سیسکو به پارسی

CCNA Wireless : 640-721

ترجمه و تالیف :

یوسف نعیمی

انجمن سیسکو به پارسی

http://forum.ciscoinpersian.com

تقدیم به پدر و مادرم

به خاطر مهربانی و صبرشان

فهرست مطالب

به نام خدا

حدود سه سال پیش پس از ۴ ساعت نشستن سر کلاس های درس کسل کننده ی دانشگاه ، روانه ی سلف سرویس شدم تا مثل همیشه هنگام غذا خوردن ، به این فکر کنم که رابطه ی مهندسی برق – مخابرات با این همه انتگرال و سری فوریه و معادلات و فرمولهای ریاضی چیست و اینکه اگر قرار بود تا ترم ۸ هم فقط و فقط ریاضیات بخوانم ، چرا رشته ی ریاضیات محض یا کاربردی را انتخاب نکردم ؟ چند وقتی بود که فکر موضوع پروژه ی کارشناسی نیز به این افکار اضافه شده بود و اینکه آیا باید مثل سایرین پروژه ای تحقیقاتی و تئوریک بردارم و باز هم ... ؟ اما آن روز ، روز دیگری بود . بطور اتفاقی گفتگوی دو نفر (که ظاهرا دانشجوی IT یا مهندسی کامپیوتر بودند) را شنیدم که در مورد طراحی شبکه های کامپیوتری و روند حرکت ترافیک در اینترنت صحبت می کردند ؛ عباراتی گنگ و نامفهوم که هیچ کدام را نمی فهمیدم ، اما آنچنان مرا به فکر فرو داشت که قید کلاس های عصر را زدم (تقریبا مثل همیشه!) و تا پاسی از شب مشغول به جستجو و تحقیق در مورد آن عبارات شدم ... Networking ... Cisco ... Microsoft ...

حدود دو سال پیش دانشگاه تمام شده بود ، پروژه ی کارشناسی ام (سیسکو) را به لطف و همکاری جناب دکتر فرخی به پایان رسانده بودم ، و مقاله ای نیز در مورد سیسکو در یک همایش (مخابرات و فناوری اطلاعات) ارائه داده بودم . اما همچنان احساس می کردم که نمی دانم در چه زمینی گام بر می دارم ؛ احساسی که اولین بار نبود آن را تجربه می کردم . اما آن روز نیز روز دیگری بود . به طور اتفاقی با سایت جناب شفق زندی آشنا شدم . مقاله ی شبکه را از کجا شروع کنیم را خواندم ، سپس بلافاصله مقاله ی طراحی یک data center را خواندم ؛ که البته تقریبا هیچ چیز از این مقاله را نفهمیدم ، اما همان روز فهمیدم که این همان کاریست که دوست دارم انجام دهم ؛ این همان چیزیست که همیشه در کلاس های سرد و خسته کننده ی دانشگاه به دنبالش می گشتم ؛ و این همان شغلیست که دوست دارم در آن بازنشسته شوم . از آن به بعد تمام مقالات و آموزش های ایشان را مطالعه کردم و در بسیاری از زمینه ها از ایشان کمک گرفتم و این افتخار را دارم که تا امروز همچنان از راهنمایی های ایشان استفاده می کنم .

حدود یک سال پیش پس از اتمام CCNA و با توجه به اینکه آشنایی نسبتا خوبی با شبکه های وایرلس و موبایل داشتم (درس مخابرات سیار جناب دکتر ندا در ترم آخر ، تنها درسی بود که برایم ارزش کلاس رفتن را داشت و از بین ۱۴۲ واحد ، تنها ۳ واحدی بود که همیشه از آن به خوبی یاد می کنم) ، تصمیم گرفتم همراه با مطالعه ی کتاب CCNA Wireless ، نکات مهم و کلیدی هر فصل را استخراج کرده و در فروم سیسکو به پارسی قرار دهم تا به رایگان در دسترس همگان قرار گیرد ؛ شاید دینم نسبت به دوستانی که خیلی چیزها از آنان آموختم ادا شود ، که ذکات علم (هرچند اندک) نشر آن است . اولین فصلی که آماده شد ، فصل ۱۲ بود که بنا به نیاز یکی از دوستان ، ابتدا روی این فصل کار کردم . سایر فصول نیز هرکدام به محض آماده شدن ، در اختیار دوستان گذاشته می شد تا بتوانند دریافت و مطالعه بفرمایند .

امروز این کتاب آماده شده و جهت دانلود در بخش نشر دانش فروم سیسکو به پارسی قرار گرفته است . هرچند در طی این مدت ، به دلایلی وقفه ای چند ماهه بین فصول مختلف بوجود آمد ، اما نهایت تلاش من بر این بوده که هیچ نکته ی مهمی از قلم نیفتد و سعی کردم این امر را با مطالعه ی چندباره ی کتاب اصلی و استخراج نکات مختلف برای تشریح مطالب محقق سازم . در برخی موارد لازم بود از سایر منابع برای توضیح بیشتر مفاهیم کمک بگیرم ؛ گاهی نیز به دلیل جذابیت موضوع برای خودم ، نکاتی خارج از کتاب اصلی اضافه نمودم که البته هم به درک بهتر سایر مطالب کمک شایانی می کند و هم شما را نسبت به ادامه ی مطالعه در مراحل بالاتر (CCNP Wireless , CCIE Wireless) ترغیب می نماید . ناگفته نماند که در تمام این مدت ، جناب آقای زندی بر تمامی مطالب نظارت داشته و نکات ارزشمندی را به من گوشزد می نمودند که باعث بهتر شدن سطح کیفی مطالب گردیدند و جا دارد از ایشان کمال تشکر را داشته باشم .

از همه ی کسانی که این کتاب را مطالعه می فرمایند تقاضا می کنم هرنوع پیشنهاد یا انتقادی را با من در میان بگذارند تا هم بتوانم ایرادات این کتاب را برطرف سازم و هم انشالله در مقالات و کتاب های بعدی این نکات را لحاظ کنم . ضمنا انتشار این کتاب در فضای حقیقی یا مجازی با ذکر نام و منبع ، بلامانع و باعث خرسندیست .

در پایان از تمامی دوستان تقاضا دارم همه با هم کمی از وقت خود را صرف نشر دانشی بکنیم که هرچند با زحمت زیاد و با صرف هزینه و وقت بسیار و احتمالا به منظور کسب درآمد به دست آمده است ، اما ارائه ی بخشی از آن به رایگان ، نه تنها می تواند رشد و پیشرفت ما را دوچندان کند ، بلکه درک مفاهیم را برای خودمان نیز بهتر و عمیق تر می سازد . از این رو چنانچه مایلید در زمینه ی مورد علاقه تان مقاله ای تالیف کنید و یا مطلب آموزشی خاصی را ترجمه بفرمایید و با سایر هموطنانمان به اشتراک بگذارید ، ما در بخش نشر دانش فروم سیسکو به پارسی دست همه ی شما عزیزان را به گرمی می فشاریم .

یوسف نعیمی
u3fnm@yahoo.com
اسفند ماه ۱۳۹۰

مقدمه جناب آقای شفق زندی

یکی از تحولات شبکه در دهه ی اخیر ، استقبال گسترده از شبکه های Wireless LAN یا WLAN است . این تکنولوژی از Ethernet بصورت بیسیم بهره می برد . بیش از ۴۰۰ کمپانی عضو WiFi Alliance هستند و ۱۱۰۰۰ محصول سازگاز با شبکه های بیسیم توسط این سازمان ثبت شده است . استفاده از این فن آوری مزایای زیادی برای شرکت ها و سازمان های گسترده به همراه داشته و سرعت توسعه شبکه ها را چند برابر کرده است .

شبکه های بی سیم نسبت به دهه ی پیش تغییر کرده و دیگر به راه اندازی چند Access-Point خلاصه نمی شوند . سیستم های مدیریت شبکه Wireless روی Mobility و Location Tracking همراه با QoS و Security پیشرفت قابل ملاحظه ای داشته اند .

از استراتژی های جدید سازمان ها استفاده از مفهوم BYOD یا Bring your own device است که به کاربران شبکه ، کارکنان یا دانشجویان این اجازه را می دهد تا دستگاههای بی سیم خود را به شبکه سازمان متصل کنند و از iPad و تلفن همراه خود برای انجام امور روزمره استفاده نمایند. این مفهوم برای یک سازمان بدون زیرساخت مناسب و امن WLAN میسر نبوده و نخواهد بود . از آنجا که بدون وجود معماری متناسب نمی توان یک شبکه را به بهره وری رساند ، مطالعه اصول اولیه و پایه ای شبکه های بیسیم به همه ی متخصصین و مهندسین شبکه پیشنهاد می شود .

کتابی که در پیش رو دارید ، این اصول را بصورت اجمالی و به زبان شیرین پارسی جهت آمادگی برای مدرک CCNA Wireless تشریح کرده است . در پایان از آقای یوسف نعیمی که زحمت ترجمه و نگارش این کتاب را به زبانی شیوا و کاربردی بعهده داشته اند تشکر می کنم . امیدوارم که این مسیر ادامه داشته باشد و مطالب شبکه به سادگی در اختیار پارسی زبانان قرار بگیرد .

شفق زندی

زمستان ۱۳۹۰

چه کسانی باید این کتاب را مطالعه کنند ؟

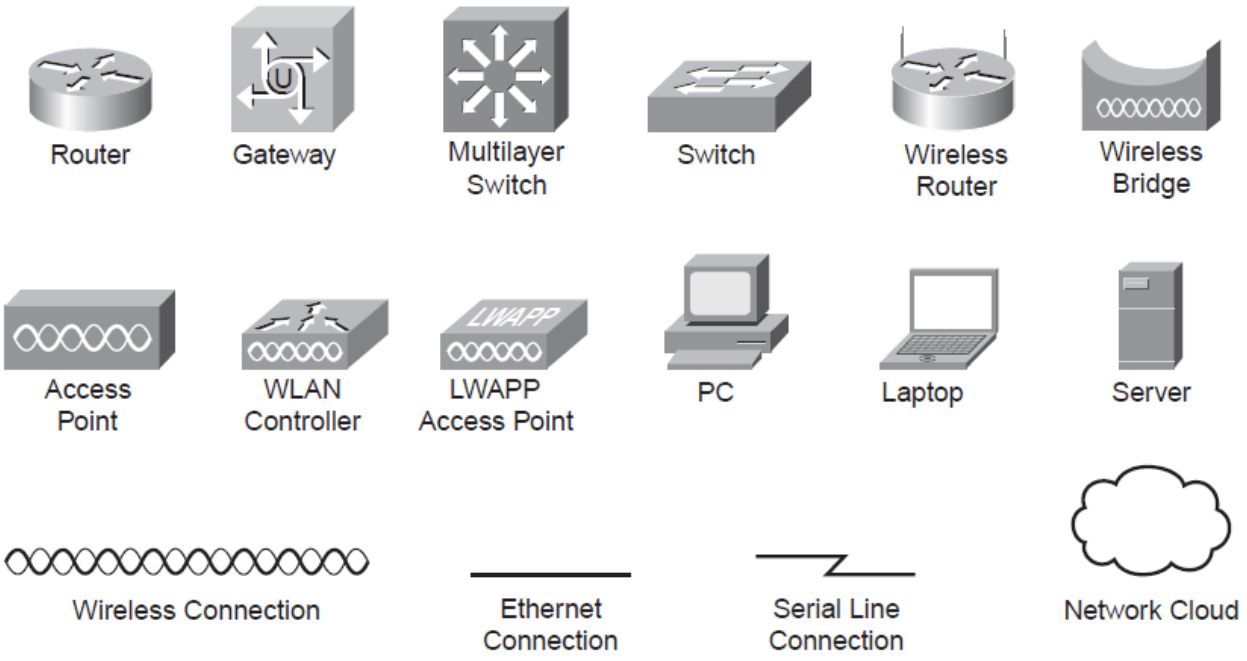
تقریبا تمام کسانی که به نوعی با شبکه های بیسیم در ارتباطند می توانند از این کتاب استفاده کنند ؛ زیرا این کتاب عموما به مفاهیم اصلی و پایه ای شبکه های بیسیم می پردازد . به عبارتی بیش از آنکه مبتنی بر محصول باشد ، مبتنی بر تکنولوژیست . یادگیری این اصول و مفاهیم ، علاوه بر آشنا کردن شما با نحوه عملکرد و تنظیمات محصولات سیسکو ، شما را قادر می سازد که به راحتی با سایر تجهیزات و دستگاههای wireless نیز کار کنید .

اما مخاطب اصلی این کتاب ، افرادی هستند که قصد دارند برای آزمون Cisco CCNA Wireless : 640-721 آماده شوند . این کتاب تمامی نکات و سرفصل های آزمون 640-721 را بطور کامل پوشش داده است ، بطوریکه معتقدم مطالعه ی کامل این کتاب ، نه تنها شما را برای این آزمون آماده می سازد ، بلکه پیش زمینه ی خوبی برای سطوح بالاتر نیز به شما خواهد داد . هرچند ، چنانچه به منظور آمادگی برای امتحان این کتاب را مطالعه می فرمایید و یا نیاز به مطالعه ی بیشتر در بخش خاصی داشتید ، سعی کنید از کتاب اصلی نیز کمک بگیرید . همچنین توصیه می شود برای دوره ی نهایی قبل از آزمون ، حتما نمونه سوالاتی را که در اول هر فصل کتاب اصلی آورده شده ، مطالعه بفرمایید .

فراموش نکنید که سوالات خود را می توانید در بخش Wireless و ارتباط بیسیم به پارسی فروم سیسکو به پارسی مطرح سازید .

فصل اول و دوم : آشنایی با مفاهیم اولیه Wireless Networking

- مفاهیم اولیه
- باند های فرکانسی
- مدولاسیون ، تکنیک ها و نحوه ی کار آنها
  - ✓ DSSS
  - ✓ Chipping Code
  - ✓ Complementary Code Keying
  - ✓ BPSK
  - ✓ QPSK
  - ✓ OFDM
  - ✓ MIMO
  - ✓ CSMA/CA
- استانداردها و تشکیلات قانون گذاری
  - ✓ FCC
  - ✓ ETSI
  - ✓ IEEE



شاید دشوارترین بخش در مباحث وایرلس ، شروع باشد ؛ آن هم اینکه از کجا و چگونه شروع کنیم . در این فصل قصد داریم به مباحث اولیه و پایه ی شبکه های وایرلس بپردازیم (به دلیل مرتبط بودن مفاهیم اولیه ، فصول اول و دوم را در یک فصل بررسی می کنیم). برخی را تا حد نیاز با جزییات بیان خواهیم کرد ، اما در مورد برخی دیگر ، تنها به تعریف بسنده خواهیم کرد و ادامه بحث را به فصول آتی موکول خواهیم نمود . شاید مطالب کمی خشک و کم انعطاف باشند (که ویژگی مطالب پایه تمام دروس مهندسی است) ، اما دانستن آنها الزامیست .

مفاهیم اولیه Wireless

Modulation : مدولاسیون به معنای اضافه کردن داده به یک سیگنال carrier می باشد . لذا برای قرار دادن data روی سیگنال RF ، به یکی از تکنیک های مدولاسیون نیاز داریم که معروف ترین آنها عبارتند از : مدولاسیون دامنه (AM) ، مدولاسیون فرکانس (FM) ، و مدولاسیون فاز (PM) .

Frequency : تعداد دفعاتی که یک موج یا یک سیگنال ، در زمان یک ثانیه ، نوسان میکند (واحد آن هرتز می باشد) .

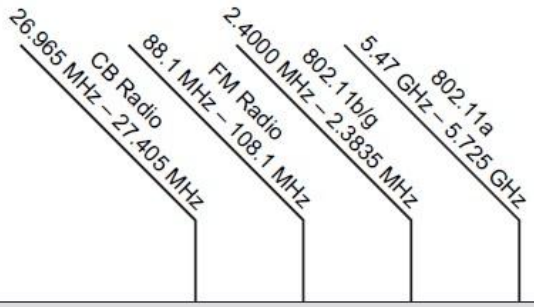
Quality : در تکنولوژی رادیو ، باندهای فرکانسی مختلف ، بر اساس کیفیت تقسیم بندی شده اند . کمترین کیفیت را باند شهروندی (Citizen's Band) دارد که دارای پهنای باند 3KHz میباشد . FM Radio کیفیت بهتری دارد (175KHz) و سپس TV Signal دارای کیفیت بسیار زیادی می باشد (4500KHz) .

Encoding : فرآیند تبدیل اطلاعات از یک شکل به شکل دیگر .

Chip یا **bit** : chip و bit درواقع یکی هستند ، اما bit نشان دهنده ی دیتا است و chip برای carrier encoding مورد استفاده قرار می گیرد . به هر کدام از اجزای پیام ، یک bit می گوییم ؛ و هنگامیکه این پیام روی carrier مورد نظر encode شد ، به آن chip می گوییم .

Access Point (AP) : به ساده ترین بیان می توان گفت که رفتار یک AP در یک شبکه ی بیسیم ، شبیه رفتار یک Hub در یک شبکه ی wired است .

Bandwidth : در کتاب ها و مباحث مخابراتی ، bandwidth به سرعت ارسال اطلاعات (Data Rate) اطلاق می شود ، اما در شبکه های کامپیوتری ، به پهنای یک کانال RF (Radio Frequency) ، پهنای باند یا bandwidth گفته می شود . در جدول زیر ، محدوده های فرکانسی را به اختصار مشاهده می فرمایید .



The Entire Electromagnetic Radio Spectrum										
ELF	SLF	ULF	VLF	LF	MF	HF	VHF	UHF	SHF	EHF
3 Hz 30 Hz	30 Hz 300 Hz	300 Hz 3 kHz	3 kHz 30 kHz	30 kHz 300 kHz	300 kHz 3 MHz	3 MHz 30 MHz	30 MHz 300 MHz	300 MHz 3 GHz	3 GHz 30 GHz	30 GHz 300 GHz

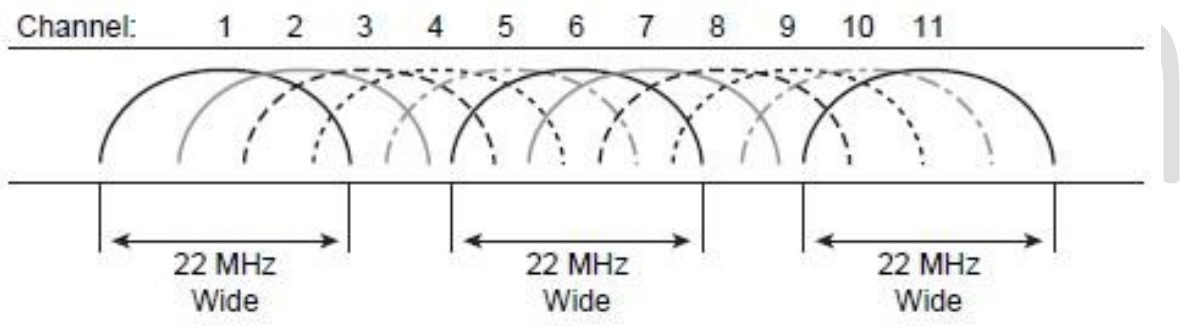
باندهای فرکانسی

900 MHz :

این باند فرکانسی در خیلی منازل کاربرد دارد و معروف ترین وسیله ای که از این فرکانس برای ارتباط استفاده می کند ، تلفن های بیسیم (Cordless Phone) است . البته مشکل اینجاست که اگر همسایه شما هم یکی از این تلفن ها داشته باشد ، در صورت استفاده ی همزمان ، تداخل رخ میدهد ؛ هرچند برخی از این تلفن ها ، کلیدی به نام Channel دارند که با زدن آن ، فرکانس را کمی جابجا می کنند تا تداخل را کم یا حذف کنند .

2.4 GHz :

این فرکانس ، شاید بیشترین استفاده را در WLAN ها داشته باشد . این range فرکانسی ، به ۱۱ کانال کوچکتر تقسیم می شود که هر کدام 22MHz پهنای باند دارند . البته چون این کانال ها با یکدیگر overlap دارند ، بیشتر از کانال های ۱ و ۶ و ۱۱ استفاده می شود که هیچ همپوشانی با هم ندارند ، لذا تداخل بین آنها به حداقل می رسد .



کانال های 2.4GHz توسط استانداردهای مختلف IEEE مثل ۸۰۲.۱۱ و نیز 802.11b/g/n مورد استفاده قرار می گیرند .

همچنین این محدوده ی 2.4GHz ، از مدولاسیون DSSS استفاده می کند .

data rate برای مدولاسیون DSSS در این محدوده فرکانسی ، مقادیر 1Mbps، 2Mbps ، 5.5Mbps ، و 11Mbps می باشد .

5 GHz :

تعداد ۲۳ کانال نامتداخل در این محدوده وجود دارد که توسط استانداردهای 802.11a/n مورد استفاده قرار می گیرند . این محدوده فرکانسی از OFDM استفاده می کند که دارای data rate های ۶ ، ۹ ، ۱۲ ، ۱۸ ، ۲۴ ، ۳۶ ، ۴۸ و 54 Mbps می باشد .

مدولاسیون ، تکنیک ها ، نحوه ی کار آنها :

مدولاسیون ، به معنای تغییرات روی یک سیگنال یا روی آهنگ تغییر (tone) آن سیگنال ، به نام carrier signal می باشد ؛ سپس داده ها طی فرآیندی به نام encoding ، به این سیگنال carrier اضافه می شود . مثلا هنگامی که آهنگی را با صدای بلند می خوانید ، در واقع دارید متن نوشته شده ای را به شکل موج صدا encode می کنید ، سپس تارهای صوتی حنجره شما آن را مدوله می کند تا صدا هر چه بلندتر و رساتر شود و مسافت بیشتری را بپیماید (و همسایه ها را شاکی تر کند) .

نکته اضافی : توجه کنید که صدا ، موج الکترومغناطیسی نیست ، بلکه فشار آکوستیکی است که در واقع فشار هوای فیزیکی متراکم و متغیر آن را بوجود می آورد.

شبکه های وایرلس ، از مدولاسیون به عنوان یک سیگنال carrier استفاده می کنند . در ادامه ، سه نوع مدولاسیون که بیشتر مورد استفاده قرار می گیرند را کمی بیشتر توضیح می دهیم :

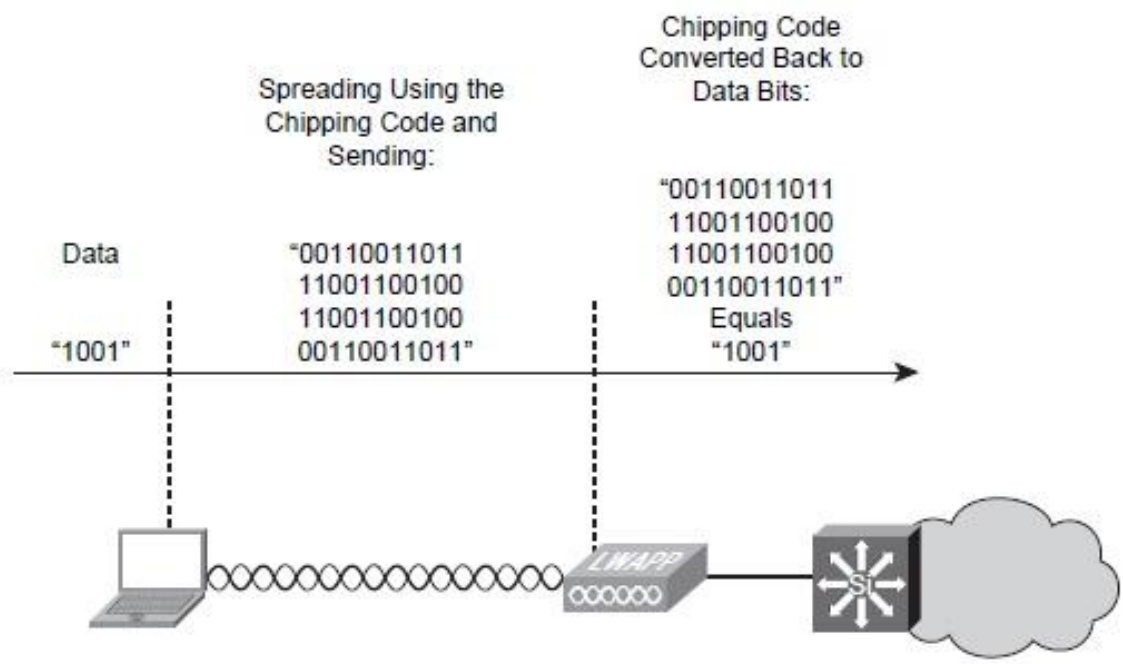
DSSS :

در Direct Sequence Spread Spectrum ، سیگنال ارسالی در تمام طیف فرکانسی مورد استفاده پخش می شود . مثلا اگر AP روی کانال ۱ سیگنال های خود را ارسال کند ، سیگنال carrier روی تمام کانال 22MHz پخش می شود (یعنی از محدوده ی ۲.۴۰۱ تا ۲.۴۲۳ GHz). برای encode کردن دیتا با استفاده از DSSS ، باید از یک chip sequence استفاده کنید .

برای درک چگونگی encode شدن و سپس مدوله دیتا در یک شبکه ی وایرلس ، باید ابتدا مفهوم چند نوع کد را بدانید .

Chipping Code :

همانطورکه قبلا گفتیم ، به هر کدام از اجزای پیام ، یک bit می گوییم ؛ و هنگامیکه این پیام روی carrier مورد نظر encode شد ، به آن chip می گوییم . فرض کنید که یک bit برای با ۱۰ تا chip درون یک chip stream باشد ؛ اگر در طول مسیر interference رخ دهد و یک یا چند chip از chip stream تغییر کند ، باز هم گیرنده می تواند bit اصلی را پیدا کند (مگر اینکه حداقل ۵ تا از این chip ها تغییر کند که در اینصورت stream کاملا عوض می شود و bit اشتباهی را نتیجه می دهد ، لذا نمی توان bit اولیه را بازسازی کرد). در مثالی کامل تر ، به این شکل توجه فرمایید :



فرض کنید می خواهیم دیتا ی ۱۰۰۱ را ارسال کنیم . بر اساس chiping code فرضی ، هر ۱ را با ۰۰۱۱۰۰۱۱۰۱۱ کد می کنیم و هر ۰ را با ۱۱۰۰۱۱۰۰۱۰۰ کد می نماییم . لذا داریم :

00110011011	11001100100	11001100100	00110011011
1	0	0	1

پس از اینکه کد بالایی ارسال شد ، در گیرنده به راحتی دوباره decode می شود و دیتا ی اصلی ، یعنی ۱۰۰۱ به دست می آید.

استفاده از chip sequence باعث می شود شبکه های ۸۰۲.۱۱ در برابر تداخل ها مقاوم تر باشند . همچنین همانطور که می بینید ، به ازای ۴ بیت دیتا ، ۴۰ بیت chipping code ارسال می شود ، لذا chipping rate از data rate خیلی بیشتر است .

Barker Code :

برای رسیدن به سرعت های 1Mbps و 2Mbps ، استاندارد ۸۰۲.۱۱ از کد بارکر استفاده می کند . در این روش ، هر بیت دیتا درون یک کد بارکر ۱۱ بیتی encode می شود و سپس بوسیله ی DSSS مدوله می گردد . البته این کد می تواند به سرعت های ۵.5 و 11Mbps نیز برسد .

Complementary Code Keying :

بر خلاف کد بارکر که تنها ۱ بیت را کد می کرد ، در این روش می توان تا ۶ بیت را بوسیله ی یک کلمه کد کرد ؛ لذا تنها برای سرعت های بالا مثل ۵.5 و 11Mbps مورد استفاده قرار می گیرد .

حال که دیتا را کد کردیم ، موقع آنست که ارسال شود ، یا اینکه روی آنتن رادیویی مدوله شود .

هرچند تکرار مکررات است ، اما توجه داشته باشید :

Encoding یعنی اینکه چگونه تغییرات در سیگنال **RF** به صفر و یک ها تبدیل می شود .

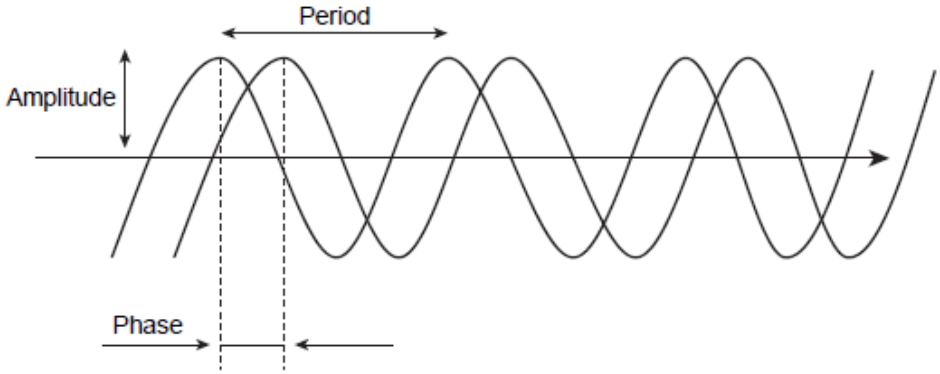
Modulation ویژگی های یک سیگنال **RF** است که تنظیم و دستکاری شده است .

در جدول زیر ، متدهای مختلف encode و modulation برای 802.11b نشان داده شده است .

Data Rate	Encoding	Modulation
1	11 chip Barker coding	DSSS Binary Phase Shift Keying
2	11 chip Barker coding	DSSS Quadrature Phase Shift Keying
5.5	8 chip encoding 8 bits CCK coding	DSSS Quadrature Phase Shift Keying
11	8 chip encoding 4 bits CCK coding	DSSS Quadrature Phase Shift Keying

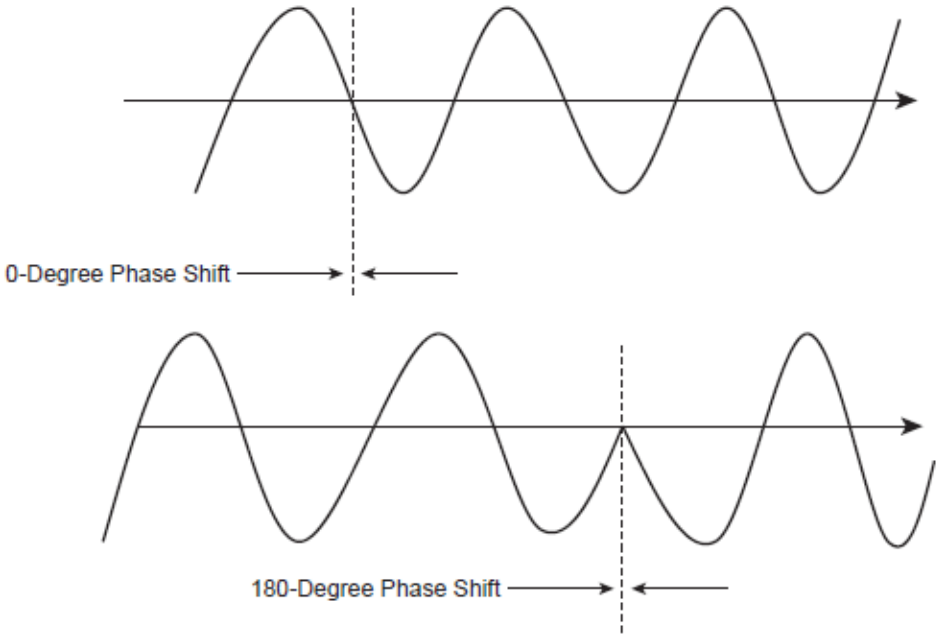
BPSK :

ابتدا با توجه به شکل زیر ، به تعریف چند عبارت مهم می پردازیم:



- ✓ **Phase** : زمان بین دوتا پیک یک سیگنال را فاز می گویند . لذا با توجه به شکل ، با اندازه گیری دو قله (یا دره) یک سیگنال متغیر ، میتوان فاز آن را اندازه گرفت . همچنین می توان گفت که فاز ، تفاوت بین دو موج ،در یک فرکانس است .
- ✓ **In-phase / Out-of-phase** : اگر اختلاف فاز دو سیگنال صفر درجه باشد ، به آنها in-phase می گویند ؛ در غیر اینصورت به آن Out-of-phase میگویند .
- ✓ **PSK** : phase shift keying نشان دهنده ی اطلاعات ، با تغییر فاز سیگنال است . یعنی مثلا به ازای کد ۰۰ ، سیگنال را ۹۰ درجه می چرخاند (تغییر فاز می دهد) ، به ازای کد ۰۱ ، آن را ۱۸۰ درجه می چرخاند و به ازای ۱۰ و ۱۱ نیز به ترتیب ۲۷۰ و ۳۶۰ درجه در سیگنال تغییر فاز ایجاد می کند .

حال می توان BPSK را تعریف کرد . BPSK در واقع یک روش ساده تر PSK است که تنها دو فاز با اختلاف ۱۸۰ درجه ایجاد می کند و برای هر سمبل ، یک بیت را مدوله می کند . در شکل زیر اختلاف فاز ۰ و ۱۸۰ درجه را می بینیم :



QPSK :

Quadrature Phase-Shift Keying برای سرعت های پایین ، قابلیت encode کردن ۲ بیت به ازای هر سمبل را دارد که این باعث دوبرابر شدن data rate در مقایسه با BPSK می شود ، در حالیکه هر دو از یک مقدار پهنای باند استفاده می کنند .

OFDM :

Orthogonal Frequency Division Multiplexing از چندین کانال 20MHz تشکیل شده که هر کانال ، خود به ۵۲ عدد subcarrier تقسیم می شود (که هر کدام 300KHz پهنای باند دارند). دیتا بصورت همزمان (simultaneously) روی همه ی subcarrier ها ارسال می شود (بصورت parallel) که این باعث سرعت بسیار بالای ارسال دیتا در OFDM می گردد .

MIMO :

Multiple-Input Multiple-Output تکنولوژی مورد استفاده در استاندارد نسبتا جدید 802.11n است . یک device که از MIMO استفاده می کند ، از چندین آنتن برای دریافت اطلاعات استفاده می کند (معمولا دو یا سه تا) ، و همچنین چندین آنتن برای ارسال اطلاعات لازم دارد . تکنولوژی MIMO می تواند data rate بالاتر از 100Mbps را با multiples کردن رشته های دیتا (بصورت همزمان) روی یک کانال فراهم آورد .

با استفاده از تکنولوژی MIMO ، یک AP می تواند با یک device که قابلیت استفاده از این تکنولوژی را ندارد نیز ارتباط برقرار کند ، و باز هم حدود ۳۰ درصد در عملکرد و کارایی شبکه های استاندارد 802.11a/b/g افزایش ایجاد می شود .

CSMA/CA :

قبلا گفتیم در یک شبکه ی وایرلس ، رفتار یک AP شبیه رفتار یک Hub است ! مشکل شبکه های وایرلس اینست که نمیتوان تشخیص داد که چه زمانی collision رخ می دهد . اگر در یک شبکه ی سیمی باشید ، با گوش کردن به خط ، یک jam signal شنیده می شود . اما در شبکه ی وایرلس ، حتی اگر همه ی دستگاهها دو آنتن داشته باشند ، اما چون یک آنتن نمی تواند هم ارسال و هم دریافت داشته باشد ، لذا jam signal شنیده نخواهد شد .

Collision avoidance ، یعنی اینکه دستگاهی که قصد ارسال دارد ، ابتدا گوش می دهد تا ببیند که خط اشغال نباشد ، سپس پیامی را روی خط می فرستد تا به بقیه اعلام کند که قصد ارسال دیتا را دارد . سپس برای یک پریود زمانی random صبر می کند تا اینکه بالاخره ارسال خود را انجام می دهد .

روش دیگر اینست که فرستنده از Ready To Send (RTS) و گیرنده از Clear To Send (CTS) استفاده کند ، این روش به بقیه ی دستگاهها اعلام می کند که برای مدت مشخصی نباید چیزی ارسال کنند .

استانداردها و تشکیلات قانون گذاری :

بواسطه ی وجود کمیته های تنظیم کننده شرایط و قوانین دستگاهها و شبکه های وایرلس در هر تکنولوژی ، می توانیم مطمئن باشیم که در هر شرایطی امکان برقراری ارتباط مناسب و بدون اشکالی وجود دارد .

در اینجا سه سازمان بزرگ و معروف را بطور خلاصه معرفی خواهیم کرد .

FCC :

Federal Communications Commission یک ارگان کاملا مستقل ، در ایالات متحده امریکا است که به تنظیم قوانین و روش های ارتباطی می پردازد . در مورد ارتباط FCC و Cisco Wireless ، باید پیش نیازهای تعریف شده در بخش پانزده FCC ، یعنی Antenna Requirements را بدانیم . این قوانین می گوید که یک آنتن باید از یک **connector** یکتا و غیر معمول (غیر رایج) استفاده کنند که به راحتی در دسترس نباشند ، تا مصرف کنندگان خانگی یا غیر معتبر نتوانند به راحتی با استفاده از این آنتن ها ، قوانین فدرال را زیر پا بگذارند . به همین علت ، سیسکو از کانکتوری به نام RP-TNC استفاده می کند (Reverse-Polarity-Threaded Neil-Concelman).

چیزی که این کانکتور را یکتا می سازد آنست که ارتباط مرکزی معکوس شده ، لذا شما نمی توانید یک آنتن معمولی را از مغازه ای خریداری نموده و به یک دستگاه وایرلس سیسکو وصل کنید .

ETSI :

European Telecommunication Standards Institue سازمانیست که وظیفه ی استاندارد سازی فرکانس ها و توان ارسالی دستگاهها را در اروپا و خیلی کشور های دیگر جهان به عهده دارد .

IEEE :

Institute of Electrical and Electronics Engineers را تقریبا همه می شناسند . بخش Wireless Standard Zone این ارگان ، استانداردهای مربوط به تکنولوژی وایرلس را تعریف کرده است . مثلا در ارتباط با پروتکل های ۸۰۲ ، موارد زیر بطور کامل شرح و بسط داده شده اند :

- ۸۰۲.۱۱ که در Wireless LAN مورد استفاده قرار می گیرد .
- ۸۰۲.۱۵ که در Wireless PAN مورد استفاده قرار می گیرد .
- ۸۰۲.۱۶ که با استانداردهای Broadband Wireless Access فعالیت می کند .

فصل سوم : آشنایی با اصول WLAN Radio Frequency

- مفاهیم و تعاریف
- مدل ها و پارامترهای محیط
  - ✓ مدل Free Path Loss
  - ✓ جذب – Absorption
  - ✓ انعکاس – Reflection
  - ✓ چند مسیری – Multipath
  - ✓ پراکندگی – Scattering
  - ✓ شکست – Refraction
  - ✓ مسیر دید – LoS
  - ✓ تفرق – Diffraction
- Freznel Zone
- RSSI
- SNR
- Link Budget

در این فصل به مفاهیم واقعی و مشکلات موجود در شبکه های وایرلس می پردازیم که اغلب آنها به واسطه ی واسط مورد استفاده (یعنی هوا) و نیز محیط اطراف ما بوجود می آیند .

مفاهیم و تعاریف :

Wavelength : طول موج ، فاصله ی بین دو قله ی متوالی یک موج (سیگنال) می باشد . فرستنده ای که درون AP قرار دارد ، یک موج به شکل یک سیگنال AC تولید می کند ، سپس این موج را به آنتن می فرستد تا از آنجا به شکل یک موج سینوسی در فضا تشعشع یابد . برخی از ویژگی های شکل موج به این ترتیب است :

- شکل موج رادیویی AM بین ۴۰۰ تا ۵۰۰ متر طول دارد .
- امواجی که در Wireless LAN ها فعالیت می کنند ، تنها چند سانتی متر طول دارند .
- موجی که توسط ماهواره ارسال می شود ، تقریبا ۱ میلی متر طول دارد .

Frequency : در مورد فرکانس در فصل قبل توضیح داده شد ؛ لذا در اینجا برخی از ویژگی های فرکانس را بیان کنیم :

- ۱ سیکل برابر است با ۱ هرتز .
- فرکانس های بالاتر ، مسافت های کوتاهتری را می پیمایند .
- اگر یک شکل موج ، در یک ثانیه ، تنها 1 بار دیده شد ، فرکانس آن موج 1Hz است .
- اگر یک شکل موج ، در یک ثانیه ، ۱۰ بار دیده شد ، فرکانس آن موج 10Hz است .
- اگر یک شکل موج ، در یک ثانیه ، 1.000.000 بار دیده شد ، فرکانس آن موج 1MHz است .
- اگر یک شکل موج ، در یک ثانیه ، 1.000.000.000 بار دیده شد ، فرکانس آن موج 1GHz است .

Amplitude : مقدار یا اندازه ی انرژی که به سیگنال داده می شود را دامنه سیگنال می گویند . در واقع این amplitude است که به موج اجازه می دهد که مسافتی را طی کند و دورتر برود . مثلا ما هرچه بلندتر حرف بزنیم ، انرژی بیشتری در سیگنال صدا قرار دارد ، پس دامنه بلندتری دارد .

EIRP : هنگانی که AP سیگنال را به آنتن می دهد ، کابلی که بین این دو قرار دارد ، مقداری از توان را تلف می کند . مقدار gain که ما استفاده میکنیم ، بستگی به نوع آنتن دارد . Effective Isotropic Radiated Power برابرست با :

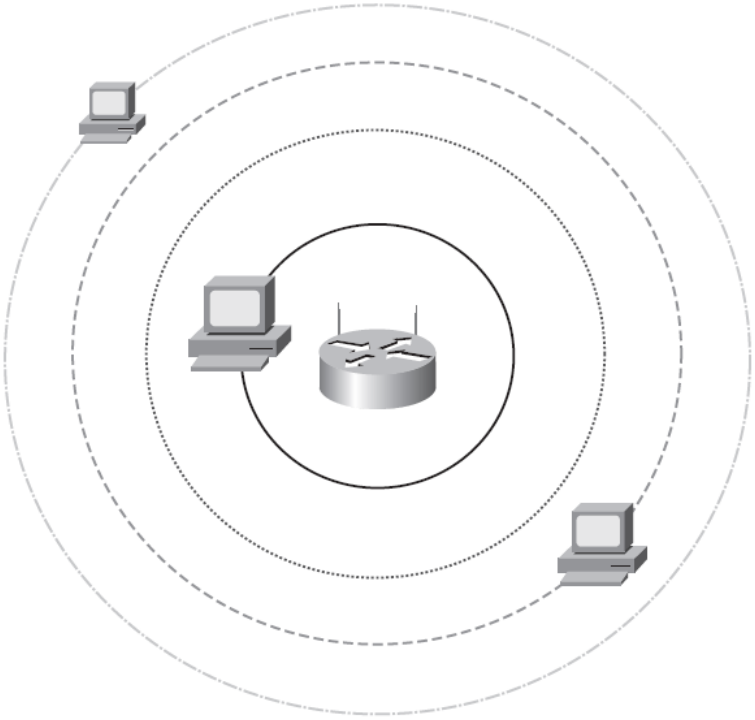
$$EIRP = transmitter\ output\ power - cable\ loss + antenna\ gain$$

مدل ها و پارامترهای محیط :

مدل Free Path Loss :

هنگامی که سنگی را درون برکه ای می اندازید ، می بینید که امواج آب شکل می گیرند و به تدریج بزرگتر و بزرگتر می شوند و با بزرگتر شدن ، ضعیف تر نیز می گردند ؛ تا زمانیکه دیگر موجی باقی نمی ماند . مثل همین کار را یک منبع مولد سیگنال می تواند انجام دهد (یک AP یا ...) .

در مدل مسیر بدون اتلاف ، هیچ چیزی وجود ندارد که موج را نگه دارد ، بلکه موج به واسطه ی تشعشع خود به تدریج ضعیف شده تا در نهایت به طور کامل از بین می رود .



در این شکل ، برای محاسبه ی محدوده ی قابل پوشش ، باید انرژی تلف شده و نیز فاصله دستگاهها را در نظر بگیریم ، زیرا هرچه از منبع سیگنال دورتر می شویم ، سیگنال دریافتی ضعیف تر می گردد .

جذب (Absorption) :

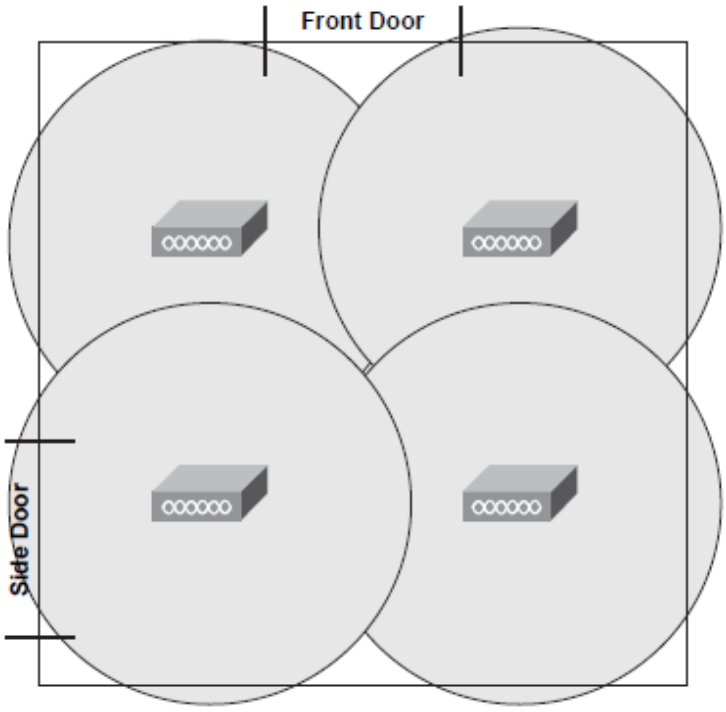
جذب ، فاکتوری است که با کاهش دادن دامنه (amplitude)ی یک سیگنال ، روی ارتباط وایرلس شما تاثیر می گذارد .

یکی از تاثیرات absorption ، ایجاد گرما است . هنگامی که چیزی یک موج را جذب می کند ، گرم می شود ! مثل این مورد را حتما در اجاق های Microwave مشاهده کرده اید (دستگاههایی که امواجی را تولید می کنند که بوسیله مواد غذایی جذب می شوند و باعث گرم شدن آنها می شود) .

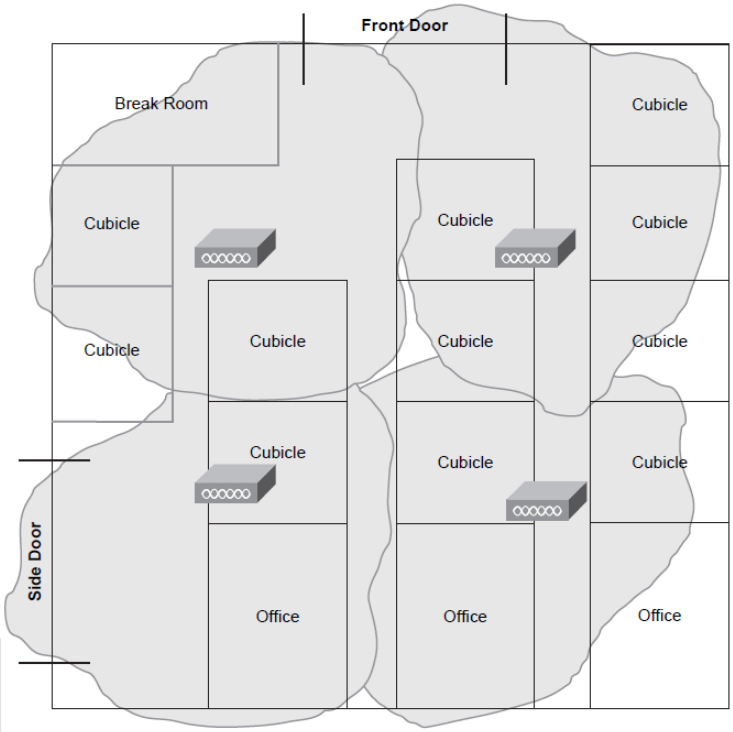
اخطار : شما می توانید یک فنجان نسکافه در دستگاه مایکروویو بگذارید و پس از مدتی می بینید که نسکافه ی شما جوش می آید ، اما فنجان شما کاملا سرد است ! علت این مسئله اینست که مایعات و مواد نرم خیلی سریع این امواج را جذب می کنند ، حال می تواند یک فنجان hot choclate باشد ، یک تکه کیک عسلی باشد ، یا اینکه مغز شما باشد !!! لذا هنگام استفاده از چنین دستگاههایی باید مطمئن شوید که محدوده ی انرژی دهی امواج ، کنترل شده و استاندارد هستند (با خریدن دستگاههای مناسب ، یا ترجیحا نخریدن آنها) . بخصوص در مورد کودکان (به دلیل روان تر بودن مایع مغزی آنها) این خطر دوچندان است و می تواند موجب ضایعات شدید مغزی در آینده شود . (زیرا بسان گرم کردن مواد غذایی ، در صورت استفاده طولانی مدت از امواج مایکروویو ، می تواند سلولهای بخشی از مغز را نیز سوزانده و نابود کند ، لذا آن بخش از مغز را از کار می اندازد که این خود موجب انواع سندرم ها ، فلج ها ، یا بیماری هایی چون آلزایمر و MS می گردد .)

مشکل اساسی در absorption اینجاست که اگر یک موج بطور کامل جذب شود ، دیگر متوقف می شود . البته این مسئله تنها فاصله ی تحت پوشش را کاهش می دهد ، و روی طول موج و فرکانس آن تاثیری ندارد .

در یک مثال ، فرض بفرمایید که می خواهید در اداره ای سرویس وایرلس راه اندازی کنید . در ابتدا که یک فضای خالی دارید ، با استفاده از datasheet هر AP مورد استفاده ، به راحتی می توانید اطلاعات لازم (شامل محدوده ی تحت پوشش ، تعداد کاربران ، نوع سرویس مورد نیاز و ...) را تکمیل نموده و تجهیزات شبکه را پیاده سازی نمایید :

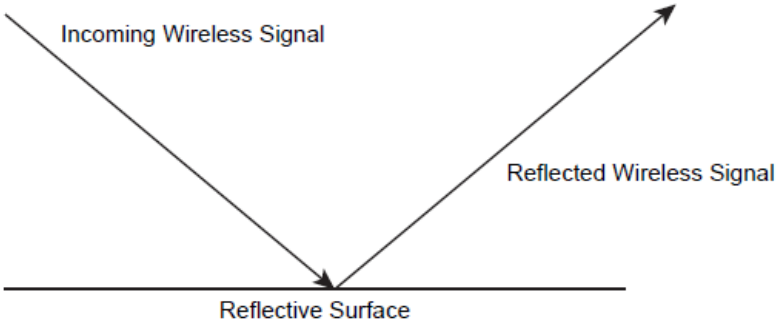


اما پس از پارتیشن بندی محیط اداره و قرار گرفتن افراد و اشیاء مختلف در محیط ، می بینید که شبکه ی شما در برخی نقاط throughput لازم را ندارد و حتی برخی کاربران از عدم اتصال به شبکه شکایت دارند ، که مهمترین علت ، جذب و تلف شدن بخشی از سیگنال های شما در محیط است :



انعکاس (Reflection) :

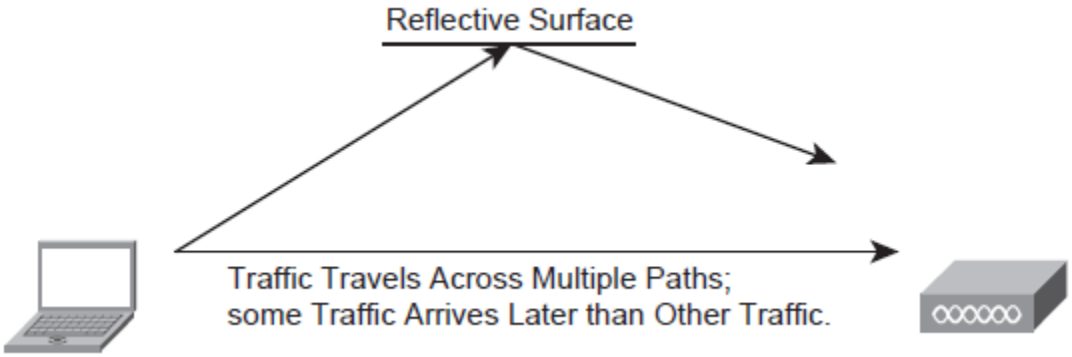
هرچند جذب باعث تضعیف سیگنال می گردد ، اما تنها عامل تضعیف نیست . انعکاس باعث می شود مسیر سیگنال عوض شده ، در یک راستای دیگر حرکت کند . همانطور که یک شعاع نور در آینه منعکس می شود ، امواج نیز توسط برخی اشیاء انعکاس پیدا می کنند . (البته در محیط های اداری شاید آینه کمتر پیدا شود ، اما اجسامی مثل مانیتور ها یا قاب های طراحی از جنس شیشه به وفور یافت می شوند.)



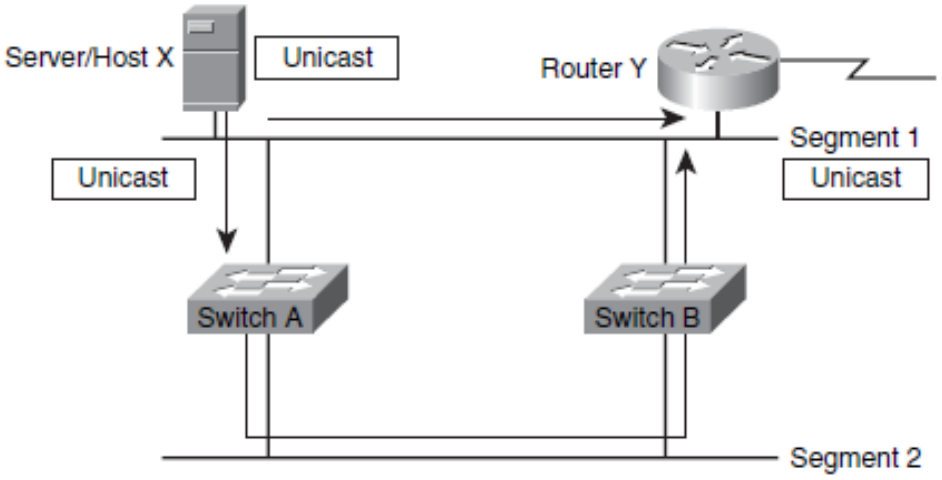
انعکاس به فرکانس بستگی دارد و اشیایی که برخی فرکانس ها را منعکس می کنند ، ممکن است برخی فرکانس های دیگر را منعکس ننمایند ؛ لذا می توان از فرکانس هایی استفاده کرد که کمتر توسط اشیاء عادی منعکس شوند .

چند مسیری (Multipath) :

پدیده ی چند مسیری هنگامی اتفاق می افتد که بخشی از سیگنال هایی که منعکس شده اند ، بصورت نا مرتب به گیرنده برسند . لذا ممکن است که گیرنده یک سیگنال را چندین بار دریافت کند . همچنین این امر می تواند سیگنال را غیر هم فاز کند (out-of-phase) ، لذا این سیگنال ها می توانند یکدیگر را خنثی کنند و یک null signal را نتیجه دهند .

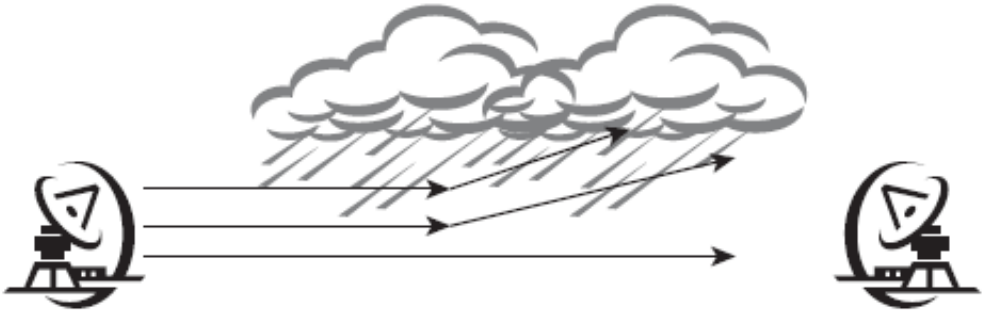


شاید بتوان گفت که این پدیده ، چیزی شبیه Multiple Frame Transmission در شبکه های LAN است که در آن ، روتر یک پکت را چندین بار از منابع مختلف دریافت می کند و در نتیجه جدول آدرس های MAC آن روتر دچار مشکل می شود .



پراکندگی (scattering) :

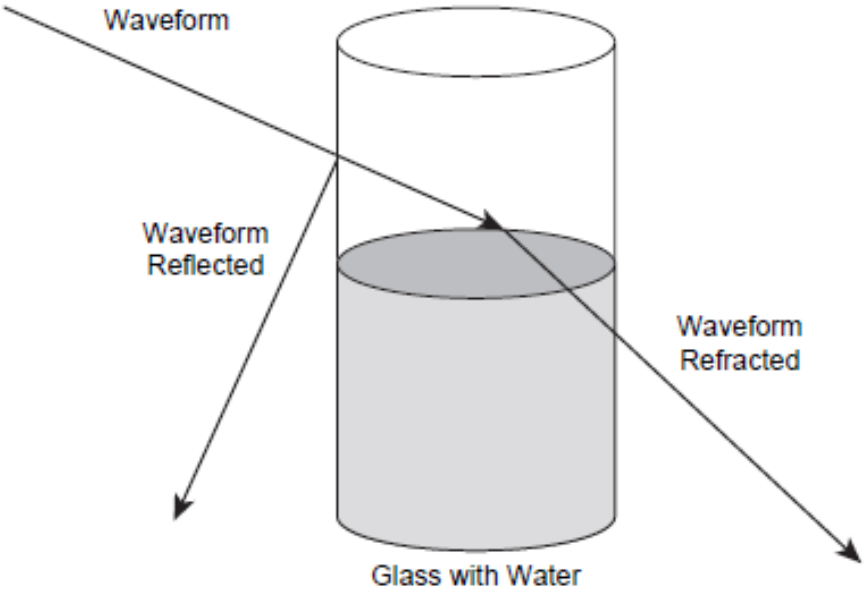
برخی اجسام که لبه های تیز دارند و نیز ذرات مختلف منعکس کننده دارند ، موجب می شوند که امواج به جهت های مختلف منحرف شوند که به این پدیده ، پراکندگی می گویند . مثل زمانی که یک شعاع نور به قطعه ای از بلور یک لوستر برخورد می کند و به جهات مختلف منعکس می شود . در محیط طبیعی ، ذرات آب ، بخار ، و یا گرد و خاک می توانند باعث پراکندگی سیگنال ها شوند و به همین علت شرایط بد جوی می تواند روی ارتباطات وایرلس تاثیر منفی بگذارد .



پراکندگی بیشتر روی طول موج های کوتاه اثر می گذارد و وابسته به فرکانس سیگنال است .

شکست (Refraction) :

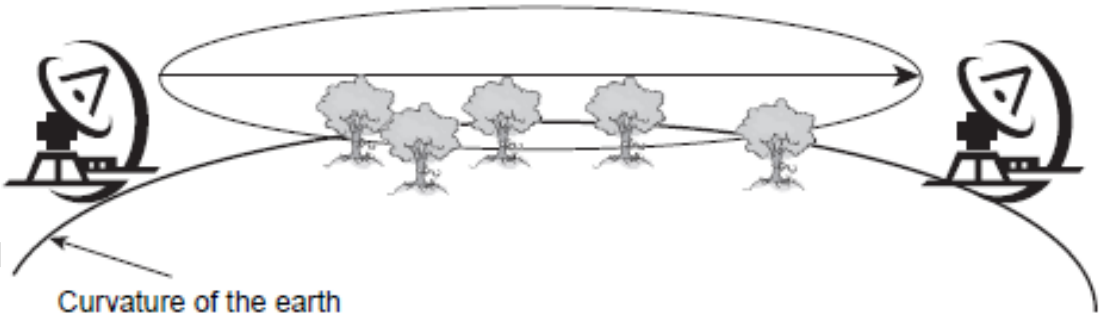
شکست به معنای تغییر در راستا یا انحراف مسیر موج است ، هنگامی که سیگنال از یک محیط با یک چگالی خاص ، وارد محیطی با چگالی دیگر می شود . بهترین مثال ، شکست نور در عبور از یک لیوان آب است ، یا در عبور از آب استخر ، لذا ما کف استخر را خیلی نزدیک می بینیم . همچنین در استخرهایی که در زیر آب موزیک پخش می شود ، اما در بیرون از آب هیچ صدایی شنیده نمی شود ، از همین ویژگی کمک می گیرند .



مسیر دید (Line Of Sight) :

در ارتباطات نزدیک ، می توان کاری کرد که فرستنده و گیرنده روبروی هم قرار گیرند و مانعی بین آنها نباشد (در اصطلاح می گوییم فرستنده و گیرنده همدیگر را ببینند) .

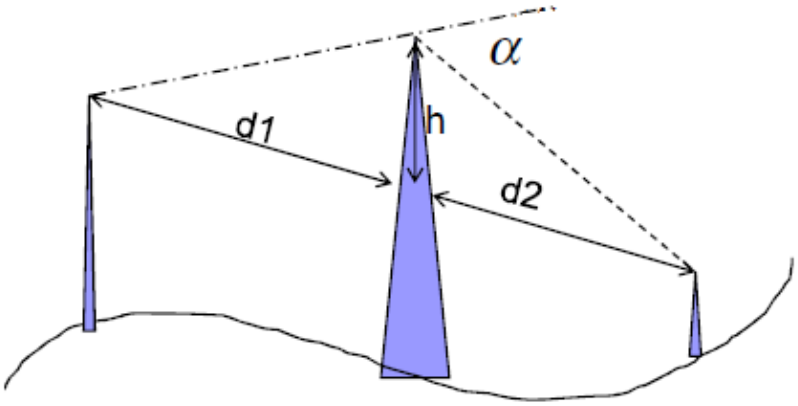
اما در فواصل دور ، علاوه بر وجود موانع طبیعی که از سر راه برداشتن آنها غیر ممکن است (مثل درختان ، کوه ها و ...) ، انحنای کره ی زمین خود به عنوان یک مانع عمل می کند .



تفرق (Diffraction) :

تفرق جزء مواردیست که هم ضرر دارد ، و هم سود ! فرض کنید که سیگنال ها قرار بود فقط به خط مستقیم حرکت کنند ، آنوقت دیگر اگر کسی پشت دیوار می ایستاد ، نمی توانست سیگنال هایی که از یک آنتن بالای دیوار می آید را دریافت کند .

تفرق عاملی است که اجازه می دهد سیگنال های رادیویی در اطراف زمین یا در پشت موانع منتشر شوند . لذا در شکل زیر ، آنتن سمت راست با اینکه پشت یک مانع قرار دارد ، اما باز هم می تواند سیگنال های آنتن سمت چپ را دریافت نماید .



به این مدل ، Knife Edge model (مدل لبه ی چاقو) گفته می شود .

Fresnel Zone :

در شکل قبل ، محدودیت هایی برای فواصل بین آنتن ها و نیز بین هر آنتن و مانع ، و همچنین برای ارتفاع هر کدام وجود دارد . لذا پارامتری تعریف می کنیم به نام fresnel که فرمول محاسبه ی آن به این ترتیب است :

$$v = h\sqrt{\frac{2(d_1+d_2)}{\lambda d_1 d_2}} = \alpha\sqrt{\frac{2d_1 d_2}{\lambda(d_1+d_2)}}$$

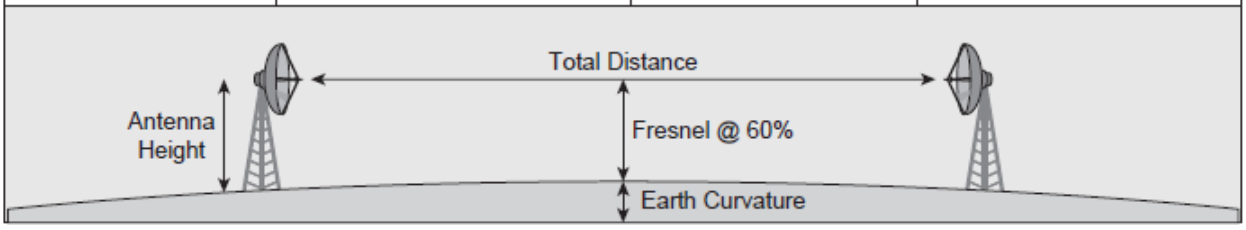
Fresnel Zone میگوید که هنگامی که دو آنتن از فاصله ی خاصی از یکدیگر قرار داشته و باهم در ارتباط باشند ، به خاطر انهنای زمین ، باید حداقل ارتفاع H را داشته باشند که این ارتفاع از این فرمول بدست می آید :

H = F + C

در این فرمول F برابر با 60 درصد مقدار Fresnel-Zone است و C هم پارامتر انحنای زمین است .

در جدول زیر ، مقادیر لازم برای پارامتر های مختلف فرمول بالا داده شده است .

2.4 GHz Systems			
Wireless Link-Distance in Miles	Approximate Value "F" (60% Fresnal Zone at 2.4 GHz)	Approximate Value "C" Earth Curvature	Value "H" Antenna Mounting Height with No Obstructions
1	14	3	17
5	31	5	36
10	43	13	56
15	53	28	81
20	61	50	111
25	68	78	146
5 GHz Systems			
1	9	3	12
5	20	5	25
10	28	13	41
15	35	28	63
20	40	50	90
25	45	78	123



توجه : در این شکل ، چنانچه در حالت بدبینانه ، انحنای زمین را خیلی زیاد فرض کنیم (یا مانعی مثل تپه در بین دو آنتن قرار دهیم) ، می توان به شکل قبل (مدل لبه چاقو) رسید .

توجه : سیگنال های Indoor ، کوچکتر از آن هستند که تحت تاثیر این امر قرار گیرند .

RSSI :

Received Signal Strength Indicator نشان دهنده ی اینست که چقدر سیگنال دریافت شده است . RSSI برای هر محصول (vendor) ، بصورت جداگانه و با دستگاههای خاص خودشان اندازه گیری می شود ، لذا scale های مختلفی دارند و در نتیجه نمی توان آنها را با یکدیگر مقایسه کرد (مثلا برخی از ۰ تا ۱۰۰ ، و برخی دیگر از ۰ تا ۶۰ تقسیم بندی می شوند) .
یکی از دستگاههای محاسبه ی RSSI در شبکه های وایرلس ، **Network Stumbler** نام دارد .

نسبت سیگنال به نویز (SNR) :

Signal-to-Noise Ratio عبارتیست برای بیان میزان قدرت سیگنال نسبت به نویزی که سیگنال را خراب و تضعیف می کند. فرض کنید در یک پارک ، مشغول صحبت کردن با دوست خود از طریق موبایل هستید ، در حالیکه کودکان زیادی آنجا مشغول بازی و سر و صدا هستند . فردی که آنسوی خط تلفن است ، نمی تواند صدای شما را به خوبی بشنود ، چون صدای بقیه ی افراد و کودکان با صدای شما تداخل می کند . حال هر چه شما بلندتر حرف بزنید ، نسبت سیگنال اصلی به سیگنال های اضافی بیشتر می شود و دوست شما صدا را بهتر می شنود . یعنی SNR سیگنال دریافتی قوی تر و بیشتر می شود .

Link Budget :

بودجه ی یک لینک ، تمام gain ها و تلفات بین فرستنده و گیرنده را در نظر می گیرد ؛ که شامل تضعیف سیگنال ، gain آنتن ، و سایر تلفات مختلف است که ممکن است بوجود بیاید . این فاکتور ، از این نظر حائز اهمیت است که بدانیم برای ارسال یک سیگنال ، چقدر توان نیاز است تا گیرنده بتواند سیگنال مناسبی دریافت نماید .

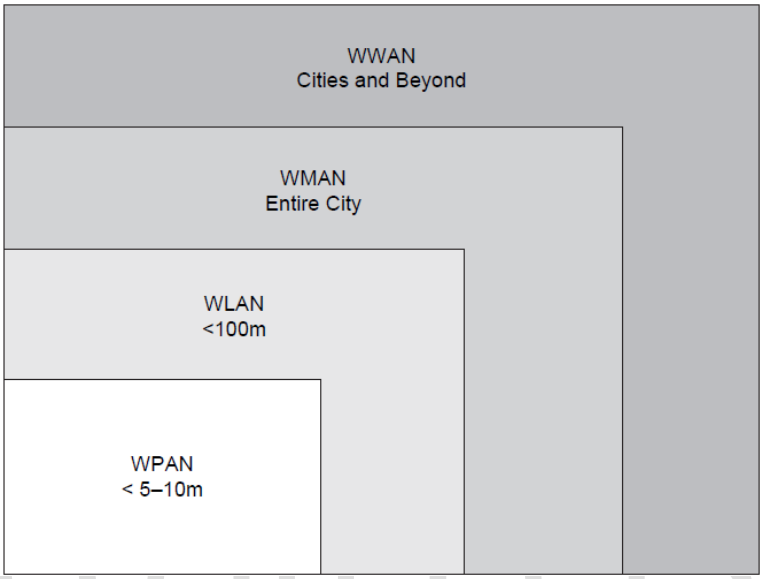
$$\text{Received Power (dBm)} = \text{Transmitted Power (dBm)} + \text{Gains (dB)} - \text{Losses (dB)}$$

فصل چهارم : آشنایی با تکنولوژی ها و توپولوژی های WLAN

- WPAN
- WLAN
- WMAN
- WWAN
- شبکه های Ad-Hoc
- ساختار شبکه
  - ✓ BSA
  - ✓ ESA
- Service Set Identifiers
- Workgroup Bridges
- Repeaters
- Outdoor Wireless Bridge
- Outdoor Mesh Networks

هنگامیکه با شبکه های وایرلس کار می کنید ، با تکنولوژی ها و توپولوژی های مختلف سر و کار دارید . بعضی مواقع نیاز به یک ارتباط peer-to-peer دارید ، و در برخی شرایط ، می خواهید بین کاربرانی که در اطاق های مختلف یک شرکت قرار دارند ، ارتباط برقرار کنید . در این فصل ، با انواع مختلف شبکه های وایرلس ، و تکنولوژی های مورد استفاده آنها آشنا خواهید شد .

در ابتدا ، چهار توپولوژی عام شبکه های وایرلس را به تشریح بیان خواهیم نمود .



WPAN :

شبکه ایست که برای فعالیت در محدوده ی ۲۰ فوتی طراحی شده است .معروف ترین WPAN که شاید همگی ما امروزه با آن سر و کار داریم ، بلوتوث است . نکته ی جالب اینجاست که بلوتوث در همان محدوده ی فرکانسی 802.11b و 802.11g فعالیت می کند ، اما به اندازه ی AP های دیگر در این محدوده ، تداخل (interference) ایجاد نمی کنند ؛ شاید توقع داشته باشید که با وجود تعداد زیادی هدفون های بلوتوثی یا موس ها و میکروفن های بلوتوثی ، تداخل زیادی بوجود بیاید ؛ اما حقیقت اینست که بلوتوث از FHSS استفاده می کند ، که باعث می شود تداخل تا حد زیادی از بین برود. (بحث Frequency Hopping Spread Spectrum فراتر از این کتاب است.) شبکه ی کوچک بلوتوث ، شامل ۸ دستگاه فعال می باشد ، اما می تواند تعداد زیادی دستگاه غیر فعال نیز داشته باشد . ویژگی های WPAN بطور خلاصه عبارتند از :

- ✓ محدوده ی آن کوتاه است – حدود ۲۰ فوت .
- ✓ تا ۸ دستگاه فعال می تواند داشته باشد .
- ✓ طیف فرکانسی آن 2.4GHz است .
- ✓ به آن piconet نیز گفته می شود (شبکه ی خیلی کوچک).

WLAN :

WLAN برای نواحی بزرگتر از WPAN طراحی شده است . در این شبکه ها ، می توان ترکیبی از AP های dual-band ، لپ تاپ ها و نیز desktop های مختلف را مشاهده نمود . WLAN از استاندارد های 802.11a/b,g,n استفاده می کنند. آنچه WLAN ها را انعطاف پذیر می سازد ، اینست که AP ها و client ها همگی dual-band هستند ؛ این امر استفاده از روش های ارتباطی مختلف در نواحی مختلف را آسان می کند و بیشتر client ها می توانند همچنان فعال باشند . برخی از ویژگی های WLAN به این ترتیب می باشند :

- ✓ استفاده از طیف فرکانسی 2.4GHz و یا 5GHz .
- ✓ محدوده ی وسیعتر نسبت به WPAN – حدود ۱۰۰ متر از AP تا client .
- ✓ برای رسیدن به فواصل دورتر ، توان خروجی بیشتری مورد نیاز است .
- ✓ WLAN ها بسیار انعطاف پذیر هستند ، لذا انتظار وجود بیش از ۸ دستگاه فعال (client) را داریم .

WMAN :

WMAN ها محدوده ی جغرافیایی وسیعی را پوشش می دهند و به عنوان سرویس های Backbone ، point-to-point ، یا حتی لینک های point-to-multipoint که می تواند جایگزین تکنولوژی هایی نظیر T1 و T3 شوند ، در نظر گرفته می شوند . باید توجه داشت که کاهش سرعت با افزایش مسافت ، امری عادی در WMAN است .
معروف ترین WMAN در دنیای امروز، WiMax است (802.16b) . WiMax می تواند به عنوان یک جایگزین برای سرویس های Broadband (مثل ارتباطات cable یا DSL) ، دسترسی last-mile را فراهم آورد .

نکته : **Last-mile** اصطلاحیست که در ارتباطات و صنایع تکنولوژی ، برای تعریف تکنولوژی ها و پروسه های مورد استفاده برای برقراری ارتباط بین مشترکین نهایی و شبکه های ارتباطی ، به کار می رود .

WWAN :

WWAN محدوده ی بسیار وسیعی را در بر می گیرد ، لذا برقراری این شبکه بسیار گران قیمت است . خدمات تلفنی که به شما ارائه می شود ، WWAN است و می تواند علاوه بر دسترسی به voice ، دسترسی به data را نیز به شما ارائه دهد . در این شبکه ها ، data rate معمولا حدود 115 kbps است (low data rate) . معروفترین تکنولوژی WWAN مورد استفاده ، GSM و CDMA می باشد ؛ هزینه های پرداختی برای دسترسی به صدا یا دیتا ، معمولا بر اساس میزان استفاده افراد از این سرویس هاست (pay for use) .

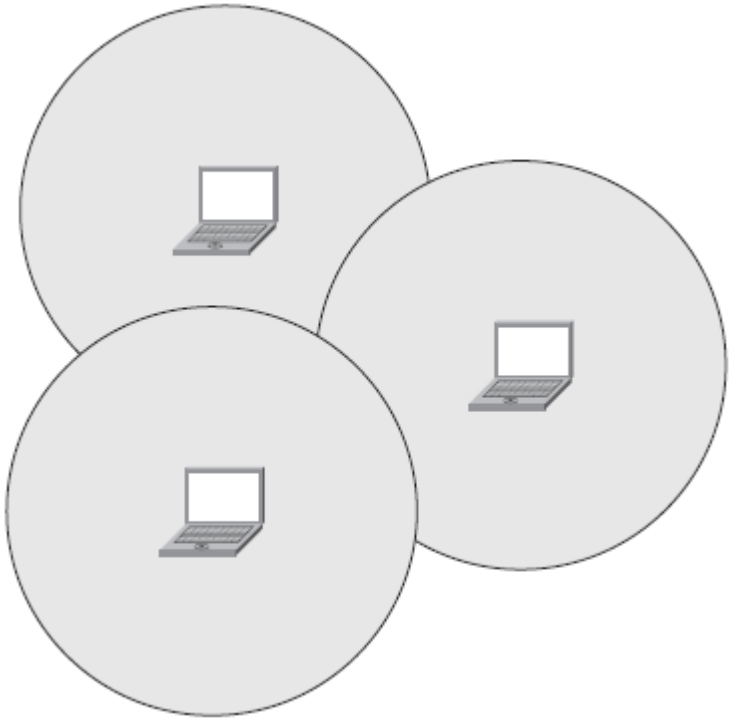
نکته : در WWAN می توان از فرکانس های unlicensed استفاده کرد ، اما این امر عمومیت ندارد ؛ چون ممکن است دیگران هم این کار را بکنند و موجب تداخل (interference) شود . لذا بهتر است فرکانس های licensed خریداری شود .

پس از بحثی کلی در مورد این چهار نوع شبکه ، در ادامه شما را با دو توپولوژی تعریف شده توسط 802.11 آشنا خواهیم کرد .

شبکه های Ad Hoc :

هنگامیکه دو کامپیوتر بصورت مستقیم با یکدیگر ارتباط برقرار می کنند ، یک شبکه ad hoc شکل گرفته است . شبکه های ad hoc برای برقرار ارتباط ، نیازی به یک دستگاه مرکزی ندارند ؛ در عوض ، یک دستگاه یک group name و radio parameter انتخاب کرده ، و دستگاه دیگر نیز از آنها برای برقراری ارتباط استفاده می کند .

- ✓ **Basic Service Set (BSS)** ناحیه ای تعریف می کند که در آن یک دستگاه ، قابل دسترسی است .
- ✓ **Independent Basic Service Set (IBSS)** به این معناست که دستگاهها برای برقراری ارتباط ، نیازی به یک دستگاه مرکزی (مثل AP) ندارند .



در این نوع طراحی ، هر کامپیوتر تنها از یک radio استفاده می کند ، لذا throughput پایین است و هر client به صورت یک دستگاه half-duplex عمل می کند ؛ زیرا نمی تواند در آن واحد هم ارسال و هم دریافت کند .

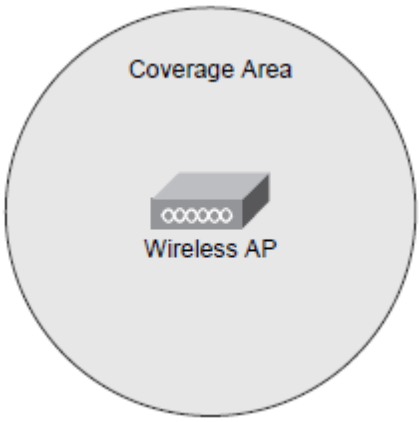
ساختار شبکه :

در شبکه های وایرلس ، AP به عنوان نقطه ی اتصال client ها در نظر گرفته می شود . می توان گفت یک AP ، در واقع چیزی بین Hub و bridge است ؛ زیرا :

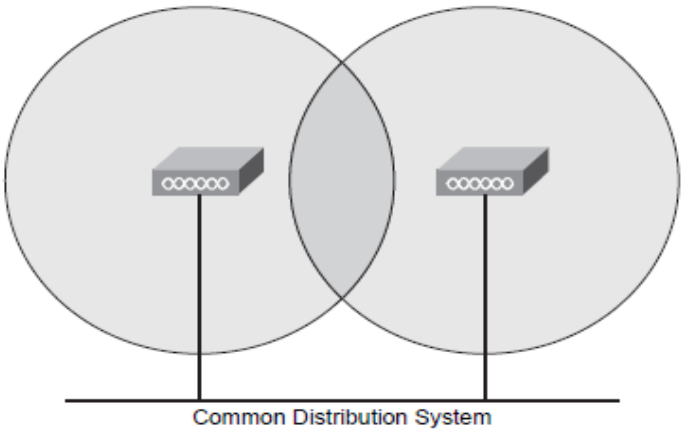
- ✓ از یک radio استفاده می کند ، لذا نمی تواند همزمان ارسال و دریافت داشته باشد (half-duplex است) .
- ✓ مانند bridge ، براساس آدرس MAC هر فریم ، تصمیم بر forward کردن آن فریم می گیرد .

تفاوت اساسی AP با bridge در اینست که فریم های وایرلس خیلی پیچیده تر از فریم های اترنت هستند . در فریم های اترنت ، دو تا آدرس MAC وجود دارد ، اما در فریم های وایرلس علاوه بر دو آدرس MAC مبدا و مقصد ، یک آدرس MAC مربوط به AP است که به workgroup وابسته است . چنانچه از workgroup bridge استفاده کرده باشید ، یک آدرس MAC هم می تواند آدرس next-hop باشد ؛ لذا در فریم وایرلس ، می توان ۳ تا ۴ آدرس MAC داشت . یک AP در واقع یک نوع wireless station است . اما چون این نام ممکن است شما را کمی گیج کند ، همیشه client ها را station می نامیم (STA) ، و AP را یک infrastructure device خواهیم نامید .

- ✓ **Basic Service Area (BSA)** : محدوده ی پوشش یک AP را BSA می گوییم .



- ✓ **Extended Service Area (ESA)** : چنانچه بیش از یک AP به یک سیستم توزیع متصل شوند ، ناحیه تحت پوشش را ESA می نامیم.



نکته : برخی AP ها می توانند بصورت یک repeater عمل کنند ، لذا نیازی به ارتباط Ethernet نخواهند داشت .

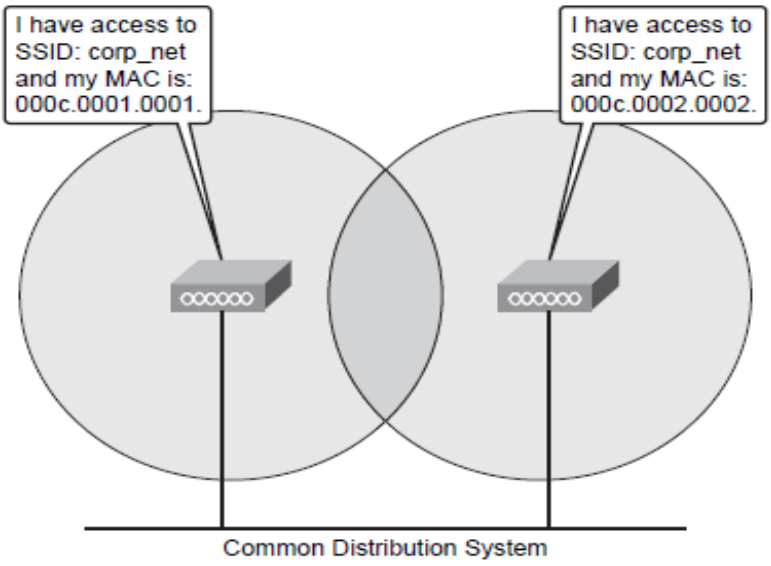
نکته : فرآیند جابجاییclient از یک AP به سمت AP دیگر را roaming می گویند . برای اینکه roaming ممکن باشد ، AP ها باید overlap داشته باشند .

Service Set Identifiers :

هنگامیکه وایرلس لپ تاپ خود را روشن می کنید ، یک popup مشاهده می کنید که: wireless networks are available یا چیزی شبیه این . هنگامی که به شبکه های موجود نگاه می کنید ، یک سری اسامی می بینید . در AP های قدیمی سیسکو ، نام **Tsunami** برای شبکه انتخاب می شد ؛ در مدل های Linksys ، معمولا همان نام **Linksys** انتخاب می شود .

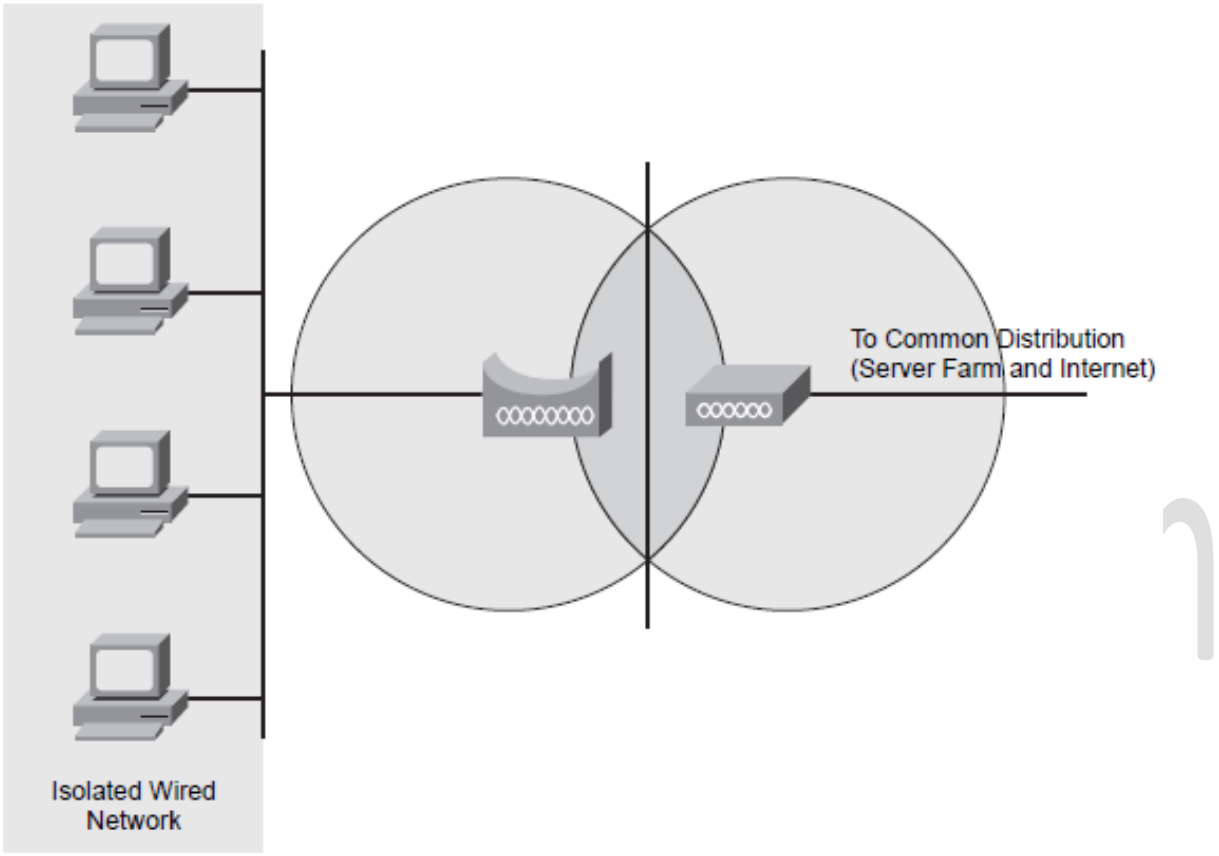
- ✓ **Service Set Identifier (SSID)** : این نام ، ترکیب آدرس MAC و نام شبکه است ؛ آدرس MAC می تواند آدرس wireless radio باشد ، یا هر MAC دیگری که AP تولید می کند .
- ✓ **Basic Service Set Identifier (BSSID)** : درصورتیکه AP فقط برای یک شبکه سرویس دهی کند ، نام آن را BSSID گویند .
- ✓ **Multiple Basic Service Set Identifier (MBSSID)** : اگر یک AP به جای یک نام ، چندین SSID داشته باشد ، در واقع چندین شبکه را سرویس دهی می کند ؛ client ها فکر می کنند که چندین AP وجود دارد (در واقع virtual AP داریم). در این حالت ، اگر user ها بطور همزمان ارسال کنند ، collision بوجود می آید ؛ زیرا در حقیقت یک سخت افزار و فرکانس برای این AP داریم .

در roaming ، علاوه بر اینکه BSA های AP ها باید overlap داشته باشند ، SSID های آنها نیز باید یکسان باشند ، هرچند آدرس MAC آنها متفاوت خواهد بود .



Workgroup Bridges :

در برخی شرایط ، ممکن است امکان کابل کشی در فواصل زیاد وجود نداشته باشد ، یا اینکه مالک ساختمان به شما اجازه ی سوراخ کردن دیوار و نصب داکت ها را ندهد . در چنین مواقعی شما می توانید از یک توپولوژی WGB مانند شکل زیر استفاده کنید :



توجه کنید که WGB برای پل زدن و برقراری ارتباط بین یک شبکه ی سیمی (wired) با یک AP که به یک سیستم توزیع متصل است ، به کار می رود .

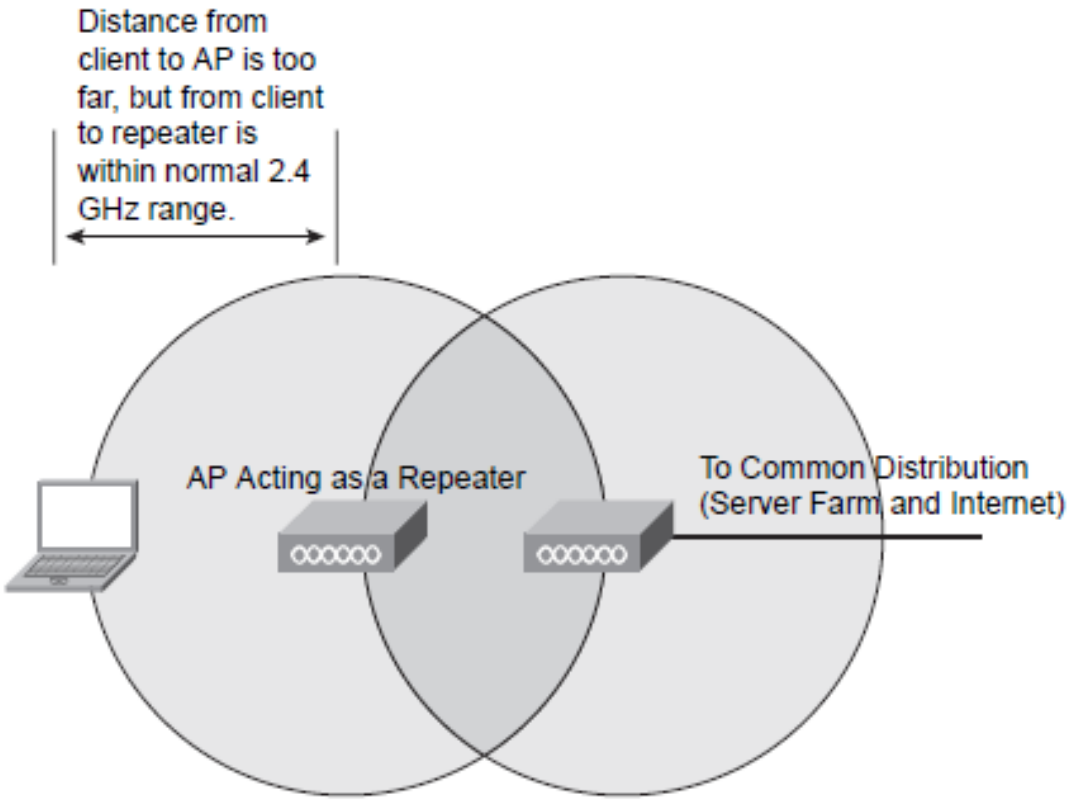
سیسکو دو نوع workgroup bridge را پیشنهاد می کند :

- ✓ **Autonomous Workgroup Bridge (aWGB)** : یک aWGB تنها به AP های سیسکویی upstream متصل می شود و هنگامیکه AP به aWGB نگاه می کند ، چندین Ethernet client می بیند .
- ✓ **Universal Workgroup Bridge (uWGB)** : یک uWGB امکان پل زدن به AP های غیر سیسکویی upstream را فراهم میکند ، و اگر AP به uWGB نگاه کند ، فقط یک single client را می بیند .

Repeaters :

در ESS ها ، برای توسعه ی پوشش شبکه ، نمی توان از WGB استفاده کرد ، چون WGB در واقع کاربران سیمی را مرتبط می کند ؛ اما می توان از repeater ها کمک گرفت .

یک repeater وایرلس ، در واقع یک AP است که برای ارتباط به شبکه ی توزیع ، به یک شبکه ی سیمی متصل نمی گردد ؛ در عوض با یک AP که بصورت فیزیکی به یک شبکه ی توزیع وصل است ، همپوشانی(overlap) می کند . مقدار این overlap ، باید حدود 50 درصد کارائی بهینه باشد .



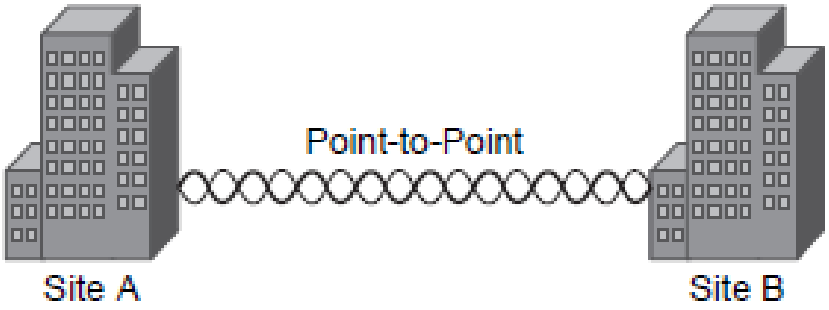
Repeater به یک کاربر اجازه می دهد که به شبکه متصل شود ، در حالیکه آن کاربر خارج از ناحیه ی سرویس دهی AP قرار دارد . البته می توان از یک AP به عنوان repeater استفاده کرد که در این حالت ، تنها از یک SSID پشتیبانی می شود .

در نهایت ، troughput کل برای هر repeater hop ، به دو نیم تقسیم می شود .

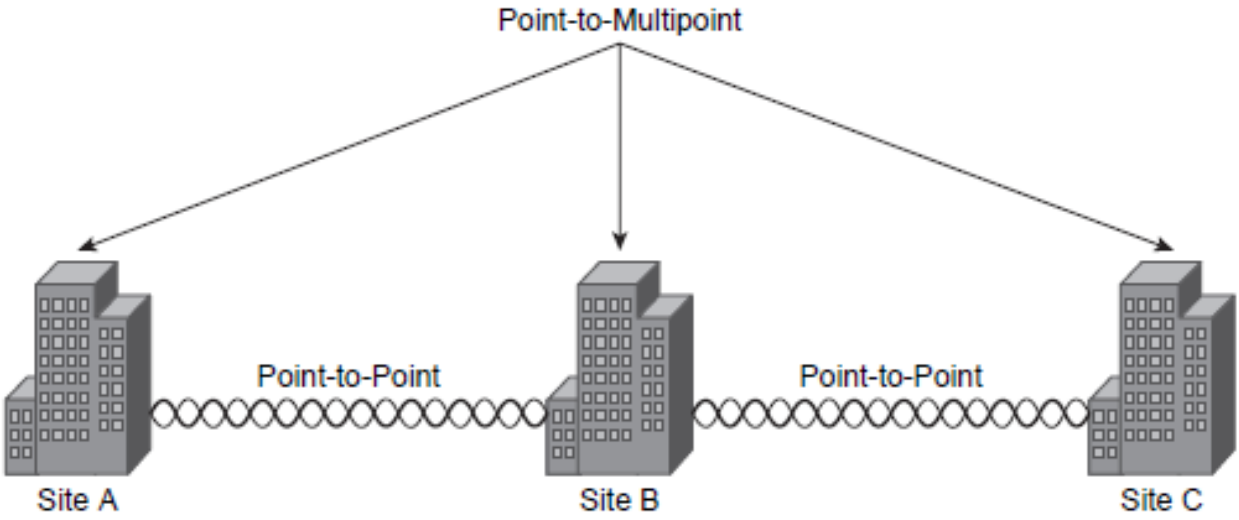
Outdoor Wireless Bridge :

می توان برای برقراری یک لینک بین دو یا چند LAN با فاصله های دور ، باز هم از wireless bridge استفاده کرد . البته از آنجا که bridging انجام می دهیم ، تکنولوژی در لایه ی ۲ انجام می شود . این کلام به این معناست که LAN ها نمی توانند ترافیک را مسیردهی کنند و در وقع routing table ندارند .

می توان دو LAN را از طریق تنظیمات point-to-point به هم متصل کرد :



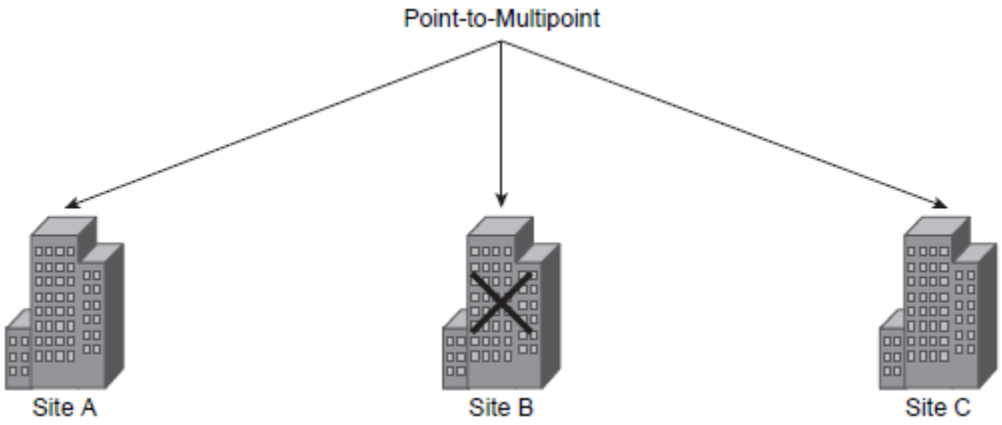
یا اینکه تعداد زیادی LAN را از طریق یک hub مرکزی ، با هم مرتبط ساخت :



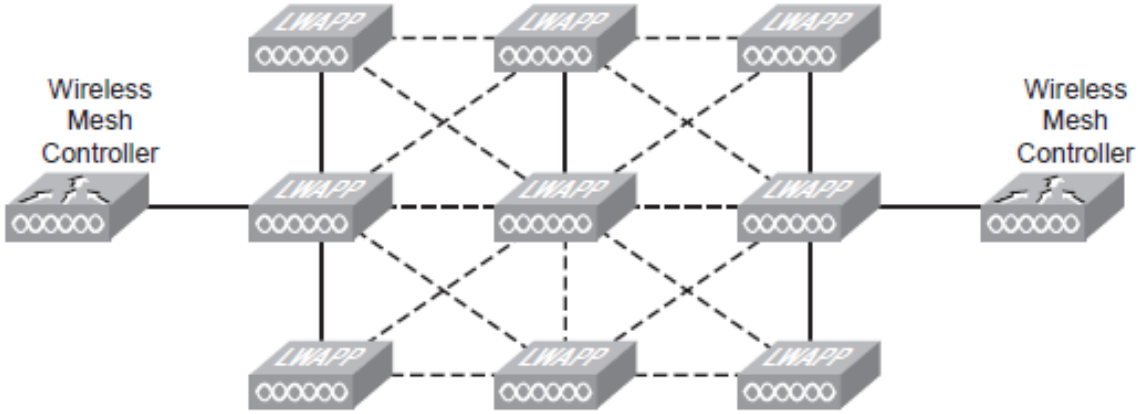
سیسکو استفاده از bridge های وایرلس سری Aironet 1400 و نیز Aironet 1300 را پیشنهاد می کند . با استفاده از مدل 1400 تنها می توان بین شبکه ها پل زد ، اما در مدل ۱۳۰۰ علاوه بر آن ، می توان client ها را نیز متصل کرد .

Outdoor Mesh Networks :

چنانچه چند شبکه توسط یک سایت مرکزی به هم متصل باشند ، در صورتیکه آن سایت مرکزی دچار مشکل شود ، ارتباط تمام شبکه ها با یکدیگر قطع می شود .



یک راه حل ، اینست که از یک شبکه ی mesh استفاده کنیم .



هنگامیکه یک شبکه ی mesh داریم ، بعضی از node ها (یا همان AP ها ی شبکه ی mesh) به یک شبکه ی wired متصل هستند و برخی node ها نقش repeater را بازی می کنند. همچنین بین هر node ، چندین مسیر وجود دارد که در صورت قطع شدن یا از کار افتادن یک route ، می توان از مسیر یا مسیر های دیگر استفاده کرد ؛ هرچند این امر هزینه های برقراری چنین شبکه ای را نیز خیلی بالا می برد .

IEEE هم اکنون روی استاندارد mesh نیز فعالیت می کند (IEEE 802.11s) .

فصل پنجم : آشنایی با آنتن ها

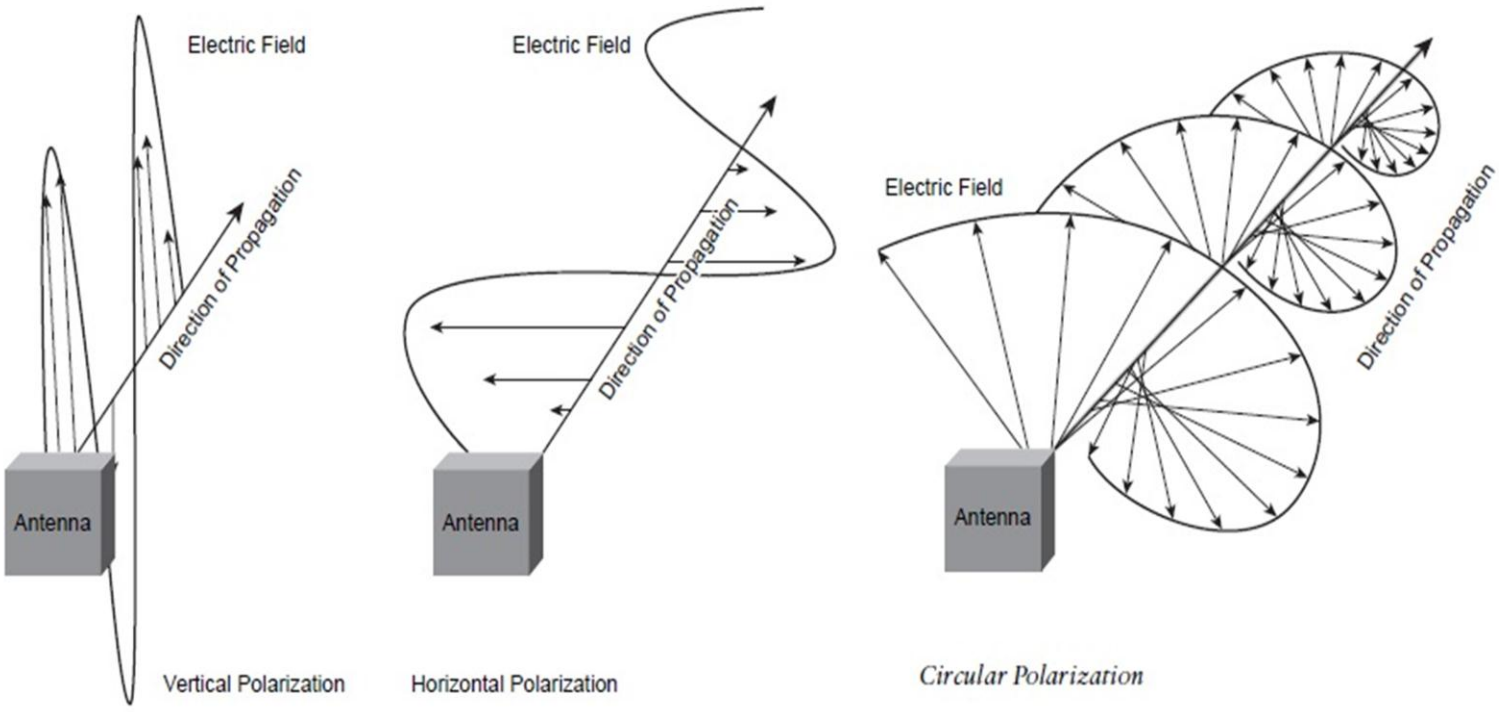
- ❖ Polarization
- ❖ Diversity
- ❖ انواع آنتن های رایج
  - ✓ Omnidirectional Antenna
    - ▪ 2.2-dBi Dipole
    - ▪ AIR-ANT 1728
    - ▪ AIR-ANT 2506
    - ▪ AIR-ANT 24120
  - ✓ Directional Antenna
    - ▪ آنتن دیواری 8.5-dBi Patch
    - ▪ 13.5 Yagi Antenna
    - ▪ 21-dBi Parabolic Dish
    - ▪ Dual-Patch Omnidirectional 5.2 dBi
- ❖ اتصالات و ابزارهای جانبی آنتن ها
  - ✓ تضعیف کننده – Attenuator
  - ✓ تقویت کننده – Amplifier
  - ✓ صاعقه گیر – Lightning Arrestor
- ❖ تقسیم کننده – Splitter

بدون شک می توان گفت که مهمترین بخش یک شبکه ی وایرلس ، آنتن ها هستند ؛ زیرا بدون آنتن ها ، سیگنال شما نمی تواند حتی یک متر را نیز طی کند . در این بخش ، در مورد ویژگی های آنتن ها صحبت خواهیم کرد ، تا با انتخاب آنتن مناسب ، مطمئن شویم که شبکه ی وایرلس ، تمام محدوده ی مورد نیاز را به خوبی پوشش داده است .

Polarization :

هدف اصلی یک آنتن ، اینست که امواج الکترومغناطیس را در فضا تشعشع کند . یک موج الکترومغناطیس می تواند به چندین شکل حرکت کند که به نحوه ی حرکت این موج ، پولاریزاسیون می گویند . سه نوع پولاریزاسیون (قطبی شدگی) داریم :

- ✓ Vertical (عمودی)
- ✓ Horizontal (افقی)
- ✓ Circular (مدور)



نکته : آنتن های سیسکو همیشه در شبکه های وایرلس ، بصورت پولاریزاسیون عمودی (vertical) هستند . یعنی میدان الکتریکی همیشه عمودی است .

نکته : میدان الکتریکی توسط بارهای ساکن ، یا جریان الکتریکی به وجود می آید .

نکته : میدان مغناطیسی توسط بارهای متحرک بوجود می آید .

Diversity (تنوع ، گوناگونی) :

یکی از راههای مقابله با multipath ، استفاده از دو آنتن در یک AP است ؛ به این امر diversity گفته می شود . در این روش ، هنگامیکه اولین فریم به AP رسید ، هر دو آنتن به فریم گوش می کنند ، لذا AP می تواند بفهمد که کدام آنتن فریم را بهتر و قوی تر دریافت می کند . از آن به بعد ، همه ی فریم ها از آن آنتن دریافت خواهند شد .

البته باید توجه داشت که آنتن ها باید یکسان باشند و هردو یک ناحیه ی مشخص را پوشش دهند .

انواع آنتن های رایج :

باید توجه داشت که همه ی آنتن ها یک مقدار انرژی را ارسال می کنند ، لذا تفاوت آنها تنها در میزان تمرکز شعاع تشعشع آنتن است (focus of beam) . برای درک بهتر ، فرض کنید یک چراغ قوه دارید که نور را به جلو پخش می کند و هرچند می توانید سطح وسیع تری را روشن کنید ، اما چنانچه مثلا از چراغ های لیزری استفاده کنید ، میبینید که شعاع نور بسیار باریک و متمرکز شده است ، و برد زیادی نیز دارد . در مورد آنتن ها هم همین مسئله صادق است . ممکن است ما آنتن را به سقف یک سالن بزرگ (مثل لابی هتل) نصب کنیم و بخواهیم که در همه ی جهات ، تشعشع داشته باشد ؛ یا اینکه بخواهیم یک لینک point-to-point با مسافت مثلا ۲۰ کیلومتر برقرار کنیم و آنتنی را انتخاب کنیم که beam آن بسیار باریک و متمرکز باشد تا بتواند آنتن مقابل خود را ببیند و تنها برای همان آنتن سیگنال ها را ارسال کند .

نکته : اگر می خواهید توان را در یک جهت خاص افزایش دهید ، باید gain آنتن را بیشتر کنید .

نکته : معمولا هنگامیکه نیاز به beam متمرکز داشته باشیم ، آنتن های با gain بالا خریداری می نماییم .

Omnidirectional Antenna :

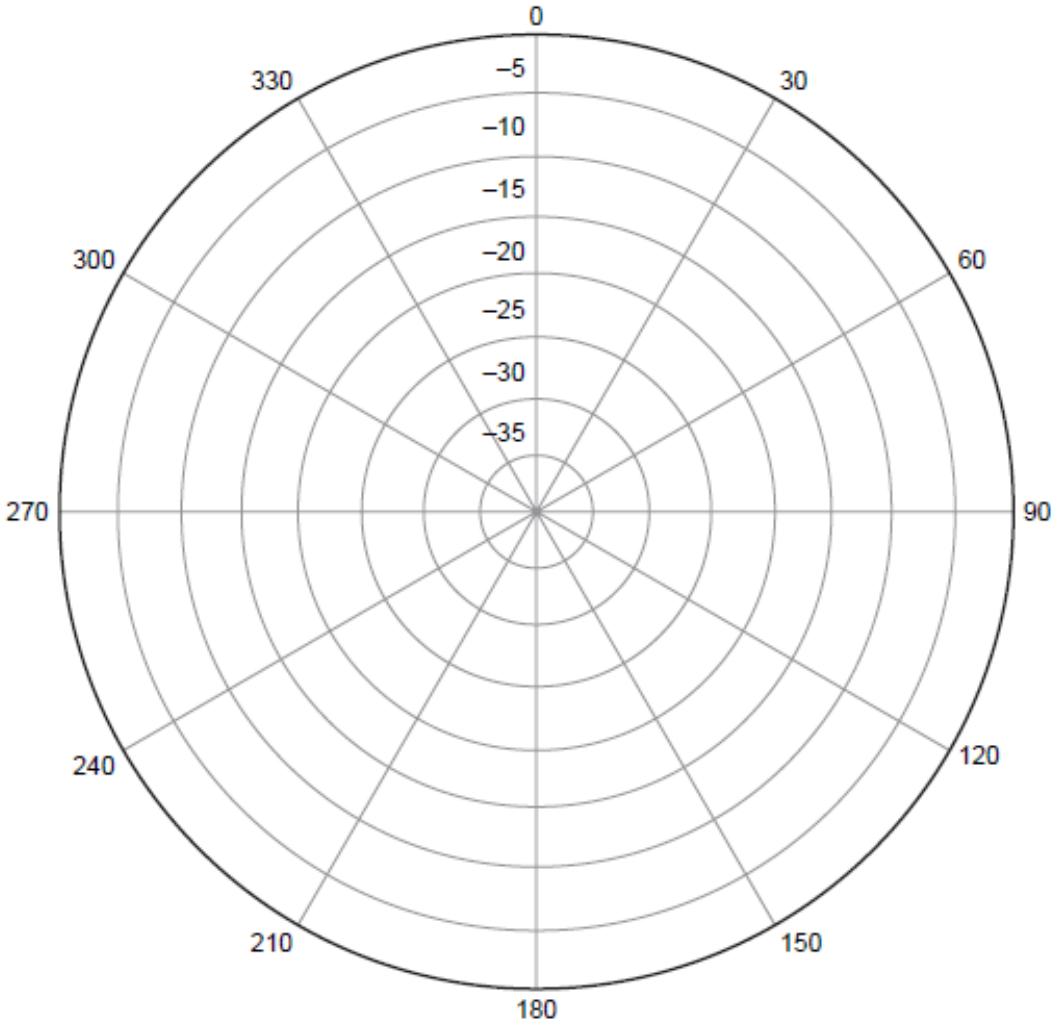
همانطور که از نامش پیداست ، این آنتن در همه ی جهات سیگنال ها را متشعشع می نماید .

دو راه برای بررسی محدوده ی پوشش یک آنتن وجود دارد ؛ یکی اینکه یک AP را در جایی قرار داده و سپس با یک client مثل لپ تاپ ، شروع به حرکت کنیم و با محاسبه ی SNR و RSSI ، به صورت تجربی coverage آنتن را محاسبه کنیم .

راه دیگر ، راهیست که از روش اول خیلی راحت تر است ، زیرا در واقع سازنده ی آنتن این اطلاعات را از طریق برخی نمودارها به ما می دهد . در این روش ، ما از اطلاعاتی که در کاتالوگ های آنتن ها و datasheet آنها وجود دارد ، استفاده می کنیم . یکی از انواع این اطلاعات ، نقشه های مختلفی است که در شرایط آزمایشگاهی از نحوه ی عملکرد آنتن تهیه شده است .

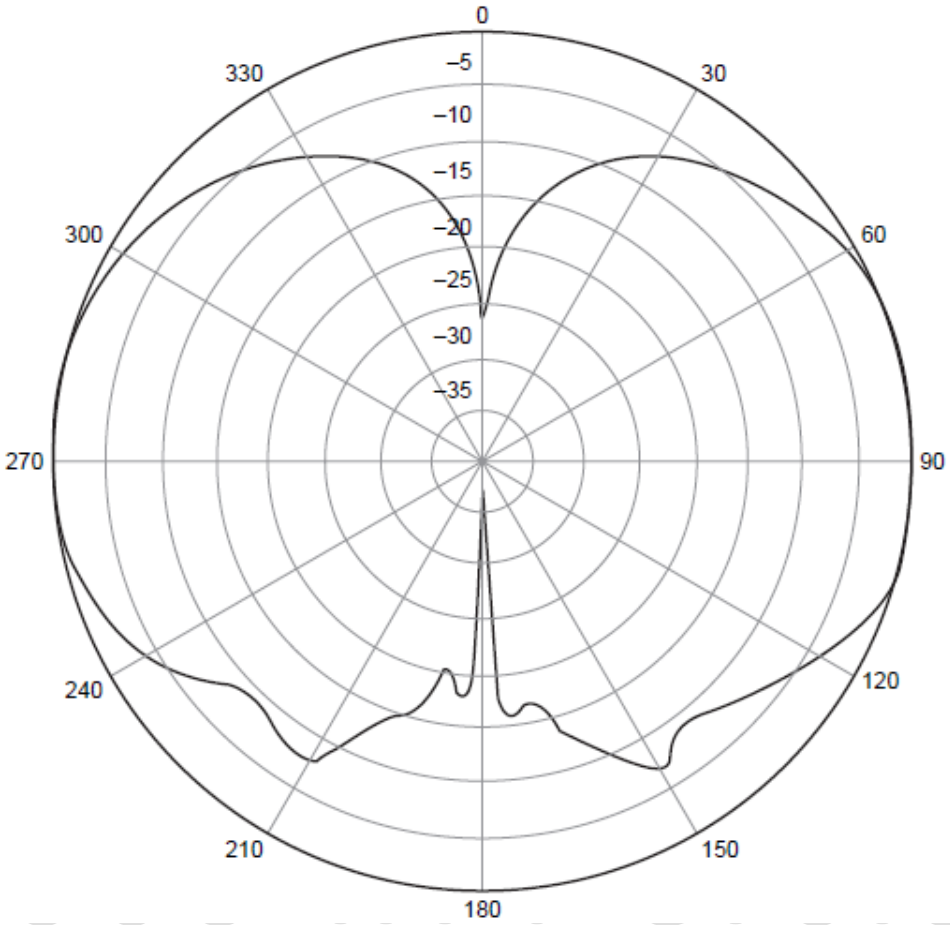
- ✓ **H-plane** : هنگامیکه به Horizontal-plane یک آنتن نگاه می کنیم ، در واقع داریم از بالا به آن آنتن نگاه می کنیم . این نقشه را Azimuth (محور) نیز می نامند .

شکل زیر ، نتیجه ی نگاه از بالا به یک آنتن omnidirectional است :

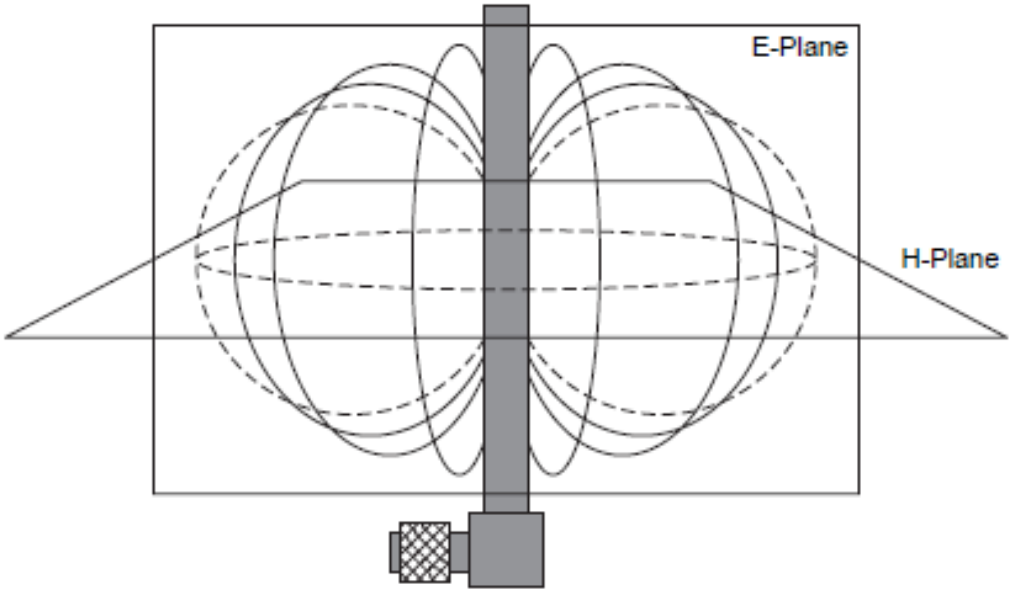


البته باید توجه داشت که این ، حالت ایده آل است و در عمل ، ساخت آنتنی که به این تقارن و یکسانی و کیفیت ، در همه ی جهات تشعشع نماید ، ممکن نیست .

- ✓ **E-plane** : Elevation-plane حاصل نگاه از کنار به یک آنتن است ، در E-plane زیر ، می بینیم که pattern آنتن ۳۶۰ درجه ی کامل نیست ، که این مسئله به خاطر محدودیت های طراحیست و به one floor معروف است . یعنی سیگنال به اطراف آنتن پخش می شود ، نه اینکه به سمت بالا یا پایین برود . لذا سیگنال ها فقط به کاربرانی که در همان طبقه ی آنتن قرار دارند می رسد ، نه آنهایی که در طبقات بالا یا پایین قرار دارند .



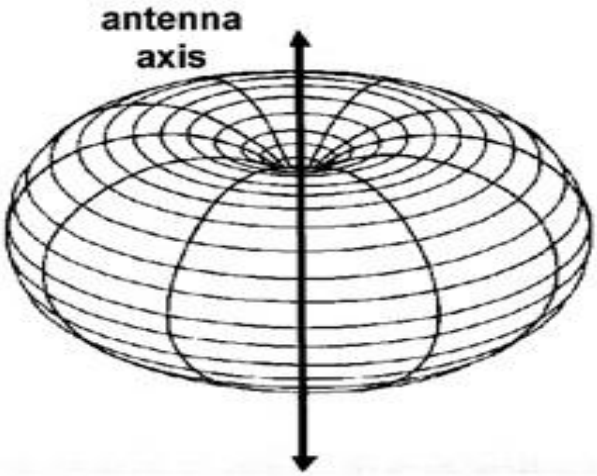
برای اینکه دید بهتری نسبت به E-plane و H-plane پیدا کنید ، به شکل زیر توجه بفرمایید :

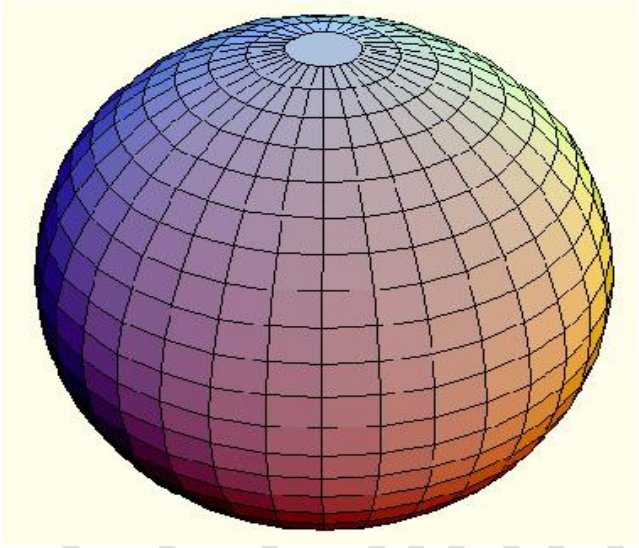


حال می توانیم چندین آنتن معروف را به همراه مشخصاتشان معرفی نماییم .

2.2-dBi Dipole :

pattern تشعشع این آنتن شبیه به دونات است ، زیرا این آنتن به صورت vertical ، تشعشع زیادی ندارد ؛ در عوض برای تشعشع H-plane طراحی شده است (شکل سمت چپ). هنگامیکه می گوییم Dipole ها دارای الگوی تشعشع شبیه به دونات (Doughnut-shaped) هستند ، باید توجه کنیم که اغلب اوقات آنتن ها با یک isotropic radiator مقایسه می شوند (شکل سمت راست). تشعشع کننده ی ایزوتروپیک ، فرض می کند که سیگنال در همه ی جهات و راستاها ، به صورت یکسان پخش و انتشار می یابد .(که البته این نگاه ، کاملا ایده آل و غیر عملیست .)

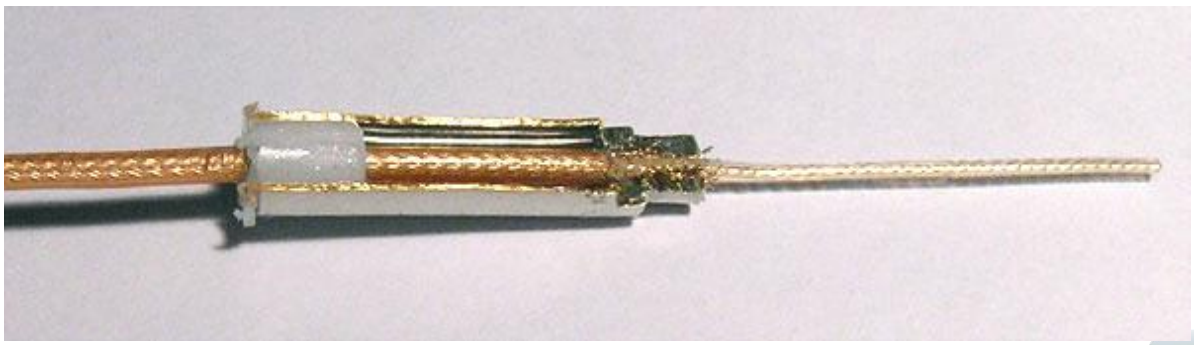




این آنتن به Rubber Duck هم معروفست . آنتن 2.14-dBi ، قابلیت تاشوندگی برای انعطاف بیشتر هنگام نصب را دارد :

چند نمونه مختلف از آنتن های rubber ducky را در شکل زیر می بینید :

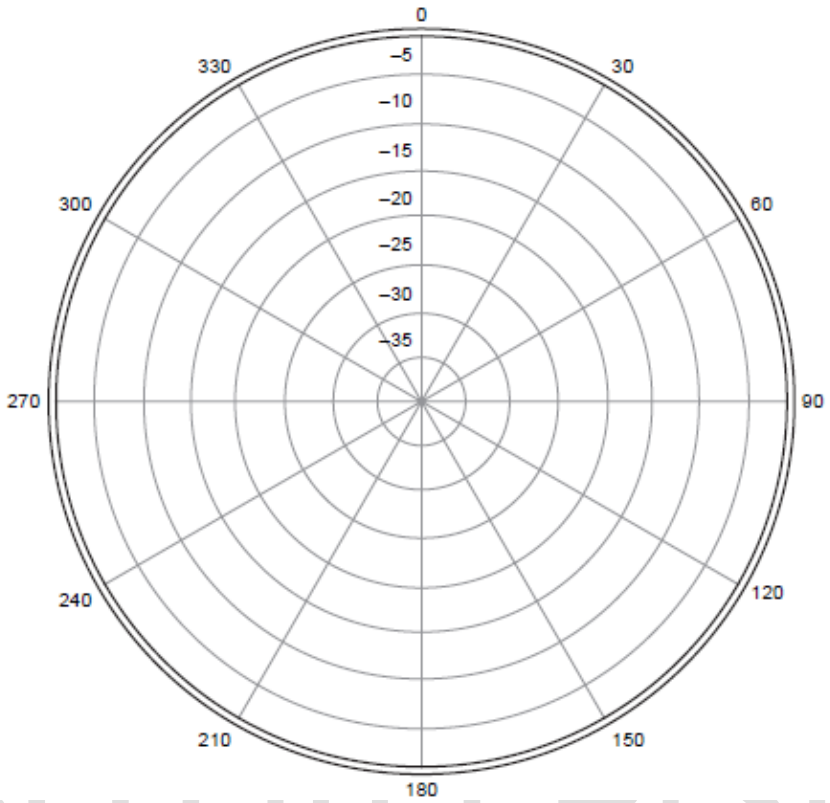
البته ساختار داخلی این آنتن ها نسبتا ساده هستند ؛ در شکل زیر جزئیات یک آنتن *WRT54GS را مشاهده می کنید :*



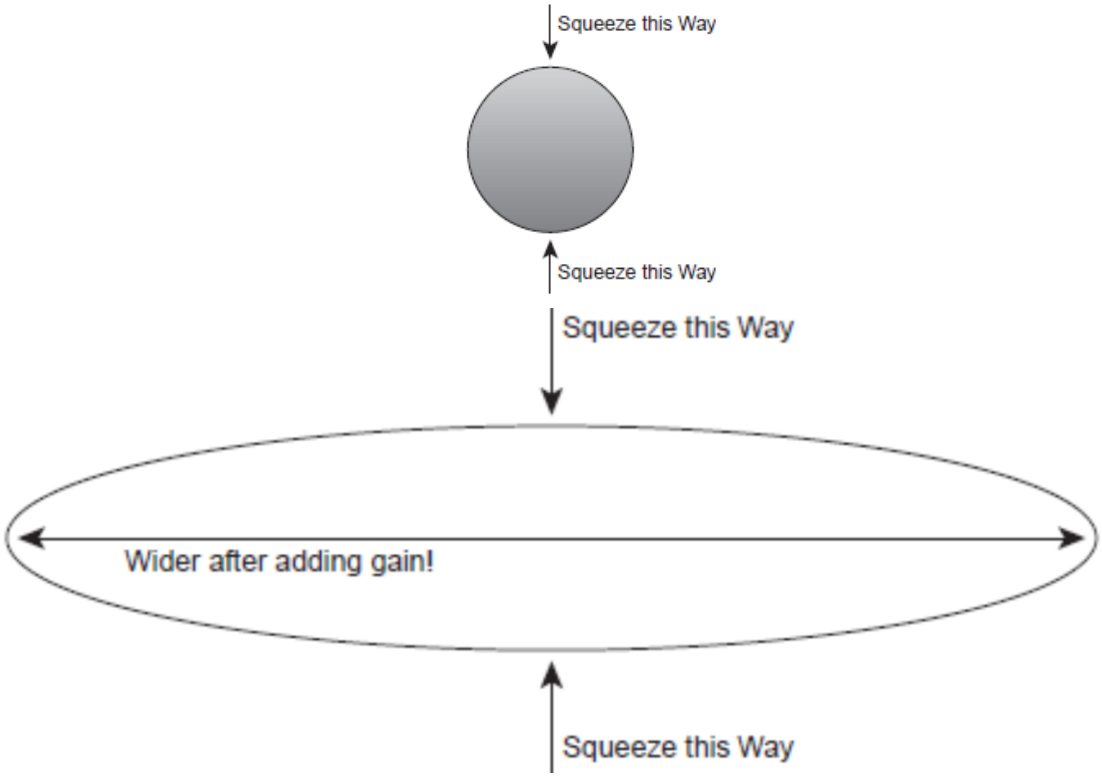
جزئیات این آنتن را در جدول زیر می توانید ببینید ، هرچند اطلاعات کافی روی خود آنتن نوشته شده است .

Gain	5.2 dBi
Polarization	5.2 dBi
H-plane	Vertical
E-plane	Omnidirectional 360 degrees
Antenna connector type	RP-TNC
Mounting	Drop ceiling cross-member indoor only

H-plane این آنتن به این شکل می باشد :



برای افزایش gain آنتن (مثلا در اینجا ، افزایش از 2.2dBi به 5.2dBi) ، باید کاری کنیم که H-plane آنتن به جای اینکه شبیه به دایره ی کامل باشد ، هرچه بیشتر بیضی شکل شود ؛ به عبارتی باید H-plane عریض تر و E-plane کوتاهتر شود .



: AIR-ANT2506

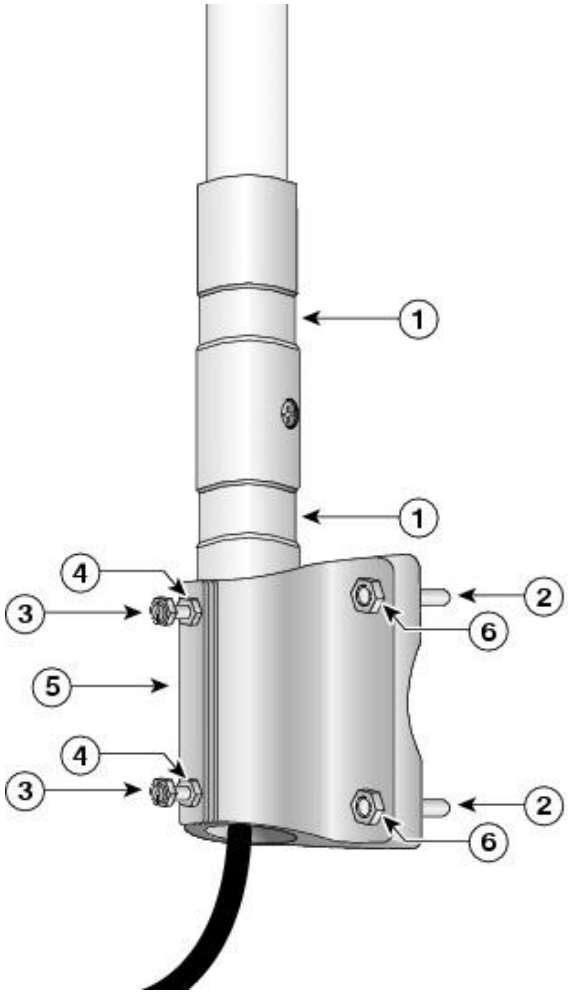
جزئیات بیشتر در مورد این آنتن را در جدول زیر می توانید بیابید :

Gain	5.2 dBi
Polarization	Vertical
H-plane	Omnidirectional 360 degrees
E-plane	RP-TNC
Antenna connector type	Mast-mount indoor/outdoor
Mounting	

AIR-ANT24120 :

از نظر ظاهری تقریبا شبیه دو آنتن قبلیست ، با این تفاوت که بیش از یک متر طول و حدود ۱.۵ کیلوگرم وزن دارد .

1	Antenna grooves
2	5/16 x 18 U-bolt
3	1/4-20 hex bolts
4	Jam nuts
5	Sandcast bracket
6	5/16-18 hex nut



سایر جزئیات آنتن را می توانید در جدول زیر مشاهده فرمایید :

Gain	12 dBi
Polarization	Linear Vertical
H-plane	Omnidirectional 360 degrees
E-plane	7 degrees
Antenna connector type	RP-TNC
Mounting	Mast-mount

Directional Antenna :

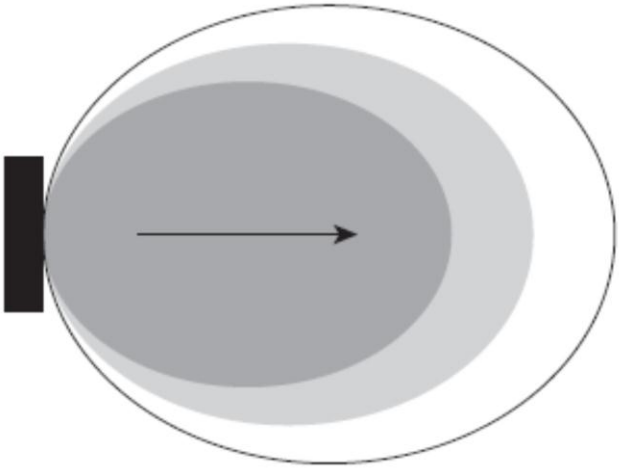
آنتن های directional ، معمولا روی دیوار ها یا در ارتفاعات نصب می شوند تا در یک جهت خاص و بصورت متمرکز ، تشعشع کنند . مورد مصرف این آنتن ها در راهروها ، سالن ها ، سوله ها یا انبار ها می باشد . همچنین برای مصارف outdoor ، می توان از این آنتن ها بصورت دیش های سهموی (parabolic) استفاده نمود .

آنتن های Directional ، گین بهتری نسبت به آنتن های omnidirectional دارند ؛ pattern تشعشع آنها متمرکز شده است . همچنین از قاعده ی one floor استفاده می کنند ؛ یعنی از نظر vertical برد زیادی ندارند ، اما از نظر horizontal محدوده ی وسیعی را پوشش می دهند . در ادامه ، با برخی از این آنتن ها بیشتر آشنا می شویم .

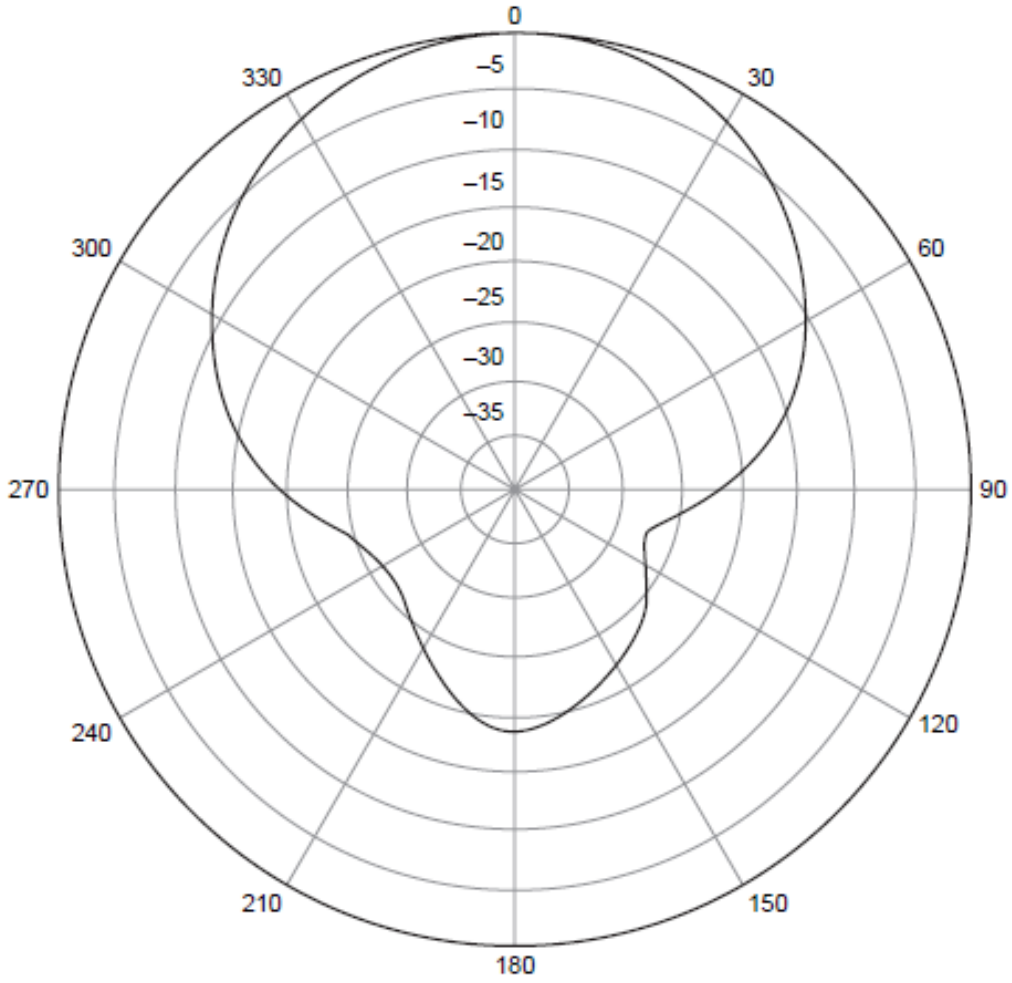
آنتن دیواری 8.5dBi Patch :

در شکل زیر ، آنتن AIR-ANT2485P-R 8.5dBi را مشاهده می کنید :

هنگامیکه این آنتن را به دیوار نصب می کنید ، pattern تشعشعی نظیر شکل زیر به شما می دهد :



در آنتن های directional ، هرچه درجه ی H-plane یا E-plane کمتر باشد ، بهتر است ؛ این به این معناست که focus سیگنال بیشتر است و gain آنتن بهتر می باشد . در شکل زیر ، H-plane آنتن AIR-ANT2485P-R 8.5dBi را مشاهده می کنید .

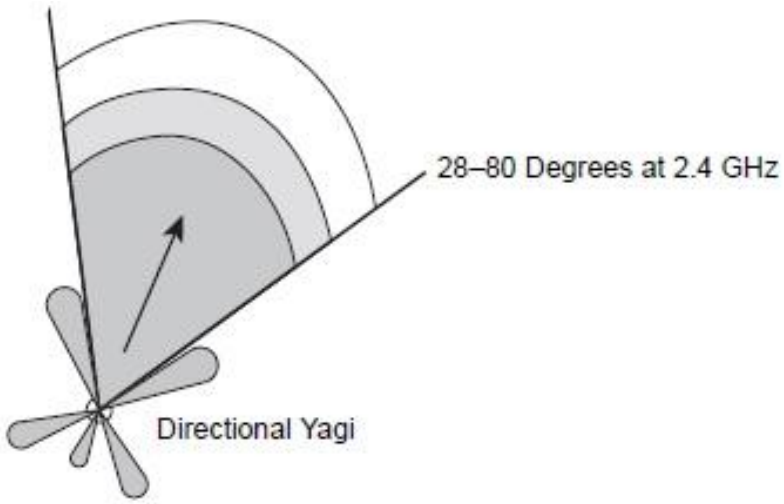


جزئیات بیشتر در مورد این آنتن را در جدول زیر میتوان یافت :

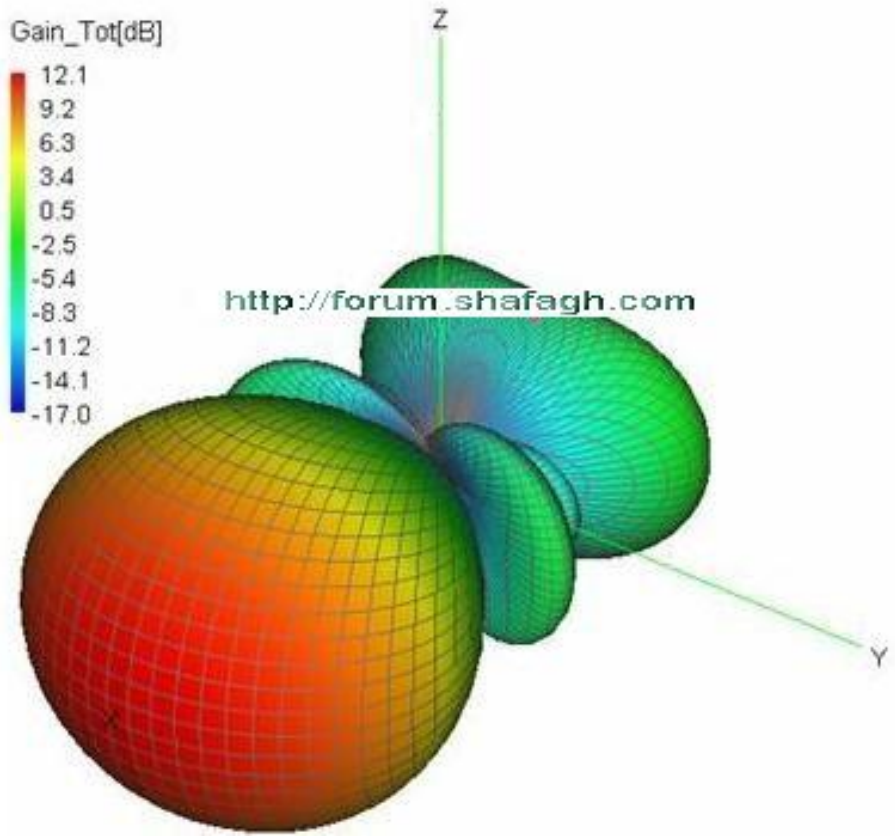
Gain	8.5 dBi
Polarization	Vertical
H-plane	66 degrees
E-plane	56 degrees
Antenna connector type	RP-TNC
Mounting	Wall mount

13.5 Yagi Antenna :

این آنتن ، یک آنتن directional است که pattern تشعشع بسیار مستقیمی دارد . به خاطر نوع پولاریزاسیون ، آنتن یاگی دارای اثر پروانه ای (butterfly effect) است ؛ یعنی علاوه بر main lobe ، تعدادی side lobe نیز دارد که در شکل زیر نشان داده شده است :

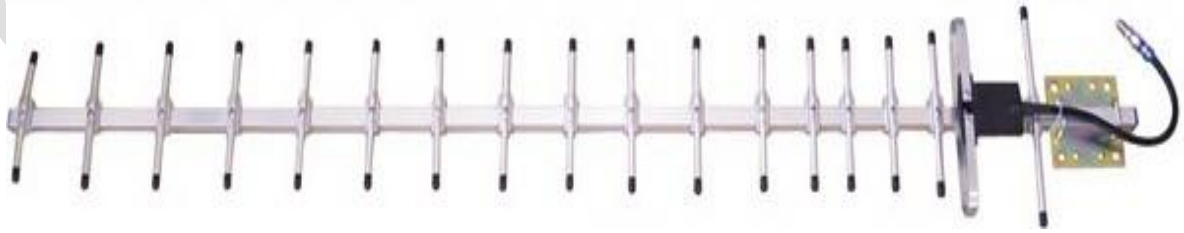


در شکل سه بعدی زیر ، بهتر می توانید نحوه ی پخش توان سیگنال آنتن یاگی را مشاهده فرمایید :



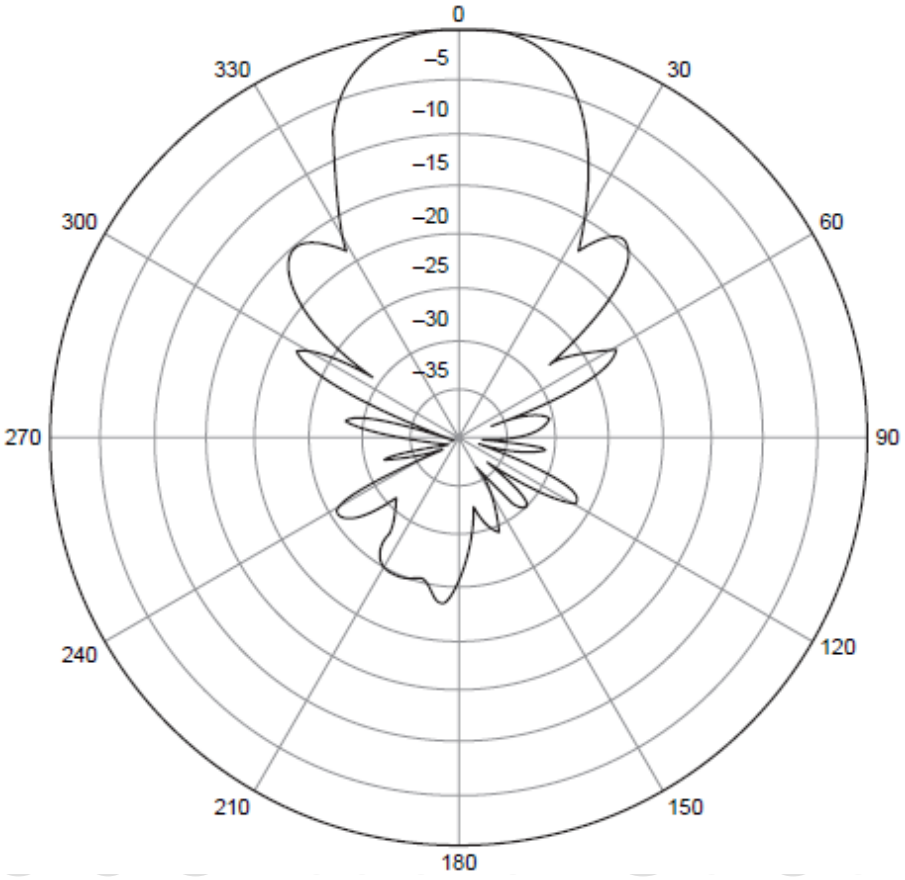
در شکل زیر ، یک آنتن یاگی AIR-ANT2410Y-R 10dBi را مشاهده می فرمایید :

هرچند در این شکل ، این آنتن طراحی خیلی شکیل و جا گرفته در یک سیلندر استوانه ای دارد ، اما آنتن داخل آن ، چیزی شبیه یک "شانه" است که یادآور آنتن های قدیمی تلوزیونی UHF است که معمولا روی پشت بام ها از آنها استفاده می شود .



در شکل زیر ، نوع دیگری از آنتن یاگی ، با نام AIR-ANT1949 13.5dBi را مشاهده می کنید :

در شکل زیر E-plane آنتن AIR-ANT1949 13.5dBi را می بینید :



در جدول زیر می توانید با برخی خصوصیات این آنتن آشنا شوید :

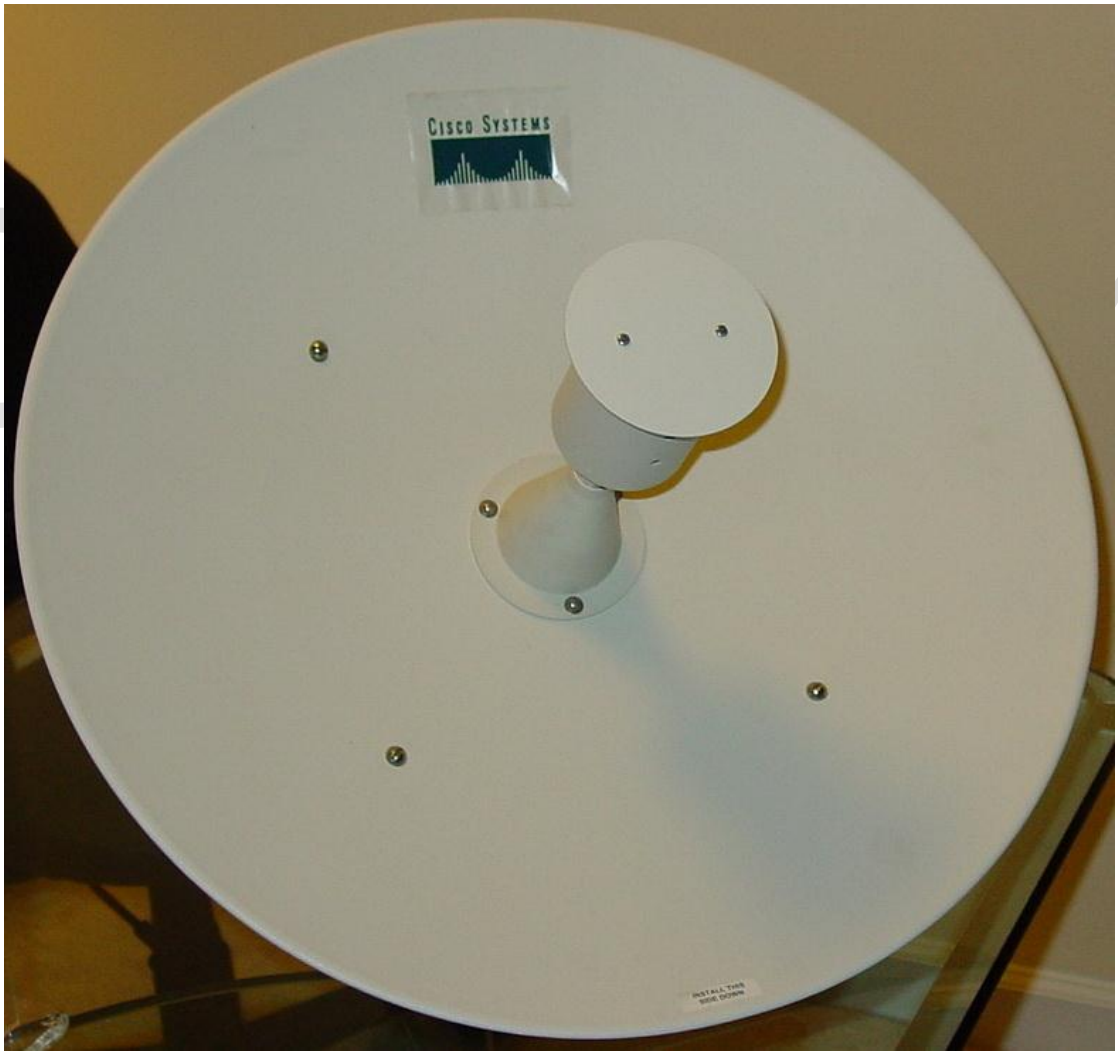
Frequency range	2.4 to 2.83 GHz
Gain	13.5 dBi
Polarization	Vertical
H-plane	30 degrees
E-plane	25 degrees
Antenna connector type	RP-TNC
Mounting	Mast/wall mount

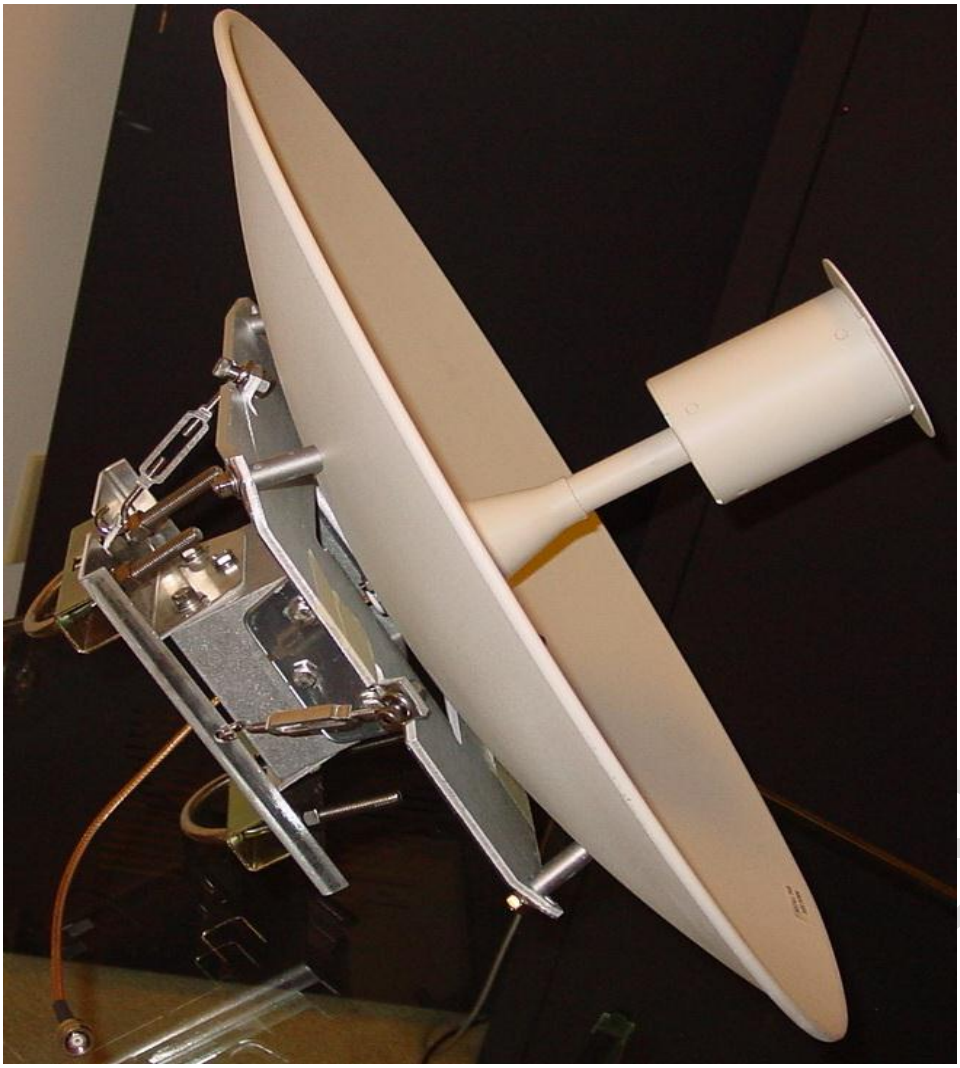
- هنگامیکه یک آنتن یاگی را نصب می کنید ، در نظر گرفتن پولاریته بسیار مهم است . لذا باید بدانید که چگونه آنتن را نصب کنید که با توجه به کاتالوگ های ضمیمه آنتن ، معمولا انتهای آنتن های یاگی سیسکو ، با یک نقطه ی سیاه مشخص شده است . مجددا توجه داشته باشید که اگر آنتن را به اشتباه نصب کنید ، کیفیت و توان سیگنال تا حد زیادی افت پیدا کرده یا کلا خراب خواهد شد .

21-dBi Parabolic Dish :

آنتن های دیش پارابولیک ، مسیر خیلی باریکی دارند و pattern تشعشع آنها بسیار متمرکز است . هنگام نصب این آنتن ، باید دقت زیادی به خرج داد ؛ و در جاهایی مثل سناریو های point-to-point میتوان از آن استفاده نمود . این آنتن ها نیز butterfly effect دارند . برخی از آنتن های دیش پارابولیک ، این مزیت را دارند که می توان در آنها polarity را تغییر داد ؛ این مسئله خیلی مهم است ، زیرا می توان آنها را در یک زاویه ی دیگر نصب کرد ، و پولاریته نحوه ی ارسال RF را تغییر می دهد .

آنتن نشان داده شده در شکل زیر ، یک آنتن AIR-ANT3338 Parabolic Dish است که تقریبا ۱۰۰ برابر از rubber duck قوی تر است .





در جدول زیر ، جزئیات این آنتن را مشاهده می کنید :

Power	5 Watts
Gain	21 dBi
Polarization	Vertical
H-plane	12 degrees
E-plane	12 degrees
Antenna connector type	RP-TNC
Mounting	Mast mount

Dual-Patch “Omnidirectional” 5.2 dBi :

شکل زیر ، آنتن AIR-ANT3213 Dual-Patch 5.2dBi را نشان می دهد :

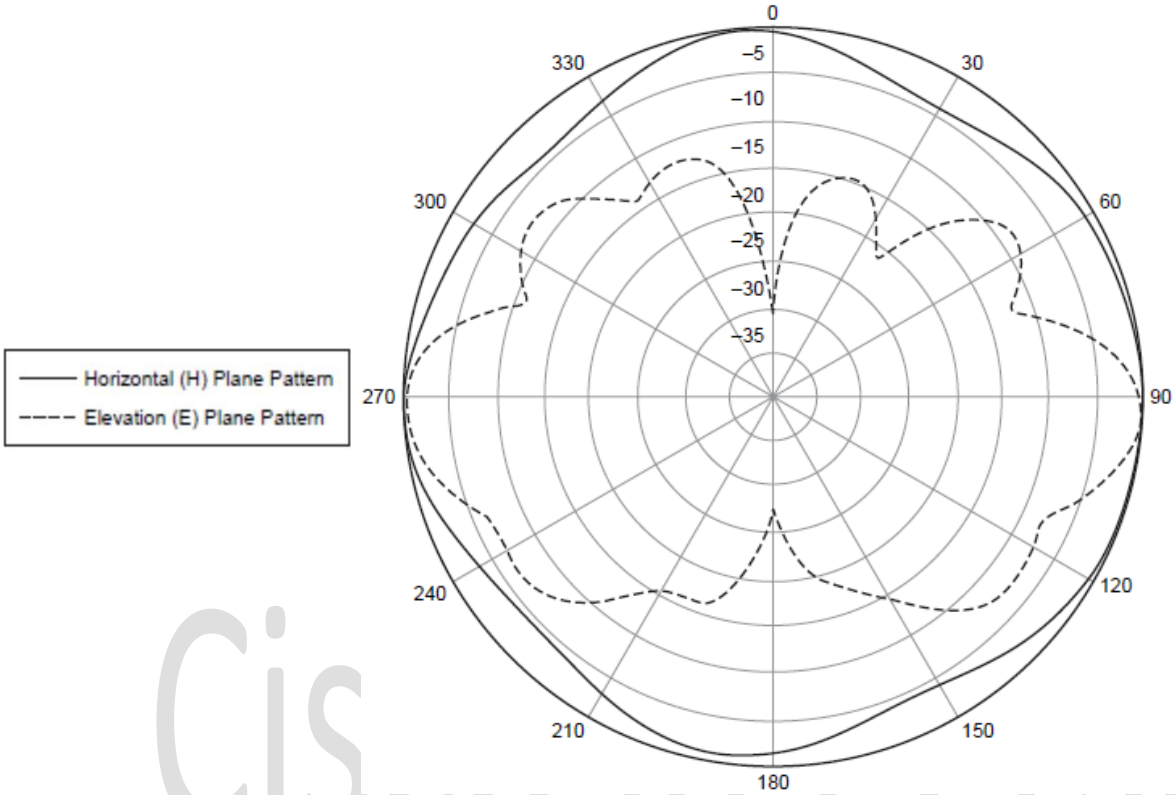
این آنتن ، یک آنتن خاص است ، زیرا در آن دو آنتن directional بصورت پشت به پشت قرار دارند که این آنتن را به نوعی omnidirectional می کند . از آنجا که در واقع دو آنتن وجود دارد ، می توان با این آنتن ها از diversity استفاده کرد .

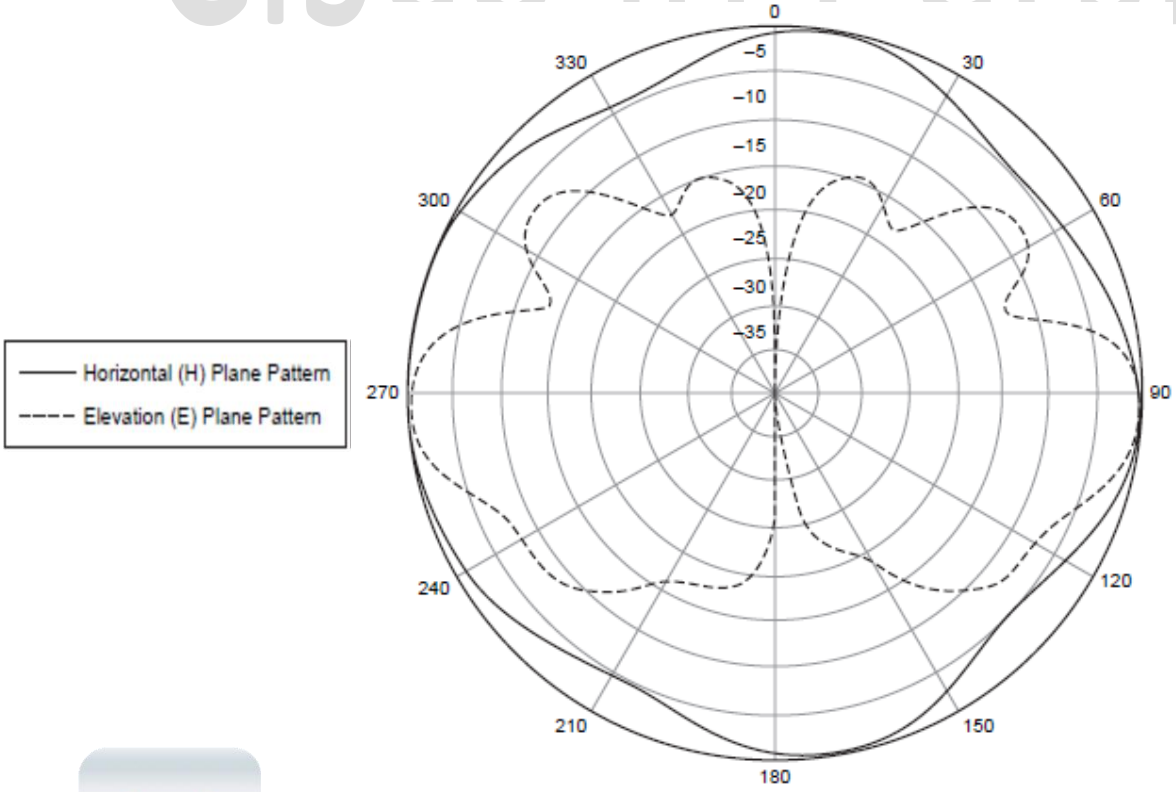
باید توجه داشت که هر دو آنتن به کار رفته ، باید یکسان باشند ، بطوریکه اگر به E-plane یا H-plane آنها نگاه کنیم ، تفاوت چندانی وجود نداشته باشد .

در جدول زیر ، برخی جزئیات این آنتن را مشاهده می فرمایید :

Frequency range	2.4 to 2.83 GHz
Gain	5.2 dBi
Polarization	Vertical
H-plane	Omnidirectional
E-plane	25 degrees
Antenna connector type	RP-TNC

همچنین در دو شکل زیر ، می توانید نمونه ی E-plane و H-plane را برای آنتن های چپ (شکل اول) و راست (شکل دوم) مشاهده نمایید .





اتصالات و ابزارهای جانبی آنتن ها :

قبلا گفتیم که آنتن های سیسکو همگی از کانکتور RP-TNC استفاده می کنند . هرچند آنتن های مختلف با vendor های مختلف ، از کانکتور های گوناگون استفاده می کنند ، اما در هر حال نکته ی مهم اینست که هر دو طرف ، باید به یک کانکتور یکسان (که در هر دو match باشند) ، متصل شوند .

چنانچه آنتن به نوعیست که نمی توان آنرا بطور مستقیم وصل کرد ، باید از کابل های مربوط به همان نوع آنتن استفاده کرد ؛ استفاده از کابل بین رادیو ی فرستنده و آنتن ، باعث بوجود آمدن اتلاف در سیگنال ها می شود .

Attenuator (تضعیف کننده) :

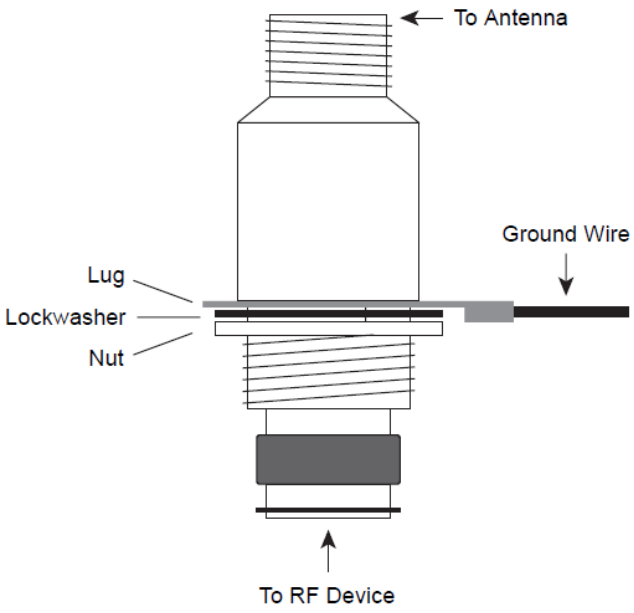
برای کاهش دادن سیگنال ، می توان از این تضعیف کننده ، بین آنتن و رادیو استفاده نمود ؛ این کار مانع از تاثیر گذاشتن سیگنال زیاد روی بقیه ی بخش های شبکه می شود .

Amplifier (تقویت کننده) :

قبلا گفتیم که اضافه کردن کابل بین رادیو و آنتن ، باعث تضعیف و اتلاف سیگنال می شود و ما نیاز داریم که گین را زیاد کنیم ؛ اما شاید نتوانیم گین کافی را جبران کنیم . لذا می توان از یک تقویت کننده بین AP و آنتن استفاده کرد تا سیگنال را تقویت کند . به این روش active amplifier می گویند ، زیرا آنتن را تقویت می کند .

Lightning Arrestor (صاعقه گیر) :

از آنجا که آنتن پارابولیک به AP و رادیو ، و در نهایت به redistribution متصل است ، اگر یک صاعقه به آن برخورد کند ، کل ولتاژ بالای صاعقه ، به شبکه می رسد و همه چیز را نابود می کند . برای جلوگیری از این مشکل ، می توان از صاعقه گیر استفاده کرد .



محدودیت های این دستگاه ، ولتاژ ۵۰ ولت در ۱۰۰ نانوثانیه است (از آنجا که زمان صاعقه ۲ میکروثانیه است ، پس این محدودیت کاملا محتاطانه و کافیست).

توجه داشته باشید که این دستگاه نمی تواند جلوی صاعقه را بگیرد ، بلکه فقط می تواند آنرا منحرف کند ؛ لذا باید حتما آنرا به زمین اتصال بدهیم (از طریق ground wire) تا صاعقه را تخلیه کند .

Splitter (تقسیم کننده) :

این دستگاه اساسا در شبکه های وایرلس outdoor استفاده می شود تا سیگنالی که از یک کابل می آید را در دو مسیر مختلف ارسال کند . همچنین با استفاده از یک اسپلیتر ، می توان سیگنالی که از یک جهت توسط یک آنتن دریافت می شود را به آنتن دیگری که به همان AP متصل است فرستاد و آن را در جهتی دیگر انتشار داد .

تقسیم کننده ، throughput و نیز محدوده ی پوشش را تا حدود ۵۰ درصد کاهش می دهد .

فصل ششم : آشنایی با پروتکل های 802.11

- پروتکل 802.11 اصلی
- پروتکل 802.11b
- پروتکل 802.11g
- نحوه ی همکاری 802.11g با 802.11b
  - ✓ ERP
  - ✓ Non-ERP
  - ✓ RTS
  - ✓ CTS
- پروتکل 802.11a
- پیش نیازهای توان 802.11a
- پروتکل 802.11n
  - ✓ Precoding
  - ✓ Spatial Multiplexing
  - ✓ Diversity Coding
- ارسال فریم ها
- ملاحظات مربوط به آنتن ها

IEEE پروتکل های وایرلس را استاندارد سازی می کند . البته تعداد این پروتکل ها بسیار زیاد است ، اما از این بین ، شما باید با عملکرد ۴ پروتکل اصلی 802.11a/b/g/n کاملا آشنا باشید ؛ زیرا امروزه از این ۴ پروتکل تقریبا در همه ی LAN های وایرلس استفاده می شود . در این فصل ، نگاهی به تاریخچه و نیز عملکرد این چهار پروتکل (که همگی در محدوده ی 2.4GHz و 5GHz فعالیت می کنند) خواهیم انداخت .

پروتکل 802.11 اصلی :

این پروتکل در سال ۱۹۹۷ معرفی شد ؛ هرچند خیلی بعید است که امروزه بتوان این پروتکل را در دستگاههای جدید مشاهده کرد ، زیرا تنها در سرعت های ۱ و 2Mbps فعالیت می کرد ! پروتکل 802.11 همچنین از تکنولوژی های FHSS (Frequency-Hopping Spread Spectrum) و DSSS (Direct Sequence Spread Spectrum) استفاده می کرد که اینها نیز تنها در سرعت های ۱ و 2Mbps کار می کردند .
در ۸۰۲.۱۱ ، چنانچه یک client در هر data rate دیگری فعالیت می کرد ، حتی اگر قابلیت کار در سرعت های ۱ یا 2Mbps را داشت ، به عنوان یک non-802.11 در نظر گرفته می شد .
پروتکل ۸۰۲.۱۱ اصلی تنها در محدوده ی فرکانسی 2.4GHz فعالیت می کرد و مورد استفاده ی باندهای صنعتی ، علمی و پزشکی (ISM bands) قرار می گرفت . محدوده ی فرکانسی 2.4GHz بسته به کشوری که در آن هستید ، تا ۱۴ کانال دارد که مثلا در امریکا ، FCC به شما اجازه می دهد از کانال های ۱ تا ۱۱ استفاده کنید ؛ یعنی ۳ کانال ناهمپوشان دارید : ۱ و ۶ و ۱۱ .

پروتکل 802.11b :

مهندسین شبکه مشاهده کردند که تکنولوژی خیلی سریعتر از استانداردها حرکت و پیشرفت می کند . ۸۰۲.۱۱ خیلی سریع از دور خارج شد ، زیرا شبکه های سیمی توانستند به 10Mbps برسند که سرعت های ۱ و 2Mbps در برابر آن قدرت رقابت نداشتند . البته vendor های مختلف روش های مختلفی برای رسیدن به سرعت های بالاتر را ارائه دادند ، اما این پروتکل های طراحی شده برای هر vendor ، خطر ایجاد مشکل در همکاری دستگاههای مختلف با هم را افزایش می داد .
وظیفه ی IEEE این بود که استانداردی تعریف کند که همه ی vendor ها بتوانند براساس قابلیت های خود از آن استفاده کنند.
در سال ۱۹۹۹ استاندارد 802.11b معرفی شد که تا سرعت 11Mbps را فراهم می آورد . این پروتکل با پروتکل قبلی کاملا سازگار است ، بطوریکه هنگام فعالیت در سرعت های ۱ و 2Mbps از همان مدولاسیون ها و coding های استاندارد ۸۰۲.۱۱ اصلی استفاده می کند ؛ در حالیکه هنگام فعالیت در سرعت های 5.5Mbps و 11Mbps از مدولاسیون های جدیدی استفاده می نماید . این استاندارد ، علاوه بر Barker 11 که در ۸۰۲.۱۱ اصلی استفاده می شود ، از Complementary Code Keying (CCK) نیز به عنوان کدینگ استفاده می کند . همچنین علاوه بر مدولاسیون DBPSK ، از DQPSK نیز استفاده می کند .

802.11b برای تغییر سرعت client ها از سرعت بالا به سرعت پایین ، از Dynamic Rate Shifting (DRS) استفاده می کند . امروزه ، استاندارد 802.11b محبوب ترین و پرکاربردترین استاندارد وایرلس است . در جدول زیر ، جزییات این استاندارد را بطور خلاصه مشاهده می کنید .

Ratified	1999
RF Technology	DSSS
Frequency Spectrum	2.4-GHz
Coding	Barker 11 and CCK
Modulation	DBPSK and DQPSK
Data Rates	1, 2, 5.5, 11 Mbps
Nonoverlapping Channels	1, 6, 11

پروتکل 802.11g :

این پروتکل در سال ۲۰۰۳ معرفی شد تا باز هم سرعت را افزایش دهد . 802.11g همچنان در محدوده ی فرکانسی 2.4GHz باقی ماند ، اما به حداکثر data rate برابر با 54Mbps رسید . در سرعت های پایین (تا 11Mbps) ، این پروتکل با 802.11b سازگار است و از همان مدولاسیون ها و کدینگ های پروتکل 802.11b استفاده می کند ؛ اما برای رسیدن به سرعت های بالاتر ، از OFDM (Orthogonal Frequency Division Multiplexing) به عنوان مدولاسیون استفاده می کند (802.11a نیز از OFDM استفاده می کند).

هنگامی که با OFDM کار می کنید ، باید مواظب توان خروجی باشید ؛ توان باید کاهش داده شود تا بتواند در مقادیر پیک ها ی مدولاسیون باقی بماند و در عین حال همچنان قوانین و آیین نامه های دولتی را رعایت کند .

در جدول زیر ، برخی جزئیات 802.11g را مشاهده می فرمایید :

Ratified	June 2003
RF Technology	DSSS and OFDM
Frequency Spectrum	2.4 GHz
Coding	Barker 11 and CCK
Modulation	DBPSK and DQPSK
Data Rates	1, 2, 5.5, 11 Mbps with DSSS 6, 9, 12, 18, 24, 36, 48, 54 Mbps with OFDM
Nonoverlapping Channels	1, 6, 11

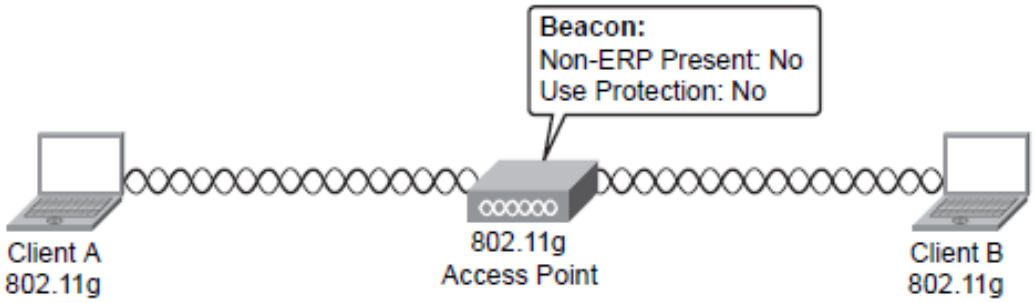
نحوه ی همکاری 802.11g با 802.11b :

نکته ی بسیار جالب در مورد 802.11g اینست که با اینکه با 802.11b کاملا سازگار است ، در صورت تمایل می توانید این قابلیت را غیر فعال کنید ؛ زیرا چنانچه بخواهید از کاربران 802.11b پشتیبانی کنید ، تمام سلول دچار مشکل سرعت پایین می شود . به عبارتی دیگر ، اگر میانگین پهنای باند در سلول 802.11g حدود 22Mbps باشد و یک کاربر 802.11b وارد شود ، کارایی کل آن سلول کاهش می یابد . علت این کاهش در کارایی ، اینست که 802.11b از OFDM پشتیبانی نمی کند . چنانچه در حالیکه کاربران 802.11g مشغول به ارسال هستند ، کاربران 802.11b نیز شروع به ارسال کنند ، collision رخ می دهد ؛ هرچند یک مکانیزم حفاظتی نیز وجود دارد که مانع از ایجاد این مشکل می شود . ابتدا دو عبارت را تعریف می کنیم :

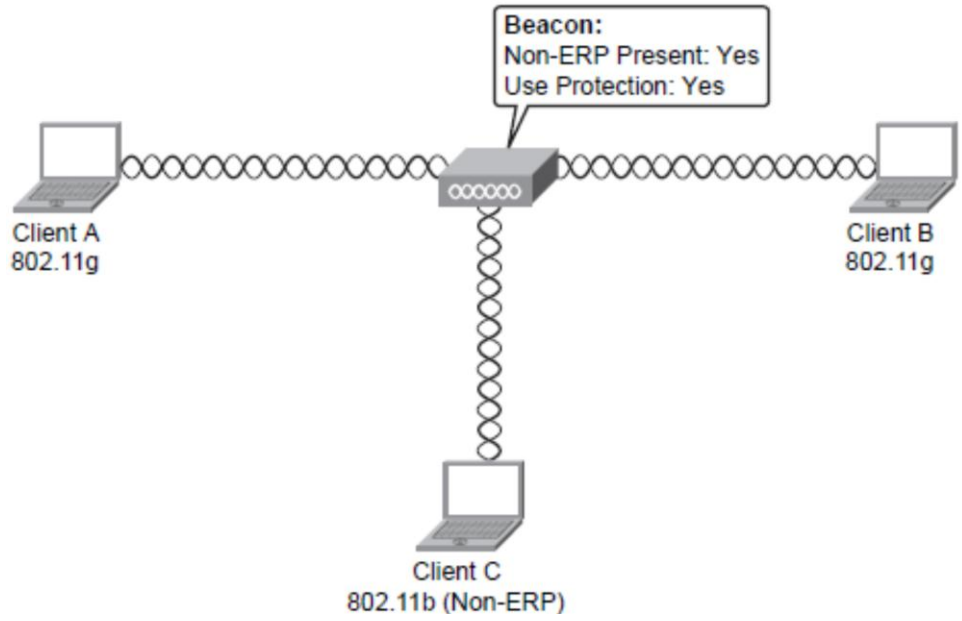
- ✓ **ERP** : Extended Rate Physical به کاربران پر سرعت اشاره دارد که از 802.11g استفاده می کنند ؛ مثل کاربران 802.11g که سرعت متوسط 22Mbps دارند .
- ✓ **Non-ERP** : به همه ی user هایی اشاره می کند که سرعت بالا ندارند ؛ یعنی آنهایی که از 802.11b استفاده می کنند و سرعت متوسط زیر 11Mbps دارند .

هنگامیکه هیچ کاربر 802.11b وجود نداشته باشد ، AP در beacon های خود اطلاعات زیر را ارسال می کند:

NON-ERP present: no
Use Protection: no



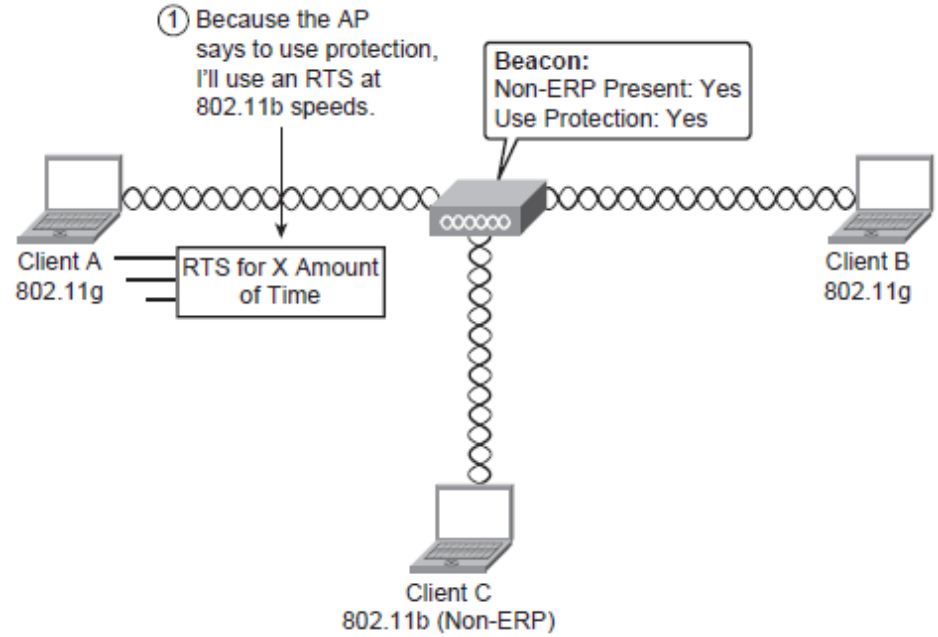
اما چنانچه یک کاربر 802.11b وارد شود (یعنی در واقع یک non-ERP در شبکه حضور داشته باشد) ، AP آن را در beacon خود اعلام می کند .



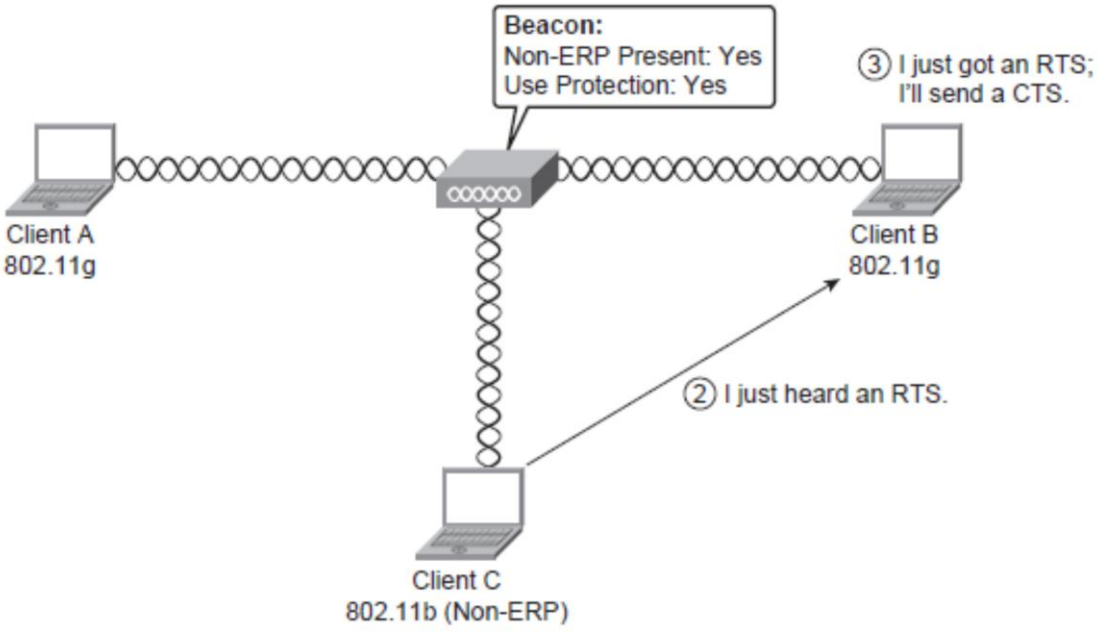
برای تشریح ادامه ی بحث ، باز هم لازم است ابتدا دو عبارت را تعریف کنیم :

- ✓ **RTS** : همانطور که از اسمش پیداست ،کاربران با ارسال Ready To Send ، به سایر client ها اعلام می کنند که آماده ی ارسال هستند . البته RTS یک پیام broadcast نیست ، بلکه یک پیام unicast است که به گیرنده 802.11g مورد نظر می رسد ، اما کاربران 802.11b نیز آن را درک می کنند .
- ✓ **CTS** : گیرنده ی RTS ، با ارسال Clear To Send ، به پیام RTS پاسخ می دهد .

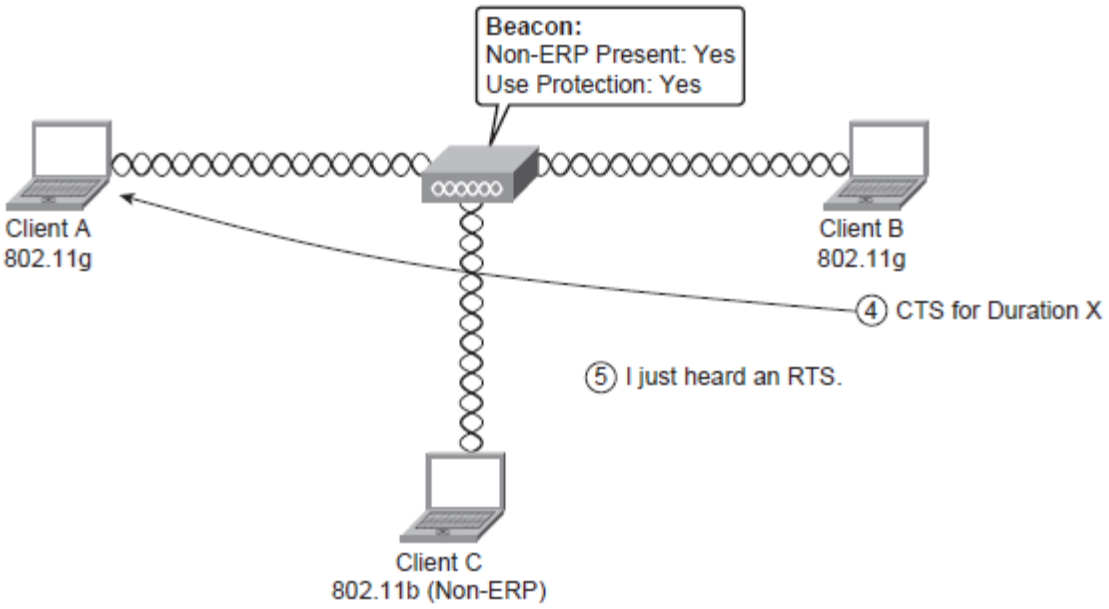
کاربران 802.11g که همان ERP ها هستند ، وقتی می خواهند با هم data را رد و بدل کنند ، ابتدا یک RTS با سرعت 802.11b ارسال می کنند ؛ که علاوه بر B ، کاربر C نیز این RTS را می شنود (چون با سرعت پایین ارسال شده است) .



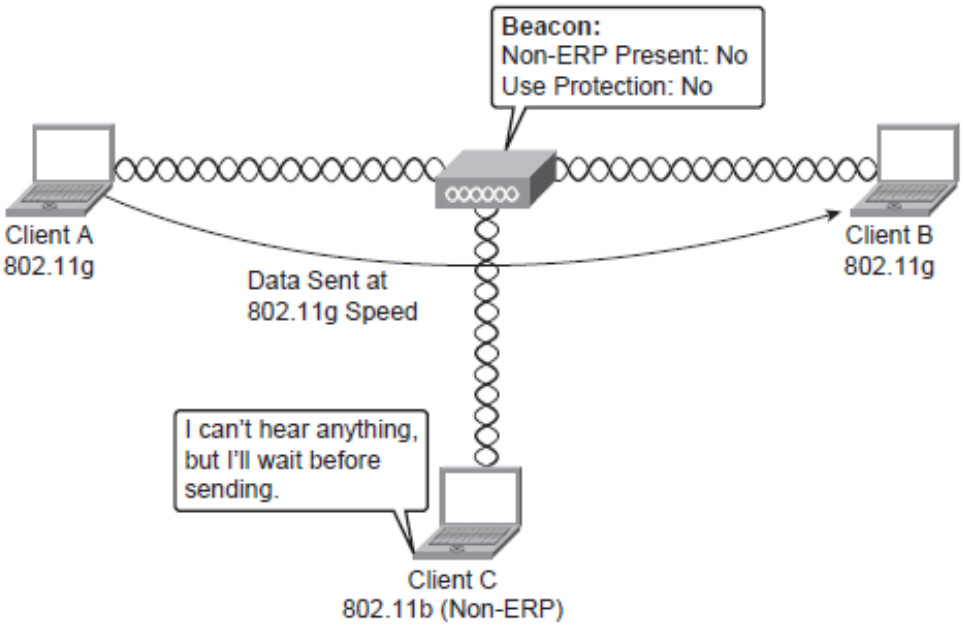
در RTS و CTS ، مدت زمان ارتباط مشخص شده است و کاربر C می داند که چه مدت زمانی باید صبر کند .



کاربر B یک CTS به A می فرستد که باز هم کاربر C نیز این پیام را می شنود .



در طول ارتباط ، تبادل دیتا با سرعت 802.11g انجام می شود و C نمی تواند آن را درک کند و در واقع فکر می کند که noise هستند ؛ اما باز هم تا زمان مشخص شده صبر می کند .



در روش RTS/CTS ، اصلا مهم نیست که کاربر 802.11b چقدر به فرستنده نزدیکتر است . اما در روش دیگری به نام CTS to self ، اگر کاربر 802.11b به فرستنده نزدیکتر نباشد ، ممکن است که نتواند پیام CTS to self را بشنود .

802.11b client یک تاثیر بد دیگر نیز بر شبکه ی 802.11g می گذارد و آن ، domino effect است . یعنی اگر یک AP در beacon خود تبلیغ کند که :

NON-ERP present: yes

Use Protection: yes

آنگاه AP دیگری که همسایه ی این AP است ، با شنیدن این beacon ، در تبلیغات خود اعلام می کند که :

NON-ERP present: no

Use Protection: yes

زیرا در شبکه ی خودش non-ERP ندارد ، اما برای محافظت از خود protection را فعال می کند . یعنی کاربران آن شبکه ، با آنکه کاملا 802.11g هستند ، اما باید عملیات protection را مرتبا (با سرعت پایین) انجام دهند .

پروتکل 802.11a :

این پروتکل در سال ۱۹۹۹ معرفی شد تا در محدوده ی فرکانسی 5GHz فعالیت کند ؛ این امر علاوه بر اینکه این پروتکل را با پروتکل های 802.11 ، 802.11b و 802.11g سازگار می کند ، مانع از به وجود آمدن تداخل با تجهیزات آن پروتکل ها می شود (زیرا همگی در محدوده ی فرکانسی 2.4GHz کار می کنند) . همچنین مانع تداخل با مایکروویو ، دستگاههای بلوتوث و تلفن های cordless می شود . البته این پروتکل هنوز به اندازه ی پروتکل های 802.11b/g معروف نشده است .

مزیت دیگر این پروتکل اینست که در همه جا بین ۱۲ تا ۲۳ کانال غیر همپوشان ارائه می دهد (که در برابر ۳ کانال پروتکل های قبلی خیلی زیاد است) .

802.11a از Convolution Coding استفاده می کند که یک نوع error correction است که در آن یک parity bit به دیتا اضافه می شود و این تصحیح خطا در طول همه ی subcarrier ها محاسبه می گردد . لذا اگر یک تداخل narrowband در روی یک subcarrier رخ داد و data را خراب کرد ، گیرنده می تواند بر اساس Convolution Coding روی یک subcarrier دیگر ، دیتا را بازسازی و ترمیم نماید .

در جدول زیر ، برخی جزئیات این پروتکل را مشاهده می کنید :

Ratified	1999
RF Technology	OFDM
Frequency Spectrum	5.0 GHz
Coding	Convolution Coding
Modulation	BPSK, QPSK, 16-QAM, 64-QAM depending on the subcarrie
Data Rates	6, 9, 12, 18, 24, 36, 48, 54 Mbps with OFDM
Nonoverlapping Channels	Each band has a 4; the middle 8 are used with 52 subcarriers c each channel.

چیزی که 802.11a را کاملا متفاوت و یکتا می سازد ، اینست که باند فرکانسی 5GHz را به چندین بخش تقسیم می کند که به هر کدام یک UNII می گویند (Unlicensed National Information Infrastructure) . هر UNII برای یک کاربرد طراحی شده است ؛ مثلا UNII-1 برای مصارف indoor با آنتن دائمی طراحی شده ، UNII-2 برای مصارف indoor یا outdoor با آنتن خارجی طراحی شده ، و UNII-3 برای outdoor bridge ها با آنتن های خارجی طراحی شده است .

Band	Frequency	Use
UNII-1	5.15–5.25 GHz (UNII Indoor)	FCC allows indoor and outdoor use.
UNII-2	5.25–5.35 GHz (UNII Low)	Outdoor/indoor with DFC and TPC
UNII-3	5.725–5.825 GHz (U-NII/ISM)	FCC allows indoor and outdoor use.
		ETSI does not allow unlicensed use.

در طیف فرکانسی 802.11a ، کانال های باند UNII-2 و بالاتر ، 30MHz فاصله دارند ، اما باندهای پایین تر 20MHz فاصله دارند .

پیش نیازهای توان 802.11a :

در جدول زیر ، قوانین توان را مشاهده می کنید که توسط FCC برای ایالات متحده امریکا وضع شده است . ستون وسط (Output Power) ، نشان دهنده ی توان خروجی در استفاده از آنتن omnidirectional با گین 6dBi است .

Band	Output Power Not to Exceed	EIRP Maximum
UNII-1	50 mW	22 dBm
UNII-2	250 mW	29 dBm
UNII-2 Extended	1 W	36 dBm
UNII-3	1W	36 dBm

البته ETSI قوانین خاص خود را برای اروپا وضع می کند که در مورد توان خروجی داریم :

Band	Output Power Not to Exceed	EIRP Maximum
UNII-1	200 mW	23 dBm
UNII-2	200 mW	23 dBm
UNII-2 Extended	1 W	30 dBm
UNII-3	Licensed use only	—

پروتکل 802.11n :

در زمان نگارش کتاب CCNA Wireless زبان اصلی سال ۲۰۰۹) ، این پروتکل هنوز در حد یک نسخه ی پیش نویس (draft) بود ، اما هم اکنون یک استاندارد است . البته مدتها قبل از اینکه 802.11n به عنوان یک استاندارد معرفی شود ، چند vendor از AP ها و client های 802.11n استفاده می کردند ؛ که این هم خود نشان دهنده ی سرعت رشد بالای تکنولوژی نسبت به استانداردهاست .

چیزی که این پروتکل را بی همتا می سازد اینست که در یک محیط تماما 802.11n ، شما می توانید به سرعت 300Mbps برسید ! (البته بر اساس بیشتر اسناد ، این پروتکل معمولا سرعت 100Mbps را ارائه می دهد ، که شاید علت این امر ، وجود کاربران پروتکل های دیگر است ؛ به عبارتی سازگاری این پروتکل با 802.11b/g/a موجب این کاهش سرعت می شود.)

سازگاری با پروتکل های قبلی و نیز قابلیت سرعت 802.11n ، ناشی از استفاده از آنتن ها و تکنولوژی های چندگانه است که MIMO نامیده می شود (Multiple-Input , Multiple-Output). MIMO از چندین آنتن برای ارسال و دریافت استفاده می کند که این امر throughput را افزایش می دهد . MIMO در سه حالت کار می کند :

۱. **Precoding** : در این حالت فرستنده چندین آنتن دارد و گیرنده تنها یک آنتن ثابت دارد . precoding از آنتن های چندگانه استفاده می کند و از فناوری TxBF بهره می جوید . در این فناوری ، اطلاعات ارسالی روی چندین آنتن ارسال می شوند و در گیرنده ، کیفیت data تا حد مطلوبی بهبود می یابد . البته این فناوری برای زمانیست که receiver ثابت باشد ؛ زیرا اگر گیرنده متحرک باشد ، دیگر امکان هماهنگ کردن data وجود ندارد (زیرا ویژگی های reflection آنتن در حال تغییر خواهد بود) . به این روش از coordination ، در واقع CSI می گویند (Channel State Information) .

۲. **Spatial Multiplexing** : در این حالت فرستنده چندین آنتن و گیرنده نیز چندین آنتن دارد . دیتا به stream هایی با سرعت پایین تر تقسیم می شود و هرکدام روی یک آنتن مجزا ، اما با فرکانس یکسان ارسال می شوند . تعداد stream ها برابر با کمترین تعداد آنتن ها در فرستنده یا گیرنده است ؛ یعنی مثلا اگر یک AP چهار آنتن دارد و client دو آنتن دارد ، شما محدود به ۲ هستید .

۳. **Diversity Coding** : در این حالت ، برخلاف حالت spatial multiplexing که از چندین stream استفاده می شد ، تنها یک stream ارسال می شود ، اما سیگنال توسط تکنیک هایی که Space-time Coding نامیده می شوند ، کد می گردد .

802.11n با سایر پروتکل های 802.11 تفاوت های دیگری نیز دارد . مثلا در لایه ی فیزیکی ، بسته به روشی که سیگنال ارسال شده است ، در مورد عکس العمل ها و تداخل ها تصمیم گیری می شود که این امر یک مزیت به حساب می آیند نه یک عیب . روش دیگری که برای افزایش throughput بکار می رود، ترکیب و تراکم کانال هاست (Channel Aggregation) . 802.11n از کانال های 20MHz و 40MHz استفاده می کند که کانال های 40MHz ، در واقع دو کانال 20MHz مجاور هستند که با هم ترکیب شده اند .

ارسال فریم ها :

802.11n تنها از روش CTS to self برای ارسال فریم ها استفاده می کند و از روش RTS/CTS استفاده نمی کند .

همچنین 802.11n به جای تایید کردن هر پکت unicast (کاری که سایر پروتکل های 802.11 انجام می دهند) ، یک بلوک از فریم ها را به یکباره Acknowledge می کند (مانند کاری که TCP انجام می دهد).

همچنین این پروتکل به جای استفاده از DIFS ، از RIFS استفاده می کند . البته در فصل آینده با این مفاهیم بطور کامل آشنا خواهیم شد ، اما بطور خلاصه ، تکنولوژی DIFS (Distributed Interframe Space) می گوید که هر sending station باید صبر کند تا یک فریم ارسال شود ، سپس فریم بعدی را ارسال کند ، که این باعث تولید overhead زیادی می گردد . 802.11n با استفاده از RIFS (Reduced Interframe Space) ، تاخیر و overhead را تا حد زیادی کم کرده و بهبود بخشیده است .

ملاحظات مربوط به آنتن ها :

هنگامیکه در datasheet ها می بینیم که مثلا نوشته شده : **2x2** ، این به معنای آنست که فرستنده روی ۲ آنتن ارسال می کند و دو تا data stream دارد ، و گیرنده روی ۲ آنتن دریافت می کند و دو تا receive chain دارد . همچنین **3x3** به معنای ۳ تا data stream و ۳ تا receive chain می باشد .

این مسئله از آنجا مهم است که در cisco 1250 AP ، این مقدار برابر با **2x3** است . در چنین شرایطی ، ما محدود به کمترین تعداد آنتن هستیم ؛ لذا در این AP نیز ما دو stream داریم .

در پایان به این نکته توجه داشته باشید که حتی اگر شما کاربران **802.11n** هم نداشته باشید ، با توجه به قابلیت های این پروتکل ، می توانید توقع داشته باشید که کارایی شبکه ی شما تا حدود ۳۰ درصد بهبود یابد .

فصل هفتم : آشنایی با Traffic Flow و AP Discovery در شبکه وایرلس

- ارسال یک فریم
  - SIFS ✓
  - PIFS ✓
  - DIFS ✓
  - Backoff Timer ✓
  - Slottime ✓
  - NAV ✓
  - Contention Window ✓
  - DCF ✓
  - PCF ✓
- Wireless Frame Header
  - SA ✓
  - TA ✓
  - DA ✓
  - RA ✓
- فریم های مدیریتی
- Beacon ها
- Passive / Active Scanning
- متصل شدن پس از probe یا beacon
- فریم های کنترلی
- Power save Mode
- A Wireless Connection

بیشتر افراد به اشتباه گمان می کنند که شبکه های wireless مانند 802.3 LAN ها کار می کنند . درصورتیکه LAN های 802.3 از آدرس های MAC استفاده می کنند ، اما LAN های وایرلس از ساختار فریم 802.11 استفاده می نمایند . در این فصل با سه نوع فریم وایرلس آشنا می شویم تا درک بهتری از عملکرد Wireless LAN ها بدست آوریم . همچنین نگاهی عمیق تر به Interframe Spacing (IFS) خواهیم داشت تا چرایی لزوم استفاده از آن را بهتر متوجه شویم .

در ابتدا ، با سه نوع فریم موجود در Wireless LAN ها آشنا می شویم :

- **Management Frames** : برای پیوستن یا ترک کردن یک سلول وایرلس به کار می رود . این نوع فریم شامل درخواست association ، پاسخ به آن ، درخواست دوباره و ... می باشد .
- **Control Frames** : برای تایید اینکه فریم های دیتا (data frames) دریافت شده اند .
- **Data Frames** : فریم هایی که حاوی دیتا ی اصلی هستند .

ارسال یک فریم :

همانطور که در فصل های قبل نیز اشاره کردیم ، شبکه های وایرلس ، half-duplex هستند ، لذا اگر بیش از یک دستگاه در آن واحد بخواهند ارسال انجام دهند ، collision بوجود می آید ؛ که این خود باعث اتلاف زمان و منابع می شود . Wireless LAN ها برای مقابله با این مشکل از CSMA/CA استفاده می کنند (Carrier Sence Multiple Access Collision Avoidance) . بخش carrier sence به معنای اینست که هر station باید تشخیص دهد که آیا کسی در حال ارسال است یا خیر ؛ که این امر بوسیله ی Clear Channel Assessment (CCA) انجام می شود . به عبارت دیگر ، CCA با انجام carrier sense در واقع دارد به خط گوش می دهد تا بفهمد که آیا station دیگری در حال Send کردن هست یا خیر .

البته ممکن است شرایطی پیش آید که دو device نتوانند به یکدیگر گوش دهند که به این حالت Hidden Node Problem می گویند . برای حل این مشکل نیز باید از Virtual Carrier Sence (VCS) کمک بگیریم .

ذکر این نکته ضروریست که medium ارتباط ، تنها در صورتی available خواهد بود که هم virtual carrier و هم physical carrier گزارش بدهند که خط آماده است .

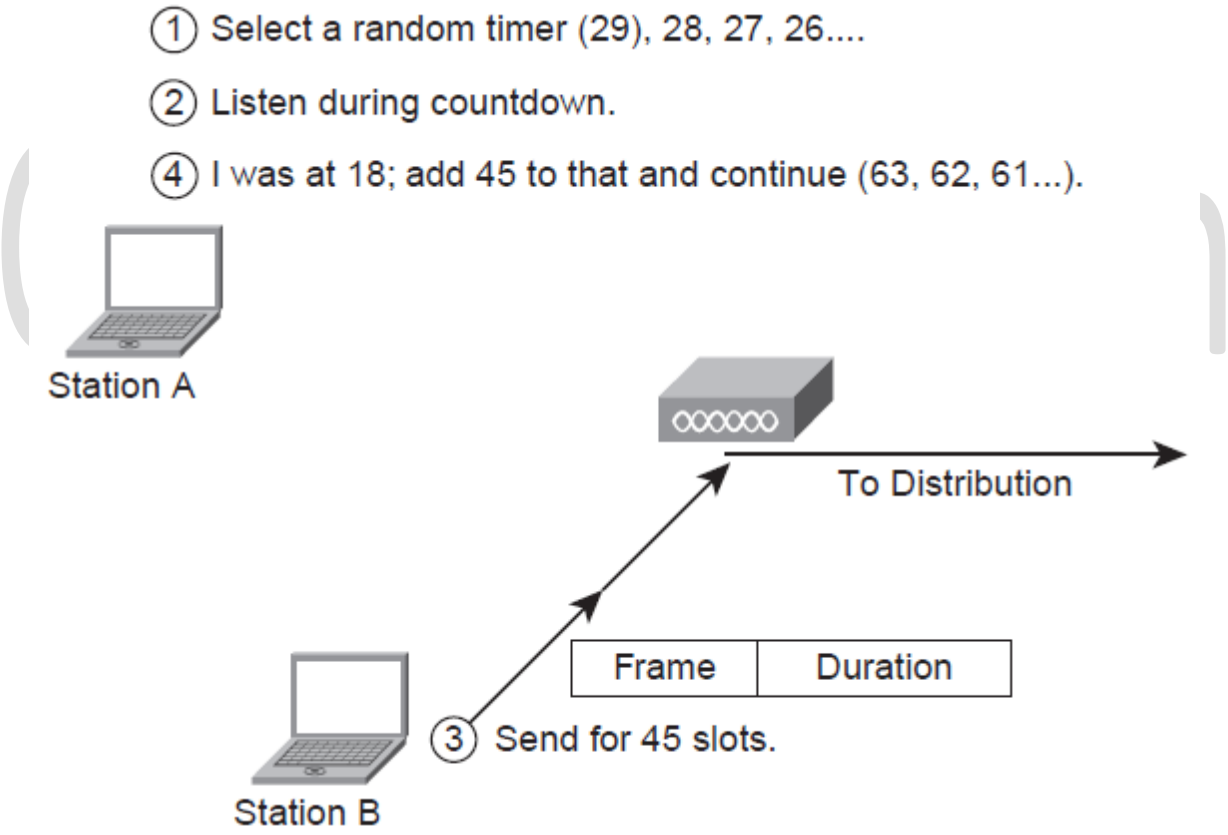
همچنین هر station باید IFS را نیز درک کند . Interframe Spacing ، مدت زمانیست که station ها قبل از اینکه ارسال کنند ، باید صبر کنند . IFS ، هم clear بودن medium را اعلام می کند و هم اطمینان می دهد که فریم ها با فاصله ارسال می شوند تا به اشتباه ترکیب و ترجمه غلط نشوند . پریود های IFS سه نوع هستند :

- **Short Interframe Space (SIFS)** : برای اولویت های بالاتر ، و نیز برای ACK .
- **Point-coordination Interframe Space (PIFS)** : برای زمانیکه AP می خواهد شبکه را کنترل کند .
- **Disributed-coordination Interframe Space (DIFS)** : فاصله ی نرمال بین فریم های دیتا را فراهم می کند .

هنگامیکه باید یک فریم را به سرعت ارسال کنیم ، از SIFS استفاده می کنیم . مثلا هنگامیکه یک فریم دیتا باید تایید شود ، قبل از اینکه بقیه ی station ها شروع به ارسال کنند ، ACK باید فرستاده شود . ارزش زمانی DIFS بیشتر از SIFS است ، لذا SIFS از DIFS پیشدستی می کند ، زیرا اولویت بالاتری دارد .

در ادامه ، ابتدا دو عبارت را تعریف کرده و سپس با یک شکل ، یک نمونه ارسال فریم را تشریح خواهیم کرد .

- **Backoff Timer** : قبل از اینکه عملیات ارسال شروع شود ، کاربر باید گوش کند (listen) . برای این کار، کاربر یک شماره ی تصادفی را انتخاب می کند و شروع به شمارش معکوس می نماید که در واقع به آن Backoff Timer می گویند .
- **Slottime** : سرعتی است که عملیات شمارش معکوس (countdown) رخ می دهد و در هر کدام از پروتکل های 802.11a/b/g متفاوت است . (می توان به آن سرعت شمارش نیز گفت .)

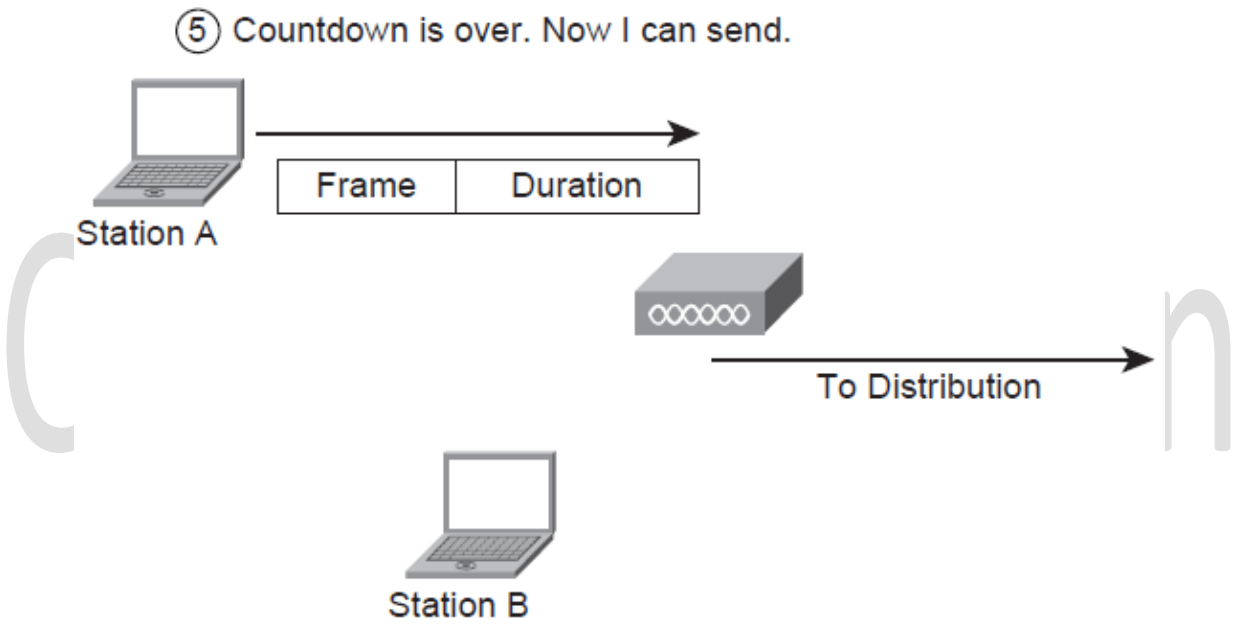


در این شکل ، پس از اینکه stationA بصورت رندم ، عدد ۲۹ را انتخاب نمود ، شمارش معکوس آغاز می شود . اما هنگامیکه شمارش به عدد ۱۸ می رسد ، stationB یک فریم ارسال می کند که دارای ارزش زمانی ۴۵ است . stationA این مقدار را به عدد ۱۸ اضافه می کند و شمارش معکوس خود را ادامه می دهد (این فرآیند NAV نام دارد) .

برای تشریح ادامه ی پروسه ی ارسال ، دو عبارت دیگر را تعریف می نماییم :

- **Network Allocation Vector (NAV)** : NAV شامل مدت زمان ارسال فریم ، زمان SIFS ، و در نهایت زمان دریافت ACK از طرف AP می باشد . وقتی client یک فریم را ارسال می کند ، در header آن فریم یک NAV می گذارد که در واقع با این کار ، medium را برای مدت زمان خاصی رزرو می کند .
- **Contention Window** : مدت زمانیکه یک station باید صبر کند تا نوبت send کردنش فرا برسد . این زمان شامل Backoff Timer اولیه ، و همه ی NAV هاییست که station های دیگر ارسال می کنند و با backoff اولیه جمع می شود .

پس از به پایان رسیدن countdown ، بالاخره stationA به زمان ۰ می رسد و می تواند ارسال را آغاز کند .



چنانچه stationA ارسال کند ، اما fail شود ، دوباره یک شماره ی random انتخاب کرده و شمارش معکوس را آغاز می کند . هر بار که عملیات ارسال fail شود ، backoff timer بزرگتر می شود ؛ برای مثال اگر اولین تایمر ، عددی بین ۰ تا ۳۱ باشد ، بعد از یک بار fail شدن ، عددی بین ۰ تا ۱۲۷ خواهد بود ، و همینطور الی آخر .

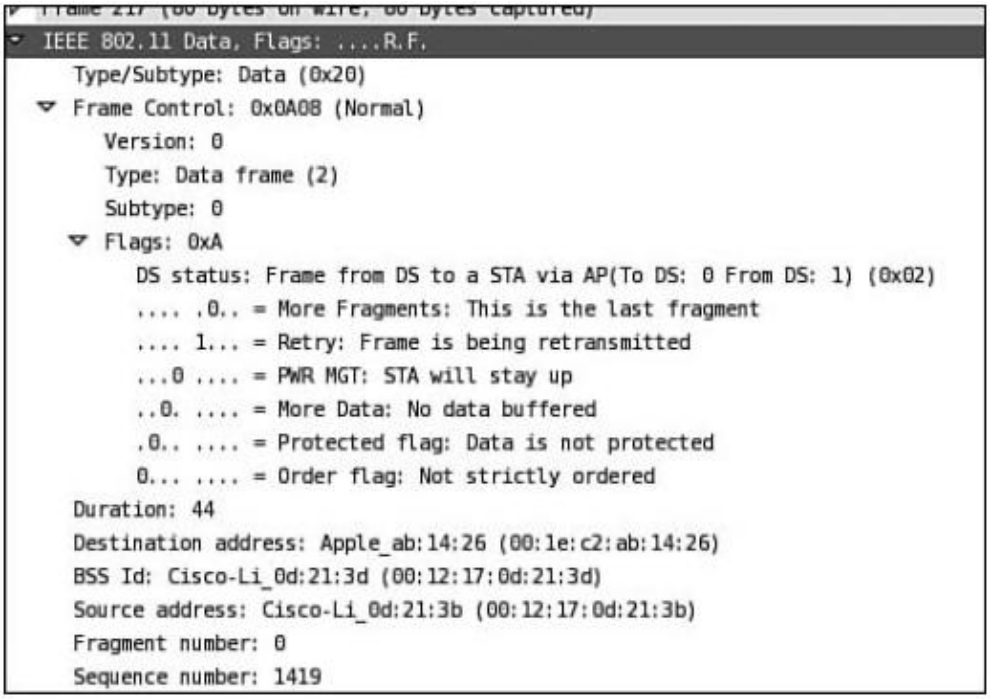
تمام این فرآیند **Distributed Coordination Function (DCF)** نام دارد ؛ به این معنی که هر station نسبت به هماهنگی برای ارسال دیتای خودش مسئول است (از distribute می توان فهمید که در این عملیات ، بین همه ی station ها تقسیم کار صورت گرفته است).

برای DCF ، یک جایگزین به نام **Point Coordination Function (PCF)** وجود دارد که به معنای اینست که فقط AP مسئول هماهنگی ارسال دیتا می باشد .

نکته ی : برخی فواصل و سکوت ها بین فریم ها طبیعی است و SIFS کوتاهترین پریود سکوت بین فریم هاست .

Wireless Frame Header :

در شکل زیر ، یک فریم وایرلس را مشاهده می فرمایید :



برخی نکات در مورد این فریم قابل توجه است :

- ✓ در فیلد Flags ، می بینیم که نوشته شده : frame **from** DS (توجه کنید ، نگفته که : frame **toward** DS) . این جمله به این معناست که این فریم در حال برگشتن از مقصد به سمت client می باشد .
- ✓ فیلد Duration مشخص می کند که medium برای چه مدت زمانی رزرو شده است (مدت زمانیکه این فریم در حال ارسال شدن است) و شامل زمان ارسال ACK و نیز reply آن نیز می شود . علت وجود این فرآیند ، جلوگیری از ایجاد collision است .
- ✓ یک فریم وایرلس می تواند تا ۳ آدرس MAC داشته باشد که در فیلد Duration می آید . مثلا در اینجا داریم :

۱. Destination MAC Address
۲. BSS ID که خود یک آدرس MAC است .
۳. Source MAC Address

- ✓ از آنجا که طول فریم وایرلس ۲۳۴۶ بایت است ، اگر این فریم بخواهد از Ethernet distribution بگذرد ، دچار مشکل می شود ؛ زیرا MTU در این محیط ۱۵۰۰ بایت است (و بسته به نوع trunking ، می تواند فریم هایی تا ۱۵۱۸ بایت را نیز ببینند) . لذا باید از fragmentation استفاده نموده و این فریم وایرلس را چند تکه کنیم .

در کل می توان ۴ نوع آدرس MAC را تعریف کرد که در شبکه های وایرلس مورد استفاده قرار می گیرند :

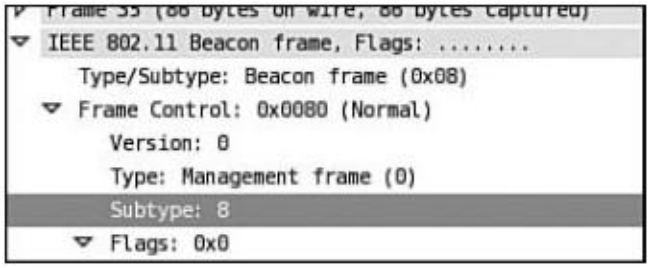
- **Source Address (SA)** : آدرس device ارسال کننده ی دیتا است ، یعنی اولین دستگاهی که دیتا از آن شروع به حرکت در شبکه می کند .
- **Transmitter Address (TA)** : آدرس دستگاهی که دیتا را تشعشع می کند (emitting device) . گاهی اوقات ممکن است این آدرس با SA متفاوت باشد . مثلا زمانیکه کاربر به یک repeater متصل باشد ، TA همان آدرس رادیوی repeater است .
- **Destination Address (DA)** : آدرس دستگاه گیرنده ی نهایی.
- **Receiving Address (RA)** : آدرس direct station که این فریم به آن ارسال می گردد (برای زمانی که فریم توسط یک wireless bridge یا repeater تقویت و رله می گردد) .

در نهایت ، فریم وایرلس درون یک Frame Body قرار می گیرد که مانند هر فریم لایه ۲ دیگری ، دارای ۲ آدرس MAC مبدا و مقصد است . Frame Body درون آخرین header نشان داده شده در شکل قبل ، encapsulate می شود . همچنین ممکن است یک FCS نیز در انتهای فریم لایه دو اضافه شود . در جدول زیر می توانید انواع فریم ها را مشاهده فرمایید . در ادامه بحث ، هر نوع از فریم ها را به تفصیل تشریح خواهیم کرد .

Management	Control	Data
Beacon	Request to Send (RTS)	Simple data
Probe Request	Clear to Send (CTS)	Null function
Probe Response	Acknowledgment	Data+CF-ACK
Association Request	Power-Save-Poll (PS-Poll)	Data+CF-Poll
Association Response	Contention Free End (CF-End)	Data+CF-Ack
Authentication Request	Contention Free End + Acknowl-edgment (CF-End +ACK)	ACK+CF-Poll
Authentication Response	CF-ACK	
Deauthentication	CF-ACK+CF-Poll	
Reassociation request		
Reassociation response		
Announcement traffic indication message (ATIM)		
Each frame type merits its own discussion to follow.		

فریم های مدیریتی :

همانطور که از نام این نوع فریم پیداست ، برای مدیریت ارتباط مورد استفاده قرار می گیرد . در این فریم ها ، **type** می گوید که این فریم management است و **subtype** آن می کوید که چه نوعی از فریم مدیریتی است .

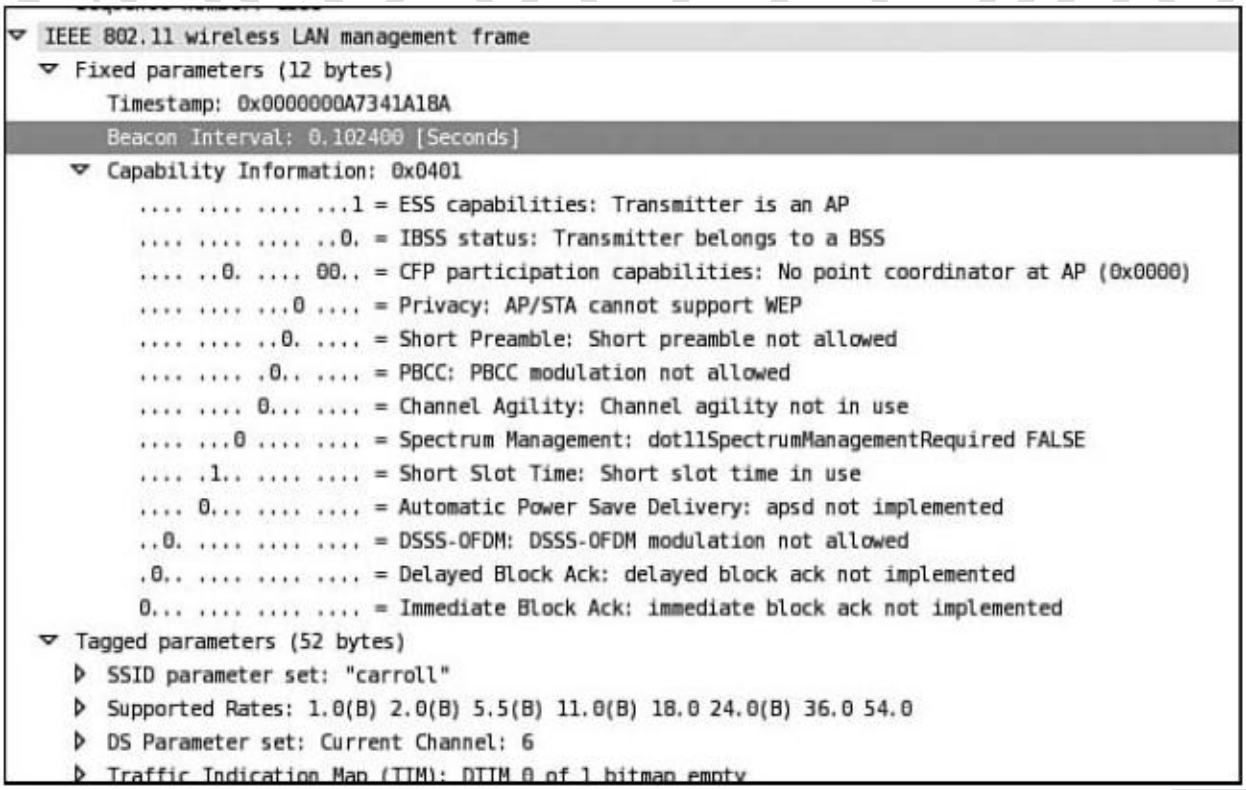


مثلا در این شکل ، شماره ی ۸ در subtype ، نشان دهنده ی اینست که این فریم ، یک beacon است .

Beacon ها :

فریم های beacon به کاربران کمک می کنند تا شبکه را پیدا کنند .

هنگامیکه client یک فریم beacon را دریافت می کند ، می تواند اطلاعات زیادی در مورد آن سلول بدست آورد . فریم beacon شامل SSID ها ، ساپورت های AP (مانند سرعت هایی که ساپورت می شوند) ، و ۶ فیلد به نام Parameter set می باشد که نشان دهنده ی متد های مدولاسیون و .. می باشند . در شکل زیر ، یک فریم beacon را با برخی از فیلد های آن مشاهده می نمایید .

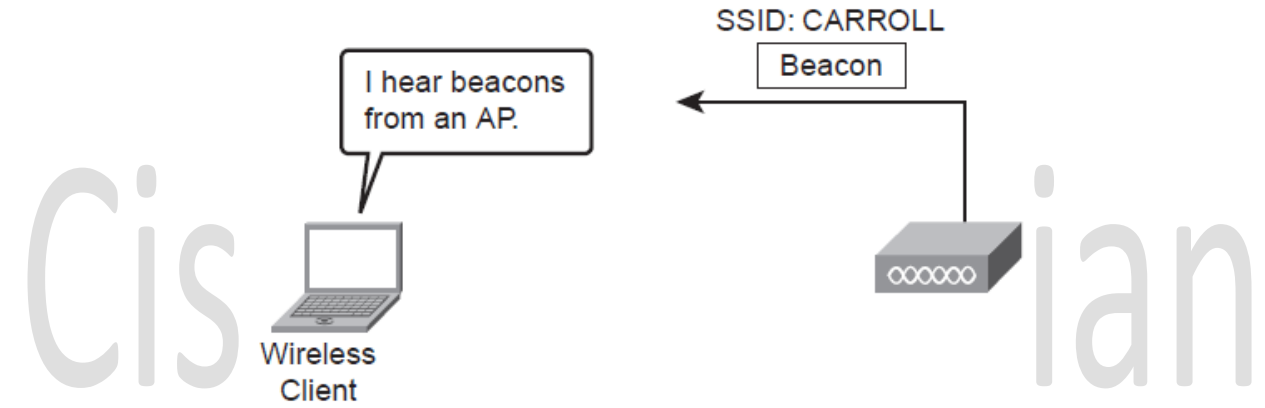


یکی از فیلد های فریم beacon ، فیلد **Capability Information** است که شامل اطلاعاتی در مورد power save mode ، authentication ، و سایر اطلاعات ابتدایی است .

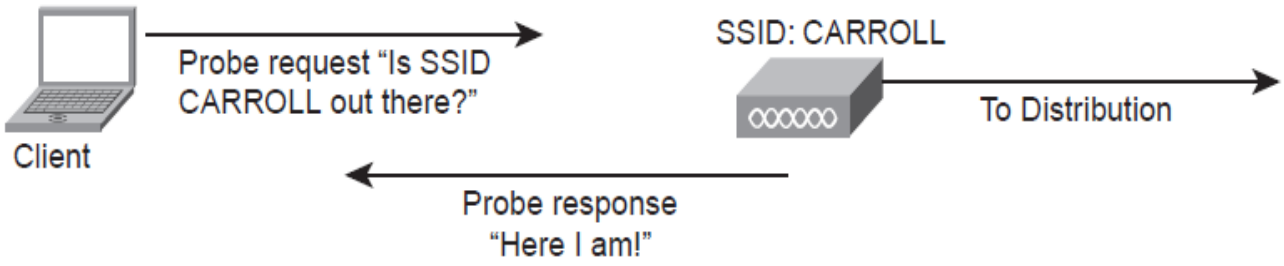
یکی دیگر از فیلدهای فریم beacon ، **TIM** است (Traffic Indication Map) که مشخص می کند که آیا AP ترافیک را برای client هایی که در حالت power-save mode هستند ، buffer می کند یا خیر .

فرآیند جستجو و یافتن شبکه توسط client ها به دو صورت انجام می گیرد :

- **Passive Scanning** : وقتی client هیچ گونه اطلاعاتی در مورد cell ندارد ، فقط منتظر می ماند و به beacon هایی که از AP ها می آیند گوش می دهد و از هر کدام ، اطلاعاتی در مورد cell های مختلف کسب می کند . این beacon ها به client اجازه می دهند تا شبکه را بصورت passive اسکن نمایند و این فرآیند ، Passive Scanning نام دارد .



- **Active Scanning** : اگر اطلاعات خاصی در مورد شبکه ای داشته باشیم (مثل هنگامیکه بخواهیم به یک cell خاص وصل شویم) ، در اینصورت می توان شبکه را بصورت active اسکن کرد . لذا باید از پیام های probe request و probe response برای پیدا کردن AP مورد نظر استفاده کرد ؛ این فرآیند ، Active Scanning نام دارد .

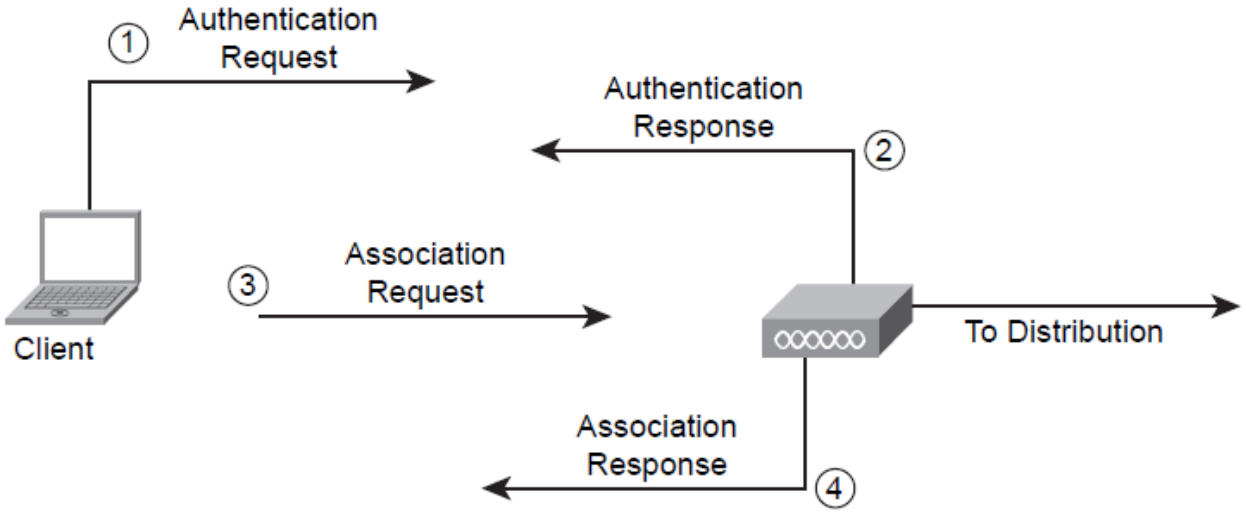


Probe response شبیه فریم beacon است و شامل اطلاعات capability ، اطلاعات authentication و ... می باشد . تنها تفاوت آنها در اینست که فریم beacon مرتبا ارسال می شود ، اما probe response تنها در پاسخ به یک probe request ارسال میگردد .

متصل شدن پس از probe یا beacon :

پس از ارسال فریم های مدیریتی beacon یا probe ، هر client برای وصل شدن باید فریم های مدیریتی authentication را ارسال کند که حاوی شماره ای برای authentication transaction (داد وستد در مورد احراز هویت) ، اطلاعاتی در مورد الگوریتم مورد استفاده در authentication ، و اطلاعاتی در مورد اینکه آیا اصلا این عملیات authentication موفق شده یا شکست خورده ، می باشد . (پس از این مرحله ، فریم های association رد و بدل می شوند تا مشارکت را بوجود آورد و در نهایت client بتواند عضو شبکه شود .)

نکته : وقتی می گوییم authentication میتواند open باشد ، این به این معناست که از هیچ authentication algorithm (مثل WEP) استفاده نمی شود . تنها علتی که از یک authentication message استفاده می شود ، اینست که بفهمیم آیا یک client قابلیت و توانایی اتصال به شبکه را دارد یا خیر .



همیشه client پیام request برای authentication را ارسال می کند و AP این پیام را response می کند .

خارج شدن از شبکه و اتصال مجدد :

هنگامیکه یک client به یک سلول متصل شد ، هم client و هم AP ، می توانند با ارسال پیام deauthentication ، ارتباط را قطع کنند . همچنین client می تواند پیام diassociation را ارسال کند که ارتباط client را قطع می کند ، اما اطلاعات authentication او را نگه می دارد و بار دیگر که client خواست دوباره به شبکه وصل شود ، دیگر نیازی به طی مراحل authentication نمی باشد .

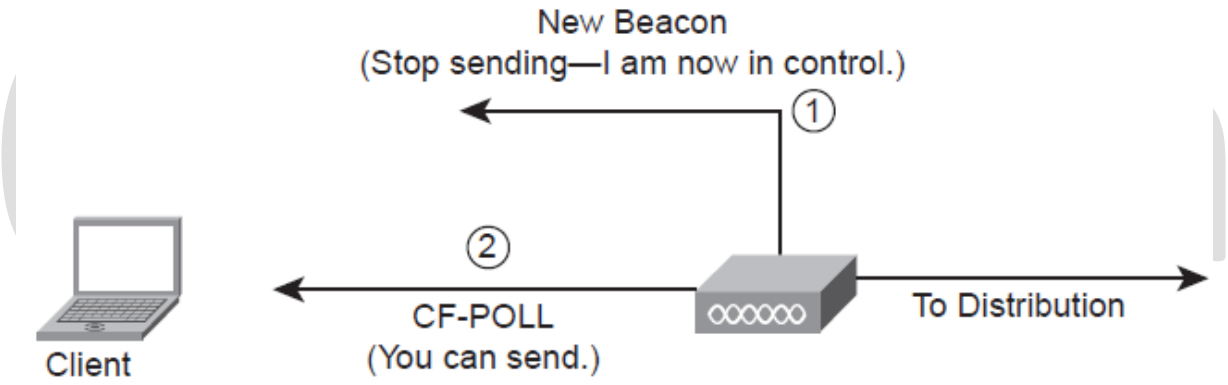
فریم های کنترلی :

معروفترین فریم کنترلی ، ACK می باشد . همچنین از دیگر فریم های کنترلی می توان RTS و CTS را نام برد (که در فصل ۶ مورد بررسی قرار گرفتند) . فریم های ACK ، RTS و CTS در حالت DCF به کار می روند .

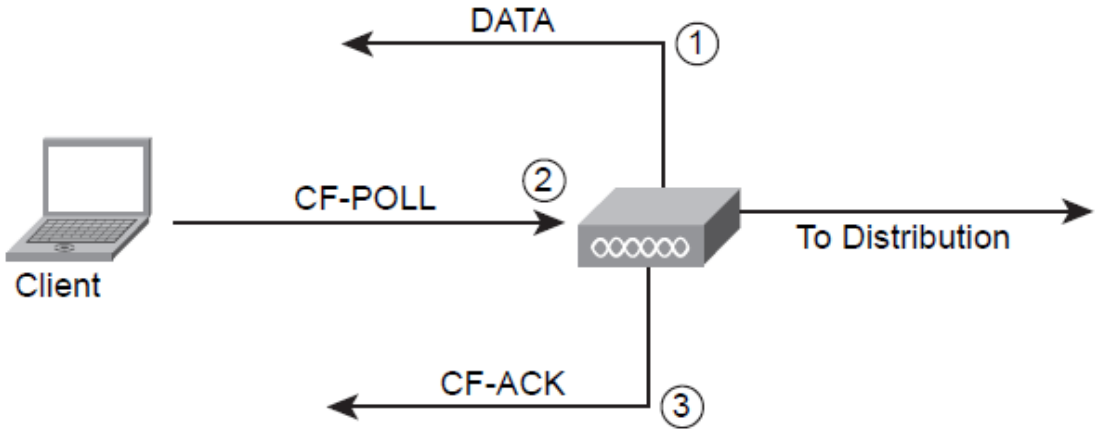
فریم های کنترلی که در حالت **PCF** به کار می روند عبارتند از : CF+End ، CF+end_ack_ ، CF-Ack ، CF Ack+CF Poll ، و CF-Poll . (CF = Contention Free)

در حالت **DCF** ، هر station خودش مسئول ارسال است ، لذا درگیری بر سر medium خیلی زیاد است . اما در حالت PCF ، تمام مسئولیت station ها با AP است ؛

AP یک beacon با طول زمانی 32768 می فرستد که در واقع همه ی station ها را مجبور می کند که ارسال را متوقف کرده و فقط listen کنند . لذا هیچ درگیری بر سر medium وجود ندارد ؛ به این حالت **CFW** می گویند (Contention Free Window) . سپس AP یک Poll message به هر کاربر می فرستد که آیا چیزی برای ارسال دارید یا خیر (که به این کار CF-Poll می گویند) . در شکل زیر CF-Poll را در حالت PCF می بینید :



در شکل زیر نیز می توانید نحوه ی کنترل ارتباطات توسط AP را مشاهده فرمایید . AP به client اجازه می دهد که data را بفرستد (CF-Poll) و سپس دریافت آن را تایید می کند (CF-ACK) .



Power Save Mode :

خیلی از مواقع دیده می شود که لپ تاپ در حالت ذخیره ی انرژی است (زمانیکه به آداپتور متصل نیست و از شارژ باطری خود استفاده می کند). در حالت power save ، یک client با استفاده از یک null function frame ، به AP خبر می دهد که به حالت sleep رفته است . پس از یک مدت زمان مشخص ، client از حالت sleep بیرون می آید (از خواب بیدار می شود) و می بیند که در این مدت ، AP همه ی ترافیک هایی که به سمت این client می آمده را buffer کرده است . هنگامیکه client یک فریم beacon می بیند که در فیلد TIM آن ، ترافیک های بافرشده لیست شده اند ، یک PS-Poll ارسال می کند و دریافت دیتا را از AP تقاضا می نماید (Power Save Poll).

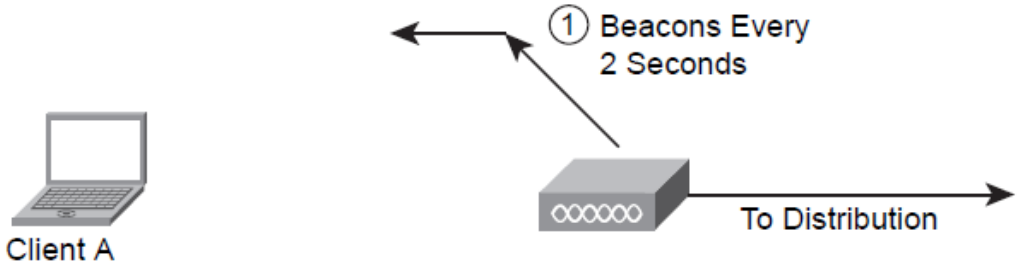
نکته : AP همه ی سرعت های الزامی (mandatory) را در advertisement خود تبلیغ می کند . همه ی client ها باید حتما این سرعت های mandatory را ساپورت کنند ، اما می توانند از سرعت دیگری استفاده کنند و ارسال و دریافت انجام دهند .

نکته : هنگامیکه data در یک rate ارسال می شود ، ACK همیشه در یک data rate پایین تر ارسال می کردد .

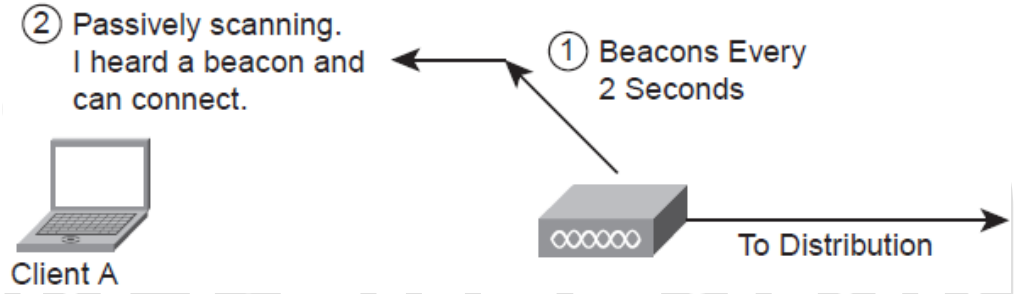
A Wireless Connection :

در پایان این فصل ، می توانیم فرآیند کامل اتصال به شبکه ی وایرلس را بطور کامل بررسی کنیم .

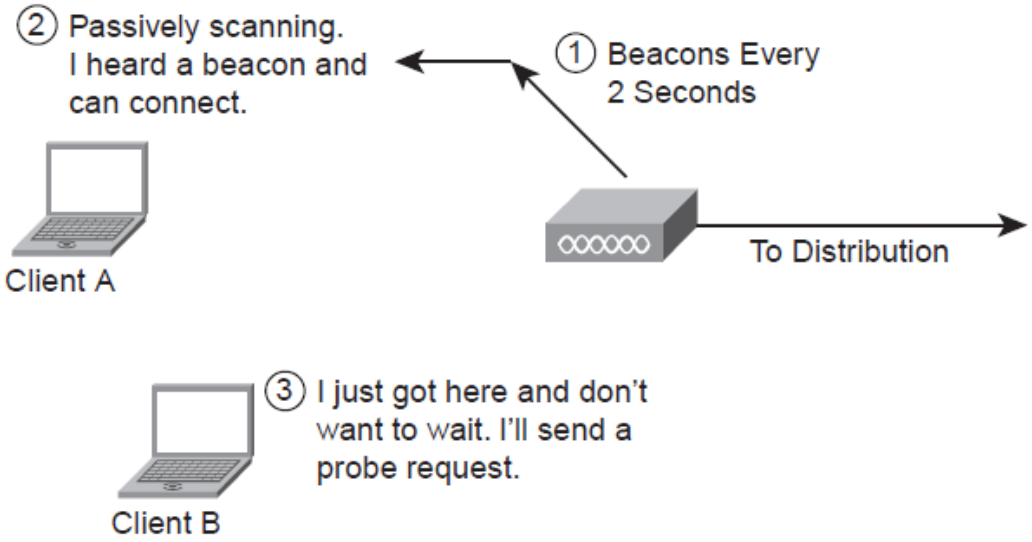
۱. AP هر ۲ ثانیه یکبار beacon های خود را ارسال می نماید .



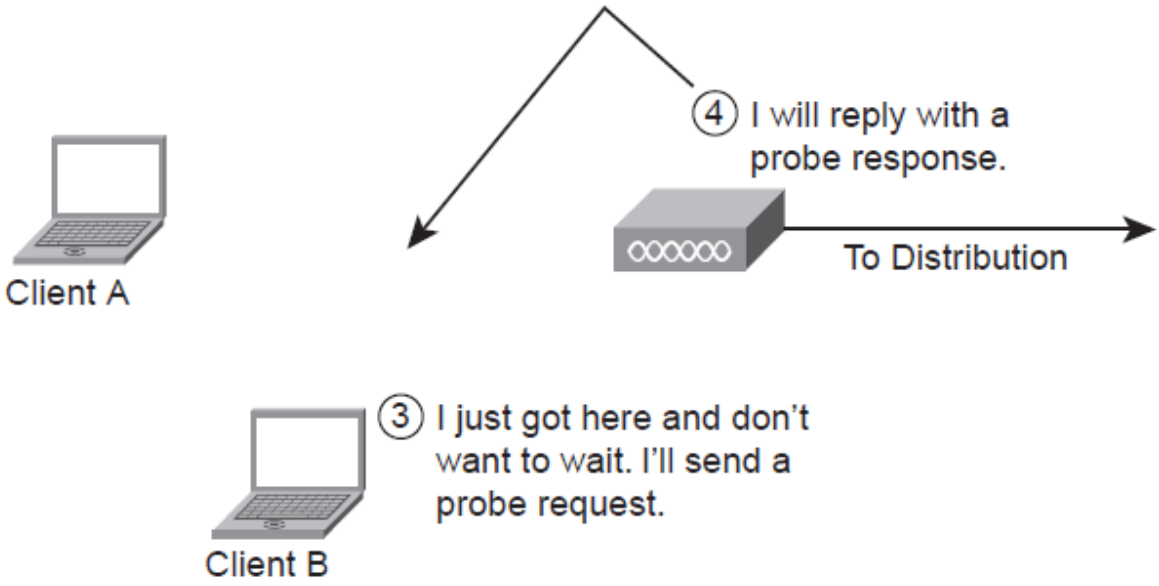
۲. clientAکه بصورت passive شبکه را اسکن می کند ، beacon را می شنود .



۳. در این زمان ، clientB وارد شبکه می شود و بصورت active شبکه را در جستجوی AP خاصی ، اسکن می نماید .

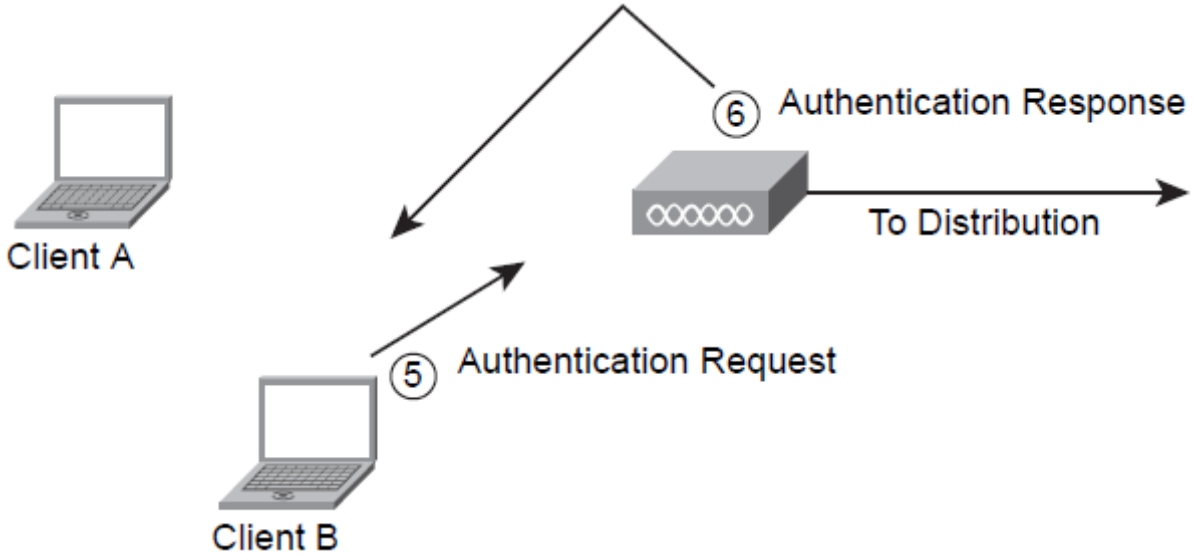


۴. AP در پاسخ به clientB ، یک probe response می فرستد که شبیه beacon است .



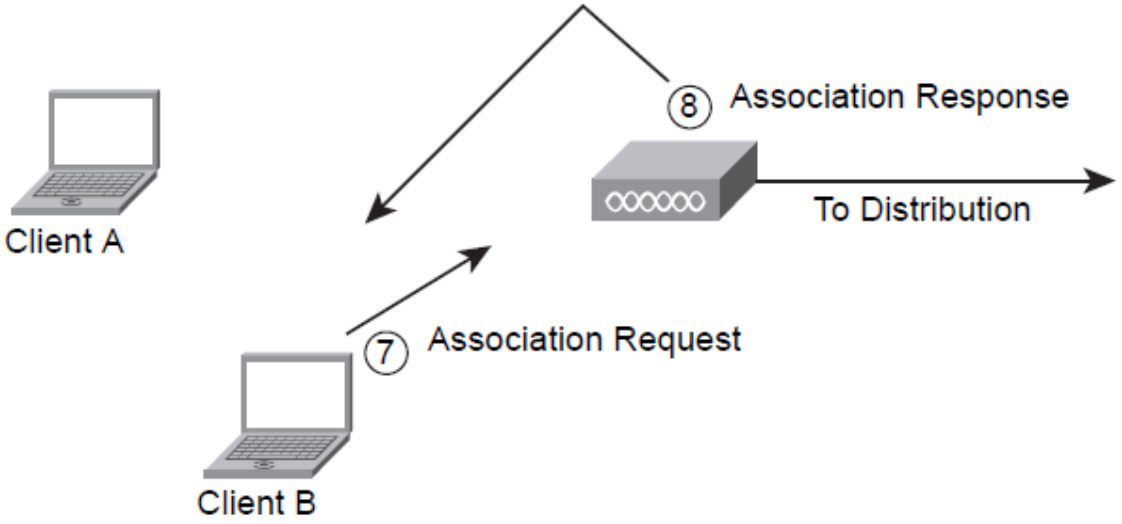
۵. از این مرحله به بعد ، فرآیند برای client های A و B یکسان خواهد بود ، لذا کافیست مکالمات clientB را بررسی کنیم . clientB یک تقاضای authentication ارسال می کند .

۶. AP هم authentication response را به client می فرستد .



۷. clientB یک تقاضای association می فرستد .

۸. AP هم association response بر می گرداند .

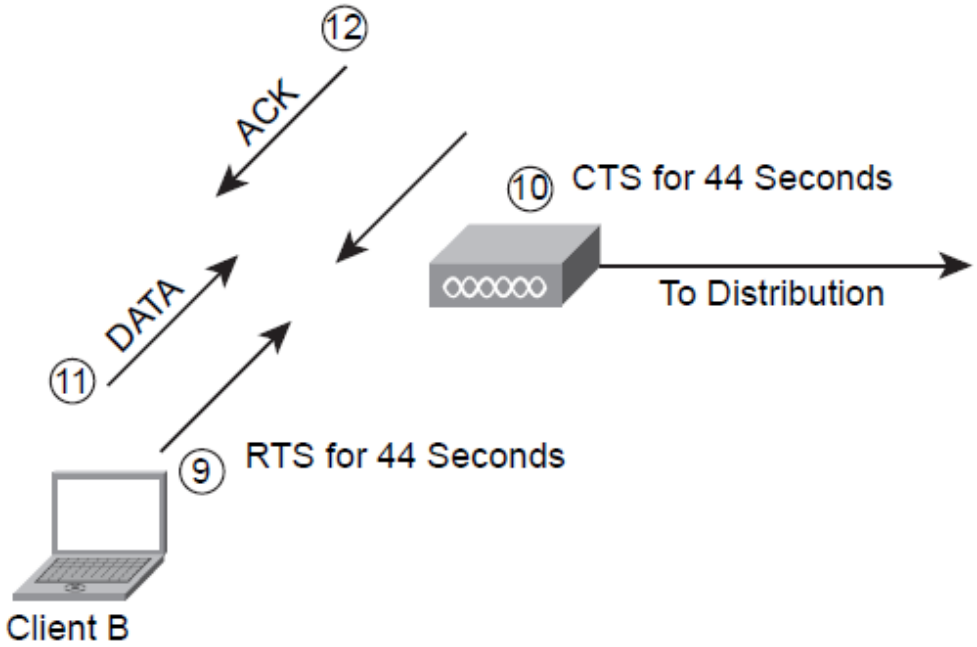


۹. هنگامیکه clientB قصد ارسال دارد ، با فرض اینکه این یک سلول ترکیبی b/g است (mixed b/g cell) ، از RTS استفاده می کند . RTS حاوی مدت زمان ارسال است .

۱۰. AP یک CTS بر می گرداند .

۱۱. clientB دیتا را ارسال می نماید .

۱۲. AP پس از دریافت هر فریم ، ACK بر می گرداند .

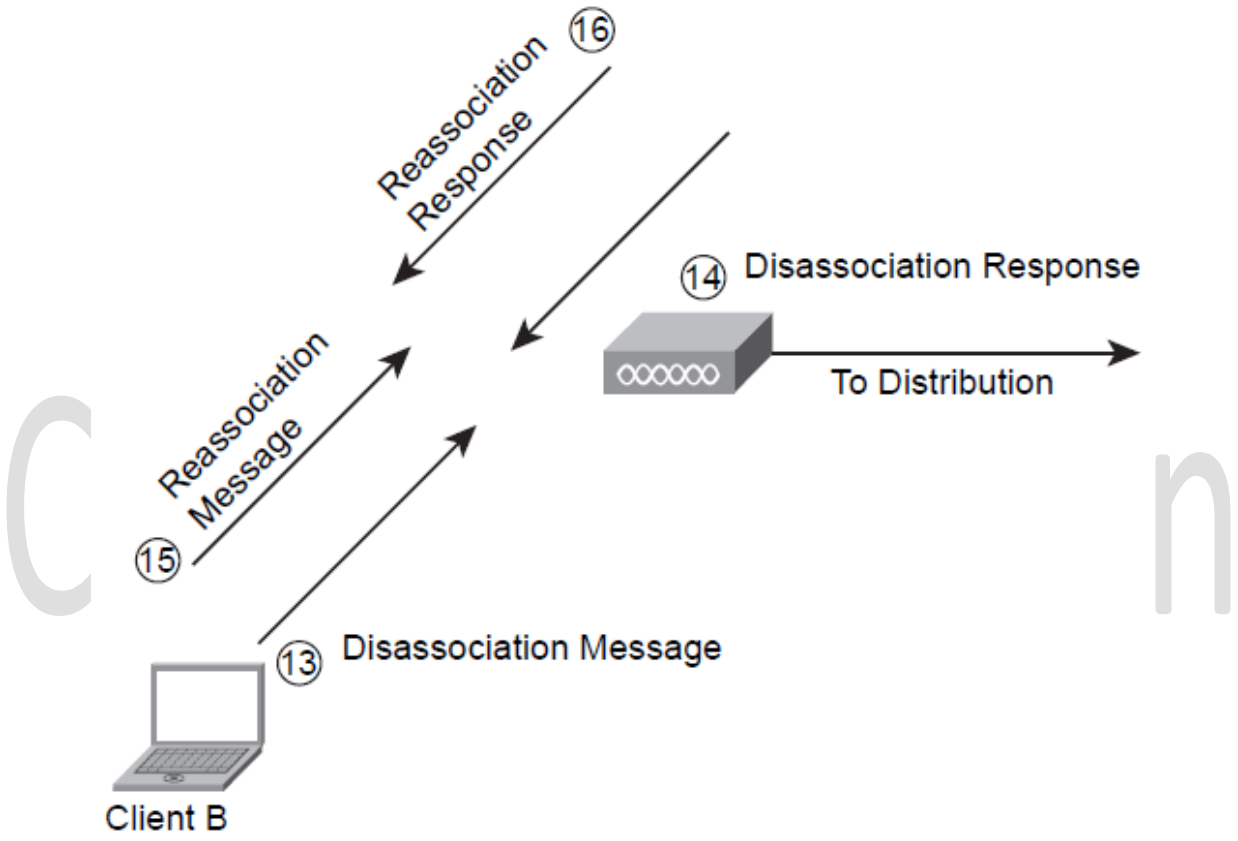


۱۳. clientB یک پیام disassociation می فرستد و شبکه را ترک می کند .

۱۴. AP با یک disassociation response پاسخ می دهد .

۱۵. clientB دوباره به شبکه بر می گردد و یک پیام reassociation ارسال می کند .

۱۶. AP هم با یک reassociation response پاسخ می دهد .



البته این فرآیند حالات مختلف دیگری نیز دارد ، اما مثال بالا می تواند دید و درک مناسبی در مورد مدیریت یک ارتباط به شما بدهد

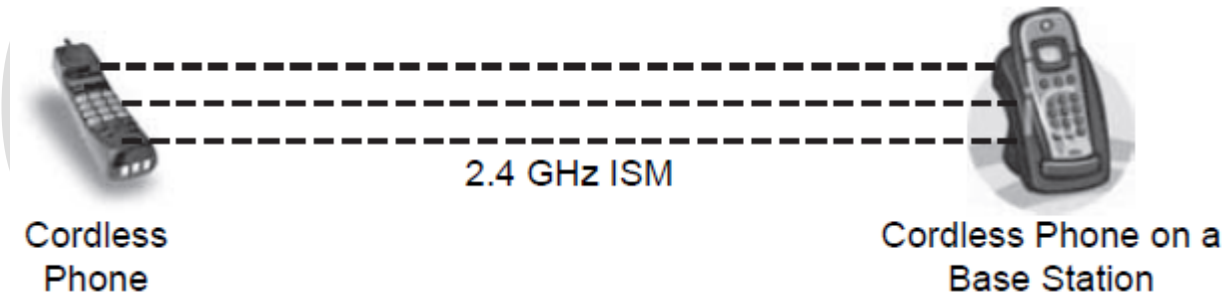
فصل هشتم : آشنایی با سایر تکنولوژی های وایرلس

- Cordless Phones
- Bluetooth
- ZigBee
- WiMax
- آشنایی با سایر مولدهای تداخل

هرچند 802.11 معروف ترین تکنولوژی وایرلس است ، اما تکنولوژی های دیگری نیز وجود دارند که بعضا بسیار پرکاربرد نیز هستند . در این فصل کوتاه ، سعی داریم به چند مورد اشاره کنیم .

Cordless Phones :

امروزه تقریبا همه با تلفن های بیسیم آشنایی دارند . برخی از این تلفن ها در فرکانس 2.4GHz و برخی دیگر در 5.8GHz فعالیت می کنند . چنانچه از 802.11a استفاده می کنید ، تلفن های بیسیم 2.4GHz مناسب است ؛ اما اگر از 802.11b/g استفاده می کنید ، باید به جای استفاده از تلفن های 2.4GHz ، از نوع 5.8GHz استفاده کنید . این تلفن ها از تکنولوژی های TDMA (Time Division Multiple Access) و FDMA (Frequency Division Multiple Access) استفاده می کنند . تکنولوژی دسترسی چندگانه (Multiple Access) ، برای این استفاده می شود که چندین گوشی بتوانند بطور همزمان به باند فرکانسی دسترسی داشته باشند . همچنین با استفاده از TDMA و FDMA ، چندین تلفن بیسیم می توانند از یک ایستگاه مرکزی (Base Station) استفاده نمایند .



تلفن های بیسیم معمولا از استاندارد DECT استفاده می کنند (Digital Enhanced Cordless Telecommunications) . BECT یک استاندارد ETSI است برای تلفن های قابل حمل دیجیتال که در تکنولوژی بیسیم که در خانه ها و مکان های تجاری وجود دارند ، استفاده می شود .

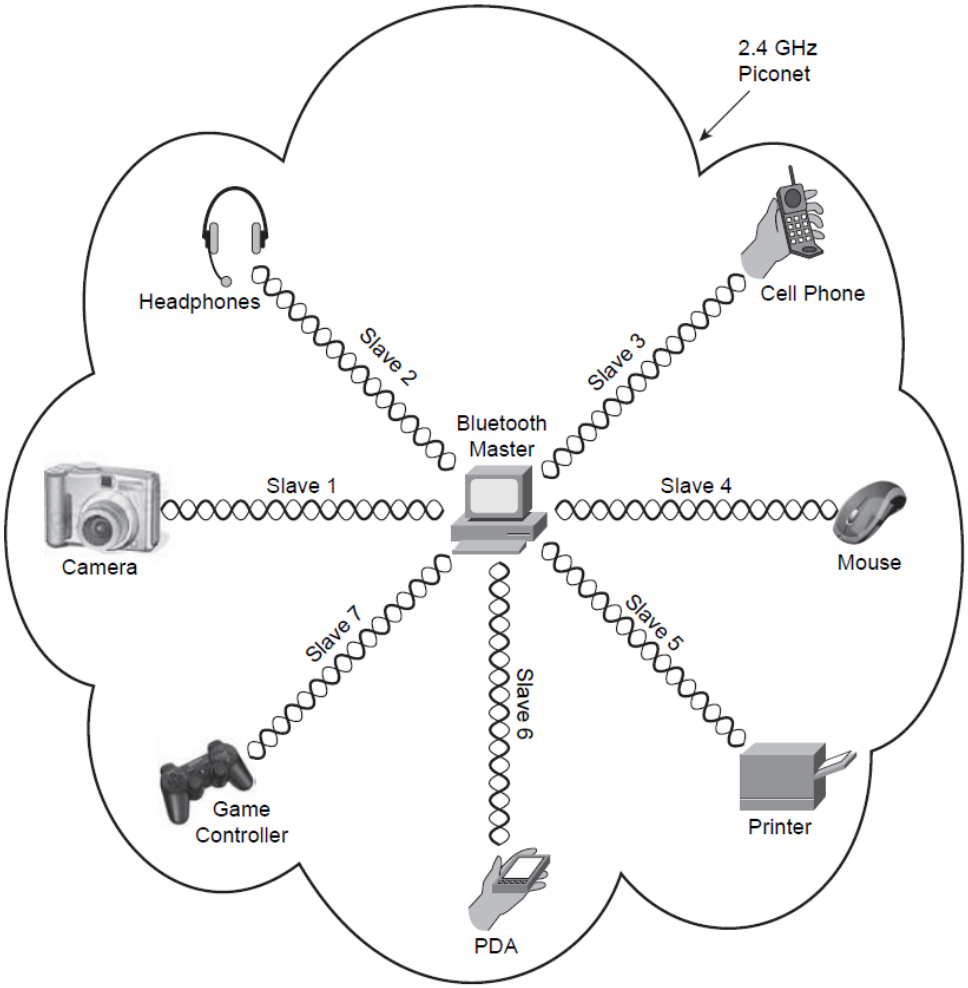
Bluetooth :

امروزه از بلوتوث در همه ی تلفن ها ، PDAها ، لپ تاپ ها ، پرینتر ها و خیلی دستگاههای دیگر استفاده می شود . بلوتوث ، مصرف توان بسیار پایینی دارد و برای همین هم برای دستگاههای متحرک که با باتری کار می کنند ، بسیار مناسب هستند .

از سال ۱۹۹۸ که گروه علاقه مندان بلوتوث تشکیل شد ، ورژن های مختلفی طراحی و به کار گرفته شد . مثلا در سال ۲۰۰۷ ، Bluetooth 2.1 وارد بازار شد که با EDR همراه بود (Enhanced Data Rate) . این ورژن یک ویژگی مهم داشت و آن هم quick pairing بود که در آن دو دستگاه خیلی زود همدیگر را پیدا می کردند . این ورژن همچنین به کمک یک ویژگی دیگر به نام sniff subrating ، عمر باتری را تا ۵ دقیقه بیشتر افزایش می داد .

تکنولوژی بلوتوث ممکن است با LAN های 802.11 تداخل پیدا کند ، چون در محدوده ی فرکانسی 2.4GHz فعالیت می کند . اما چون برای فعالیت در مساحت تقریبا 35 فوتی طراحی شده ، توان ارسالی خیلی پایینی دارد و از FHSS استفاده می کند ، خیلی بعید است که تداخل بوجود آید .

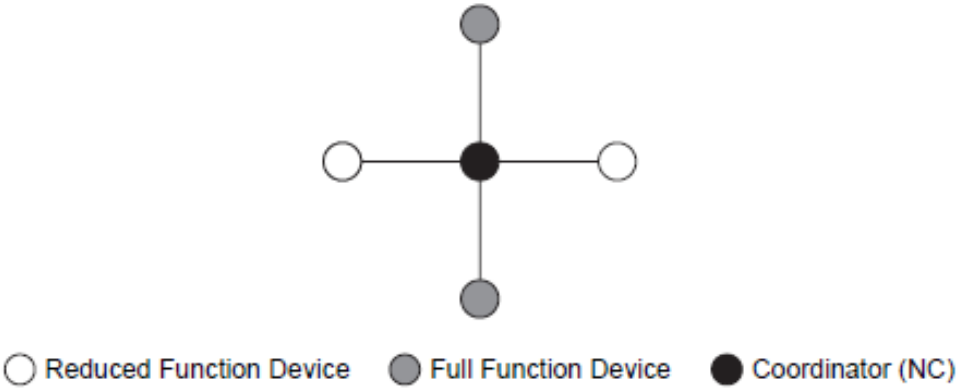
بلوتوث به عنوان یک piconet نیز در نظر گرفته می شود ؛ زیرا به ۸ دستگاه اجازه می دهد که با هم جفت شوند (یک master و هفت slave) .



ZigBee :

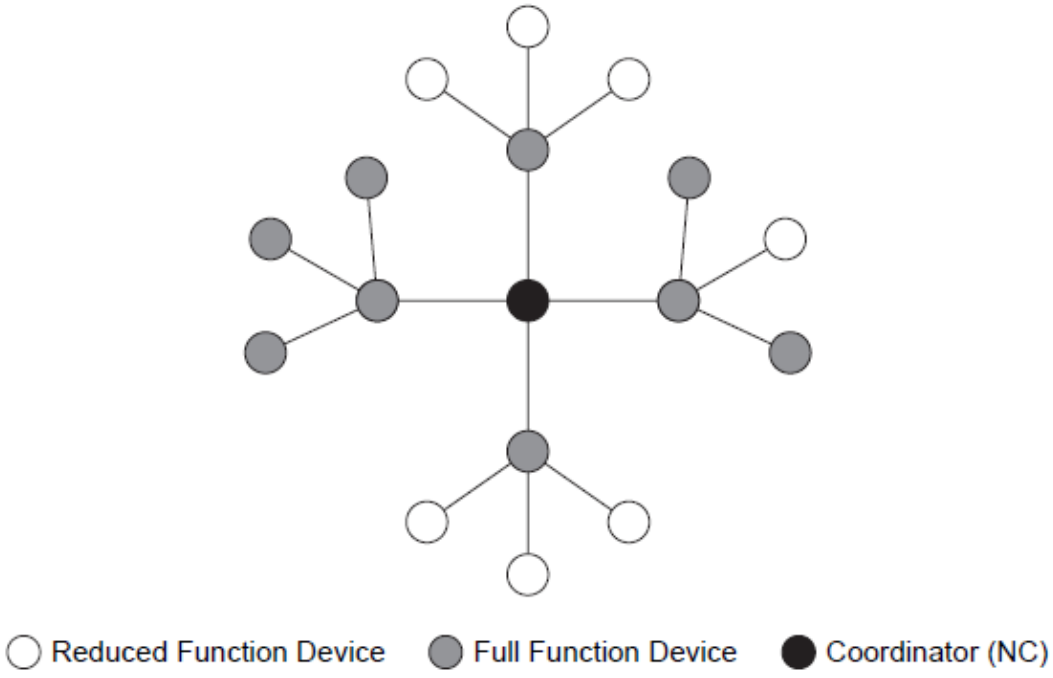
ZigBee شامل digital radio های کوچک و low power می شود که بر اساس 802.15.4 برای WPAN ها طراحی شده اند ؛ مانند Headphone های بلوتوث که با گوشی موبایل در ارتباط است . البته این تکنولوژی بیشتر برای کنترل و مانیتورینگ به کار می رود ؛ در باندهای ISM فعالیت می کند ، و بیشترین کاربرد آن برای اتوماسیون های اداری ، صنعتی ، و خانه می باشد .

در شکل زیر یک توپولوژی star می بینید که دستگاه مرکزی یک NC است (Networrk Coordinator) . سایر دستگاهها می توانند full-function یا reduced-function باشند .



یک دستگاه full-function ، می تواند ارسال ، دریافت و یک سری کارهای دیگر را انجام دهد ؛ اما یک دستگاه reduced-funtion ، همه ی این قابلیت ها را ندارد و تنها می تواند کارهایی چون گزارش دمای یک سیستم به کنترلر را انجام دهد .

در توپولوژی خوشه ای (cluster) ، در واقع یک star گسترده و توسعه یافته در LAN داریم .



WiMax :

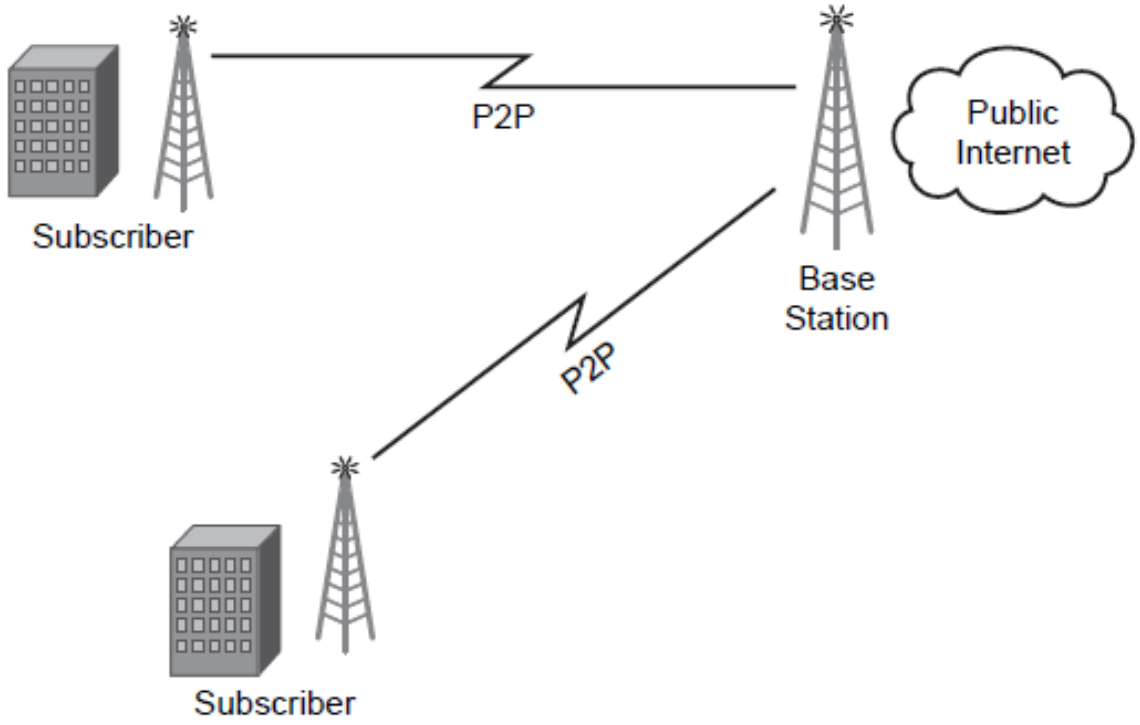
Worldwide Interoperability for Microwave Access یک تکنولوژی مبتنی بر استاندارد است که می تواند به عنوان یک جایگزین برای سرویس های Broadband سیمی (مثل ارتباطات cable یا DSL) ، به راحتی دسترسی last-mile را فراهم آورد .

نکته : Last-mile اصطلاحیست که در ارتباطات و صنایع تکنولوژی ، برای تعریف تکنولوژی ها و پروسه های مورد استفاده برای برقراری ارتباط بین مشترکین نهایی و شبکه های ارتباطی ، به کار می رود .

در یک سلول معمولی با شعاع ۳ تا ۱۰ کیلومتر ، WiMax ظرفیت رسیدن به پهنای باند 40 Mbps به ازای هر کانال را دارد . این پهنای باند کافیست تا صدها لینک تجاری با سرعت اتصال T1 و هزاران مشترک عادی با سرعت اتصال DSL ، بصورت همزمان پشتیبانی شوند .

برخی از فراهم کنندگان سرویس (service providers) از این تکنولوژی به عنوان جایگزینی برای DSL یا Cable modem استفاده می کنند . محدوده ی سیگنال در این سناریو ی Non-LOS حدود ۳ تا ۴ مایل است ، و data rate هم حدود 30Mbps است (هرچند معمولا کمتر هم می شود – حدود 15Mbps) .

اما حالت LOS WiMax که بیشتر شبیه T1 قدیمی است ، سرعت دیتا حدود ۳۰ تا ۷۰ مگا بیت بر ثانیه است (می توان گفت 40Mbps Real) . این سناریو در واقع یک توپولوژی Point-to-Point است و سرویس های Backbone یا Backhaul را فراهم می آورد .



WiMax در باند فرکانسی 10GHz تا 66GHz فعالیت می کند ، لذا هیچ تداخلی با LAN های 802.11 ندارد .

آشنایی با سایر مولدهای تداخل :

انواع دیگر تداخل در محدوده های فرکانسی یکسان رخ می دهند که از این میان می توان به موارد زیر اشاره کرد :

- **مایکروویو ها (فعالیت در ۱ تا 40GHz)**
- **دوربین های X11 وایرلس (فعالیت در 2.4GHz)**
- **سیستم های راداری (فعالیت در ۲ تا 4GHz برای نظارت در محدوده های متوسط ، کنترل ترافیک نهایی ، و کنترل آب و هوا در محدوده های وسیع . همچنین فعالیت در ۴ تا 8GHz برای ردیابی در محدوده های وسیع و سیستم های هوابرد)**
- **سنسورهای متحرک (فعالیت در 2.4GHz)**
- **نورپردازی فلورسنت (فعالیت در 20KHzیا بالاتر)**
- **آداپتورها و کنترلر های بازی (معمولا فعالیت در 2.5GHz)**

هرچند در هنگام طراحی و کار با شبکه های وایرلس ، باید از ابزار های اندازه گیری قدرت سیگنال و نیز محدوده ی پوشش استفاده کنید ، اما باز هم باید متوجه سایر دستگاهها و منابع ایجاد کننده ی تداخل باشید تا بتوانید راحت تر و سریع تر ، مکان مناسب برای نصب AP ها و سایر تجهیزات را پیدا کنید .

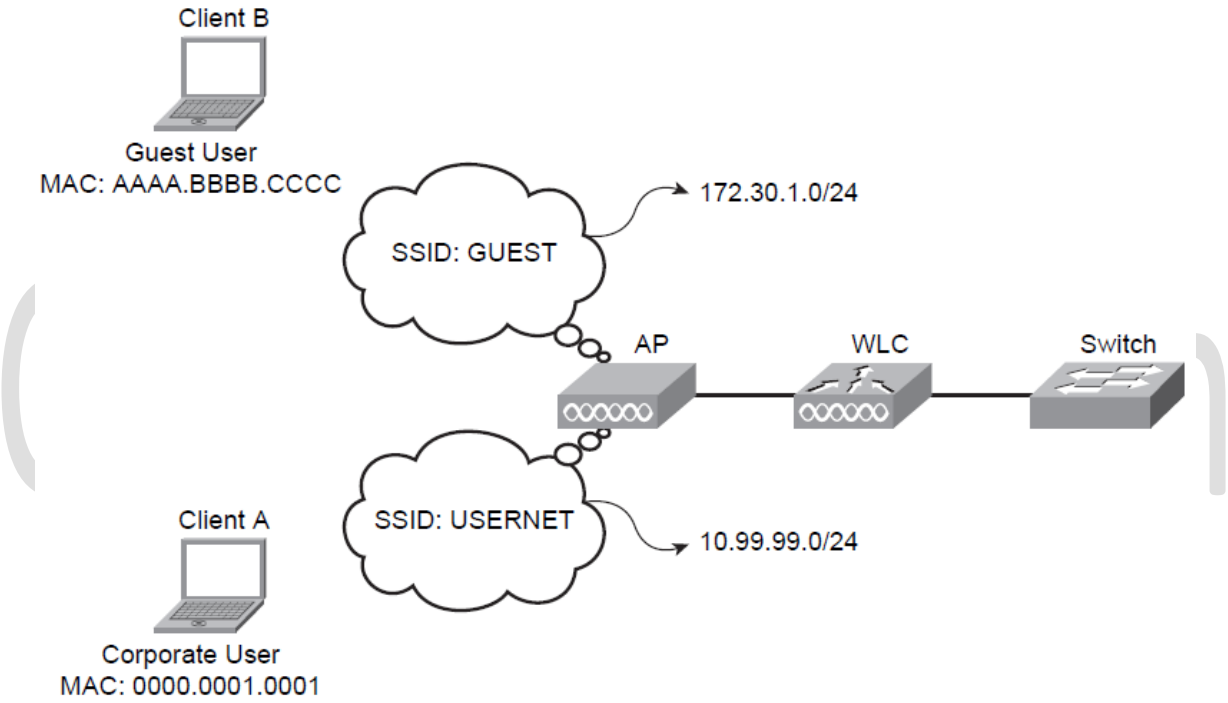
فصل نهم : انتقال پکت ها از شبکه ی وایرلس به شبکه ی سیمی

- فرآیند **Association**
- ارتباط با یک **Host** در یک **subnet** دیگر
- کنترل شبکه با استفاده از **VLAN** ها

اگر فصل های گذشته را مطالعه کرده باشید ، الان دید خوبی نسبت به نحوه ی انتقال فریم ها روی شبکه ی وایرلس دارید . اما در یک شبکه ی وایرلس یکپارچه سیسکو ، فریم ها در شبکه ی وایرلس باقی نمی مانند ، بلکه از یک AP سبک وزن به یک WLCمی روند (Wireless LAN Controller) . البته lightweight AP و WLC در فصل ۱۰ مورد بررسی قرار می گیرند ، اما در این فصل خواهیم دید که چگونه ترافیک شبکه در حین انتقال از AP به سمت WLC و از آنجا به شبکه ی سیمی دچار تغییر می شود .

فرآیند Association :

در طول این فصل ، به کرات از توپولوژی منطقی زیر استفاده خواهیم کرد .



همانطور که در این توپولوژی می بینید ، کاربران وایرلس در محدوده ی AP ی قرار دارند که چندین SSID را تبلیغ می کند . یک AP می تواند چندین SSID را تبلیغ نماید ، اما در واقع از یک رادیو استفاده می نماید . در واقع SSID و IP Subnet برای اینست که شبکه ی وایرلس را بصورت منطقی (logical) ، مجزا (seprate) کنیم .

تقاضای association که از طرف client به AP می رود ، شامل data rate ها و قابلیت های client می باشد . association response هم که از طرف AP است ، شامل data rate هایی است که AP قابلیت ساپورت آنها را دارد ، همچنین شامل سایر قابلیت های AP ، و نیز شماره ی شناسایی(identification) برای آن association می باشد .

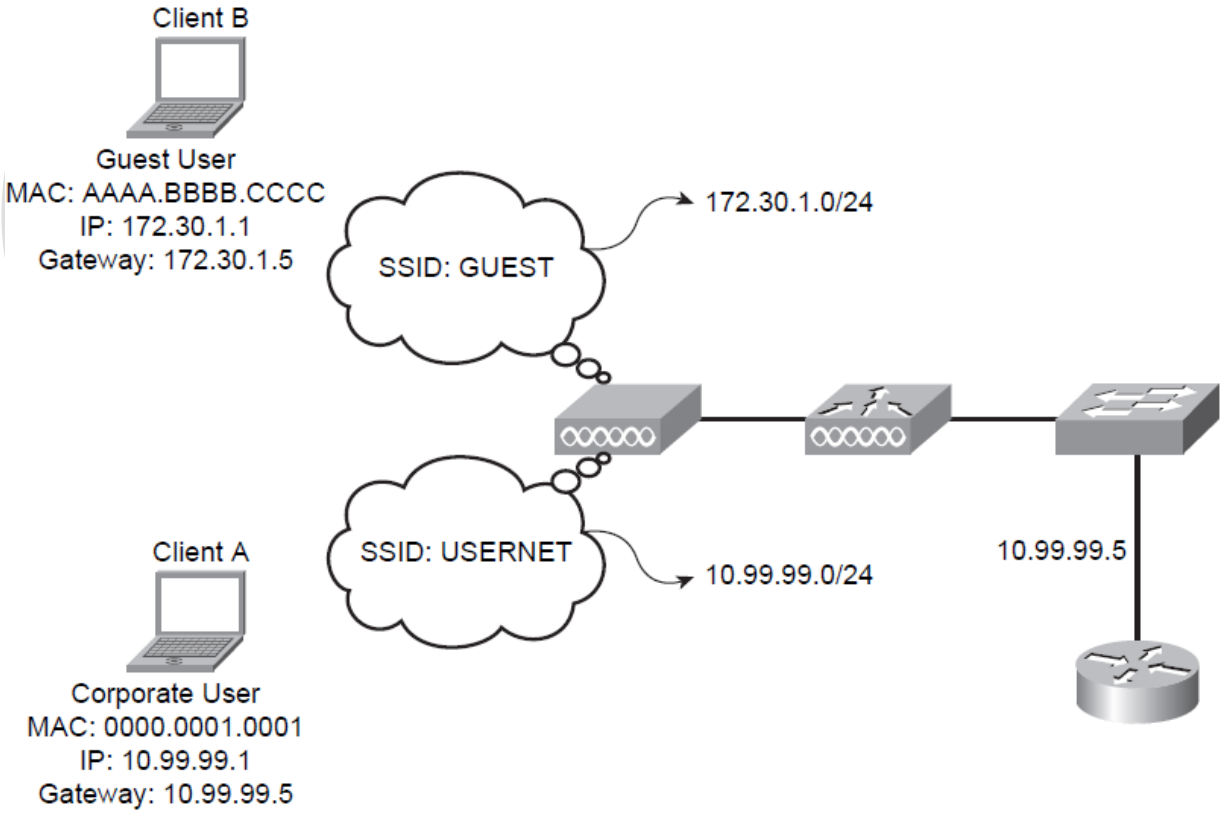
تمام فریم های مدیریتی در پایین ترین سرعت پشتیبانی شده ارسال می شوند ، در حالیکه header های دیتا می توانند سریعتر از فریم های مدیریتی ارسال شوند ، و خود فریم های دیتا هم در بالاترین سرعت ممکن ارسال می گردند .

بطور کلی می توان گفت برای برقراری ارتباط client با AP ، این مراحل به ترتیب انجام می شوند :

۱. بسته به اینکه client ها بصورت active یا passive شبکه را اسکن کنند ، request ، response ، و یا beacon ها ارسال می گردند .
۲. Authentication و association انجام می گیرد .
۳. Client باید سرعت را تشخیص دهد و معین کند که این کار را با استفاده از SNR (Signal-to-Noise Ratio) و RSSI (Received Signal Strength Indicator) انجام می دهد . وقتی client سرعت را مشخص کرد ، AP نیز با همان سرعت ارسال را انجام می دهد .

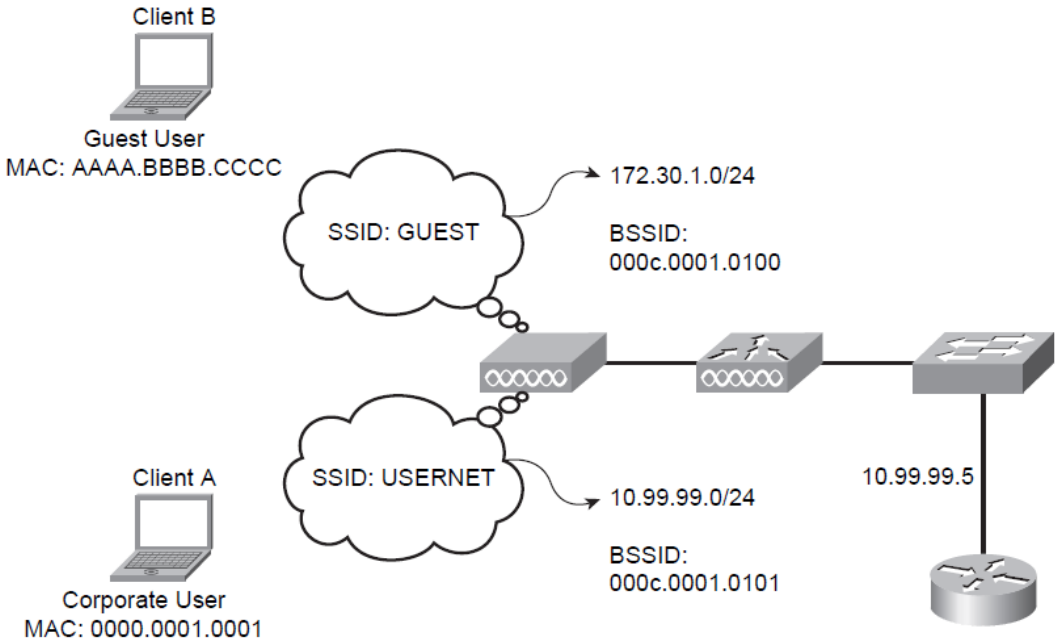
ارتباط با یک Host در یک Subnet دیگر :

چنانچه مطابق شکل زیر ، clientA بخواهد با clientB ارتباط برقرار کند ، قوانین IP همچنان برقرارند و لذا این دو نمی توانند مستقیما با هم داده ها را رد و بدل کنند .



بر اساس قوانین پایه ای IP ، این دو client ابتدا تشخیص می دهند که در یک subnet قرار ندارند و سپس تصمیم می گیرند که از یک Default gateway استفاده کنند تا داده هایشان را ارسال نمایند . همچنین اگر یک client هنوز هیچ ارتباطی با Default gateway برقرار نکرده باشد ، از ARP استفاده می کند تا MAC را بدست بیاورد .

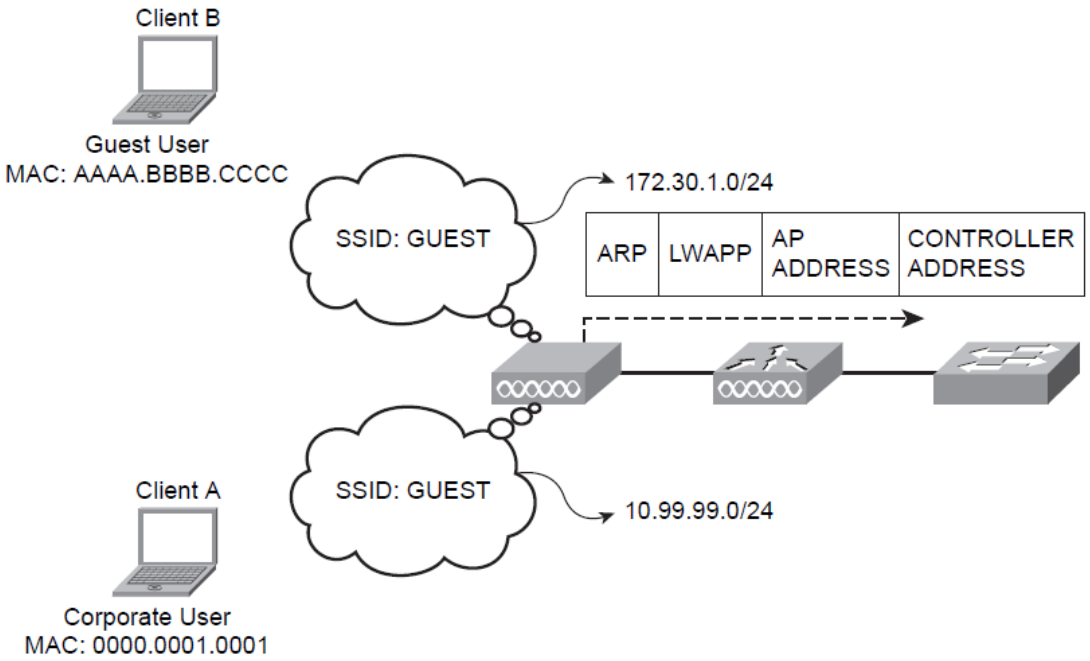
در این ARP ، سه تا MAC داریم که address1 همان RA ، address2 همان SA ، و address3 همان DA می باشد .



Frame Control	000c.0001.0101 ADDRESS 1	0000.0001.0001 ADDRESS 2	FFFF.FFFF.FFFF ADDRESS 3	ARP

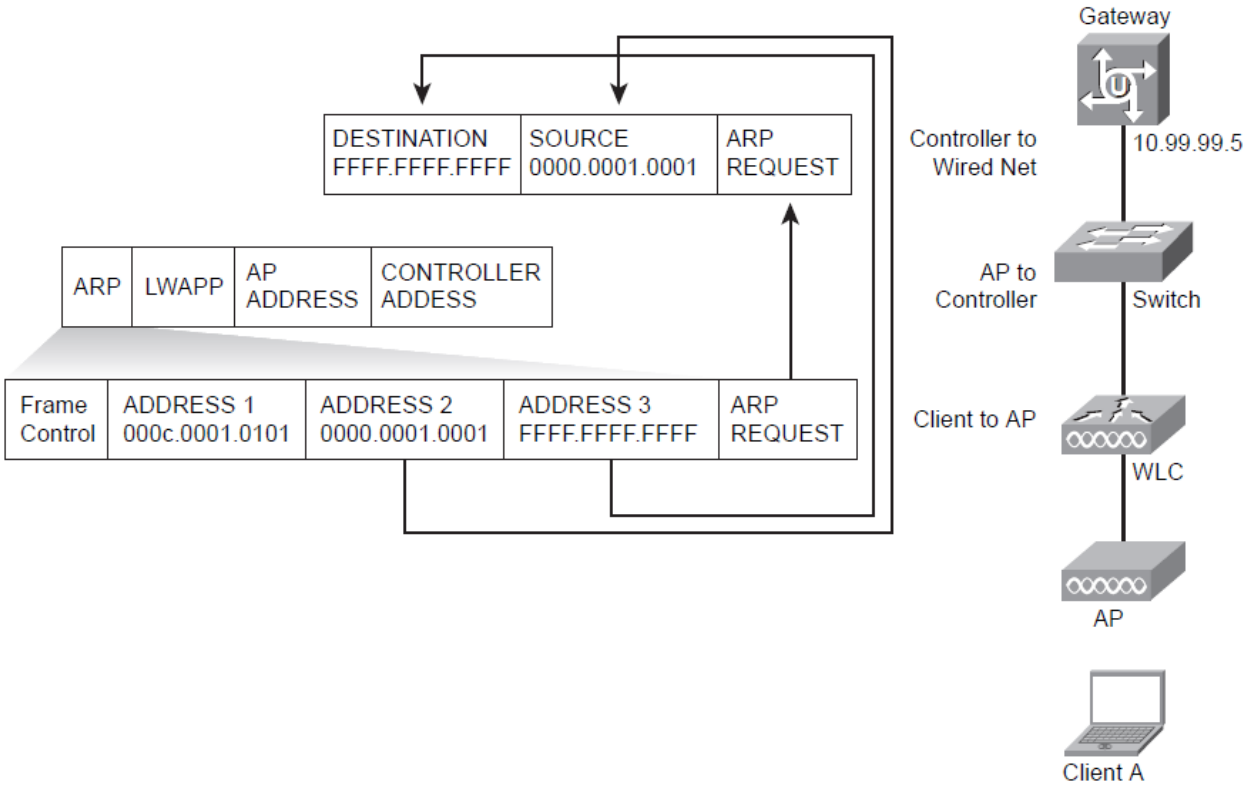
ARP ⟶ WHO IS 10.99.99.5

هنگامیکه AP پیغام ARP را دریافت می کند ، ابتدا FCS را چک می کند و سپس به اندازه ی SIFS صبر می کند . سپس یک Ack به client می فرستد (توجه کنید که این Ack با ARP response تفاوت دارد و نباید اشتباه گرفته شوند). سپس فریم ARP را بوسیله ی LWAPP (LightWeight Access Point Protocol) به WLC خود فورووارد می کند .



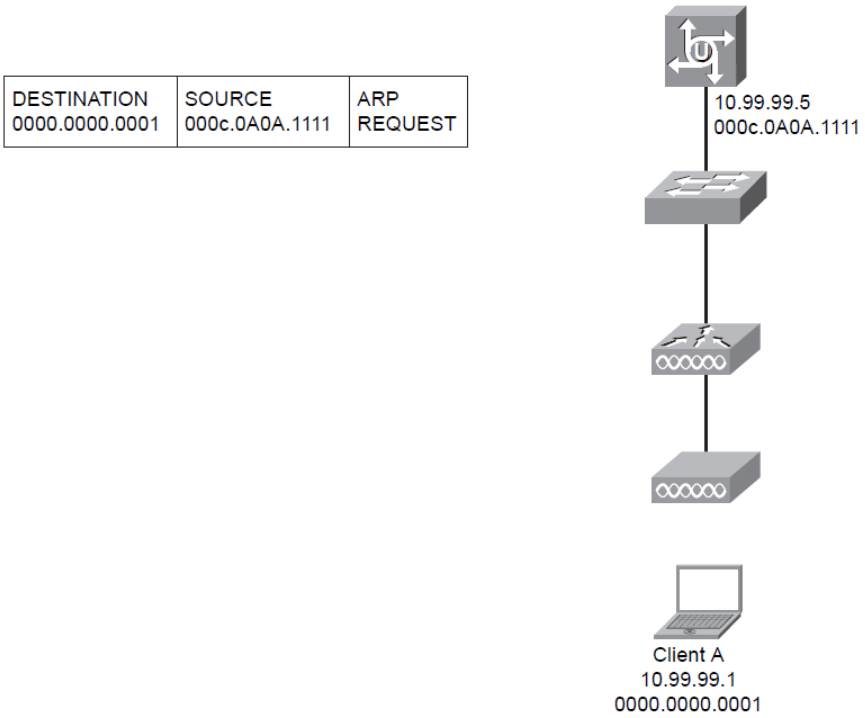
فریم LWAPP که از AP به سمت WLC حرکت می کند ، روی یک مسیر wired (سیمی) حرکت می کند ؛ لذا باید از استاندارد 802.3 استفاده کند . LWAPP ، فریم را encapsulate می کند ، بطوریکه در header جدید ، آدرس IP و MAC مربوط به AP به عنوان source ، و آدرس IP و MAC مربوط به WLC به عنوان destination قرار داده می شود ؛ اما هنوز فریم اصلی 802.11 را داریم که ۳ آدرس MAC دارد .

وقتی WLC فریم LWAPP را می گیرد ، آن را بصورت ۸۰۲.۳ در می آورد ؛ لذا اولین آدرس MAC را drop می کند ، دومین MAC را به عنوان source فریم ۸۰۲.۳ ، و سومین MAC را به عنوان destination فریم 802.3 قرار می دهد (که در واقع broadcast است) . سپس این فریم ۸۰۲.۳ را به شبکه ی wired موجود فوروارد می کند .

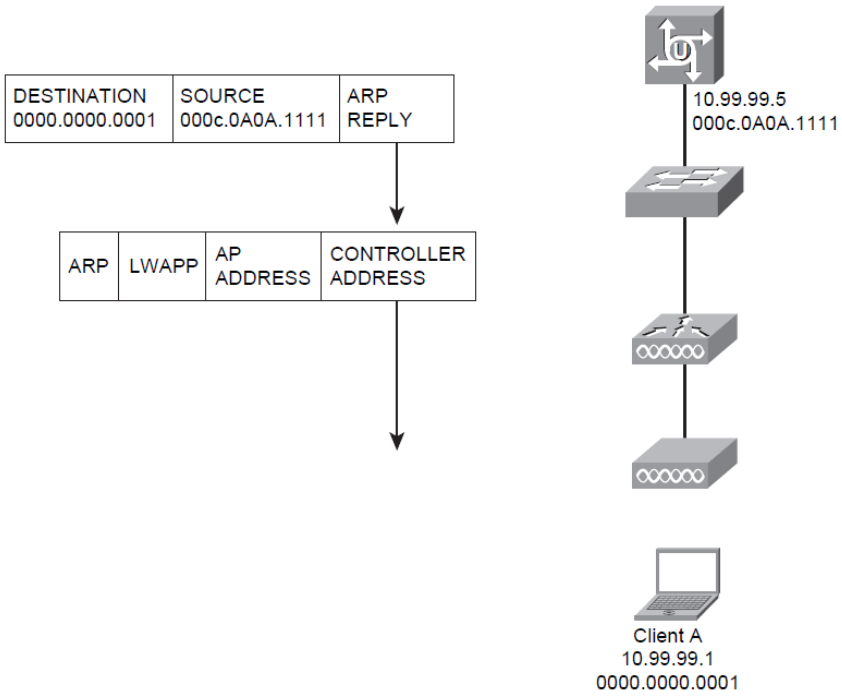


سپس فریم به سوییچ می رسد و سوییچ هم این فریم دریافتی را flood می کند (چون آدرس مقصد آن بصورت broadcast است) .

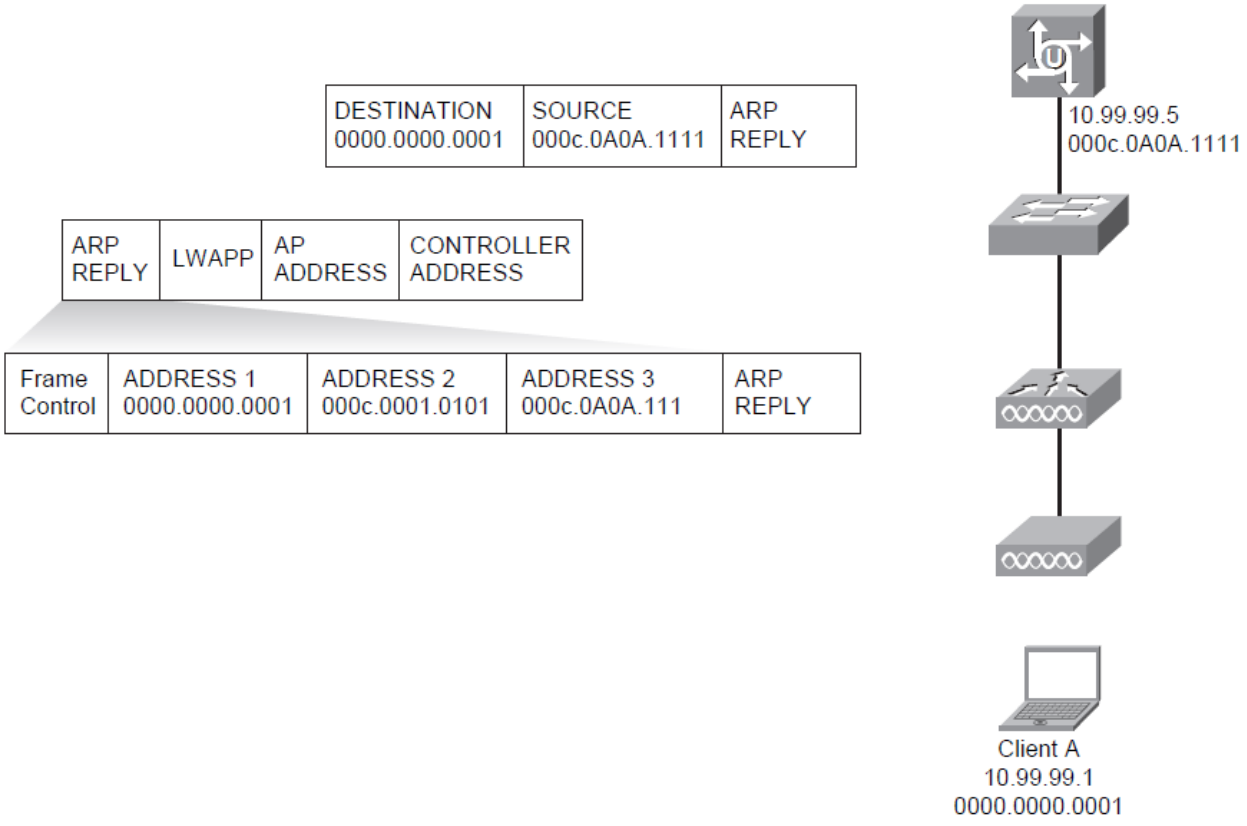
در نهایت فریم به یک layer 3 device می رسد که خوشبختانه همان Default gateway است . روتر با استفاده از آدرس های MAC خودش به این تقاضای ARP پاسخ می دهد .



ARP response بصورت پیام unicast باز می گردد ، لذا سوییچ هایی که در طول مسیر هستند ، به جای flooding روی همه ی پورت ها ، مستقیما فریم را به پورت هایی فوروارد می کنند که به client وایرلس می رسند . وقتی پیام از GW به WLC رسید ، WLC آن را rewrite می کند و دوباره بصورت یک فریم 802.11 در می آورد و SA را آدرس MAC مربوط به default gateway ، DA را آدرس client ، و TAرا آدرس AP قرار می دهد . حال دوباره یک LWAPP داریم .



سپس WLC ، فریم LWAPP را به سمت AP فوروارد می کند .



پس از رسید پیام به AP ، عملیات buffering و نیز backoff timer و counting down شروع می شود . اگر در طول count down یک فریم وایرلس توسط AP شنیده شود ، مقدار reservation فریم شنیده شده به مقدار countdown اضافه می گردد . در نهایت ، فریم بصورت یک فریم 802.11 ارسال می گردد . client هم پس از دریافت فریم ، به اندازه ی SIFS صبر کرده ، سپس Ack را می فرستد و این فرآیند به پایان می رسد .

کنترل شبکه با استفاده از VLAN ها :

با مطالعه ی بخش قبل ، شاید این سوال برای شما بوجود بیاید که AP و WLC چگونه می تواند دو subnet مجزا که روی یک شبکه ی wired هستند را از هم جدا کند ؟ پاسخ این سوال ، استفاده از vlan هاست .

یک vlan ، مفهومی در شبکه های سوییچینگ است که موجب می شود کاربران را در لایه های منطقی از هم جدا کنیم . با استفاده از vlan ها درسمت سیمی AP و WLC ، نتیجه ی کار به این صورت خواهد بود :

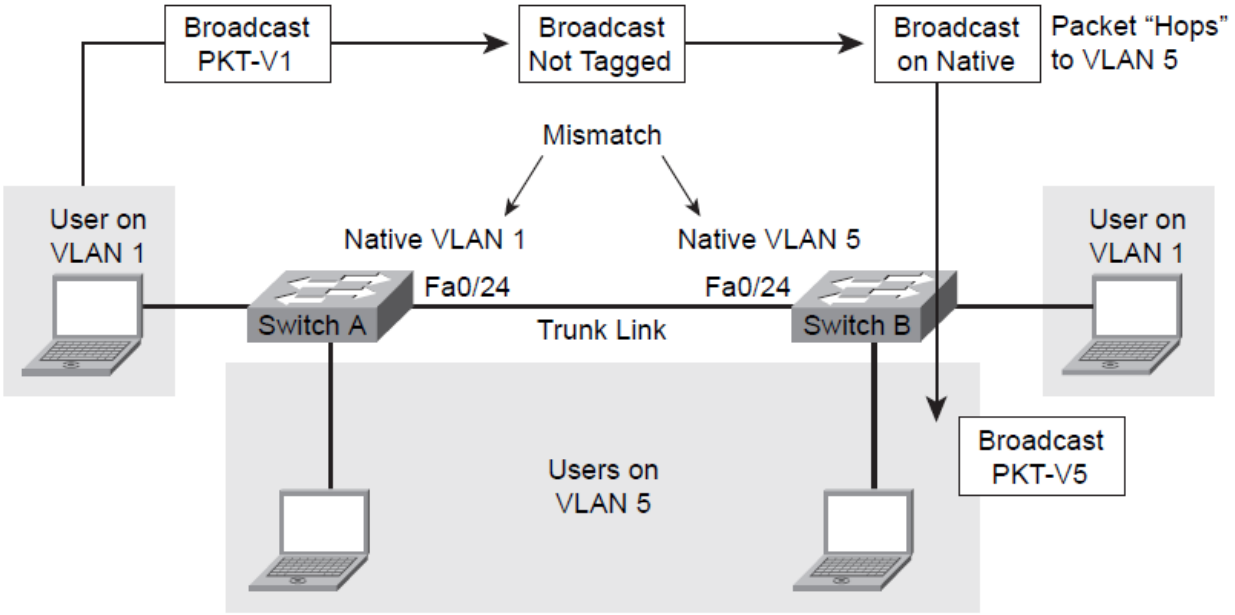
SSID = Logical Subnet = Logical VLAN or Logical Broadcast Domain

هنگامیکه فریم های وایرلس از AP به سمت شبکه ی سیمی حرکت کردند ، باید روی یک سیم فیزیکی مشترک حرکت کنند . شاید فکر کنید این امر خیلی مشکل است ، زیرا داشتن چندین SSID به معنای وجود بیش از یک شبکه است ! اما با استفاده از پروتکل 802.1Q این کار اصلا دشوار نیست .

802.1Q یک تگ ۴بایتی روی هر فریم ۸۰۲.۳ قرار می دهد تا مشخص کند که این فریم متعلق به کدام vlan است . لذا هرچند این فریم ها روی یک سیم حرکت می کنند ، اما بصورت منطقی توسط vlan بندی از هم جدا شده اند . سوییچ های پایانی دو طرف لینک ترانک ، با توجه به همین تگ 802.1Q می فهمند هر فریم را باید به کدام vlan بدهند .

نکته : تمام ترافیکی که روی لینک ترانک ارسال می شود ، دارای یک تگ است (بغیر از native VLAN) . در سوییچ های سیسکو ، native VLAN بصورت پیش فرض ، VLAN1 است .

نکته : باید توجه داشت که native VLAN ها در دو طرف یک لینک ، یکسان باشند ؛ وگرنه هر سوییچ فرض می کند که native VLAN سوییچ دیگر ، همانند native VLAN خودش است ، لذا فریم ها به اشتباه برای VLAN های مختلف ارسال می شوند .



مثلا در شکل قبل ، switchA دارای native VLAN1 است و switchB دارای native VLAN5 می باشد . اگر سوییچ A یک فریم broadcast بدون تگ ارسال کند (از native VLAN1) ، سوییچ B آن فریم را برای همه ی user های native VLAN5 خودش ارسال می نماید !

به عنوان نکته ی پایانی توجه داشته باشید که در CCNA Wireless ، فرض می شود که شما دوره ی CCNA را گذرانده اید یا لااقل با مفاهیم آن آشنایی دارید .

برای مطالعه در مورد VLAN ها ، به فصل دوم کتاب ICND2 نوشته ی آقای Steve Mcquerry مراجعه کنید . همچنین برای دوره ی اجمالی ، می توانید فصول Day22 – Day 24 کتاب 31 Days Before Your CCNA Exam را مطالعه بفرمایید .

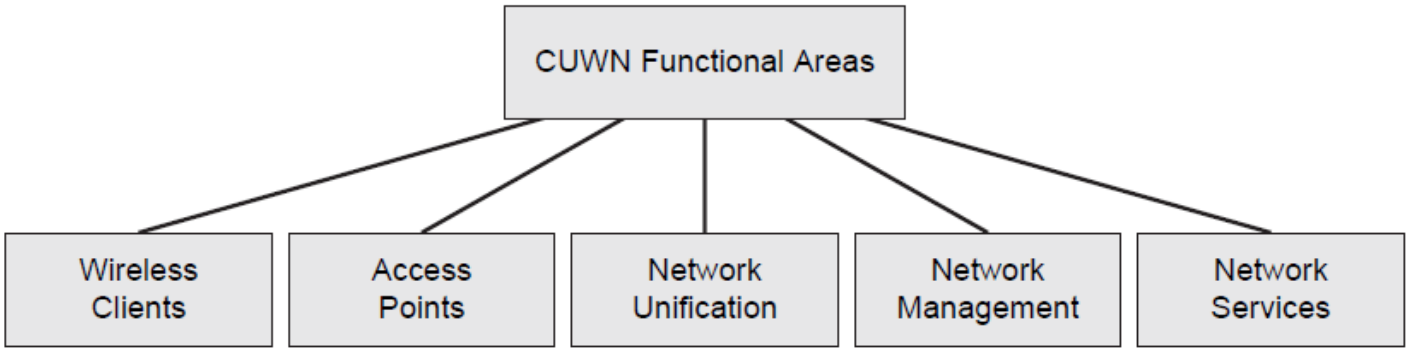
فصل دهم : آشنایی با معماری شبکه های وایرلس سیسکو

- CUWN
- پشتیبانی از چند شبکه توسط یک AP
- معماری CUWN
  - ✓ Cisco 1130AG series AP
  - ✓ Cisco 1240AG series AP
  - ✓ Cisco 1250AG series AP
  - ✓ Cisco 1300 series AP/Bridge
  - ✓ Cisco 1400 series Wireless Bridge
  - ✓ Cisco 44xx series WLC
  - ✓ Cisco 3750-G WLC
  - ✓ Cisco WiSM
  - ✓ Cisco 2106 WLC
  - ✓ Cisco WLCM
- مدیریت شبکه وایرلس

طراحی های اولیه شبکه های وایرلس تنها مبتنی بر AP های مستقل بودند که Autonomous AP ها یا fat AP نامیده می شدند . یک Autonomous AP دستگاهیست که مبتنی بر هیچ نوع کنترل مرکزی نمی باشد . اما با توسعه ی شبکه های وایرلس ، مشکلاتی نظیر عدم انعطاف پذیری ، مشکل در نگهداری تنظیمات و configuration ، و نیز مشکل در مانیتورینگ موقعیت و وضعیت هر AP بوجود آمدند . این مشکلات ، نیاز به وجود یک کنترل متمرکز را دو چندان نمود ، و CUWN مبتنی بر Centralized Control می باشد . در این فصل با این نوع طراحی آشنا می شویم .

CUWN :

یک Lightweight AP توسط یک کنترلر مدیریت می شود ، یعنی configuration خود را از یک controller می گیرد . لذا ما تمام تنظیمات را روی کنترلر انجام می دهیم و هرگاه محیط یا شرایط تغییر کرد ، AP بصورت دینامیک خود را update می نماید . این نوع AP توسط یک WLC کنترل و مانیتور می گردد .



یک WLC می تواند بین ۶ تا ۳۰۰ عدد AP را مدیریت کند . AP برای برقراری ارتباط با WLC ، از یک پروتکل به نام LWAPP استفاده می کند (Lightweight AP Protocol) . مثلا AP با استفاده از LWAPP ، می تواند اطلاعات و پیام های کنترلی را با controller رد و بدل کند .

LWAPP علاوه بر data ی اصلی ، اطلاعاتی در مورد SNR و RSSI را نیز در header خود نگهداری می کند که WLC از این اطلاعات برای بهبود coverage area استفاده می نماید .

- ✓ **Split MAC Design** : یکی از طراحی های WLC است که به معنای اینست که می توان پروتکل های 802 را بین AP و controller ، split کنیم . از یک طرف ، AP ها پکت های time-sensitive و بخش real-time را پیگیری می نمایند و از سوی دیگر ، controller پکت هایی که time-sensitive نیستند را handle می کند .
- ✓ **Coverage Hole** : زمانی بوجود می آید که AP در یک ناحیه down شود .

نکته : توجه کنید که AP وظایفی چون association و authentication را انجام نمی دهد ؛ این کارها بر عهده ی controller است .

نکته ی تکراری و تاکیدی : بین AP و WLC ، همه ی client data از طریق LWAPP tunnel و درون wired domain عبور می کند .

LWAPP می تواند در دو حالت فعالیت کند :

۱. Layer 2 LWAPP mode : این حالت فقط با آدرس های MAC کار می کند . AP باید در یک subnet با controller باشد . این روش ، flexibility زیادی برای تنظیمات مشترک ها ندارد .

۲. Layer 3 LWAPP mode : این حالت هم با MAC و هم با IP کار می کند . این پروتکل به admin شبکه اجازه می دهد که AP ها را در subnet ها جداگانه قرار دهد .

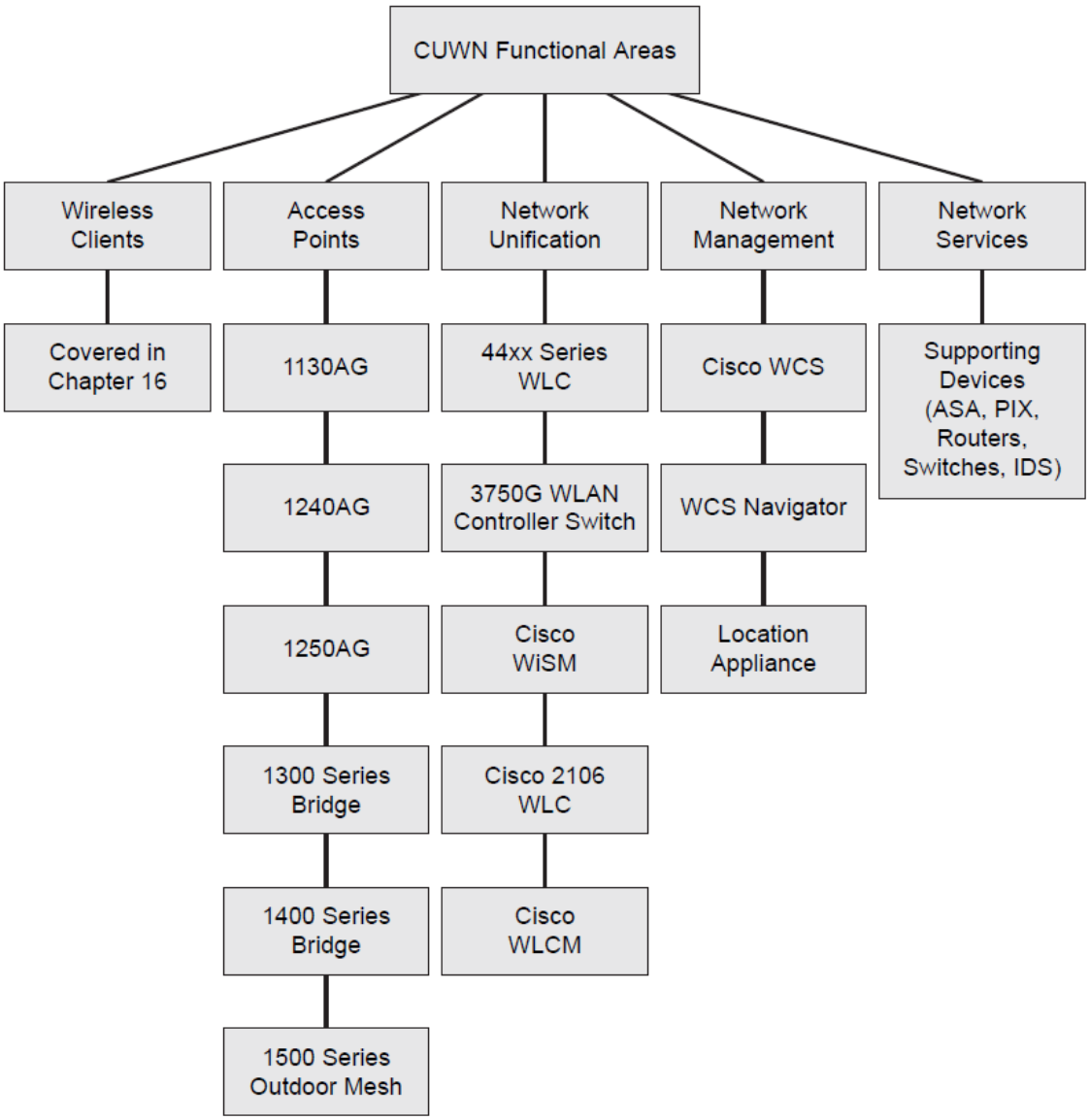
پشتیبانی از شبکه توسط یک AP :

WLAN مفهوم SSID روی فضای وایرلس ، و مفهوم VLAN روی فضای wired را در کنار هم قرار می دهد . با استفاده از چندین WLAN مجزا و مستقل ، می توان QOS های مختلف را روی انواع ترافیک هایی که برای هر کدام اختصاص یافته اند ، اجرا نمود .

- ✓ هر Lightweight AP می تواند تا ۵۱۲ عدد vlan مختلف را ساپورت کند .
- ✓ هر WLC می تواند تا ۱۶ عدد WLAN را به هر AP اختصاص دهد و به هر کدام از این WLAN ها ، یک WLAN ID اختصاص می دهد . این WLAN ID ، یک عدد بین ۱ تا ۱۶ است و ما نمی توانیم آن را انتخاب کنیم .
- ✓ هر AP تا ۱۶ عدد SSID را ساپورت می کند که هر SSID نشان دهنده ی یک vlan است . لذا اگرچه تا ۵۱۲ عدد vlan ساپورت می شود ، اما فقط ۱۶ تای ان استفاده می شود .

معماری CUWN :

در شکل زیر می توانید تمام اجزاء CUWN را مشاهده فرمایید :



در مورد client ها در فصل ۱۶ به تفصیل سخن خواهیم گفت و در ادامه ی این فصل ، در مورد AP ها صحبت خواهیم نمود .

AP ، بین client device و wired network به نوعی bridge می زند . ویژگی اصلی AP های CUWN ، اینست که در واقع zero-touch management هستند ، یعنی نیازی به دسترسی مستقیم به آنها نیست (البته با فرض اینکه ارتباط layer 2 برقرار باشد) . لذا به محض اینکه plug in شدند و روشن شدند ، نیاز به انجام هیچ کاری در لایه ی AP نیست .

در ادامه ، با برخی از این AP ها بیشتر آشنا خواهیم شد .

Cisco 1130AG series AP :

برخی ویژگی های این سری ، بطور خلاصه عبارتند از :

- Autonomous / Lightweight
- 802.11a/b/g
- Integrated antennas
- Can operate at H-REAP device
- 802.11i/WPA2-compliant
- Office/hospital invironements
- 3dB gain for 2.4GHz
- 4.5dB gain for 5GHz

✓ **H-REAP یا همان Hybrid Remote Edge AP ، دستگاهیست که در یک گوشه ی دور یک WAN کار می کند و کنترلر آن در بخش core site است .**

Cisco 1240AG series AP :

برخی ویژگی های این سری ، بطور خلاصه عبارتند از :

- Autonomous / Lightweight
- 802.11a/b/g
- Only external antennas (dipole) with RP-TNC connectors
- Operate at H-REAP devices
- 802.11i/WPA2-compliant

Cisco 1250AG series AP :

از آنجا که این نوع AP ها از 802.11n draft استفاده می کنند (در زمان نگارش این کتاب (سال ۲۰۰۹) هنوز 802.11n یک استاندارد نبوده است)، می توان به data rate در حدود 300 Mbps روی هر رادیو با استفاده از تکنولوژی 2-by-3 MIMO رسید .

برخی ویژگی های این سری ، بطور خلاصه عبارتند از :

- Autonomous / Lightweight
- 802.11n draft version 2.0
- Modular
- 802.11i/WPA2-compliant
- 2.4GHz & 5GHz

Cisco 1300 series AP/Bridge :

این مدل دارای یک محافظ سخت است که می توان آن را در محیط های پرمخاطره نیز نصب کرد . سری ۱۳۰۰ ، در واقع یک point-to-point bridge **و نیز** point-to-multipoint bridge **خیلی خوب می باشد .**

برخی ویژگی های این سری ، بطور خلاصه عبارتند از :

- Bridge /support wireless clients too
- Only 802.11b/g
- Only 2.4GHz radio
- Integrated antenna & antenna connectors (2 versions)
- College campus with quad-type area , parks

Cisco 1400 series wireless bridge :

این مدل برای شبکه های point-to-point و point-to-multipoint طراحی شده است .

- Only Bridge
- Only standalone (it does not support LWAPP)
- Could change the polarization
- High-gain internal radio

جدول زیر ، مقایسه ای بین مدل های مختلف AP ها آورده است :

AP	Modes Supported	Environment	Antennas Supported	802.11 Protocols Supported	Max Data Rates Supported
1130AG	Autonomous/ lightweight AP.HREAP	Indoor	Integrated	a/b/g	54 Mbps
1240AG	Autonomous/ lightweight AP.HREAP	Rugged Indoor	External	a/b/g	54 Mbps
1250 AP	Autonomous/ lightweight AP	Rugged Indoor	External	a/b/g/n	300 Mbps
1300 AP/bridge	Autonomous/ lightweight AP, bridge	Outdoor	Internal or External	b/g	54 Mbps
1400	Bridge only (not an AP)	Outdoor	Internal or External	a/b/g	N/A

Cisco 44XX series WLC :

سری ۴۴۰۰ ، یک اینترفیس 10/100 دارد که به آن service port می گویند و برای ارتباطات SSH یا SSL برای اهداف مدیریت است . service port برای مدیریت out-of-band است ، اما برای مدیریت device لازم نیست ؛ زیرا Device ها را می توان از طریق اینترفیس مدیریت منطقی کنترلر (management logical controllers interface) مدیریت کرد . همچنین یک پورت console وجود دارد که با نرم افزارهای hyperterminal یا ... می توان به device وصل شد .

- Standalone WLC
- 12 , 25 , 50 , 100 Aps
- Supports 5000 MAC Addresses in database

هنگامیکه یک AP به یک WLC متصل می شود ، کنترلر AP را upgrade یا downgrade می کند ؛ زیرا AP و کنترلر باید در یک version باشند .

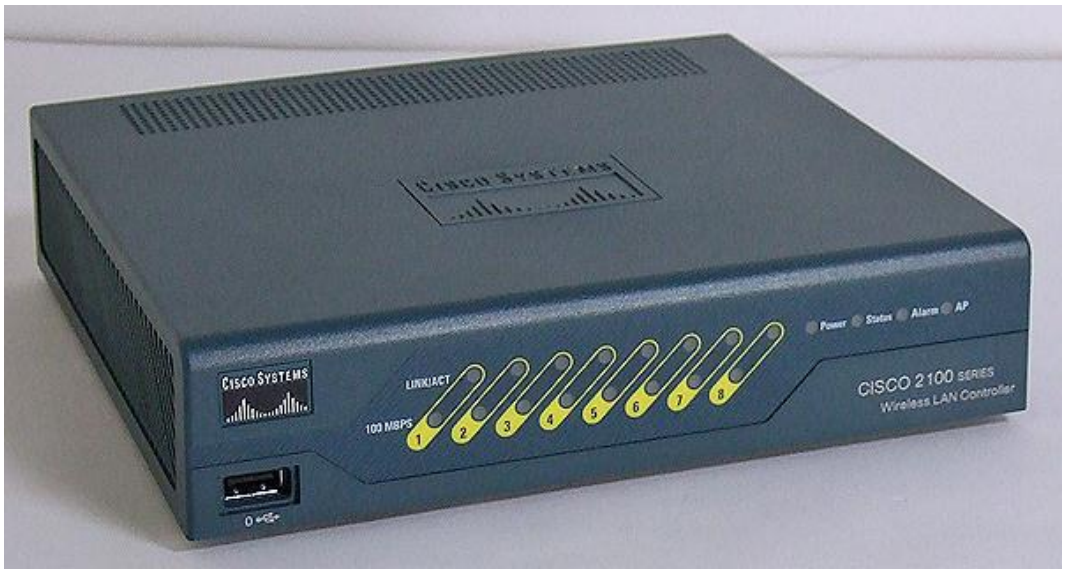
Cisco 3750-G WLC :

این مدل شبیه سری ۴۴۰۰ است و تنها در پورت های فیزیکی با هم تفاوت دارند .

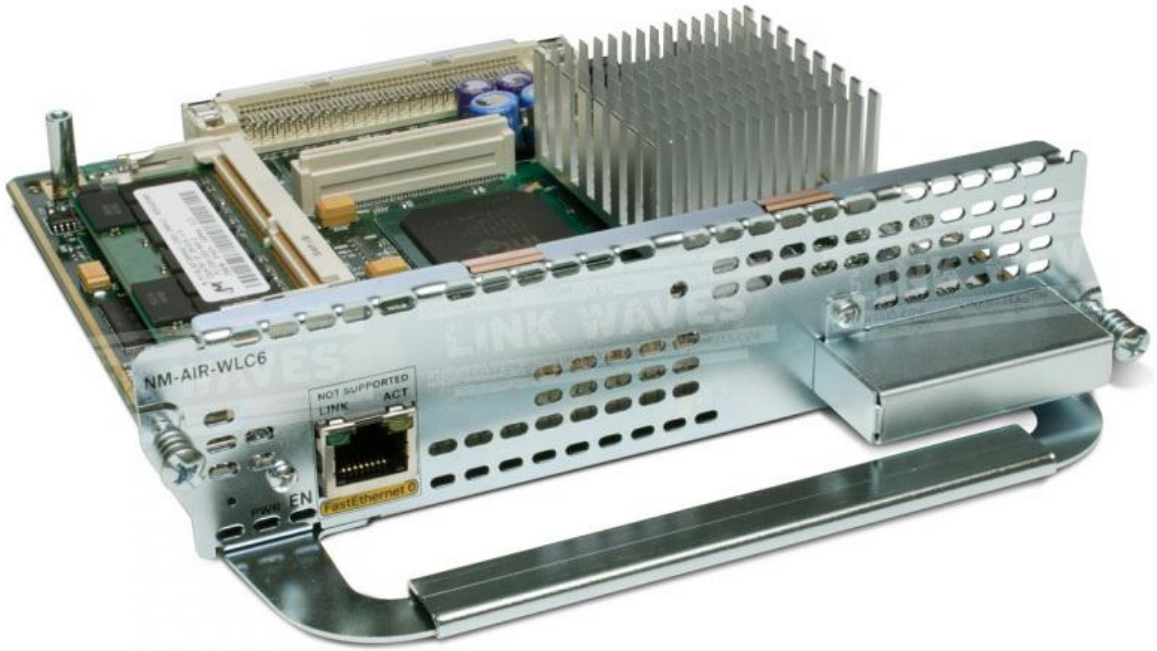
Cisco WiSM :

WiSM یک Service Module است که روی سوییچ های سری ۶۵۰۰ یا روتر های سری ۷۶۰۰ نصب می شود . تقریبا شبیه 4400 WLC است ، اما تا ۳۰۰ عدد AP ساپورت می کند (هر blade دو تا کنترلر دارد و هر کنترلر تا ۱۵۰ عدد AP ساپورت می کند) . همچنین می توان ۱۲ تا از آن را در یک mobility domain بصورت cluster در آورد .

Cisco 2106 WLC :



این سری نیز شبیه ۴۴۰۰ است ، اما 8 پورت سوییچ built-in دارد . ۶ عدد AP ساپورت می کند ، یک پورت کنسول RJ-45 و نیز دو پورت RJ-45 دارد که PoE ساپورت می کنند . می توانید این WLC ها را در محیط های کوچک مشاهده کنید .



این مدل برای روتر های ISR طراحی شده است ؛ شبیه 2106 است ، اما پورت کنسول یا AP متصل به خودش ندارد .
۸ یا ۱۲ عدد AP ساپورت می کند . این مدل را در دفاتر کوچک می توان مشاهده نمود .

در جدول زیر می توانید مدل های مختلف کنترلر ها را با یکدیگر مقایسه نمایید :

Controller Mode	Number of APs Supported	Environment Deployed In
4400	Up to 100	Enterprise
3750G	—	Enterprise
WiSM	300 per WiSM, up to 3600	Enterprise (service module)
2106	6	Branch
WLCM	6	Branch

مدیریت شبکه های Wireless :

WCS یا همان Wireless Control System یک مرکز مدیریت (برای ۳۰۰۰ عدد Lightweight AP و ۱۲۵۰ عدد Autonomous AP) است . WCS روی windows server یا Red Hat Linux server کار می کند . برای کنترل ۳۰۰۰ عدد AP نیاز به WCS Navigator داریم . WCS Navigator به ما این اجازه را می دهد تا سیستم های کنترلی وایرلس مختلف را هدایت کنیم . با استفاده از WCS Navigator ، می توان تا ۳۰.۰۰۰ عدد AP را در یک طراحی ، و تا ۲۰ طراحی WCS را کنترل نمود .

همچنین یک وسیله ی مفید دیگر وجود دارد به نام Cisco Wireless Location Appliance که برای ردیابی و مکان یابی دستگاههای Wi-Fi و RFID tag ها به کار می رود .

فصل یازدهم : آشنایی با فرآیند پیوستن AP به controller

- LWAPP
- LWAPP Layer 2 Transport Mode
- LWAPP Layer 3 Transport Mode
- چگونه LWAPP AP یک WLC را جستجو می کند
- نحوه ی انتخاب و پیوستن AP به کنترلر
- نحوه ی همسان سازی AP با کنترلر
- نحوه ی دریافت تنظیمات LWAPP AP از کنترلر
- Redundancy برای APها و کنترلر ها
- انواع فعالیت های AP
  - ✓ Local mode
  - ✓ Monitor mode
  - ✓ Sniffer mode
  - ✓ Rogue Detection mode
  - ✓ H-REAP mode
  - ✓ Bridging mode

زمانیکه یک Lightweight AP بوت می شود ، نمی تواند بدون کنترلر فعالیت کند و نیاز دارد که به یک کنترلر join شود . در این بخش با LWAPP و انواع فعالیت آن آشنا خواهیم شد . همچنین خواهیم دید که چگونه AP می تواند کنترلر ها را جستجو کند و از بین چندین کنترلر ، به یکی متصل شود و configuration های لازم را از آن بگیرد .

LWAPP :

LWAPP می تواند در دو حالت Layer2 و نیز Layer3 فعالیت کند (هرچند Layer2 دیگر از رده خارج شده و سیسکو پیشنهاد می کند که تنها از Layer3 استفاده شود) .

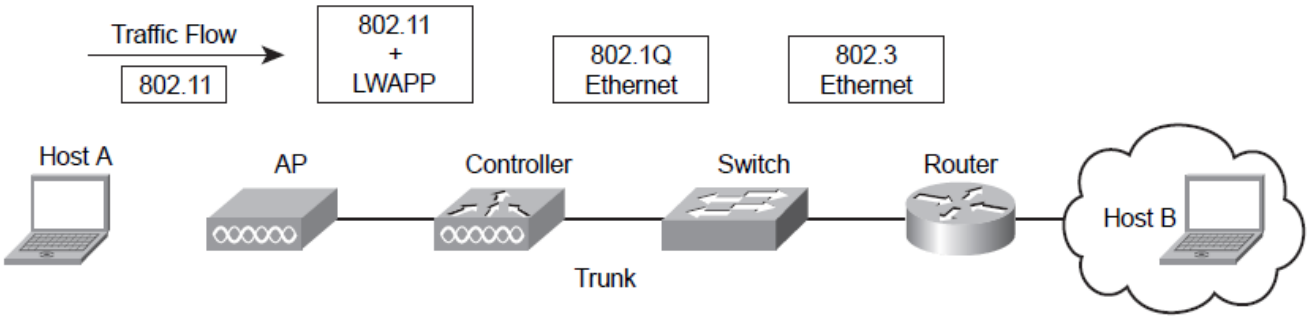
چنانچه AP دارای IP باشد ، مراحل فعالیت LWAPP بدین ترتیب می باشد :

۱. **Discovery** : در این مرحله پیام های درخواست و پاسخ discovery (بین AP و WLC) مبادله می شود .
۲. **Choosing** : در این مرحله ، AP از بین response های مختلف ، یک WLC را انتخاب می کند .
۳. **Joining** : در این مرحله ، پیام های درخواست و پاسخ پیوستن به LWAPP بین AP و WLC رد و بدل می گردد . این فرآیند شامل Authentication نیز می شود . یک encryption key تولید می شود تا بقیه ی فرایند پیوستن و نیز پیام های کنترلی LWAPP را امن و secure کند .
۴. **Synchronization** : پس از پیوستن AP به کنترلر ، چنانچه AP firmware با WLC مورد نظر یکی نباشد و mismatch وجود داشته باشد ، AP ورژن جدید را از WLC دانلود کرده ، خود را sync می کند .
۵. **Provisioning** : در این مرحله setting ها هماهنگ می شود (مثل SSID ، امنیت). همچنین پارامترهای 802.11 مانند سرعت ، کانال ها ، power و ... تنظیم می شوند .
۶. **Runtime** : پس از طی مراحل قبلی ، AP و WLC وارد runtime می شوند و ترافیک دیتا را سرویس دهی می کنند . طی این مرحله ، مرتبا پیام های keepalive ها ی LWAPP رد و بدل می شوند . چنانچه یک AP تعداد خاصی keepalive را از دست بدهد ، سعی می کند تا یک WLC جدید پیدا کند (discovery) .

LWAPP Layer 2 Transport Mode :

در این حالت حتی اگر همه ی AP ها هم IP بگیرند ، باز هم ارتباط AP با WLC در فریم های اترنت است ، نه پکت های IP . در این حالت AP باید در همان Ethernet network باشد که WLC قرار دارد ؛ لذا این حالت خیلی انعطاف پذیری ندارد .

توجه : پکت های دیتا بین client ها و سایر host ها ، همگی IP هستند .



LWAPP Layer 3 Transport Mode :

سیسکو این حالت را پیشنهاد می کند ، چون انعطاف پذیری بیشتری دارد . پیام های دیتا و کنترل L3 LWAPP روی شبکه ی IP توسط پکت های UDP منتقل می شوند .

Control message : UDP 12223 , Data message : UDP 12222

در این حالت ، بین آدرس IP مربوط به AP ، و آدرس IP مربوط به اینترفیس AP-manager کنترلر ، یک LWAPP Tunnel بوجود می آید .

نکته : وقتی فریم به WLC می رسد ، تمام header های آن برداشته می شود و WLC خودش اطلاعات لازم را اضافه می کند . مثلا در Layer3 ، وقتی فریم از AP به WLC می رسد ، تمام header های IP ، UDP ، Ethernet ، و غیره از فریم اصلی 802.11 حذف می شود و WLC خودش آن را در فریم اترنت encapsulate می کند .

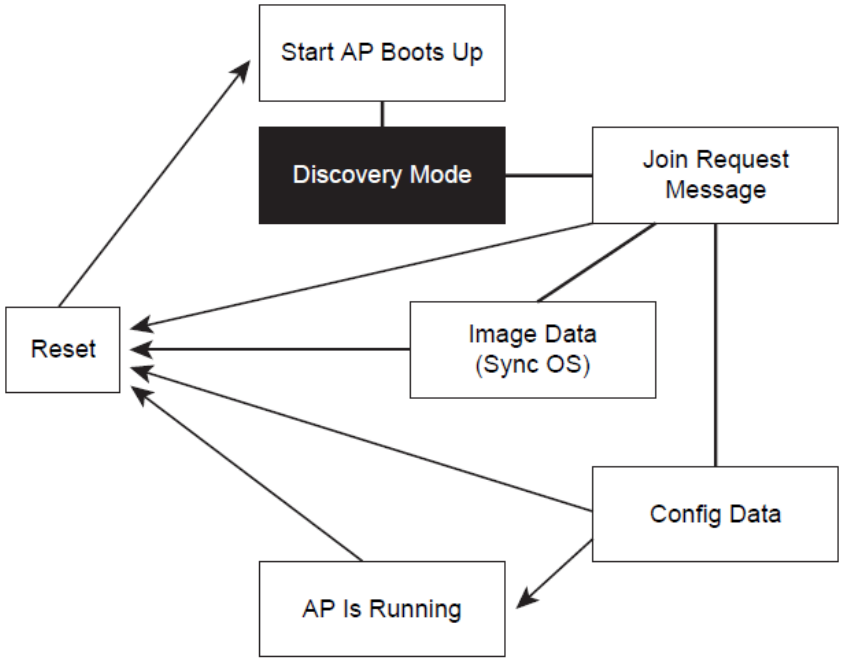
نکته : فرآیند ارسال فریم ها از client ها در حالت layer 3 ، شبیه به حالت layer 2 است ؛ اما در حالت Layer 3 ، فریم ها در UDP در واقع encapsulate می شوند .

توجه : همه ی عملیات encapsulate کردن فریم روی UDP و اعمال LWAPP header روی فریم و پکت ها ، در فاصله ی بین AP و WLC انجام می شود . یعنی در مسیر رفت ، AP این اطلاعات را اضافه کرده و با رسیدن به WLC این اطلاعات remove می شوند . در مسیر برگشت نیز WLC این اعمال را انجام می دهد تا اینکه AP همه ی آنها را برداشته و فریم 802.11 را می سازد .

چگونه یک LWAPP AP یک WLC را جستجو می کند :

Lightweight AP بصورت پیش فرض ، zero-touch است و نیازی به تنظیم ندارد و بصورت plug-and-play کار می کند . فرآیند discovery این AP ها به این شکل است :

۱- ابتدا AP یک تقاضا بصورت Layer 2 Broadcast ارسال می کند که مسلما fail می شود .
۲- AP در این مرحله IP خود را چک می کند ؛ اگر IP نداشت ، از DHCP استفاده می کند .
۳- AP با استفاده از اطلاعاتی که DHCP به او داده ، شروع به برقراری ارتباط با WLC می کند ؛ زیرا در Layer 3 ، به IP و Gateway نیاز داریم .
۴- اگر WLC پیدا شد ، WLC تقاضای AP را پاسخ می دهد (response)، وگرنه AP دوباره مرحله ی ۱ را تکرار می کند .



نکته : سیسکو از فرآیند hunting و الگوریتم discovery استفاده می کند تا AP بتواند تا حد ممکن هرچه WLC می تواند پیدا کند . AP یک لیست از این WLC ها می سازد تا بعدا بتواند یکی را انتخاب کند و به آن join شود .

برای پیدا کردن کنترلر ۳ راه وجود دارد (توجه کنید ، برای Dicovery ، نه Join) :

۱- ارسال LWAPP Discovery Requst توسط AP که می تواند در لایه ی ۲ یا ۳ ارسال گردد .
۲- استفاده از DHCP و خاصیتی در option آن که در هر vendor متفاوت است . مثلا option 43 می تواند IP اینترفیس مدیریتی یک کنترلر را بدست آورد .
۳- استفاده از DNS . با استفاده از DHCP ، اطلاعات IP یک DNS server را پیدا کرده ، سپس DNS entry مربوط به Cisco-LWAPP-Controller را پیدا می کنیم (یعنی آدرس اینترفیس مدیریتی کنترلر را پیدا می کنیم که AP می تواند به این اینترفیس یک Unicast Query ارسال نماید).

پروسه ی Layer3 Discovery شامل مراحل زیر می شود :

۱- AP یک subnet broadcast انجام می دهد تا ببیند آیا در local subnet هیچ کنترلری در لایه ی ۳ فعالیت می کند یا خیر .

۲- AP سپس OTAP را اجرا می کند (over-the-air provisioning در این کتاب بررسی نخواهد شد).

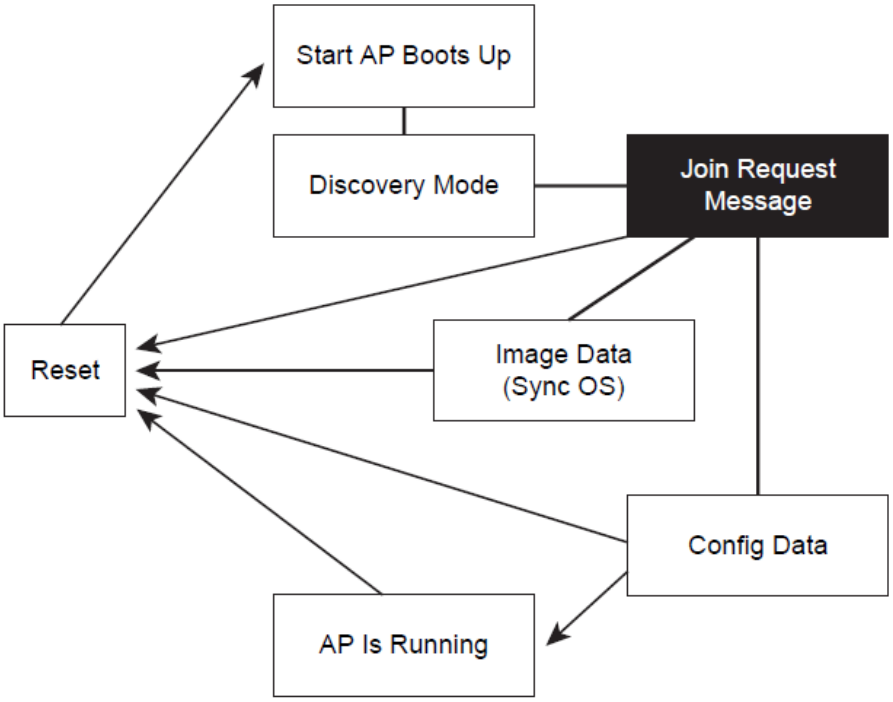
۳- هنگامیکه AP های دیگری به کنترلر join شده اند ، پیام هایی ارسال می کنند که برای resource management به کار می رود . AP می تواند به این پیام ها (که حاوی IP کنترلر نیز هست) گوش کرده و با یاد گرفتن آدرس IP کنترلر ، یک پیام discovery مستقیم به کنترلر ارسال نماید .

۴- این مرحله **AP Priming** نام دارد و درواقع شامل اتفاقاتیست که پس از associate شدن AP با حداقل یک کنترلر بوقوع می پیوندد .

پس از اینکه AP با WLC مورد نظر associate شد ، یک لیست از سایر کنترلر هایی که به آن WLC متصل هستند را می گیرد که همگی بخشی از Mobility Group هستند . این اطلاعات در NVRAM ذخیره می شود و برای ارتباط با آن کنترلر ها ، AP یک Broadcast به WLC خودش و سایر آن کنترلر ها ارسال می کند .

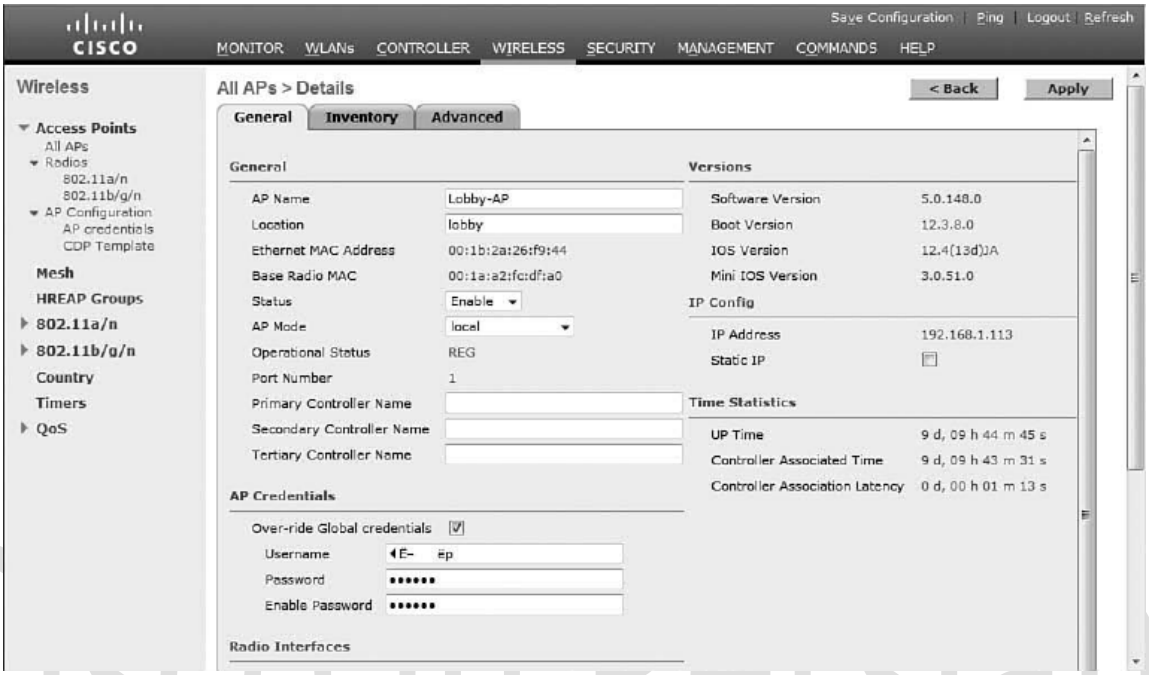
نکته : Primary WLC در FLASH ذخیره می شود ، سپس AP Priming انجام می شود تا سایر کنترلر ها پیدا شوند که اینها در NVRAM ذخیره می گردند تا در صورت reboot شدن ، از بین نروند . اما اطلاعات configuration در RAM قرار می گیرد و با Reboot شدن پاک می شود .

مرحله ی بعد ، join شدن AP به کنترلر است .



نحوه ی انتخاب و پیوستن AP به کنترلر :

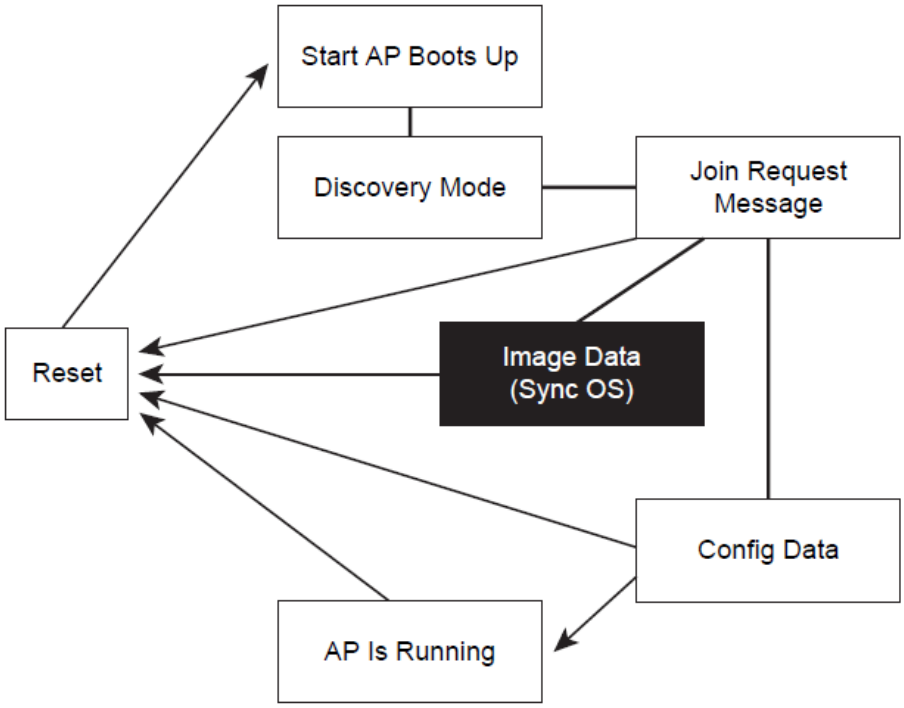
۱- AP اولین controller را انتخاب می کند و آن را به عنوان Primary در نظر می گیرد . می توان کنترلر اولیه را در هر AP تنظیم و در FLASH ذخیره نمود .



۲- AP دومین و نیز سومین کنترلر را انتخاب می کند .

۳- اگر هیچ اطلاعاتی نبود ، به حالت Master Controller می رود . هر Mobility Group تنها می تواند یک Master داشته باشد . پس از اینکه همه ی AP ها را شناساندیم ، باید این حالت را Disable کنیم .

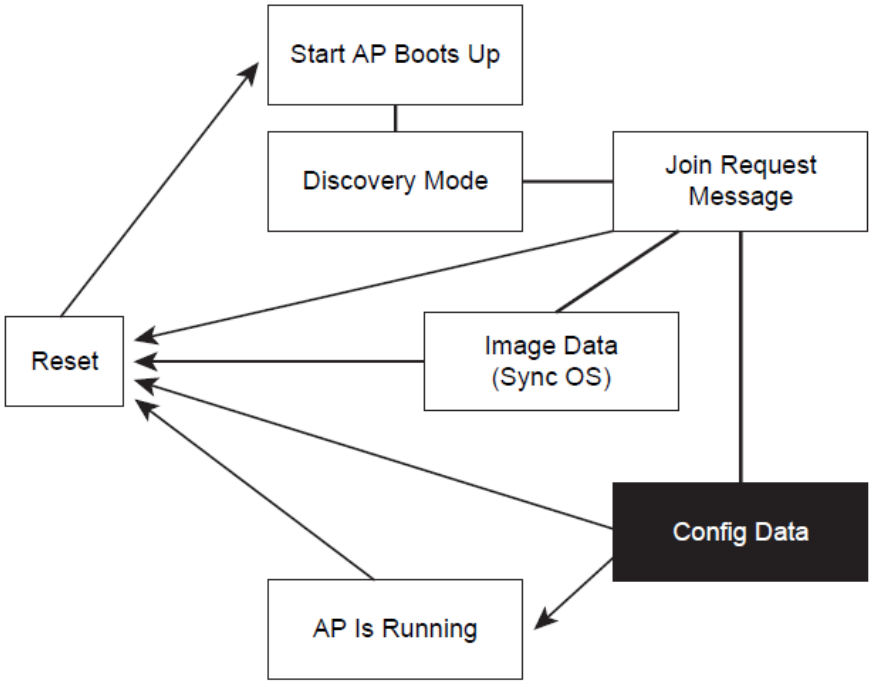
نحوه ی همسان سازی AP با کنترلر:



پس از join شدن ، اگر AP با WLC همسان و sync نباشد و image های مختلفی داشته باشند و در ورژن firmware های آنها mismatch وجود داشته باشد ، AP وارد مرحله ی Image Data (Sync OS) می شود ؛ وگرنه این مرحله را skip می کند .
در این مرحله ، کنترلر AP را Upgrade یا Downgrade می کند و سپس آن را reset می نماید . پس از Reset ، دباره پروسه ی boot up ، سپس Discovery و سپس Joining تکرار می شود .

سپس وارد مرحله ی Config Data می شود و AP تمام configuration خود را از کنترلر دریافت می نماید .

نحوه ی دریافت تنظیمات LWAPP AP از کنترلر:



در مرحله ی Config Data ، ابتدا AP پیام LWAPP Configuration Request را برای کنترلر می فرستد که حاوی پارامترهاییست که باید config شود (هم حاوی فیلد های خالیست که باید توسط کنترلر پر شوند و هم شامل value هاییست که توسط AP قبلا Set شده اند). کنترلر در پاسخ ، تمام این فیلد ها را تنظیم کرده و دوباره به AP می دهد .

نکته : این مقادیر در RAM ذخیره می گردند . خیلی مهم است که بدانید این مقادیر در FLASH ذخیره نمی گردند و با reboot شدن AP ، تمام این فرآیند ها دوباره از اول شروع می شود .

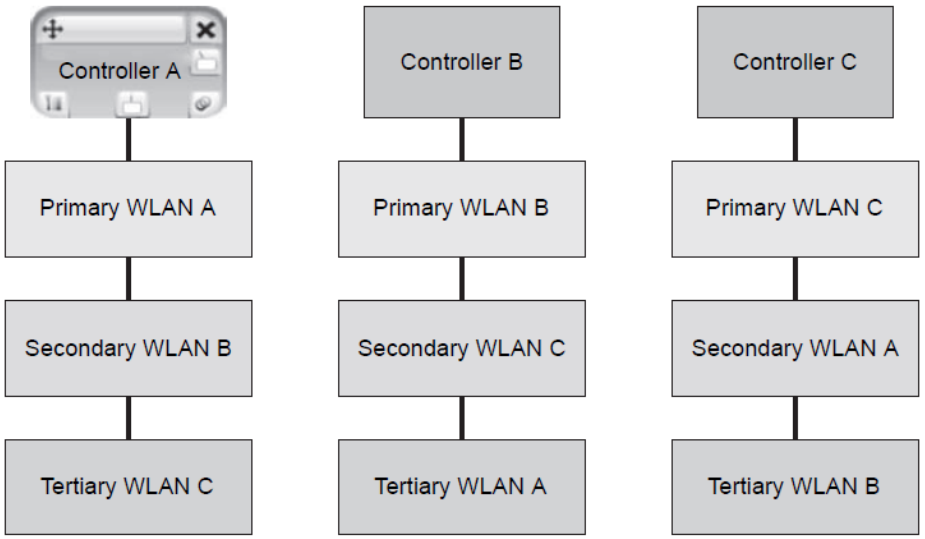
Redundancy برای AP ها و کنترلر ها :

در سطح CCNA Wireless ، شما باید با دو نوع redundancy آشنا باشید :

۱- **AP Redundancy** : این نوع در شرایطیست که AP ها در یک RF Domain قرار دارند و لذا طوری طراحی شده اند که در صورت وجود پوشش ضعیف ، بتوانند یکدیگر را ساپورت کنند ، که این کار را می توانند با افزایش سطح توان خروجی (با تغییر یک یا دو level) یا حتی با تغییر کانالی که در آن فعالیت می کنند ، انجام دهند .

۲- **Controller Redundancy** : این نوع از Redundancy خود شامل چند فرم مختلف است :

A. استفاده از کنترلر های Primary ، Secondary و نیز Tertiary .



B. استفاده از LAG یا همان Link Aggregation یا استفاده از چندین AP Manager

C. استفاده از پورت های Primary و Backup روی یک کنترلر

طراحی های رایج برای Controller Redundancy شامل موارد زیر می باشند :

- ✓ **N+1** : قرار دادن یک Backup برای چندین کنترلر . در این روش اگر بیش از یک کنترلر down شود ، مشکل بوجود می آید .
- ✓ **N+N** : هر کنترلر خودش Backup کنترلر دیگریست . در این روش ، بین AP ها و کنترلر ها نیاز به Load-Balancing داریم . چنانچه یک کنترلر با تعداد زیادی AP اشباع شود ، طراحی خوبی نخواهد بود .
- ✓ **N+N+1** : مانند N+N است ، اما یک کنترلر اضافه به عنوان Backup کلی وجود دارد که همه ی AP ها به آن به عنوان Tertiary (سومی) اشاره می کنند .

برای مطالعه ی بیشتر در زمینه ی **Redundancy** ، به بخش نشر دانش انجمن سیسکو به پارسی مراجعه فرمایید :

Redundancy – Resiliency - Backup

انواع فعالیت های AP :

هرچند بیشتر مردم از AP انتظار دارند که به آنها اینترنت بدهد ، اما AP می تواند در حالت های گوناگون فعالیت های مختلفی انجام دهد .

- ✓ **Local Mode** : در این حالت AP تمام کانال ها را در پریود های ۱۸۰ ثانیه ای اسکن می کند (برای خدماتی چون monitoring ترافیک) . این حالت می تواند برای Site Survey نیز مورد استفاده قرار گیرد .

- ✓ **Monitor Mode** : این حالت Passive است ؛ یعنی AP هیچ گونه ترافیکی ارسال نمی کند و اجازه ی ارتباط کاربران را نمی دهد . این حالت برای یافتن Rogue AP یا IDS Machines ، همچنین برای Troubleshooting یا Site Survey به کار می رود . AP هایی که در این حالت هستند ، می توانند برای دقت بالاتر ، با Location Appliance فعالیت کنند . دستور زیر می توان مقدار کانالی که مانیتور می شود را تغییر دهد :

Config advanced 802.11b monitor channel-list

- ✓ **Sniffer Mode** : این حالت در Data Capturing به کار می رود و با یک Omnipeak ، Airmagnet ، یا یک Wireshark Server به فعالیت می پردازد .

- ✓ **Rogue Detection Mode** : در این حالت ، رادیو های AP خاموش هستند و روی شبکه ی wired به پیام های ARP گوش می دهند . چنانچه یک ARP روی wired LAN شنیده شود ، کنترلر یک alarm تولید می کند .

- ✓ **H-REAP Mode** : این حالت برای موقعی طراحی شده که AP هایی در اطراف WAN دارید و می خواهید کنترلر را در بخش مرکزی بگذارید . در این حالت AP تنها در مرحله ی اولیه نیاز به برقراری یک ارتباط کوتاه با کنترلر دارد ، و از آن به بعد می تواند بدون استفاده از کنترلر به فعالیت کن (در سطحی پایین تر) ادامه دهد . این حالت ، شامل دو مدل connected و standalone می باشد .

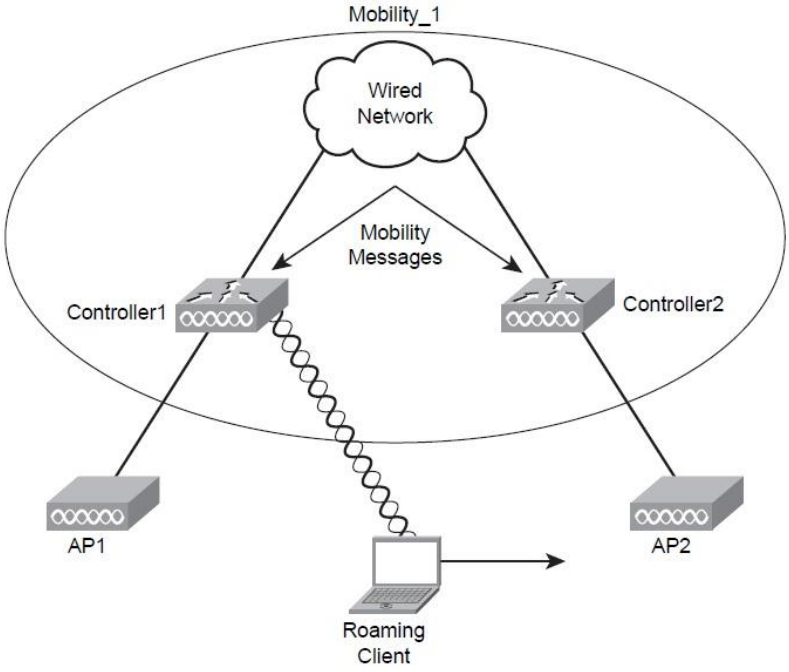
- ✓ **Bridging Mode** : در این حالت ، AP نقش یک bridge را بازی می کند و اجازه ی دسترسی کاربر را می دهد . Ap می تواند از لینک های point-to-point یا point-to-multipoint استفاده کند . برای تشخیص بهترین مسیر ، AP از یک پروتکل به نام AWPP استفاده می کند (Adaptive Wireless Path Protocol) که سیسکو برای indoor AP ها به آن iMesh می گوید ، و برای outdoor AP ها ، آن را mesh می نامد .

- Mobility ❖
- Roaming ❖
  - Layer 2 Roaming ✓
  - Layer 3 Roaming ✓

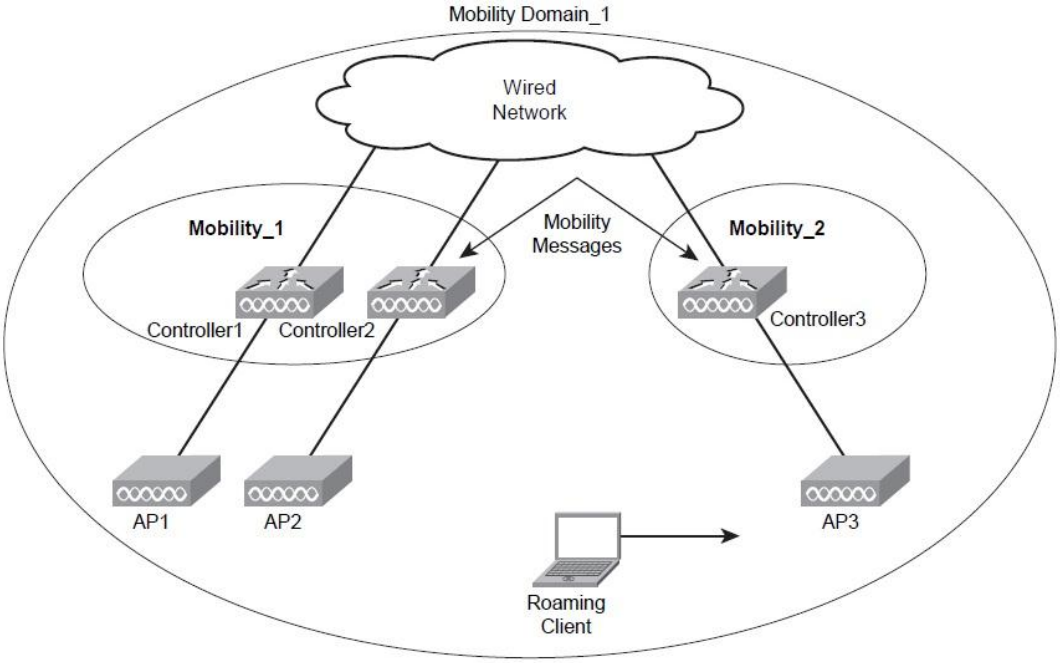
کاربران دوست دارند به راحتی در شبکه ی وایرلس جابجا شوند ، بدون اینکه مشکلی در ارتباط آنها بوجود آید ؛ در چنین جایی roaming وارد عمل می شود . در این فصل با اجزاء این قابلیت بیشتر آشنا می شویم .

Mobility :

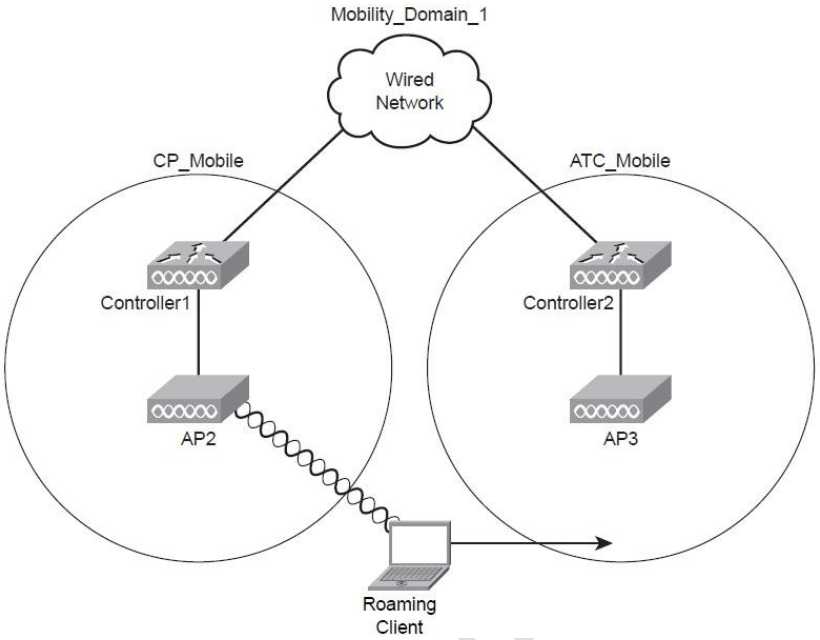
mobility group از ترکیب چندین کنترلر که هرکدام دربرگیرنده ی چندین AP می باشند ، تشکیل شده است :



و چندین mobility group با هم ، یک mobility domain را تشکیل می دهند :

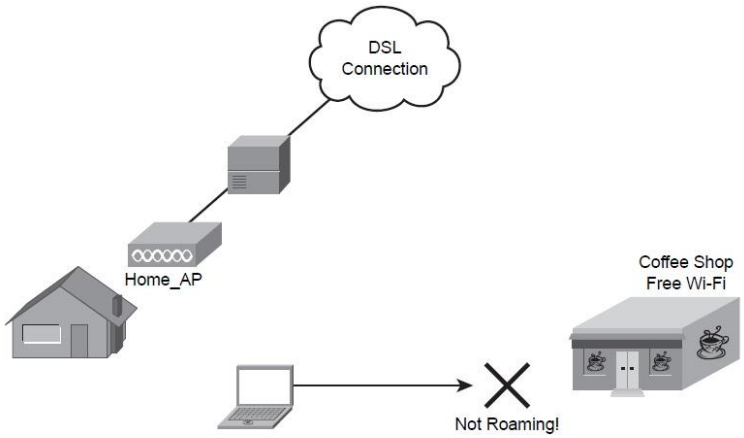


کنترلر هایی که در یک mobility group هستند ، می توانند با یکدیگر ارتباط داشته باشند و همگی دارای virtual gateway IP Address یکسانی هستند .



Roaming :

Roaming به معنای حرکت کاربر از یک AP به AP دیگر است ، در حالیکه همچنان در حال برقراری ارتباط و transmission است . عملیات roaming میتواند بین چندین mobility group انجام شود ، اما باید حتما درون یک mobility domain انجام گیرد ؛ زیرا اگر یک کاربر که در یک domain خاص ، associate شده است (و البته قبل از آن authenticate شده) ، به mobility domain دیگری برود ، چون در دامین جدید اطلاعاتی در مورد این client موجود نیست ، باید دوباره عملیات association را انجام دهد ، لذا IP جدیدی دریافت خواهد کرد و همه ی session هایی کنونی باید restart شوند ! لذا مثلا در شکل زیر ، client نمی تواند roaming کند ، چون با حرکت به سمت کافی شاپ ، یک IP جدید خواهد داشت و session هایی که active بودند ، همگی restart می گردند.



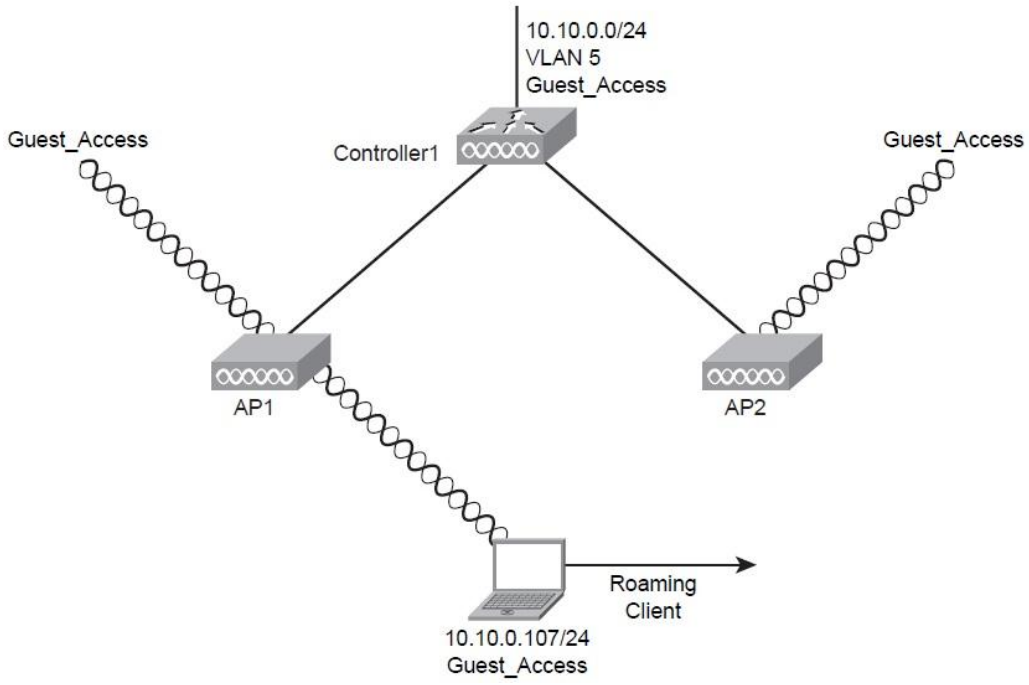
برای انجام roeming ، کنترلر ها باید چند شرط زیر را داشته باشند :

- ✓ همگی عضو یک mobility domain باشند .
- ✓ همگی یک code revision را run کنند .
- ✓ همگی روی یک LWAPP mode عمل کنند .
- ✓ ACL روی شبکه یکسان باشد .
- ✓ SSID همه ی آنها (در مورد WLAN) یکسان باشد.

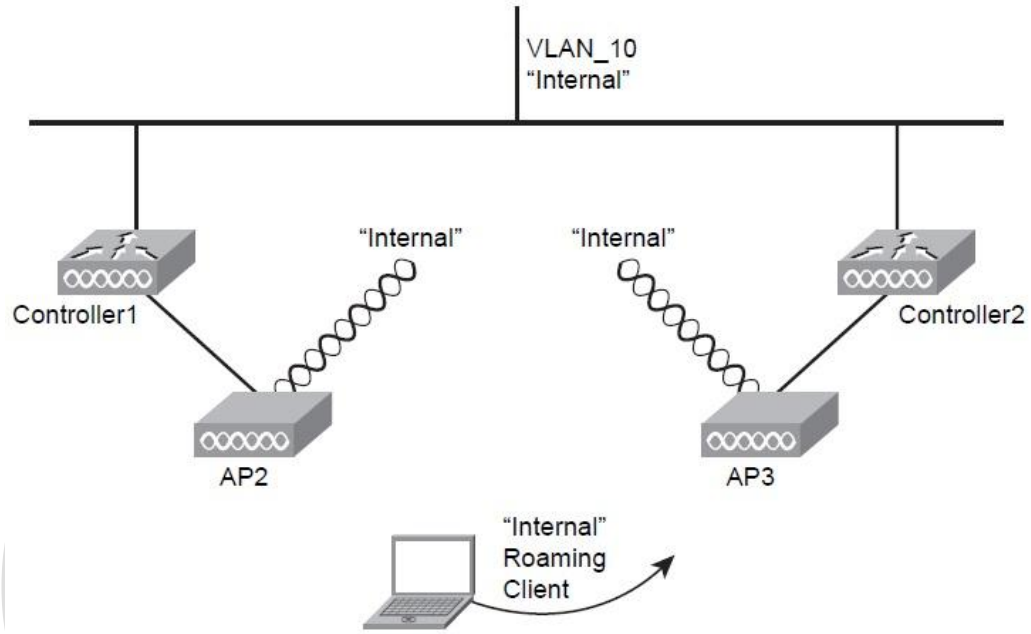
به طور کلی دو نوع roaming وجود دارد :

۱. **Layer 2 Roaming** : هنگامیست که یک client از یک AP به AP دیگری roam می کند ، در حالیکه IP subnet خودش را حفظ میکند. در این نوع roaming ، کاربردر مسیر حرکت خود ، در یک IP subnet و نیز در یک Vlan باقی می ماند . نتیجه اینکه نیازی به فرآیند DHCP برای assign کردن IP جدید نخواهد بود (زیرا DHCP می تواند باعث قطع شدن session شود).

- **Intracontroller Roaming** : وقتی کاربر به AP جدید رسید ، یک query برای authentication ارسال میکند . AP این query را برای کنترلر ارسال میکند و کنترلر می فهمد که این client قبلاauthenticate شده است (منتهی از طریق یک AP دیگر) . تمام این فرآیند در یک کنترلر انجام می پذیرد و کمتر از 10 ms زمان می برد .



- **Intercomntroller Roaming** : بین چندین کنترلر ، اما درون یک mobility group انجام می شود . در این حالت ، با حرکت client از یک کنترلر به کنترلر دیگر ، اطلاعات و Database آن ، به کنترلر ثانویه منتقل شده و از روی کنترلر اولیه remove می گردد . این فرایند در حدود 20 ms زمان می برد .



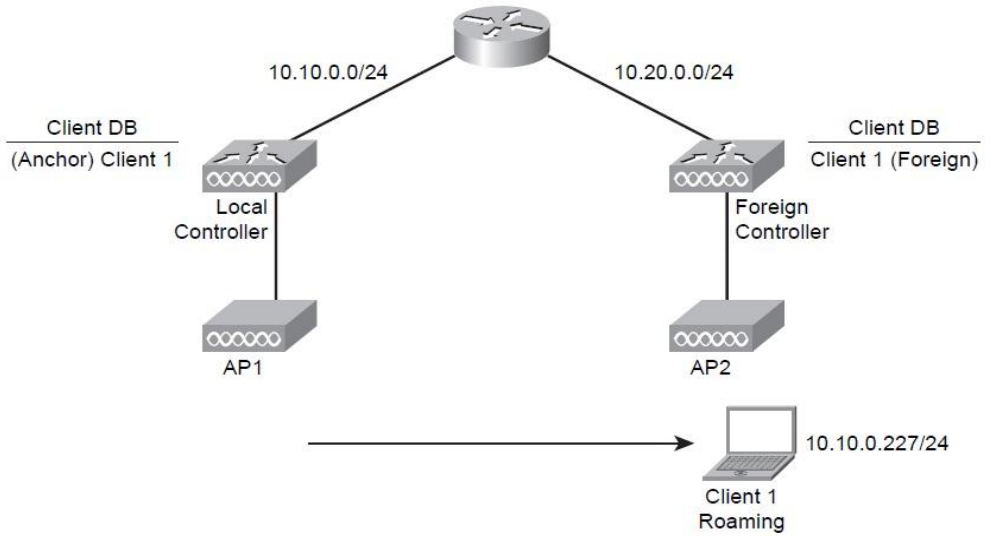
توجه : در هر دوحالت Inter وIntra ، فرآیند roaming از نظر client شبکه ، کاملا transparent و نامحسوس می باشد .

۲. **Layer 3 Roaming** : هنگامیست که یک کاربر از یک AP روی یک subnet خاص ، به AP دیگری روی یک subnet دیگر roam می کند ، اما همچنان از یک SSID استفاده می کند . در این حالت ، با وجود اینکه کنترلر ها روی subnet های مختلف هستند ، اما client آدرس های IP را تغییر نمی دهد ؛ در عوض ، کنترلرها به کنترلر اصلی tunnel می زنند . در واقع این حالت ، یک نوع تنظیم smoke-and-mirrors است ، لذا در واقع می توان شبکه را متقاعد کرد که اصلا roaming اتفاق نیفتاده است .

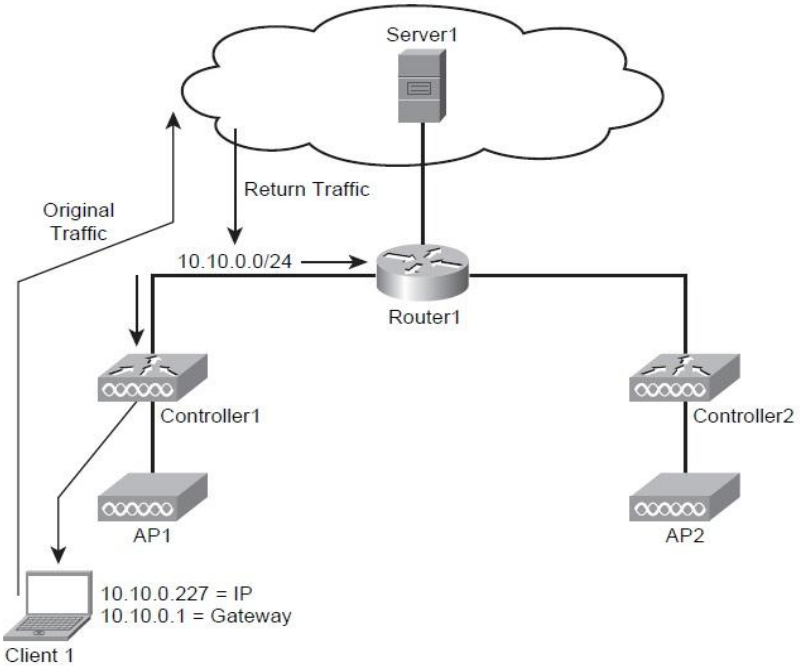
در این حالت با حرکت client از یک کنترلر به کنترلر دیگر ، client's entry در کنترلر اصلی به عنوان anchor مارک زده می شود و Database آن به Foreign Controller کپی می گردد (توجه : remove نمی شود) و در آنجا به عنوان Foreign مارک زده می شود . (Original Controller = Anchor Controller)

این نوع roaming ، از دو نوع tunneling استفاده می کند :

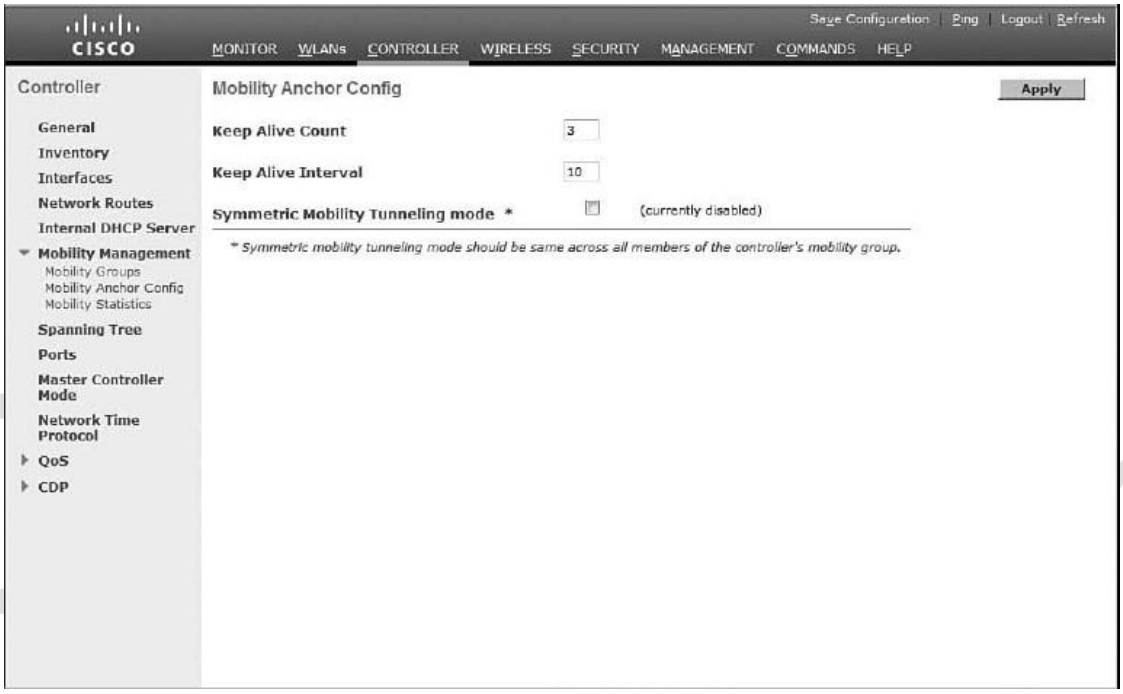
- **Asymmetric tunneling** : در این حالت ، بدون در نظر گرفتن آدرس مبدا ، ترافیک از کاربر به سمت destination میرود و در بازگشت ، به کنترلر اصلی (به نام anchor controller) رفته ، سپس به کنترلر جدید tunnel میشود .

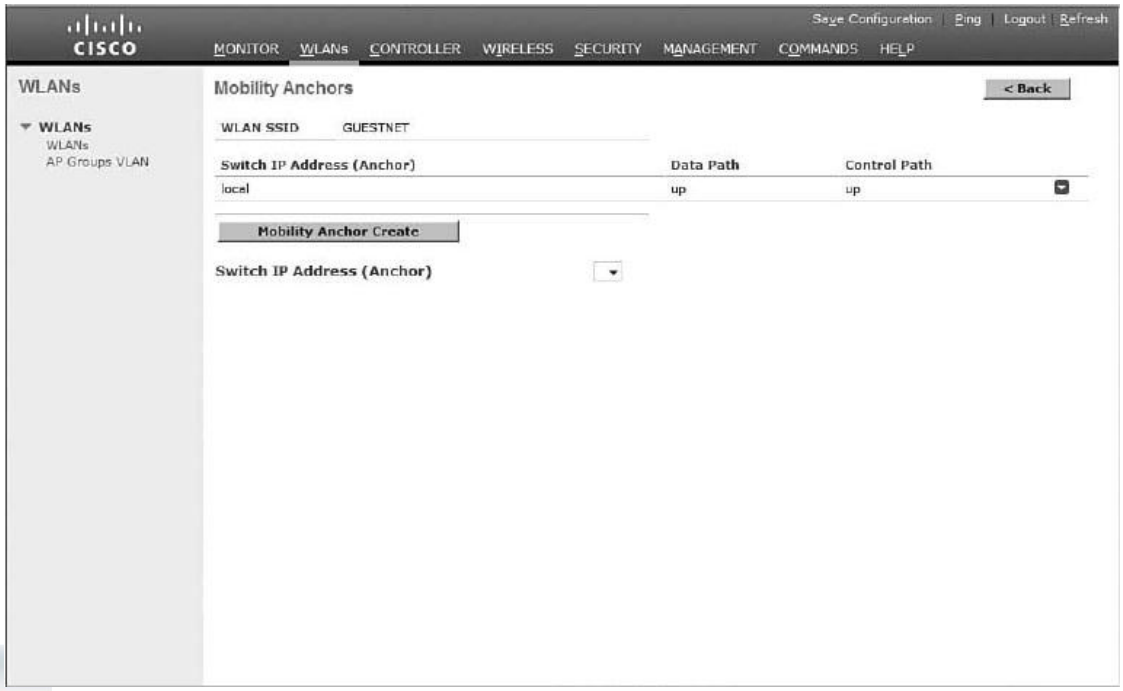


- **Symmetric tunneling** : در این حالت ، ترافیک از کاربر به anchor controller و سپس destination می رود ، و در بازگشت به anchor controller آمده ، سپس از طریق foreign controller دوباره به کاربر tunnel می شود . در این حالت اگر client به کنترلر جدیدی برود ، Database آن به foreign controller جدید منتقل می شود ، اما anchor controller بدون تغییر باقی می ماند .



البته قابلیتی به نام mobility anchor وجود دارد که کنترل بیشتری روی user traffic دارد و باعث می شود که کاربران بتوانند به هر کنترلی که می خواهند ، anchor شوند (نه اینکه صرفا به اولین کنترلر anchor باقی بمانند) ؛ چون با گذشت زمان و تغییر شرایط ، ممکن است فاصله ی آنها خیلی زیاد شده ، روی کیفیت ارتباط تاثیر بگذارد . همچنین می توان مثلا کاربران را به اینترفیس DMZ یک فایروال anchor کرد تا هر ترافیکی ، ابتدا از firewall بگذرد و سپس به client برسد . برای ساخت و تنظیم mobility anchor به این ترتیب عمل می شود :





فصل سیزدهم : تنظیمات اولیه و مانیتورینگ با کنترلر

- Static Interface
  - Management Interface ✓
  - AP Manager Interface ✓
  - Virtual Interface ✓
  - Service Port ✓
- اتصال به کنترلر
- تنظیمات اولیه CLI
- تنظیمات اولیه Web
- Monitoring با استفاده از کنترلر
- مدیریت Rogue AP
- مدیریت کاربران

هدف نهایی در هر شبکه ی وایرلس ، برقراری ارتباط از یک کاربر به سوی WLAN و از آنجا به سمت مقصدی دیگر است . لذا باید با نحوه ی کار کنترلر ها آشنا باشید ، همچنین باید نحوه ی برقراری ارتباط با یک کنترلر ، نحوه ی تنظیمات WLAN از طریق GUI یک کنترلر ، و نیز چگونگی مانیتورینگ کنترلر را بدانید . در این فصل به همه ی این موارد خواهیم پرداخت .

Static Interface :

برخلاف اینترفیس های dynamic که توسط administrator ها تعریف می شوند ، اینترفیس های استاتیک توسط system ها معرفی می گردند . این اینترفیس ها شامل انواع زیر می شوند :

- ✓ **Management Interface** : اینترفیس مدیریتی می تواند فریم ها را بدون tag ارسال کند . لذا فریم ها به native vlan هر سوییچ ارسال می شوند و دارای تگ 1Q. نخواهند بود . AP از این اینترفیس برای پیدا کردن کنترلر استفاده می کند .
- ✓ **AP Manager Interface** : آدرسی که به این اینترفیس داده می شود باید یکتا باشد ، چون در ارتباطات بین AP و WLC به عنوان SA از آن استفاده می شود .
- ✓ **Virtual Interface** : این اینترفیس ، همه ی پورت های فیزیکی کنترلر را کنترل می کند . مثلا وقتی یک کاربر می خواهد از طریق web به شبکه وایرلس وصل شود ، ابتدا به اینترفیس مجازی redirect می شود تا عملیات Authentication انجام شود ، سپس به home page خود می رود .
- ✓ **Service Port** : نوع دیگری از اینترفیس استاتیک است که برای مدیریت out-of-band به کار می رود ؛ لذا می تواند به منظور recovery سیستم یا نگهداری سیستم مورد استفاده قرار گیرد . این پورت ، تنها پورتیست که هنگام بوت شدن کنترلر نیز active است .

نکته : از طریق web interface نمی توان برای Service port یک default gateway تنظیم کرد ، اما می توان از طریق CLI یک static route تعریف نمود. برای این کار از دستور ***config route*** استفاده می نماییم .

اتصال به کنترلر :

با استفاده از یک کابل سریال DB9 می توان به اینترفیس سریال متصل گردید . در شکل زیر ، مراحل بوت شدن کنترلر را مشاهده می فرمایید :

```
Bootloader 4.1.171.0 (Apr 27 2007 - 05:19:36)
Motorola PowerPC ProcessorID=00000000 Rev. PVR=80200020
CPU: 833 MHz
CCB: 333 MHz
DDR: 166 MHz
LBC: 41 MHz
L1 D-cache 32KB, L1 I-cache 32KB enabled.
I2C: ready
DTT: 1 is 20 C
DRAM: DDR module detected, total size:512MB.
512 MB
8540 in PCI Host Mode.
8540 is the PCI Arbiter.
Memory Test PASS
FLASH:
Flash Bank 0: portsize = 2, size = 8 MB in 142 Sectors
8 MB
L2 cache enabled: 256KB
Card Id: 1540
Card Revision Id: 1
Card CPU Id: 1287
Number of MAC Addresses: 32
Number of Slots Supported: 4
Serial Number: FOC1206F03A
Unknown command Id: 0xa5
```

```
Unknown command Id: 0xa4
Unknown command Id: 0xa3
Manufacturers ID: 30464
Board Maintenance Level: 00
Number of supported APs: 12
In: serial
Out: serial
Err: serial

.o88b. d888888b .d8888. .o88b. .d88b.
d8P Y8 `88' 88' YP d8P Y8 .8P Y8.
8P 88 `8bo. 8P 88 88
8b 88 `Y8b. 8b 88 88
Y8b d8 .88. db 8D Y8b d8 `8b d8'
`Y88P' Y888888P `8888Y' `Y88P' `Y88P'
Model AIR-WLC4402-12-K9 S/N: FOC1206F03A
Net:
PHY DEVICE : Found Intel LXT971A PHY at 0x01
FEC ETHERNET
IDE: Bus 0: OK
Device 0: Model: STI Flash 8.0.0 Firm: 01/17/07 Ser#: STI1M75607342054704
Type: Removable Hard Disk
Capacity: 245.0 MB = 0.2 GB (501760 x 512)
Device 1: not available
Booting Primary Image...
Press <ESC> now for additional boot options...
***** External Console Active *****
Boot Options
Please choose an option from below:
1. Run primary image (version 4.1.192.17) (active)
2. Run backup image (version 4.2.99.0)
3. Manually update images
4. Change active boot image
5. Clear Configuration
Please enter your choice:
```

در ابتدا کنترلر دنبال یک configuration file می گردد . اگر آن را پیدا کرد که load کرده و از ما تقاضای username و password می کند . اما اگر هیچ configuration ی وجود نداشت ، یک پیغام می دهد که اعلام می کند که هیچ تنظیمی وجود ندارد . (این واکنش ، تقریبا شبیه به روتر است که اگر فایل config نداشته باشد ، وارد setup mode می شود و از آنجا یک سری تنظیمات را می توان انجام داد.)

```
Starting LOCP: ok
Starting CIDS Services: ok
Starting Ethernet-over-IP: ok
Starting Management Services:
Web Server: ok
CLI: ok

Secure Web: Web Authentication Certificate not found (error).
(Cisco Controller)


Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_32:af:43]:
```


تنظیمات اولیه CLI :

در این مرحله ، می توان تنظیمات مختلفی را انجام داد که در شکل زیر مشاهده می نمایید :

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_32:af:43]: WLC_1
Enter Administrative User Name (24 characters max): admin
```

```
Enter Administrative Password (24 characters max): *****
Re-enter Administrative Password : *****
Service Interface IP Address Configuration [none][DHCP]: 10.1.1.1
Invalid response

Service Interface IP Address Configuration [none][DHCP]: none
Service Interface IP Address: 10.1.1.1
Service Interface Netmask: 255.255.255.0
Enable Link Aggregation (LAG) [yes][NO]:
Management Interface IP Address: 192.168.1.75
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 192.168.1.1
Management Interface VLAN Identifier (0 = untagged):
Management Interface Port Num [1 to 2]: 1
Management Interface DHCP Server IP Address: 192.168.1.1
AP Transport Mode [layer2][LAYER3]:
AP Manager Interface IP Address: 192.168.1.80
AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (192.168.1.1):
Virtual Gateway IP Address: 1.1.1.1
Mobility/RF Group Name: CP_Mobile1
Enable Symmetric Mobility Tunneling [yes][NO]: no
Network Name (SSID): OpenAccess
Allow Static IP Addresses [YES][no]:
Configure a RADIUS Server now? [YES][no]:
Enter the RADIUS Server's Address: -
Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.
Enter Country Code list (enter 'help' for a list of countries) [US]:
Enable 802.11b Network [YES][no]:
Enable 802.11a Network [YES][no]:
Enable 802.11g Network [YES][no]:
Enable Auto-RF [YES][no]:
Configuration saved!
Resetting system with new configuration...

Configuration saved!
Resetting system with new configuration...
Bootloader 4.1.171.0 (Apr 27 2007 - 05:19:36)
Motorola PowerPC ProcessorID=00000000 Rev. PVR=80200020
CPU: 833 MHz
CCB: 333 MHz
DDR: 166 MHz
LBC: 41 MHz
```

```
L1 D-cache 32KB, L1 I-cache 32KB enabled.
I2C: ready`
DTT: 1 is 31 C
DRAM: DDR module detected, total size:512MB.
512 MB
8540 in PCI Host Mode.
8540 is the PCI Arbiter.
Memory Test PASS
```

پس از اینکه کنترلر reboot شد ، از ما تقاضای username و password می کند :

```
Enter User Name (or 'Recover-Config' this one-time only to reset configura-
tion to factory defaults)
User: admin
Password:*****
(Cisco Controller) >
```


برای ذخیره کردن تنظیمات ، از دستور زیر می توان استفاده نمود :

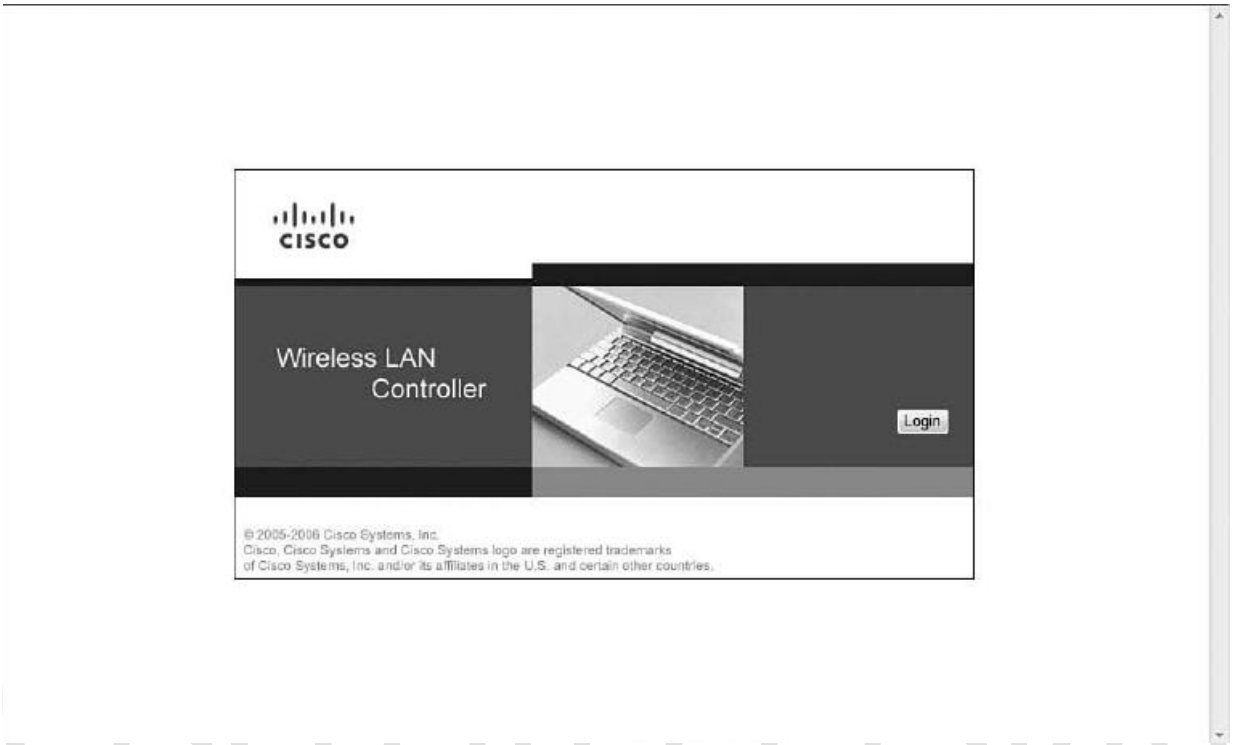
```
(Cisco Controller) >save config
Are you sure you want to save? (y/n) y

Configuration Saved!
(Cisco Controller) >
```

همچنین می توانید از دستورات debug استفاده نمایید .

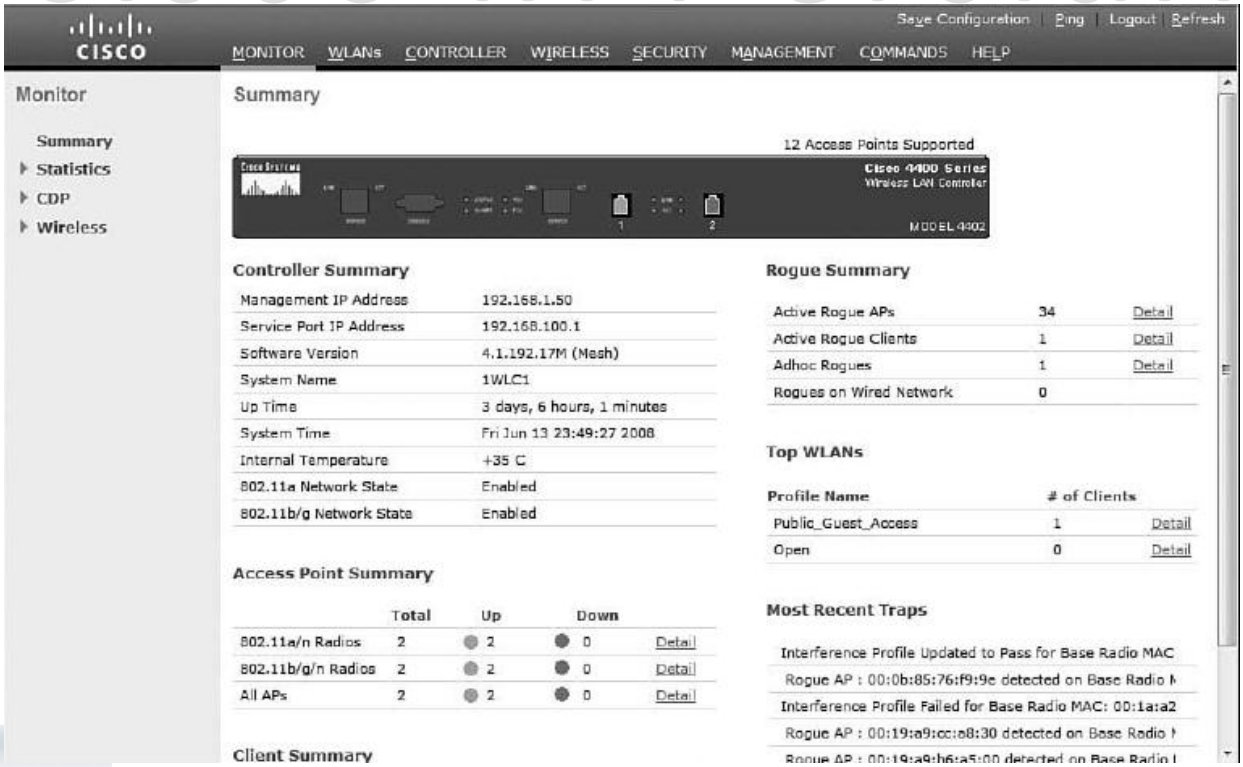
نکته : دستور Debug از طریق web interface قابل اجرا نیست .

تنظیمات اولیه Web :

ابتدا به آدرس IP پیشفرض کنترلر (که معمولا 192.168.1.1 است) ، متصل می شویم :

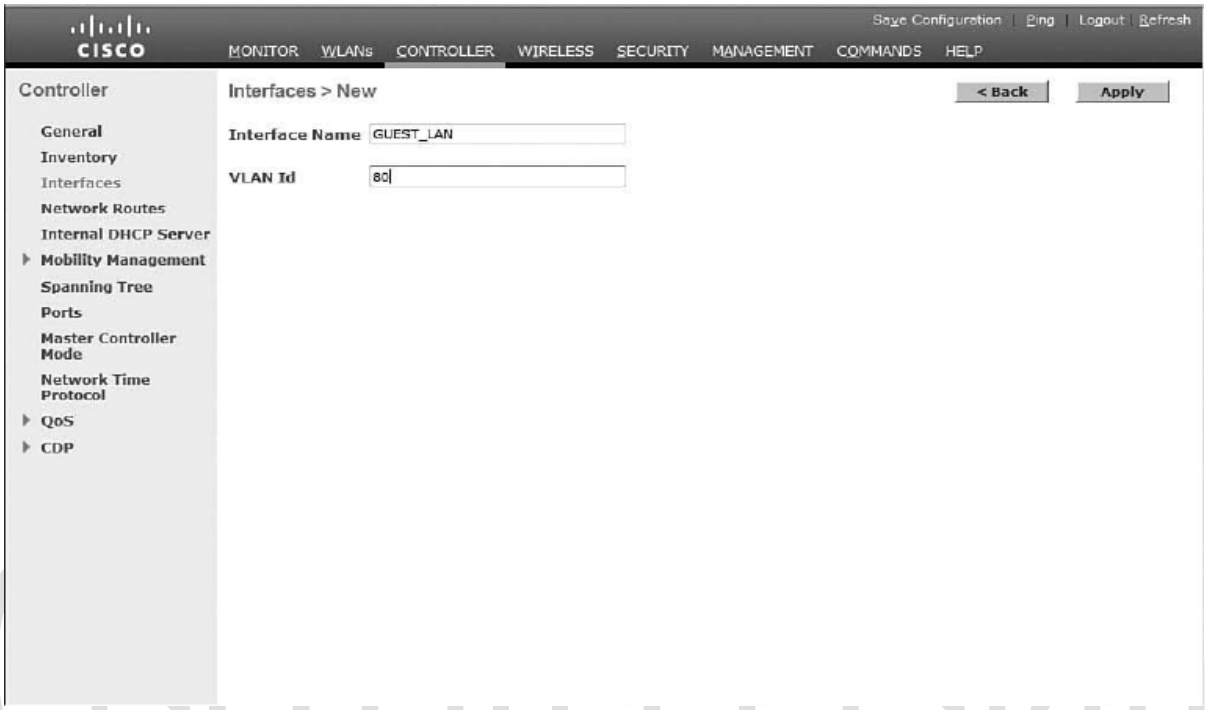


پس از اتصال ، صفحه ی خلاصه ی وضعیت کنترلر را مشاهده می کنید :

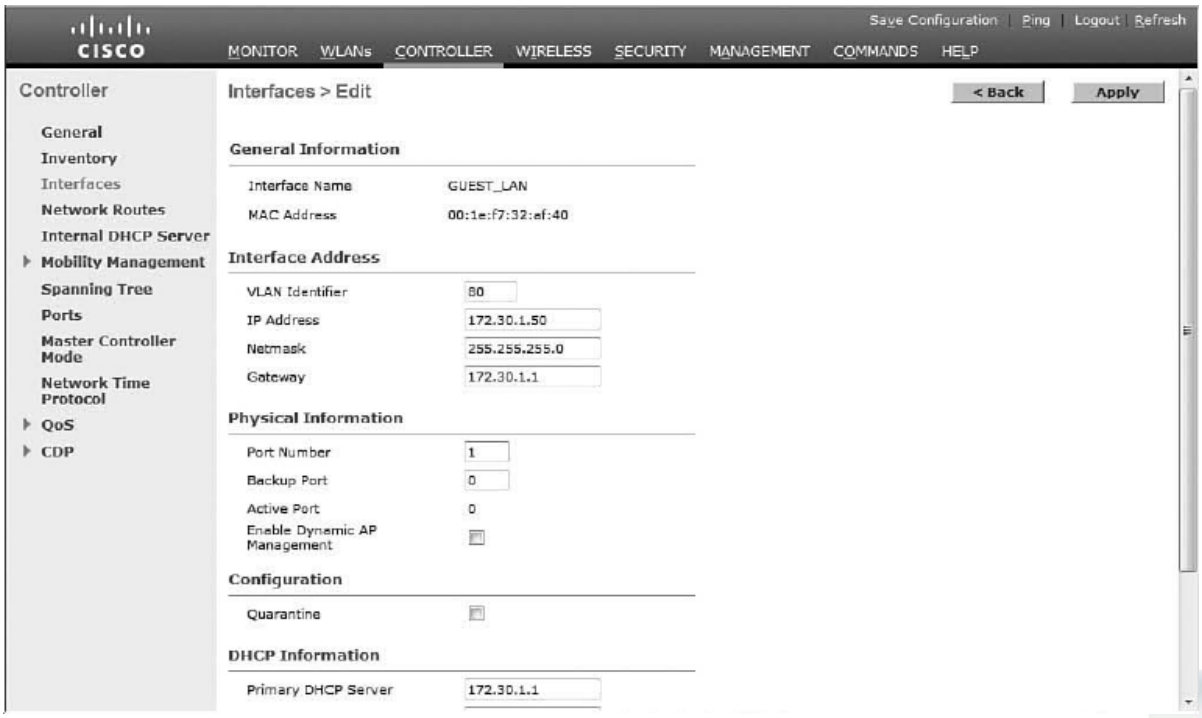


سپس نوبت به ساخت controller interface می رسد . توجه داشته باشید که بخش WLAN ، قسمت وایرلس را تعریف می کند ، و بخش Interface ، قسمت wired تنظیمات را مشخص می نماید .

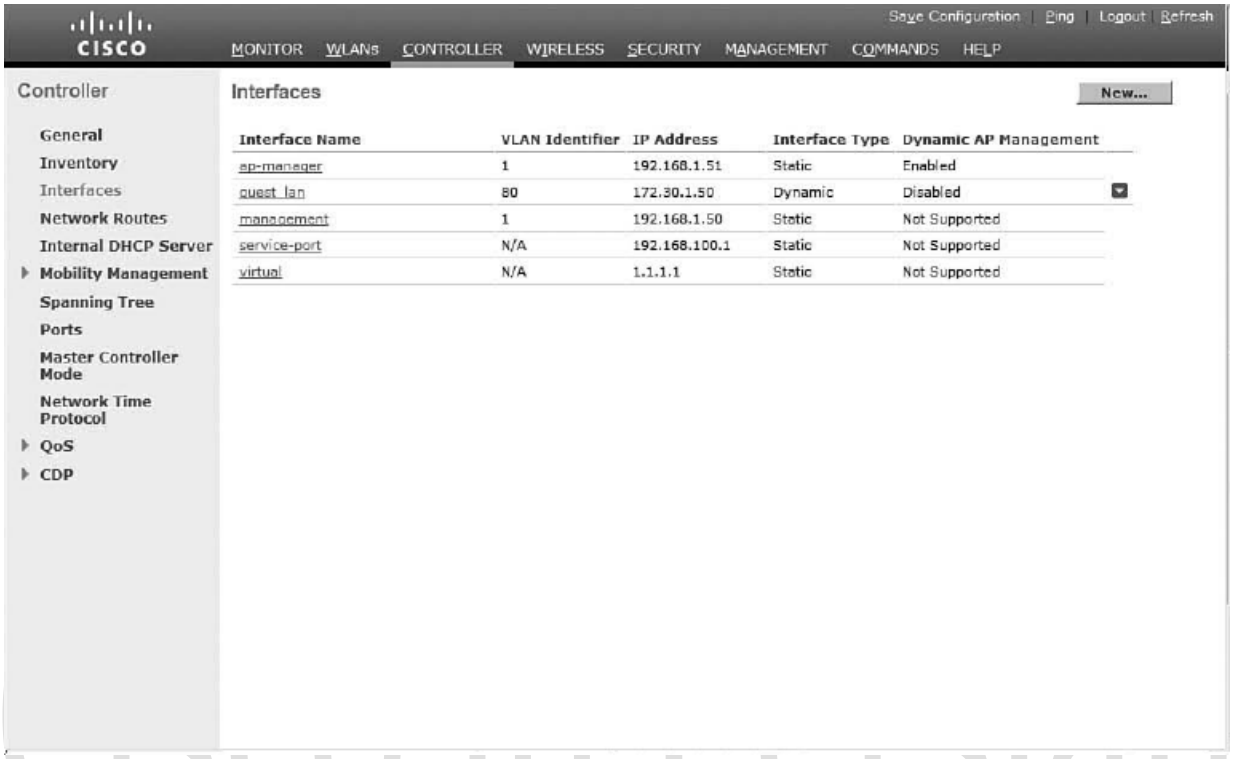
به زیر گروه Controller/Interfaces/New بروید و یک اینترفیس جدید بسازید :



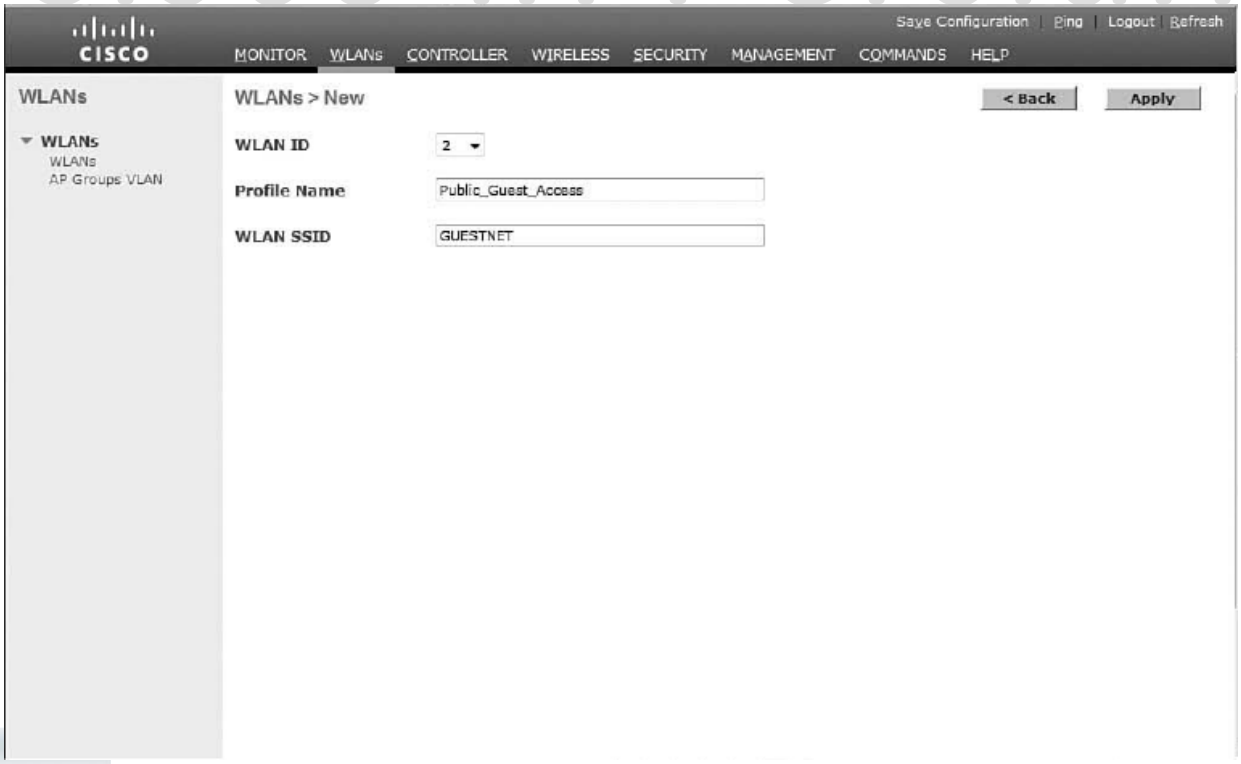
پس از Apply کردن ، می توانید سایر تنظیمات ، از جمله IP address را اعمال نمایید . همچنین می توانید DHCP Server را فعال نمایید .



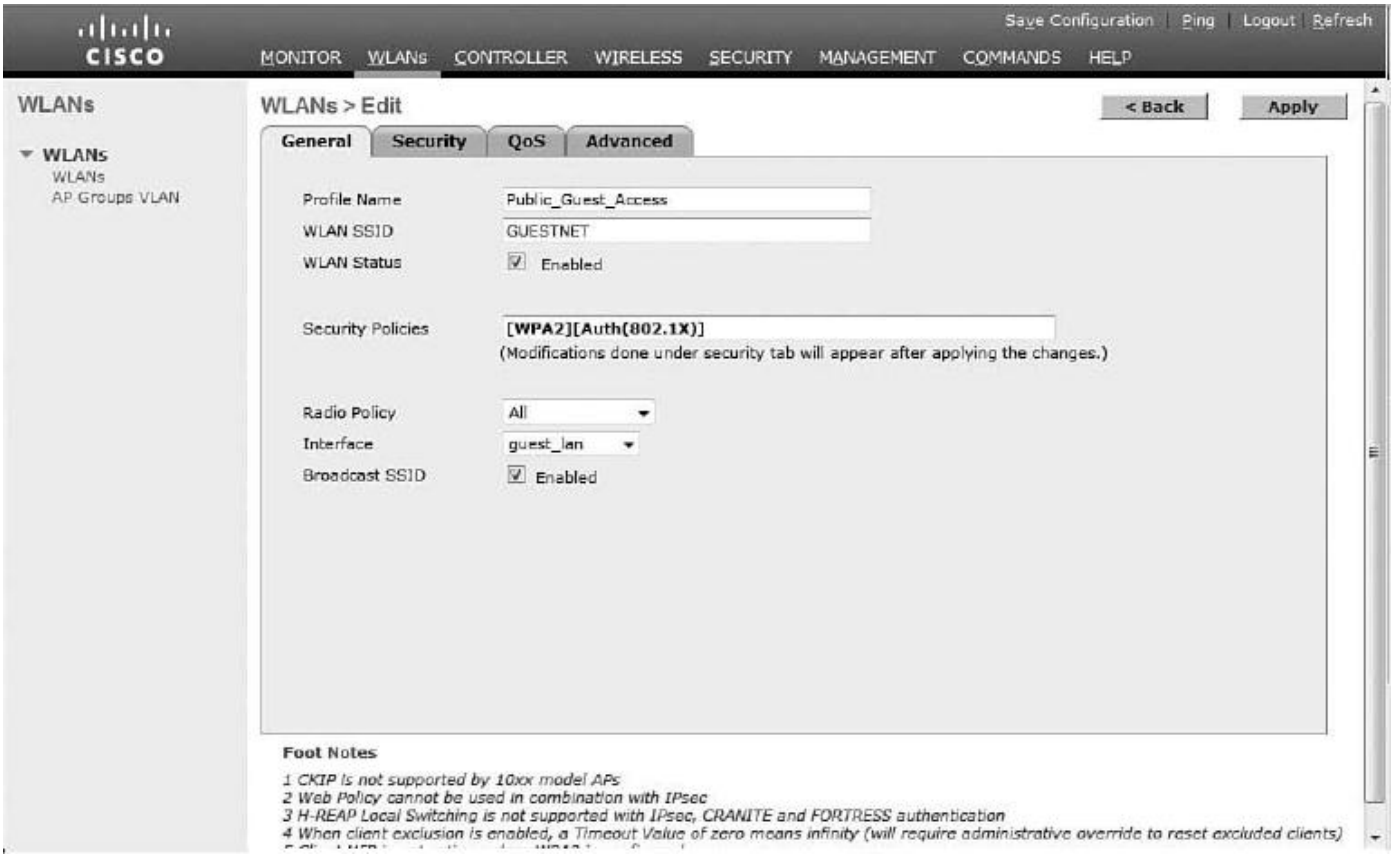
با Apply کردن ، پیامی دریافت می کنید که نشان می دهد WLAN ها بطور موقت غیر فعال شده اند . این اتفاق طبیعی است . با مشاهده ی لیست اینترفیس ها ، می توانید نتیجه ی تنظیمات خود را ببینید :



حال یک WLAN بسازید و آن را به یک اینترفیس اختصاص دهید : WLANs/New



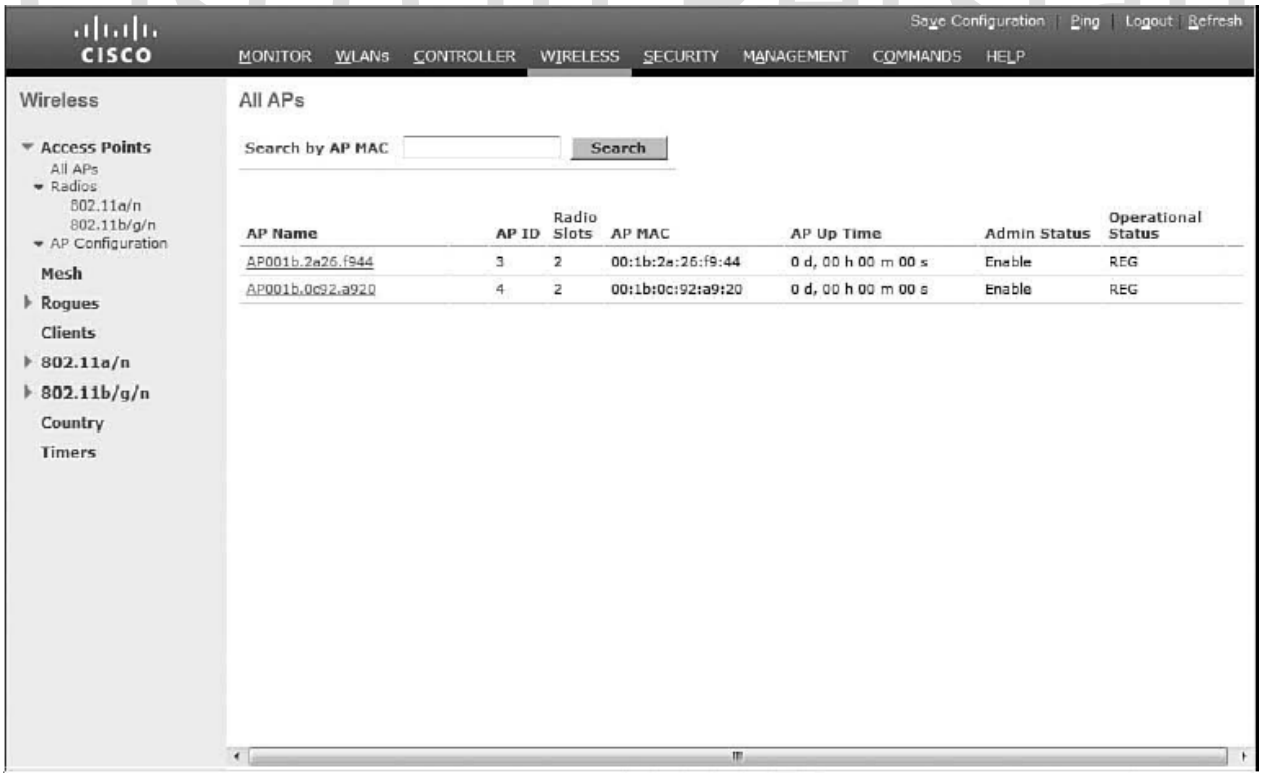
با Apply کردن ، می توانید سایر تنظیمات را اعمال کنید و مثلا برای Radio Policy ، گزینه ی all انتخاب شده باشد ، تمام radio ها برای شبکه ی GUESTNET فعال خواهد بود .



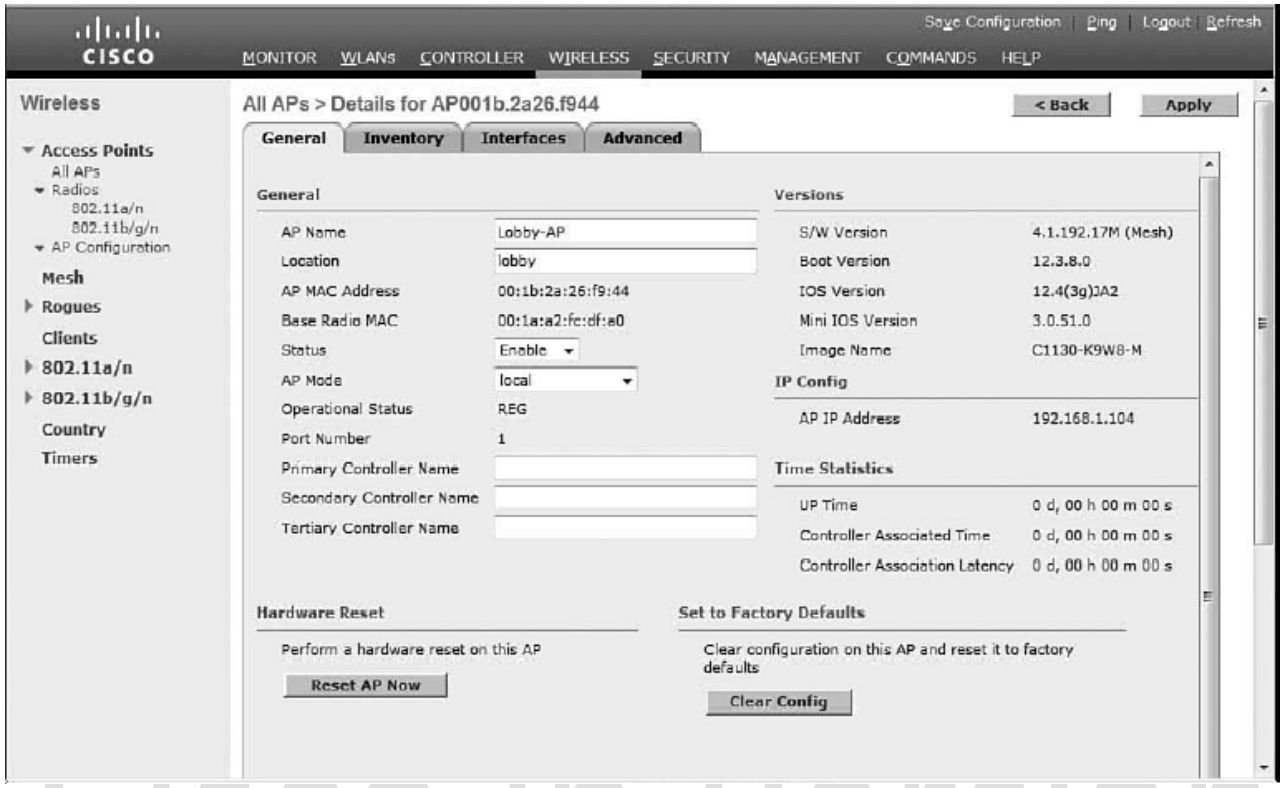
توجه داشته باشید که اینترفیس مناسب را برای هر WLAN انتخاب نمایید ، وگرنه افراد مختلف به شبکه های اشتباه متصل خواهند شد و دسترسی های غیر مجاز شکل خواهد گرفت .

در نهایت با Apply کردن به سربرگ WLAN باز خواهید گشت و نتیجه ی تنظیمات را مشاهده خواهید نمود :

در مرحله ی بعد ، چنانچه مایلید AP ها را نام گذاری نمایید ، Wireless/Access Points/ All Aps

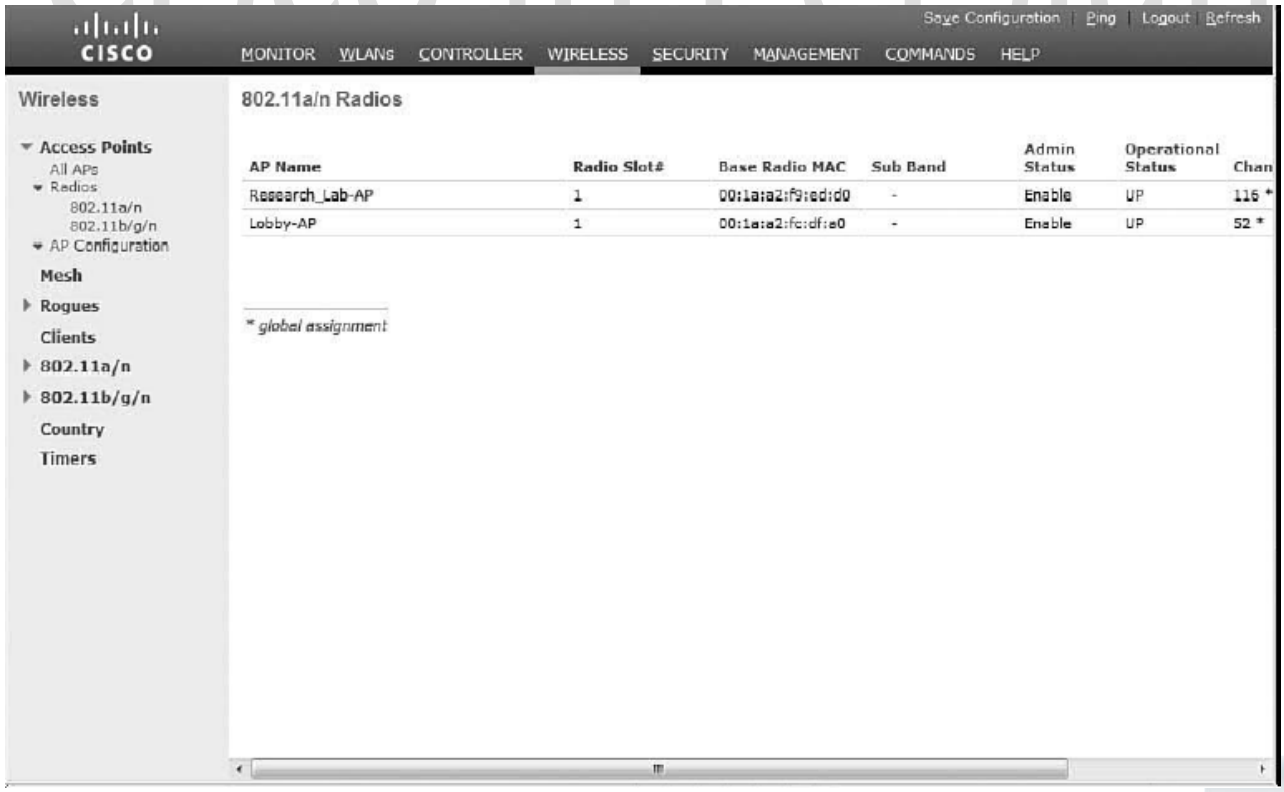


از بین این لیست ، AP مورد نظر را انتخاب نموده و نام آنرا تغییر دهید .

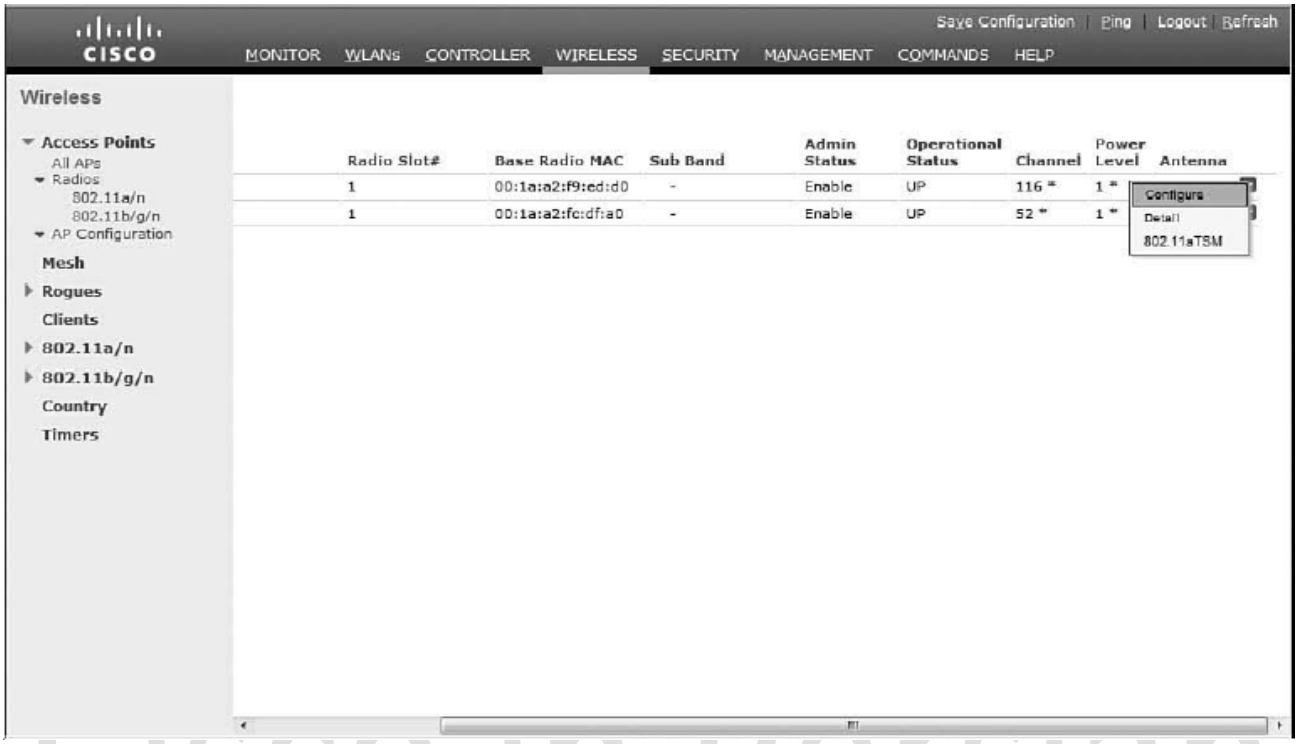


برای محدود کردن دسترسی به AP ، به سربرگ زیر بروید :

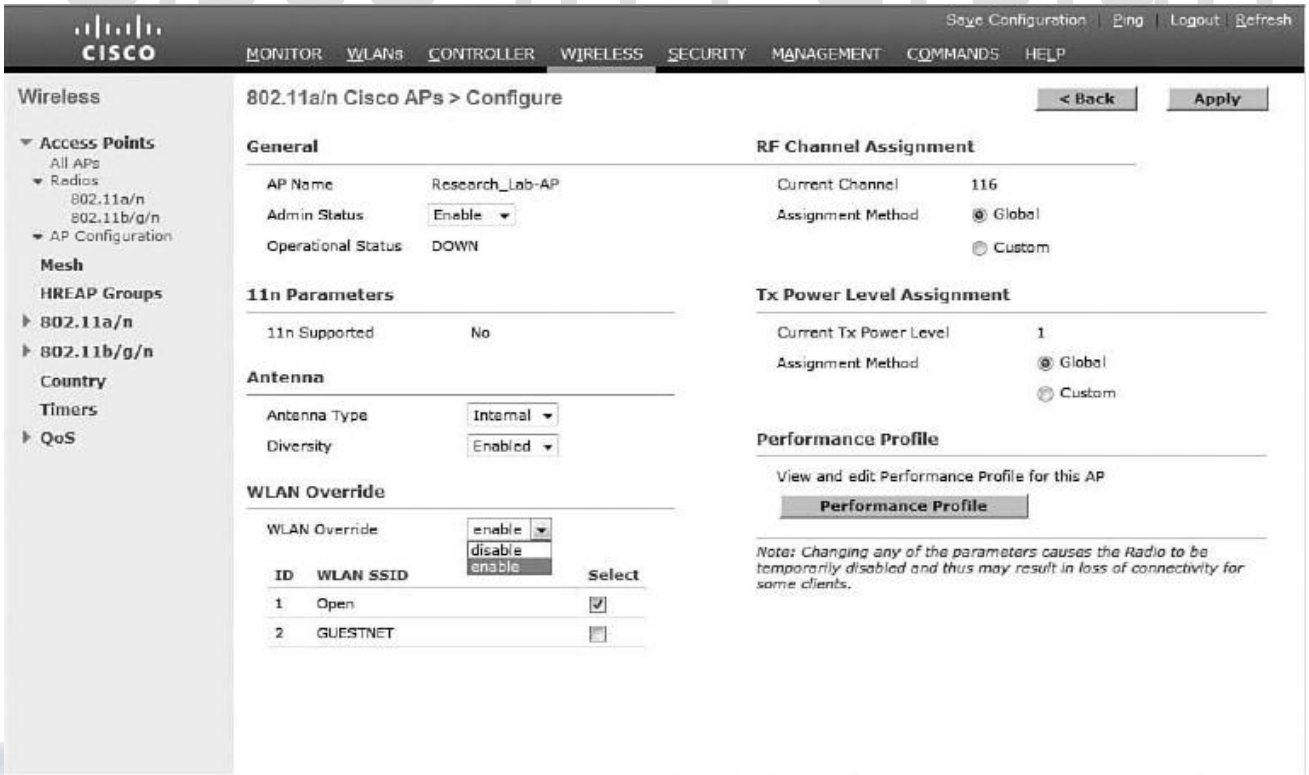
Wireless / Access Points / Radios / 802.11a/n



با کلیک بر روی فلش سمت راست AP مورد نظر ، منوی زیر را می بینید :

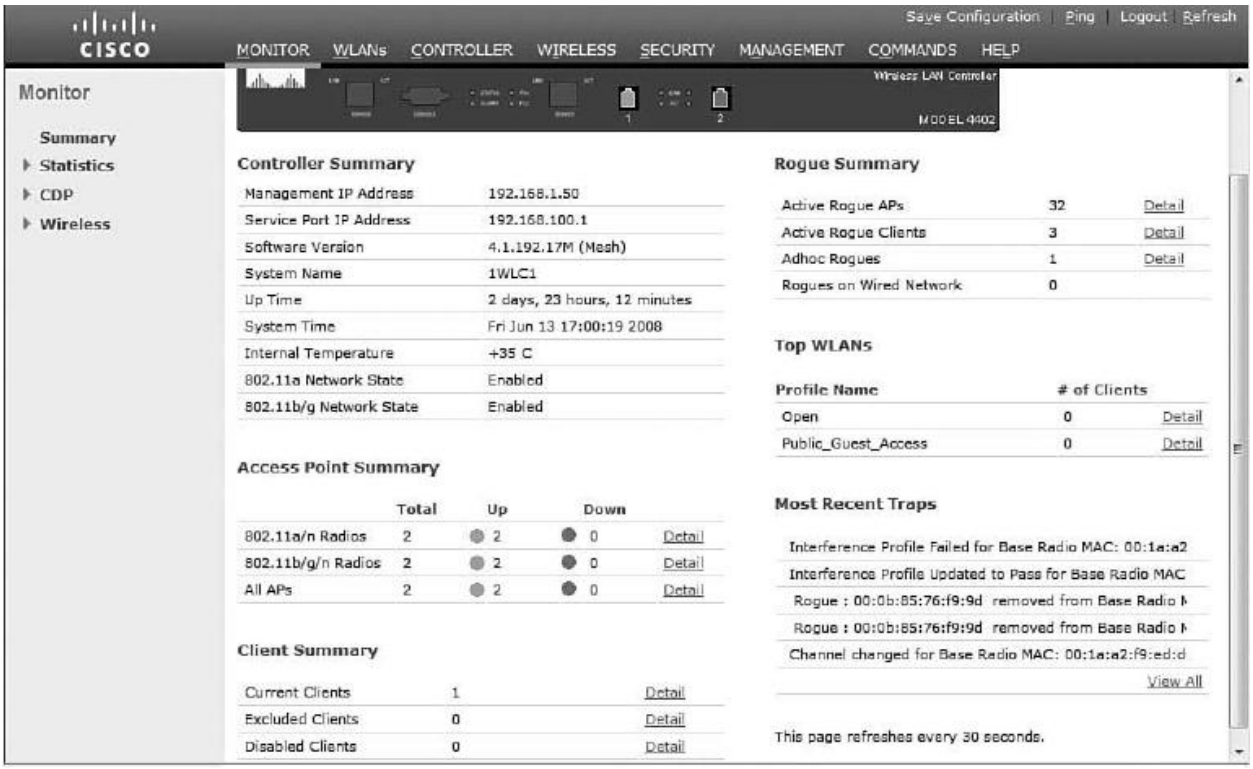


گزینه ی configure را انتخاب نمایید . سپس در بخش WLAN Override ، گزینه ی enable را انتخاب کنید . با این کار ، از لیست wlan ها ، wlan هایی که باید با این AP ارتباط داشته باشند را مشخص می نماییم .



Monitoring با استفاده از کنترلر:

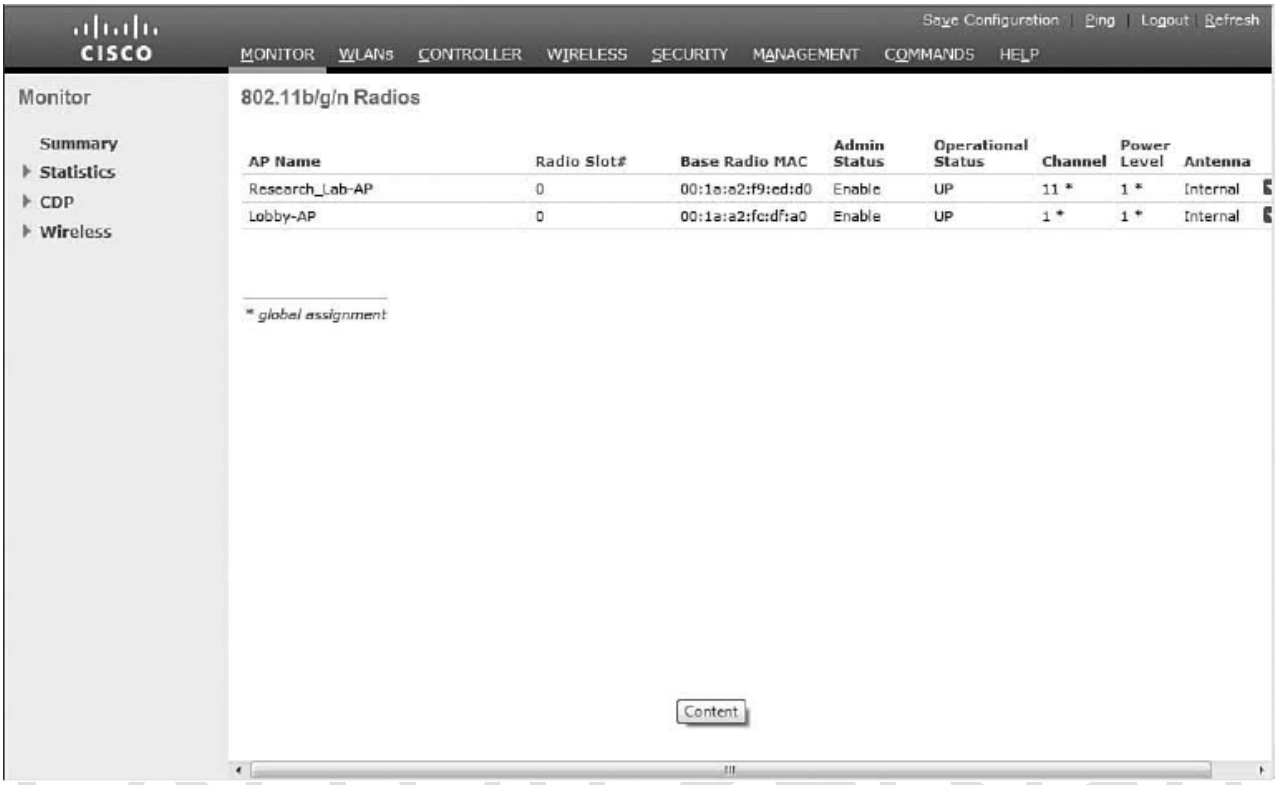
هنگامیکه به کنترلر log in می کنید ، اولین چیزی که مشاهده می کنید ، صفحه ی خلاصه وضعیت کنترلر است .



همانطور که می بینید این صفحه شامل بخش های مختلف است .

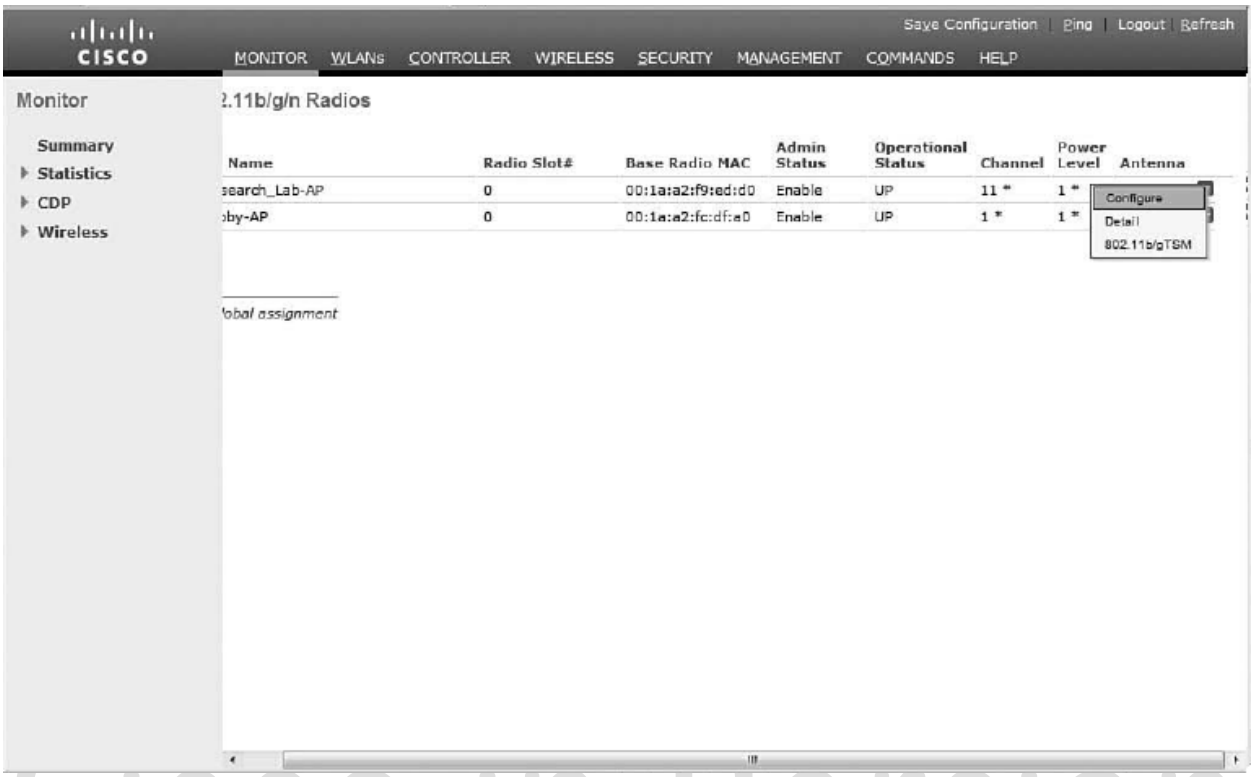
مثلا در بخش client summary ، هر کاربری که یک probe ارسال کرده باشد (حتی اگر هنوز associate هم نشده باشد)، جزو current client قرار می گیرد . لذا این عدد همیشه کمی اغراق شده است و شاید تعداد واقعی کاربران کنونی را نشان ندهد . اما اگر در سمت چپ ، روی wireless و سپس client کلیک کنیم ، در قسمت status مشخص می شود که این client در حال حاضر در چه وضعیتی قرار دارد .

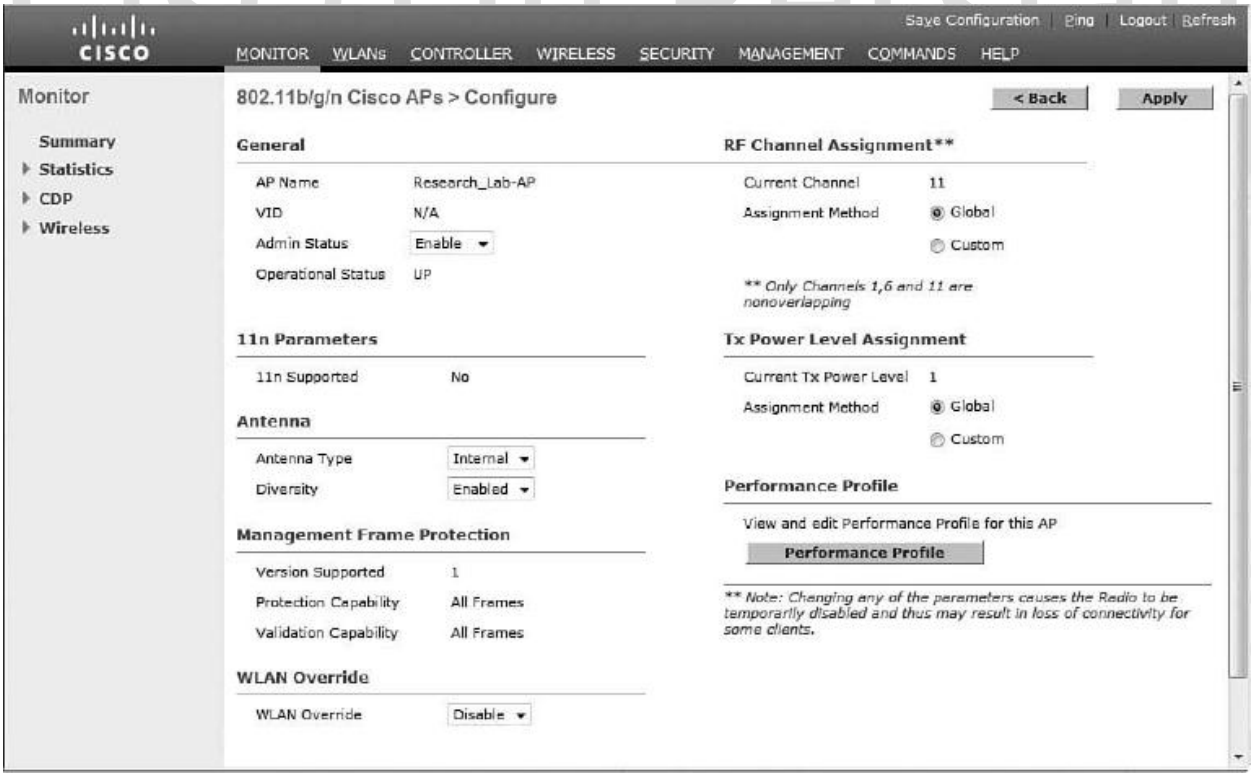
در بخش AP summary ، با کلیک روی detail هر رادیو ، AP هایی که در این وضعیت هستند را مشاهده می کنید :



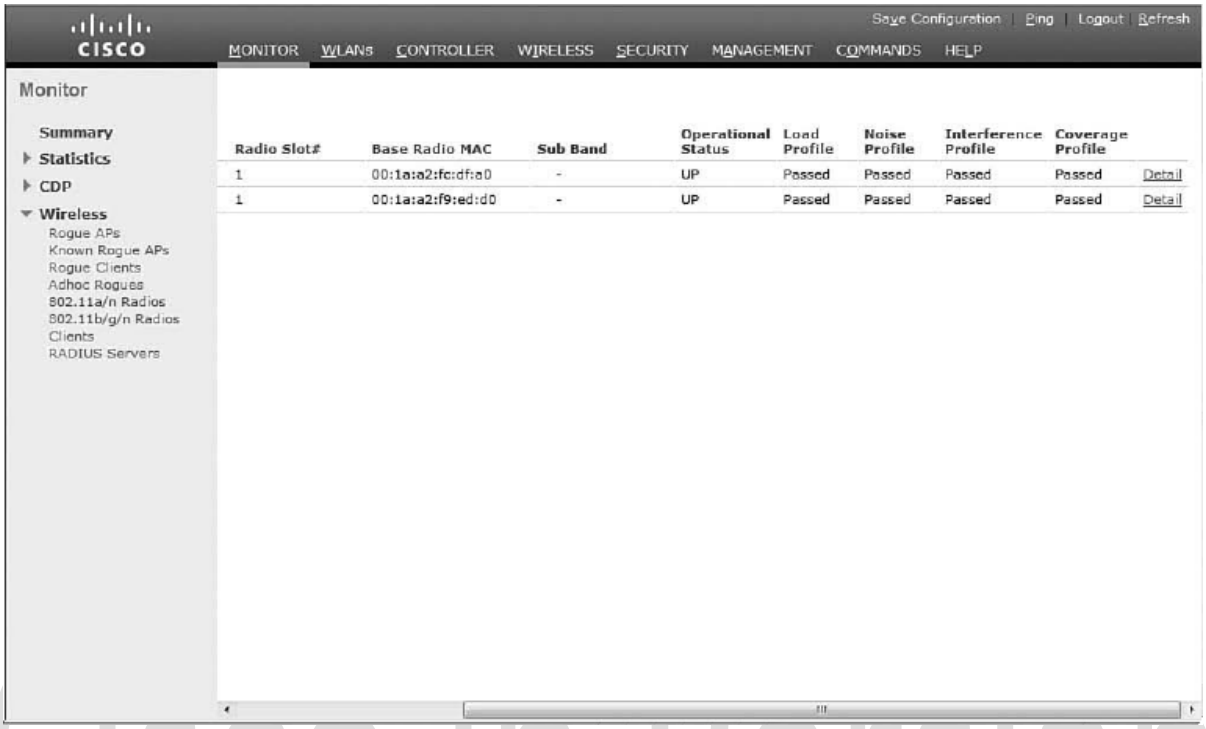
اگر مقدار power level برابر با 1 باشد ، به معنای بالاترین مقدار توان در کشور مورد نظر است . هرچه این عدد را بزرگتر کنیم ، مقدار توان کمتر می شود . مثلا اگر از ۱ به ۲ تغییر دهیم ، توان به اندازه ی ۵۰ درصد کاهش می یابد و اگر از ۲ به ۳ تغییر دهیم ، باز هم ۵۰ درصد از توان کم می شود (یعنی در کل ۲۵ درصد کاهش داریم).

برای تغییر تنظیمات هر AP به این شکل عمل کنید :

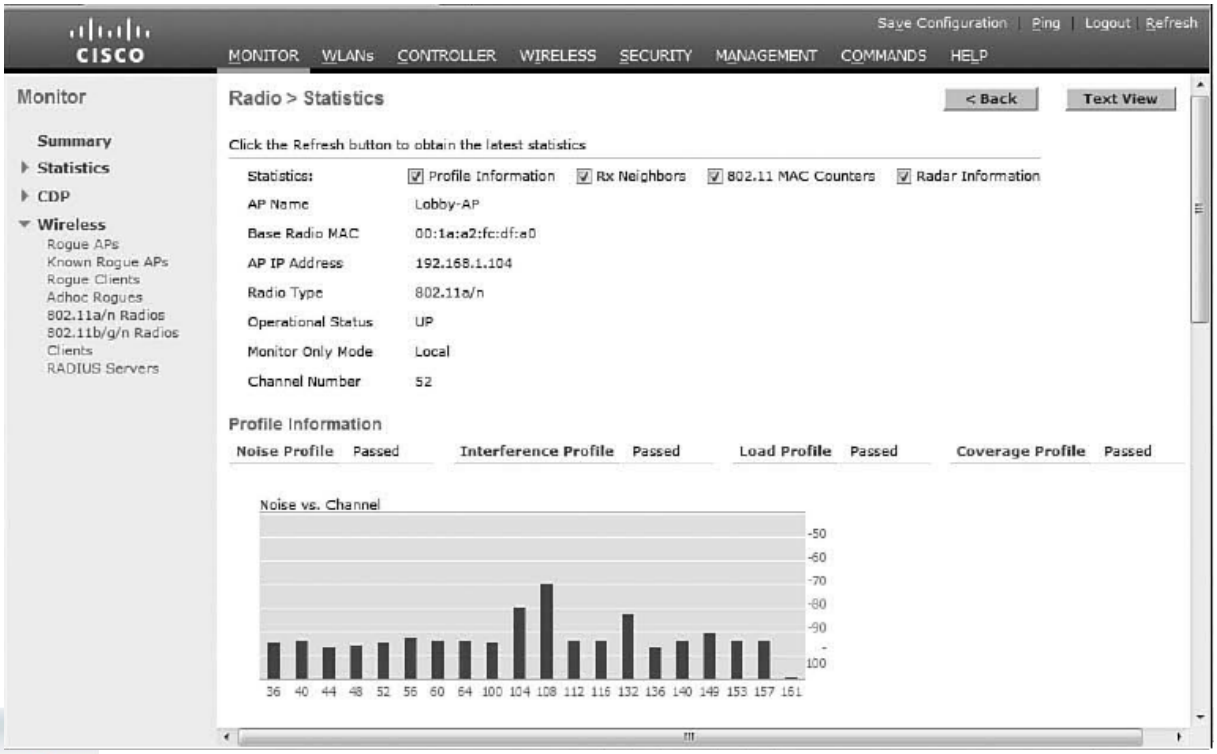




مقدار Load Profile بصورت پیشفرض بر روی ۸۰ درصد تنظیم شده است :

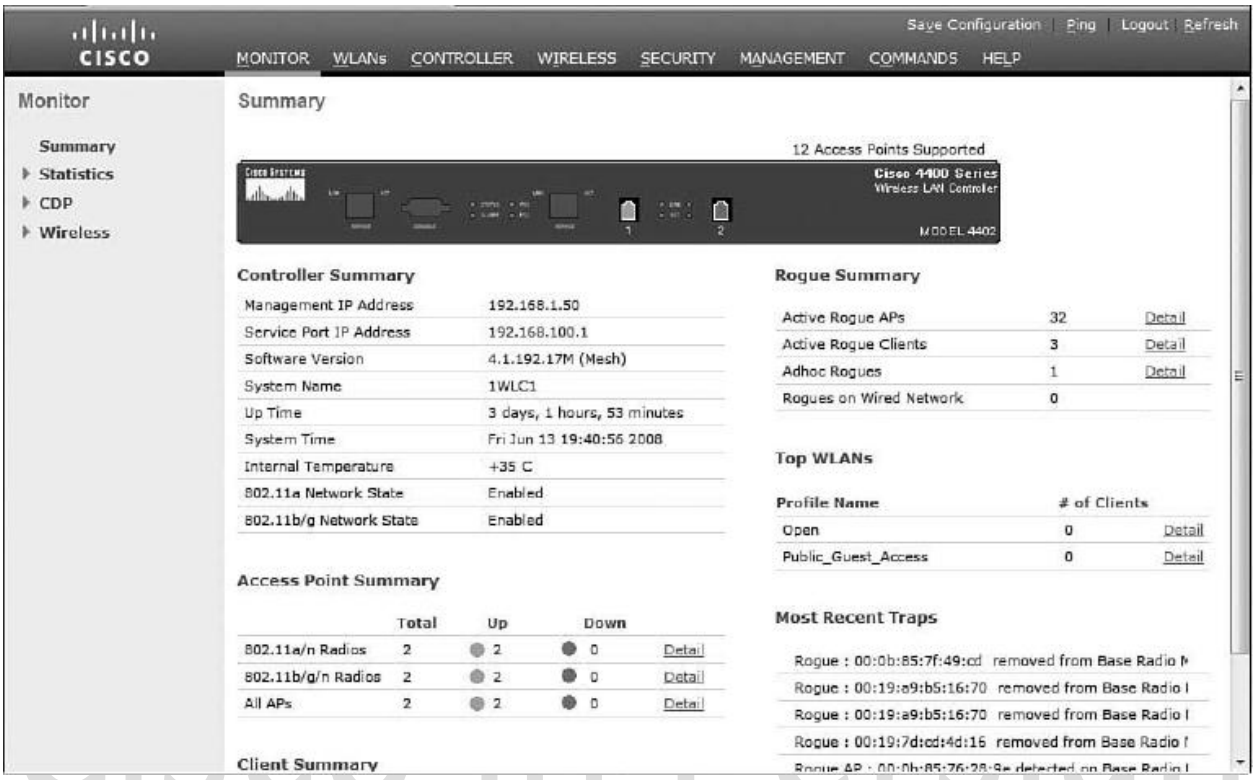


اگر Load روی این AP از این مقدار مرزی بیشتر شود ، یا SNR خیلی کم شود ، یا اگر تداخل زیادی روی کانالی که این AP در آن کار می کند وجود داشته باشد ، یا اگر کاربر ها roam کنند اما AP دیگری پیدا نکنند ، این پروفایل انواع warning ها را نمایش می دهد .

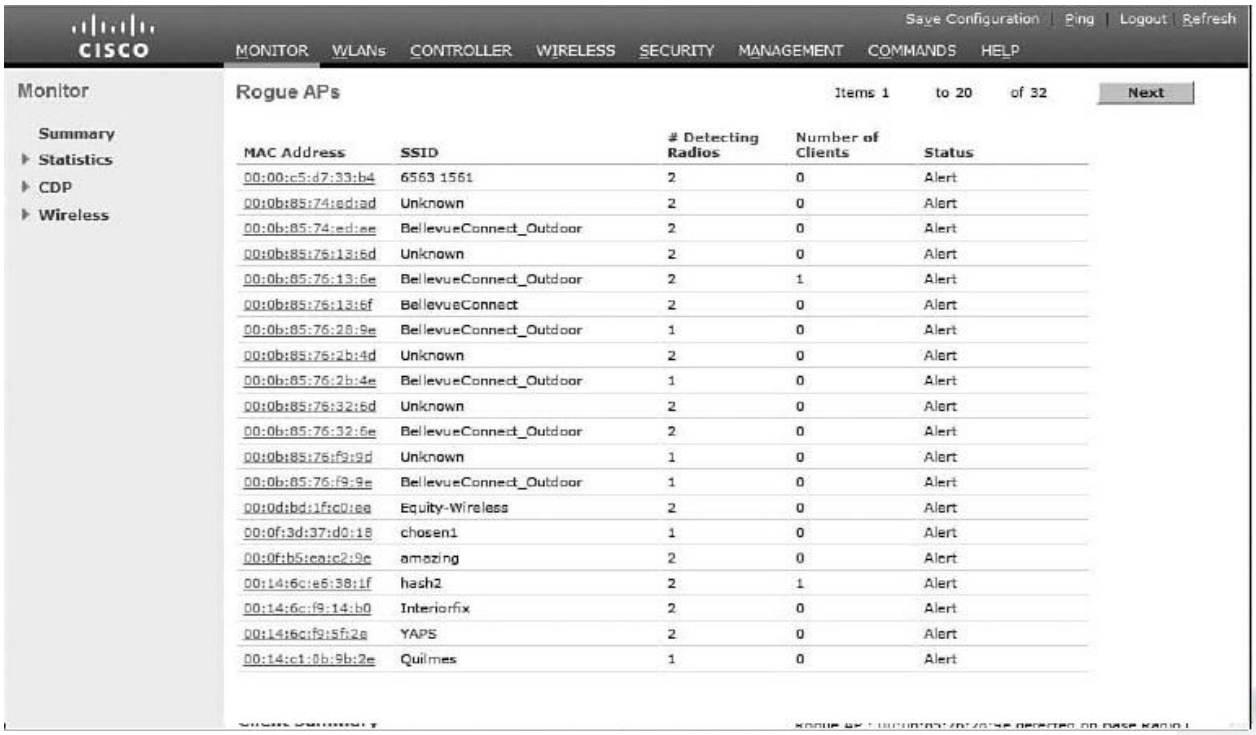


مدیریت Rogue AP ها :

Rogue AP الزاما یک AP خرابکار نیست ؛ بلکه هر AP است که برای کنترلر ناشناخته است .

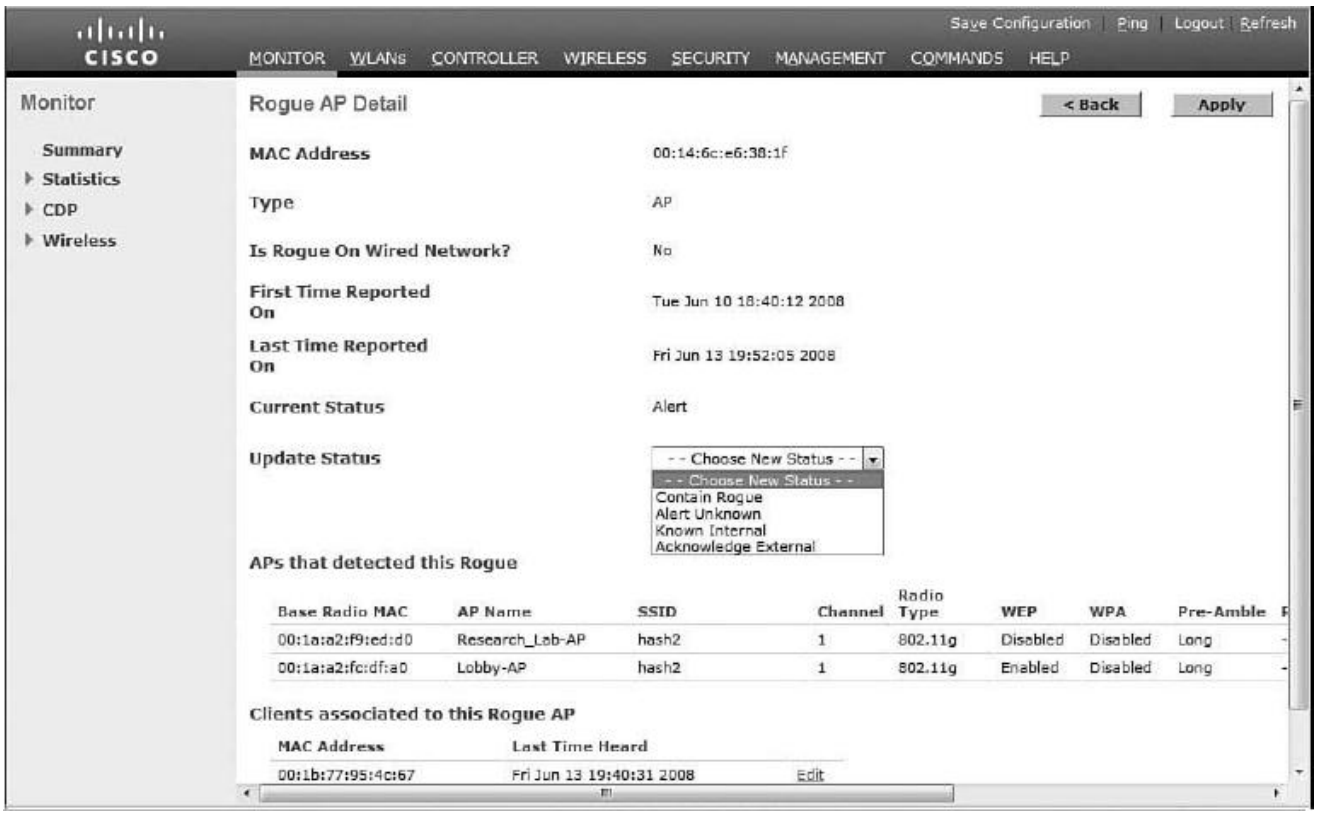


شما می توانید از طریق اینترفیس کنترلر ، rogue AP ها را مدیریت نمایید . با کلیک کردن روی detail :



نکته ی مهم در مورد تعداد رادیو ها (# detecting radios) اینست که هرچه این عدد کمتر باشد ، بهتر است . به عبارت دیگر ، هرچه یک rogue AP را رادیو های کمتری ببینند ، بهتر است ؛ زیرا به این معناست که این AP در گوشه ی شبکه قرار دارد (شاید AP همسایه ی ماست و تداخلی کوچک ایجاد کرده است) . اما اگر رادیو های زیادی آن را ببینند ، یعنی در قلب شبکه ی ما قرار گرفته است (احتمالا یک هکر است و قصد خرابکاری دارد).

با کلیک بر روی هرکدام از این MAC ها ، جزییات بیشتری مشاهده می شود :

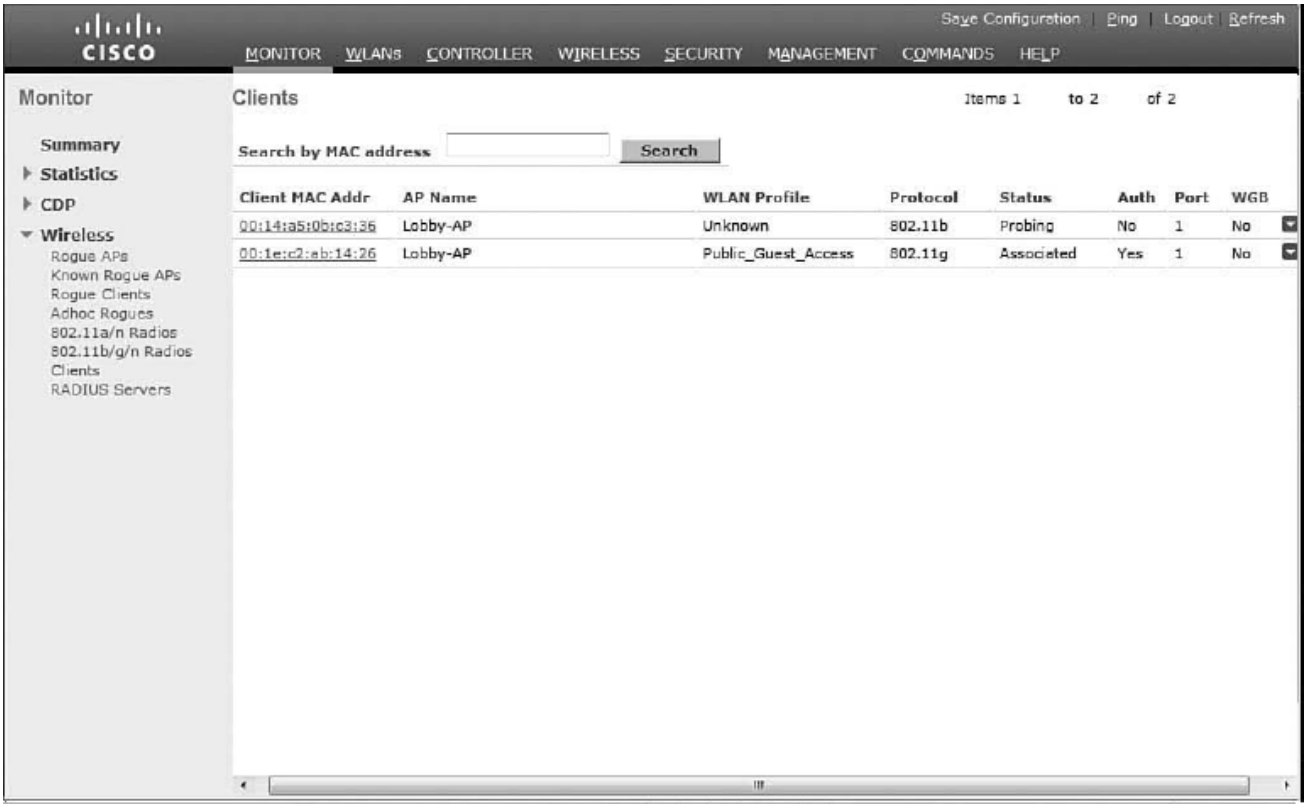


چنانچه در بخش update status ، گزینه ی contain را انتخاب کنیم ، AP رفتار جالبی نشان می دهد . در واقع AP آدرس MAC این rogue را روی فریم خودش می گذارد و یک deauthentication به همه جا ارسال می نماید . لذا تمام کاربران شبکه که این فریم را دریافت می کنند ، فکر می کنند Rogue AP این پیام را فرستاده ، لذا association خود را با آن rogue به هم می زنند و دیگر ارتباطی با contained AP برقرار نخواهند کرد .

البته برای هر AP می توان حداکثر ۳ تا rogue را contain کرد ؛ زیرا به ازای هر contained AP حدود ۱۰ درصد CPU hit بوجود می آید و سیستم قابلیت تحمل حداکثر ۳۰درصد CPU hit را دارد .

مدیریت کاربران :

در بخش کاربران نیز می توان تنظیمات مختلفی اعمال نمود .



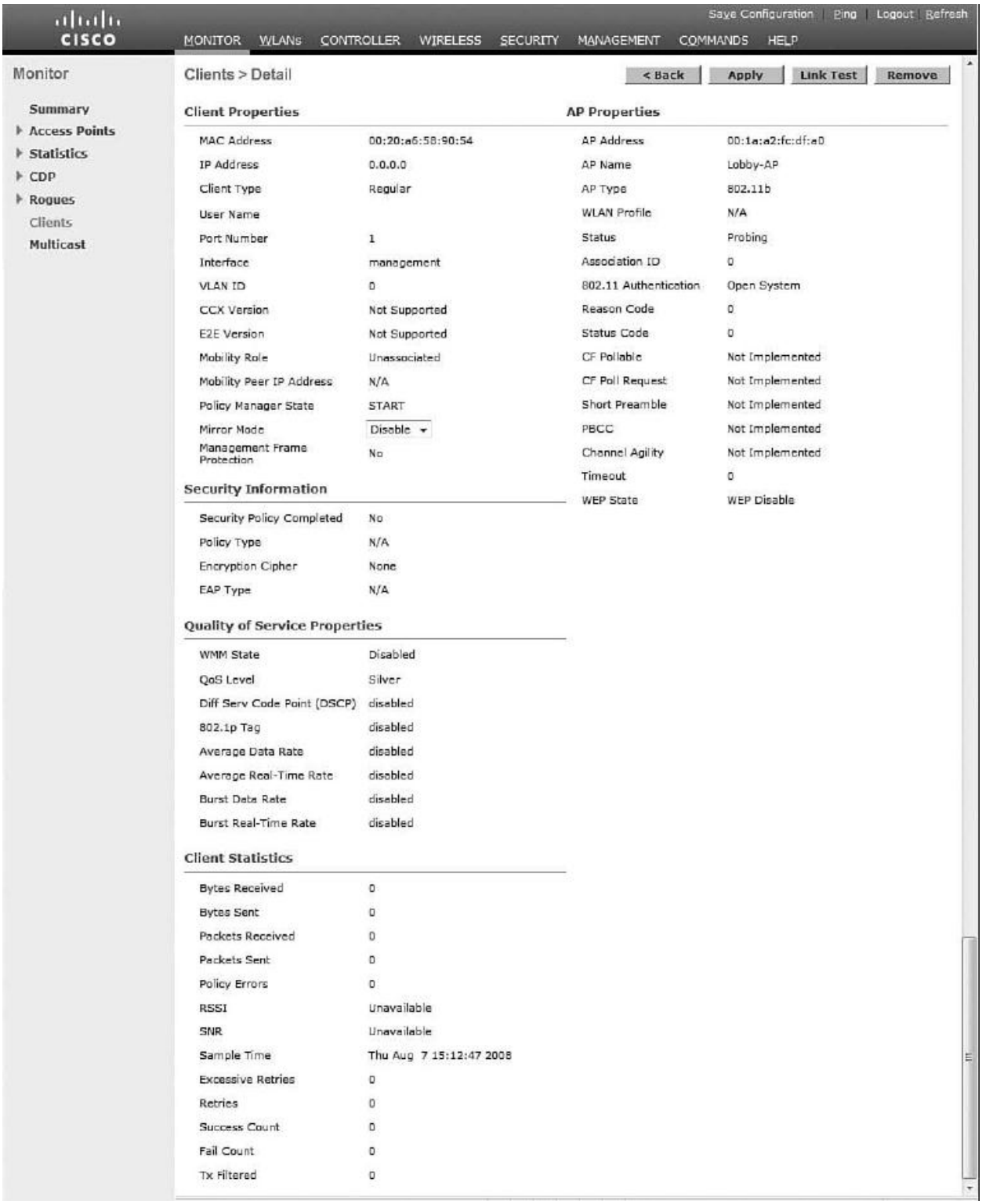
مثلا چنانچه مثل مراحل قبل ، روی فلش سمت راست کلیک کنیم ، چند گزینه مشاهده می شود :

Disable : یک کاربر را غیر فعال می کند ، تا زمانیکه دوباره آنرا enable کنیم .

Remove : یک کاربر را در حالت disassociate قرار می دهد ، اما می تواند خودش دوباره برای association تلاش نماید .

LinkTest : برای تست کردن یک لینک کاربر (بوسیله ی ارسال تعدادی پکت و محاسبه ی SNR ، طول سیگنال و ...) به کار می رود .

برای مشاهده ی جزییات بیشتر ، روی آدرس MAC کاربران کلیک نمایید :


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Monitor
Summary
Access Points
Statistics
CDP
Rogues
Clients
Multicast
Clients > Detail
< Back
Apply
Link Test
Remove
Client Properties
MAC Address 00:20:a6:58:90:54
IP Address 0.0.0.0
Client Type Regular
User Name
Port Number 1
Interface management
VLAN ID 0
CCX Version Not Supported
E2E Version Not Supported
Mobility Role Unassociated
Mobility Peer IP Address N/A
Policy Manager State START
Mirror Mode Disable
Management Frame Protection No
AP Properties
AP Address 00:1a:a2:fc:df:e0
AP Name Lobby-AP
AP Type 802.11b
WLAN Profile N/A
Status Probing
Association ID 0
802.11 Authentication Open System
Reason Code 0
Status Code 0
CF Pollable Not Implemented
CF Poll Request Not Implemented
Short Preamble Not Implemented
PBCC Not Implemented
Channel Agility Not Implemented
Timeout 0
WEP State WEP Disable
Security Information
Security Policy Completed No
Policy Type N/A
Encryption Cipher None
EAP Type N/A
Quality of Service Properties
WMM State Disabled
QoS Level Silver
Diff Serv Code Point (DSCP) disabled
802.1p Tag disabled
Average Data Rate disabled
Average Real-Time Rate disabled
Burst Data Rate disabled
Burst Real-Time Rate disabled
Client Statistics
Bytes Received 0
Bytes Sent 0
Packets Received 0
Packets Sent 0
Policy Errors 0
RSSI Unavailable
SNR Unavailable
Sample Time Thu Aug 7 15:12:47 2008
Excessive Retries 0
Retries 0
Success Count 0
Fail Count 0
Tx Filtered 0

فصل چهاردهم : تبدیل AP های Standalone به LWAPP

- AP modes
- تبدیل Lightweight به Standalone

اکثر AP های سیسکو قابلیت فعالیت در هر دو حالت Autonomous و Lightweight را دارند . در این فصل نحوه ی دسترسی به AP های Standalone را خواهیم آموخت ؛ همچنین به تنظیمات و چگونگی تبدیل این AP ها به حالت Lightweight خواهیم پرداخت .

AP modes :

هر AP که قابلیت فعالیت در هر دو حالت Autonomous و Lightweight را داشته باشد ، حالت Autonomous را انتخاب می کند و برای استفاده در حالت Lightweight ، باید خودمان دستگاه را به این حالت تغییر دهیم ؛ برای انجام این کار دو راه وجود دارد :

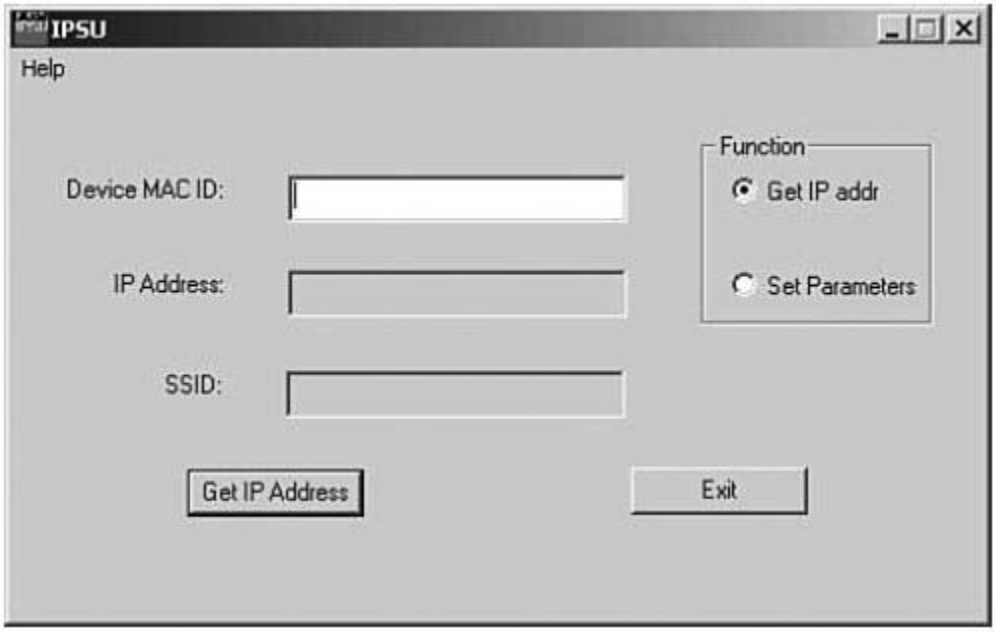
۱- استفاده از یک windows application به نام upgrade tool

۲- استفاده از WCS (Wireless Control System)

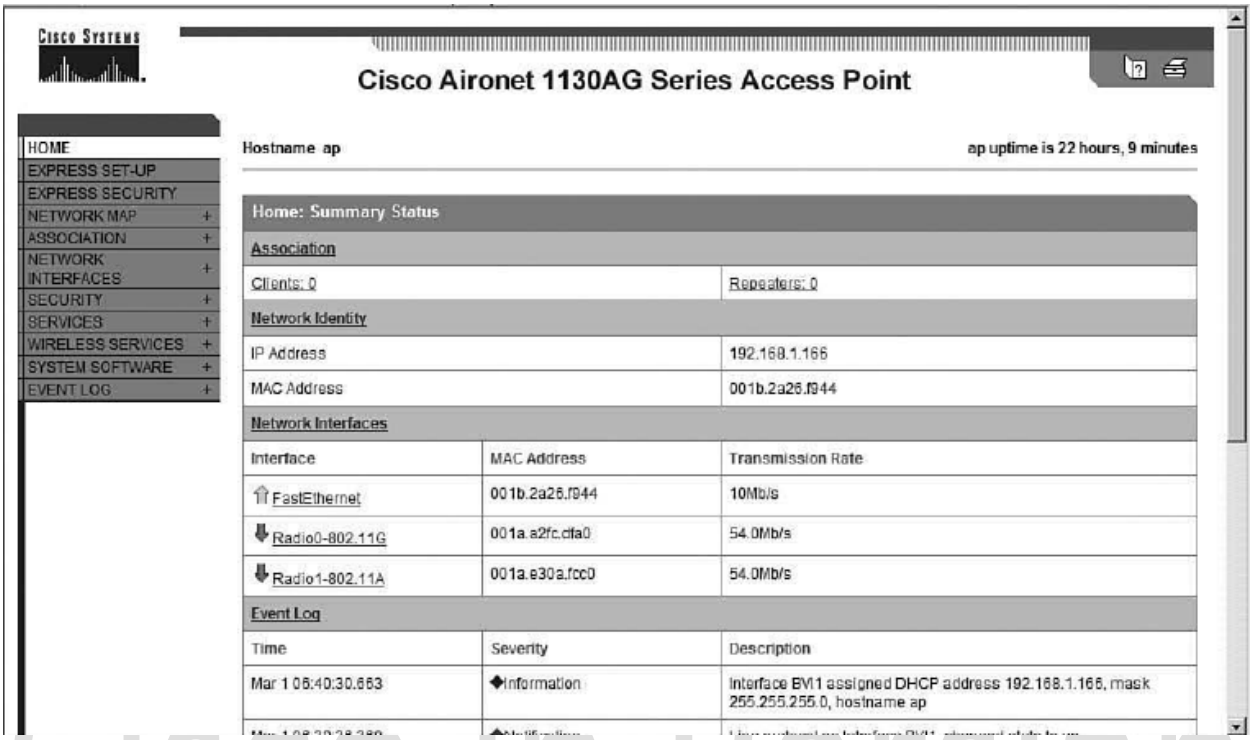
پس از اینکه AP در حالت Lightweight قرار گرفت ، دیگر می توان آن را از طریق WLC کنترل و مدیریت نمود .

هنگامیکه یک Autonomous AP را Plug in می کنیم ، آدرس IP خودش را از طریق DHCP به دست می آورد ، اما SSID ندارد و radio هم بصورت پیشفرض خاموش است (برای امنیت بیشتر).

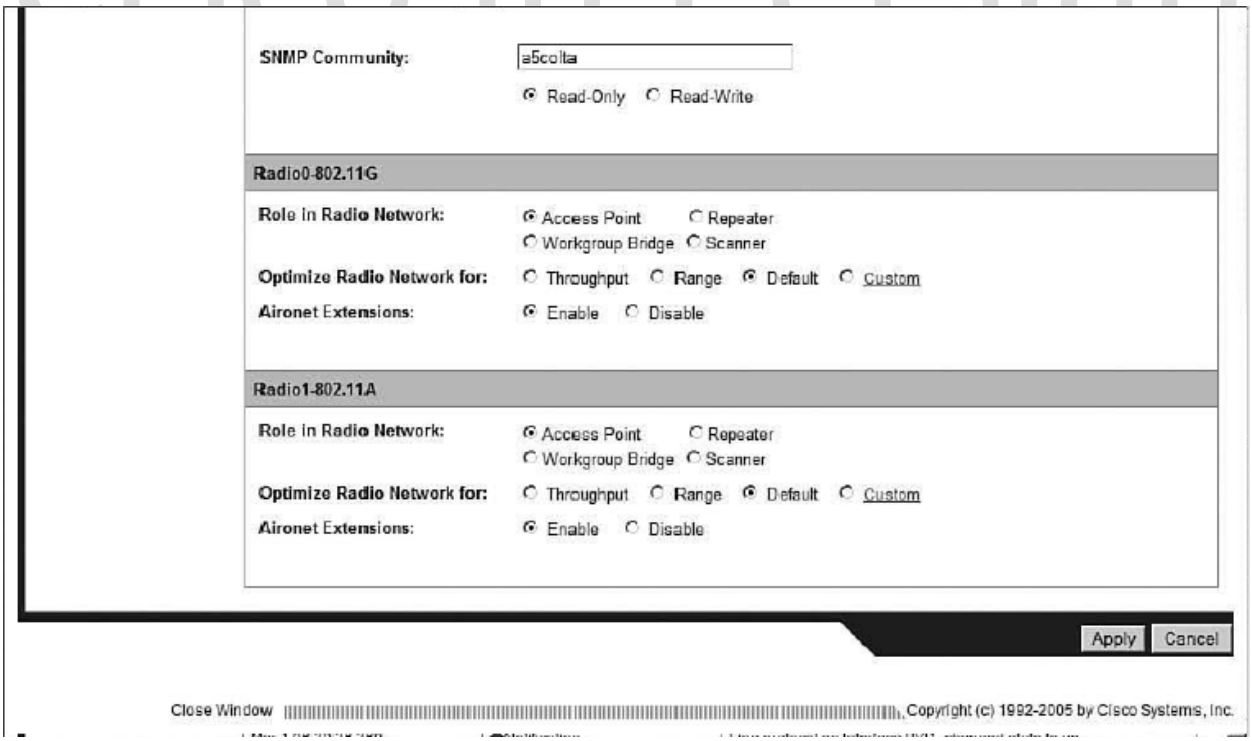
مشکل اساسی اینجاست که ما آدرس IP آن را نداریم تا به آن وصل شویم . این آدرس IP را می توان از چند طریق به دست آورد ؛ مثلا می توان روی سوییچی که به AP وصل است ، از CDP استفاده کرد ؛ یا اینکه می توان از دستور **show arp | include** *mac-address* استفاده نمود . همچنین می توان از IPSU استفاده کرد که نرم افزاریست که آدرس IP را از روس MAC به دست می آورد (MAC هر AP روی خود دستگاه ، یا روی جلد کارتون آن نوشته شده است).



پس از بدست آوردن IP و لاگین کردن به AP ، صفحه ی زیر را مشاهده خواهید نمود :

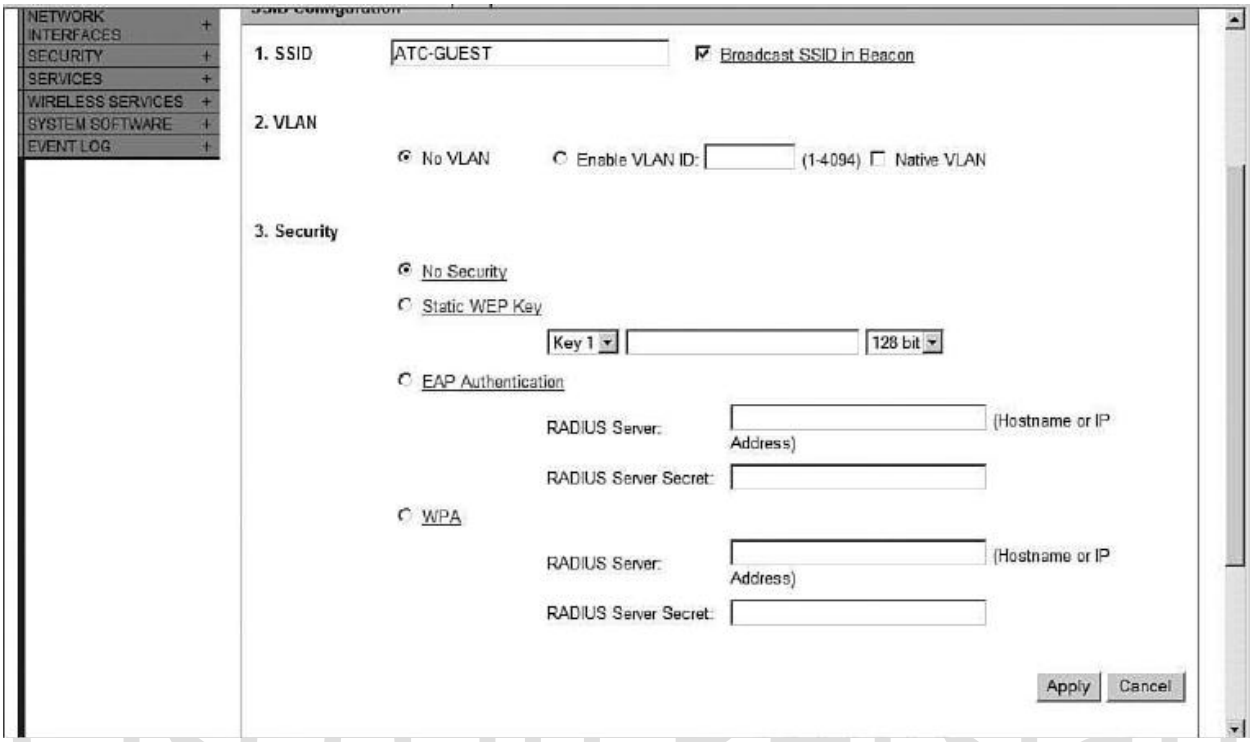


چنانچه می خواهید به سرعت AP را تنظیم کنید ، از بخش های Express Set-up و Express Security استفاده نمایید . مثلا در بخش Express Set-up ، در زیر بخش Radio Properties دارید :



توجه : در قسمت SNMP Community ، گزینه ی Read-Write یک حالت نا امن است .

همچنین در بخش Express Security ، می توانید تنظیمات امنیتی و نیز تنظیمات SSID را داشته باشید :



چنانچه VLAN ID ها را فعال کنید ، می توانید چندین SSID داشته باشید و تنظیمات امنیتی را برای هریک بطور جداگانه کانفیگ کنید . روی این AP می توان تا ۸ عدد SSID ساخت .

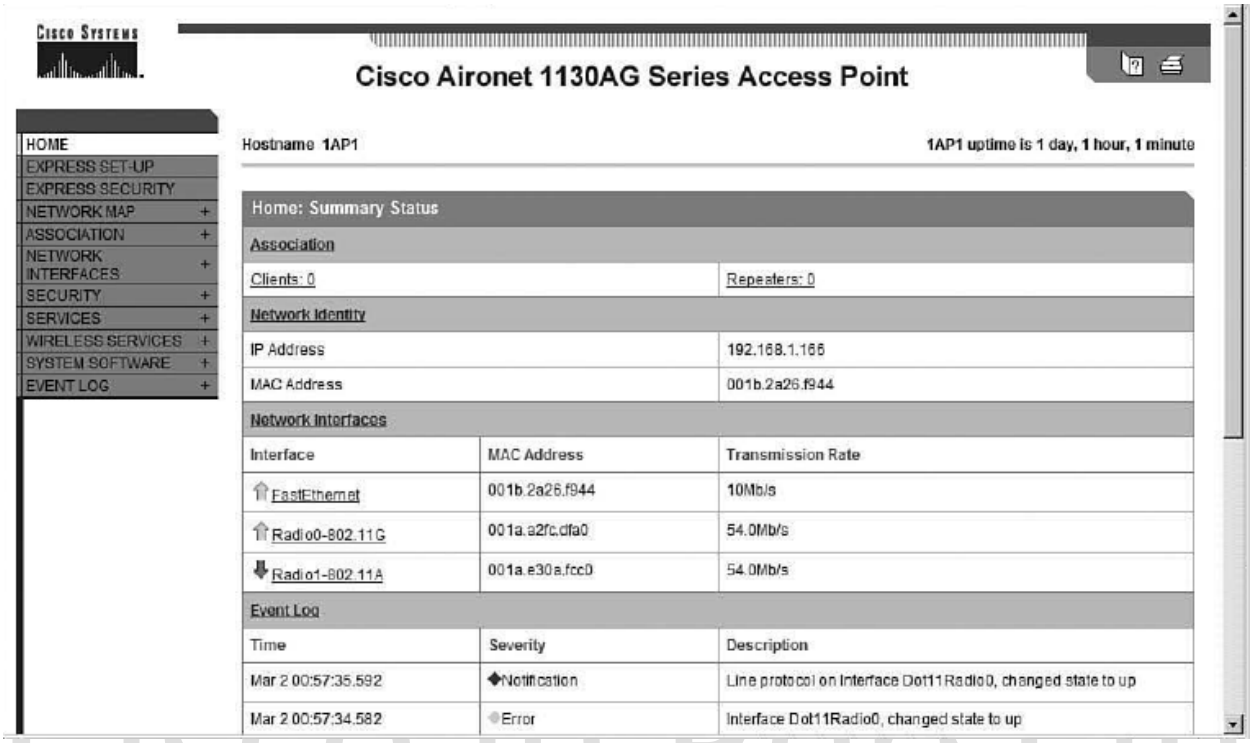
توجه : در این منو ،کلید Edit وجود ندارد ؛ به عبارتی اگر یک SSID ساختید ، برای تغییر مشخصات آن ، تنها می توانید آن را حذف کرده و دوباره یک SSID تعریف کنید .

توجه : نمی توان یک SSID را روی یک Radio Interface خاص تنظیم کرد . SSID تنظیم شده ، روی همه ی اینترفیس های AP اعمال می شود . البته با رفتن به باکس SECURITY ، می توان این کار را انجام داد ، اما در محیط Express این امر ممکن نیست .

توجه : نمی توان بیش از یک Authentication Server تنظیم نمود .

توجه : نمی توان انواع حالت های Authentication را با هم داشت .

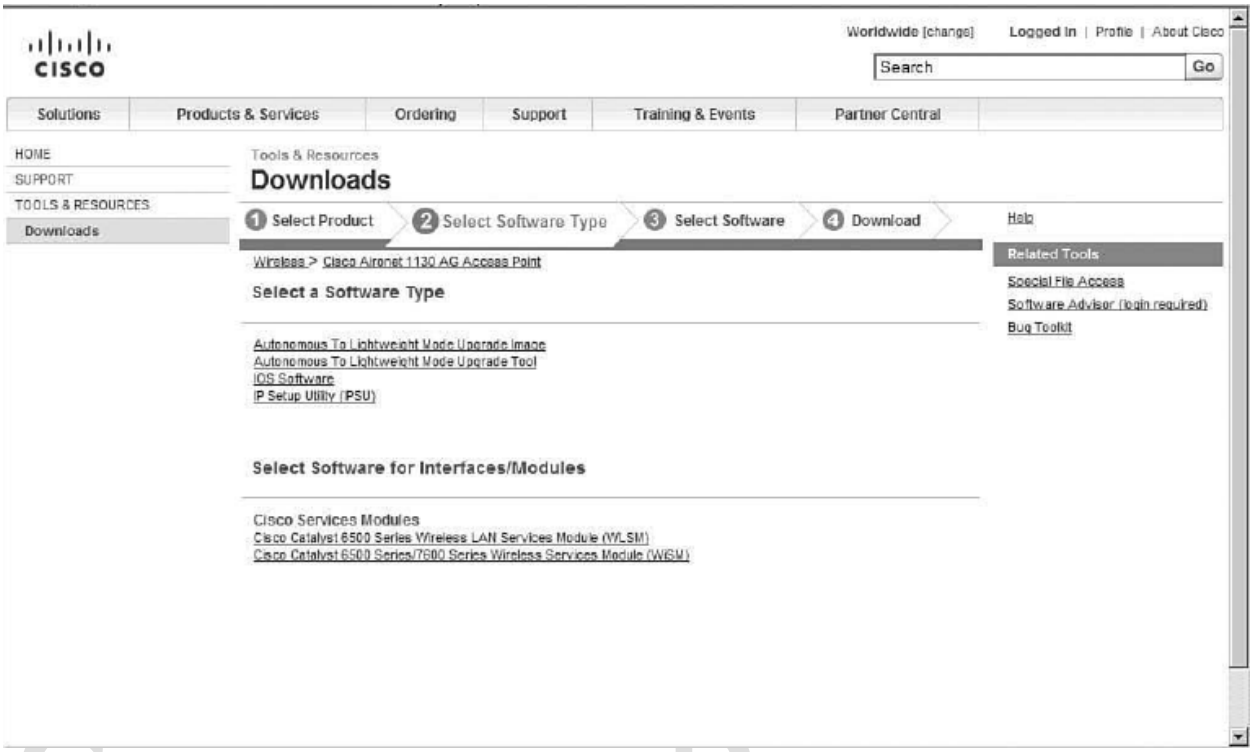
برای فعال کردن Radio ها می توان از بخش Network Interfaces استفاده کرد :



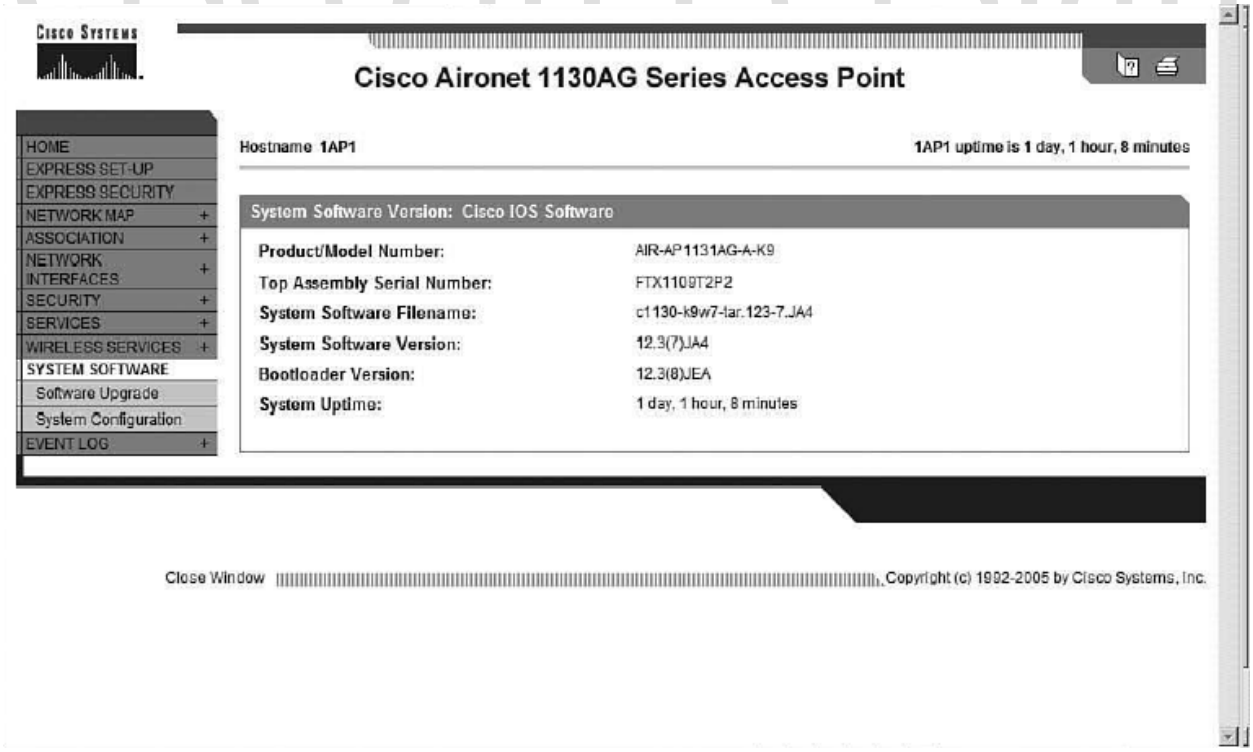
توجه : هدف اصلی ما اینست که AP بتواند با یک controller کار کند ، لذا باید Autonomous AP را به Lightweight AP تبدیل نمود .

برای این کار چندین راه وجود دارد .
یک روش ، استفاده از WCS است که در آن می توان یک AP را اضافه نموده و آن را به LWAPP ارتقا داد .

راه دیگر (همانطور که پیشتر نیز اشاره شد) ، استفاده از IOS to LWAPP Conversion Utility است که شامل یک نرم افزار Tool برای نصب روی کامپیوتر و یک image برای upgrade روی AP می باشد .
برای این کار می توانید به سایت www.cisco.com/go/wireless بروید .
سپس روی AP مورد نظر خود کلیک کیرده ، سپس در باکس Support ، لینک Download Software را انتخاب نمایید .
سپس AP مورد نظر را انتخاب نموده و پس از وارد کردن username و password سیسکو ، می بینید که صفحه ای نمایش داده می شود و نرم افزار های مورد نیاز را به شما پیشنهاد می کند :



توجه : ورژن IOS باید 12.3(7)JA یا بالاتر باشد .



توجه : در حالت Lightweight ، دیگر AP نمی تواند بدون کنترلر کار کند . همچنین پورت Console دیگر مورد استفاده قرار نمی گیرد .

توجه : upgrade ، فقط از حالت Layer3 LWAPP Mode پشتیبانی می کند .

توجه : AP های سری ۱۱۳۰ ، ۱۲۰۰ ، و ۱۳۰۰ می توانند از Standalone به LWAPP تبدیل شوند ؛ اما سری های ۱۴۰۰ یا ۱۵۰۰ چنین امکانی ندارند .

توجه : پس از اینکه از ورژن IOS مطمئن شدید ، باید مطمئن شوید که AP و کنترلر هر دو در یک subnet کار می کنند ، و اینکه آیا کنترلر توسط AP قابل دسترسی است یا خیر .
این کار را می توانید با استفاده از DHCP option-43 یا با استفاده از DNS انجام دهید .

تبدیل Lightweight به Standalone :

برای تبدیل Lightweight به Autonomous ، دو راه داریم :

۱- در محیط CLI ، از دستور زیر استفاده کنیم :

Config apt ftp-downgrade *tftp-server-ip-address filename apname*

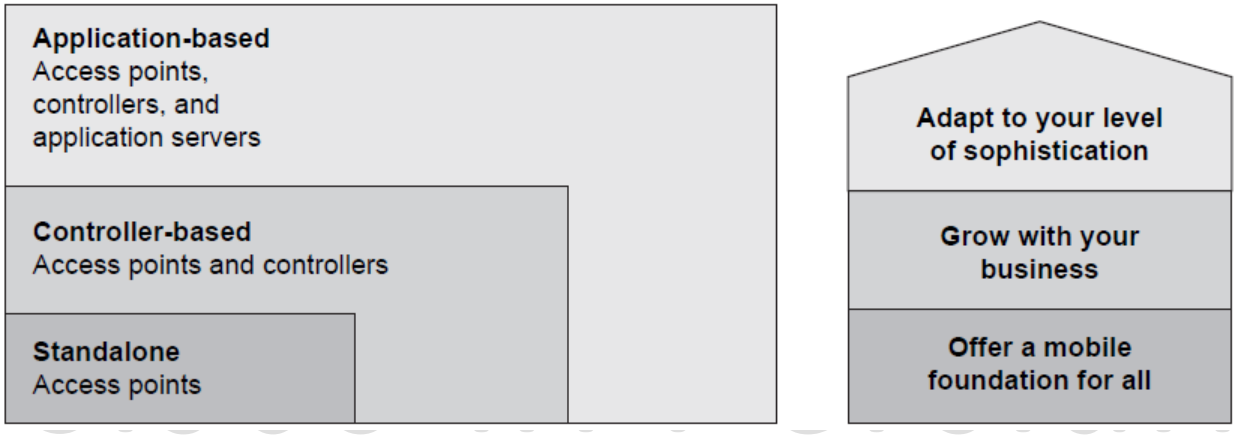
۲- تنظیمات AP را به Factoru Default باز گردانیم (با نگهداشتن کلید mode ، تا زمانیکه AP دوباره reboot گردد و LED آن به رنگ قرمز در آید . در این حالت AP در حالتی بالا می آید که Lightweight Code خود را در نظر نمی گیرد و آدرس 10.0.0.1 را به خود می گیرد).

فصل پانزدهم : آشنایی با Cisco Mobility Express

- ❖ سیستم ارتباطی Small Business
- ❖ Cisco 521 AP
- ❖ Cisco 526 Wireless Express
- ❖ تنظیمات 521 AP و 526 Controller
  - ✓ استفاده از CLI برای تنظیم کنترلر
  - ✓ استفاده از Web Interface برای تنظیم کنترلر
  - ✓ استفاده از Cisco Configuration Assistant

Cisco Mobility Express طراحی شده تا برای محیط های متوسط و کوچک ، سرویس وایرلس فراهم کند که تقریبا شبیه معماری Lightweight است (البته دقیقا LWAPP نیست ، اما زیرمجموعه ی عملکرد LWAPP می باشد ؛ به این معنا که هرچند AP مدل ۵۲۱ یه نوعی LWAPP را اجرا می کند ، اما نمی تواند با کنترلر های enterprise ارتباط برقرار کند) .
در این فصل با ابعاد مختلف این نوع طراحی آشنا می شویم ؛ همچنین تنظیمات AP مدل ۵۲۱ و نیز کنترلر مدل ۵۲۶ را خواهیم دید .

سیستم ارتباطی Small Business :



طراحی Cisco Mobility Express برای محیط های کوچکی مناسب است که نیاز به AP های مبتنی بر Controller دارند ، اما قصد ندارند تعداد AP هایشان را از ۱۲ عدد بیشتر کنند ؛ زیرا این معماری اجازه می دهد که ۲ کنترلر با هم ارتباط داشته باشند ، و هر کنترلر هم از ۶ عدد AP پشتیبانی می کند . لذا در کل می توان ۱۲ عدد AP را ساپورت کرد که برای small business خیلی خوب است .

در این طراحی همه دستگاهها بوسیله ی یک Application مرکزی به نام CCA مدیریت می شود .
(Cisco Configuration Assistant)

با وجود قابلیت های مختلفی که Cisco Mobility Express دارد (مانند CCA یا RRM) ، این طراحی ویژگی های self-configuring ، self-optimizing ، و self-healing (در زمان بروز تداخل) دارد .

Cisco 521 AP :

این AP نمی تواند با کنترلر های CUWN ارتباط برقرار کند ، زیرا یک سیستم سخت افزاری در حین پروسه ی bootup شدن AP ، به AP اجازه ی متصل شدن به هیچ کنترلی (به غیر از 526) را نمی دهد .

برخی ویژگی های این AP عبارتند از :

- ✓ 802.11g radio
- ✓ Variable transmit power settings
- ✓ Integrated antennas
- ✓ IEEE 802.11i0compliant ; WPA2 and WPA certified
- ✓ Multipurpose and lockable mounting bracket
- ✓ Power over Ethernet (IEEE 802.3af and cisco Inline Power)

Cisco 526 Wireless Express Controller :

یک کنترلر ۵۲۶ می تواند تا ۶ عدد cisco 521 AP را ساپورت کند ؛ همچنین در هر شبکه ۲ تا کنترلر می توانند با هم ارتباط برقرار کنند .

در مقام مقایسه ، طراحی Cisco Mobility Express شبیه به CUWN است ، با این تفاوت که CUWN ورژن enterprise و کامل LWAPP را اجرا می کند ، اما Cisco Mobility Express تنها بخشی از LWAPP را اعمال می کند .

برخی از ویژگی های کنترلر ۵۲۶ عبارتند از :

- ✓ Secure network access for guest users
- ✓ Support for cisco-over-WLAN optimization
- ✓ Easy management with CCA
- ✓ Support for cisco LWAPP
- ✓ Multiaccess point RRM
- ✓ Wired/wireless network virtualization

تنظیمات AP 521 و Controller 526 :

برای تنظیم Mobility Express سه راه داریم که هر سه روش باید روی کنترلر انجام شود و نمی توان AP را کانفیگ کرد .
ابتدا از طریق console به کنترلر وصل می شویم و تنظیمات اولیه را اجرا می کنیم . سپس با استفاده از آدرس IP کنترلر و از طریق آدWeb Interface ، وارد محیط تنظیمات کنترلر شده و configuration های تکمیلی را انجام می دهیم . در نهایت برای مدیریت کامل ، می توان از نرم افزار CCA استفاده نمود .

استفاده از CLI برای تنظیم کنترلر :

فرآیند بوت شدن کنترلر را در شکل زیر مشاهده می کنید .

```
Booting Primary Image...
Press <ESC> now for additional boot options...

Boot Options

Please choose an option from below:

1. Run primary image (Version 4.2.61.8) (active)
2. Run backup image (Version 4.1.154.22)
3. Manually upgrade primary image
4. Change active boot image
5. Clear Configuration

Please enter your choice:
```

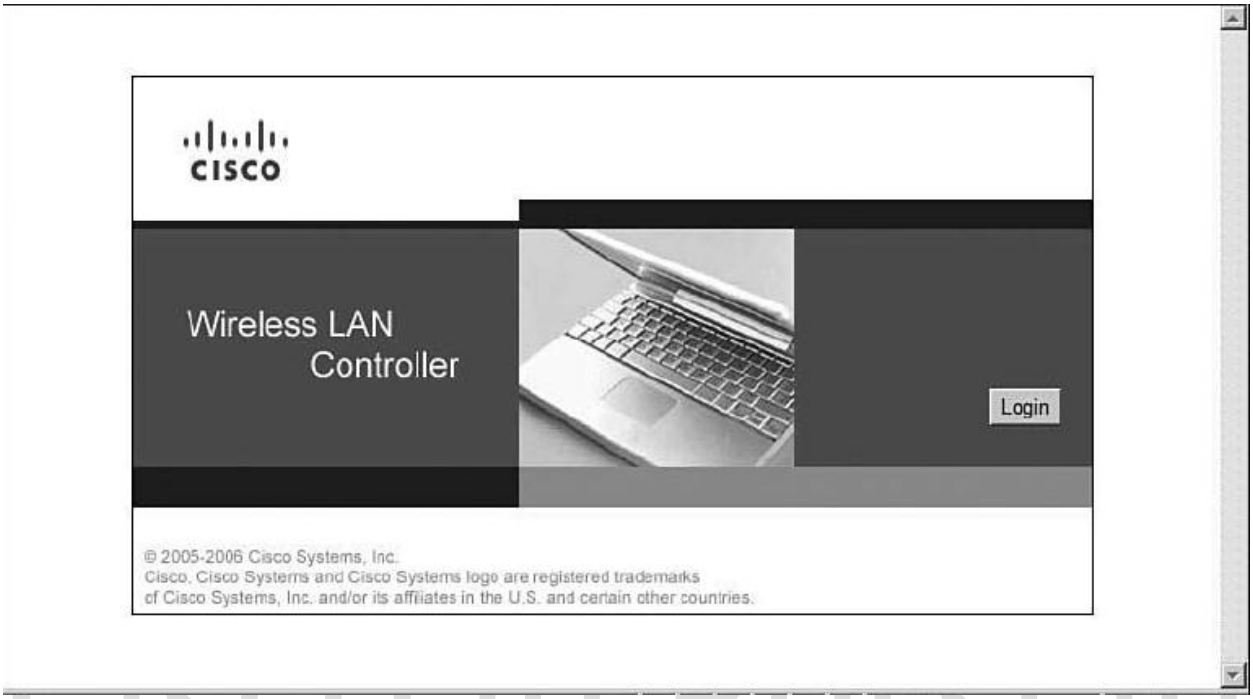
چنانچه بخواهید تنظیمات اولیه را انجام دهید ، پس از کامل شدن پروسه ی boot ، کنترلر بدون هیچ configuration اولیه ، یک setup wizard در اختیار شما قرار می دهد که می توانید موارد متعددی را تنظیم نمایید .

در شکل زیر می توانید این موارد را مشاهده فرمایید :

```
Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup
System Name [Cisco_be:7a:e0]: 526-3
Enter Administrative User Name (24 characters max): admin3
Enter Administrative Password (24 characters max): *****
Re-enter Administrative Password : *****

Management Interface IP Address: 10.30.1.100
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.30.1.254
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 2]: 1
Management Interface DHCP Server IP Address: 10.30.1.253

AP Manager Interface IP Address: 10.30.1.101

AP-Manager is on Management subnet, using same values
AP Manager Interface DHCP Server (10.30.1.253):

Virtual Gateway IP Address: 1.1.1.1

Mobility/RF Group Name: CP-POD3

Enable Symmetric Mobility Tunneling [yes][NO]: NO

Network Name (SSID): IUWNE-301
Allow Static IP Addresses [YES][no]: YES

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]: US

Enable 802.11b Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: no
Configure the system time now? [YES][no]: no

Warning! No AP will come up unless the time is set.
Please see documentation for more details.

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```

استفاده از Web Interface برای تنظیم کنترلر :

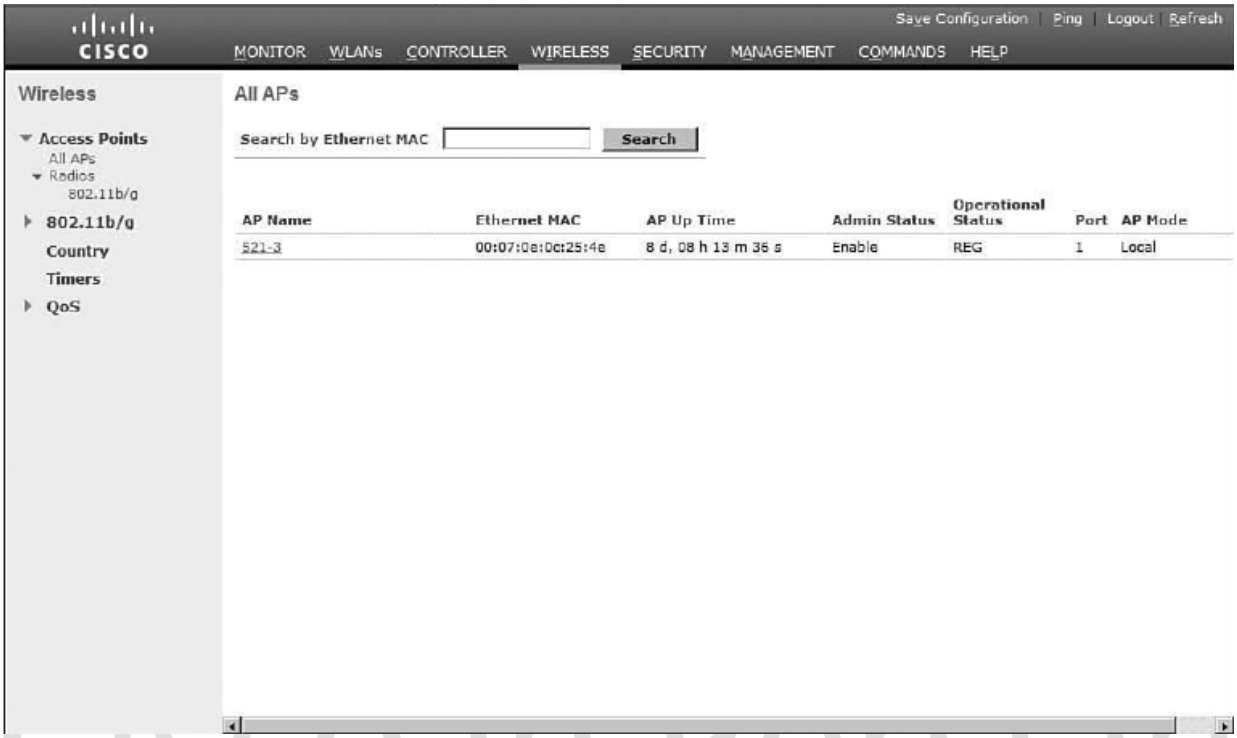
برای دسترسی به کنترلر از طریق web interface ، باید آدرس IP اینترفیس مدیریتی کنترلر را وارد نمایید .



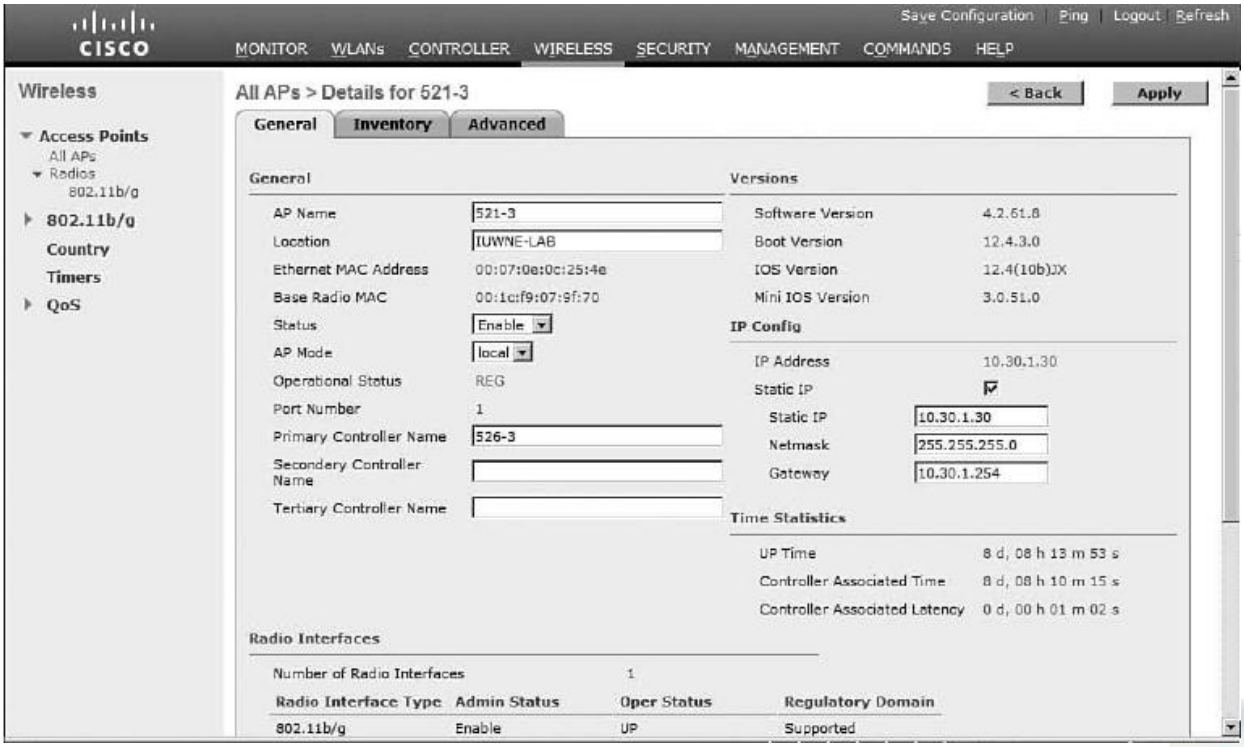
توجه : این ارتباط کاملا امن است (از طریق HTTPS).

پس از login کردن ، صفحه ی خلاصه وضعیت کنترلر را مشاهده خواهید نمود .

AP و کنترلر یکدیگر را پیدا خواهند نمود . از منوی WIRELSS می توانید ببینید که AP پیدا شده است .

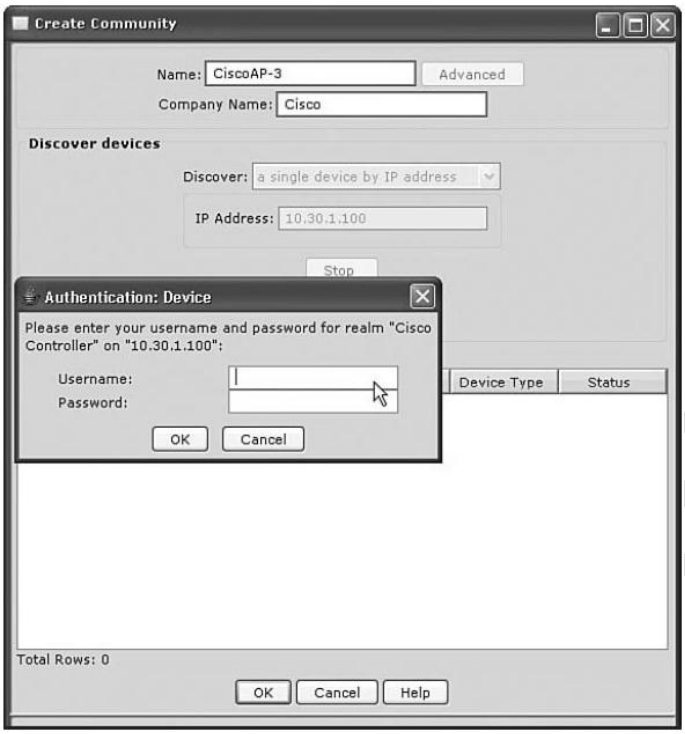


چنانچه AP مورد نظر را انتخاب کنید ، وارد منویی می شوید که می توانید جزییات بیشتری را کانفیگ نمایید .



استفاده از Cisco Configuration Assistant :

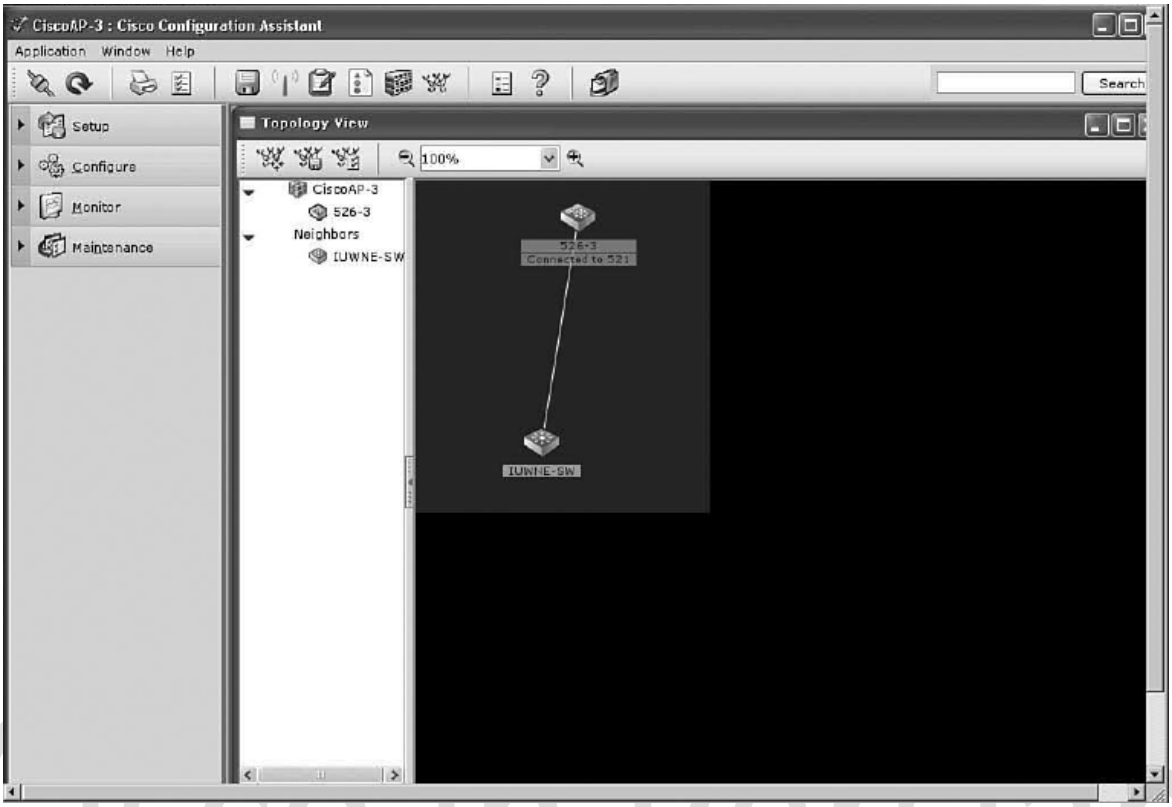
CCA یک بزار مدیریتی است که روی سیستم windows نصب می شود و بر اساس Cisco Network Assistant کار می کند که برای طراحی Cisco Mobility بهینه شده است .
پس از نصب و اجرای نرم افزار ، ابتدا باید یک Community بسازید که در واقع نامیست که شما به شبکه ی Mobility Express خود می دهید .

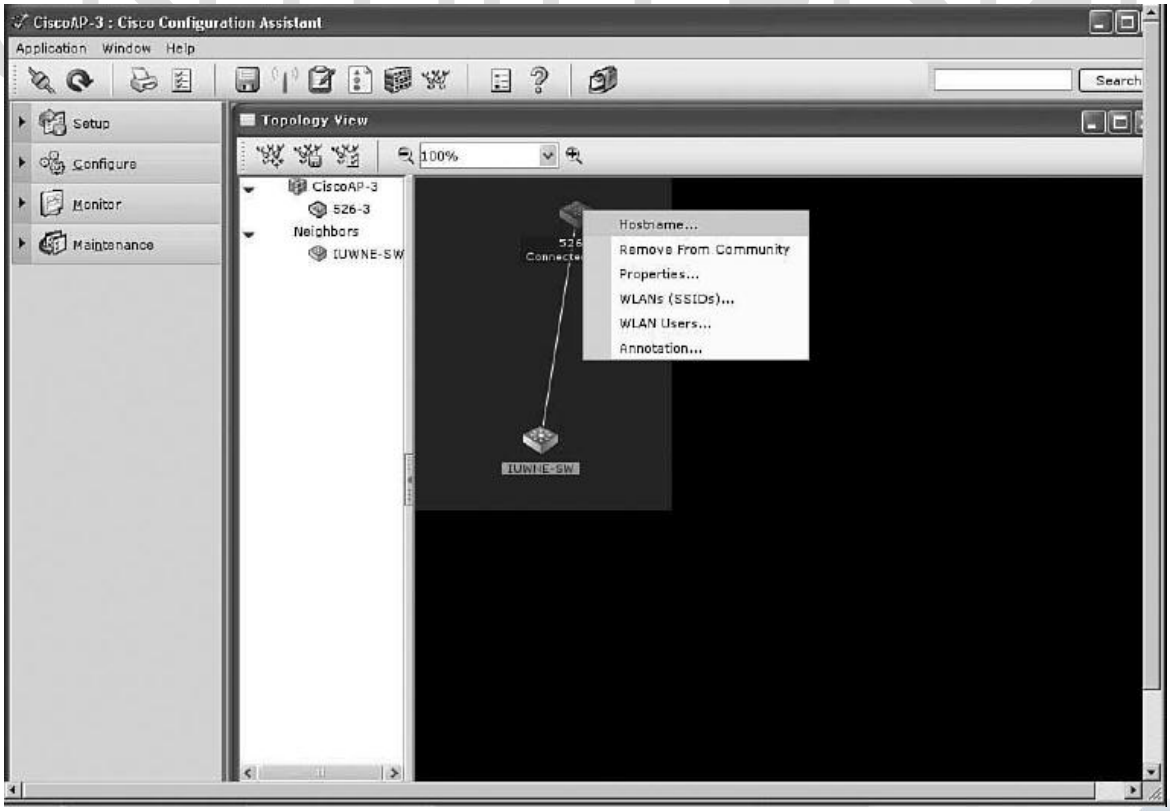


CCAتمام Standalone AP ها را پیدا خواهد کرد . اگر از CCA 1.5 یا بالاتر استفاده می کنید ، می توانید Standalone AP ها را به Lightweight تبدیل نمایید .
CCA همچنین با استفاده از CDP و IP Discovery می تواند کنترلر ها را نیز پیدا کند .

نکته : CDP یا همان Cisco Discovery Protocol ، یک پروتکل اختصاصی سیکو است که می تواند اطلاعاتی در مورد دستگاههایی که مستقیما به هم متصل هستند ، کسب نماید .

در دو شکل زیر ، می توانید Topology view را مشاهده کنید .
همچنین می بینید که با کلیک راست روی هر دستگاه ، می توان به راحتی آنرا کانفیگ نمود .





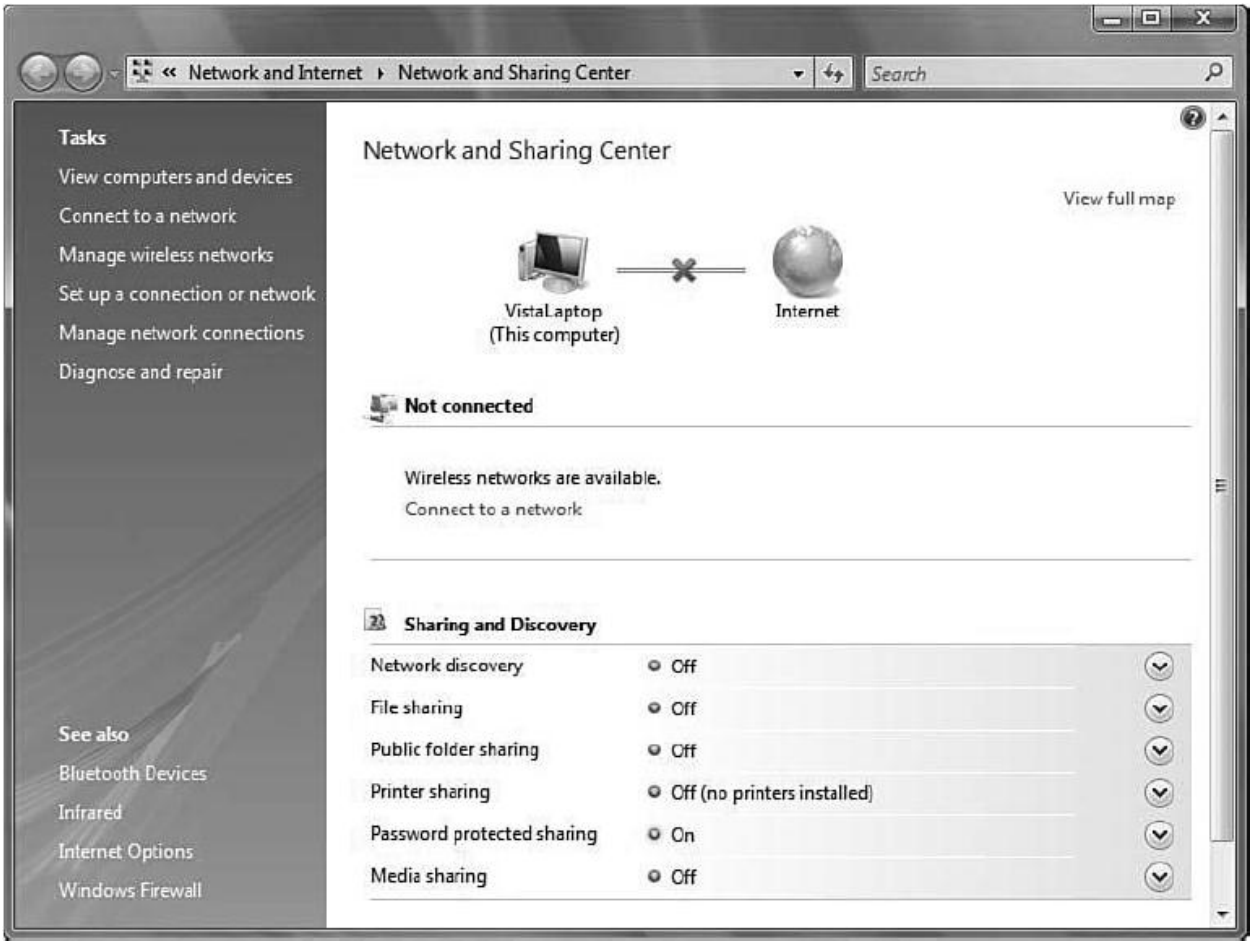
فصل شانزدهم : کاربران Wireless

- ❖ استفاده از windows برای اتصال به یک Wireless LAN
- ❖ استفاده از Macintosh برای اتصال به یک Wireless LAN
- ❖ استفاده از Linux برای اتصال به یک Wireless LAN
- ❖ استفاده از ADU برای اتصال به یک Wireless LAN
  - ✓ اطلاعات Adaptor
  - ✓ Advanced Statistics
  - ✓ ابزار Site Survey
  - ✓ ACAU
  - ✓ Cisco SSC

در یک محیط متحرک و متغیر ، تمامی کاربران با تمامی سیستم عامل های مختلف (اعم از Windows ، Linux ، Mac ، و ...) باید بتوانند با شبکه ی وایرلس ارتباط برقرار نمایند . در این فصل ، به ابزار های تنظیم شبکه که در دستگاههای ویندوز ، لینوکس و مکینتاش کاربرد دارند می پردازیم . همچنین با ابزاری به نام ADU آشنا می شویم که سیسکو طراحی نموده است تا تنظیم جزییات شبکه راحت تر شود و برخی امکانات اضافی نیز در اختیار ما قرار می دهد .

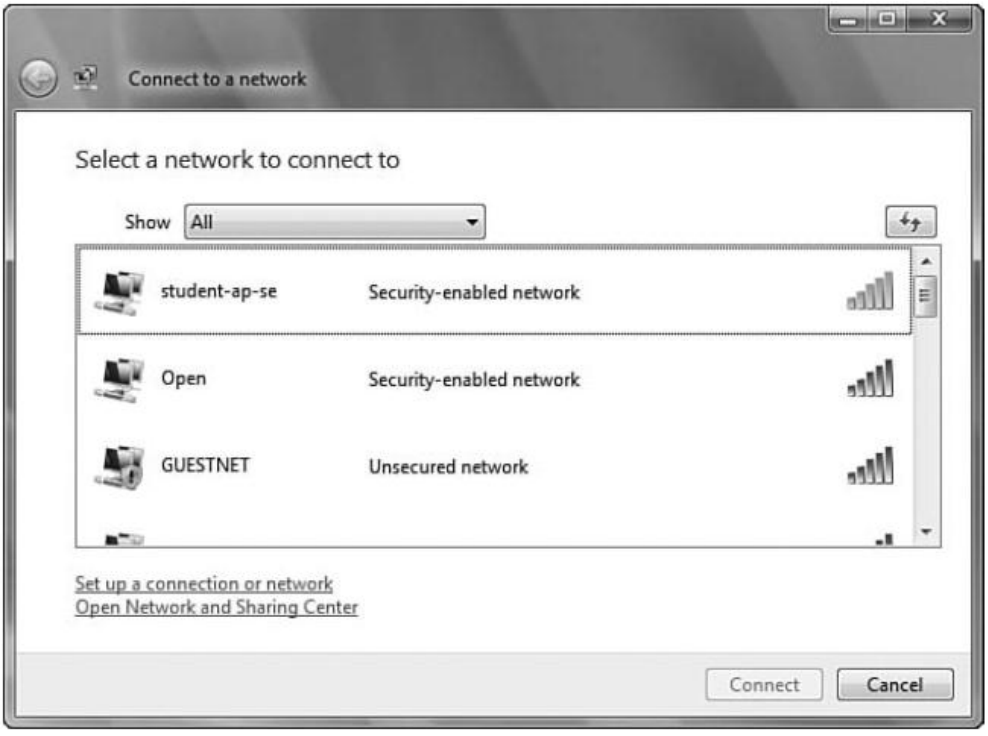
استفاده از Windows برای اتصال به یک Wireless LAN :

WZC یا همان Wireless Zero Configuration ، نرم افزار تنظیمات وایرلس روی Microsoft Windows است و یک سری قابلیت های اولیه برای دسترسی به شبکه ی وایرلس را در اختیار ما قرار می دهد ، اما برای troubleshooting مناسب نیست . خیلی از vendor ها مانند IBM یا Lenovo یک نرم افزار برای کاربران خود دارند که جایگزین WZC شده است .



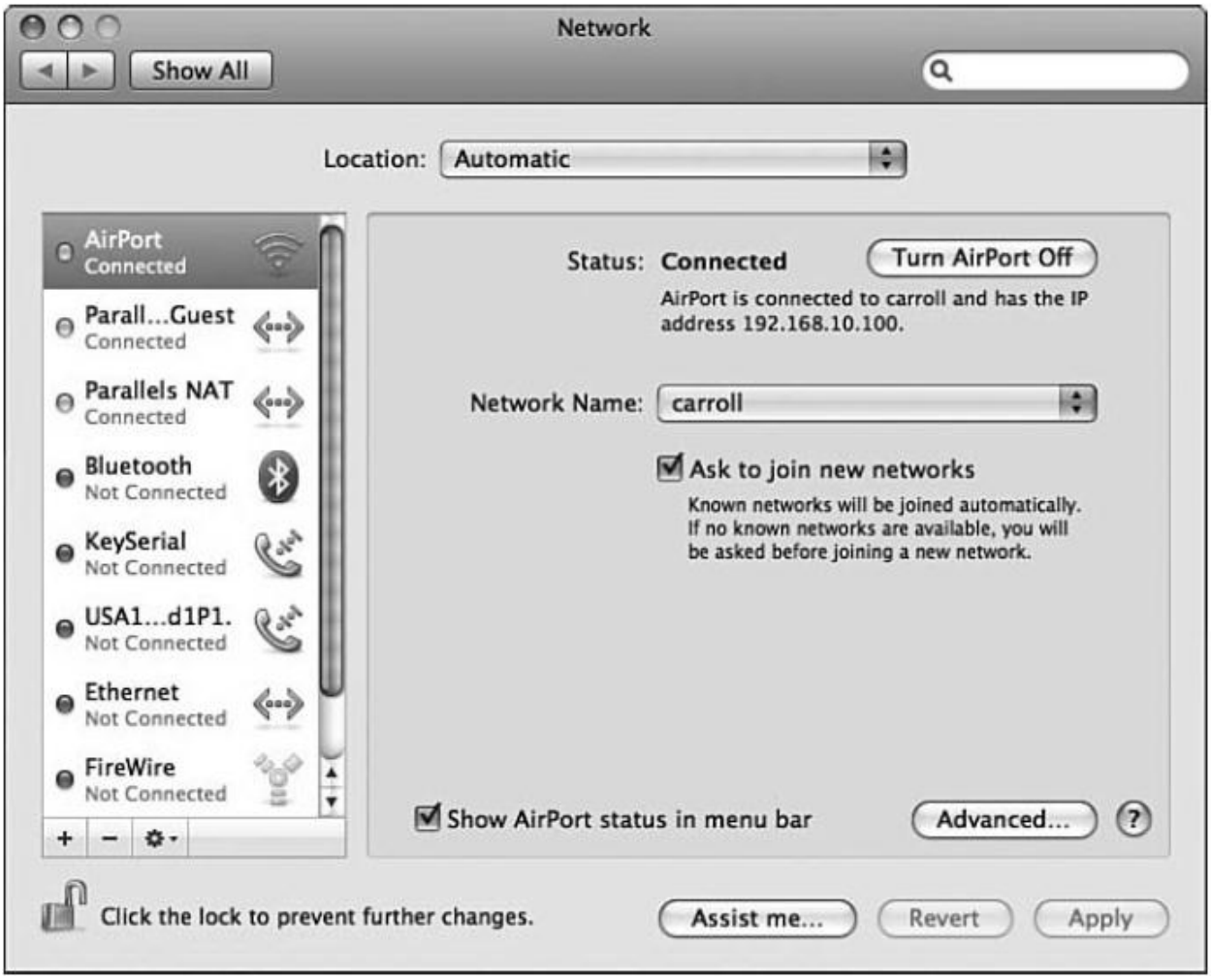
WZC ابتدا به دنبال AP می گردد تا در واقع به شبکه های Infrastructure متصل گردد . اگر موفق نشد ، شبکه های Ad-Hoc را امتحان می نماید . اگر باز هم موفق نشد ، خودش شروع به ارسال beacon می کند و خود را به عنوان node اول شبکه در نظر می گیرد و منتظر می ماند تا بقیه به آن وصل شوند . چنانچه باز هم موفق نشد ، شبکه های Non-preffered را امتحان می کند که البته بصورت پیشفرض disable است و باید آن را فعال نمود .
در نهایت اگر هیچ کدام از این مراحل منجر به ایجاد ارتباط به یک شبکه ی وایرلس نشد ، WZC برا ی خودش یک Network Name تصادفی انتخاب کرده و کارت شبکه ی خود را در حالت Infrastructure قرار می دهد و هر ۶۰ ثانیه به دنبال یک شبکه ی جدید ، تمام محدوده ی خود را scan می کند .

هنگامیکه کاربر WZC می خواهد به یک شبکه متصل شود ، از روش Active Scanning استفاده می کند .
در حالت Active Scanning ، در واقع WZC پیام های Probe Request را با فیلد SSID خالی ارسال می نماید که به آن Active Null Scanning می گویند (زیرا هنوز نام SSID را نمی داند). AP هایی که این پیام را می شنوند ، لیستی از SSID های در دسترس را به عنوان پاسخ می فرستند (response) که WZC از بین SSID های این لیست (Preffered Networks)، به ترتیب یکی را انتخاب می کند و تلاش می کند به آن متصل شود .



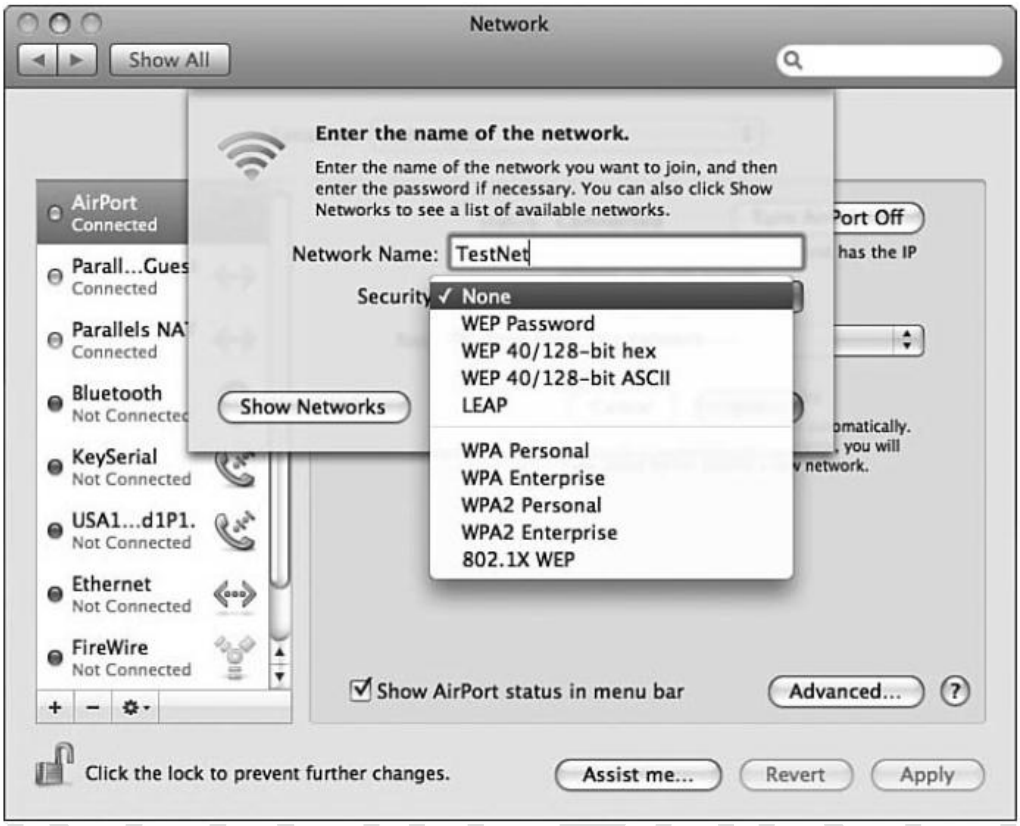
استفاده از Macintosh برای اتصال به یک Wireless LAN :

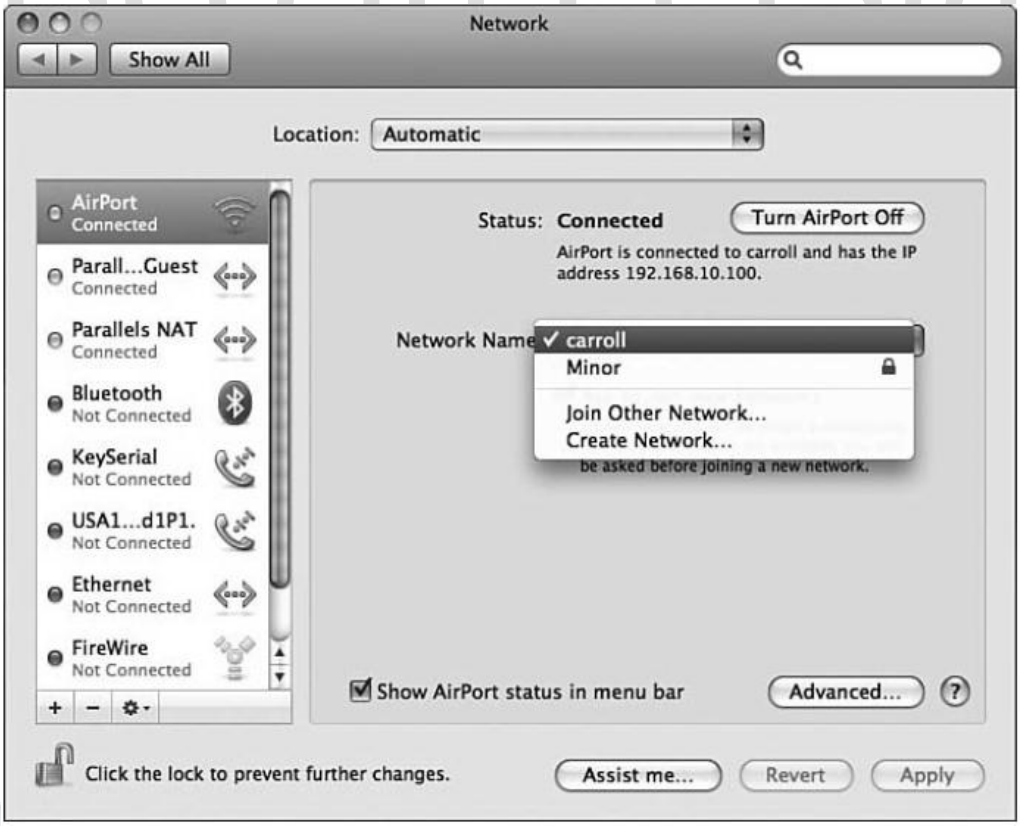
چنانچه از مکینتاش استفاده می کنید ، می توانید با استفاده از AirPort یا AirPort Extreme ، تنظیمات WLAN را انجام دهید .



روی Mac OSX 10.5 یا بالاتر ، می توانید تنظیمات امنیتی را برای هر شبکه (SSID) اعمال کنید .

همچنین می توانید از روی شبکه هایی که AirPort پیدا کرده ، یکی را انتخاب و جزییات آن را مشاهده و تنظیم کنید .



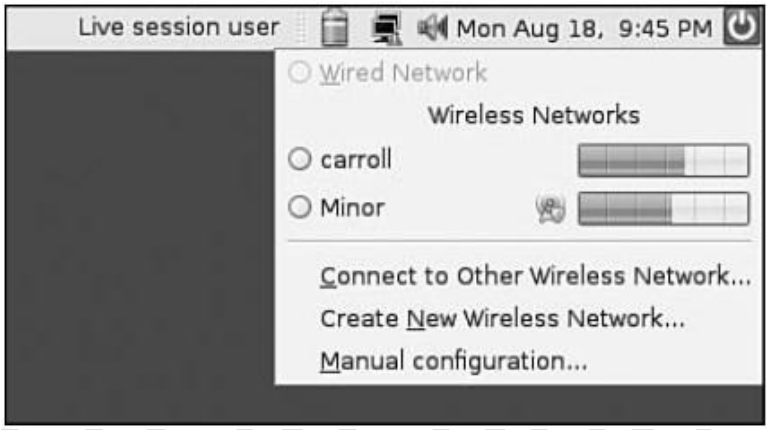


استفاده از Linux برای اتصال به یک Wireless LAN :

برای کار با WLAN ها ، لینوکس هم اینترفیس مبتنی بر دستور (Command-line) و هم ابزار گرافیکی (GUI) در اختیار دارد .

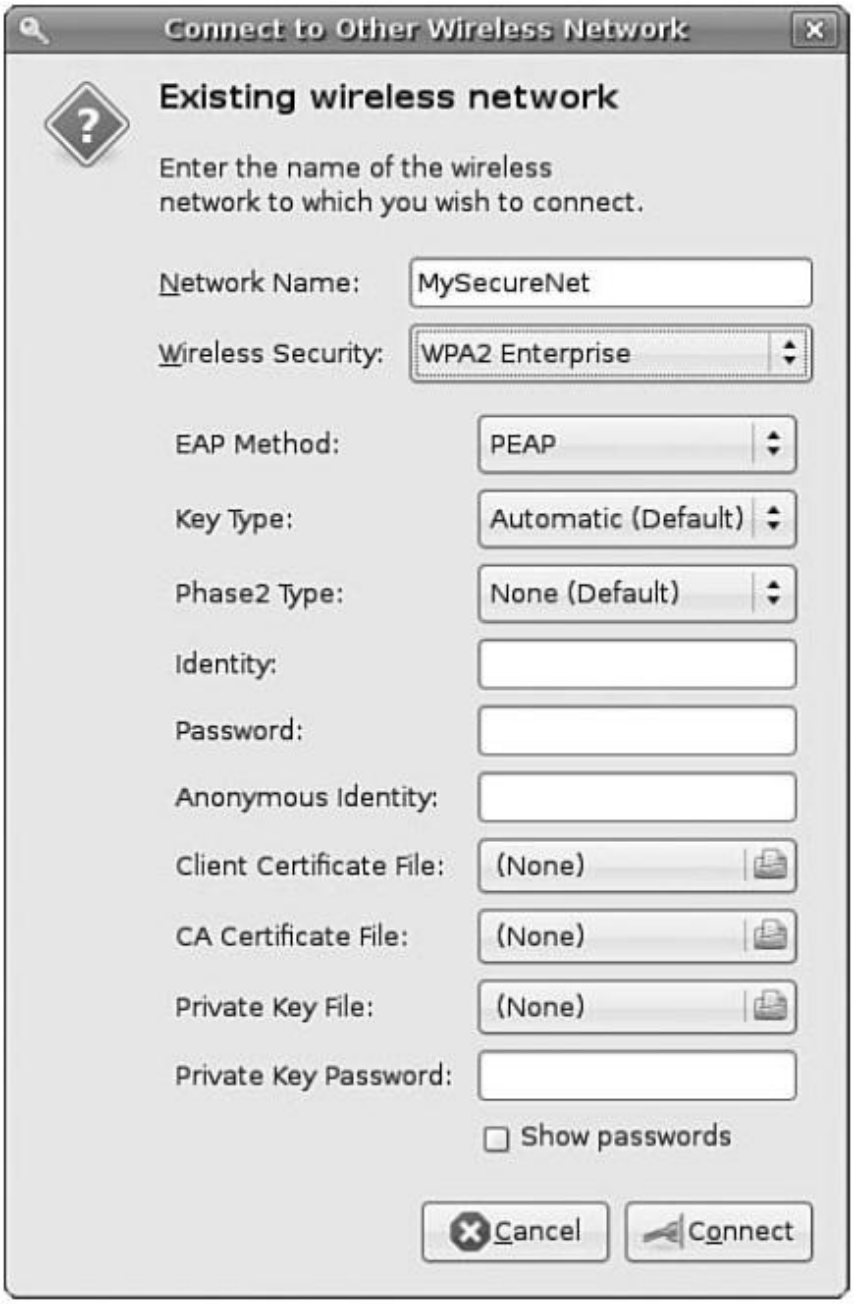
iwconfig ، همان ابزار command-line لینوکس است و تقریبا شبیه به ipconfig (که برای کار با Ethernet است) ، می باشد .

NetworkManager ، ابزار GUI لینوکس است که با آن می توان Wireless Profile ها را ساخته و تنظیم نمود .



برای شروع پروسه ی تنظیم پروفایل ها ، روی Connect to Other Wireless Network کلیک کنید .
سپس نام شبکه و تنظیمات امنیتی آن را وارد نمایید .

پس از این مرحله ، گزینه های متعددی پیش رو خواهید داشت که می توانید هر کدام را تنظیم نمایید .



هنگامیکه روی connect کلیک می کنید ، ابزار NetworkManager پیام های Discovery را با مشخصات تنظیم شده ارسال می کند. چنانچه به هر علتی ، پارامترهای اشتباهی وارد شده باشند ، یک message box نمایش داده می شود که از شما می خواهد اشتباه خود را تصحیح نمایید .

اگر یک connection به خاطر وجود پارامترهای اشتباه نتواند برقرار شود ، باز هم در لیست Available Network قرار می گیرد ؛ البته توان سیگنال آن صفر خواهد بود .

استفاده از ADU برای اتصال به یک Wireless LAN :

شما برای اتصال به یک WLAN چندین راه دارید . سیسکو نرم افزاری برای مدیریت یک کارت وایرلس a/b/g تهیه نموده است که ADU نام دارد (Aironet Desktop Utility).

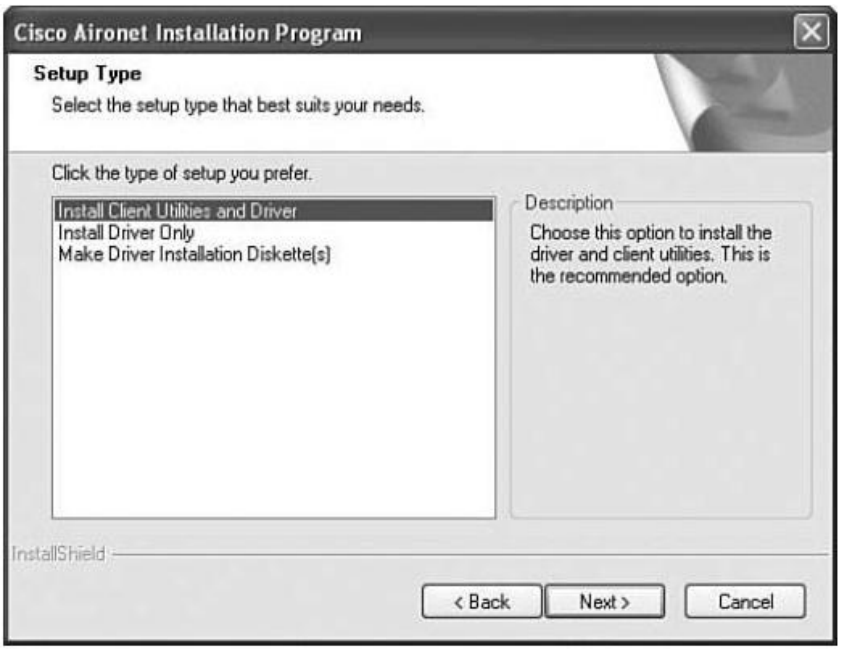
همچنین ASTU (Aironet System Tray Utility) یک جزء زیرمجموعه ی ADU است و در واقع برخی از option های ADU را ندارد .

ADU و ASTU نسبت به WZC امکانات بیشتری دارند و تمام feature های کارت های شبکه را در بر می گیرند (در صورتیکه WZC اینطور نیست).

برای مقایسه ی ویژگی های WZC و ADU ، جدول زیر را مشاهده بفرمایید :

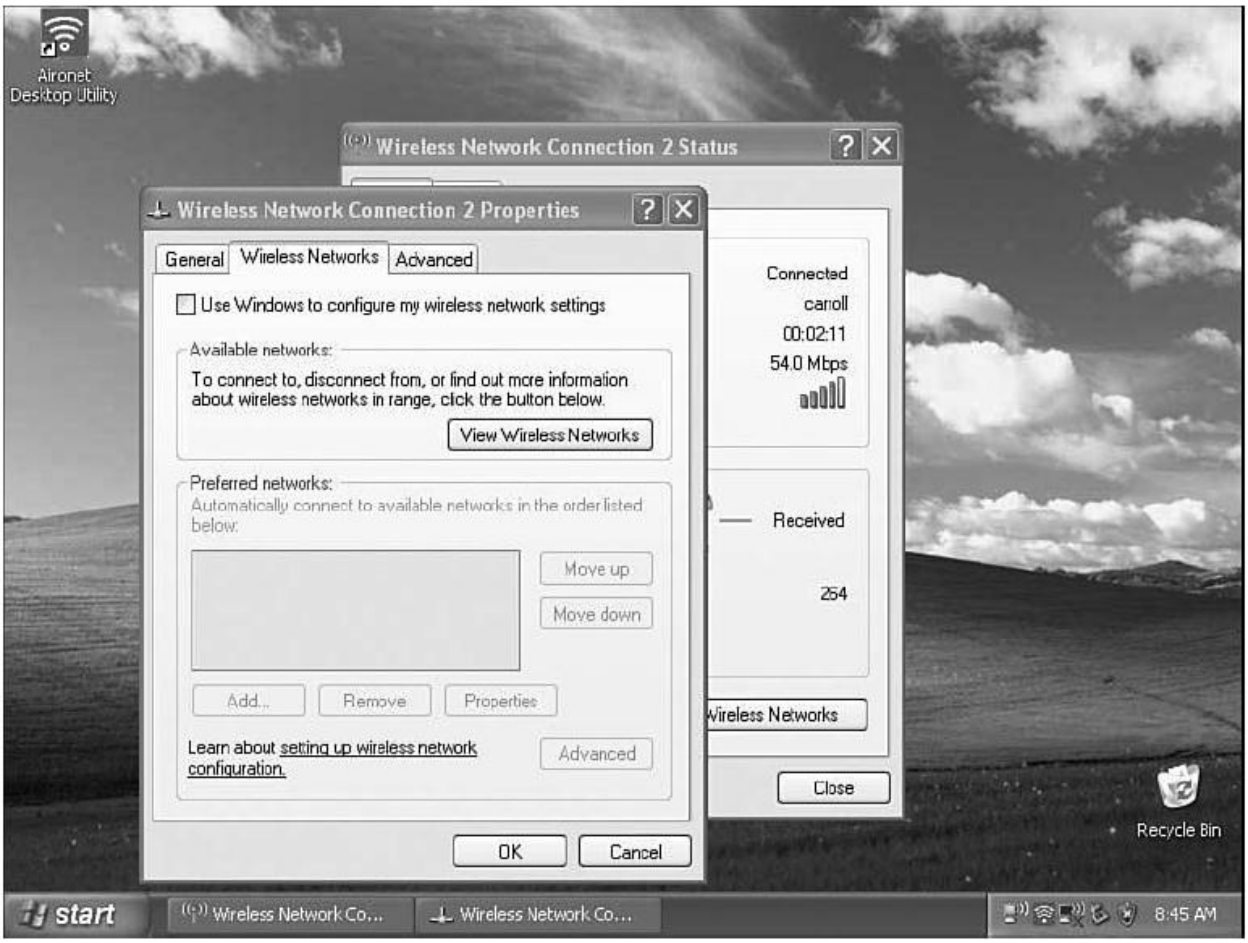
Capability	WZC	ADU
Scan different channels	No	Yes
Determine which APs are on which channels	No	Yes
Determine the authentication and security configurations of each detected AP	No	Yes
Get RSSI information	No	Yes
Get SNR information	No	Yes

برای نصب ADU ، می توانید به طریق زیر عمل کنید .



چنانچه گزینه ی Install Driver Only را انتخاب کنید ، یعنی شما مدیریت پروفایل ها و اتصال به شبکه را با WZC انجام می دهید .

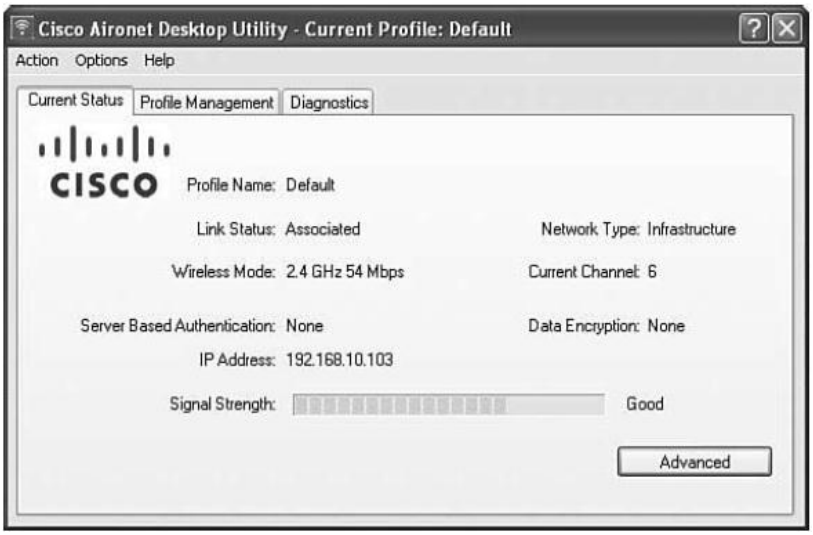
نکته : به شکل زیر توجه نمایید .



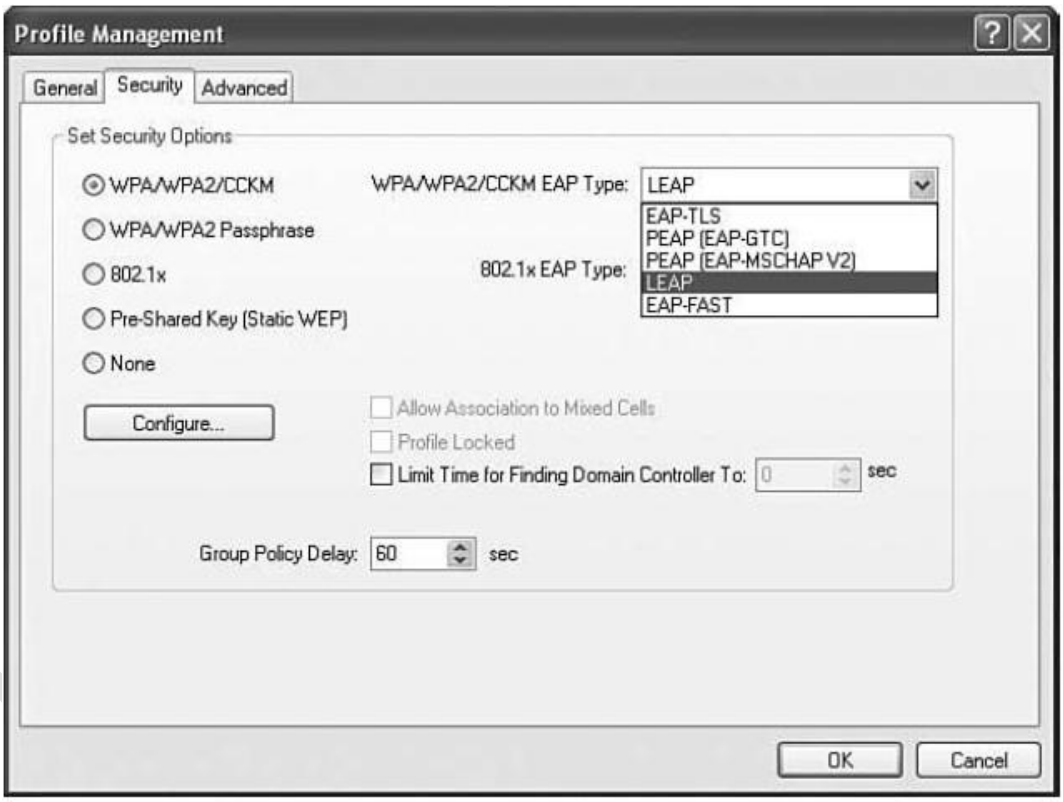
چنانچه می خواهید از ADU استفاده نمایید ، حتما توجه کنید که تیک گزینه ی زیر ، برداشته شده باشد :

- Use Windows to configure my wireless network settings

با کلیک راست بر روی آیکون ASTU ، می توانید موارد مختلفی را تنظیم نمایید . اینترفیس ADU بدین شکل است.



همچنین می توانید در Profile Management ، در تب Security تنظیمات امنیتی را اعمال نمایید .

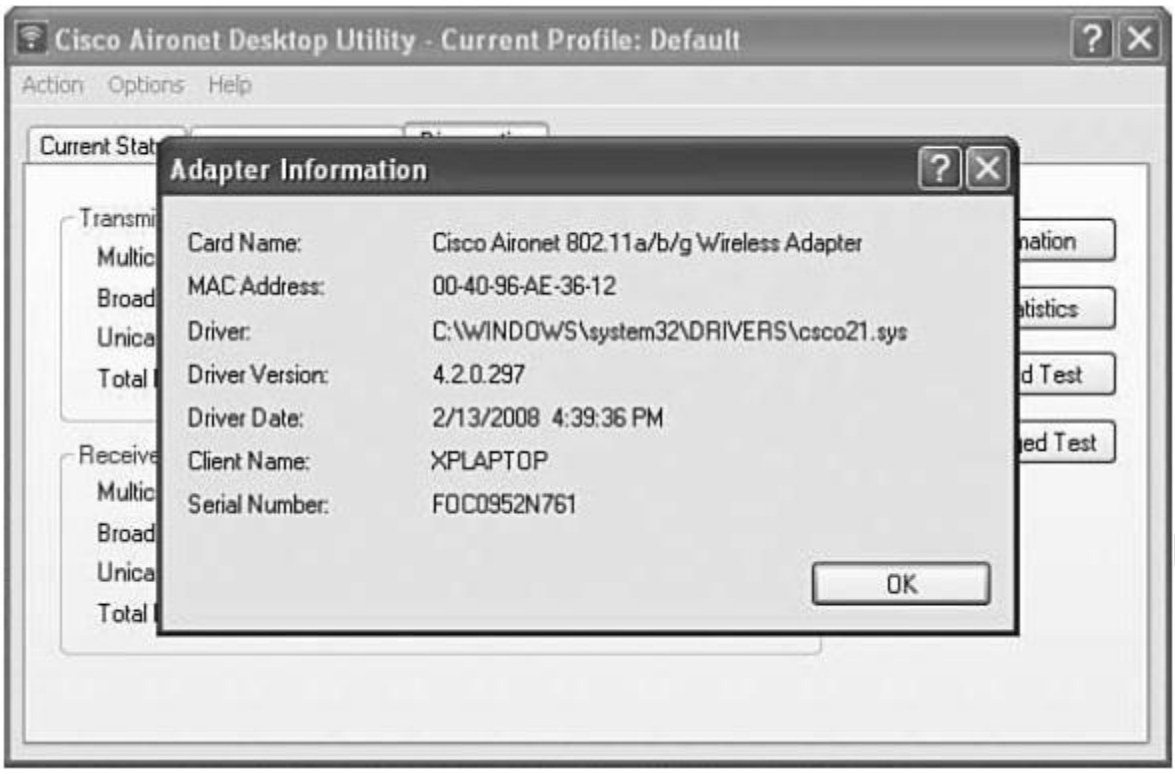


در جدول زیر ، می توانید بین حالت های مختلف security ، مقایسه ای داشته باشید .

Security Option	Encryption	Authentication
WPA/WPA2/CCKM	Rotating key	EAP methods (see 802.1x)
WPA/WPA2 Passphrase	Rotating key	8 to 63 ASCII or 64 hexadecimal passphrase
802.1x	None	EAP-TLS, PEAP, LEAP, EAP-FAST, host-based EAP (host-based is not an option for WPA/WPA2/CCKM)
Pre-Shared Key (Static WEP)	Weak	None
None	None	None

اطلاعات Adaptor :

در اینترفیس ADU ، چنانچه روی Diagnostics کلیک کنید ، در بخش Adaptor Information اطلاعات خوبی نظیر آدرس MAC کارت شبکه ، و نیز ورژن driver را مشاهده می کنید .



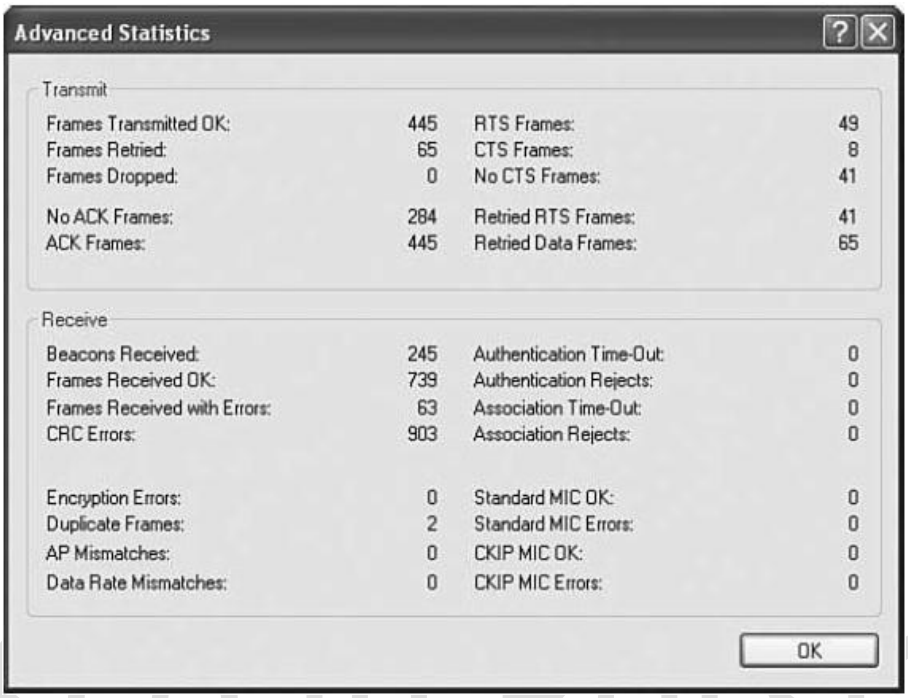
روی کنترلر می توانید با استفاده از آدرس MAC کاربر ، یک debug فعال کنید تا بتوانید اطلاعات خاصی از کاربران خود کسب کنید .
همچنین اطلاعات driver می توانند در Cisco Support Center برای پیدا کردن Bug Report ها به کار روند .

همانطور که می بینید ، برای نصب محصولات سیسکو ، می توان از قابلیت های خود windows استفاده نمود ، اما بهتر است از ADU و ACAU استفاده نمود (Aironet Client Administration Utility) ؛ زیرا قابلیت های بسیار زیادی در اختیار ما قرار می دهند .

همچنین می توانید از CASSU (Cisco Aironet Site Survey Utility) برای طراحی اولیه شبکه وایرلس بهره بجویید .

Advanced Statistics :

این بخش اطلاعات بیشتری در مورد فریم هایی که ارسال یا دریافت شده اند می دهد .



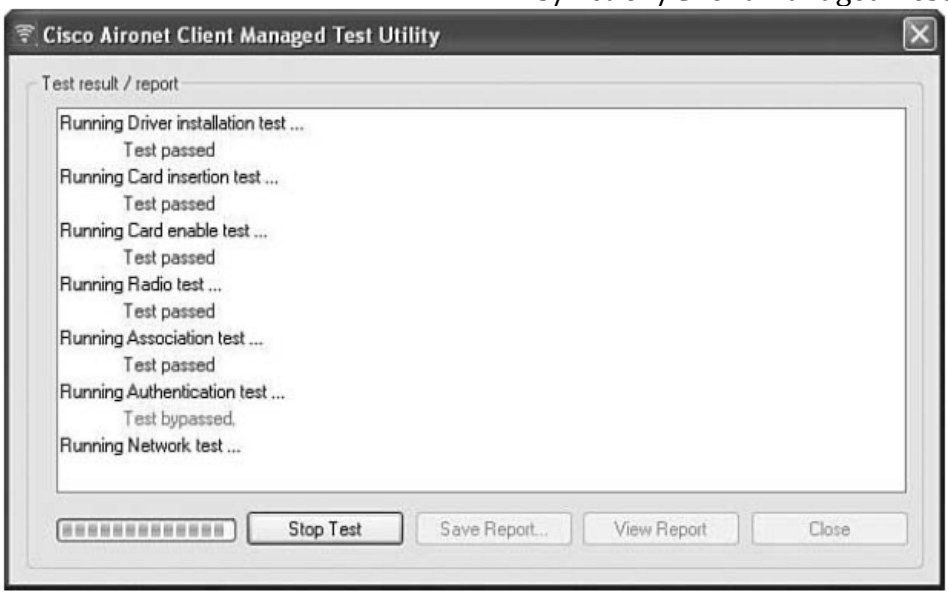
مثلا اگر مقدار زیادی frame retries **داشته باشید ، به معنای** collision **است .**

و CTS **و** RTS **نشان دهنده ی** frame error **یا کیفیت پایین لینک ارتباطیست .**

Authentication rejects **و** Authentication time-out **هم نشاندهنده ی مشکلات** AAA srever **می باشد .**

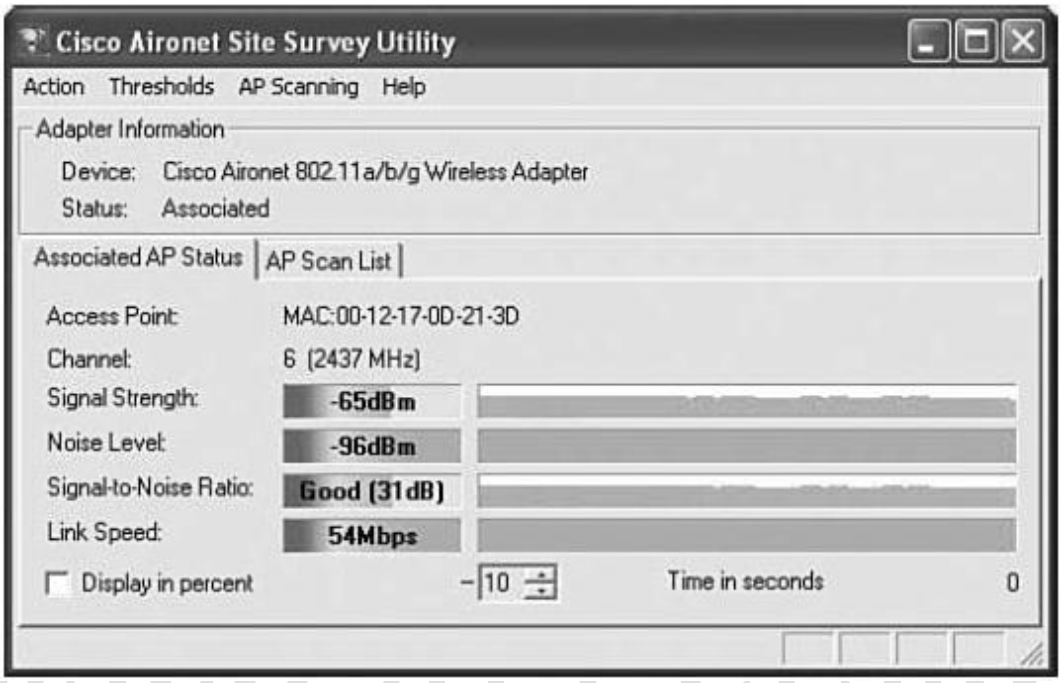
همچنین ابزاری برای تست کردن عملکرد و نیز troubleshooting **وجود دارد که از بخش زیر قابل اجراست :**

ADU/Action/Client Managed Test/Start Test

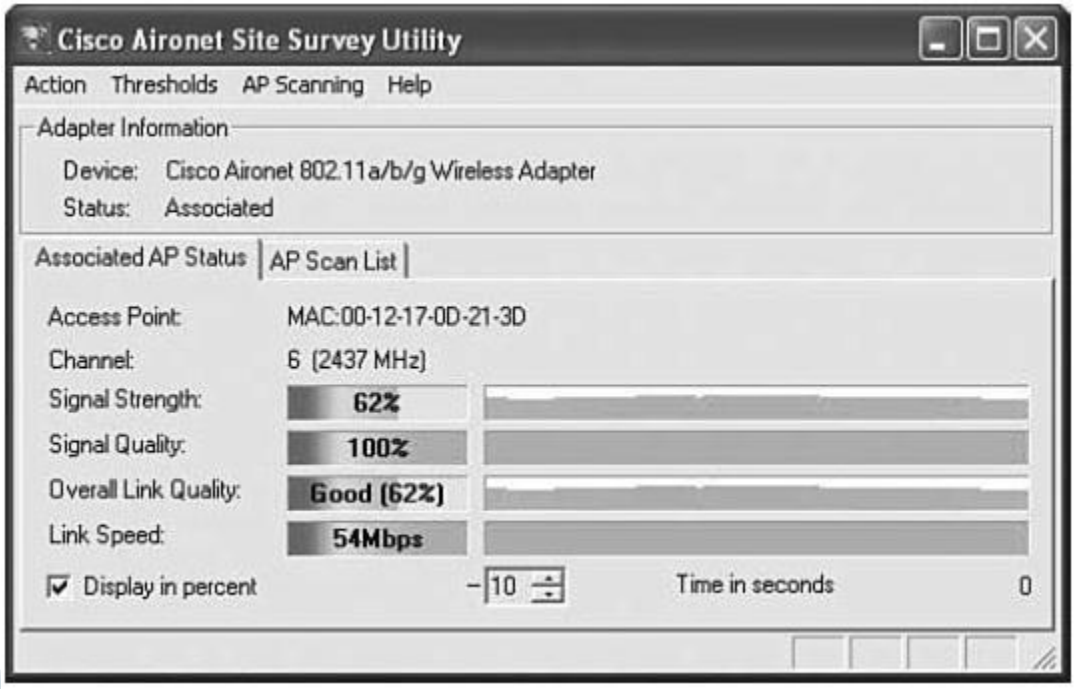


ابزار Site Survey :

ابزار (Cisco Site Survey Utility) CSSU نرم افزاریست که البته یک نقشه از شبکه ارائه نمی دهد ، اما می تواند اطلاعات خوبی در مورد کیفیت و قدرت سیگنال دریافتی به شما بدهد .

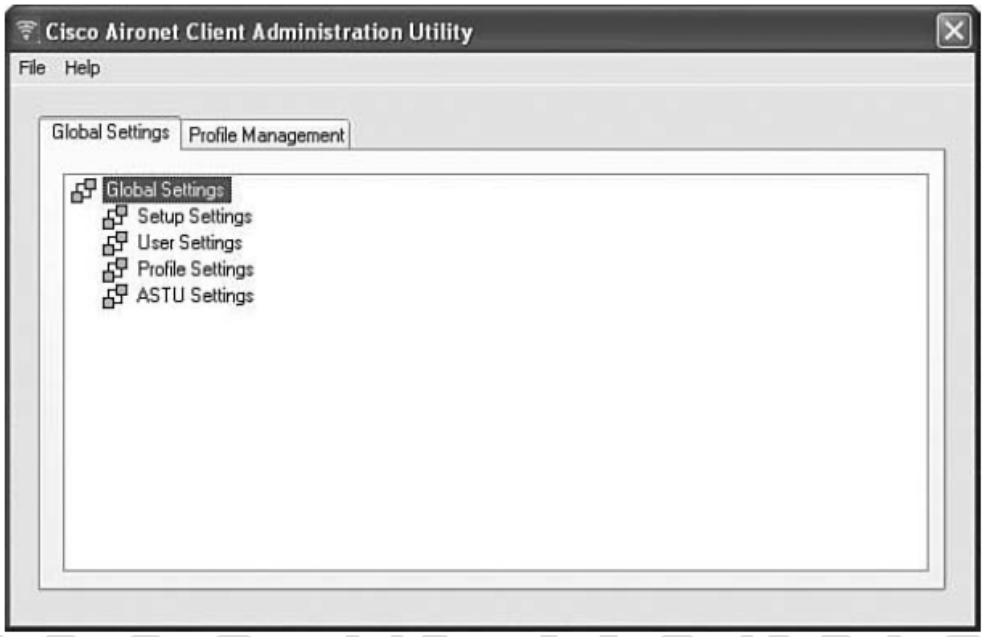


خروجی را هم بر اساس دسیبل و هم بر اساس درصد می توانید مشاهده کنید که البته دسیبل دقیق تر است .



Aironet Configuration Administration Utility :

ACAU طراحی شده تا فرآیند نصب ADU و پروفایل های کاربران را بصورت خودکار انجام دهد .



پروفایلی که اینجا ساخته می شود ، شبیه به پروفایلیست که در ADU ساخته می شود ؛ با این تفاوت که این پروفایل ها local نیستند .

سپس باید این پروفایل ها را در همان دایرکتوری که ADU عمل می کند ذخیره نماییم تا با بالا آمدن ADU ، این پروفایل را به عنوان تنظیمات بپذیرد و اعمال نماید .

Cisco Secure Services Client :

Cisco SSC یک نرم افزاری کاربری است که 802.1x authentication را هم برای کاربر و هم برای دستگاهها فراهم می سازد (هم برای شبکه های wired و هم برای شبکه های wireless).

SSC برای اجرای نرم افزار ، نیازی به کارت وایرلس سیسکو ندارد . می توان گفت SSC جایگزینی برای WZC است با قابلیت هایی متفاوت و کامل تر .

یکی از قابلیت های SSC اینست که در صورتیکه آداپتور وایرلس توانست به یک شبکه ی وایرلس متصل شود ، کاربران می توانند بصورت اتوماتیک اینترفیس سیمی را غیر فعال کنند .

SSC سه نوع لایسنس دارد :

۱- لایسنس رایگان ۹۰ روزه که البته تمام امکانات را دارد .
۲- نسخه ی دایم (فقط برای شبکه ی wired).
۳- نسخه ی دایم (برای شبکه های Wired و Wireless).

فصل هفدهم : امنیت شبکه های Wireless

- ❖ مخاطرات شبکه های بیسیم
  - ✓ شبکه های Ad-hoc
  - ✓ Rogue AP
  - ✓ Client Missassociation
- ❖ Management Frame Protection
  - ✓ Infrastructure MFP
  - ✓ Client MFP
- ❖ انواع حملات وایرلس
  - ✓ Passive Attacks
  - ✓ Active Attacks
  - ✓ Inline Attacks
  - ✓ Offline Attacks
  - ✓ Reconnaissance Attacks
  - ✓ Access Attacks
  - ✓ DoS Attacks
- ❖ Open Authentication
- ❖ PSK & WEP
- ❖ MAC Address Filtering
- ❖ Authentication مرکزی
- ❖ 802.1x و نحوه ی عملکرد آن
- ❖ فرآیند EAP
  - ✓ Authentication Server
  - ✓ EAP-TLS
  - ✓ EAP-FAST
  - ✓ PEAP
  - ✓ LEAP
- ❖ WPA
- ❖ WPA2

کاملا مشخص است که شبکه های وایرلس امنیت کمتری نسبت به شبکه های wired دارند . در این فصل ، با انواع روش های امن کردن یک شبکه ی وایرلس آشنا می شوید . برخی از روش ها برای شناسایی کاربران به کار می روند ، و برخی دیگر هم راهکارهایی جهت پنهان کردن اطلاعات ارسالی ارائه می دهند ؛ روش هایی هم هستند که هر دو کاربرد را دارند .

مخاطرات شبکه های بیسیم :

مشکلات و خطراتی که در شبکه های وایرلس وجود دارند ، بسته به نوع و ساختار شبکه و کاربران متفاوت هستند . در ادامه به چندین نوع از این تهدیدات امنیتی می پردازیم .

شبکه های Ad Hoc :

در این شبکه ها ، این احتمال وجود دارد که یک هکر یا attacker به یک کاربر مجاز متصل شود ، سپس به بخش secured wired LAN شبکه bridge بزند و به این ترتیب مراحل اولیه ی شناسایی و قوانین امنیتی را دور بزند .

Rogue AP ها :

این AP می تواند با اجرای یک نرم افزار روی یک لپ تاپ ، مثلا نقش DHCP server را بازی کند ؛ IP ها را عوض کند و مسیر ترافیک را به سمت خود یا هر جای دیگری تغییر دهد .

چنانچه یک کاربر به یک rogue AP متصل شود ، باید به عنوان rogue client در نظر گرفته شود . زیرا هر کاربری که به این AP ها متصل می شود ، مراحل و پل های امنیتی را دور می زند و به درستی شناسایی نمی شود .

Client Misassociation :

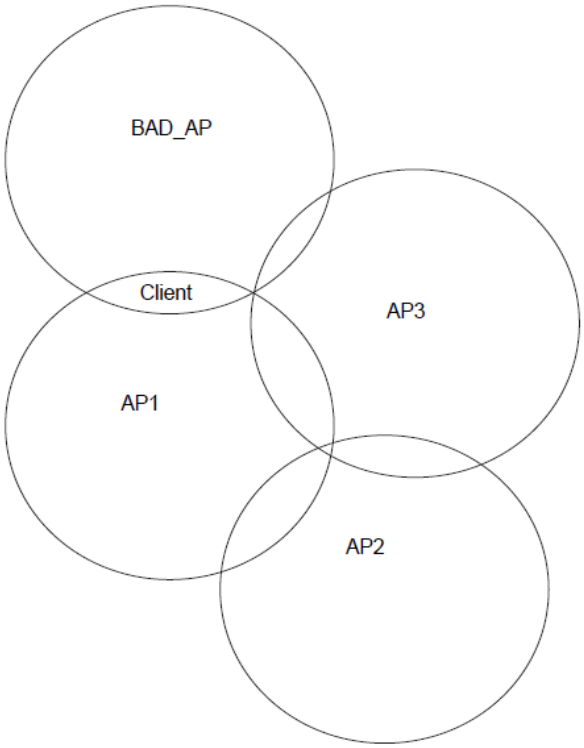
هنگامیکه کاربر به یک AP متصل می شود ، سیستم عامل معمولا SSID را ذخیره می کند . association اشتباه زمانی رخ می دهد که کاربر به اشتباه با یک rogue AP ارتباط برقرار کرده و associate شود ؛ به عبارت دیگر یک rogue AP وارد شده و SSID مورد نظر ما را یاد گرفته و آن را با beacon هایش تبلیغ کند . لذا این کاربر به اشتباه به آن وصل می شود و از آنجا به اینترنت متصل شده و از آن به بعد ، هر اطلاعاتی که ارسال و دریافت می کند ، دقیقا تحت نظارت و مانیتورینگ rogue AP قرار خواهد داشت . این امر را Management Frame Spoofing می گویند و برای جلوگیری از آن باید از Management Frame Protection استفاده نمود .

Management Frame Protection :

MFP دو روش برای محافظت دارد :

- ✓ در **Infrastructure MFP** ، هر فریم مدیریتی یک cryptographic hash به نام MIC دارد که قبل از FCS به فریم اضافه می گردد . لذا WLAN یک key یکتا دارد که به هر radio روی AP ارسال می گردد . لذا AP فریم های مدیریتی را ارسال می کند و شبکه می فهمد که AP در protection mode قرار دارد . لذا اگر کسی SSID را به دروغ تبلیغ نماید و آن key یکتا را نداشته باشد ، WLAN آن پیام را invalidate می کند . این امر باعث می شود که سایر AP ها که فریم های نامعتبر را می شنوند ، به کنترلر گزارش دهند .

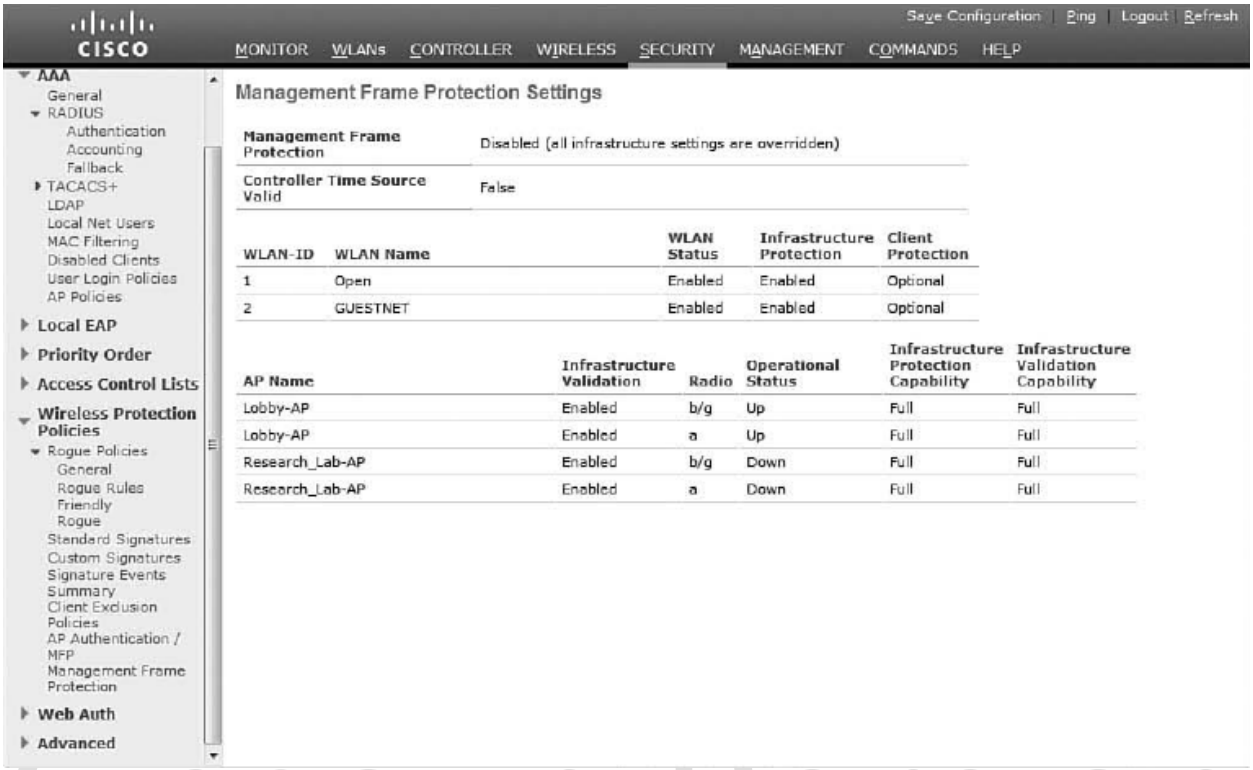
- ✓ در **Client MFP** ، اگر کاربر دارای CCXv5 یا ورژن بهتر باشد ، می تواند با AP مذاکره نموده و MIC را بدست آورد .



بهترین ویژگی این روش ، گستردگی تشخیص است . مزیت دیگر Client MFP اینست که شبکه را نسبت به حمله های DoS محافظت می کند . مثلا اگر یک rogue AP یک فریم deauthentication ارسال کرد ، کاربر می تواند ببیند که این containment frame هیچگونه MIC ندارد ، لذا آن را دور می اندازد .

برای تنظیم MFP ابتدا باید آن را فعال نمایید :
SECURITY / Wireless Protection Policies / AP Authentication/MFP

برای دیدن MFP با WLC ، به بخش زیر بروید :
SECURITY / Wireless Protection Policies / Management Frame Protection



انواع حملات وایرلس :

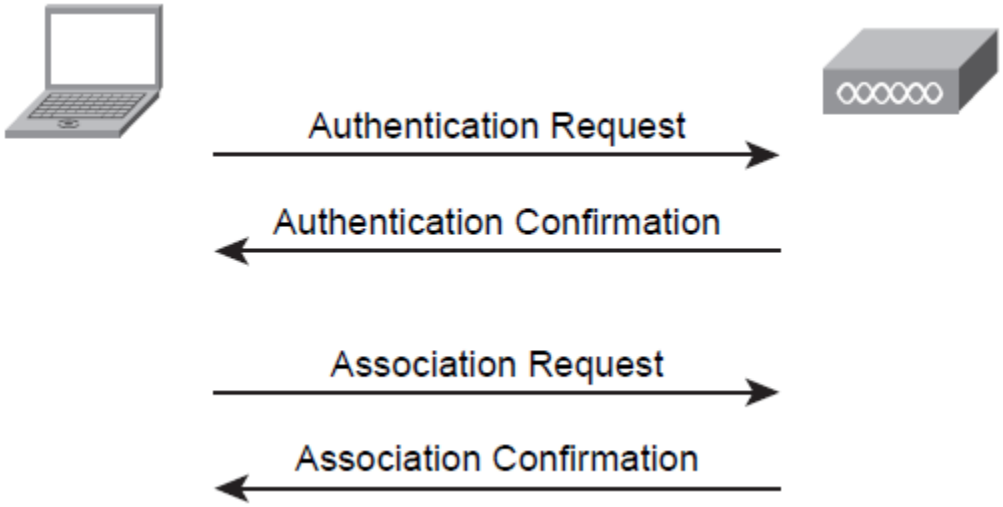
- **Passive Attack** : هکر چیزی به شبکه ارسال نمی کند ، بلکه تنها از اطلاعات شبکه استفاده می نماید.
- **Active Attack** : هکر بصورت فعال با شبکه تعامل دارد . مثلا از یک rogue AP استفاده می کند (یا حملاتی مانند DoS دارد).
- **Inline Attack** : هکر به همان کانالی که شبکه ی وایرلس فعال و متصل است ، وصل می شود .
- **Offline Attack** : هکر به یک کانال دیگر متصل است و از آن طریق به شبکه ی وایرلس دسترسی دارد .

چند نمونه از حملاتی که هم به شبکه های وایرلس و هم به شبکه های سیمی اعمال می شوند عبارتند از :

- **Reconnaissance Attack** : در حملات شناسایی ، هکر سعی می کند اطلاعات مختلفی از شبکه ی شما بدست آورد . برای جلوگیری از این حملات ، باید SSID را پنهان نمود ؛ یعنی آن را تبلیغ نکنیم .
- **Access Attack** : هکر سعی دارد به منابع ، دستگاهها ، و اطلاعات مختلف شبکه دسترسی پیدا کند . برای جلوگیری از این حملات ، می توان از شناسایی بر اساس آدرس MAC استفاده کرد یا از WEP بهره جست .
- **Denial-of-Service (DoS) Attack** : این نوح حملات ، مانع از دسترسی کاربران مجاز به شبکه و منابع اطلاعاتی می شود . برای جلوگیری از DoS ، باید از IDS/IPS در شبکه های سیمی ، و نیز از MFP استفاده نماییم .

Open Authentication :

این نوع شناسایی ، در واقع بخشی از فرآیند Association است .



این نوع از authentication بیشتر در hot spot ها مورد استفاده قرار می گیرد ؛ یک روش امنیتی لایه ۲ است .

برای تنظیم آن ، در بخش Security ، گزینه ی None را انتخاب نمایید .

PreShared Key Authentication with Wired Equivalent Privacy :

با static WEP ، شما کاربران را شناسایی نمی کنید ؛ شما بررسی می کنید که آیا آنها یک key دارند یا خیر . شما نمی دانید که آنها چه کسی هستند ، فقط می دانید که آنها Key شما را می دانند .

در WEP ، ابتدا کاربر یک تقاضا به AP می فرستد . AP در پاسخ ، یک متن را به کاربر می دهد . کاربر توسط یک static WEP key که خودش دارد ، این متن را encrypt کرده و به AP می فرستد . AP متن جدید را با متن اصلی و WEP key مقایسه کرده و سپس کاربر را associate می نماید .

نکته : می توان گفت که خطر WEP از Open Authentication نیز بیشتر است . زیرا یک attacker می تواند با capture کردن متن اصلی (challenge text) و پاسخ آن (که همان encrypt شده است) ، به راحتی static WEP key را بدست آورد .

نکته : WEP از روش RC4 encryption استفاده می کند .

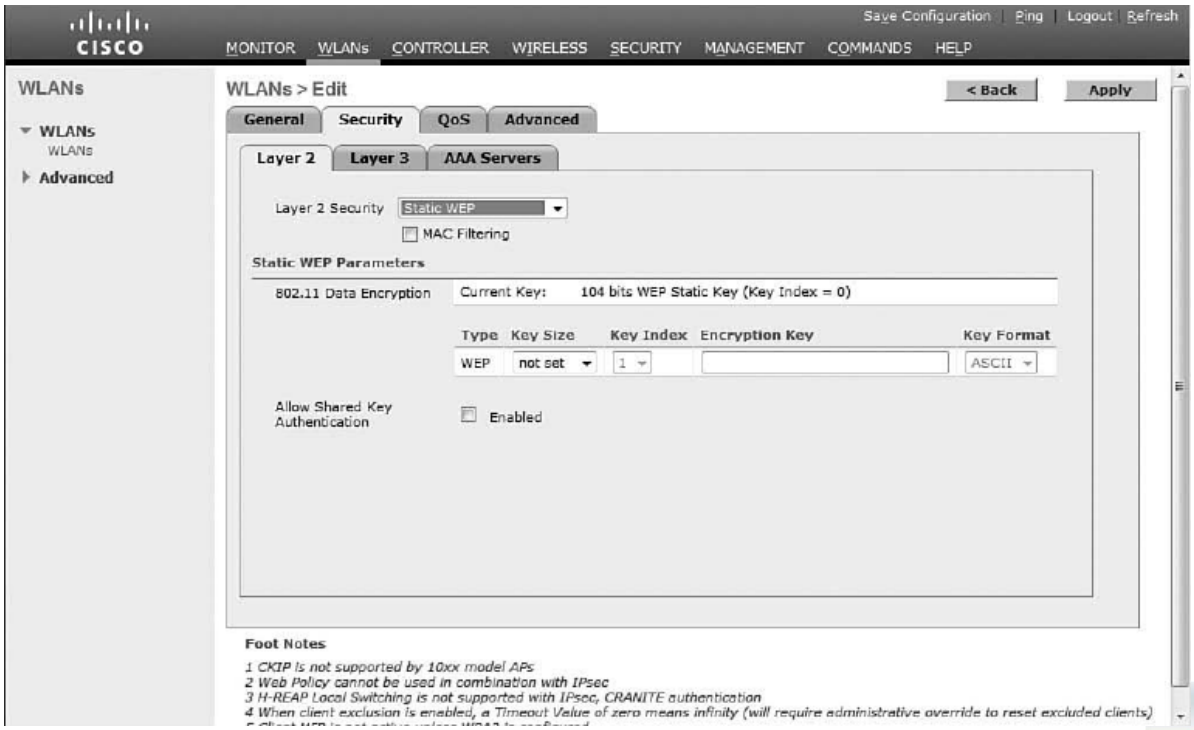
نکته : پس از authentication ، کاربر یک association برقرار کرده و شروع به send/receive می کند . لذا بعد از association ، دیگر WEP هیچ گونه protection یا encryption روی دیتا انجام نمی دهد .

نکته : نکته ی مهم دیگر در مورد WEP ، اندازه ی key است ؛ سه گزینه پیش رو داریم :

1. 40-bit key
2. 104-bit key
3. 128-bit key

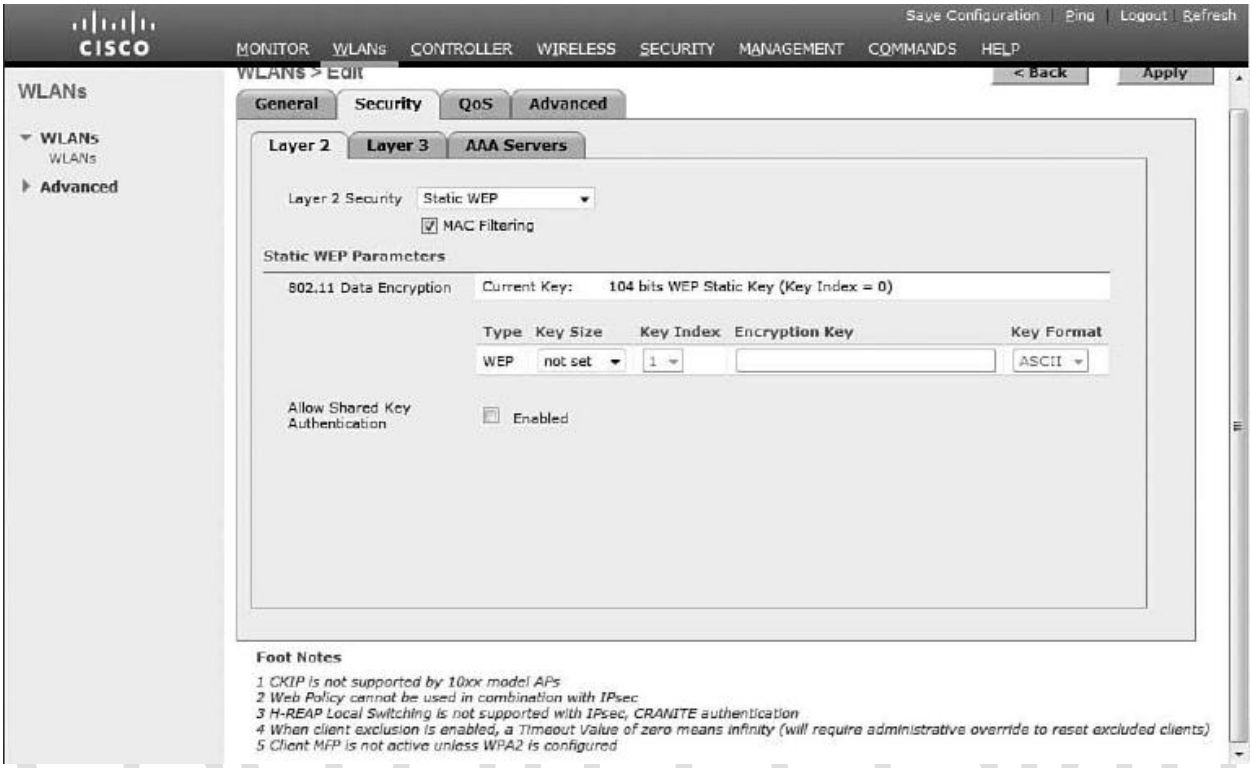
ما فقط می توانیم از ۱۰۴ بیت استفاده کنیم ؛ زیرا اگر ۲۴ بیت IV را به این گزینه اضافه کنیم ، ۱۲۸ بیت می شود که مورد قبول ویندوز است . در دو حالت دیگر ، مقادیر غیر قابل قبولی بدست می آید .

نکته : IV یا همان Initialization Vector ، در واقع تعدادی از بیت هاست که encryption key را تولید می کند .



MAC Address Filtering :

این روش توصیه نمی شود ، زیرا به راحتی می توان آدرس های MAC را spoof کرد .



Authentication مرکزی :

هنگامیکه پلیس راهنمایی ما را به خاطر سرعت زیاد متوقف می کند ، از ما تقاضای گواهینامه می کند . البته پلیس شناسایی و Identification را خودش انجام نمی دهد ، بلکه شخص ثالثی که پلیس به او اعتماد دارد این کار را انجام می دهد (مثلا از یک کامپیوتر استعلام می گیرد). در PKI یا Public Key Infrastructure نیز همین اتفاق می افتد . لذا به جای اینکه شناسایی بصورت محلی باشد و هر کس خودش این کار را انجام دهد ، این امر بصورت مرکزی (توسط یک سرور) انجام می گیرد .

PKI از certificate های دیجیتال استفاده می کند که توسط شخص ثالثی امضا شده اند ؛ این شخص ثالث ، می تواند یک CA باشد (Certificate Authority).

اولین گام اینست که یک CA Certificate بسازیم که از راههای مختلف ، از جمله CA server می توان این کار را انجام داد . از این به بعد ، هر وسیله ای که می خواهد ارتباطی برقرار کند ، از CA کمک می گیرد تا از امضای certificate دستگاه دیگر تاییدیه بگیرد . سپس authenticate می شوند .

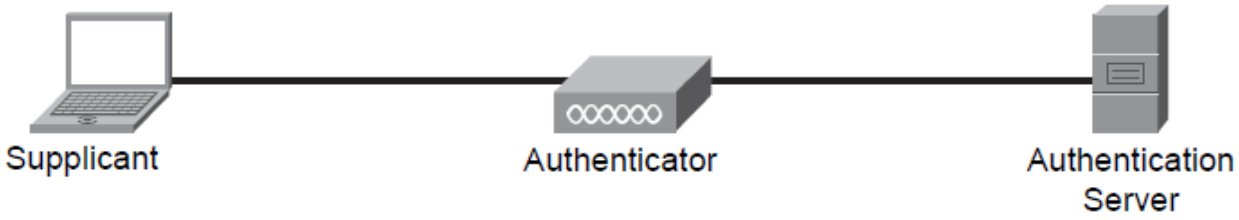
همچنین می توان از Self-Signed Certificate استفاده کرد . لذا باید ابتدا certificate را به certificate store خود ذخیره کنیم ، سپس certificate را تائید نماییم .

این Certificate ها در 802.1x authentication مورد استفاده قرار می گیرند .

این Certificate ها همچنین می توانند برای LWAPP control data مورد استفاده قرار بگیرند .

802.1x و نحوه ی عملکرد آن :

802.1x یک استاندارد تایید صلاحت است که توسط IEEE تعریف شده است . 802.1x یک روش باز یا بسته کردن یک پورت بر اساس یک موقعیت خاص است . موقعیت خاص ، هنگامیست که یک AAA server یک کاربر را شناسایی و تایید کند . 802.1x یک framework است که از انواع روش های EAP برای ارتباطاتش بهره می جوید . در گذشته ، 802.1x در سمت سیمی شبکه به کار می رفت .



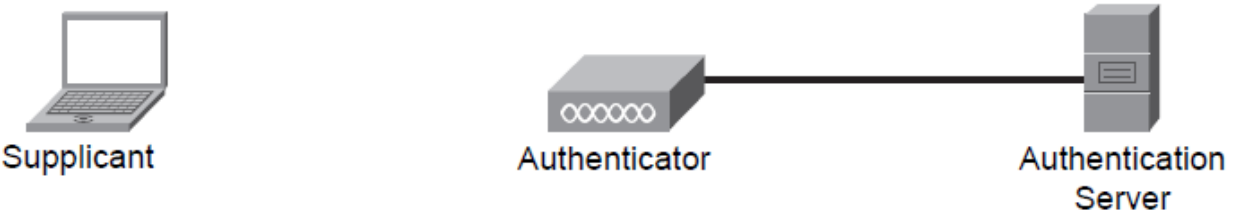
دستگاهی که می خواهد به شبکه ی سیمی بپیوندد ، supplicant (درخواست کننده) نام دارد .

Supplicant ، دستگاهیست که می تواند از یک روش EAP برای ثابت کردن اعتبار خود به authentication server استفاده نماید .

Authentication server ، در واقع یک AAA server است که لیستی از کاربران دارد که می تواند supplicant را تایید صلاحیت نماید .

بین supplicant و authentication server یک سوییچ وجود دارد . بین supplicant و authenticator از EAP over LAN استفاده می شود .

اگر این سوییچ را با یک AP عوض کنیم :



در این حالت ، بین supplicant و authenticator از EAP over WLAN استفاده می گردد .

فرآیند authentication به این ترتیب است :

۱. ابتدا open authentication بین کاربر و AP رخ می دهد .
۲. پس از انجام open authentication ، هرکدام از طرفین می توانند فرآیند 802.1x را آغاز نمایند .
۳. تمامی ارتباطات بین supplicant به AP و از AP به RADIUS و برعکس انجام می شود تا در نهایت RADIUS یک WEP key به AP و از آنجا به supplicant می دهد تا بر اساس آن ترافیک را encrypt کند . این فرآیند 802.1x نام دارد .

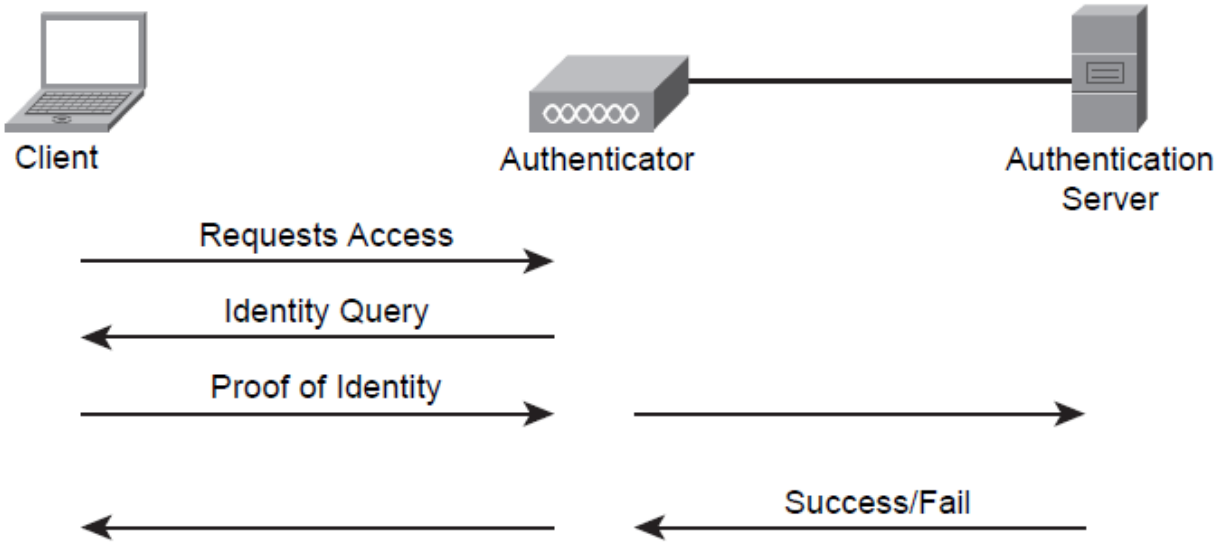
AP خودش WEP key جلسه را نگه می دارد تا بتواند ترافیک بین AP و کاربر را encrypt و امن نماید .

فرآیند EAP :

802.1x چیزی بیش از یک framework نیست . 802.1x فقط مشخص می کند که اعتبار نامه ی کاربران ارسال شده یا خیر ، اما چگونگی ارسال آن را مشخص نمی سازد .

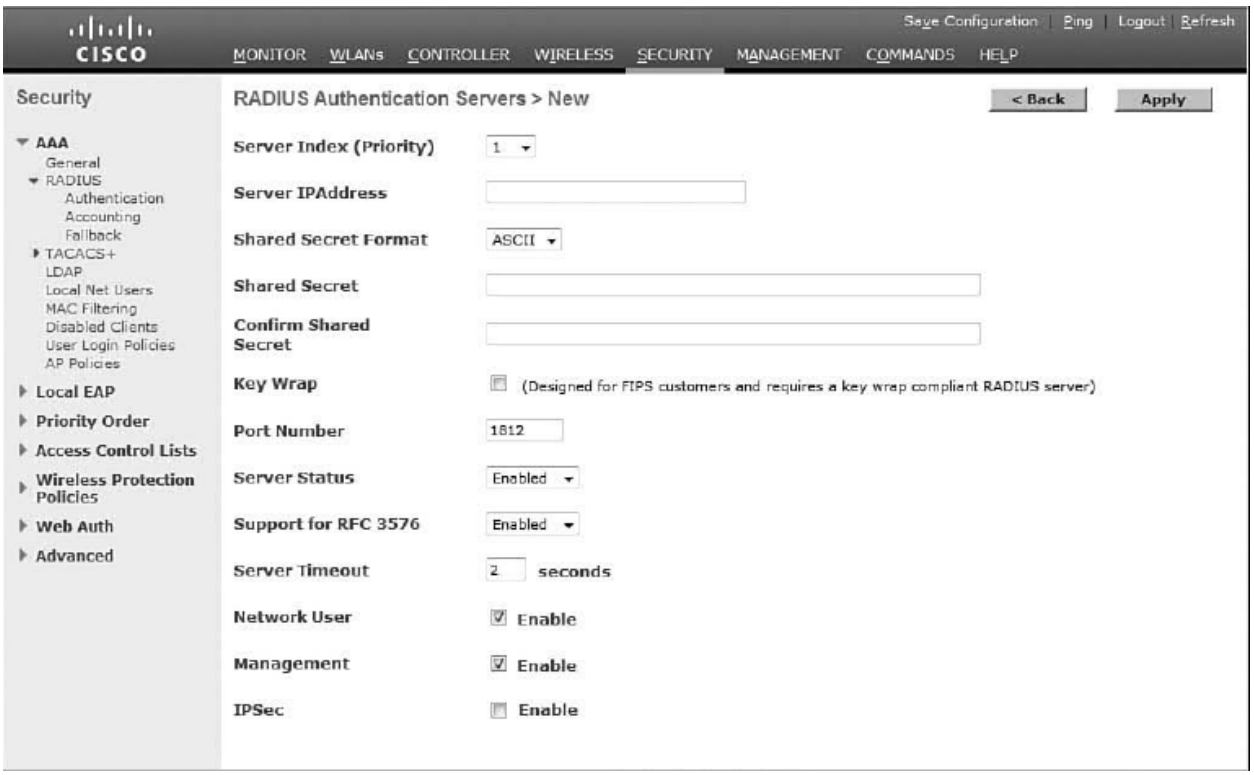
EAP نحوه و چگونگی ارسال اعتبار نامه ی کاربران را کنترل می کند و در این حالت فرقی ندارد که از چه نوع EAP استفاده می کنید ؛ همگی از یک روش استفاده می نمایند .

در EAP کاربر یک تقاضا به AP ارسال می کند . AP از او تقاضای نشان دادن مدارک شناسایی می کند . کاربر Identity خود را به AP می دهد . AP آن را به authentication server ارسال نموده و جواب نهایی را به کاربر باز می گرداند .

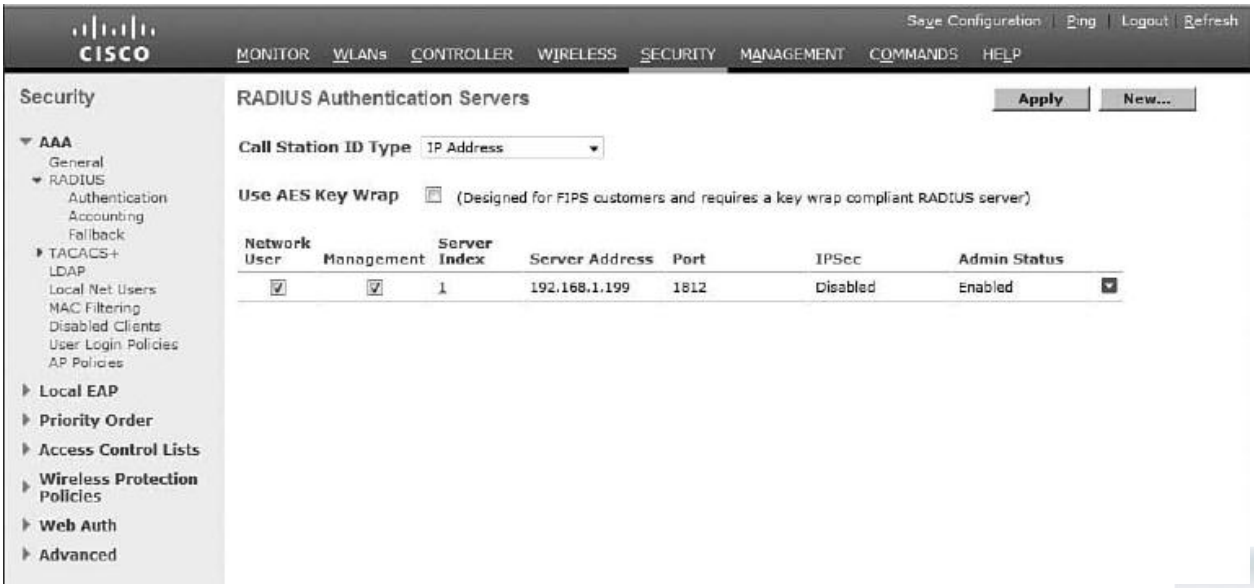


Authentication Server :

این سرور می تواند external باشد ، یا Cisco Secure Access Control Server باشد (ACS) ، یا اینکه یک RADIUS server رایگان باشد ؛ در اینصورت شما باید محل RADIUS server را در اینترفیس کنترلر تعریف نمایید . SECURITY / RADIUS Authentication Servers / New



برای دیدن سرورهای لیست شده در صفحه ی RADIUS Authentication Servers :

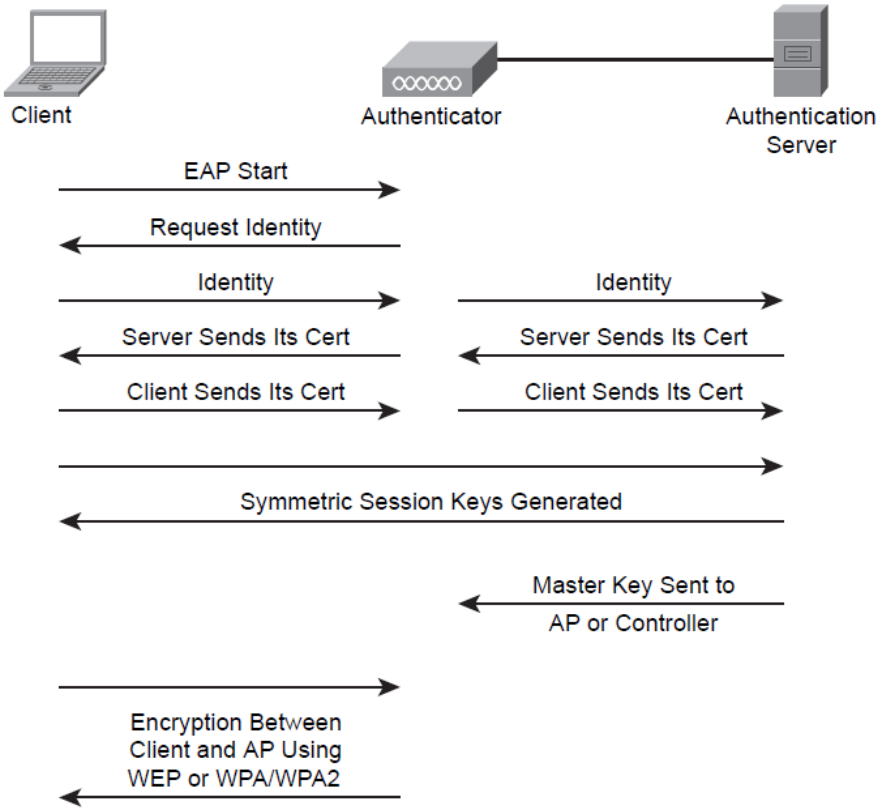


EAP-TLS :

Extensible Authentication Protocol-Transport Layer Security یک روش EAP معمول برای شبکه های وایرلس است . در EAP-TLS باید یک certificate هم روی suplicant و هم روی authentication server نصب شود ؛ به همین علت این روش یکی از امن ترین روش های موجود ست . البته این روش overhead زیادی دارد ، لذا توصیه می شود از EAP-FAST استفاده شود که امنیت آن کمی کمتر است ، اما بسیار سریعتر است .

نکته : ارتباطات EAP-TLS تقریبا شبیه به SSL encryption است ، هرچند TLS نسبت به SSL ارجحیت دارد .

نکته : EAP-TLS یک encrypted Tunnel ایجاد می کند تا certificate کاربران درون آن ارسال گردد .



نکته : در EAP ، کاربر certificate خود را به server می داد و Server آن را تایید می نمود . اما در EAP-TLS پس از این مرحله ، هردو certificate های خود را رد و بدل می کنند تا عملیات شناسایی کامل شود .

نکته : در روش های قبل دیدیم که از public/private key استفاده می شد ؛ آن روش ها هرچند مناسب بودند ، اما خیلی CPU extensive بودند و شمان زیادی نیز می برد ؛ لذا از EAP-TLS استفاده می کنیم .

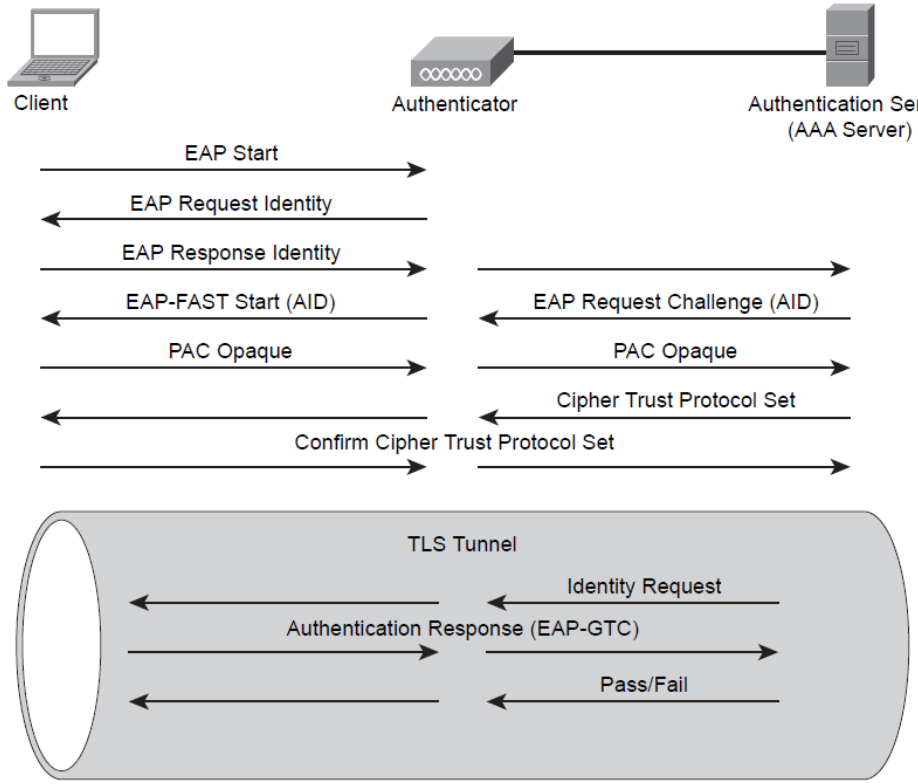
نکته : Symmetric Session Key یک روش برای encrypt کردن داده هاست که یک تونل بین supplicant و authentication server می سازد . در این مسیر می توان از WEP یا WPA/WPA2 استفاده کرد . اگر از WPA2 استفاده کنیم ، server یک master key به authenticator می دهد که در نهایت مسیر بین کاربر و authenticator را امن می کند .

EAP-FAST :

Extensible Authentication Protocol – Flexible Authentication via Secure Tunnel توسط سیسکو ارتقا داده شده و هدف آن ، برطرف کردن ضعف های موجود در LEAP بوده است . EAP-FAST از PKI استفاده نمی کند ؛ در عوض از یک shared secret key بسیار قدرتمند به نام PAC استفاده می کند که روی هر کاربر یکتاست (Protected Access Credential).

EAP-FAST در سه فاز رخ می دهد :

- فاز صفر : PAC تهیه می شود .
- فاز یک : پس از اینکه کاربر و AAA server یکدیگر را با استفاده از PAC شناسایی و authenticate کردند ، یک تونل TLS بین آنها ایجاد می شود .
- فاز دو : با استفاده از یک روش دیگر EAP ، و با استفاده از password یا generic token cards ، کاربر به AAA server شناسانده و authenticate می شود .



نکته : PAC Opaque یک فیلد با طول متغیر است که می تواند توسط authentication server تفسیر گردد . PAC Opaque برای تایید اعتبار کاربران مورد استفاده قرار می گیرد .

نکته : authentication server در واقع PAC Opaque را با استفاده از یک master key (که برای استخراج PAC key مورد استفاده قرار می گرفت) ، encrypt می کند .

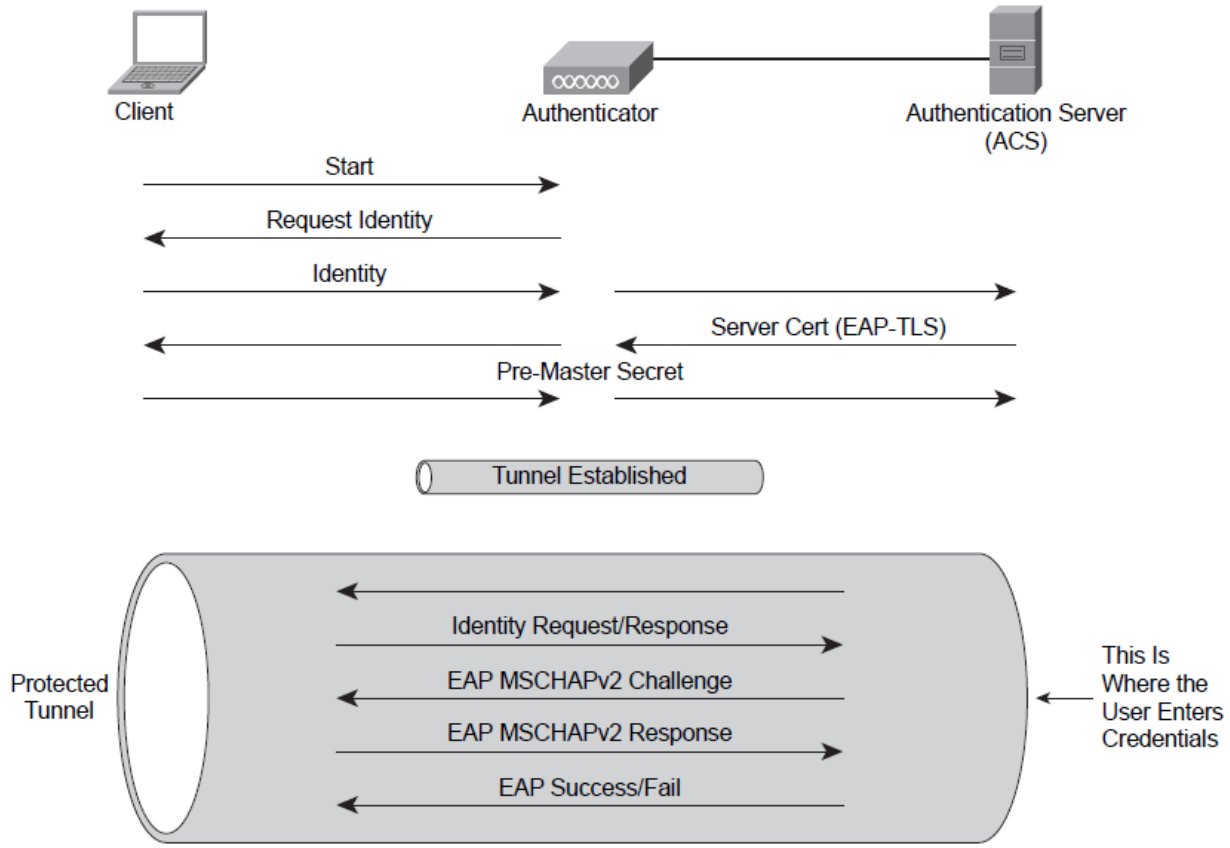
نکته : کاربر بر اساس AID ، یک PAC به سرور ارسال می کند و همچنین یک PAC Opaque نیز می فرستد که برای شناسایی و تایید مدارک کاربر توسط Server به کار می رود .

PEAP :

در Protected EAP ، از certificate فقط در سمت server استفاده می شود که برای ساختن تونل به کار می رود ، سپس authentication واقعی درون این تونل انجام می شود .

PEAP برای authenticate کردن کاربر درون یک encrypted tunnel ، از یکی از این دو روش استفاده می کند :

1- MS-CHAPv2 : Microsoft Challenge Handshake Authentication Protocol version 2
2- GTC : Generic Token Card



LEAP :

Lightweight EAP بصورت افتخاری اینجا مورد بحث قرار می گیرد ؛ زیرا یک روش سیسکویی EAP است که همچنان در شبکه های 802.11b دیده می شود .

LEAP نسبت به حملات offline بسیار حساس و آسیب پذیر است و در صورت امکان ، باید از کاربرد آن خودداری نمایید .

LEAP از یک الگوریتم اختصاصی برای ساختن session key اولیه استفاده می نماید .

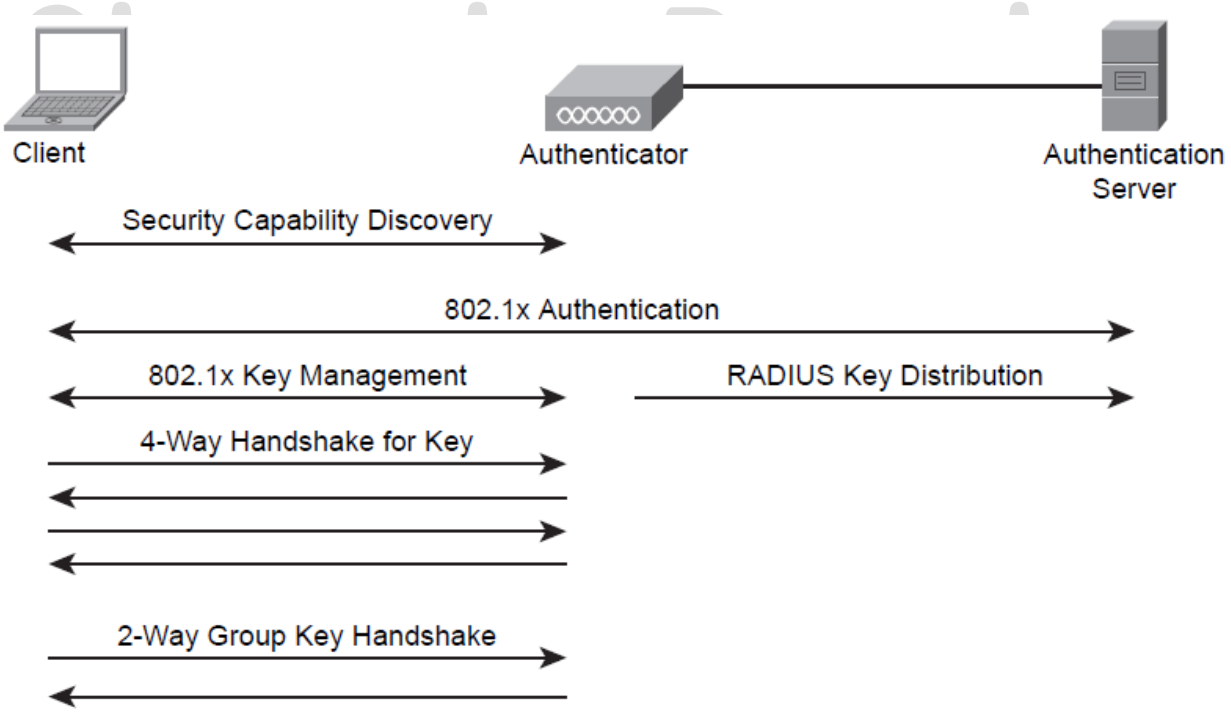
WPA :

WEP از RC4 استفاده می کرد که خیلی ضعیف بود و بهتر بود که از AES encryption استفاده نماید ، اما این کار نیاز به ارتقاء سخت افزاری تجهیزات داشت ؛ لذا WPA بوجود آمد که هرچند همچنان از RC4 استفاده می کند ، اما IV بزرگتری نسبت به WEP برخوردار است که این امر باعث می شود (بدون نیاز به سخت افزار جدید) ، حدس زدن key ها نسبت به WEP خیلی سخت تر شود . WPA همچنین از پروتکل TKIP استفاده می نماید تا بصورت اتوماتیک مرتبا key ها را تغییر دهد .

WPA دو حالت authentication را پیشنهاد می کند :

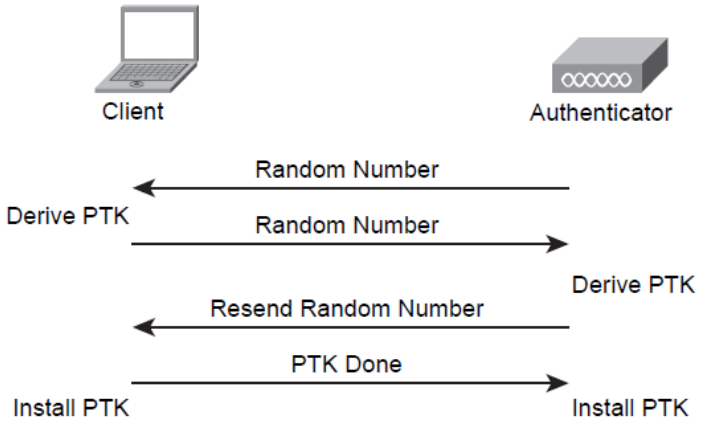
- Enterprise mode : در این حالت ، نیاز به یک authentication server داریم .
- Personal mode : این حالت که از حالت قبلی ضعیف تر است ، از preshared key استفاده می شود .

فرآیند WPA authentication بدین شکل می باشد :



نکته : AP و کاربر یک PMK یا Pairwise Master Key یکسان دارند که در طول session باقی می ماند .

فرآیند WPA Four-Way Handshake به این ترتیب است :



AP یک عدد تصادفی تولید کرده و به کاربر ارسال می نماید .

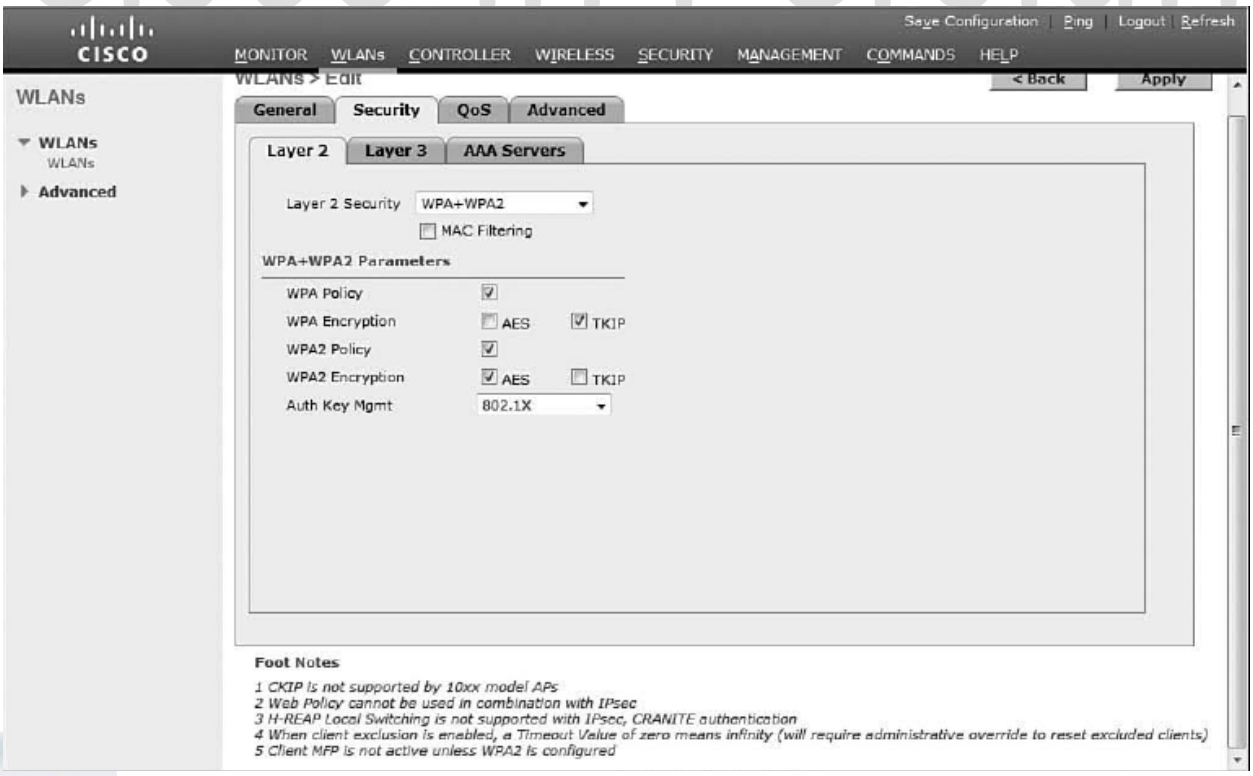
کاربر از یک passphrase استفاده می نماید تا از این عدد تصادفی ، یک key بدست آورد تا ترافیک را به سمت AP خودش encrypt نماید .

کاربر هر یک عدد تصادفی را همراه با MIC (برای اطمینان از دستکاری نشدن داده ها) به AP می فرستد و AP از روی آن ، یک key برای encrypt کردن unicast data به سمت کاربر استفاده می کند .

AP یک عدد تصادفی می فرستد که با key بدست آمده encrypt شده است .

در نهایت تایید می شود که PTK در هر دو طرف قرار گرفته است .

برای تنظیم WPA ، به بخش WLANs / Edit رفته ، WPA+WPA2 را انتخاب کنید .



WPA2 :

برای استفاده از WPA2 ، نیاز به سخت افزار جدید داریم ؛ زیرا WPA2 برای استفاده از AES encryption طراحی شده است .

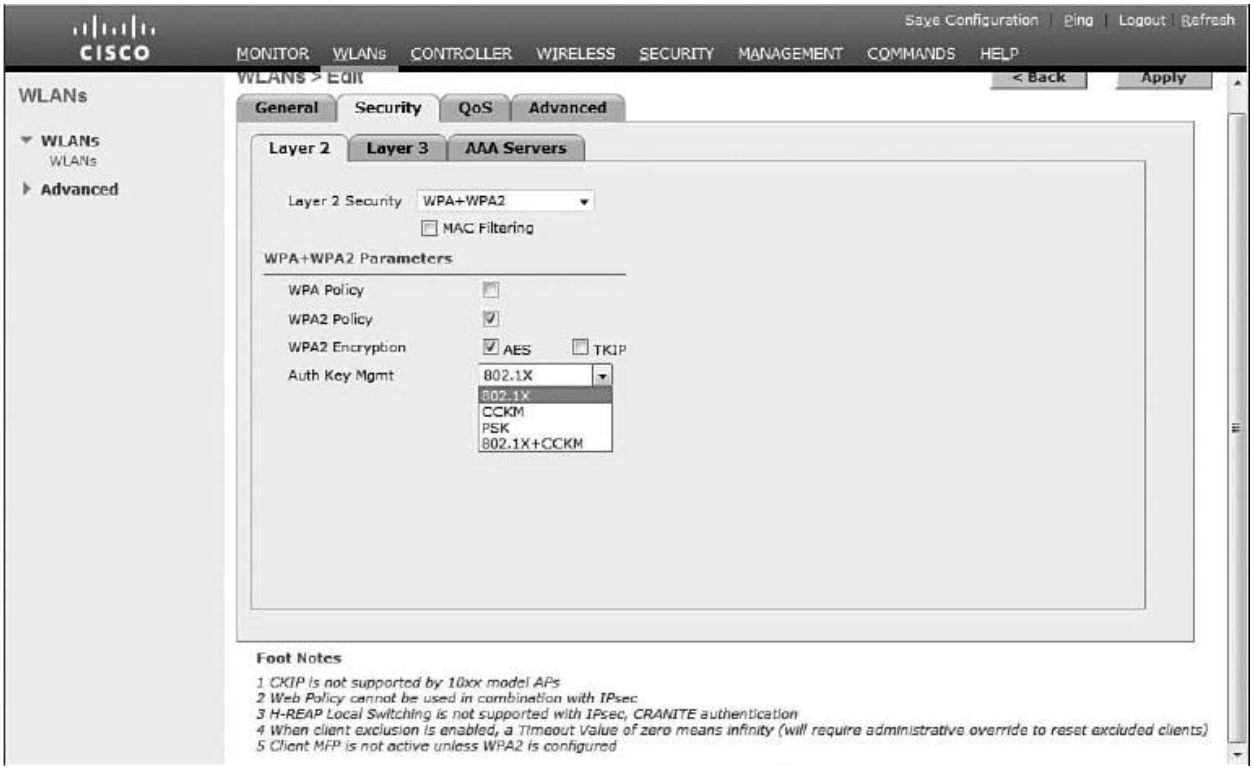
نکته : WPA با استاندارد 802.11a و WPA2 با استاندارد 802.11i کار می کند .

نکته : AES/CCMP همچنان با IV و MIC کار می کند ، ولی IV بعد از هر بلوک رمز (cipher) ، افزایش می یابد .

نکته : WPA ملزم به استفاده از TKIP است ، و استفاده از AES در آن اختیاریست .

نکته : WPA2 ملزم به استفاده از AES است و نمی تواند از TKIP استفاده کند .

برای تنظیم WPA2 به بخش WLANs / Edit بروید و WPA2 Policy را انتخاب نموده ، AES یا TKIP را انتخاب کنید .



فصل هجدهم : مدیریت شبکه های گسترده توسط WCS

- Wireless Control System
- WCS Templates
- Configuration Group
- Auto Provisioning
- نقشه ها و AP ها در WCS
- Planning mode
- Monitoring با استفاده از WCS
- نکته ی خارج از کتاب

هدف از CUWN ایجاد یک مدیریت مرکزی است تا بتوان از کنترلر ، هرگونه تنظیمات اختصاصی را روی همه ی دستگاههای شبکه اعمال و همچنین عملکرد آنها را مدیریت و مانیتور کرد . البته چنانچه شبکه وایرلس گسترده تر شود و نیاز به استفاده از چندین کنترلر باشد ، برای تمام بخش ها از WCS یا Wireless Control System استفاده می شود . همچنین Cisco Wireless Location Appliance می تواند به ما کمک کند تا همه چیز را تحت نظر داشته باشیم و دستگاهها و کاربران را ردیابی کنیم . این فصل خلاصه ایست از نحوه ی نصب و مدیریت WCS و نیز کنترل کنترلر ها و مدیریت AP ها توسط WCS .

Wireless Control System :

WCSیک نرم افزار browser-based است که بوسیله ی آن می توان از طریق یک اینترفیس ، چندین کنترلر را مدیریت نمود (Planning , Design , Management).

WCS مبتنی بر یک سیستم licensing است که می تواند بین ۵۰۰ تا ۲۵۰۰ عدد AP را ساپورت کند .

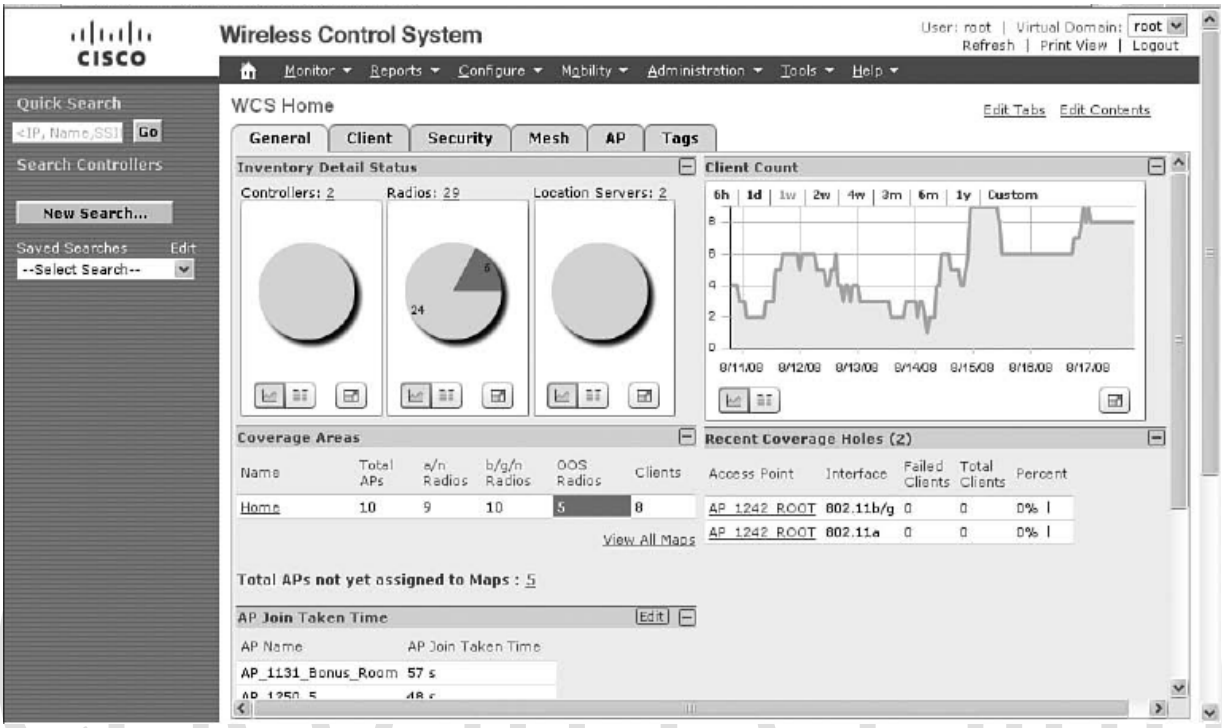
Cisco Wireless Location Appliance از طریق یک اینترفیس WCS قابل دستیابی است و نقشه ی کامل کاربران شبکه را به ما می دهد که کاربردهای فراوانی دارند .

WCS را هم می توان روی windows و هم می توان روی Linux نصب نمود ؛ هرچند برای مصارف گسترده ، Cisco توصیه می کند که از Linux استفاده نمایید .

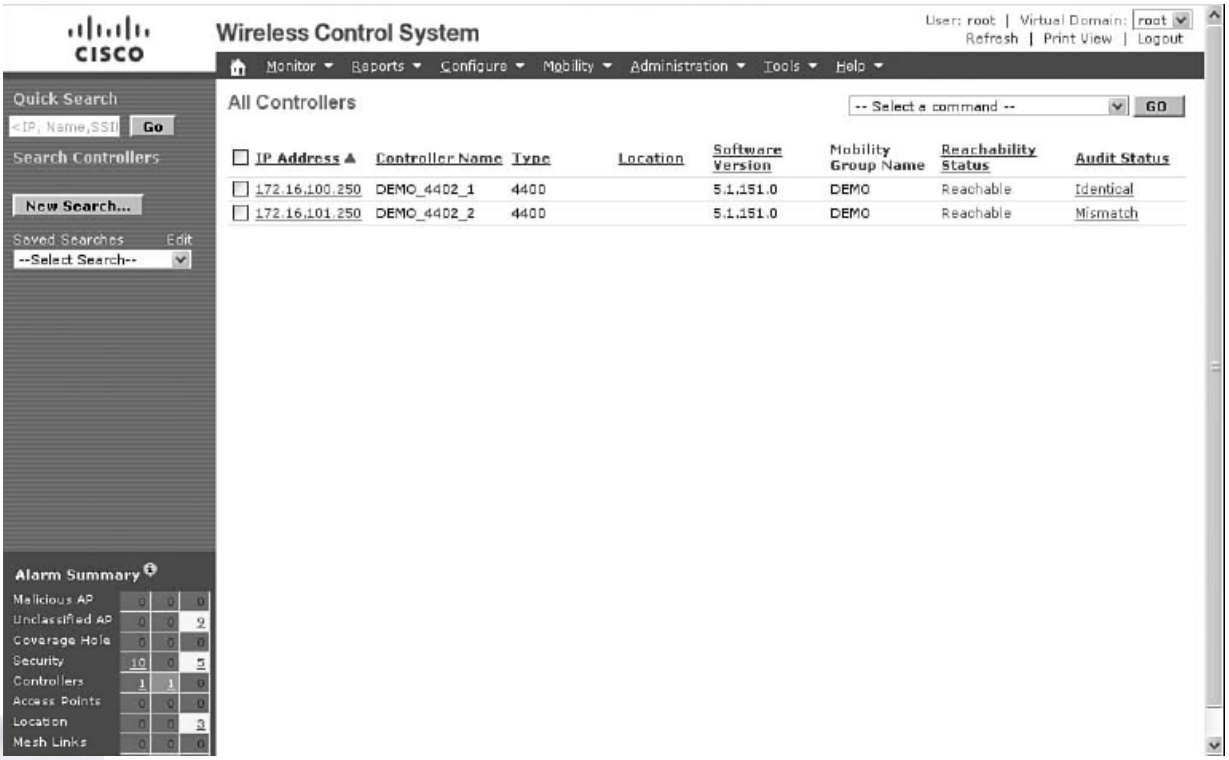
توجه داشته باشید که شما به HTTP پورت ۸۰ و نیز پورت ۴۴۳ نیاز دارید . زیرا WCS در واقع به عنوان یک Apache Web Server عمل می کند ؛ با پورت های ۲۱ برای FTP ، پورت ۶۹ برای TFTP ، و پورت ۱۶۹ برای SNMP traps . در جدول زیر می توانید پورت های WCS را مشاهده بفرمایید .

Port	Use
HTTP: Configurable during install (80 by default)	Web access
HTTPS: Configurable during install (443 by default)	Secure web access
1315	Java
1299	Java
6789	—
8009	Java
8456	Java
8005	—
69	TFTP
21	FTP
162	SNMP traps
8457	—

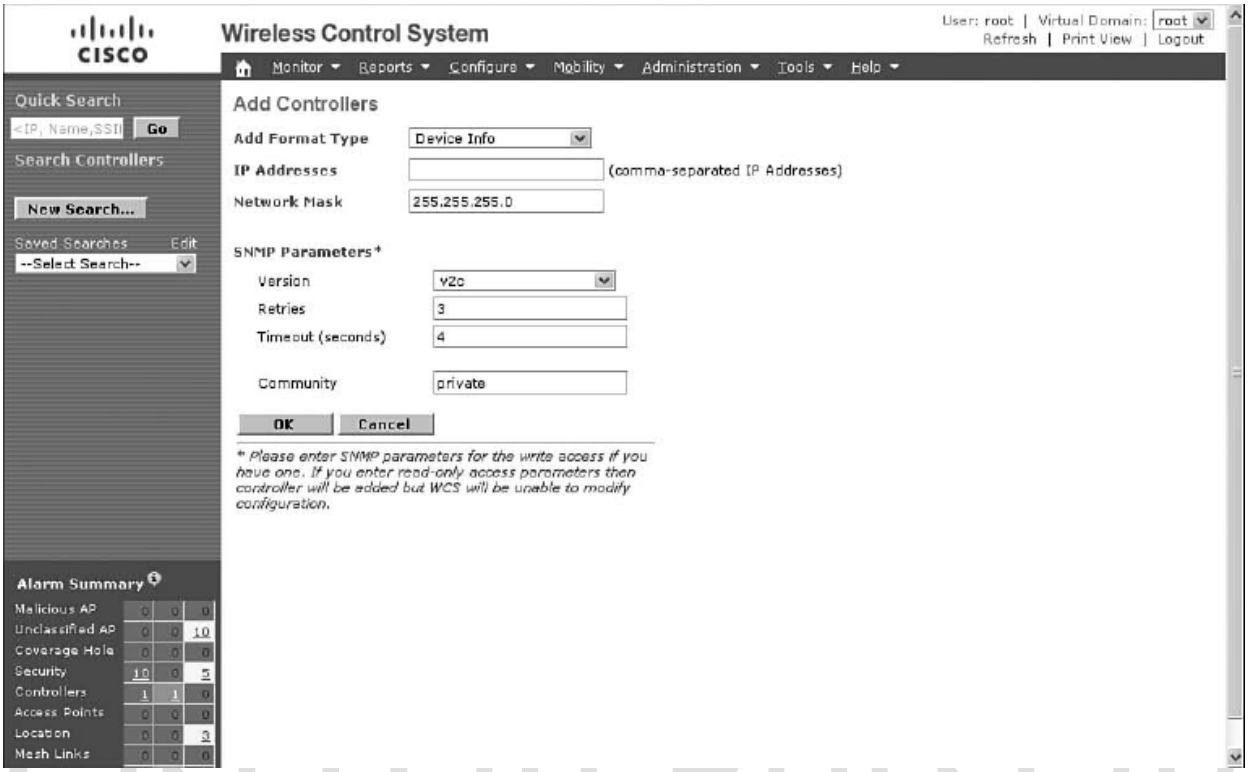
توجه : از آنجا که هم WCS و هم IIS سعی می کنند پورت ۸۰ را امن کنند ، نصب هر دو با هم مشکل ایجاد می کند .
لذا هنگام نصب WCS باید توجه کنید که IIS نصب نشده باشد ، یا اینکه آنرا shut down کنید .
صفحه ی اصلی WCS را WCS Home می نامند .



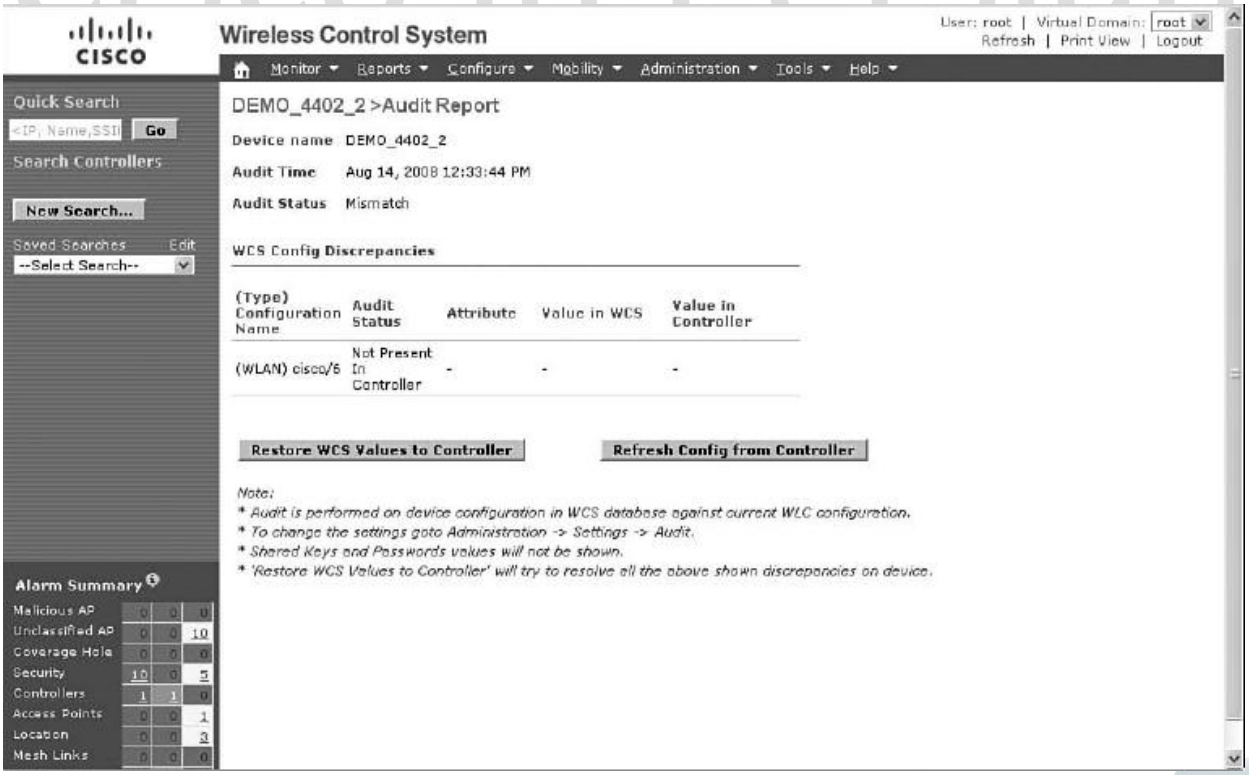
برای اضافه کردن کنترلر ها به WCS ، به زیربخش Configure / Controllers بروید .



در select command ، با انتخاب Add Controller و کلیک روی Go ، می توانید صفحه ی تنظیمات را ببینید .



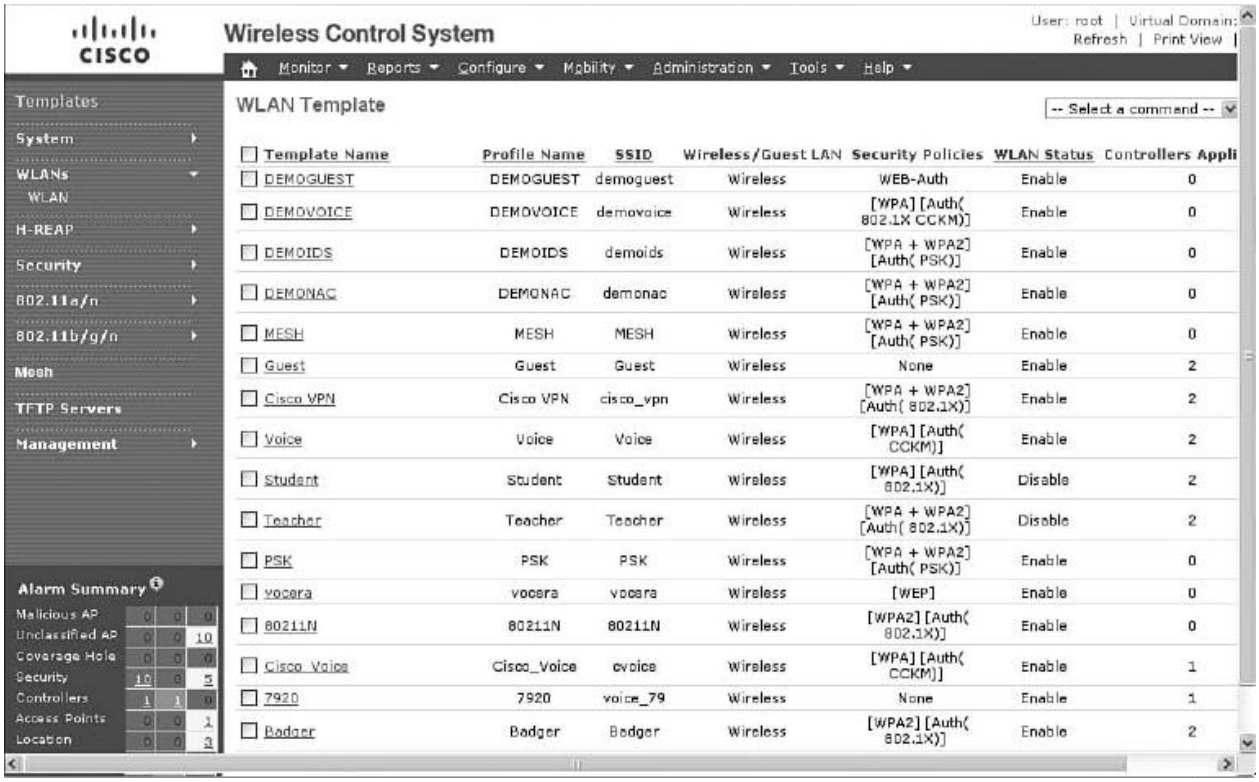
برای اینکه مطمئن شوید تمام تنظیمات ، مناسب هستند : Configure / Controllers / Audit Now / Go



WCS Templates :

استفاده از WCS Templates **به ادمین شبکه اجازه می دهد که تنظیمات را یک بار اجرا نموده و آنها را به چندین دستگاه دیگر اعمال نماید . لذا به راحتی می توان** Template **را** save **نموده و آن را به چندین کنترلر اعمال نمود .**

Configure / Controller Templates / Apply to Controllers

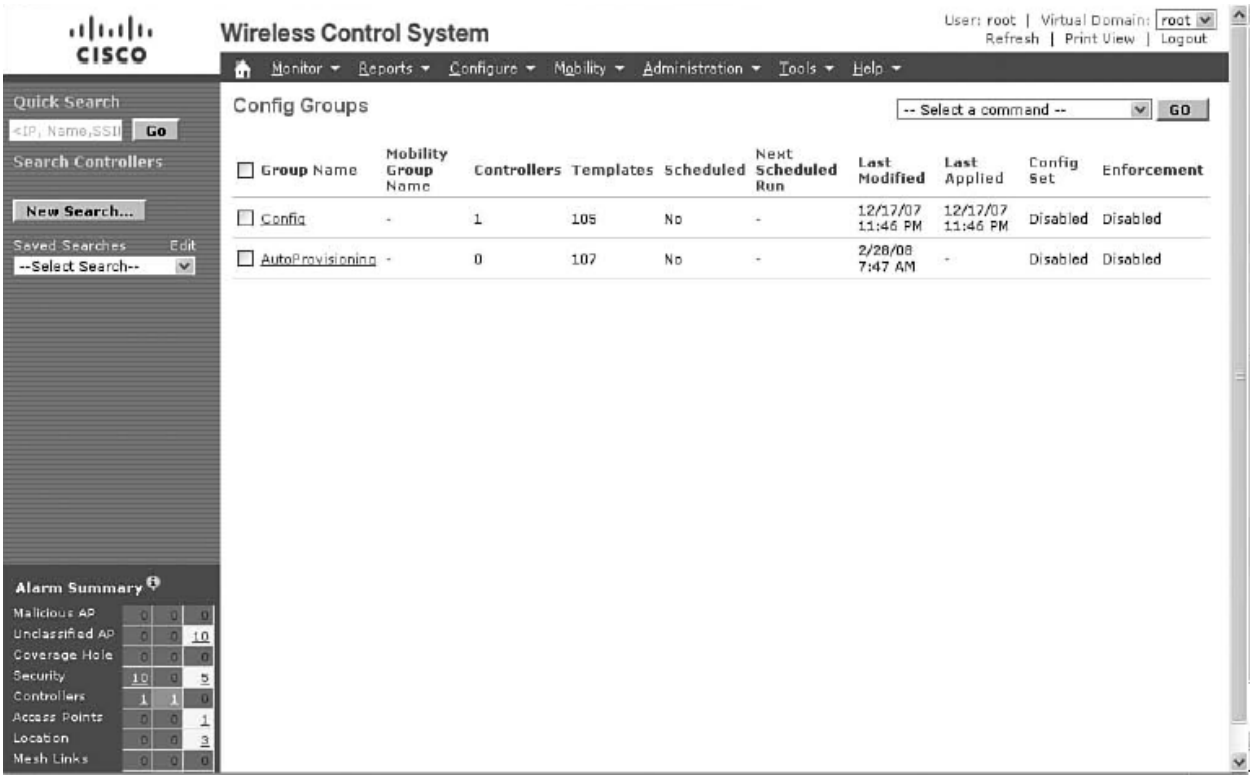


نکته : از آنجا که WCS **تمام شبکه های وایرلس را** track **می کند ، حجم اطلاعات خیلی خیلی زیاد خواهند شد و ما را دچار مشکل می کند ؛ لذا باید از** aggregation **استفاده کنیم . برای تنظیم** aggregation **به این بخش بروید :**

Administration / Settings / Data Management

Configuration Group :

Configuration Group ، راهیست برای اعمال تنظیمات به چندین کنترلر ، بطوریکه انگار در واقع یکی هستند . چنانچه تغییری در تنظیمات ایجاد کنید ، این تغییرات به تمام کنترلر های یک گروه اعمال می شود . شما می توانید Controller Templates را به Configuration Group اعمال نمایید .



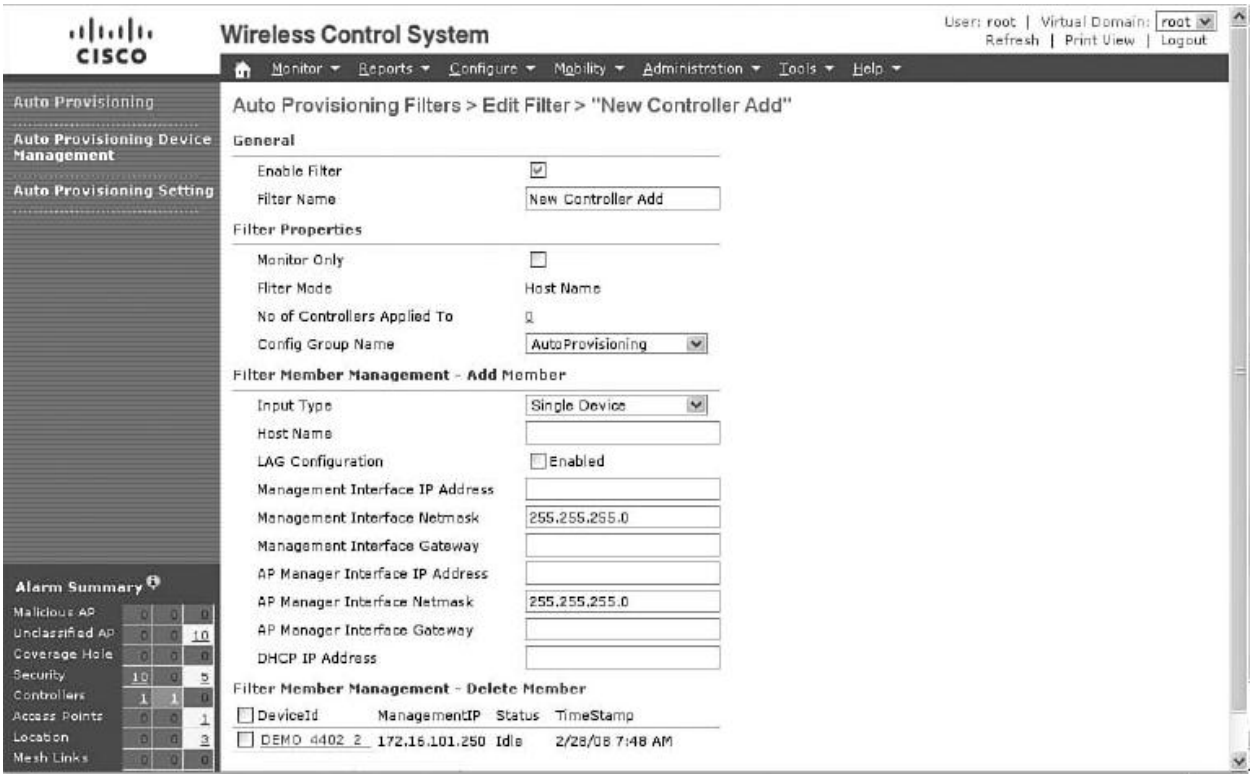
نکته : برای دیدن لیست افرادی که به WCS لاگین کرده اند ، به زیر بخش زیر بروید :

Administration / AAA / Users / Audit Trail

Auto Provisioning :

Auto Provisioning برای ساده تر کردن طراحی و تنظیم شبکه در هنگام وجود بیش از یک کنترلر است .

Configure / Auto Provisioning



ابتدا یک فیلتر بسازید تا مشخص شود که چه دستگاههایی باید Auto Provision شوند .

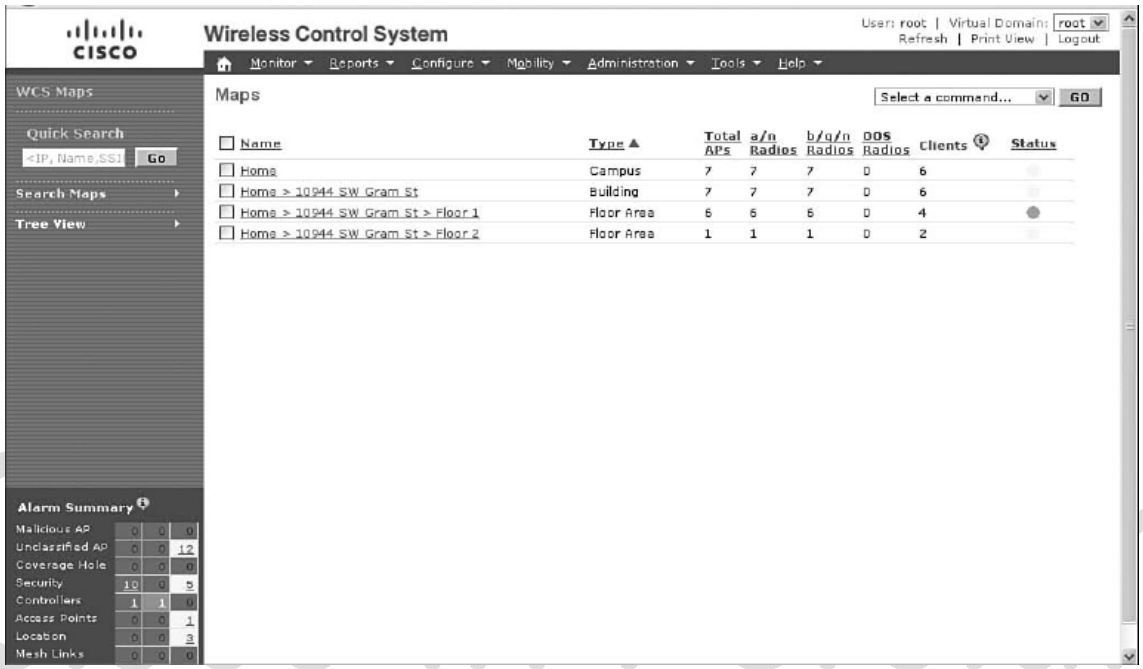
Select a Command / Add Filter

سپس مشخص کنید که چگونه کنترلر باید در شبکه شناسایی شود .

اتفاقی که در Auto Provisioning می افتد اینست که هنگامیکه کنترلر برای اولین بار به شبکه متصل می شود ، هیچ valid configuration ی ندارد ، لذا سعی می کند از DHCP server یک IP بگیرد . DHCP server هم به option 150 ارجاع می دهد ؛ که آدرس IP یک server با فایل configuration کنترلر است . آدرس server ، همان WCS server است .

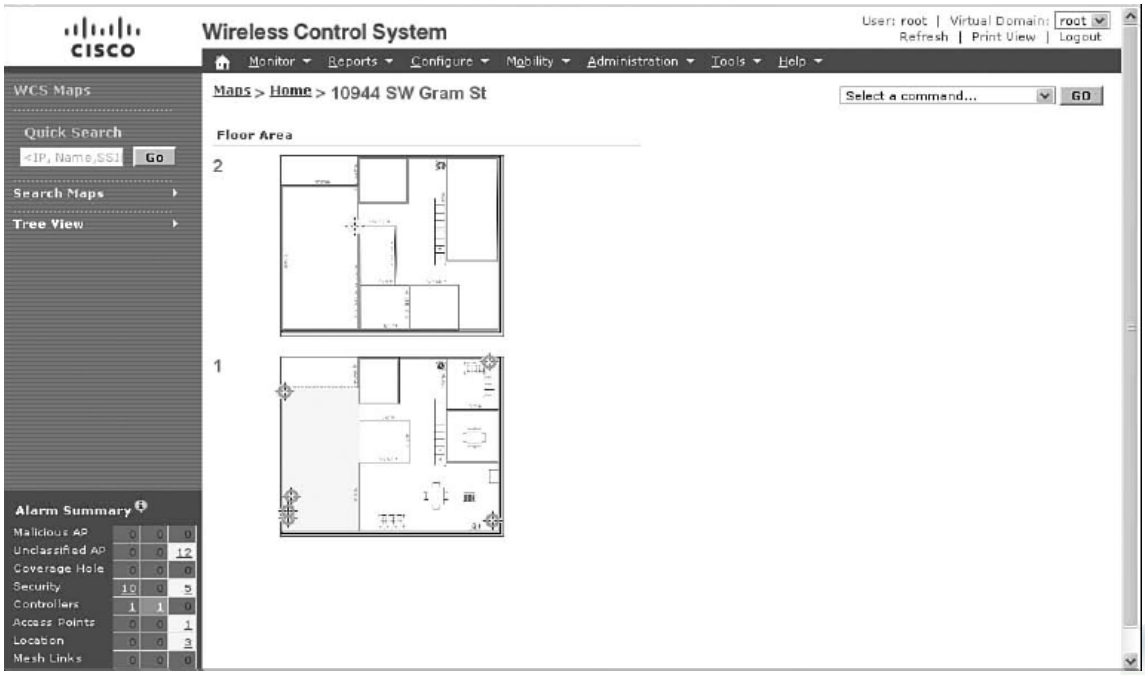
نقشه ها و AP ها در WCS :

Map ها در WCS طراحی شده اند تا یک visual representation از شبکه های وایرلس به ما بدهند . نقشه ها فقط برای مانیتورینگ بعد از نصب شبکه به کار نمی روند ، بلکه برای نصب و طراحی اولیه نیز می توان از آنها استفاده نمود . مثلا از Planning Mode می توان برای فهیدن اینکه در یک فضا چند AP لازم داریم ، و اینکه آنها را باید کجا نصب کنیم استفاده کرد . برای رفتن به این بخش : Monitor / Maps

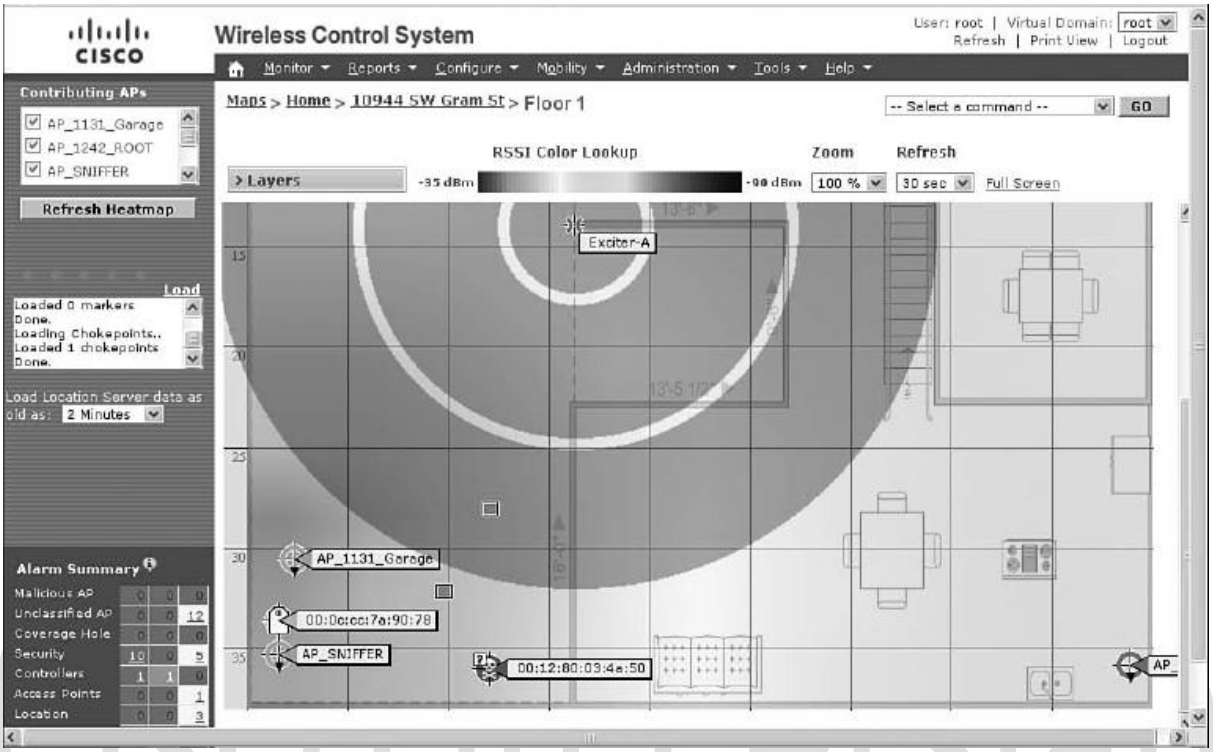


توجه : ابتدا باید ساختمان ها و طبقات را مشخص نمود ، سپس AP ها را اضافه می کنیم .

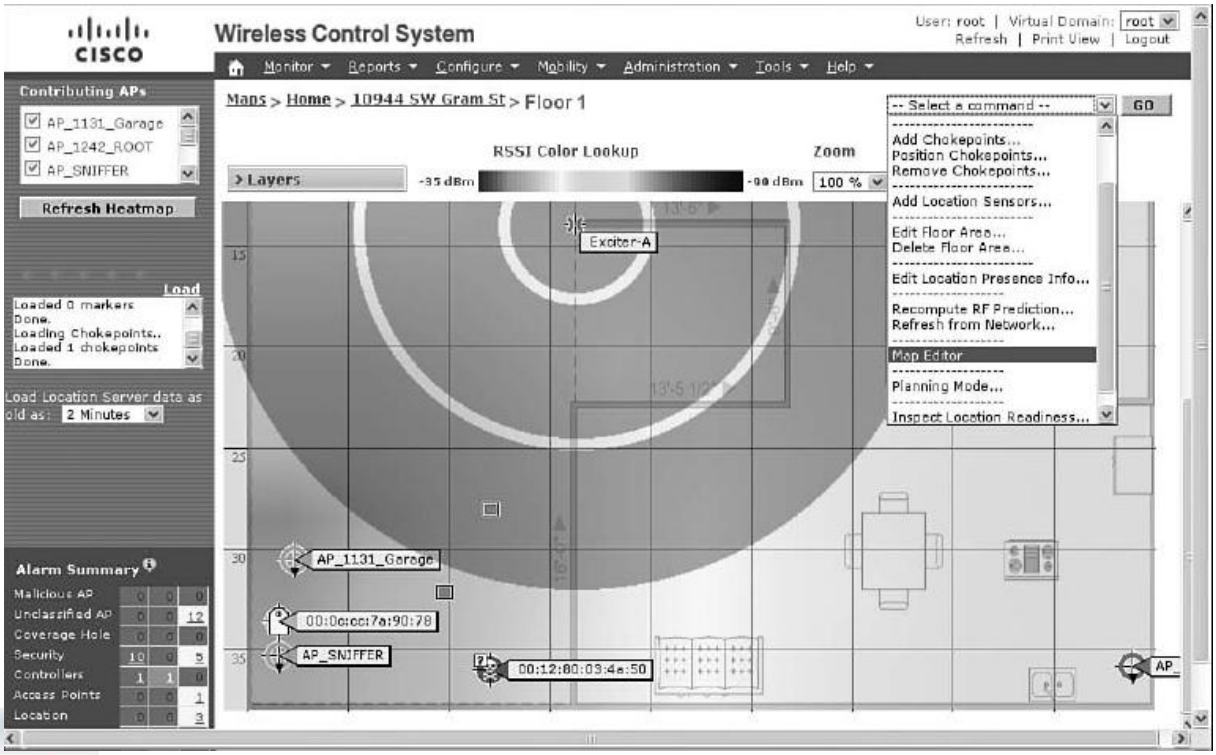
توجه : نمی توان طبقه ای را بزرگتر از هم کف طراحی کرد .



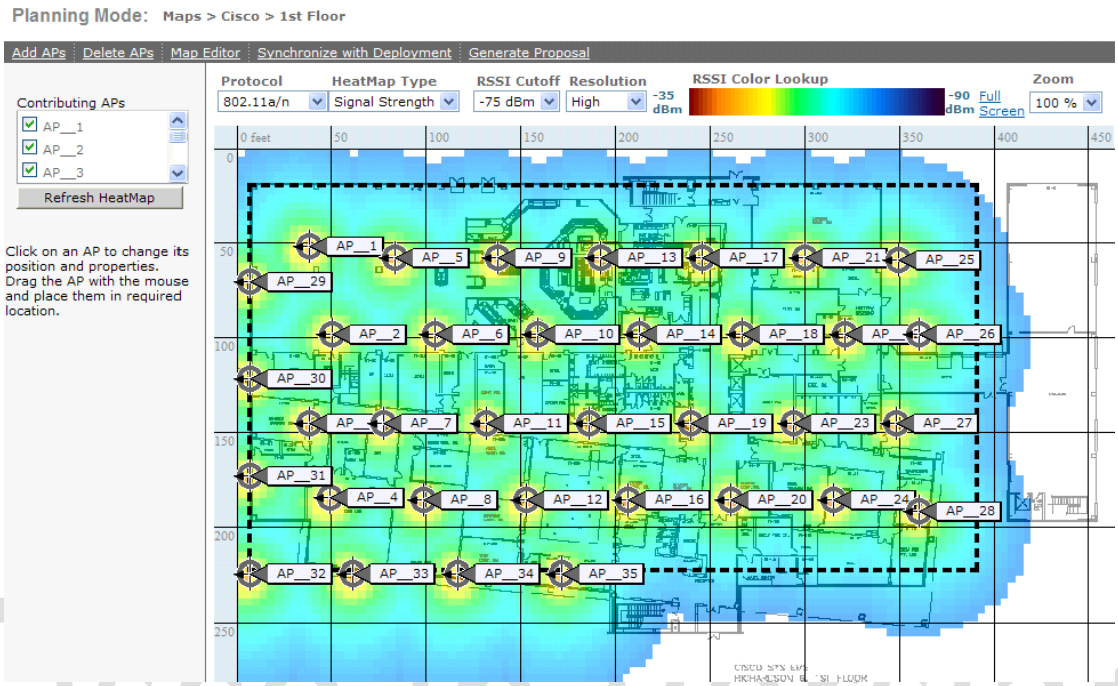
در هر طبقه ، می توان جنس کف ، نوع سقف ، و نیز نوع دیوار ها (بتنی ، کاذب ، پارتیشن ، ...) را مشخص نمود .
نقشه های پیش بینی RF ، نقشه های حرارتی هستند که شامل AP ها ، کاربران و مزاحمان (rogues) می باشند .



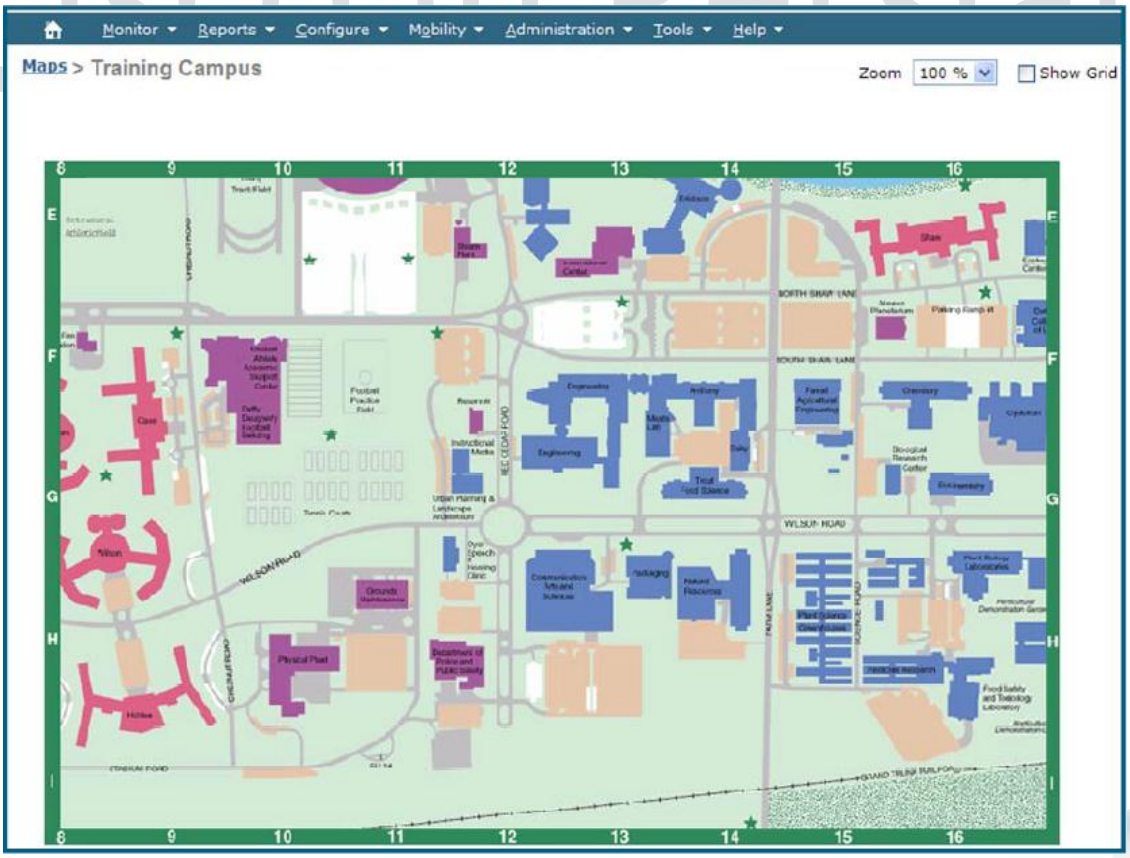
توجه کنید که طراحی و برداشت اولیه (Site Survey) ، در یک زمان مشخص (که آنرا انجام می دهیم) معتبر می باشد و در آینده با تغییر شرایط فیزیکی و محیطی ، تغییر می نماید .



نکته اضافی ۱ : منظور از Heat Map ، نقشه ایست که با استفاده از رنگ ها ، قدرت سیگنال را در هر نقطه مشخص می کند . هدف اصلی استفاده از این نقشه ها ، تخمین دقیق محدوده ی پوشش هر AP است .

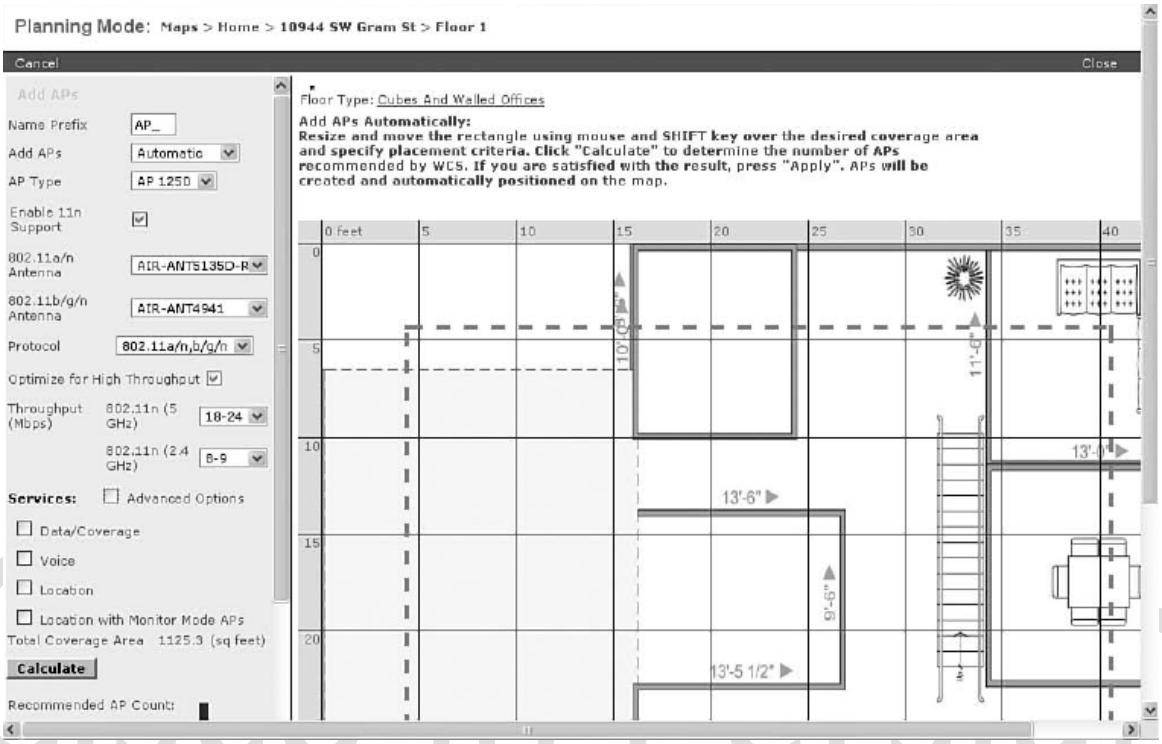


نکته اضافی ۲ : این نقشه ها محدود به ساختمانها نمی شوند ، بلکه می توانند محیط های وسیع را نیز شامل شوند .

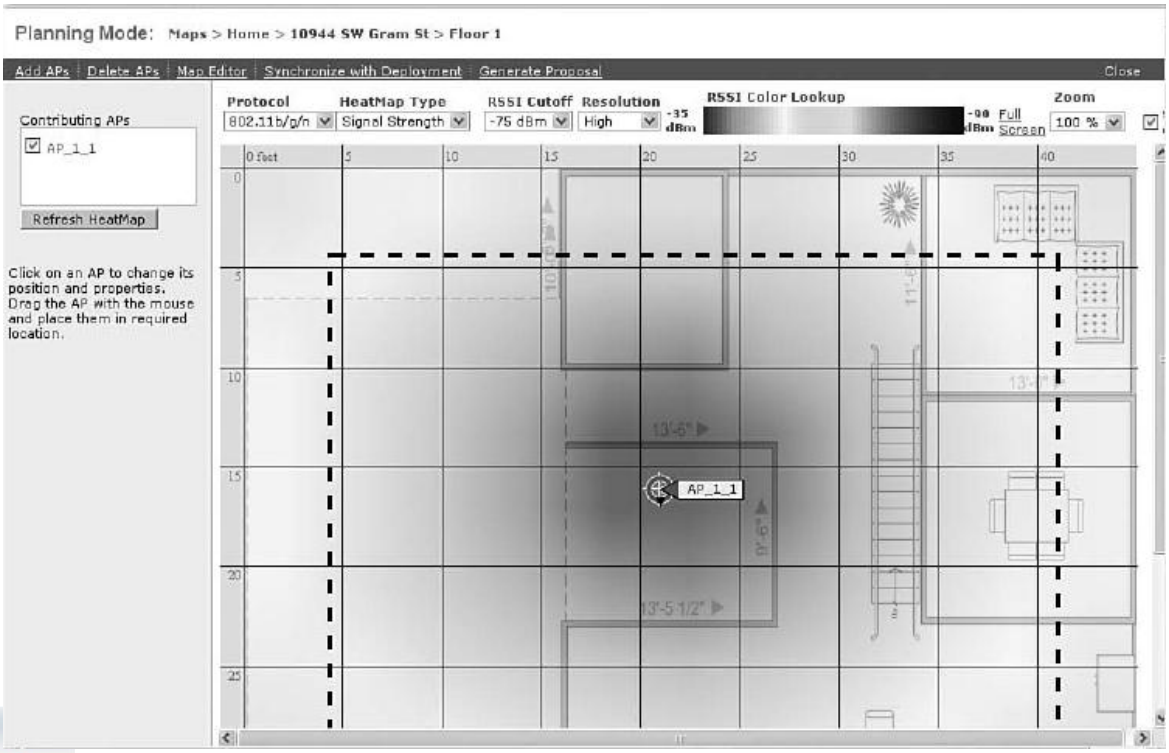


Planning Mode :

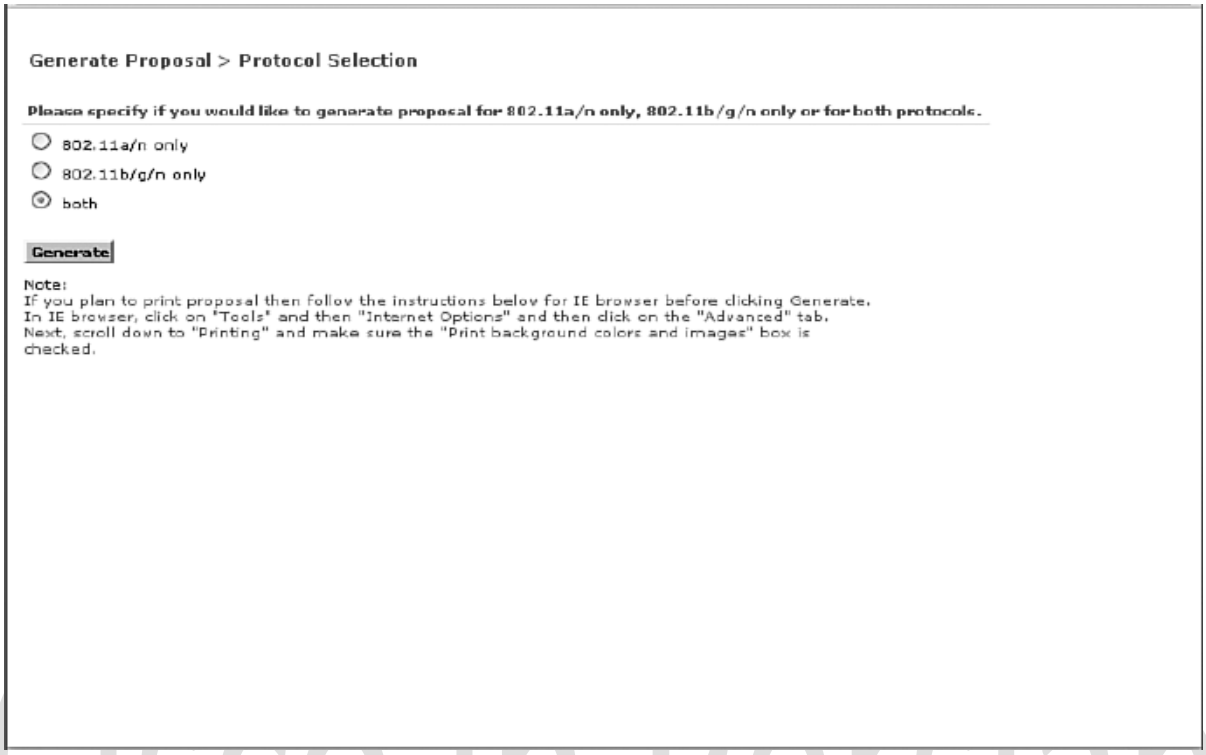
برای اینست که تشخیص دهیم برای یک محدوده ی خاص ، چه تعداد AP نیاز داریم . از منوی سمت چپ ، می توانید تنظیمات مورد نظر خود (که انتظار دارید در شبکه ی خود از آنها استفاده نمایید) را انتخاب کنید .



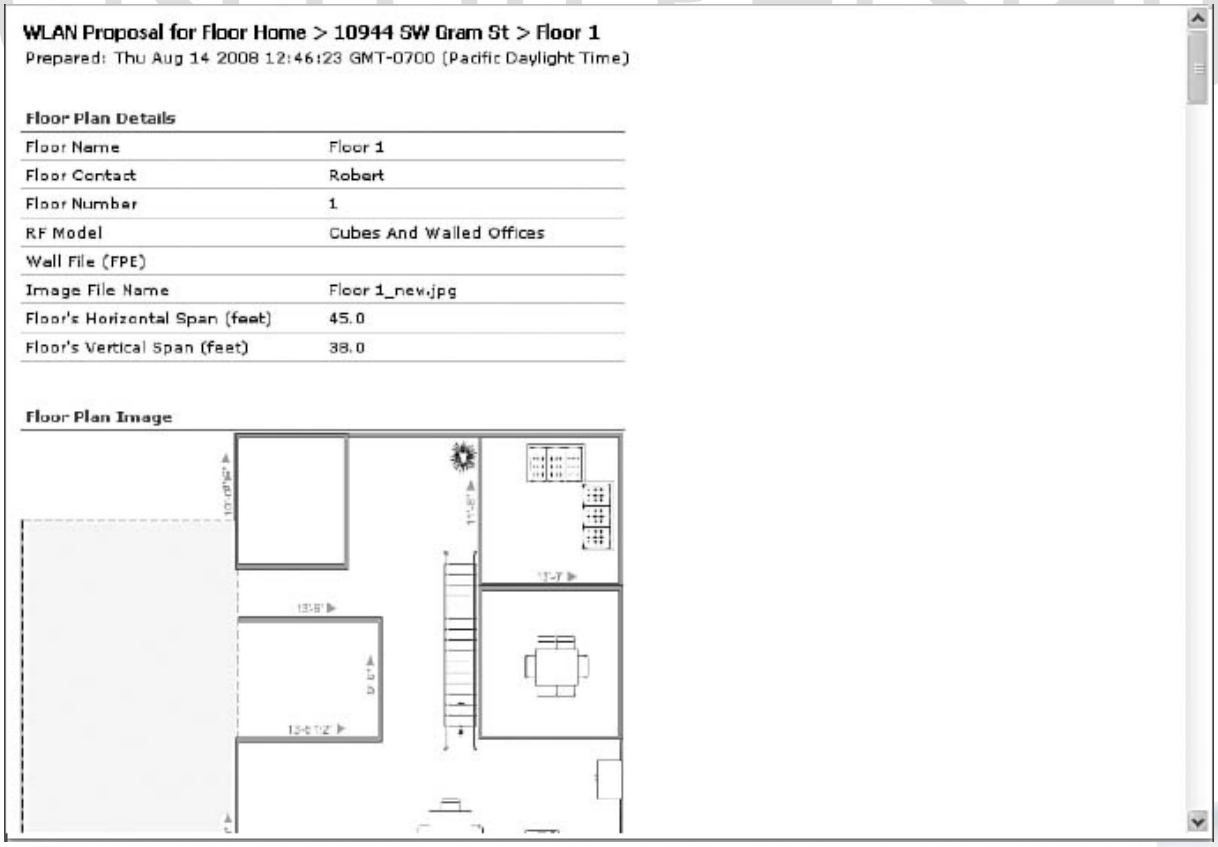
با انتخاب نوع AP و کلیک روی calculate ، نرم افزار AP های فرضی را روی نقشه جایگذاری می کند .



با کلیک روی Generate Proposal ، می توانید یک پروپوزال تهیه کنید .

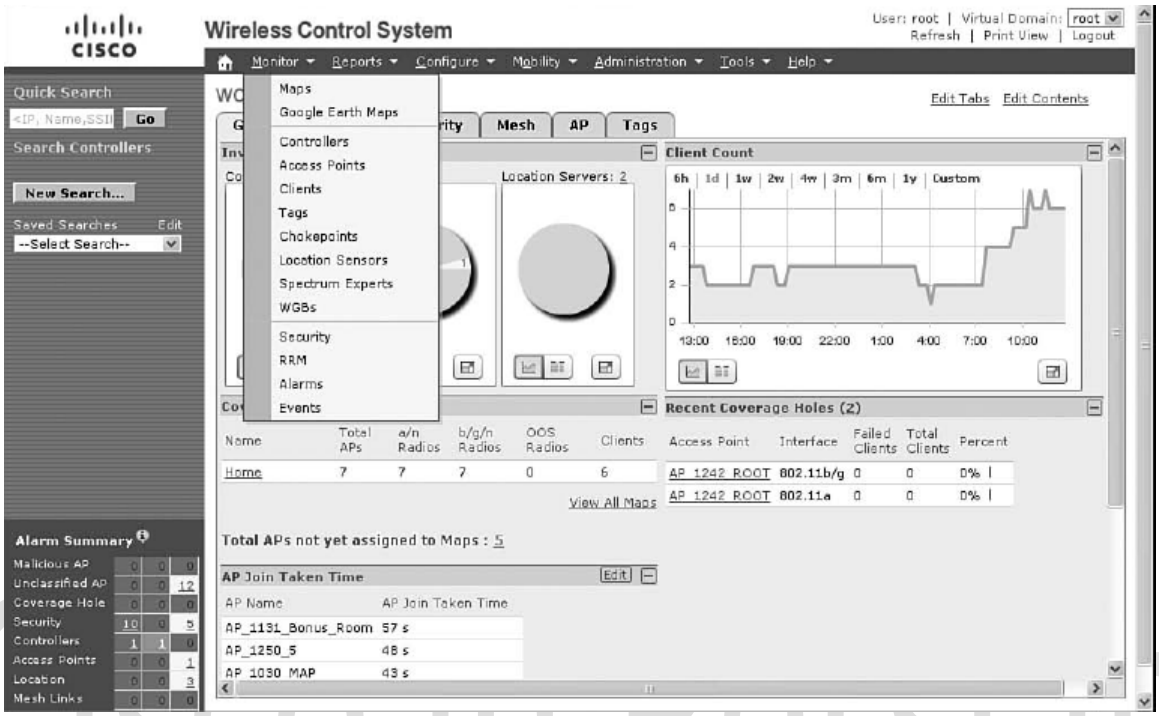


سپس با انتخاب پروتکل مورد نظرتان ، و کلیک روی Generate ، می توانید پروپوزال خود را مشاهده کنید .



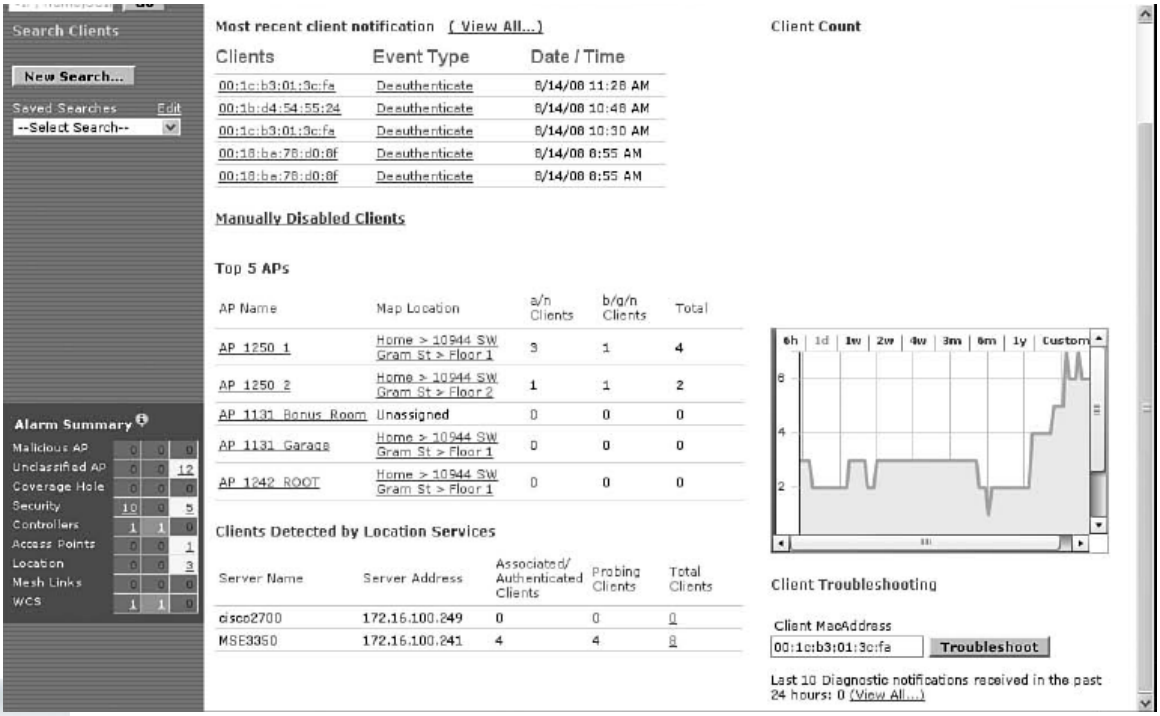
Monitoring با استفاده از WCS :

با استفاده از منوی مانیتور WCS ، می توانید شبکه ی وایرلس و اجزاء آن مانند AP و کنترلر و ... را مانیتور کنید .



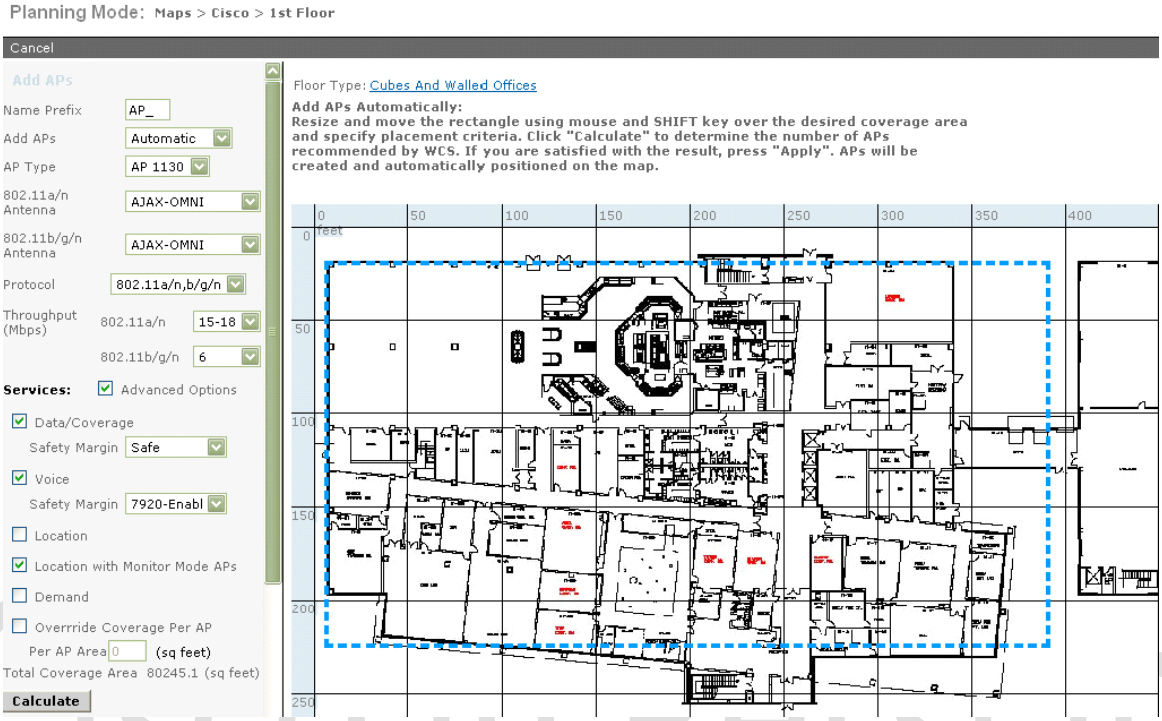
Alarm Summary که در شکل بالا می بینید ، هر ۱۵ ثانیه یک بار refresh می شود .

ویژگی دیگری که وجود دارد ، عیب یابی کاربران است که می توان با وارد کردن آدرس MAC کاربر مورد نظر ، به رفع نقص و نیز تنظیم جزییات آن پرداخت . Monitor / Clients / Client MacAddress / Tshoot



نکته خارج از کتاب :

در CCNP Wireless ، در کورس CUWSS : 642-731 نکات جالبتری در مورد WCS و امکانات آن خواهید خواند .



همچنین در مورد Location-based Deployment خواهید دید که چگونه می توان با استفاده از WLAN Infrastructure ، بطور همزمان هزاران دستگاه را ردیابی نمود .

Example of a single-floor location management deployment

همچنین خواهید دید که چگونه با استفاده از RF Spectrum Analysis Tool ها می توان به بهترین نحو ، برای هر محیطی شبکه ای بهینه طراحی و پیاده سازی نمود .

البته این ابزار ها محدود به سیسکو نمی شوند و کمپانی های مختلف ، ابزار های مختلفی برای طراحی و مدیریت شبکه هایشان در اختیار دارند . همچنین نوع این نرم افزارها نسبت به کاربرد هایشان متفاوت است .

مثلا کمپانی موتورولا ، نرم افزاری به نام Motorola LinkPlanner دارد که چنانچه دو نقطه ی مختلف را روی نرم افزار GoogleEarth مشخص نمایید ، تمامی مشخصات بین این دو نقطه را تهیه نموده و برای هر نوع لینکی که لازم داشته باشید ، پیشنهاد های مختلفی ارائه می دهد ؛ بخصوص اگر از نسخه های Licensed استفاده کنید ، جدیدترین اطلاعات ساختمان ها و موانع جدید را نیز لحاظ خواهد نمود (امکانات این نرم افزار از حوصله ی این کتاب خارج است) .

برای اطلاعات بیشتر : Motorola PTP LinkPlanner User Manual

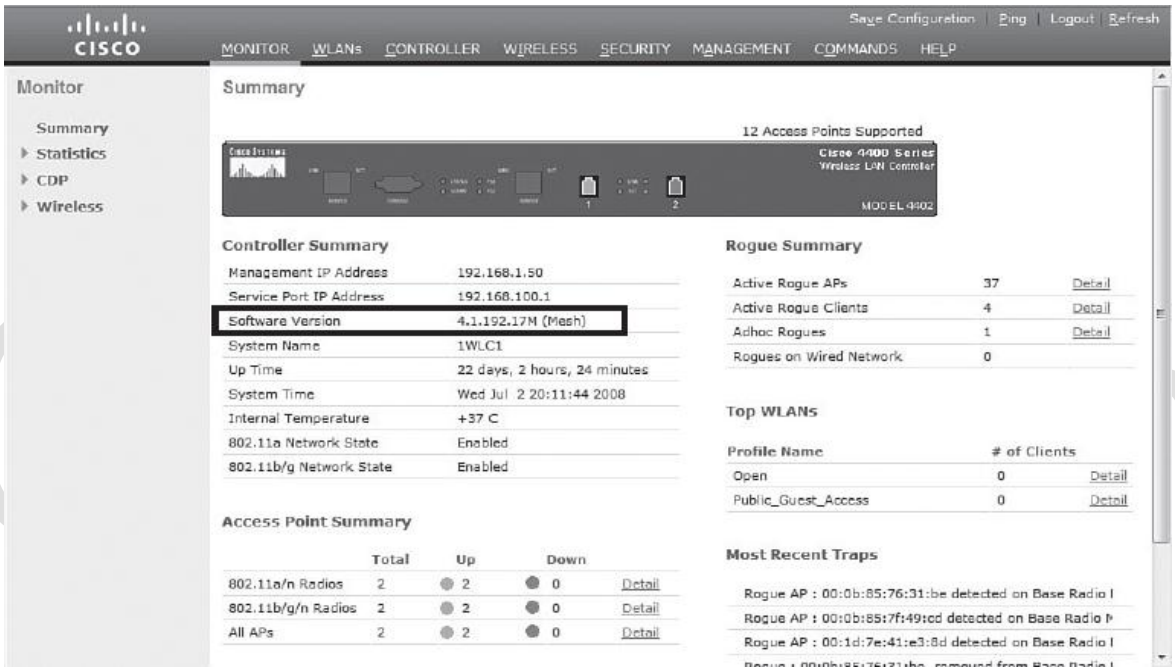
فصل نوزدهم : نگهداری و مدیریت شبکه های وایرلس

- مشخصات تجهیزات وایرلس و جزئیات آنها
- Upgrade با استفاده از WCS
- Reset to Factory Default

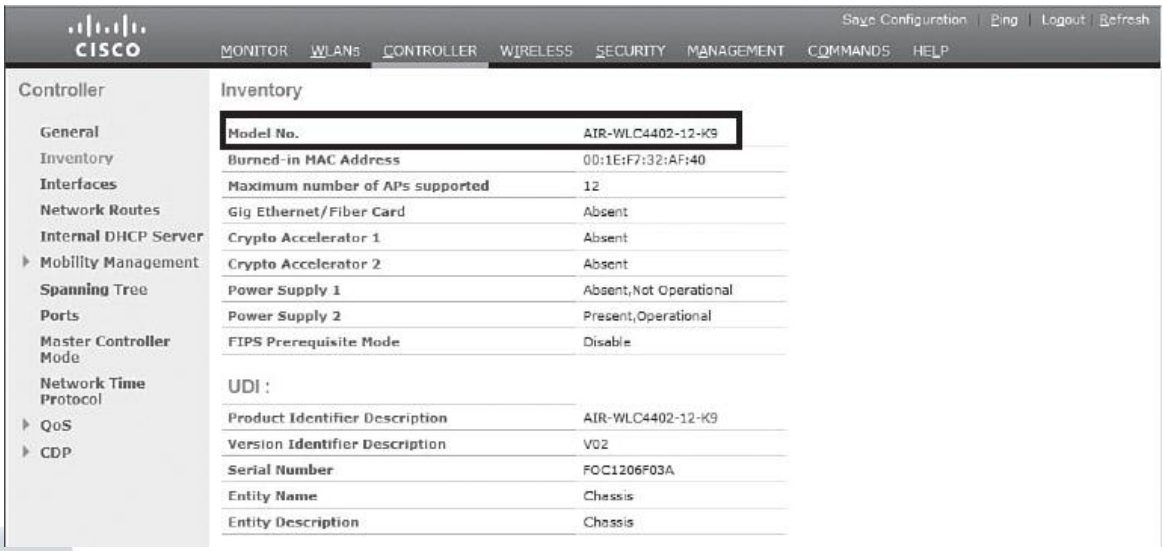
بخشی از مدیریت روزانه ی شبکه ی وایرلس ، شامل کار کردن با image های کنترلر ها و AP ها می باشد . AP ها باید version code یکسانی با کنترلر خود داشته باشند . Cisco پیشنهاد می کند که خود کنترلر ها نیز دارای version code یکسانی باشند . در این فصل با نحوه ی upgrade کردن کنترلر ، AP و WCS ، و نحوه ی مدیریت فایل های configuration آشنا می شوید.

مشخصات تجهیزات wireless و جزئیات آنها :

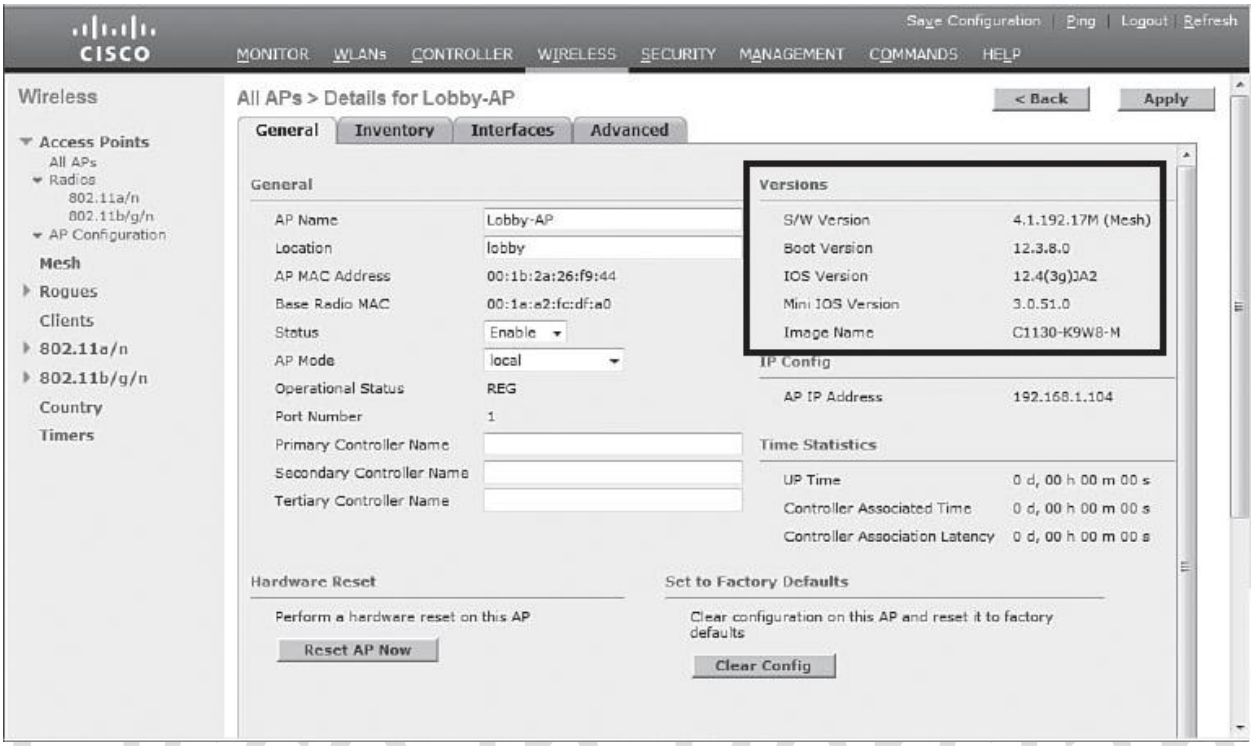
برای دیدن ورژن نرم افزارکنترلر به این بخش بروید : Monitor /Summary



و برای دیدن نوع سخت افزار کنترلر به بخش Controller / Inventory مراجعه کنید .

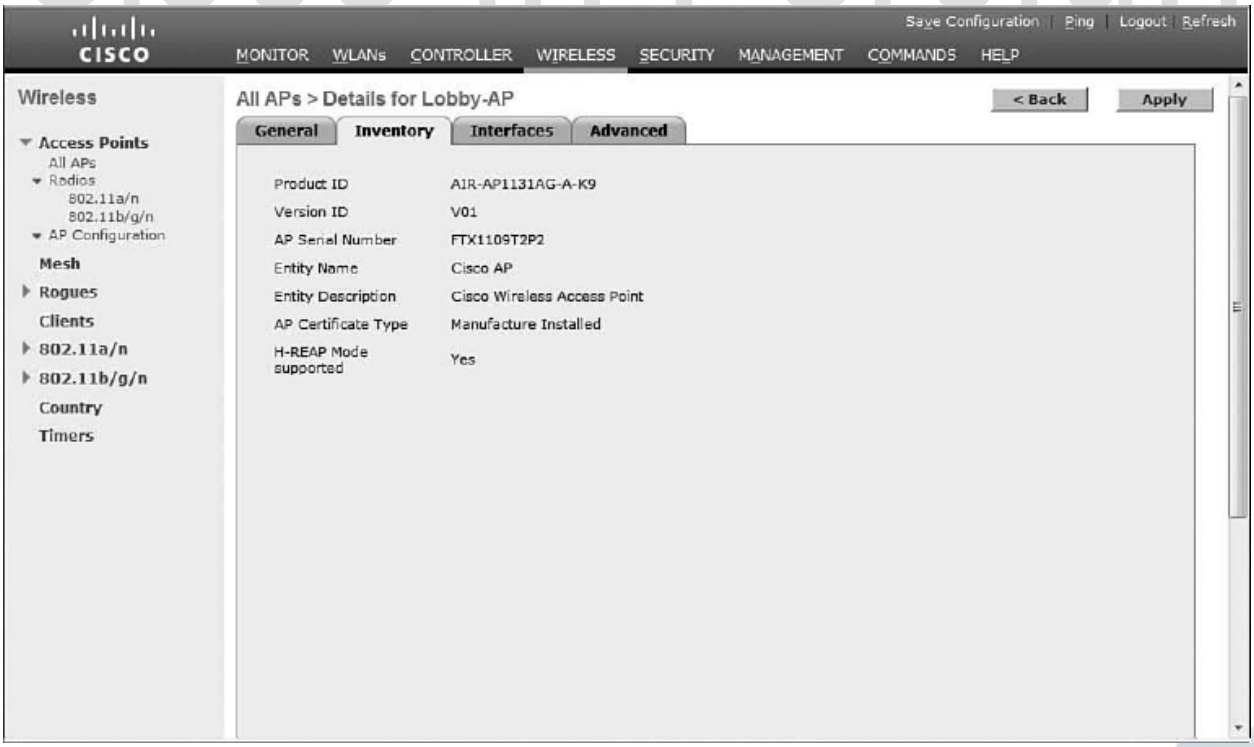


برای دیدن ورژن نرم افزار AP به بخش Wireless / All Aps بروید و AP خود را انتخاب نمایید :



توجه کنید که ورژن نرم افزار AP باید با ورژن نرم افزار کنترلر یکسان باشد .

برای دیدن نوع سخت افزار AP ، از پنجره ی بالا ، به بخش Inventory بروید .

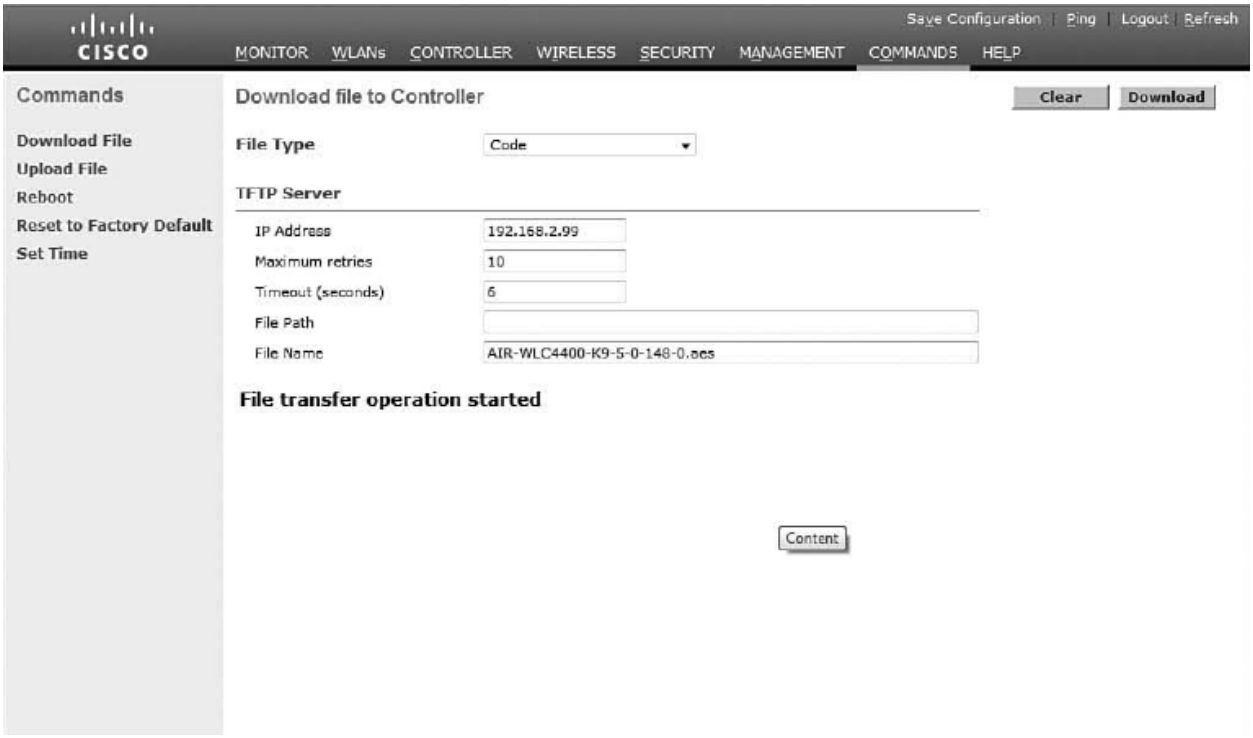


کنترلر را هم از طریق CLI و هم از طریق اینترفیسweb-based می توان upgrade نمود . برای راحتی و سادگی ، روش web-based را انتخاب می کنیم .

Image مورد نظر باید دارای پسوند aes. باشد که یک فایل فشرده شده ی آرشیوی است و شامل سه فایل است :

- ✓ **RTOS :** The Controller's Real-Time Oprating System
- ✓ **CODE :** Airwave Director , command-line interface , controller's switch web interface
- ✓ **Ppcboot.bin :** The Controller's bootloader

سپس باید فایل aes. را روی TFTP server قرار داد .



همینکه انتقال شروع شد ، صفحه مرتبا refresh می شود . کنترلر فایل image را به تدریج درون RAM کپی می کند . پس از اینکه عملیات انتقال تمام شد ، کنترلر فایل را درون flash می ریزد . از این به بعد image موجود کنونی تبدیل به backup image می شود . پس از اتمام این مرحله ، باید کنترلر را reboot نمود .

پس از boot دوباره ، حتما ورژن ها را چک کنید .

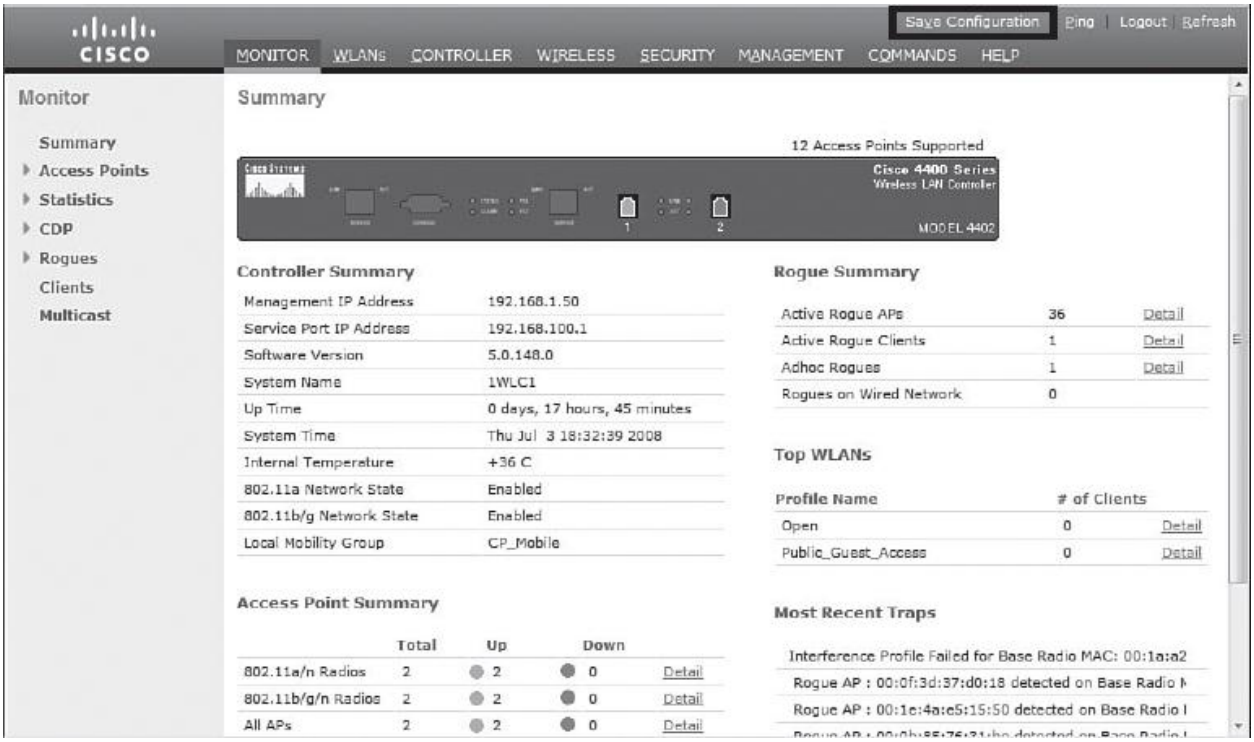
Upgrade با استفاده از WCS :

شما می توانید کنترلر ها را با استفاده از WCS نیز upgrade کنید . توجه داشته باشید که upgrade کردن کنترلر ، AP ها را نیز upgrade می کند ؛ زیرا آنها خودشان را با همان کد ها sync می کنند . مراحل بدین شکل می باشند :

۱. با ping کردن کنترلر و TFTP server ، مطمئن شوید که WCS با آنها ارتباط دارد و مشکلی وجود ندارد .
۲. Configure / Controllers
۳. Select a Command / Download Software
۴. TFTP Server on WCS System
۵. Browse . فایل ها روی Root Directory که در TFTP server تعریف کردید ، آپلود می شوند .
۶. Download . WCS نرم افزار را به کنترلر دانلود می کند و کنترلر کد ها را روی flash RAM می ریزد .

پس از upgrade شدن کنترلر AP ها نیز خود را sync می کنند ، اما تنها ۲۰ عدد AP بطور همزمان می توانند upgrade شوند .

فراموش نکنید که حتما با کلیک روی save configuration ، تنظیمات خود را ذخیره کنید .



فایل Configuration در کنترلر ها ، با فایل configuration روتر ها و سوییچ ها متفاوت است ؛ این فایل متنی نیست ، بلکه بصورت یک فایل XML است .

نکته : دستور ***show running-config*** محتوای تنظیمات را خط به خط نشان می دهد .

نکته : دستور ***show run-config*** اطلاعاتی در مورد وضعیت سیستم ارائه می دهد .

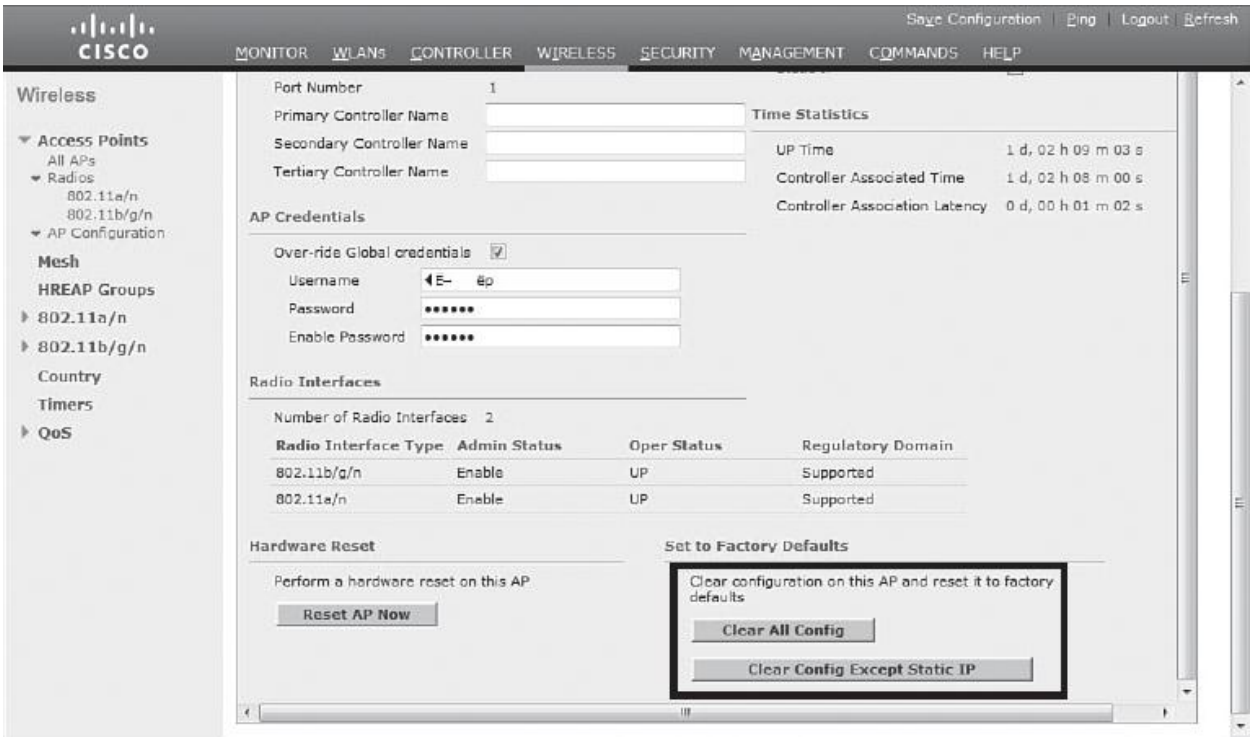
در شکل صفحه ی بعد ، خروجی دستور ***show running-config*** را مشاهده می فرمایید .

```
(Cisco Controller) > show running-config

 802.11a 11nSupport a-mpdu tx priority 0 disable
 802.11a cac voice tspec-inactivity-timeout ignore
 802.11a cac video tspec-inactivity-timeout ignore
 802.11a cac voice stream-size 84000 max-streams 2
 802.11b 11nSupport a-mpdu tx priority 0 disable
 802.11b cac voice tspec-inactivity-timeout ignore
 802.11b cac video tspec-inactivity-timeout ignore
 802.11b cac voice stream-size 84000 max-streams 2
 aaa auth mgmt local radius
 advanced 802.11a receiver pico-cell-V2 rx_sense_thrld 0 0 0
 advanced 802.11a receiver pico-cell-V2 cca_sense_thrld 0 0 0
advanced 802.11a receiver pico-cell-V2 sta_tx_pwr 0 0 0
 Location Summary
 Algorithm used:                 Average
 Client
        RSSI expiry timeout: 150 sec
        Half life:                60 sec
        Notify Threshold:         0 db
 Calibrating Client
        RSSI expiry timeout: 30 sec
        Half life:                0 sec
 Rogue AP
        RSSI expiry timeout:   120 sec
        Half life:                0 sec
        Notify Threshold:         0 db
 RFID Tag
        RSSI expiry timeout: 5 sec
        Half life:                0 sec
        Notify Threshold:         0 db
 location rssi-half-life tags 0
location rssi-half-life rogue-aps 0
 location expiry tags 5
 location expiry client 150
 location expiry calibrating-client 30
 location expiry rogue-aps 120
 advanced eap identity-request-timeout 1
 advanced eap identity-request-retries 20
 advanced eap request-timeout 1
 ap syslog host global 255.255.255.255
interface create guest_lan 80
interface address ap-manager 192.168.1.51 255.255.255.0 192.168.1.1
interface address dynamic-interface guest_lan 172.30.1.50 255.255.255.0 172.30.1.1
interface address management 192.168.1.50 255.255.255.0 192.168.1.1
```

```
interface address service-port 192.168.100.1 255.255.255.0
interface address virtual 1.1.1.1
interface dhcp ap-manager primary 192.168.1.1
interface dhcp dynamic-interface guest_lan primary 172.30.1.1
interface dhcp management primary 192.168.1.1
interface dhcp service-port disable
interface vlan ap-manager 1
interface vlan guest_lan 80
interface vlan management 1
interface port ap-manager 1
interface port guest_lan 1
interface port management 1
 load-balancing window 5
 logging buffered 1
 mesh security eap
 mgmtuser add admin **** read-write
 mobility group domain CP_Mobile
 mobility group anchor wlan add 2 192.168.1.50
 mobility dscp value for inter-controller mobility packets 0
 network webmode enable
 network rf-network-name CP_Mobile
 radius fallback-test mode off
 radius fallback-test username cisco-probe
 radius fallback-test interval 300
 snmp version v2c enable
 snmp version v3 enable
 sysname 1WLC1
 wlan create 1 Open Open
 wlan create 2 Public_Guest_Access GUESTNET
 wlan interface 2 guest_lan
 wlan session-timeout 1 1800
 wlan session-timeout 2 disable
 wlan wmm allow 1
 wlan wmm allow 2
 wlan security wpa disable 2
 wlan security web-auth server-precedence 1
 wlan security web-auth server-precedence 2
 wlan security wpa akm ft reassociation-time 0 1
 wlan security wpa akm ft over-the-air disable 1
 wlan security wpa akm ft over-the-ds disable 1
 wlan security wpa akm ft reassociation-time 0 2
 wlan security wpa akm ft over-the-air disable 2
 wlan security wpa akm ft over-the-ds disable 2
 wlan enable 1
 wlan enable 2
```

Reset to Factory Default :

گفتیم که در حالت کلی ، ما AP را تنظیم نمی کنیم ، بلکه AP خودش را با کنترلر همسان می کند . اما در بعضی مواقع لازم است که مثلا AP را به تنظیمات کارخانه برگردانیم ؛ در چنین مواقعی باید حتما به AP دسترسی فیزیکی داشته باشیم .



همچنین چنانچه بخواهیم کنترلر رابه تنظیمات اولیه بازگردانیم ، باید از COMMANDS / reset to factory default استفاده کنیم .

توجه : کنترلر باید حتما reboot شود تا تغییرات اعمال گردد . زیرا configuration فقط در NVRAM ذخیره نشده ، بلکه در RAM نیز فعال است و تنها با reboot بطور کامل پاک می شود .

توجه : با انجام این کا ر ، شما ارتباط خود را با کنترلر از دست می دهید .

فصل بیستم : عیب یابی شبکه های وایرلس

- مشکلات رایج در سمت کاربران
  - ✓ Hiden node
  - ✓ Exposed node
  - ✓ Near/Far
- استفاده از CLI برای عیب یابی
- استفاده از Controller Interface برای عیب یابی
- استفاده از SNMP
- استفاده از WCS version 5.x برای عیب یابی کاربران

در این فصل با انواع مشکلاتی که ممکن است در شبکه ی وایرلس بوجود آید آشنا می شویم ؛ همچنین به انواع روش ها ، تکنیک ها ، دستورات ، و تنظیماتی که می تواند این مشکلات را برطرف کند خواهیم پرداخت . هرچند هر فردی ممکن است روش خاصی برای عیب یابی شبکه داشته باشد ، در این فصل انواع مهارت ها (قبیل کار با CLI ، اینترفیس کنترلر ، WCS و ...) را مرور خواهیم نمود .

مشکلات رایج در سمت کاربران :

- ✓ کارت شبکه ی کاربران را چک کنید . بسیاری از لپ تاپ ها یک سوییچ سخت افزاری دارند که می توانند کارت شبکه ی وایرلس را غیر فعال نمایند .
- ✓ SSID را چک کنید که به درستی تنظیم شده باشد .
- ✓ آدرس MAC کاربر را چک کنید تا جزء Blacklist شبکه قرار نگرفته باشد .
- ✓ اگر از 802.1x استفاده می کنید ، مطمئن شوید سمت کاربر می تواند EAP-TLS را ساپورت کند .
- ✓ مطمئن شوید آدرس IP کاربر توسط ACL در شبکه فیلتر نشده باشد .
- ✓ Firewall و Antivirus کاربر را چک کنید تا مطمئن شوید جلوی دسترسی کاربر به شبکه را نمی گیرد .

بررسی این مشکلات ، می تواند زمان عیب یابی شبکه را به حداقل برساند .

مشکلات مربوط به Hidden Node :

هنگامیکه دو کاربر در محدوده ی یک AP باشند ، اما در دو طرف cell قرار گرفته باشند ، به عبارتی آنقدر از هم دور باشند که یکدیگر را نبینند و نتوانند RTS/CTS را بشنوند ، بطور همزمان شروع به ارسال می کنند و نهایتا منجر به ایجاد collision می شوند .

برای حل این مشکل می توان Maximum Frame Size را کاهش داد . همچنین می توان آنها را مجبور به ارسال RTS/CTS نمود . راه دیگر کوچک تر کردن محدوده ی cell است که این کار با کاهش دادن توان ارسالی AP میسر می گردد . هدف از همه ی این کارها اینست که کاربران را وادار کنیم که به یکدیگر گوش دهند .

مشکلات مربوط به Exposed Node :

هنگامیکه دو سلول وایرلس که در یک کانال فعالیت می کنند ، خیلی به هم نزدیک باشند ، باعث ایجاد تداخل بر روی یکدیگر می شوند ؛ بخصوص در شبکه های وایرلس B/G که تنها ۳ کانال غیر همپوشان داریم . چنانچه کاربران هر سلول پکتی ارسال کنند ، collision رخ می دهد .

روش ساده برای حل این مشکل ، تغییر توپولوژی و یا حداقل تغییر نحوه ی تخصیص کانال هاست . در برخی موارد ممکن است نتوان این کارها را انجام داد و شما مجبور شوید از 802.11a استفاده کنید که کانال های بیشتری در اختیارتان می گذارد .

مشکلات مربوط به Near/Far :

این مشکل مربوط به زمانیست که سیگنال AP خیلی قوی است و به کاربران خیلی دور نیز می رسد (cell خیلی بزرگ است) ، اما سیگنال کاربران آنقدر قوی نیست که از دورترین نقطه ی cell بتواند به AP برسد .

برای حل این مشکل باید از امکانات کنترلر استفاده کنید . کنترلر می تواند سیگنال کاربران را مانیتور نموده و منابع رادیویی مناسب را در محل های مناسب پیش بینی نماید تا بتوان سیگنال را تقویت یا تکرار نمود .

استفاده از CLI برای عیب یابی :

یکی از دستورات مفید ، ***show client summary*** است که لیست کاربرانی که associate شده اند یا در حال association هستند را نمایش می دهد .

```
(Cisco Controller) >show client summary

Number of Clients................................ 1

MAC Address AP Name Status WLAN Auth Protocol Port
----------------- ---------------- ------------ ---- ---- -------- ----

00:13:e8:a9:e1:29 Lobby-AP Probing N/A No 802.11b 1

 (Cisco Controller) >
```

برای دیدن جزئیات هر کاربر ، از دستور ***show client detail*** استفاده نمایید .

```
(Cisco Controller) >show client detail 00:15:af:0a:0b:71
Client MAC Address.............................. 00:15:af:0a:0b:71
Client Username ................................ N/A
AP MAC Address.................................. 00:1a:a2:fc:df:a0
Client State.................................... Probing
Wireless LAN Id................................. N/A
BSSID........................................... 00:1a:a2:fc:df:9f
Channel......................................... 11
IP Address...................................... Unknown
Association Id.................................. 0
Authentication Algorithm........................ Open System
Reason Code..................................... 0
```

```
Status Code..................................... 0
Session Timeout................................. 0
Client CCX version.............................. No CCX support
Mirroring....................................... Disabled
QoS Level....................................... Silver
Diff Serv Code Point (DSCP)..................... disabled
802.1P Priority Tag............................. disabled
WMM Support..................................... Disabled
Mobility State.................................. None
Mobility Move Count............................. 0
Security Policy Completed....................... No
—More— or (q)uit
Policy Manager State............................ START
Policy Manager Rule Created..................... Yes
NPU Fast Fast Notified.......................... No
Policy Type..................................... N/A
Encryption Cipher............................... None
Management Frame Protection..................... No
EAP Type........................................ Unknown
Interface....................................... management
VLAN............................................ 0
Client Capabilities:
CF Pollable..................................... Not implemented
CF Poll Request................................. Not implemented
Short Preamble.................................. Not implemented
PBCC............................................ Not implemented
Channel Agility................................. Not implemented
Listen Interval................................. 0
Client Statistics:
Number of Bytes Received........................ 0
Number of Bytes Sent............................ 0
Number of Packets Received...................... 0
Number of Packets Sent.......................... 0
Number of Policy Errors......................... 0
Radio Signal Strength Indicator................. Unavailable
—More— or (q)uit
Signal to Noise Ratio........................... Unavailable
Nearby AP Statistics:
TxExcessiveRetries: 0
TxRetries: 0
RtsSuccessCnt: 0
RtsFailCnt: 0
TxFiltered: 0
TxRateProfile: [0,0,0,0,0,0,0,0,0,0,0,0]
Research_Lab-AP(slot 0) ....................
```

```
antenna0: 5 seconds ago -93 dBm.................. antenna1: 4293918453 seconds ago
-128 dBm
Lobby-AP(slot 0) ........................
antenna0: 4293918453 seconds ago -128 dBm........ antenna1: 5 seconds ago -94 dBm
```

توجه داشته باشید که اطلاعاتی که دستورات ***show*** به شما نشان می دهند ، همگس static هستند ؛ یعنی وضعیت و موقعیت شبکه را در زمانیکه این دستورات را وارد کرده اید به شما نشان می دهند .

برای دیدن اطلاعات real-time ، باید از دستورات ***debug*** استفاده نمایید . برای دیدن انواع دستورات ***debug*** :

```
(Cisco Controller) >debug ?

aaa Configures the AAA debug options.
airewave-director Configures the Airewave Director debug options
ap Configures debug of Cisco AP.
arp Configures debug of ARP.
bcast Configures debug of broadcast.
cac Configures the call admission control (CAC) debug options.
cdp Configures debug of cdp.
crypto Configures the Hardware Crypto debug options.
dhcp Configures the DHCP debug options.
client Enables debugs for common client problems.
disable-all Disables all debug messages.
dot11 Configures the 802.11 events debug options.
dot1x Configures the 802.1X debug options.
iapp Configures the IAPP debug options.
ccxrm Configures the CCX_RM debug options.
ccxdiag Configures the CCX Diagnostic debug options.
locp Configures the LOCP debug options.
l2roam Configures the L2 Roam debug options.
l2age Configures debug of Layer 2 Ago Timeout Messages.
lwapp Configures the LWAPP debug options
mac Configures MAC debugging
--More-- or (q)uit
```

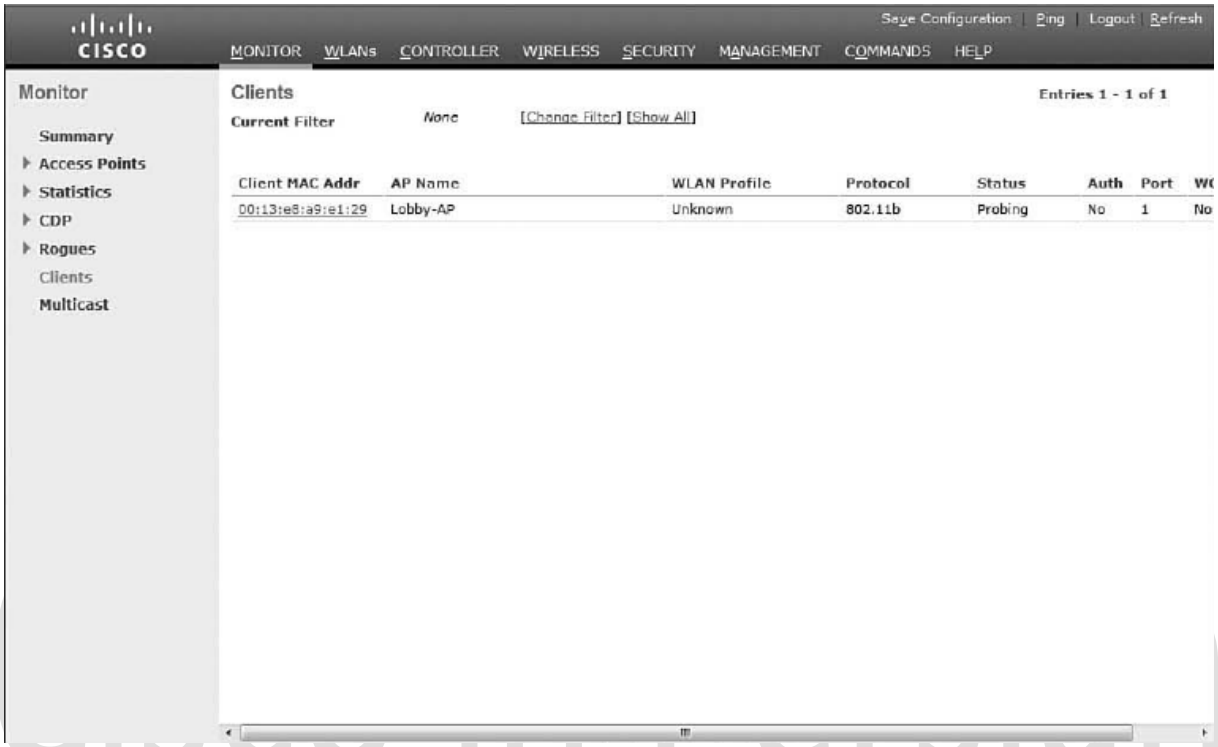
البته روند کار به این ترتیب است که ابتدا مثلا با دستور ***debug mad addr 00:1a:a2:f9:ed:d0*** عملیات Debug را برای این کاربر فعال می کنید . سپس با دستور ***debug lwapp events enable*** مشخص می کنید که کنترلر باید برای آدرس mac داده شده از چه نوع debugging استفاده نماید .

در نهایت با استفاده از دستور ***show debug*** می توانید تنظیمات خود را مشاهده کنید .

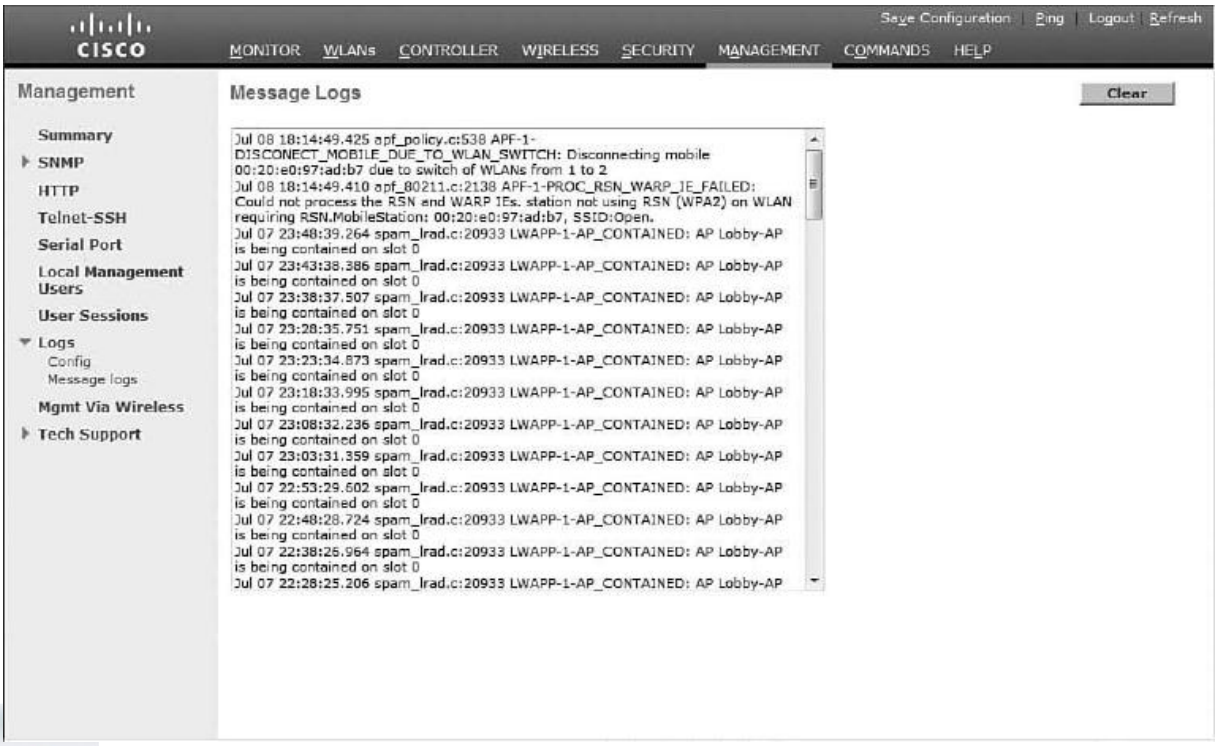
فراموش نکنید که پس از انجام عیب یابی ، این فرآیند را با دستور ***debug disable-all*** غیر فعال سازید .

استفاده از Controller Interfce برای عیب یابی :

کنترلر امکانات زیادی دارد که به عیب یابی شبکه کمک می کند . مثلا web-interface زیر ، دقیقا معادل خروجی دستور ***show client summary*** است .



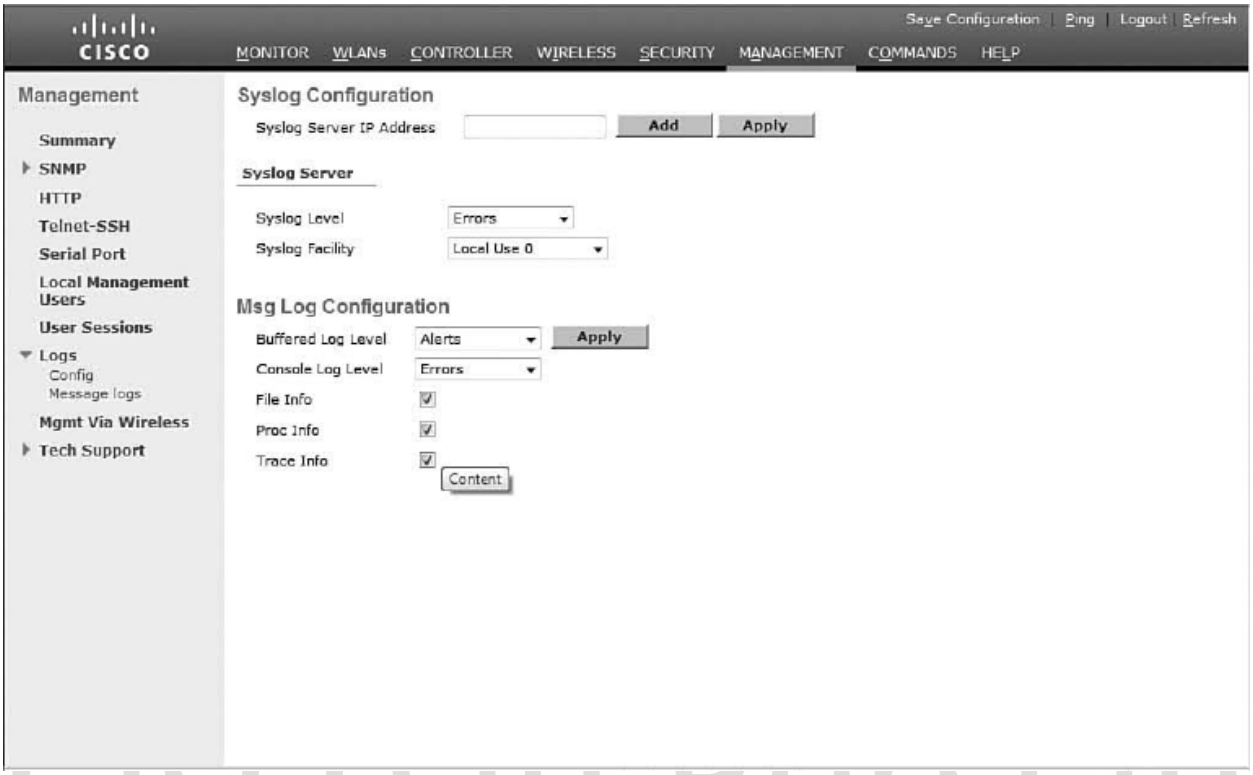
همچنین برای دیدن log های کنترلر : MANAGEMENT / Logs / Message logs



همچنین در صفحه ی syslog ، می توانید level های مختلفی برای logging قرار دهید . این level ها مقدار اطلاعاتی که باید capture شوند را مشخص می نماید . بطور کلی ، هرچه این عدد بزرگتر باشد ، اطلاعات بیشتری جمع آوری و ضبط می شود .

Facility Name	Facility Level
Kernel	0
User Process	1
Mail	2
System Daemons	3
Authorization	4
Syslog	5
Line Printer	6
USENET	7
Unix-to-Unix Copy	8
Cron	9
—	10
FTP Daemons	11
System Use 1	12
System Use 2	13
System Use 3	14
System Use 4	15
Local Use 0	16
Local Use 1	17
Local Use 2	18
Local Use 3	19
Local Use 4	20
Local Use 5	21
Local Use 6	22
Local Use 7	23

برای تغییر تنظیمات logging ، به بخش MANAGEMENT / Logs / Config بروید .



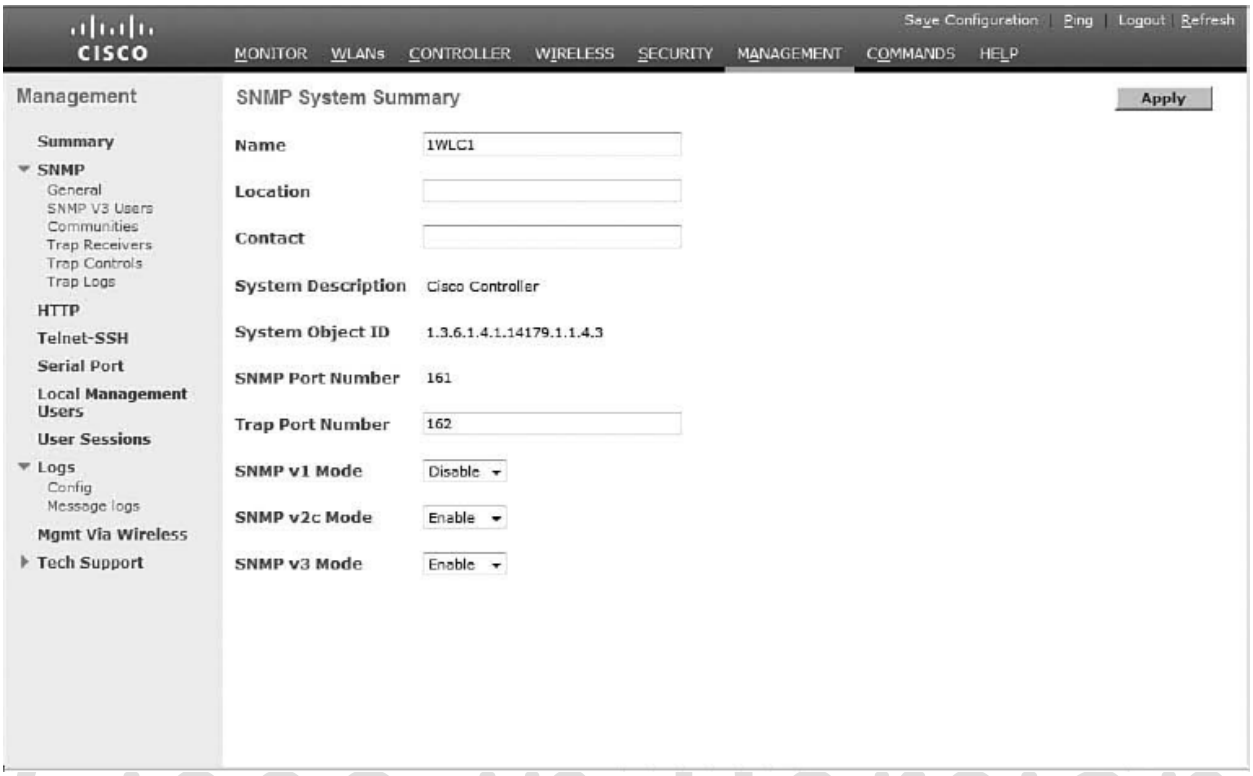
در بالا می توان آدرس IP یک Syslog server را وارد کرد تا log های این کنترلر به آنجا ارسال گردد . همانند TFTP server ، اینجا نیز می توان از یک نرم افزار به عنوان Syslog server استفاده نمود .
Message log ها ، شامل اطلاعاتی در مورد ساختار شبکه ، موارد مربوط به کاربران ، authentication ، و مسایل مربوط به اتصال AP ها می باشد .

استفاده از SNMP :

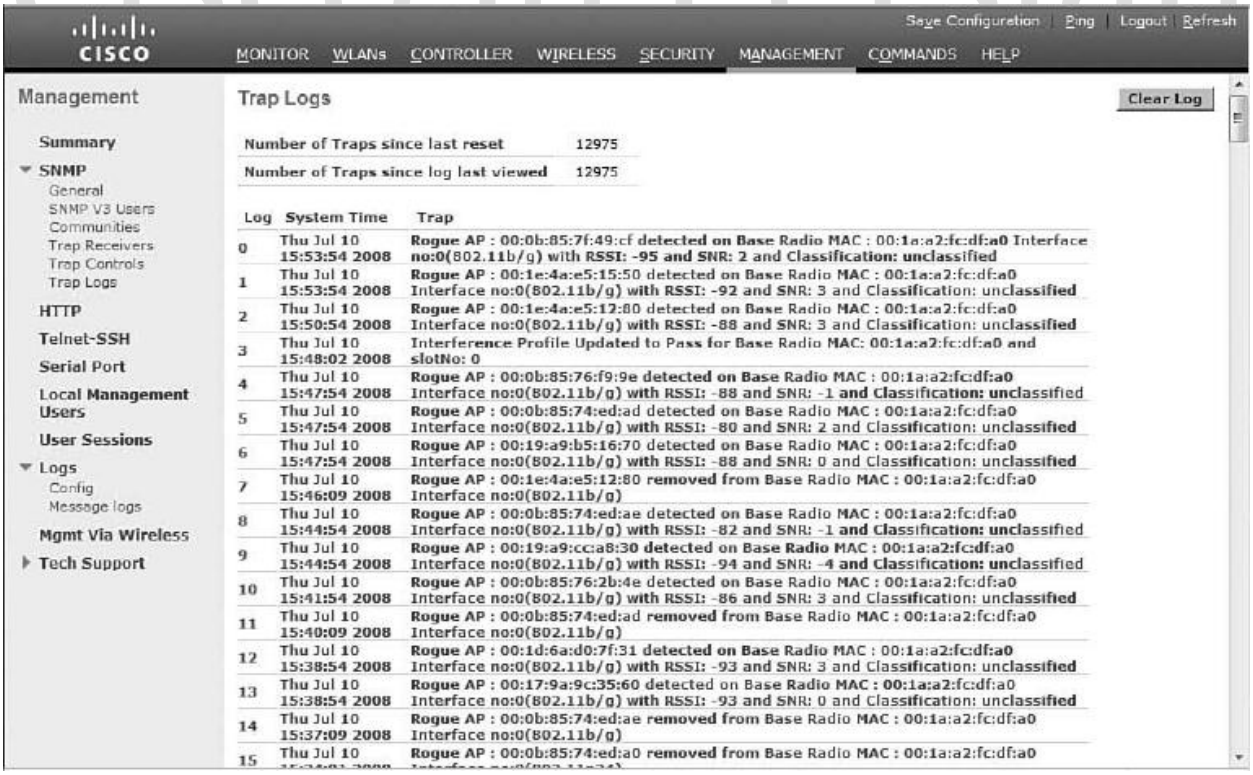
با استفاده از SNM gets/sets ، می توانید اطلاعات مختلفی در مورد وضعیت کنترلر به دست آورید که این امر ، مدیریت و کنترل کردن کنترلر از راه دور را میسر می سازد .

توجه : SNMPv1 امن نیست و بهتر است غیر فعال باشد .
توجه : SNMPv2c در حالت read-only است .
توجه : SNMPv3 کاملا امن است و توصیه می گردد .

برای تنظیم SNMP ، به بخش MANAGEMENT / SNMP / General بروید .

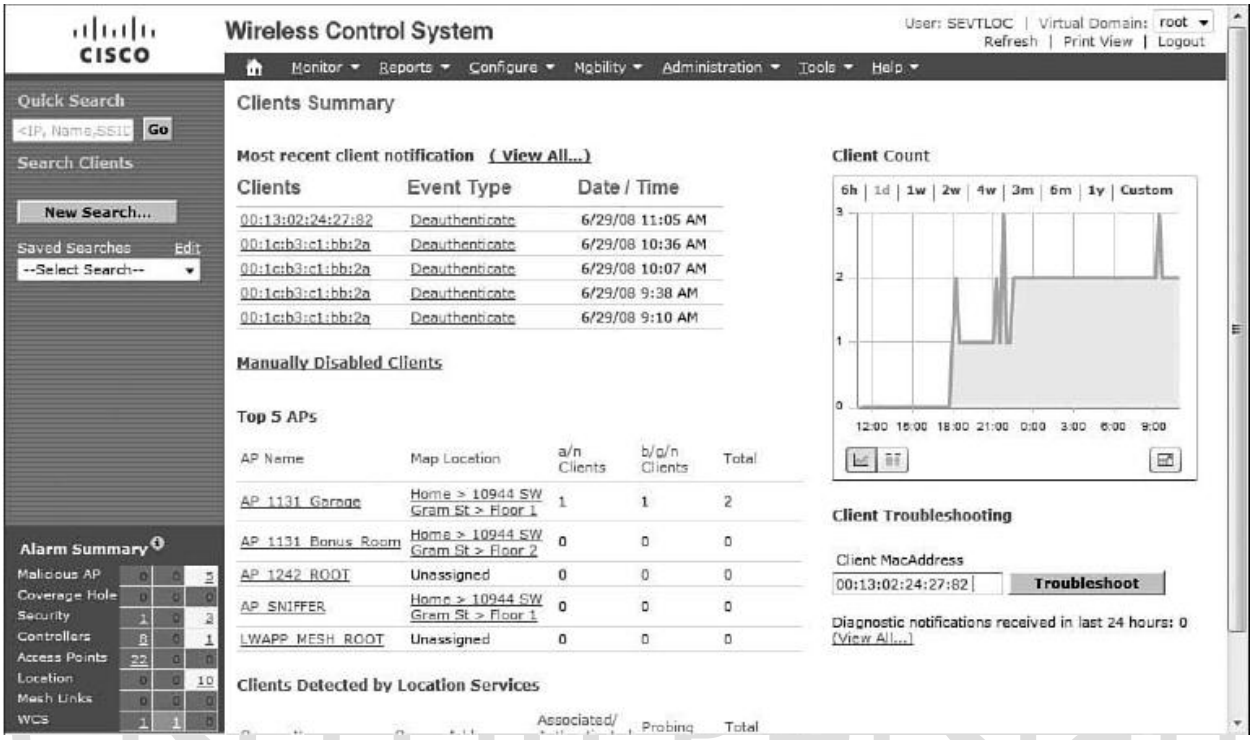


همچنین برای دیدن SNMP trap logs ، می توانید به بخش MANAGEMENT / SNMP / Trp Logs بروید .



استفاده از WCS version 5.x برای عیب یابی کاربران :

با رفتن به Monitor / Client ، می توانید به عیب یابی مشکلات کاربران بپردازید .



توجه کنید که استفاده از alarm ها با استفاده از رنگ های مختلف می تواند کمک بزرگی در عیب یابی به شما بکند .

قرمز : خطرناک

نارنجی : خطر زیاد

زرد : خطر کم

Cisco in Persian

yousef@shafagh.com
u3fnm@yahoo.com