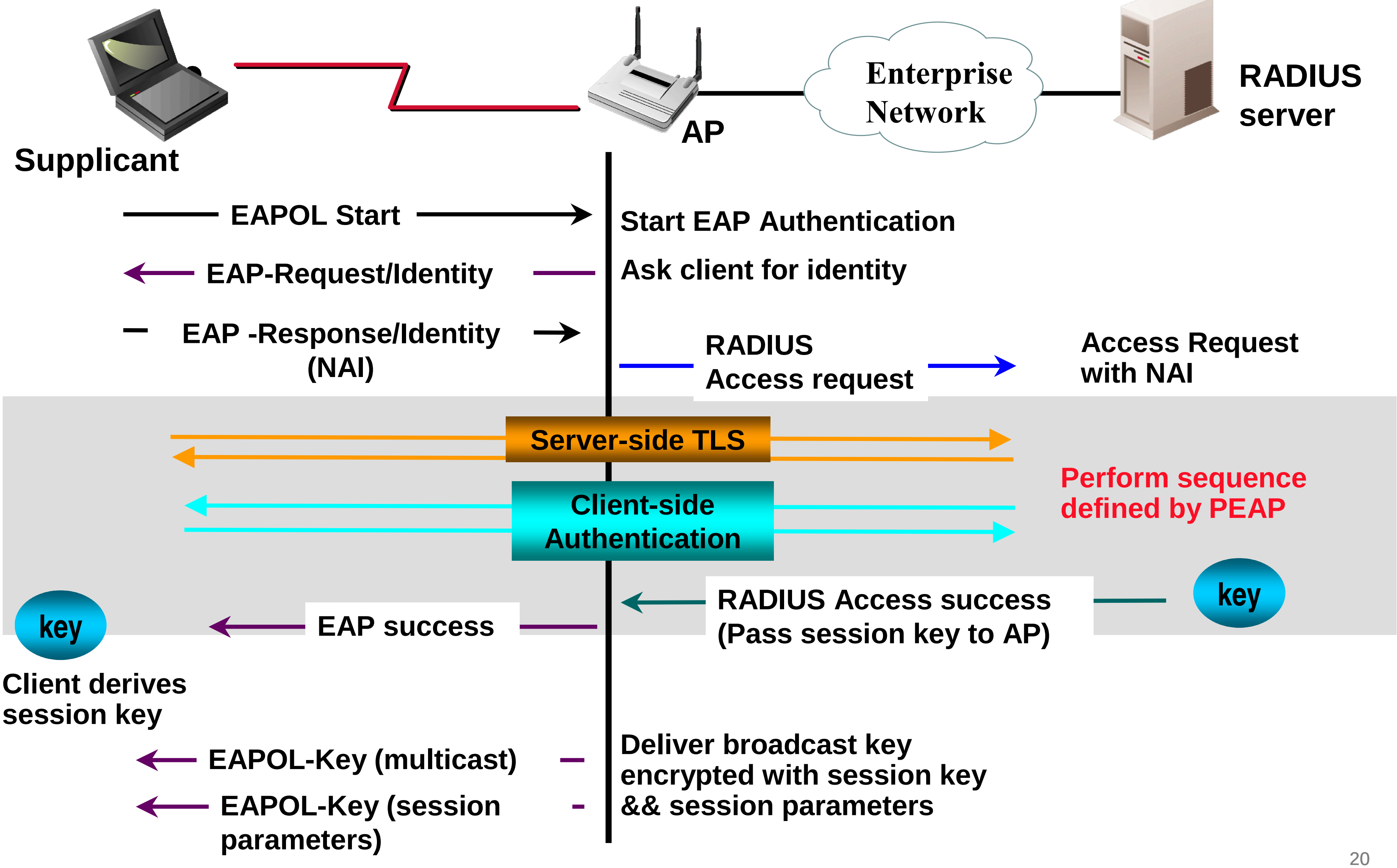
Operating System 802.1x Support?

- **Microsoft Windows XP Professional Microsoft Windows 2000 & 2000 Server, NT4.0, ME, 98 & 98SE (Microsoft add-on)**
  http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/8021xclient.asp
  http://support.microsoft.com/default.aspx?scid=kb;en-us;313664
- **Linux (Open Source add-on)**
  http://www.open1.com/
- **Sun Solaris (Open Source add-on)**
  http://www.open1.com/
- **Cisco LEAP/PEAP client (wireless only)**
- **Funk client (wireless only?)**
  http://www.funk.com/
- **MeetingHouse Client**
  http://www.mtghouse.com/

Some 802.1x supplicants for wired and wireless

Wireless	Wired
EAP-Cisco **(LEAP)**	—
PEAP **(Cisco or MS supplicant)**	**PEAP** **(MS supplicant)**
EAP-TLS **(MS supplicant)**	**EAP-TLS** **(MS supplicant)**
—	**EAP-MD5** **(MS supplicant**

A Closer Look at PEAP Auth



Supplicant

AP

Enterprise Network

RADIUS server

EAPOL Start

Start EAP Authentication

EAP-Request/Identity

Ask client for identity

EAP -Response/Identity (NAI)

RADIUS Access request

Access Request with NAI

Server-side TLS

Client-side Authentication

Perform sequence defined by PEAP

RADIUS Access success (Pass session key to AP)

key

EAP success

key

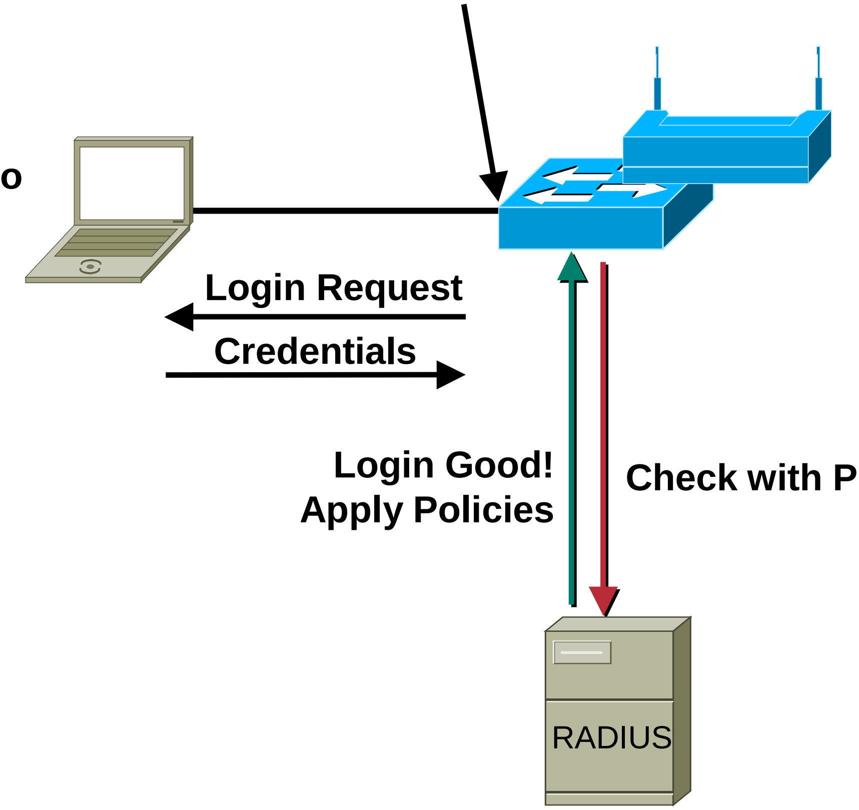
Client derives session key

EAPOL-Key (multicast)

EAPOL-Key (session parameters)

Deliver broadcast key encrypted with session key && session parameters

Example Solution — Access Control and User Policy Enforcement



Switch Applies Policies and Enables Port

- Set port VLAN to 5

User Has Access to Network, with Applicable VLAN

Login Request

Credentials

Login Good! Apply Policies

Check with Policy DB

This Is John Doe! He Goes into VLAN 5

Deployment Recommendations

- If deploying or testing 802.1x in the next 3-4 months:

  Wired Authentication

  For authentication using Username/Password credentials use WinXP or Win2K clients with PEAP/MS-CHAPv2 against MS Win2K Server IAS. Provides single login for Windows & 802.1x. -> ACS 3.2

  For stronger security use WinXP or Win2K clients with EAP-TLS against ACS 3.1.1 if group policies are not needed, and Win2K Server IAS if group policies are needed. SmartCards are an additional option with EAP-TLS. -> ACS 3.2

  Wireless Authentication

  For wireless authentication using ACU, use LEAP or Cisco PEAP against ACS 3.1.1.

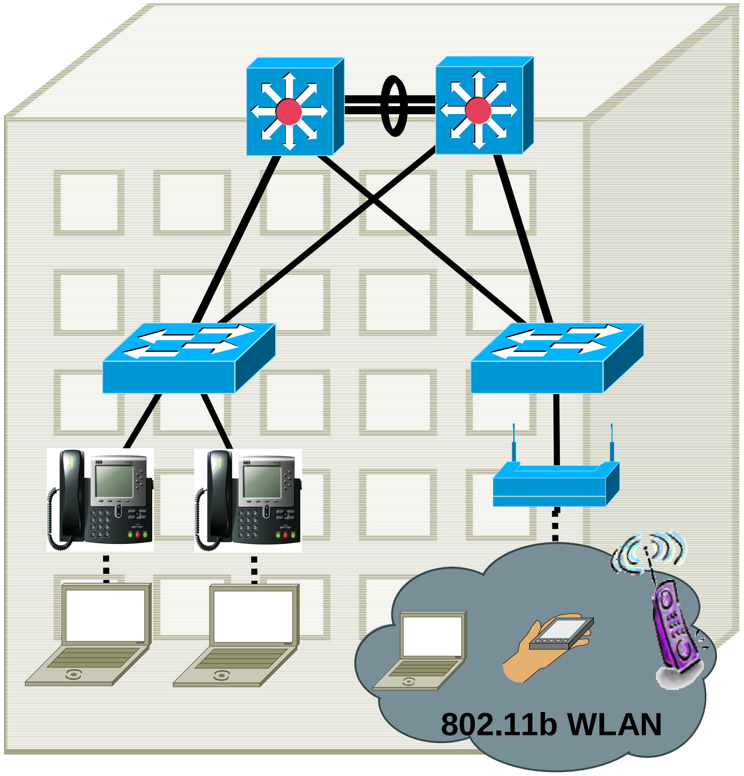
  For Wireless authentication using Windows wireless client use EAP-TLS against ACS 3.1.1.

- If deploying or testing 802.1x 4+ months out:

  Use ACS for all AAA functionality once PEAP/MS-CHAPv2 is available.

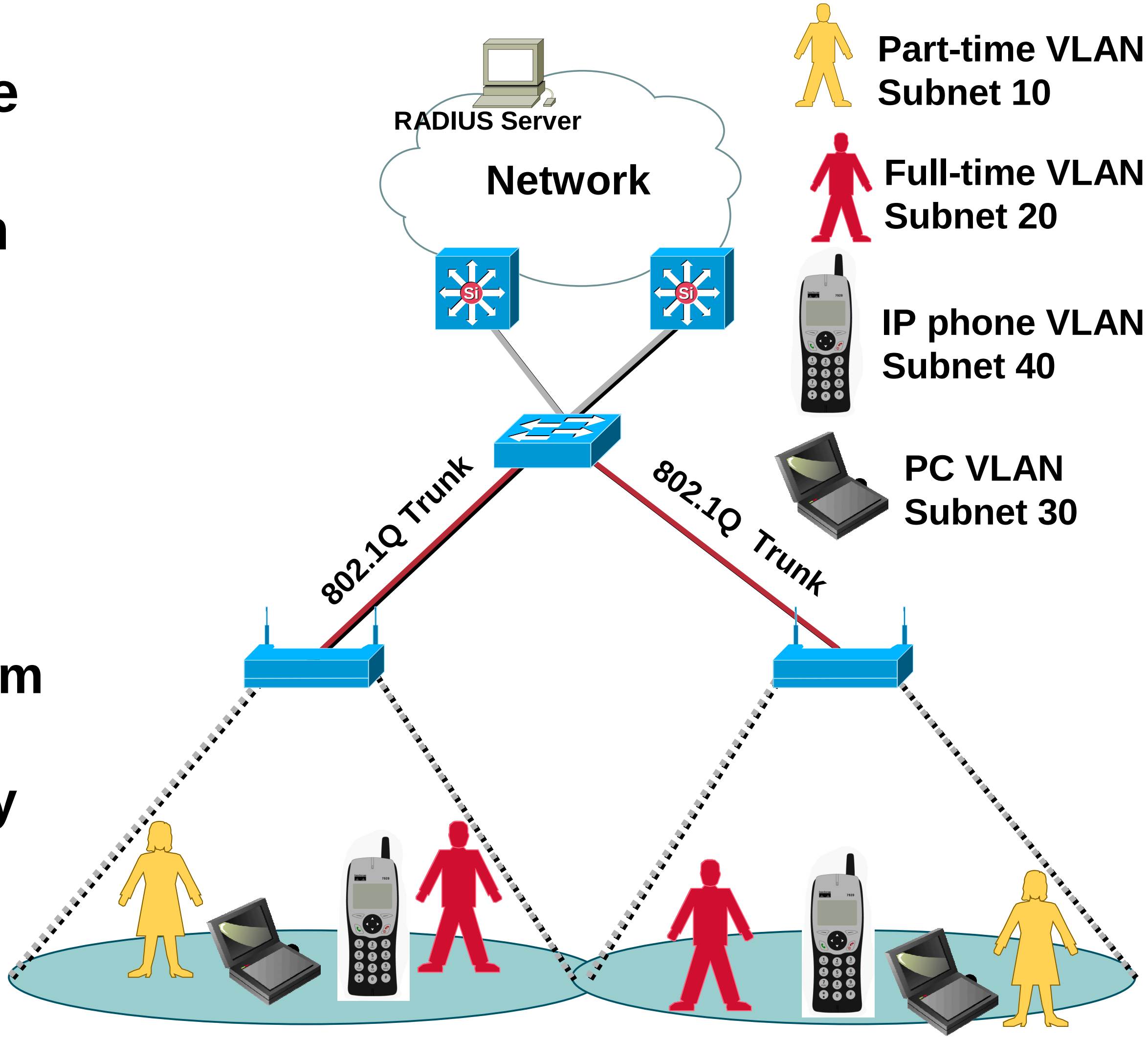
Campus WLAN Design

- .11b vs .11a
- Security
- VLANs
- QoS
- L2/L3 Roaming
- Voice
- Product Line



Extending Wired VLANs to Wireless

- Use AP VLANs to implement user/device differentiation
- Use multiple SSIDs on the wireless interface
  - –SSID to VLAN-id mapping done by AP and enforced by RADIUS server
  - –Implement an Authentication and Encryption mechanism per VLAN/SSID
  - –Implement a security and QoS policy per VLAN/SSID both on wireless and wired sides



Summary of Rules for VLAN Deployment

1. Ability to provision an 802.1Q hybrid trunk on the Switch between it and the AP/Bridge
2. Maximum of 16 VLANs per ESS are supported; each wireless VLAN is represented with a unique SSID name
3. Maximum of 1 “primary”/Guest SSID per ESS is supported (This is the only SSID that is broadcast by the AP)
4. Maximum of 1 unencrypted VLAN per ESS is supported
5. User must configure a unique broadcast key per VLAN
6. Ability to enable TKIP/MIC/Broadcast key rotation per VLAN
7. Ability to configure OPEN, Shared-Key, MAC, Network-EAP (LEAP), and EAP authentication types per SSID

Summary of Rules for VLAN Deployment

8. Shared-Key Authentication supported only on the SSID mapped to the native VLAN (this is most likely to be the “Infrastructure” SSID)

9. A unique policy group (set of L2/L3/L4 filters) is allowed per VLAN

10. Each SSID is mapped to a default wired VLAN; Ability to override this default SSID to VLAN-id using RADIUS-based VLAN access control mechanisms are supported

    RADIUS-based VLAN-id assignment per user is supported

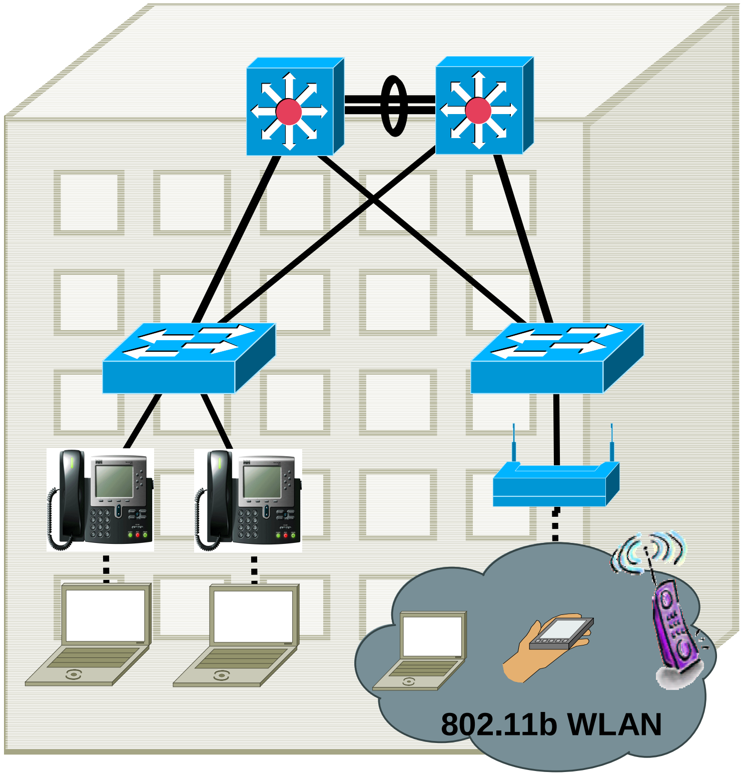
    RADIUS-based SSID access control per user is supported

11. Ability to assign a CoS mapping per VLAN (8 different levels of priorities are supported)

12. Ability to control number of clients per SSID

Campus WLAN Design

- .11b vs .11a
- Security
- VLANs
- QoS
- L2/L3 Roaming
- Voice
- Product Line

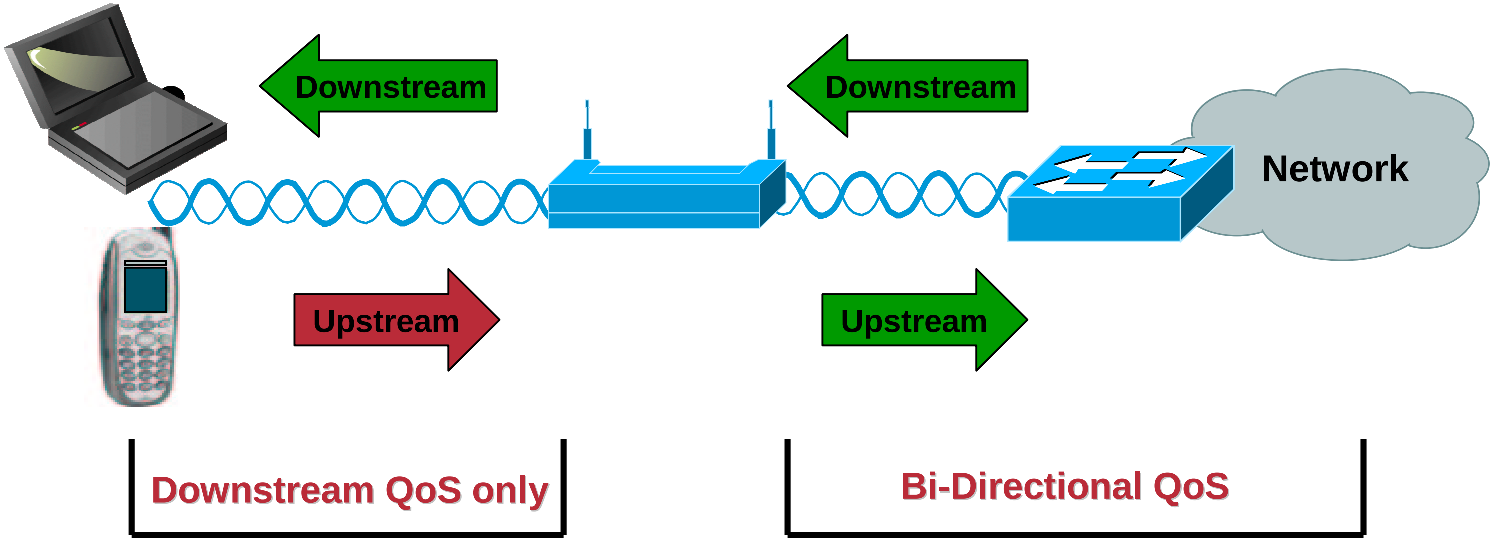


Drivers for QoS in WLAN Networks

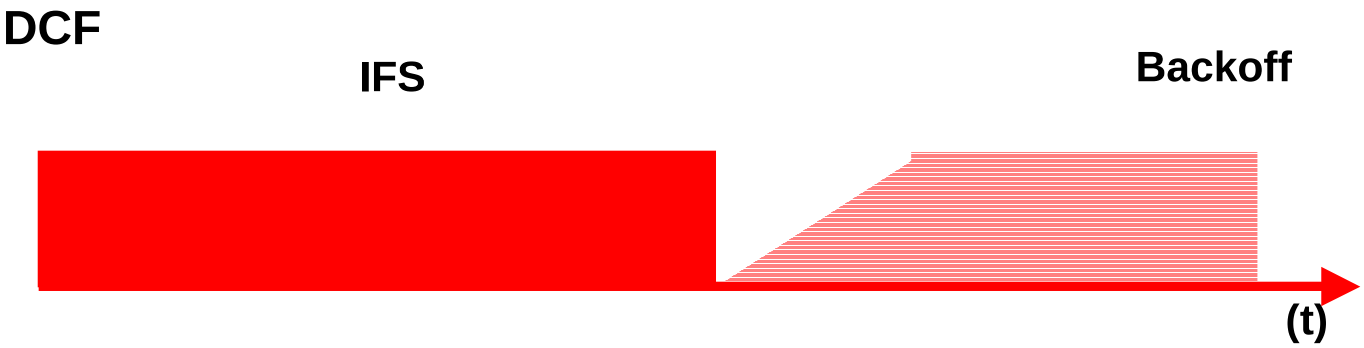
- Combined deployment of data, voice, and video applications over WLAN – Converged networks
- Having the ability to minimize end-to-end delay and jitter for voice and video applications
- Becomes critical in a congested WLAN environment
- Mobility in clients means that simple capacity planning is insufficient to control quality –QoS is perhaps more important in Mobile Networks

WLAN QoS

- WLAN AP can use “EDCF like” functionality to provide “soft” QoS for downstream traffic based on packet classification



Distributed Coordination Function (DCF)

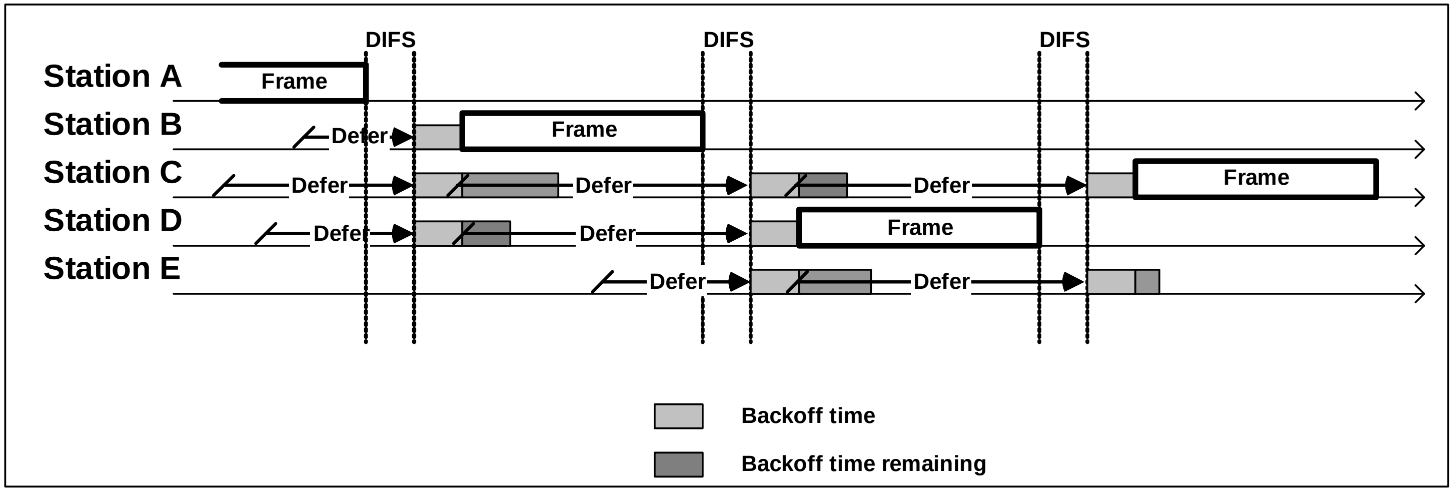


- **What is DCF?**

  Distributed Coordination Function

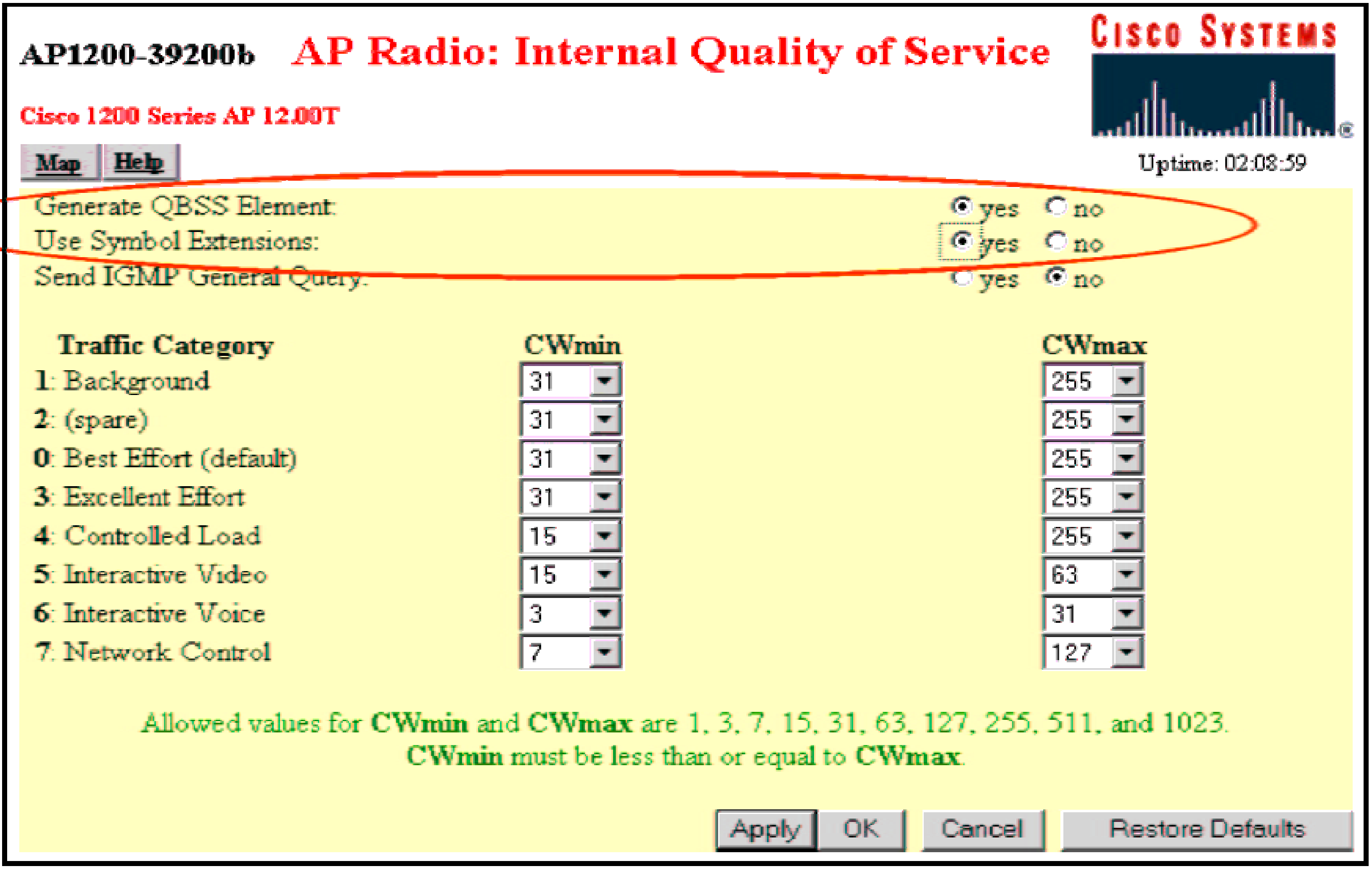
- **Uses IFS and backoff for CSMA**
- **Use RTS/CTS for CA**

Distributed Coordination Function (DCF)



- The interframe space begins when the medium becomes free
  - SIFS, and PIFS are shorter than the DIFS
- Once the DIFS expires the random back off mechanism kicks in
  - First random backoff number is between 0 and CWmin
  - If retransmission is required CWmin doubles until it reaches CWmax

Altering Random backup



AP1200-39200b **AP Radio: Internal Quality of Service**

Cisco 1200 Series AP 12.00T

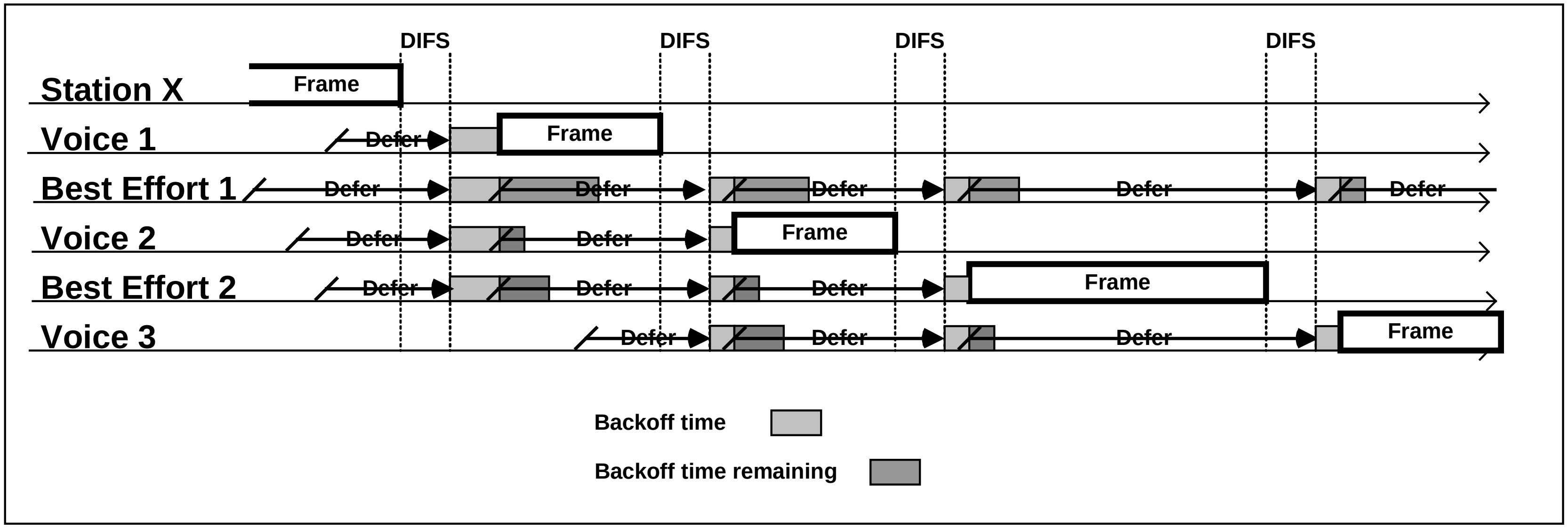
Uptime: 02:08:59

Generate QBSS Element:	● yes	○ no
Use Symbol Extensions:	● yes	○ no
Send IGMP General Query:	○ yes	● no

Traffic Category	CWmin	CWmax
1: Background	31	255
2: (spare)	31	255
0: Best Effort (default)	31	255
3: Excellent Effort	31	255
4: Controlled Load	15	255
5: Interactive Video	15	63
6: Interactive Voice	3	31
7: Network Control	7	127

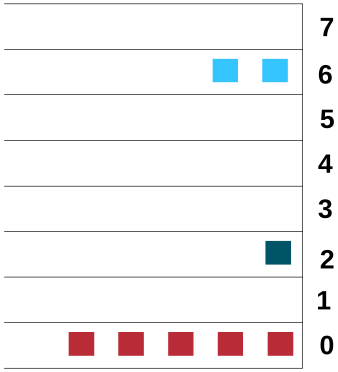
Allowed values for **CWmin** and **CWmax** are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023.
CWmin must be less than or equal to **CWmax**.

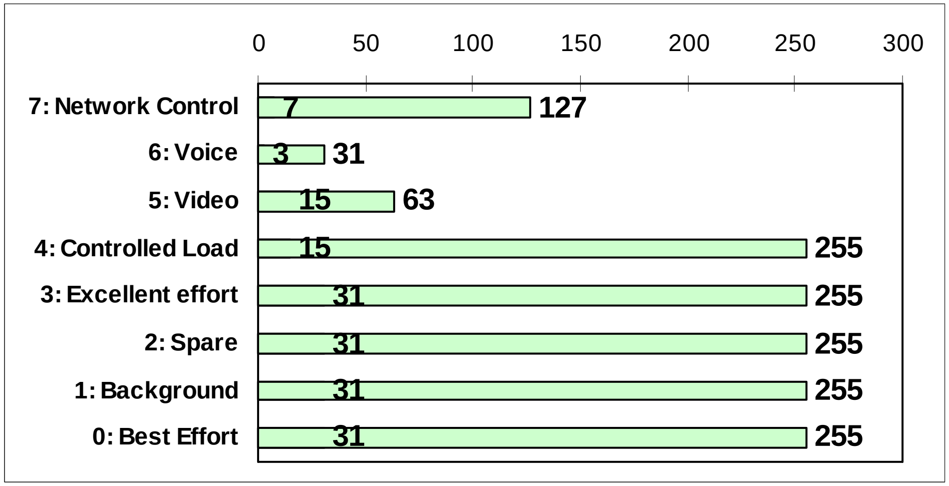
EDCF: CWmin and CWmax



- **CWmin and CWmax a manipulated to give different QoS**
- **This is a statistical process**

“EDCF like” QoS in 12+ code on AP

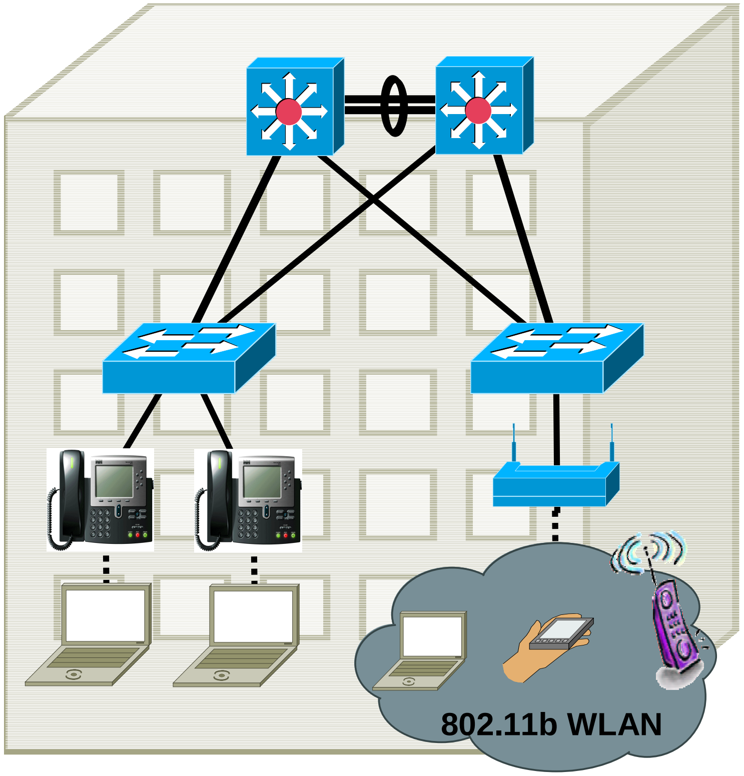




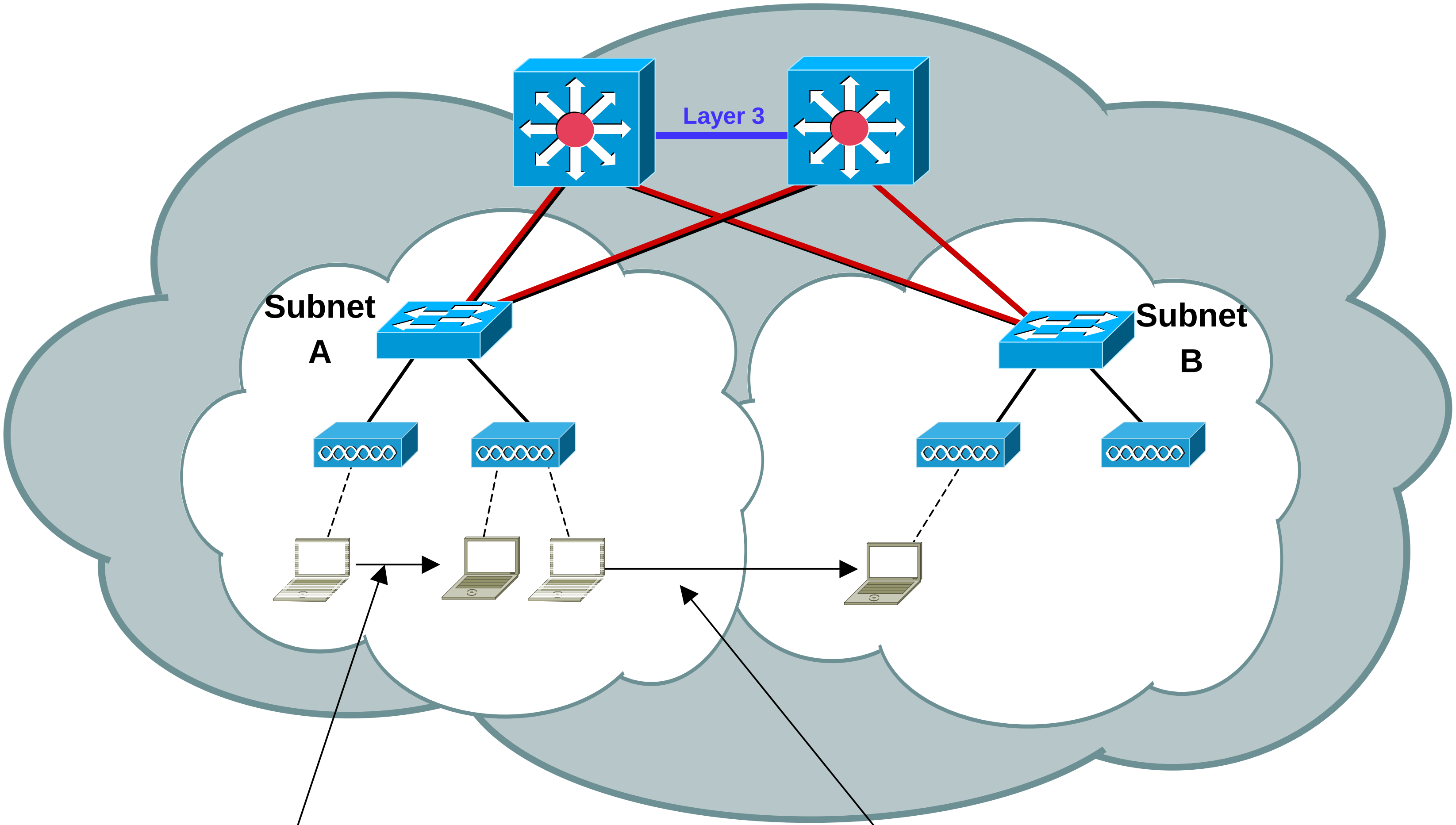
- Per-Station QoS mapping (for the VoIP handsets)
- 802.1p (802.1Q priory bits) to CoS Mapping
- Egress Policy-Group (Filter) based CoS Mapping
- IP Differentiated Services Code Point (DSCP) to CoS mapping
- VLAN-id to CoS mapping

Campus WLAN Design

- .11b vs .11a
- Security
- VLANs
- QoS
- L2/L3 Roaming
- Voice
- Product Line



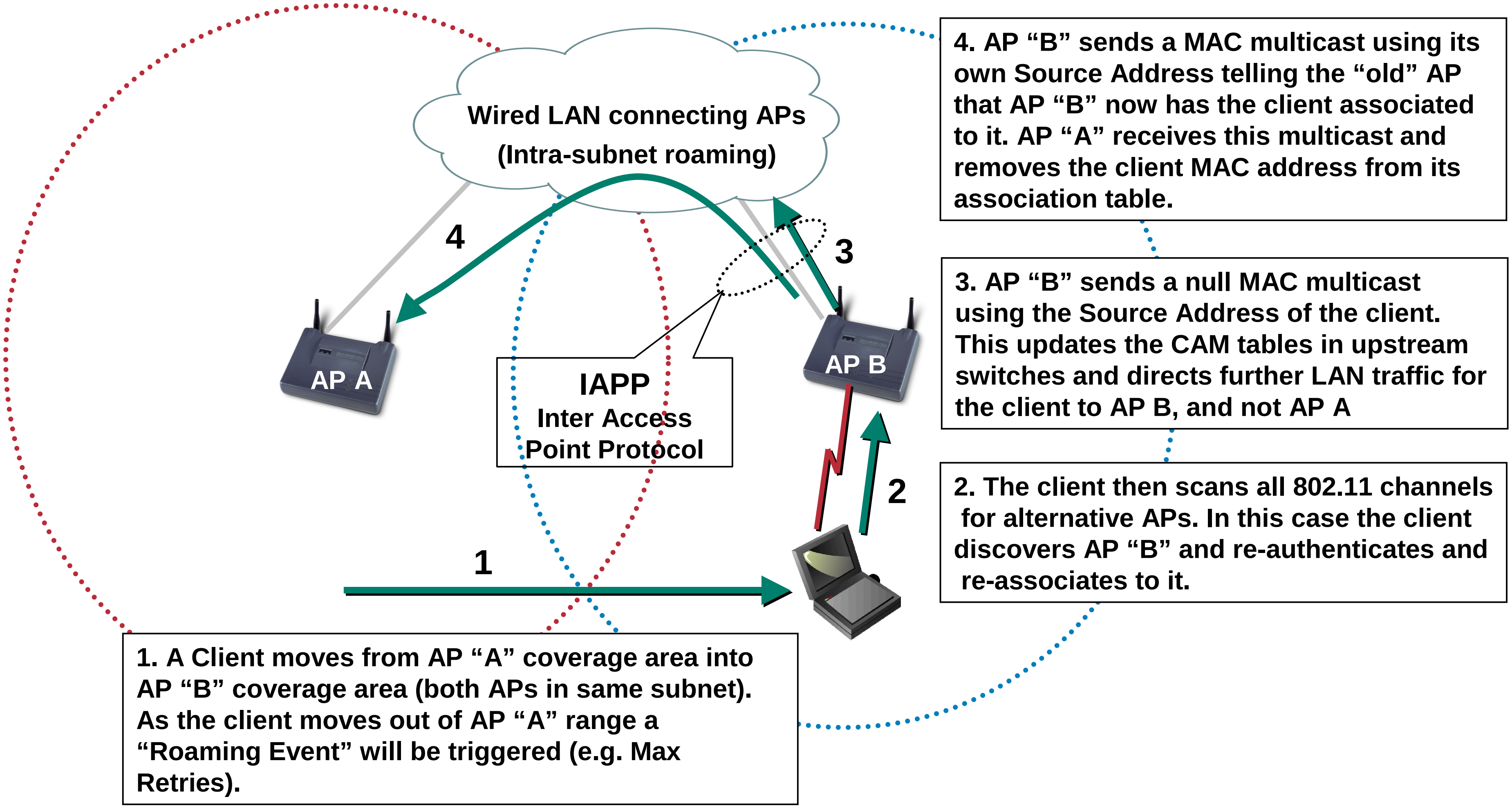
Roaming Types
(Layer 2, and Layer 3)



L2 Roaming

L3 Roaming (Mobile IP)

Same VLAN Roaming



Wired LAN connecting APs
(Intra-subnet roaming)

4

3

AP A

AP B

IAPP
Inter Access
Point Protocol

2

1

4. AP "B" sends a MAC multicast using its own Source Address telling the "old" AP that AP "B" now has the client associated to it. AP "A" receives this multicast and removes the client MAC address from its association table.

3. AP "B" sends a null MAC multicast using the Source Address of the client. This updates the CAM tables in upstream switches and directs further LAN traffic for the client to AP B, and not AP A

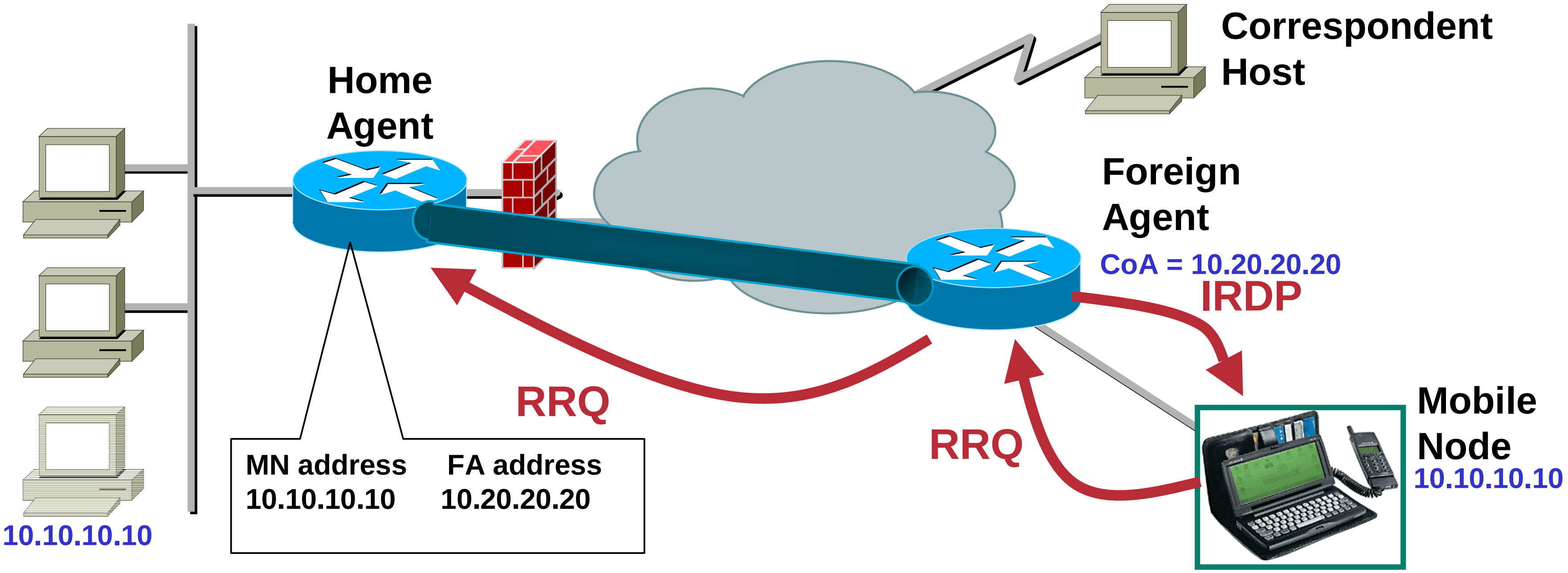
2. The client then scans all 802.11 channels for alternative APs. In this case the client discovers AP "B" and re-authenticates and re-associates to it.

1. A Client moves from AP "A" coverage area into AP "B" coverage area (both APs in same subnet). As the client moves out of AP "A" range a "Roaming Event" will be triggered (e.g. Max Retries).

Mobile IP - What Do I Gain?

- Hierarchical network design for WLAN
  - Mobile IP makes both network designer and mobile user happy
- Seamless transition between Layer 2 connections
  - Continuous “best available” network connectivity
  - Any media that supports IP can support Mobile IP
    - Wired (Ethernet), Wireless (Cellular – 2.5G, 3G and WLAN)
- Application transparency
  - Works with all IP applications
  - Maintains the same IP Address while roaming
  - No authentication is required at each network change
  - Ability to “Push” to the mobile user any time anywhere

Mobile IP
(registration)

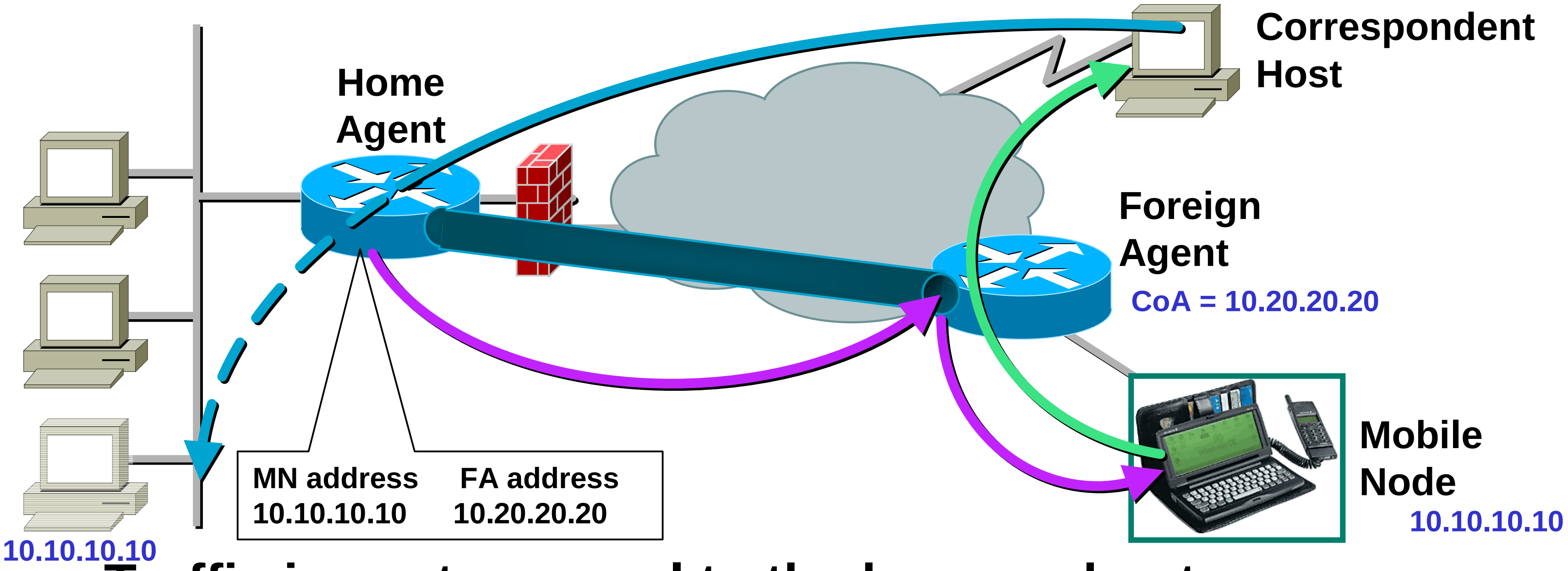


MN address	FA address
10.10.10.10	10.20.20.20

- MN discovers FA – IRDP, MN can solicit IRDP advertisement
- MN sends Registration Request (RRQ) to FA
- Foreign Agent checks RRQ, and forwards to Home Agent
- Home Agent checks RRQ (authentication), and creates binding Table entry correlating MN IP address with FA Care of address (CoA) address

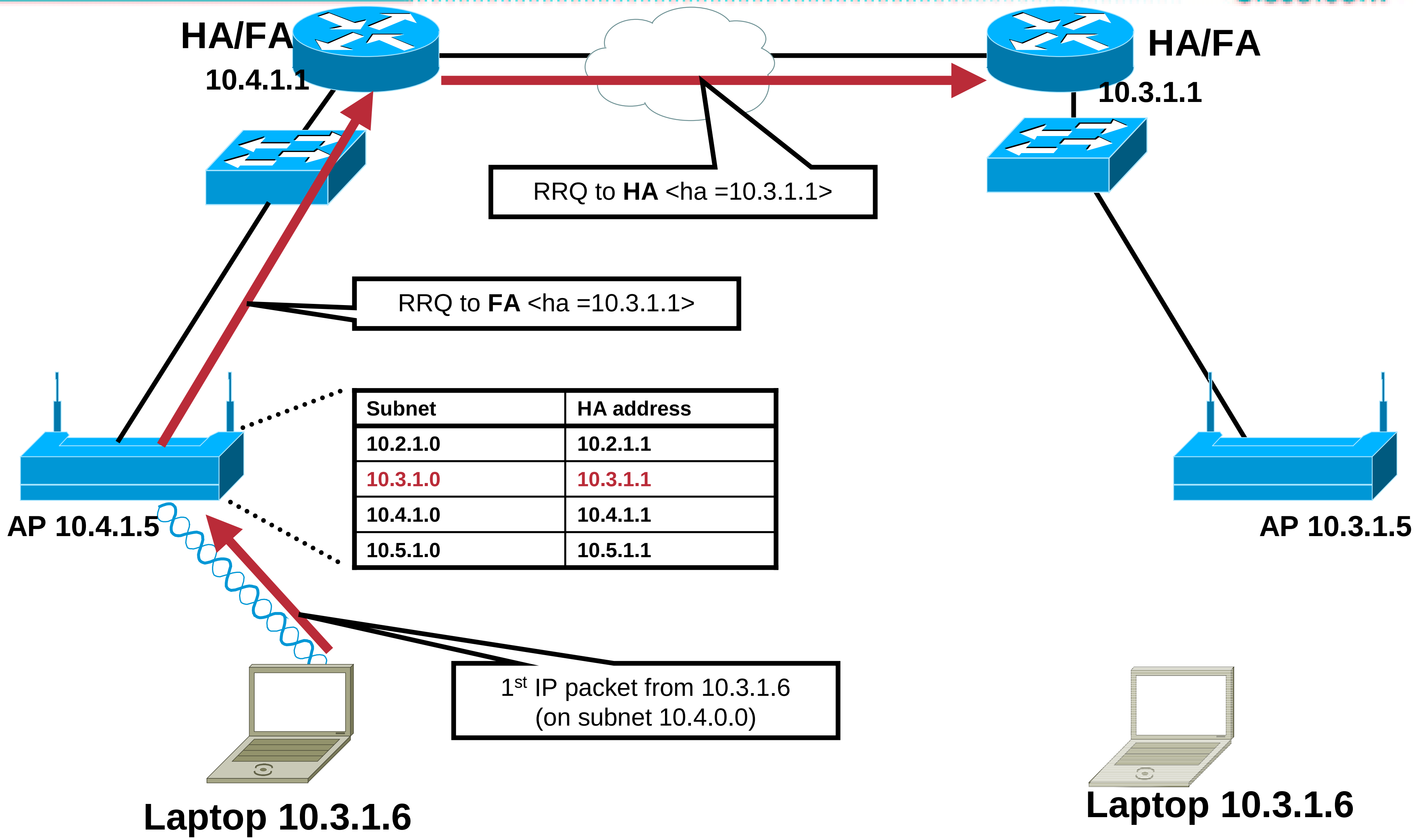
Mobile IP

(Standard Packet Forwarding)



- Traffic is sent as usual to the home subnet
- The home agent intercepts the traffic while the mobile node is registered as away
- Traffic is tunneled to the CoA of the MN and forwarded to MN
- Traffic from the mobile node can go directly to the correspondent host

Proxy Mobile IP - registration



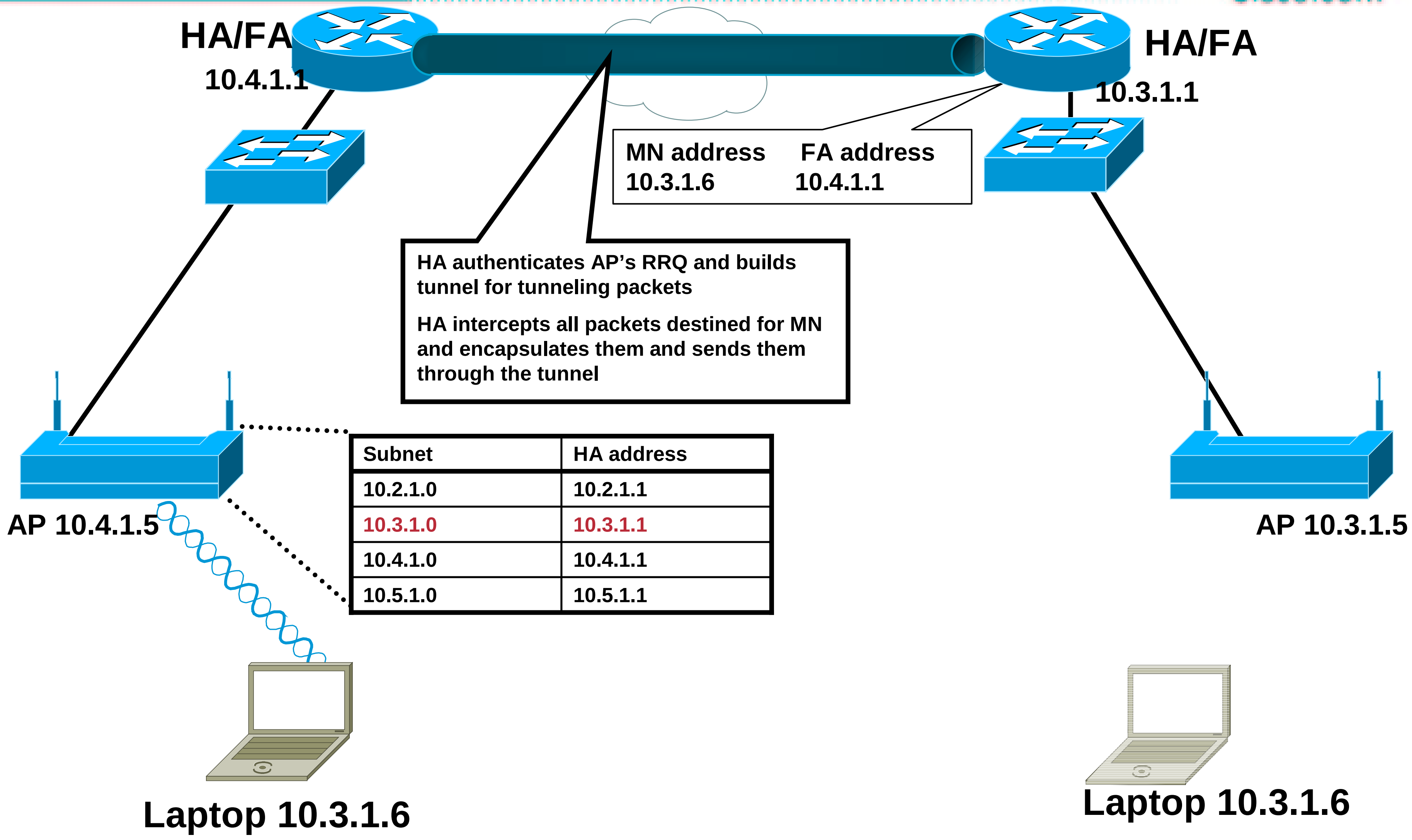
RRQ to **HA** <ha =10.3.1.1>

RRQ to **FA** <ha =10.3.1.1>

Subnet	HA address
10.2.1.0	10.2.1.1
10.3.1.0	10.3.1.1
10.4.1.0	10.4.1.1
10.5.1.0	10.5.1.1

1st IP packet from 10.3.1.6
(on subnet 10.4.0.0)

Proxy Mobile IP – Tunnel built



MN address	FA address
10.3.1.6	10.4.1.1

HA authenticates AP’s RRQ and builds tunnel for tunneling packets

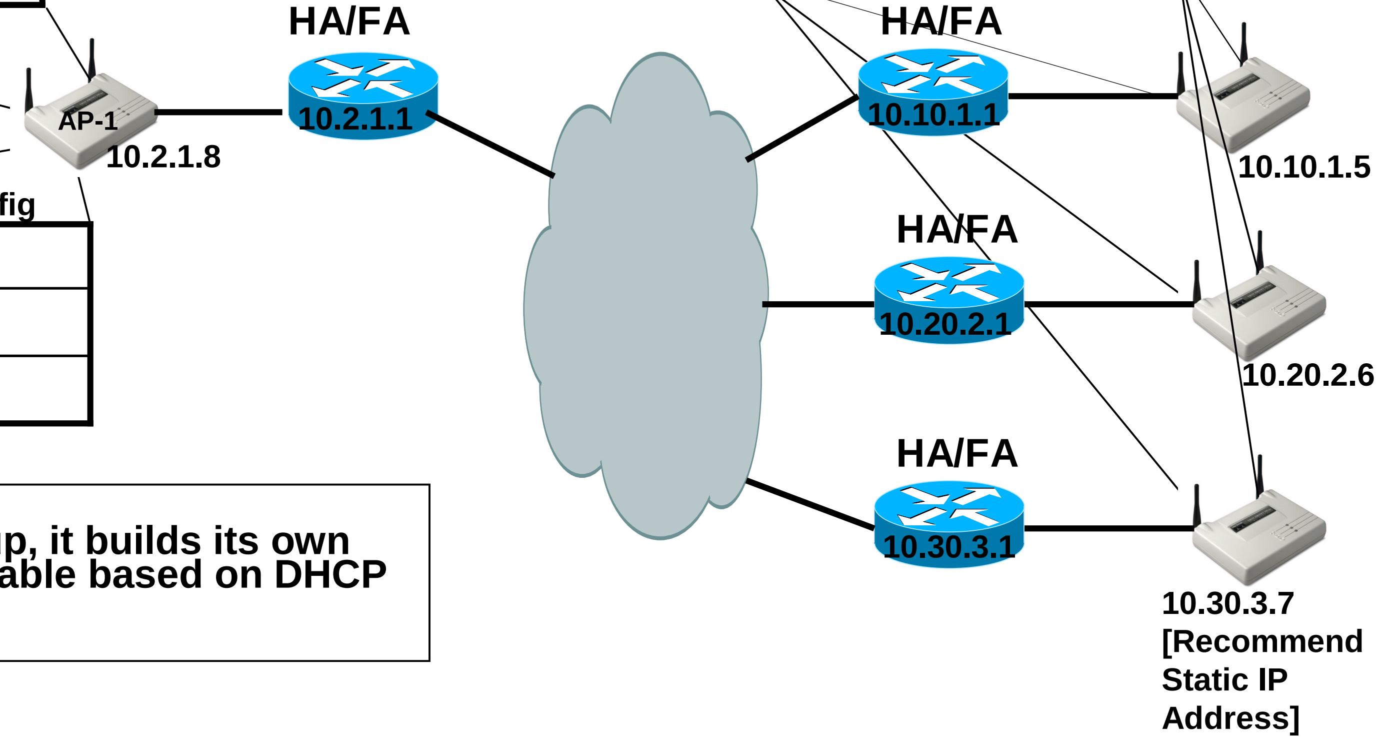
HA intercepts all packets destined for MN and encapsulates them and sends them through the tunnel

Subnet	HA address
10.2.1.0	10.2.1.1
10.3.1.0	10.3.1.1
10.4.1.0	10.4.1.1
10.5.1.0	10.5.1.1

How is the AP subnet/HA table built?

Subnet	HA address
10.2.2.0	10.2.1.1

Subnet	HA address
10.10.1.0	10.10.1.1
10.20.2.0	10.20.2.1
10.30.3.0	10.30.3.1

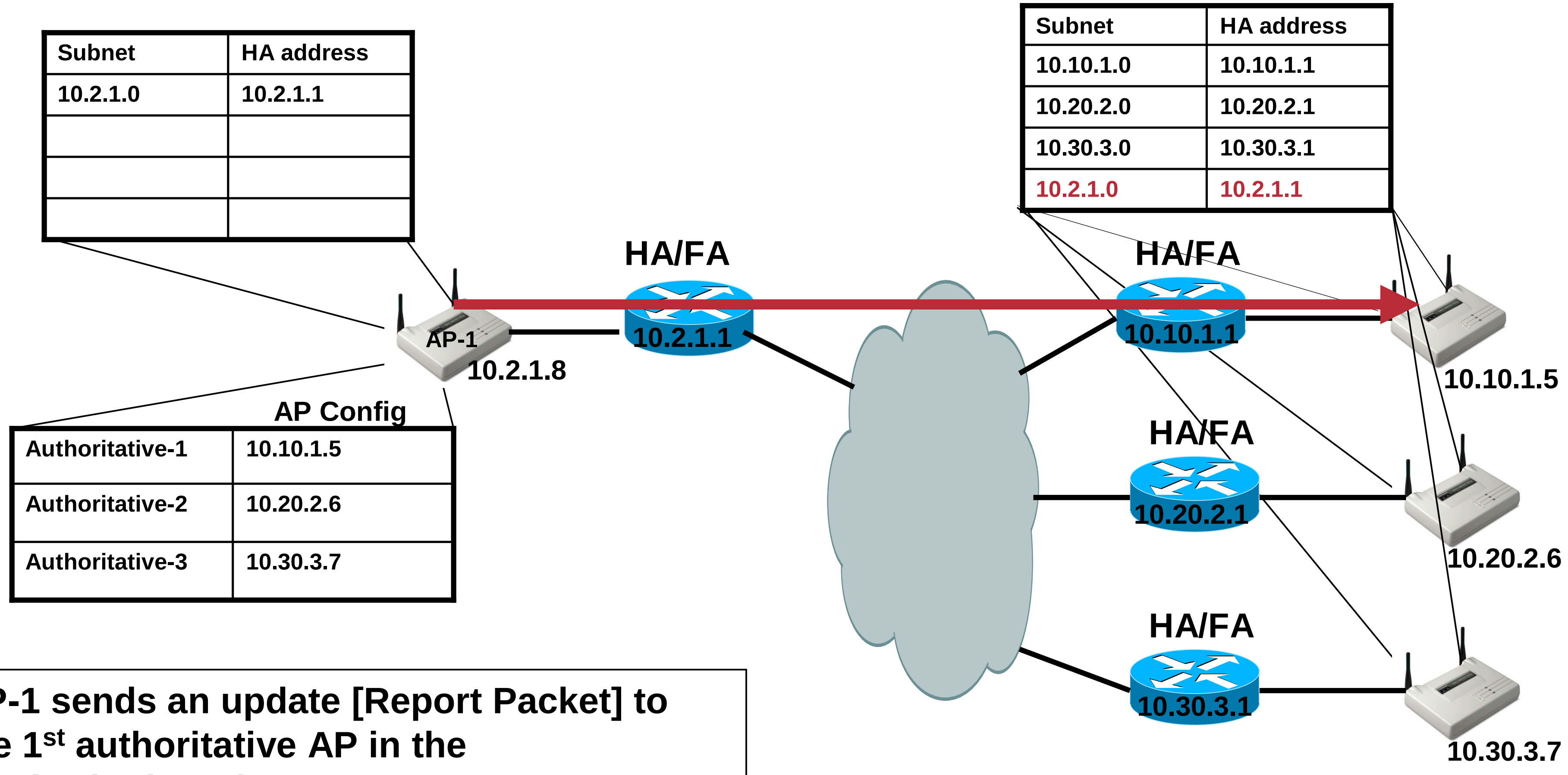


AP Config

Authoritative-1	10.10.1.5
Authoritative-2	10.20.2.6
Authoritative-3	10.30.3.7

When a new AP-1 boots up, it builds its own entry in its “Subnet/HA” table based on DHCP acquired default gateway

How is the AP subnet/HA table built?



Subnet	HA address
10.2.1.0	10.2.1.1

Subnet	HA address
10.10.1.0	10.10.1.1
10.20.2.0	10.20.2.1
10.30.3.0	10.30.3.1
10.2.1.0	10.2.1.1

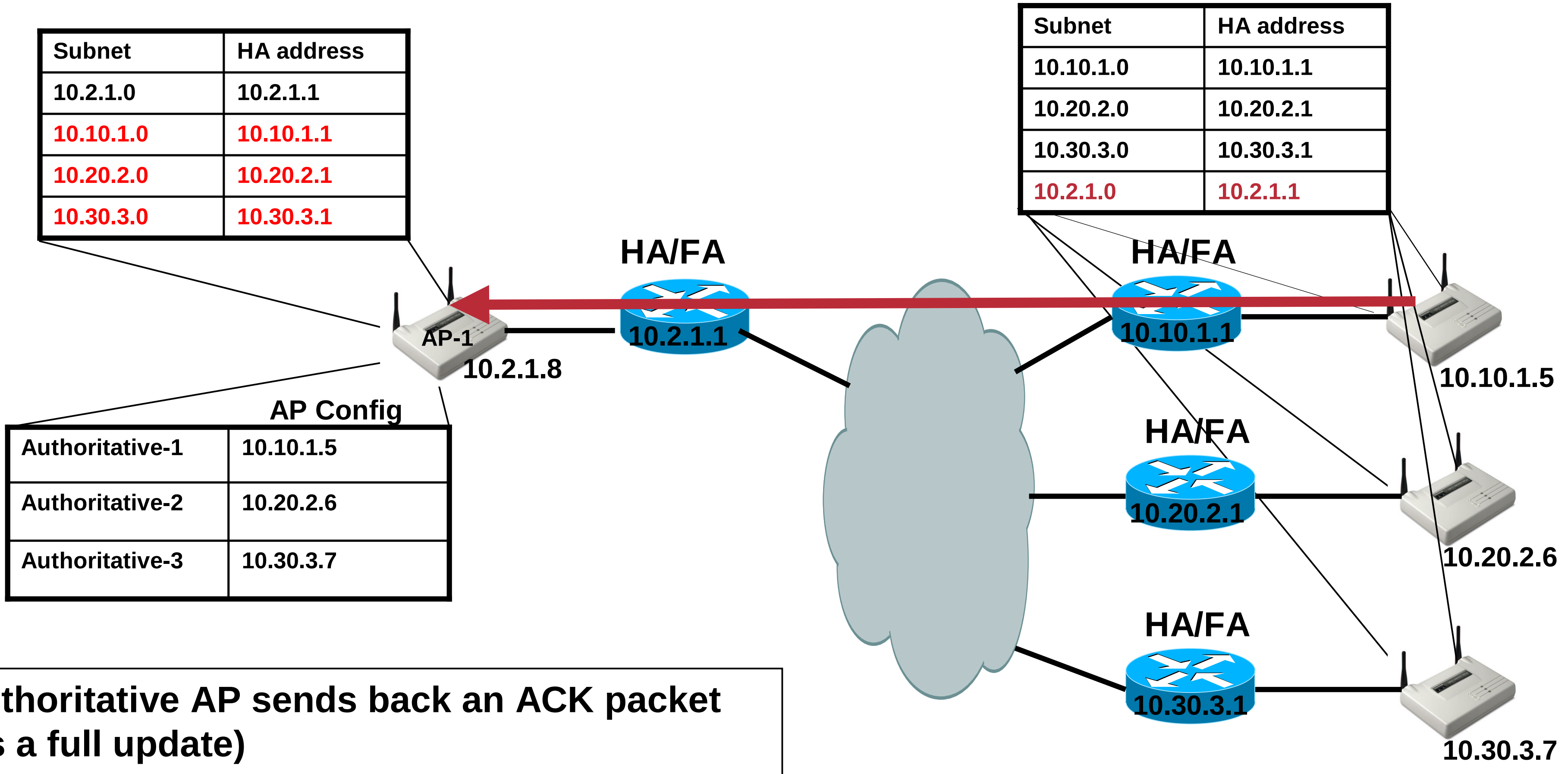
AP Config

Authoritative-1	10.10.1.5
Authoritative-2	10.20.2.6
Authoritative-3	10.30.3.7

AP-1 sends an update [Report Packet] to the 1st authoritative AP in the “authoritative” list

Authoritative-1 updates its Subnet/HA table with the new AP information

How is the AP subnet/HA table built?



Subnet	HA address
10.2.1.0	10.2.1.1
10.10.1.0	10.10.1.1
10.20.2.0	10.20.2.1
10.30.3.0	10.30.3.1

Subnet	HA address
10.10.1.0	10.10.1.1
10.20.2.0	10.20.2.1
10.30.3.0	10.30.3.1
10.2.1.0	10.2.1.1

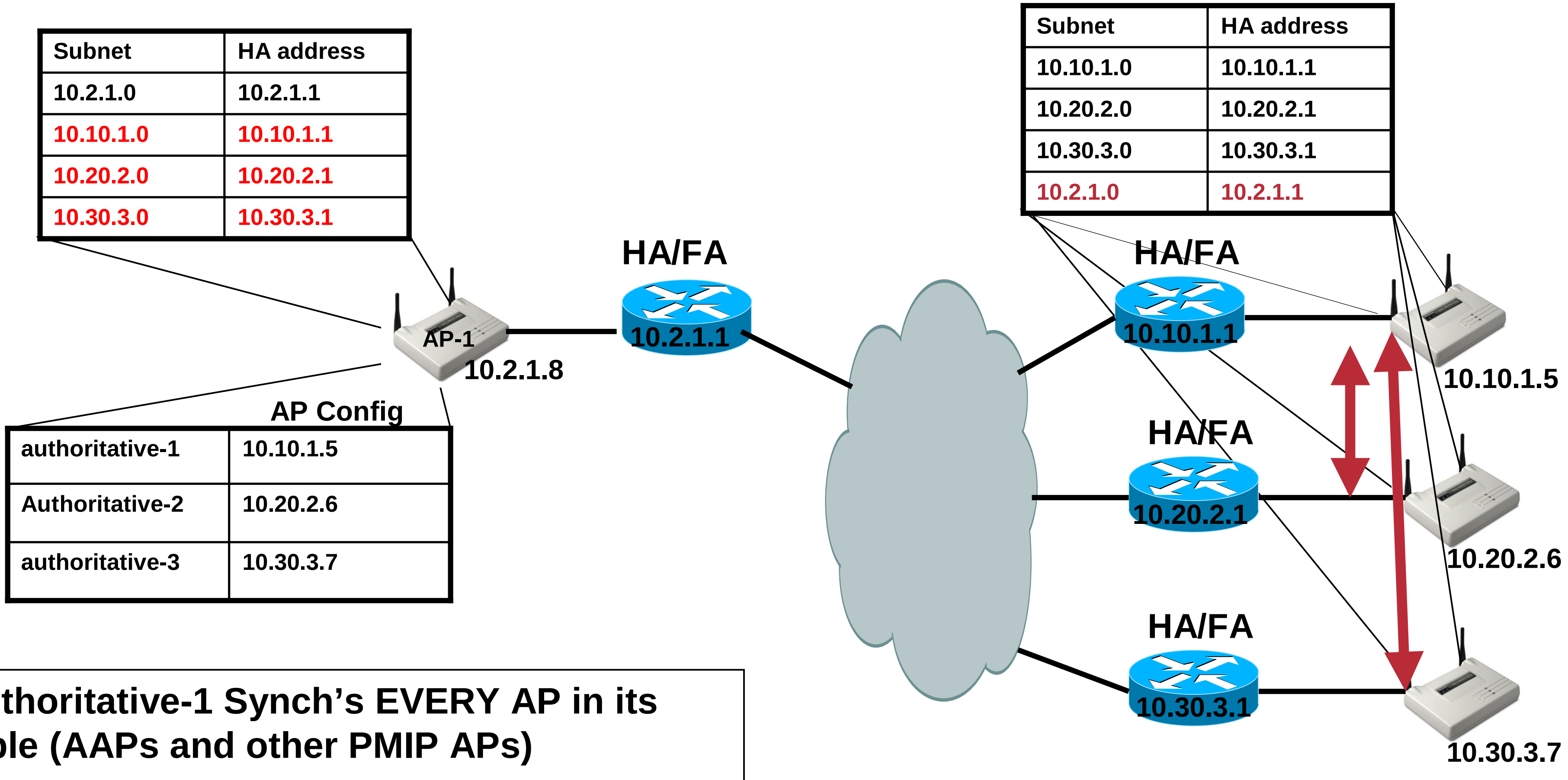
AP Config

Authoritative-1	10.10.1.5
Authoritative-2	10.20.2.6
Authoritative-3	10.30.3.7

Authoritative AP sends back an ACK packet (as a full update)

If AP-1 does not get an acknowledgement from Authoritative-1 within a timeout period, it will try Authoritative-2, then Authoritative-3

How is the AP subnet/HA table built?



Subnet	HA address
10.2.1.0	10.2.1.1
10.10.1.0	10.10.1.1
10.20.2.0	10.20.2.1
10.30.3.0	10.30.3.1

AP Config

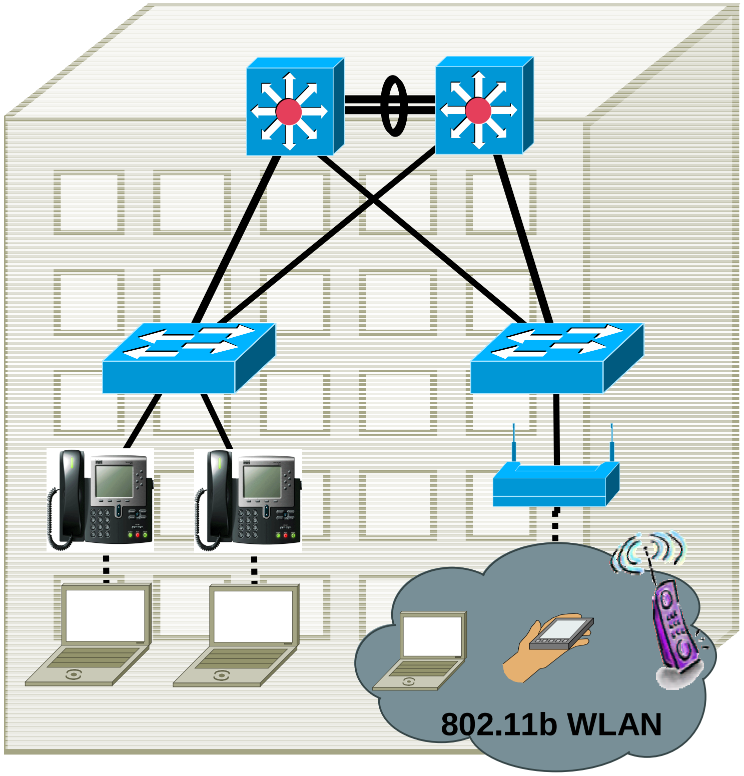
authoritative-1	10.10.1.5
Authoritative-2	10.20.2.6
authoritative-3	10.30.3.7

Subnet	HA address
10.10.1.0	10.10.1.1
10.20.2.0	10.20.2.1
10.30.3.0	10.30.3.1
10.2.1.0	10.2.1.1

Authoritative-1 Synch’s EVERY AP in its table (AAPs and other PMIP APs)

Campus WLAN Design

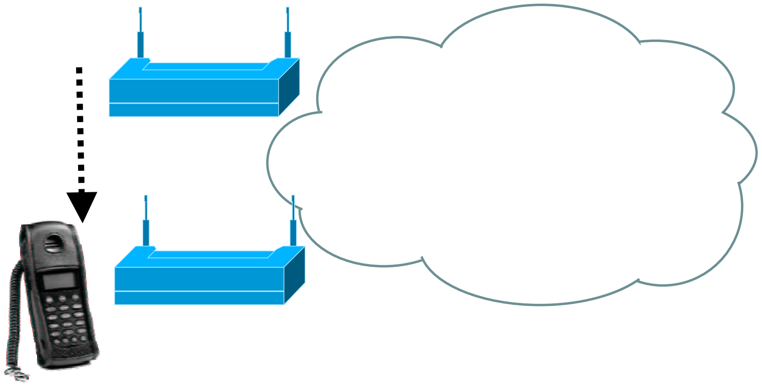
- .11b vs .11a
- Security
- VLANs
- QoS
- L2/L3 Roaming
- Voice
- Product Line



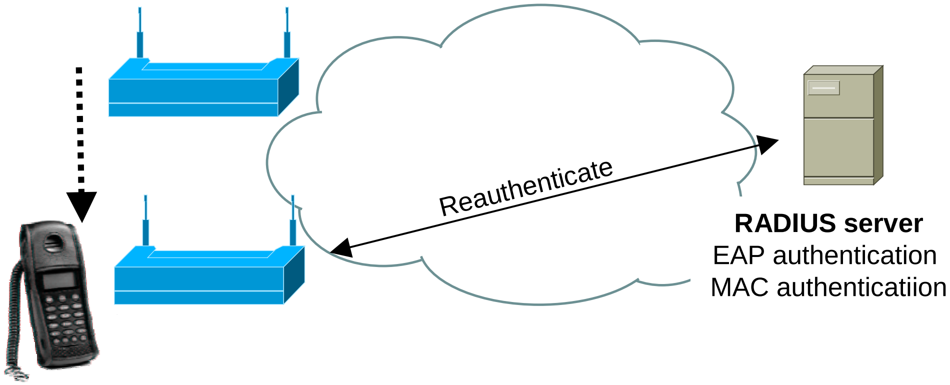
Voice and L2 roaming

- Be aware that a WLAN station re-authenticates every time it roams to a new AP
- Additional latency will be introduced when this re-authentication requires a radius server
  - Is RADIUS server on Campus or WAN
- Consider using static WEP and VLAN with L3 filters instead of EAP or MAC security

STATIC WEP

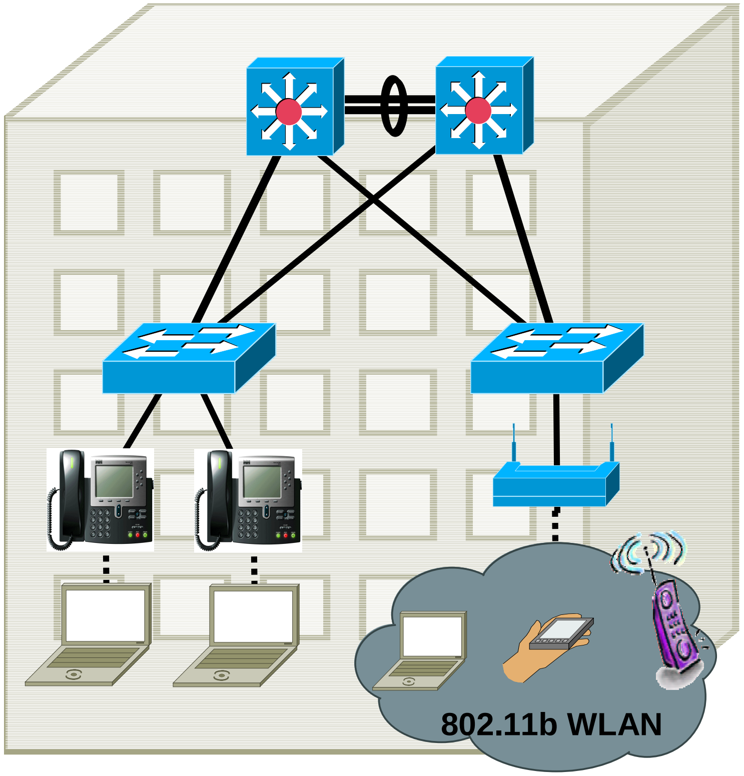


EAP authentication



Campus WLAN Design

- .11b vs .11a
- Security
- VLANs
- QoS
- L2/L3 Roaming
- Voice
- Product Line



Wireless Product Line

No Security

Public Access

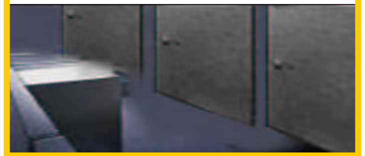
Basic Security

Telecommuter and Small Business

Enhanced Security

Mid-Market and Enterprise

Specialized Security

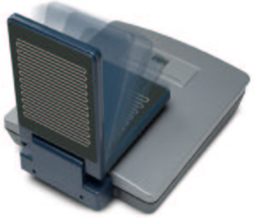


Mobile User and Public Access

Cisco Aironet 350 Series (.11b)

Cisco Aironet 1100 Series Built-in .11b, future .11g

Cisco Aironet 1200 Series Built-in .11b module



Cisco Aironet 1200 Series Built-in .11b/11a module

Cisco Aironet 1200 Series future .11g Upgrade

CISCO SYSTEMS ®

EMPOWERING THE
INTERNET GENERATION℠