Chương 7:

Mạng không dây

Chương 7: Mạng không dây cục bộ (Wireless LANs)

Chương này sẽ mô tả những xu hướng và chuẩn kỹ thuật gặp phải trong việc phát triển mạng LAN không dây (WLAN)

Mục tiêu

Sau khi hoàn tất bài học, SV có khá năng mô tả những yếu tố ảnh hưởng và những tiêu chuẩn hệ thống mạng LAN không dây qua các nhiệm vụ sau:

1. Mô tả những nhu cầu thực tế cần đến dịch vụ WLAN
2. Mô tả sự khác biệt giữa việc thực thi mạng WLAN và LAN
3. Xác định các đặc tính của việc truyền dẫn sử dụng sóng radio trong mạng WLAN
4. Xác định các tổ chức định ra các chuẩn cho mạng WLAN
5. Mô tả hệ thống 3 băng tầng không đăng ký được sử dụng cục bộ trong mạng không dây FCC bởi tổ chức ITU-R
6. So sánh những sự khác biệt giữa những chuẩn trong IEEE 802.11
7. Mô tả về hệ thống chứng nhận Wi-Fi

XU HƯỚNG CỦA WIFI TRONG TƯƠNG LAI

1. Định tuyến băng tần đơn (Single-band Router) sẽ trở nên xưa cũ. Mục đích của truy cập mạng wifi là để sử dụng các video trực tuyến (với YouTube hay các ứng dụng trên điện thoại…) vì thế dùng truy cập ở băng tầng đơn 2.4 GHz sẽ không tốt nhất và phản tác dụng trong việc trải nghiệm video streaming tối ưu.

Khi băng tần 2.4 GHz mắc vào nhiều rắc rối và bị nghẽn mạng, yêu cầu được nhiều hơn từ kết nối mạng wifi thì bấy giờ sự khác biệt giữa băng tần đơn và kép sẽ hiện ra cụ thể nhất.
Do nhu cầu của người dùng ngày càng lớn, điển hình là xem hay xử lý video, kiểm soát thông tin cá nhân nặng trên những ứng dụng lưu trữ đang ngày càng thông dụng.

2. Loại bỏ chuẩn Legacy 802.11x
Phần lớn phần cứng và hệ thống mạng phù hợp với Wi-Fi 802.11n
Bộ định tuyến tín hiệu wifi sử dụng chuẩn 802.11n sẽ cung cấp dung lượng băng thông nhanh hơn và sẽ hợp lý để người sử dụng khai thác tối ưu và có năng suất cao những dụng cụ dùng truy cập không dây mới nhất (kể cả máy tính xách tay và máy tính bảng).

3. Thiết bị chuẩn 802.11AC ra mắt

802.11ac là chuẩn không dây mới với khá nhiều tính năng mạnh có khả năng cung cấp vận tốc liên kết dữ liệu thô lên tới 1 Gbps. Chuẩn 802.11ac trên lý thuyết chỉ chạy trong phổ tần 5 GHz nên sự thông suốt cao hơn và cũng ít bị sự cố hơn.

Chuẩn này còn được gọi là VHT (viết tắt của Very High Throughput – tạm dịch là siêu thông lượng), tốt cho giải trí như xem video HD, có trên thị trường năm 2012 với có khả năng phục vụ tầm phủ sóng tốt hơn, vận tốc nhanh hơn gấp 2 lần so với chuẩn 802.11n.
Redpine Signals vào tháng 12/2012, mô-đun Quali-Fi 802.11ac, có độ tiêu thụ năng lượng thấp như di động.
Wi-Fi 5G (vì 802.11ac là tiêu chuẩn IEEE đời thứ 5 cho công nghệ mạng Internet không dây phổ biến).

4. Thiết bị dùng chuẩn Wi-Gig:

WiGig được phát triển để có thể hỗ trợ cho hai chuẩn chuẩn 802.11n và 802.11ac. Về lý thuyết, WiGig có dung lượng băng thông đạt tốc độ nhanh gấp bảy lần so với những thiết bị dùng chuẩn 802.11n và 802.11ac. Công nghệ này sẽ được sử dụng để phủ sóng Wi-Fi cho toàn bộ căn nhà và có thể được dùng cho một số yêu cầu riêng, yêu cầu năng suất cao như giải trí ở nhà, xem video trực tuyến có độ phân giải cao.

5. Sản phẩm gia đình có sẵn Wi-Fi gia tăng

Với công nghệ và tính năng hiện đại như HomePlug Gree của Qualcomm (tên đầy đủ Qualcomm Atheros QCA7000 HomePlug Gree) sẽ đem lại cho khách hang với mức tiêu thụ điện năng nhỏ.
Được cài đặt trên ô tô điện, năng lượng thông minh, những thiết bị giám sát từ xa qua Smartphone.

6. Điều hành nhà từ xa ngày càng phổ biến

Điều khiển trên điện thoại thông minh, laptop để giúp đỡ khách hàng có thể giám sát an ninh hay điều khiển từ xa mọi thứ xảy ra trong căn nhà từ bất cứ đâu, có thể tắt đèn, bật máy nước nóng hay kích hoạt hệ thống báo động... và ấn nhẹ lên các chức năng trên màn hình điện thoại với kết nối Wi-Fi.

7. Tín hiệu Wi-Fi mở rộng rộng hơn

Các địa điểm phát sóng Wi-Fi đang có ở khắp nơi, dù lượng người kết nối không nhiều hoặc bị bảo mật. Dự đoán, sắp tới sẽ là năm xuất hiện sóng Wi-Fi công cộng (không mất phí và kinh doanh), phân bố nhiều tại các thành phố lớn và trung tâm thương mại.

8. Dễ dàng thực hiện

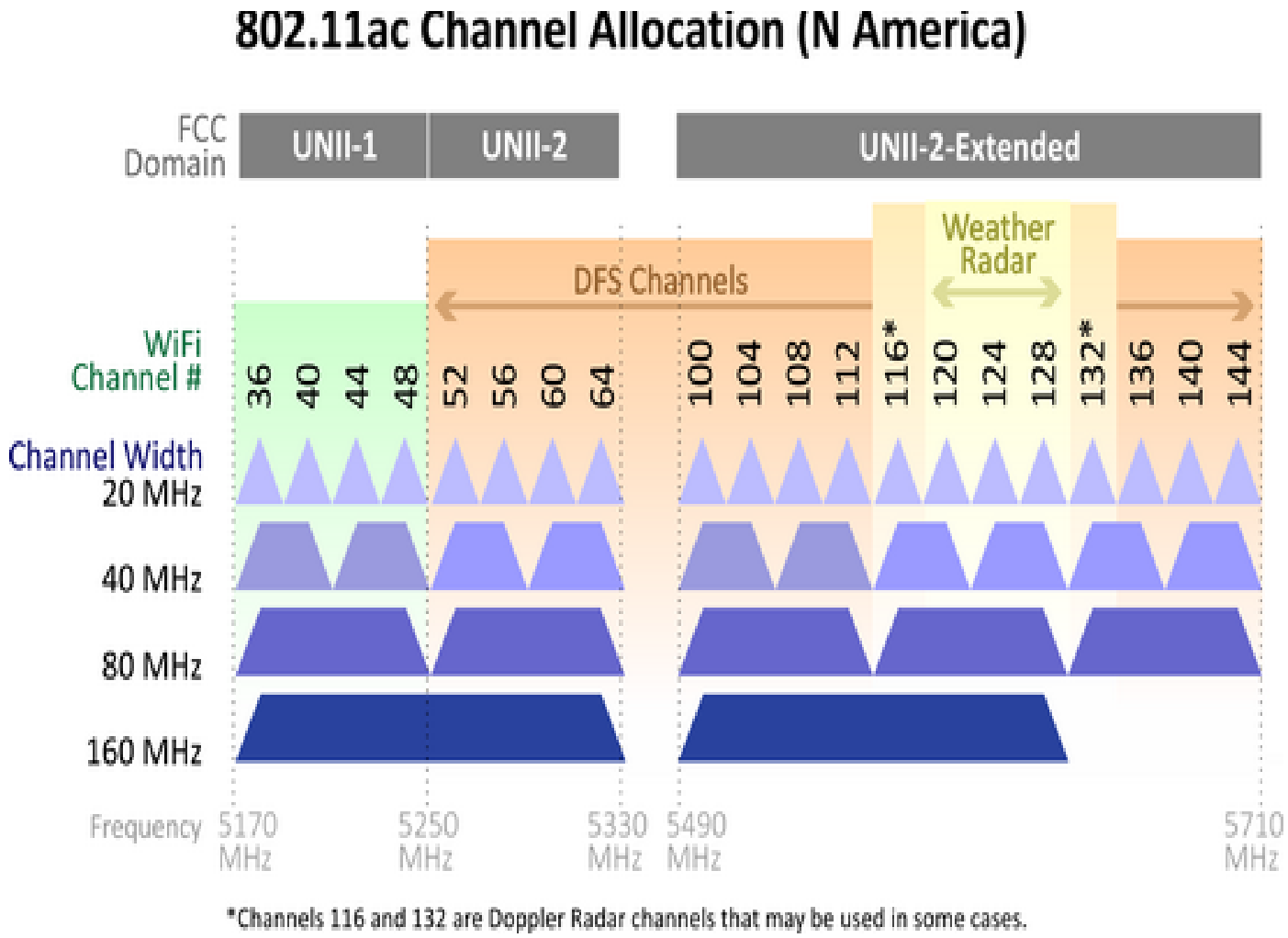
Các thiết bị đã đơn giản hóa việc cài đặt một hệ thống mạng không dây. Thực sự, nhiều doanh nghiệp sản xuất đã nhận ra kết luận, hầu hết khách hàng của họ không cần và không có ý định hiểu bất kể bước gì phức tạp của 802.11n, giao tiếp RF, định hướng hay các thông số khó nhớ mà chỉ cần cắm – chạy. Cisco Linksys, Netgear, D-Link và Belkin đã khiến tất cả vấn đề biến thành đơn giản hơn, chỉ cần vài ba bước nhấn chuột.

9. Tốc độ vẫn vai trò chính

Tốc độ của mạng Wi-Fi ngày càng cao từ mức 300 Mbps và tăng lên đến mức độ 600 Mbps vào cuối năm 2011. những router phục vụ hai băng tần đạt mức tốc độ 900 Mbps, tương ứng với 450 Mbps cho mỗi băng tần.

10. Công nghệ – thiết bị chơi trò "đuổi bắt"

Một số bộ định tuyến không dây "siêu nhanh", sản phẩm mới nhất trên thị trường sử dụng đến ba ăng-ten phát sóng, sử dụng bộ truyền/nhận 3×3 để khuếch đại tín hiệu được nhanh hơn và nhiều công nghệ khác nữa. Các router được tung ra chỉ có tốc độ 300 Mbps hoặc 600 Mbps với 2×2 ăng-ten.



2. Mô tả sự khác biệt giữa việc thực thi mạng WLAN và LAN

- Môi trường WLAN, sóng radio được sử dụng tại lớp vật lý (trong mô hình OSI).
- WLAN sử dụng phương thức truy nhập CSMA/CA thay vì CSMA/CD trong mạng LAN Ethernet. Khả năng phát hiện xung đột không được trang bị trong hệ thống WLAN bởi vì một máy khi gởi sẽ không đồng thời nhận tín hiệu vào tại thời điểm đó. Thay vào đó, hệ thống WLAN sử dụng tín hiệu RTS (Ready to send – sẵn sàng gởi) và CTS (Clear to send – sẵn sàng nhận) để tránh xung đột trong quá trình truyền dẫn.
- Định dạng khung dữ liệu mà hệ thống WLAN sử dụng khác định dạng khung dữ liệu trong hệ thống Ethernet LAN. WLANs có thêm một số yêu cầu trên phần định dạng khung lớp 2. Sóng radio sẽ tạo ra một số vấn đề không gặp như trong môi trường LAN.
- Vấn đề kết nối trong mạng WLAN xảy ra thường là liên quan đến vấn đề tầm phủ sóng, quá trình truyền sóng radio, méo dạng sóng và nhiễu từ những dịch vụ không dây hay những hệ thống WLANs khác.
- Vấn đề đảm bảo sự riêng tư cũng là một thử thách bởi sóng radio có thể lọt ra ngoài tầm kiểm soát vật lý.

Trong môi trường WLAN, những người dùng di động kết nối với hệ thống mạng thông qua điểm truy cập (Access Point), được xem như tương tự với HUB trong môi trường Ethernet LAN

2. Mô tả sự khác biệt giữa việc thực thi mạng WLAN và LAN

- Người dùng di động không có kết nối vật lý vào môi trường mạng.

- Những thiết bị di động thường sử dụng pin làm nguồn năng lượng chính.

- WLAN phải tuân theo một số quy định về tần số ở nước sở tại.

- Mục tiêu của việc chuẩn hóa để đưa ra các tiêu chuẩn nhằm giúp mạng WLAN có mặt rộng khắp trên toàn thế giới. Bởi vì mạng WLAN sử dụng tần số radio, do vậy phải tuân theo quy định về tần số và công suất phát ở nước sở tại. Yêu cầu này không xảy ra trong hệ thống mạng LAN có dây.

3. Xác định các đặc tính của việc truyền dẫn sử dụng sóng radio trong mạng WLAN

a. Tần số radio được bức xạ vào không khí qua các anten tạo thành sóng radio

- Tần số radio trải từ dải băng tần AM đến dải tần số sử dụng cho điện thoại di động (cell phone). Chủ đề này nhằm xác định đặc tính của tần số radio được sử dụng truyền dẫn trong mạng WLAN.

-Tần số radio được bức xạ ra không gian nhờ các anten, và anten là nơi tạo ra các sóng radio. Khi sóng radio truyền, nó có thể bị hấp thu (bởi vật ngăn trở như bức tường,…) hay bị phản xạ (bởi bề mặt kim loại,…). Những nguyên nhân này sẽ khiến vùng phủ sóng bị thiếu sóng hay chất lượng tín hiệu thấp.

b. Các vật thể có thể làm ảnh hưởng sóng radio:

- Phản xạ: xảy ra khi tần số sóng radio bị dội ra trên bề mặt của các vật thể như bề mặt của kim loại hoặc gương.
- Tán xạ: xảy ra khi tần số sóng radio va phải những bề mặt gồ ghề và bị phản xạ ra nhiều hướng khác nhau.
- Hấp thu: xảy ra khi tần số sóng radio bị hút vào các vật thể như bức tường.

c. Tần số cao cho phép truyền tốc độ nhanh nhưng khoảng cách truyền lại ngắn.

- Tốc độ dữ liệu càng cao thì khoảng cách truyền càng ngắn bởi thiết bị nhận yêu cầu một tín hiệu mạnh phải có thông số SNR (Signal-to-Noise– tỷ số tín hiệu trên nhiễu) tốt để có thể nhận được thông tin.

- Công suất truyền càng cao, tầm phủ sóng càng xa. Để tăng gấp đôi tầm phủ sóng, công suất phát sẽ phải tăng lên 4 lần.

- Tốc độ truyền cao yêu cầu nhiều băng thông. Việc tăng băng thông có thể được thực hiện qua việc tăng tần số hoặc sử dụng một số phương pháp điều chế phức tạp.

- Tần số truyền càng cao khoảng cách truyền càng ngắn bởi nó dễ dàng bị hấp thu và suy hao. Vấn đề này có thể được giải quyết bởi một số anten thích hợp.

4. Các tổ chức định ra các chuẩn cho mạng WLAN

ITU-R:

International Telecommunication Union-Radiocommunication Sector

Chỉ ra các tần số sóng được sử dụng trong WLAN

IEEE:

Institute of Electrical and Electronic Engineers

802.11 là tài liệu về các chuẩn kỹ thuật

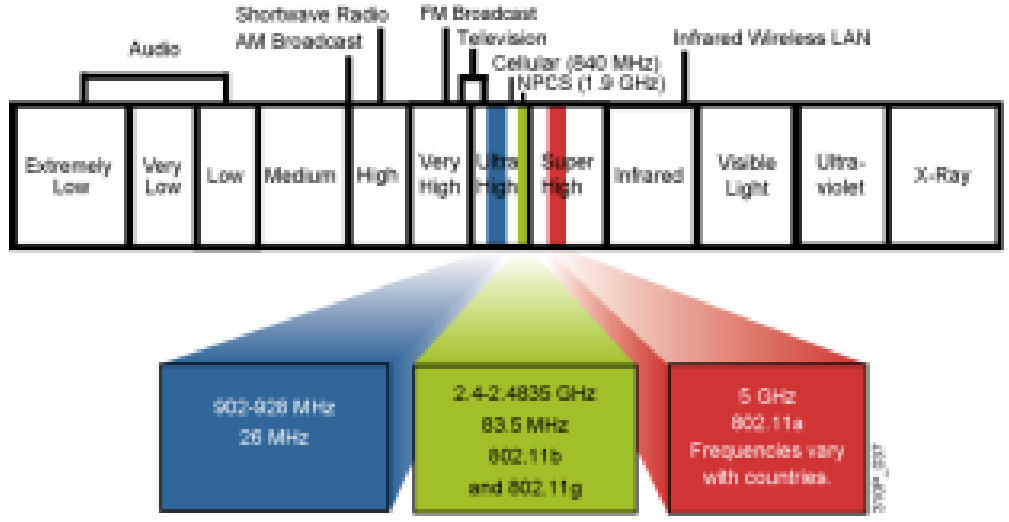
Wi-Fi Alliance:

Tổ chức phi lợi nhuận

Thúc đẩy sự phát triển của WLAN qua các chứng nhận liên vận hành giữa các hang trên dòng sản phẩm cho WALN

•Có một vài băng tần radio không cần đăng ký tần số khi hoạt động. Chủ đề này mô tả 3 dãy băng tần không cần đăng ký được sử dụng cục bộ trong mạng không dây FCC của tổ chức ITU-R

ITU-R với FCC Wireless



- ISM: industry, scientific, and medical frequency band
- Không cần đăng ký sử dụng
- Không được dành riêng
- Có khả năng bị can nhiễu

•Có 3 băng tần không cần đăng ký tần số khi sử dụng: 900 MHz, 2.4 GHz và 5 GHz. Dãy băng tần 900 MHz và 2.4 GHz được biết đến như dãy băng tần dùng cho Công nghiệp, Khoa học và Y tế, trong khi đó dãy băng tần 5 GHz thì thường được biết đến như dãy băng tần UNII (Unlicensed National Information Infrastructure).

•Những tần số nằm trong trong những dải băng tần trên bao gồm:

- Băng tần 900-MHz: 902 MHz đến 928 MHz

- Băng tần 2.4 GHz: 2.400 MHz đến 2.483 MHz (tại Nhật, dải băng tần này được mở rộng đến 2.495 MHz)

- Băng tần 5GHz: 5.150 MHz đến 5.350 MHz, 5.725 MHz đến 5.825 MHz, một số nước hỗ trợ việc sử dụng các dãy băng tần giữa 5.350 MHz và 5.725 MHz. Không phải tất các các quốc gia đều cho phép sử dụng chuẩn 802.11a với dãy băng tần 5GHz.

• Kế tiếp dãy tần số của WLAN trong dãy phổ trên là tần số của những dịch vụ không dây khác như điện thoại di động và dãy băng tần hẹp cho các dịch vụ giao tiếp cá nhân (PCS – Personal Communication Services). Những tần số sử dụng cho mạng WLAN là những dãy tần của ISM.

•Vận hành các thiết bị không dây trên những tần số không cần đăng ký thì không cần sự cấp phép. Tuy nhiên không một người dùng nào được độc chiếm bất kỳ một tần số nào. Ví dụ, băng tần 2.4 GHz được sử
dụng cho mạng WLAN, truyền hình, Bluetooth, vi ba và các hệ thống điện thoại không dây (cordless).

• Mặc dù 3 dãy băng tần không cần đăng ký thì không cần phải được cấp phép để vận hành cá thiết bị, tuy nhiên chúng cũng phải được tuân theo qui định của một số quốc gia sở tại trong một số lĩnh vực như công suất truyền, độ lợi anten, tổng suy hao trên: thiết bị truyền dẫn, cáp, và độ lợi của anten.

• Công suất bức xạ vô hướng hiệu dụng (EIRP) là đơn vị cuối cùng của việc đo lường được giám sát bởi các tổ chức quản lý nội tại. Do đó, cần cẩn trọng trong việc thay đổi các thành phần của thiết bị không dây như
việc thêm vào hoặc nâng cấp anten để mở rộng tầm phủ sóng. Kết quả có thể làm cho hệ thống WLAN không còn hợp pháp theo những quy định của cơ quan quản lý nội tại nữa.

EIRP = công suất phát + độ lợi anten – suy hao trên cáp dẫn.

6. So sánh những sự khác biệt giữa những chuẩn trong IEEE 802.11

So sánh các chuẩn IEEE 802.11

	802.11b	802.11a	802.11g	
Băng tần	2.4 GHz	5 GHz	2.4 GHz	
Số lượng kênh	3	Up to 23	3	
Truyền phát	Direct Sequence Spread Spectrum (DSSS)	Orthogonal Frequency Division Multiplexing (OFDM)	Direct Sequence Spread Spectrum (DSSS)	Orthogonal Frequency Division Multiplexing (OFDM)
Tốc độ [Mb/s]	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54

•Các tiêu chuẩn của IEEE định nghĩa trên lớp vật lý và phân lớp MAC của lớp liên kết dữ liệu theo tham chiếu trong mô hình OSI. Những chuẩn không dây 802.11 nguyên gốc đã được hoàn tất vào năm 1997. Vào năm 1999 các chuẩn này đã được điều chỉnh lại để tạo ra chuẩn 802.11a/b và sau đó một lần nữa được xác nhận lại ở chuẩn 802.11g vào năm 2003.

•1 kênh truyền và trải dữ liệu qua tất cả các tần số được định nghĩa trên kênh truyền đó.

•Chuẩn IEEE 802.11 chia băng tần ISM 2.4 GHz thành 14 kênh truyền, tuy nhiên một số cơ quan quản lý như FCC sẽ chỉ định kênh truyền nào được sử dụng, ví dụ như việc sử dụng kênh truyền từ số 1 đến 11 tại Mỹ. Mỗi kênh truyền trong dãy băng tần 2.4 GHz có băng thông là 22 MHz và chỉ cách nhau 5 MHz trên phổ tần số, do đó phổ của một kênh truyền sẽ bị chồng một phần với phổ của các kênh truyền liền trước và sau nó. Vì vậy, các kênh truyền cần được cách nhau qua 5 kênh truyền khác để không xảy ra hiện tượng chồng phổ này. Ví dụ, khi ta sử dụng 11 kênh truyền FCC, có 3 kênh truyền không trùng nhau là: 1, 6 và 11.

•Mạng không dây sử dụng cơ chế truyền bán song công (half-duplex), do vậy thông lượng truyền dẫn cơ bản chỉ vào khoản một nữa tốc độ dữ liệu. Do đó, muc tiêu chính của chuẩn 802.11b là nhằm đạt được tốc độ truyền cao hơn ở băng tần ISM 2.4 GHz để tăng thị phần khách hàng và khuyến khích sự chấo nhận của khách hàng của hệ thống chứng nhận Wi-Fi.

•Chuẩn 802.11b định nghĩa việc sử dụng DSSS với thuật toán điều chế mới CCK (Complementary Code Keying) cho một tốc độ truyền cao hơn là 5.5 và 11 Mbps trong khi đó vẫn giữ kiểu điều chế cũ Barker ở tốc độ 1 và 2 Mbps. Chuẩn 802.11b vẫn dùng băng tần ISM 2.4 GHz như chuẩn 802.11 trước đo, mục tiêu nhằm đưa vào chuẩn 802.11b khả năng tương thích lùi với chuẩn cũ 802.11 ở tốc độ truyền liên quan là 1 và 2 Mbps.

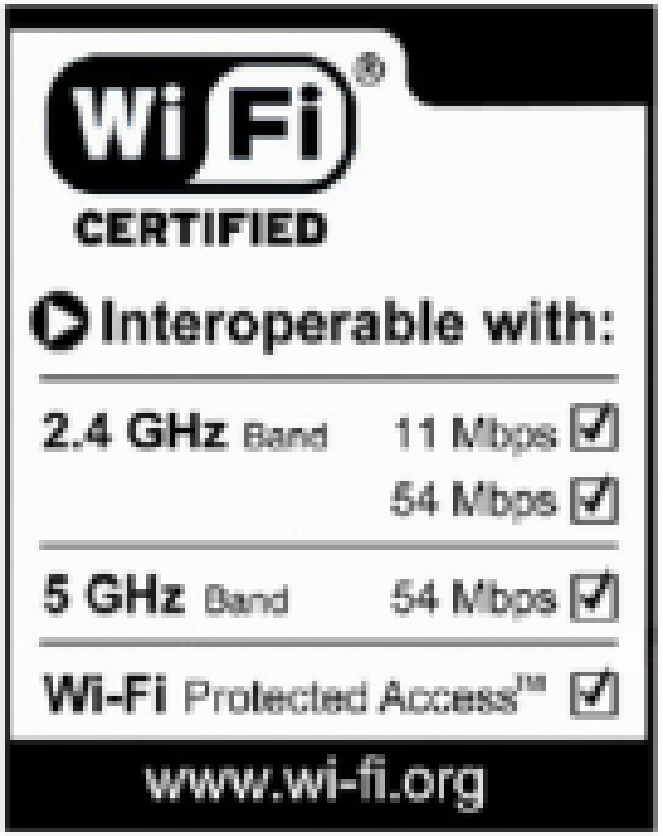
•IEEE đã phát triển một chuẩn khác là 802.11a. Động cơ thúc đẩy 802.11a là sử dụng một kiểu trải phổ (OFDM – Ortogonal Frequency Division Multiplexing) và công nghệ điều chế tín hiệu khác. 802.11a sử dụng dãy tần số rộng hơn trên dãy tần 5 GHz UNII.
Chuẩn 802.11a không được chấp nhận rộng rãi bởi vì các tài liệu để sản xuất các chip hỗ trợ chuẩn 802.11a ít phổ biến và điều này cũng tạo ra tiền đề dẫn đến giá thành cao trong việc phát triển hệ thống mạng sử dụng chuẩn 802.11a.

•Những chuẩn mới đây được phát triển bởi IEEE đều duy trì việc sử dụng chuẩn 802.11 MAC với tốc độ cao hơn trên băng tần ISM 2.4 GHz. IEEE 802.1g ra đời với sự cải thiện việc sử dụng kiểu trải phổ OFDM từ chuẩn 802.11a để đạt được tốc độ cao hơn và tương thích với chuẩn 802.11b sử dụng kiểu trải phổ DSSS. 802.11g hoạt động trên băng tần ISM 2.4 GHz. Tốc độ dữ liệu DSSS là 1, 2, 5.5 và 11Mbps và tốc độ dữ liệu OFDM là 6, 9, 12, 18, 24, 48 và 54Mbps đều được hỗ trợ bởi chuẩn 802.11g. IEEE chỉ yêu cầu trên 3 tốc độ dữ liệu bắt buộc là 6, 12 và 24Mbps mà sẽ không quan tâm đến các thiết bị hỗ trợ chuẩn 802.11a hay 802.11g OFDM.

7. Chứng nhận Wi-Fi

Wi-Fi Alliance **chứng nhận khả năng liên vận hành**
giữa các sản phẩm.

Các sản phẩm bao gồm 802.11a, 802.11b, 802.11g, dual-band
và kiểm tra về bảo mật.



Cisco là một thành viên sáng lập của Wi-Fi Alliance.
Những sảm phẩm được chứng nhận có thể tham khảo tại
http://www.wi-fi.com.

•Wi-Fi Alliance là tổ chức toàn cầu và phi lợi nhuận ra đời nhằm cải thiện sự phát triển và khả năng được chấp nhận của WLAN. Một trong những lợi điểm lớn nhất của Wi-Fi Alliance là nhằm đảm bảo khả năng liên vận hành giữa các sản phẩm 802.11 từ các hãng khác nhau bằng cách cung cấp các chứng nhận.
Những hãng được chứng nhận khả năng liên vận hành này mang lại khả năng chắc chắn cho người sử dụng các sản phẩm của họ. Chứng nhận Wi-Fi bao gồm trên cả 3 công nghệ của IEEE cũng như những chuẩn mới đang phát triển như chuẩn về bảo mật.

Wi-Fi Alliance cũng đã chứng nhận chuẩn bảo mật IEEE 802.11i là WPA (Wi-Fi Protected Access), và sau này được chỉnh sửa lại thành chứng nhận WPA2 sau bản ra đời cuối của chuẩn IEEE 802.11i.

Tóm tắt

Con người luôn mong đợi một kết nối tai mọi lúc mọi nơi, tuy nhiên lợi điểm lớn nhất của WLAN là giảm thiểu chi phí.

Cả WLAN và LAN đều dùng phương thức CSMA nhưng WLAN thì tránh còn LAN thì dùng phương pháp phát hiện đụng độ.

Tần số radio được bức xạ ra khỏi không trung nhờ anten, nơi nó có thể bị phản xạ, tán xạ, hay hấp thu.

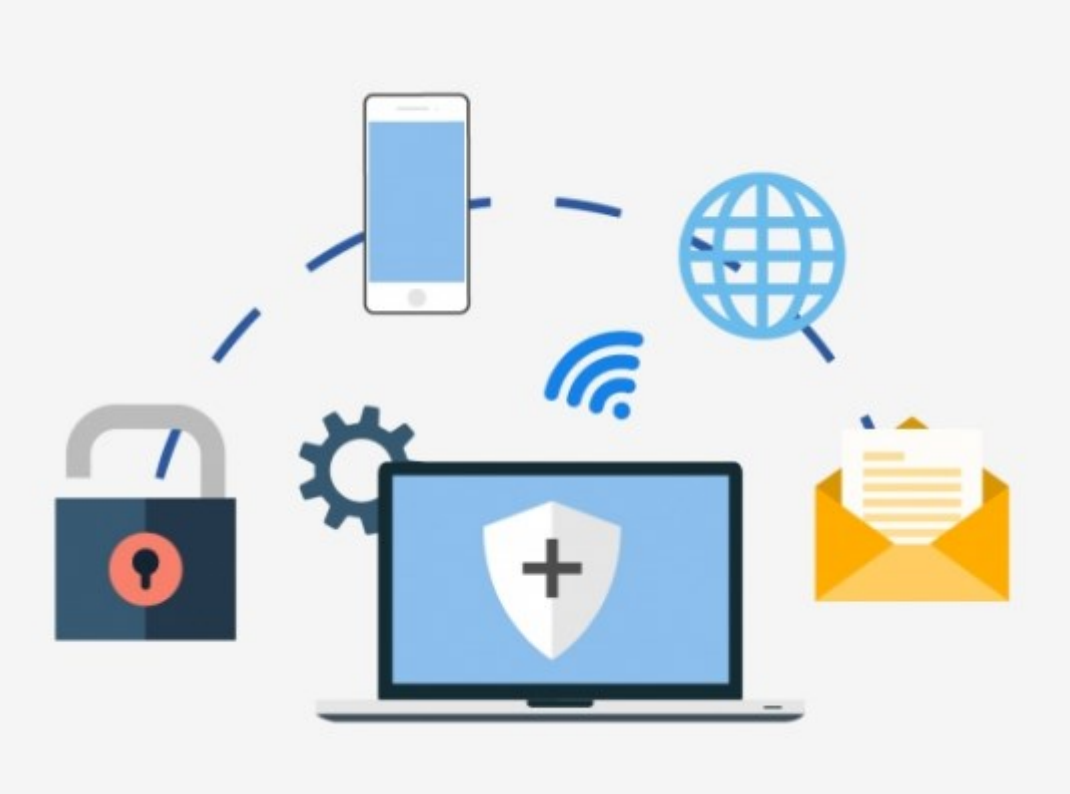
IEEE định nghĩa các chuẩn cho WLAN

Các tần số quy định cho WLAN bởi ITU là không cần đăng ký.

Chuẩn 802.11 là một bộ chuẩn định nghĩa về tần số và băng tần cho WLAN.

Một trong nhưng lợi điểm của Wi-Fi là mang lại chứng nhận sự tương thích giữa các sản phẩm 802.11

Chương 7:



Bảo mật mạng không dây

Mục tiêu

Sau khi hoàn tất bài học, SV có khả năng mô tả các vấn đề liên quan đến việc bảo mật trên môi trường WLAN và những tính năng sẵn sàng nhằm tăng khả năng bảo mật trên hệ thống mạng. Khả năng này được thể hiện qua các nhiệm vụ sau:

- Mô tả những nguy cơ trong các dịch vụ WLAN
- Mô tả những phương pháp làm giảm nhẹ các mối nguy hiểm trong dịch vụ WLAN
- Mô tả sự tiến triển của các công nghệ bảo mật trong WLAN
- Mô tả quá trình liên kết của các WLAN Client
- Mô tả quá trình tăng cường khả năng bảo mật của IEEE 802.1X
- Mô tả các kiểu WPA

Các mối đe dọa trên môi trường WLAN

"WAR DRIVERS"	HACKERS	EMPLOYEES
Find "Open" Networks; Use Them to Gain Free Internet Access	Exploit Weak Privacy Measures to View Sensitive WLAN Info and Even Break into WLANs	Plug Consumer-Grade APs/Gateways into Company Ethernet Ports to Create Own WLANs
	 THE WALL STREET JOURNAL. Hackers Can Penetrate Wireless Network	

Với những hệ thống IEEE 802.11a/b/g, chúng ta không thể tránh được khả năng hacker sẽ có thêm những hệ thống WLAN không bảo mật để lựa chọn. Ta có thể dùng khá nhiều những phần mềm mã nguồn mở để thu thập vào khai thác những điểm yếu trong phương thức bảo mật WEP (Wired Equivalent Privacy) của chuẩn 802.11.

Một số phầm mềm sniffer cho phép những kỹ sư mạng có thể thu thập dữ liệu để phân tích, kiểm tra và chỉnh sửa những vấn đề tồn tại trong hệ thống mạng của họ. Tuy nhiên cũng chính những phần mềm này có thể sẽ được sử dụng bởi những hacker để dò tìm và khai thác các lỗ hổng bảo mật trên mạng.

•Thuật ngữ “war driving” ban đầu được dùng với nghĩa là dùng một thiết bị quét số điện thoại di động (cell phone) nhằm tìm ra một số điện thoại nào đó để khai thác. Giờ đây, thuật ngữ này lại lại được hiểu như việc dùng một laptop như một Client để dò tìm một hệ thống WLAN 802.11b/g nào đó.
•Hầu hết các thiết bị được bán ra hiện nay đều được tính hợp sẵn khả năng WLAN. Người dùng đầu cuối thường thì cũng không chỉnh những thông số mặc định của nhà sản xuất hoặc chỉ sử dụng chuẩn bảo mất WEP, điều này không tối ưu hóa được quá trình bảo mật trong mạng WLAN. Với việc kích hoạt chuẩn mã hóa WEP cơ bản hay thậm chí là không bảo mật, việc bị thu thập và lấy đi một số thông tin nhạy cảm như thông tin đăng nhập, số tài khoản và một số thông tin riêng tư khác là hoàn toàn có thể.

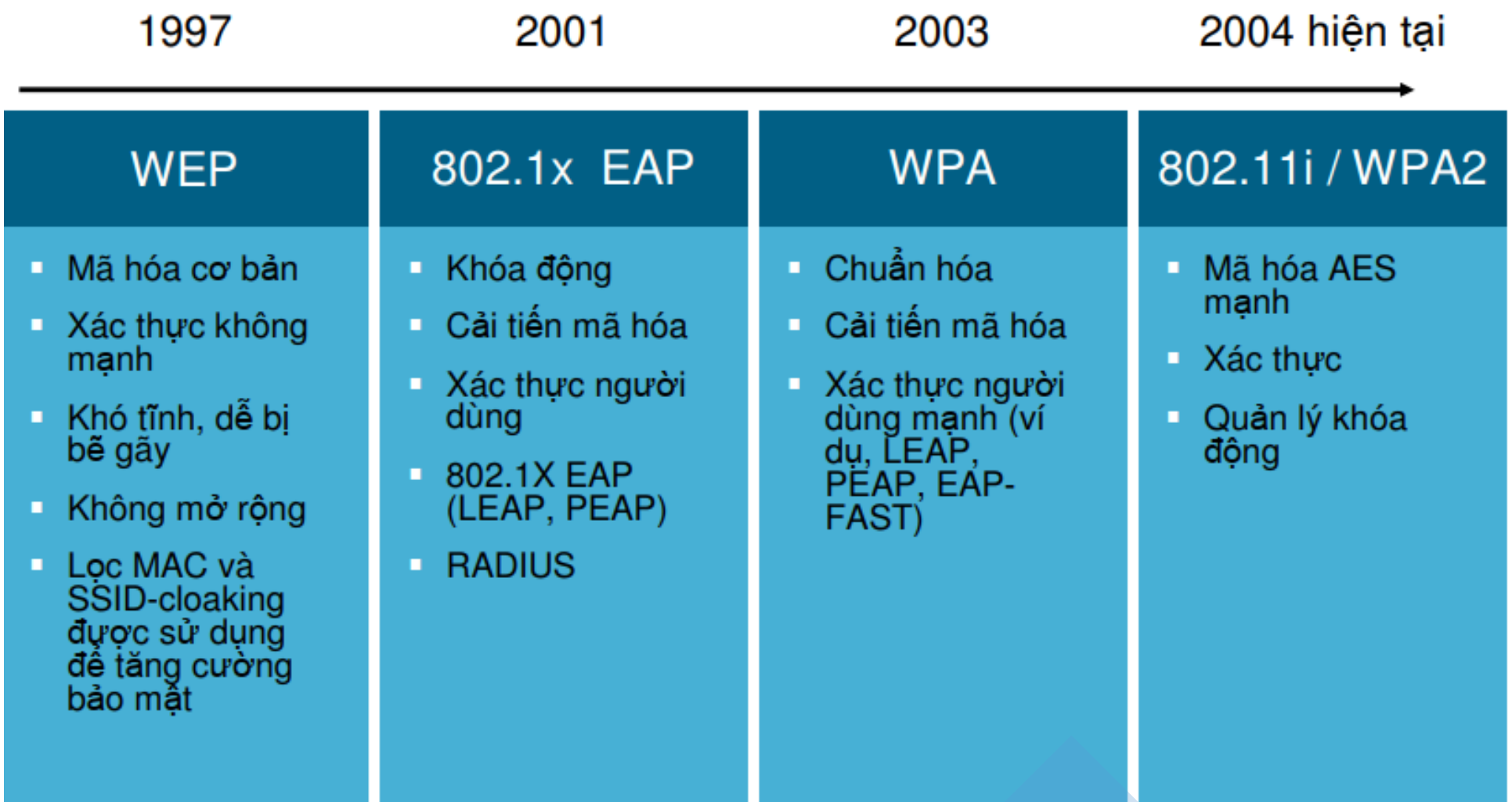
•Một rogue Access point là một Access point đặt trong môi trường mạng WLAN, Access point này được sử dụng để can thiệp vào sự vận hành bình thường của hệ thống mạng. Nếu một rogue Access point được thiết lập với từ khóa WEP đúng đang dùng trong mạng, dữ liệu phía người dùng có thể bị nghe lén. Một rogue Access point cũng có thể được cấu hình để cung cấp cho những người dùng không có quyền trên hệ thống những thông tin như địa chỉ MAC của các người dùng khác trong mạng cả mạng không dây và có dây, hay có thể thu thập và tạo ra những gói dữ liệu giả, hay thậm chí là chiếm quyến vào truy xuất vào các máy chủ. Kiểu thông dụng và đơn giản nhất để thiết lập một rogue Access point là được cài đặt bởi người dùng hợp lệ trong hệ thống. Những người dùng thiết lập các Access point để sử dụng cho mục tiêu gia đình trên hệ thống mạng doanh nghiệp mà không quan tâm đến vấn đề bảo mật sẽ tạo ra những nguy cơ bảo mật khá lớn.

Giảm nhẹ các mối đe dọa

Control and Integrity	Privacy and Confidentiality	Protection and Availability
Xác thực	Mã hóa	Ngăn ngừa xâm nhập (IPS)
Đảm bảo những client hợp lệ liên kết với những access point tin cậy.	Bảo vệ dữ liệu khi truyền và nhận.	Theo dõi và giảm nhẹ những truy xuất không được phép hay những truy xuất không hợp lệ.

•Chủ đề này mô tả quá trình làm giảm nhẹ các mối nguy hiểm về vấn đề bảo mật trên hệ thống WLAN
•Để bảo vệ hệ thống WLAN, yêu cầu phải thực hiện thông qua các bước sau:
- Xác thực người dùng, mục tiêu nhằm đảm bảo những người dùng hợp pháp có thể truy xuất vào hệ thống mạng thông qua những Access point tin cậy.
- Mã hóa, mục tiêu nhằm tạo sự riêng tư và bí mật
- Triển khai hệ thống phát hiện xâm nhập (IDS – Intrusion Detection System) và hệ thống ngăn chặn xâm nhập (IPS – Intrusion Prevention System) để bảo vệ hệ thống mạng trước những nguy cơ bảo mật
•Một giải pháp cơ bản cho vấn đề bảo mật mạng không dây là triển khai tính năng xác thực và mã hóa để bảo vệ dữ liệu. Hai giải pháp này có thể được triển khai theo từng cấp độ tùy thuộc vào quy mô hệ thống mạng. Những hệ thống mạng doanh nghiệp lớn hơn cần có thêm những cấp độ bảo mật được mang lại bởi những thiết bị như IPS. Hiện tại IPS không những có khả năng phát hiện các cuộc tấn công vào mạng không dây mà còn có thể bảo vệ hệ thống mạng trước những người dùng không hợp pháp.

Quá trình phát triển các chuẩn bảo mật trên mạng LAN không dây



•Hầu hết ngay khi các chuẩn bảo mật mới ra đời, các hacker sẽ cố gắng khai thác những điểm yếu trên những chuẩn này. Để chống lại quá trình đó, các chuẩn bảo mật lại liên tục được nâng cấp để tăng cường khả năng bảo mật. Chủ đề này sẽ mô tả quá trình phát triển của vấn đề bảo mật trong mạng WLAN.
•Ban đầu, bảo mật trong môi trường WLAN được định nghĩa dựa trên từ khóa WEP 64 bit cho cả 2 tiến trình mã hóa và xác thực. Từ khóa WEP 64 bit bao gồm 40 bit cho từ khóa thực sự và 24 bit cho Vector khởi tạo. Phương pháp xác thực này thực sự không mạnh và thậm chí có thể bị dàn xếp từ khóa giữa các người dùng. Bởi vì các từ khóa được quản lý một cách thủ công do vậy phương pháp này không thể mở rộng một các linh động trên các hệ thống mạng lớn được. Các công ty cố gắng khắc phục yếu điểm này với một số kỹ thuật SSID và lọc địa chỉ MAC.
•SSID là tên dùng để xác định hệ thống mạng WLAN và là thông số có thể cấu hình được. Cả Client và Access point phải cùng sử dụng giống nhau giá trị SSID này để giao tiếp. Nếu Access point được cấu hình để broadcast giá trị SSID trên toàn hệ thống mạng, Client sẽ liên kết với Access point đó bằng giá trị SSID nhận được. Access point có thể được cấu hình để không broadcast giá trị SSID ra ngoài (SSID cloaking), điều này mang lại cấp độ bảo mật đầu tiên trên hệ thống mạng WLAN bởi các hacker sẽ gặp khó khăn hơn để xác định sự tồn tại của Access point này.

được cấu hình bằng tay trên Access point để cho phép hoặc không cho phép dựa trên địa chỉ vật lý của các client. Tuy nhiên địa chỉ MAC có thể dễ dàng bị giả, do đó phương pháp lọc địa chỉ MAC không còn được xem là một đặc tính bảo mật nữa.

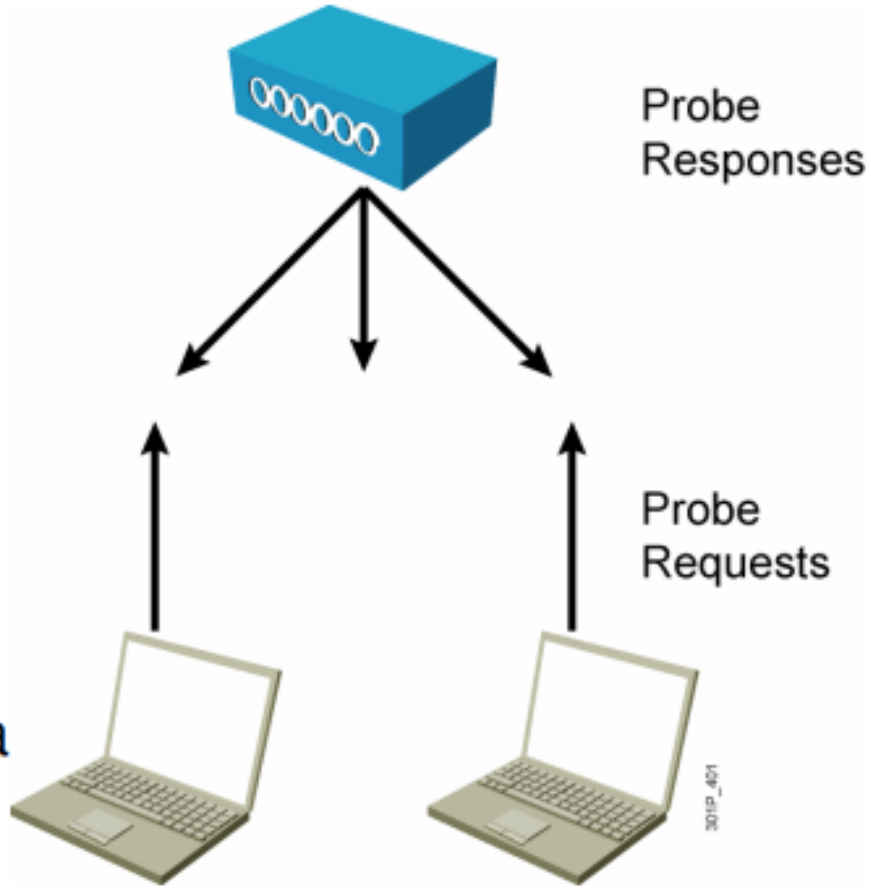
•Trong thời gian mà ủy ban 802.11 bắt đầu tiến trình nâng cấp khả năng bảo mật trên hệ thống WLAN, các hãng độc lập đã sớm triển khai các chuẩn bảo mật trên hệ thống mạng WLAN của họ. Cisco đã sớm phát triển chuẩn mã hóa WEP trên việc cải thiện thuật toán RC4. Cisco thực thi chuẩn TKIP (Temporal Key Integrity Protocol) để mã hóa trên từng gói dữ liệu và Cisco MIC (Message Integrity Check) để bảo vệ từ khóa WEP. Cisco cũng đã dùng chuẩn xác thực 802.11x từ môi trường dây dẫn sang môi trường không dây và tự động hóa các từ khóa sử dụng bằng Cisco LEAP (Lightweight Extensible Authentication Protocol) nhằm tập trung hóa cơ sở dữ liệu.

•Ngay sau khi Cisco triển khai các chuẩn bảo mật trên mạng WLAN, Wi-Fi Alliance đã đưa ra chuẩn WPA (Wi-Fi Protected Access) như một chuẩn tạm thời cho một phần của chuẩn bảo mật 802.11i đang được mong đợi dùng chuẩn xác thực 802.1x và cải thiện quá trình mã hóa WEP. Chuẩn TKIP mới ra đời tương tự như Cisco TKIP và Cisco MIC nhưng các chuẩn này không tương thích với nhau.

•Ngày nay, 802.11i đã được phê chuẩn và chuẩn bảo mật AES (Advanced Encryption Standard) đã thay thế WEP và được xem như một chuẩn bảo mật nhất để mã hóa dữ liệu. Những hệ thống IDS trên WLAN cũng được triển khai để xác định những cuộc tấn công và bảo vệ hệ thống mạng. Wi-Fi Alliance chứng nhận các thiết bị 802.11i dưới

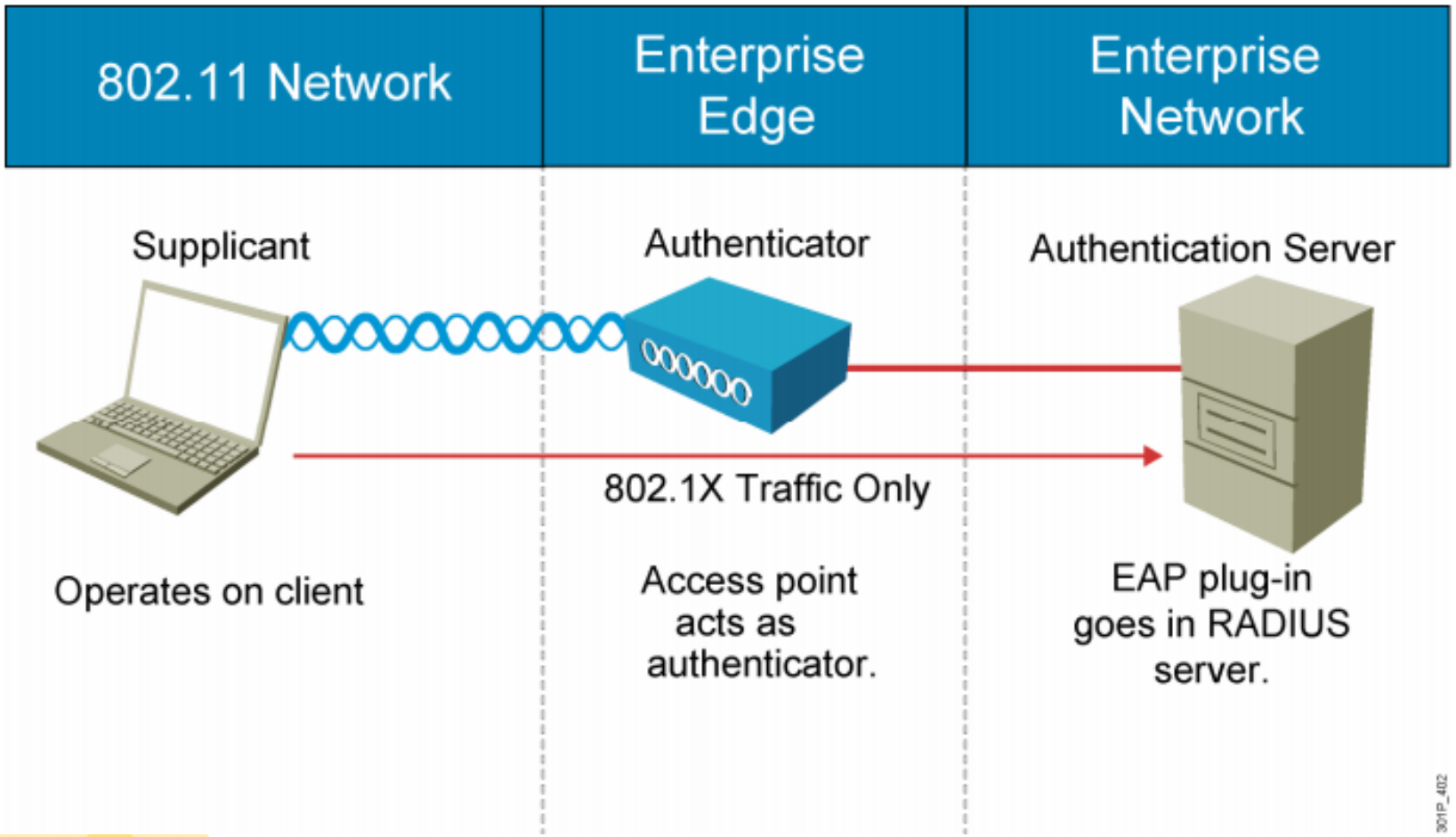
Quá trình liên kết Client không dây

- Access point gởi ra các beacon thông báo SSID, tốc độ và các thông tin khác.
- Client dò tất cả các kênh.
- Client lắng nghe beacon và phản hồi với access point.
- Client sẽ liên kết với access point nào có sóng mạnh nhất.
- Client vẫn lắng nghe các beacon khác để có thể thực hiện tiến trình roaming
- Trong suốt quá trình liên kết, SSID, địa chỉ MAC và các thông số bảo mật sẽ được gửi đến access point.



Trong quá trình liên kết với Access point, các Access point sẽ gởi ra tín hiệu beacon để thông báo một số thông tin bao gồm SSID, tốc độ dữ liệu, và các thông tin khác. Các Client quét tất cả kênh truyền, lắng nghe các beacon và phản hồi lại cho các Access point. Client sẽ liên kết với Access point nào có tín hiệu sóng mạnh nhất. Nếu tín hiệu sóng yếu đi, client sẽ lập lại quá trình quét để liên kết với Access point khác (tiến trình này được gọi là roaming). Trong suốt quá trình liên kết, các thông số SSID, địa chỉ MAC và các thông số bảo mật sẽ được gởi lên Access point từ client và các Access point sẽ kiểm tra các thông số này.
Quá trình liên kết từ client đến Access point thực sự chỉ là quá trình thứ 2 trong tiến trình 2 bước. Tiến trình đầu tiên là xác thực, kế đến là liên kết, các client phải trải qua cả 2 tiến trình này để có thể trao đổi dữ liệu với các client khác thông qua Access point. Quá trình xác thực client xảy ra tại tiến trình đầu tiên không giống như quá trình xác thực trên mạng (nhập vào tên người dùng và mật khẩu để truy cập vào mạng). Quá trình xác thực client ở đây chỉ đơn giản là bước đầu tiên (kế theo là quá trình liên kết) giữa client và Access point để có thể thiết lập kết nối. Chuẩn 802.11 chỉ đưa ra 2 phương pháp để xác thực, xác thực mở (open authentication) và xác thực dùng khóa chia sẻ (shared key authentication). Chứng thực mở đơn thuần chỉ là quá trình trao đổi 4 gói dữ liệu hello ban đầu mà không cần phải kiểm tra bởi client hay Access point nhằm cho phép kết nối được dễ dàng thực hiện.

Cách vận hành của 802.1X trên mạng LAN không dây



•Access point đóng vai trò như người yêu cầu xác thực cho phép client thực hiện liên kết qua chuẩn xác thực mở. Access point sẽ đóng gói tất cả dữ liệu 802.11x yêu cầu xác thực và gởi đến server xác thực. Tất cả các các dữ liệu khác truy xuất vào tài nguyên mạng sẽ bị khóa lại.
•Sau khi nhận được dữ liệu trả về từ RADIUS server, Access point sẽ đóng gói lại và chuyển về client. Mặc dầu tiến trình xác thực này nhằm để xác định người dùng hợp lệ trên hệ thống mạng nhưng nó cũng có nghĩa là các client cũng đang xác thực server để đảm bảo client không truy xuất vào một server giả mạo.
•Trong khi một hệ thống mạng lớn sử dụng một server xác thực tập trung, các mạng doanh nghiệp nhỏ sẽ đơn thuần chỉ dùng Access point với từ khóa chia sẽ như một server để xác thực cho các client.

Mode WPA và WPA2

	WPA	WPA2
Enterprise mode (Kinh doanh, giáo dục, chính phủ)	Xác thực: IEEE 802.1X/EAP Mã hóa: TKIP/MIC	Xác thực : IEEE 802.1X/EAP Mã hóa: AES-CCMP
Personal mode (SOHO, sử dụng tại nhà hay cá nhân)	Xác thực: PSK Mã hóa: TKIP/MIC	Xác thực: PSK Mã hóa: AES-CCMP

•Chuẩn WPA cung cấp khả năng xác thực được hỗ trợ thông qua chuẩn 802.1x và khóa chia sẻ (Pre-shared Key). WPA cung cấp khả năng mã hóa được hỗ trợ thông qua chuẩn TKIP. Chuẩn TKIP bao gồm MIC và PPK (Per-packet Keying) sử dụng thông qua “initialization vector hashing” và broadcast key rotation”.
•Khi so sánh với WPA, quá trình xác thực của WPA2 thì vẫn không thay đổi nhưng quá trình mã hóa được thực hiện bởi AES với giao thức AES-CCMP (AES Counter with CBC MAC Protocol).
•**Enterprise mode**
“Enterprise mode” là thuật ngữ dành cho những sản phẩm đã được kiểm tra về khả năng liên vận hành ở cả 2 kiểu PSK và 802.1X/ EAP cho chức năng xác thực. Chuẩn 802.1X yêu cầu phải có một AAA server khi được sử dụng. “Enterprise mode” được đưa ra nhằm đáp ứng nhu cầu trong môi trường mạng doanh nghiệp.
•**Personal mode**
“Personal mode” là thuật ngữ được sử dụng cho những sản phẩm đã được kiểm tra về khả năng liên vận hành duy nhất kiểu PSK cho chức năng xác thực. Quá trình này yêu cấu cấu hình PSK bằng tay trên cả Access point và client. PSK xác thực người dùng thông qua mật mã hoặc mã định danh trên cả client và Access point. Trong trường hợp này không cần phải sử dụng đến server xác thực.
“Personal mode” được đưa ra nhằm đáp ứng nhu cầu trong môi trường SOHO.

Tóm tắt

Một điều chắc chắn là các hacker sẽ xâm nhập vào mạng WLAN không bảo mật.

Giải pháp cơ bản nhất để bảo mật WLAN là xác thực người dùng và mã hóa dữ liệu.

Những chuẩn WLAN bao gồm các chuẩn bảo mật.

– WEP
– 802.1x EAP
– WPA
– 802.11i/WPA2

Access point gởi ra các beacon thông báo SSID, tốc độ và các thông tin khácVới chuẩn 802.1X access point đóng vai trò như một người đòi xác thực.

WPA cung cấp xác thực qua IEEE 802.1X và PSK và bao gồm hai mode

– Enterprise mode
– Personal mode

Mạng không dây cục bộ (Wireless LANs)

Mục tiêu

Sau khi hoàn tất bài học, bạn có khả năng mô tả những nhân tố ảnh hưởng đến
việc thực thi mạng WLAN thông qua các nhiệm vụ sau:

- Mô tả mô hình IEEE 802.11
- Mô tả dịch vụ WLAN BSA
- Mô tả ảnh hưởng của khoản cách và tốc độ trên dịch vụ WLAN
- Mô tả các nhân tố cần quan tâm trong việc thực thi triển khai các Access point
- Mô tả cách triển khai mạng WLAN cơ bản
- Mô tả các phương pháp để đưa mạng không dây vào laptop
- Mô tả các vấn đề phổ biến gặp phải và phương pháp khắc phục trên mạng WLAN

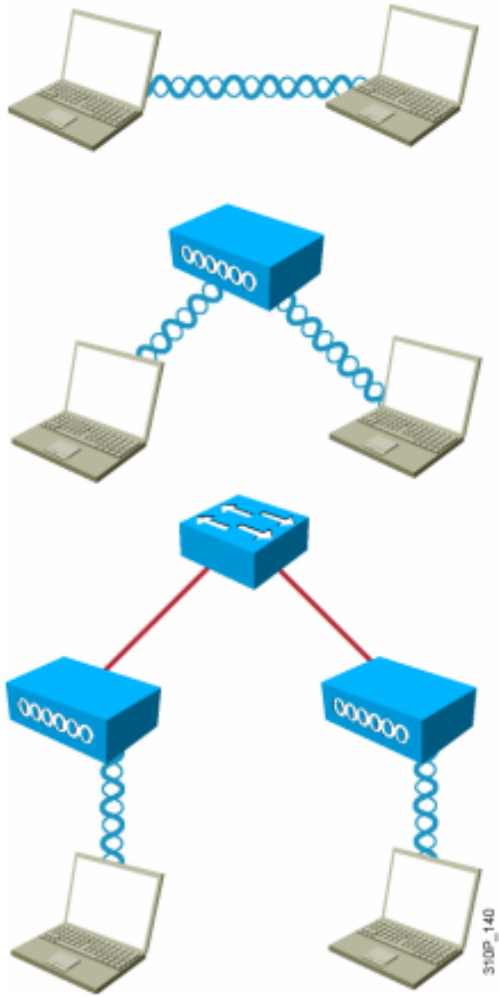
Xây dựng khối mô hình 802.11

Ad hoc mode:

- Independent Basic Service Set (IBSS)
  - Các client di động kết nối mà không cần access point ở giữa.

Infrastructure mode:

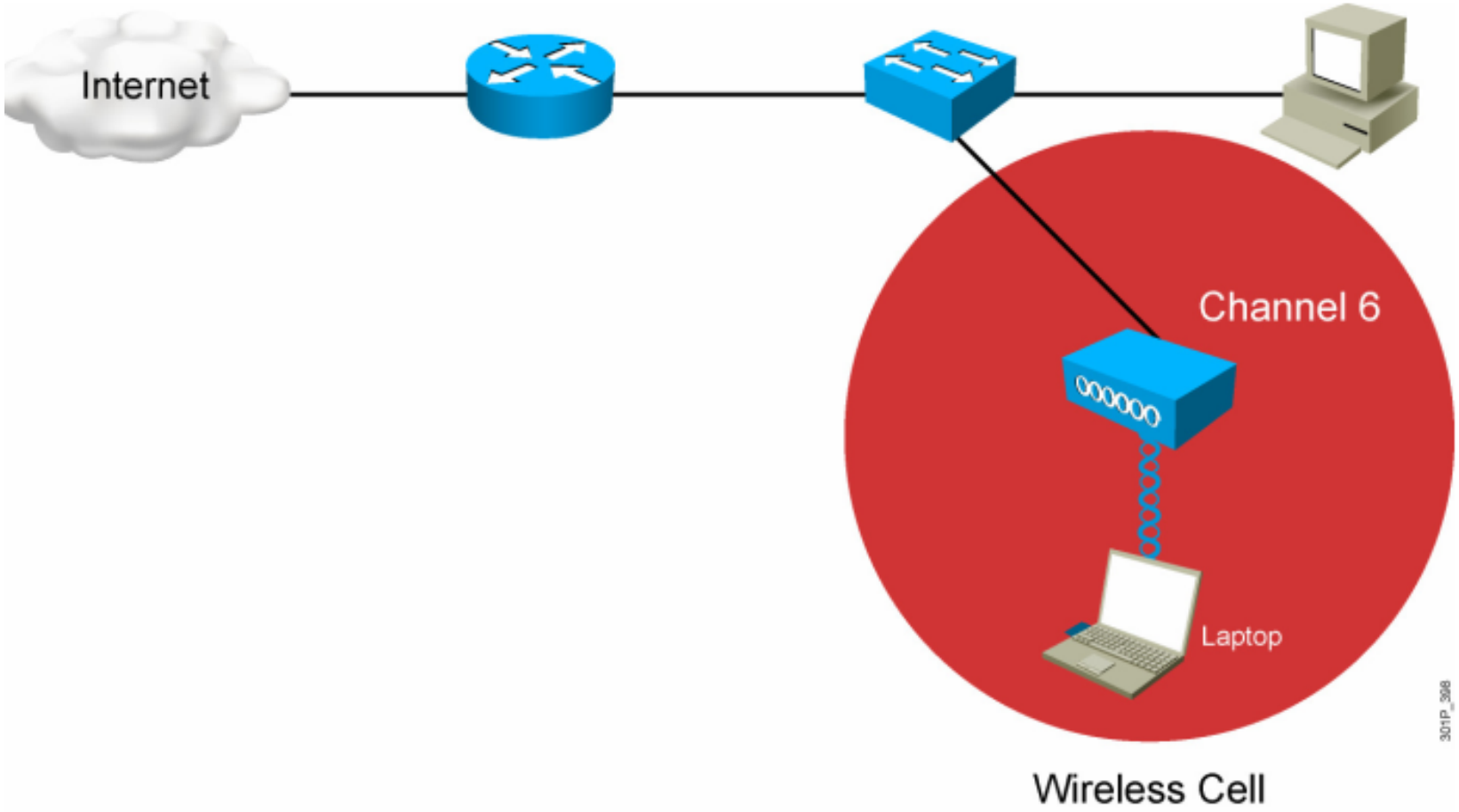
- Basic Service Set (BSS)
  - Các client di động dùng một access point để giao tiếp với nhau và với mạng có dây.
- Extended Service Set (ESS):
  - Hai hay nhiều kiểu BSS được kết nối với nhau .



•Chuẩn 802.11 cung cấp một số mô hình (mode) có thể sử dụng để xây dựng các khối mạng WLAN
•Ad hoc mode: IBSS (Independent Basic Service Set) là mô hình ad hoc mode. Các client di động kết gắng trực tiếp với nhau mà không thông qua thiết bị Access point trung gian ở giữa. Một số hệ điều hành như Windows cũng đã giúp cho mô hình peer-to-peer như thế này được dễ dàng thiết lập hơn. Kiểu thiết lập này cho thường được sử dụng cho các văn phòng nhỏ, nơi mà các laptop có thể nối không dây với các PC hay các laptop khác để đơn thuần là chia sẻ dữ liệu. Môi trường này có tầm phủ giới hạn, tất cả mọi người đều phải thấy nhau. Một yếu điểm trong môi trường này là khó khăn trong vấn đề bảo mật.
•Infrastructure mode: trong mode này, các client sẽ nối thông qua Access point. Infrastructure mode tồn tại dưới 2 hình thức:
- BSS (Basic Service Set): Trong mode này, tất cả các client chỉ sử dụng một Access point để nối với nhau hoặc để nối về mạng có dây. BSSID (Basic Service Set Identifier) là địa chỉ MAC của card radio trên Access point trong mode này. Trong khi BSS là mode cơ bản để xây dựng mô hình WLAN và BSS Access point được duy nhất xác định thông qua BSSID thì bản thân nguyên cả hệ thống WLAN sẽ dùng SSID để quảng bá sụ tồn tại của nó với các client. SSID được xem như tên của hệ thống WLAN, có thể được cấu bởi người dùng và được tạo từ 32 ký tự có phân biệt chữ hoa và chữ thường.

- ESS (Extended Service Set): Là hệ thống mạng WLAN được mở rộng
với hai hay nhiều hơn các BSS gắn kết với nhau thông qua hệ thống
kết nối trung gian hoặc môi trường dây dẫn. ESS thông thường cũng
sử dụng chung giá trị SSID để cung cấp khả năng roaming giữa Access
point này và Access point khác mà người dùng không cần phải thiết lập
lại cấu hình.
•Trên là những mô hình chuẩn được đưa ra bởi 802.11, tuy nhiên các
mô hỉn khác như repeater, bridges và workgroup bridge là những mô
hình mở rộng được đưa ra từ các hãng.

Mô hình BSA – Tầm phủ cơ bản



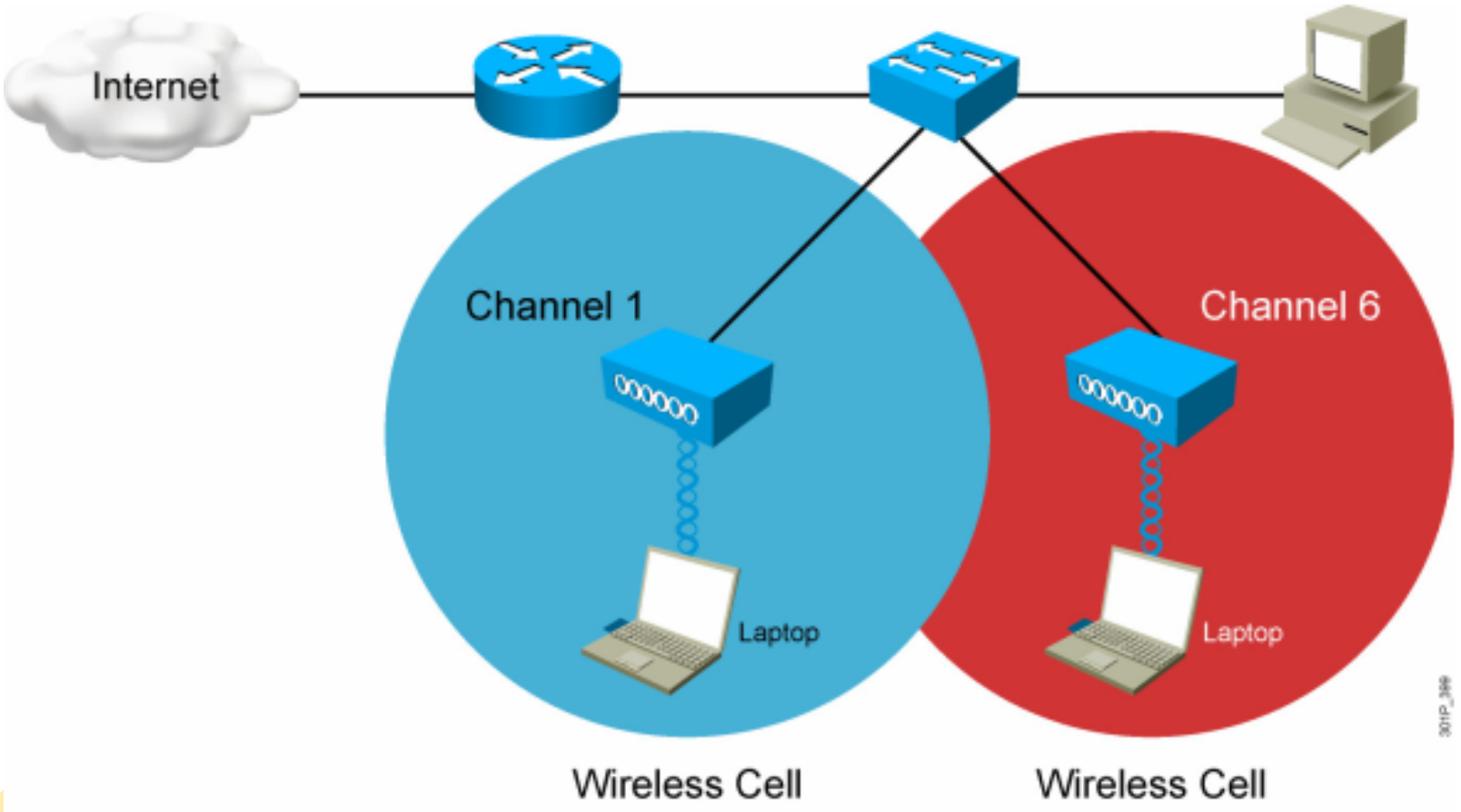
BSA (Basic Service Area) là một khu vực vật lý của tầm phủ sóng sóng radio được cung cấp bởi Access point trong mode BSS. Diện tích khu vực này tùy thuộc vào năng lượng sóng radio mà Access point phát ra. Những năng lượng này lại phục thuộc vào các yếu tố như công suất phát, loại anten, và các vật thể xung quanh ảnh hưởng đến sóng radio. Khu vực phủ sóng như vậy được biết đến như một cell. Vậy khi BSS là kiểu mô hình thì BSA lại được biết đến như một dạng vùng phủ sóng và hai thuật ngữ này có thể được dùng qua lại trong một khái niệm không dây cơ bản.

Access point sẽ được gắn vào backbone mạng Ethernet và giao tiếp với tất cả các thiết bị không dây khác trong khu vực cell. Access point được xem là master trong cell và điều khiển tất cả các lưu lượng luồng dữ liệu đến và từ hệ thống mạng. Các thiết bị từ xa sẽ không giao tiếp trực tiếp với nhau mà chỉ giao tiếp trực tiếp với Access point. Access point có thể được điều chỉnh về thông số kênh truyền và tên SSID duy nhất trên hệ thống mạng.

Access point broadcast tên của hệ thống mạng trong cell thông qua giá trị SSID qua các beacon. Các beacon được Access point broadcast nhằm thông báo sự tồn tại của dịch vụ không dây. Các giá trị SSID được sử dụng để cách ly về mặt luận lý các hệ thống WLAN. Giá trị này phải hoàn toàn giống nhau giữa Access point và các client. Tuy nhiên, các client có thể cấu hình không cần giá trị SSID (SSID rỗng) để có thể phát hiện tất cả các Access point và nhận giá trị SSID của một Access point cụ thể nào đó.

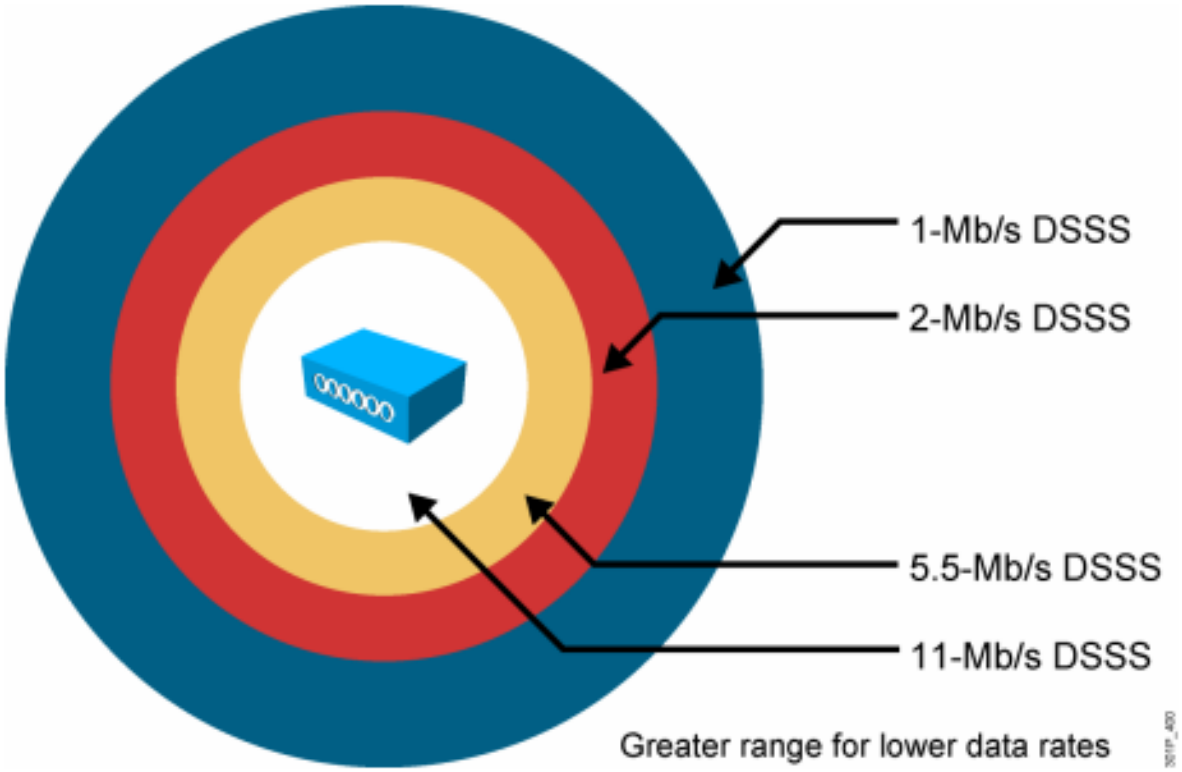
Một ví dụ phổ biến của tiến trình dò tìm là quá trình dò tìm được sử
dụng bởi ứng dụng tích hợp sẵn WZC (Wireless Zero Configuration) khi
mà một laptop được sử dụng tại một vị trí mới. Người dùng sẽ được
hiển thị thông tin của dịch vụ không dây mới và được yêu cầu để kết
nối hoặc được cung cấp các thông số về từ khóa để truy cập. Quá trình
broadcast SSID có thể được ngưng kích hoạt trên Access point, nhưng
sẽ làm người dùng không còn thấy được SSID trong beacon nữa.

Mô hình ESA – Tầm phủ mở rộng



•Nếu một cell không cung cấp đủ vùng phủ sóng, có thể đưa thêm bất kỳ
các cell nào vào hệ thống mạng để mở rộng tầm phủ sóng. Tầm phủ
sóng được tạo từ nhiều cell được gọi là ESA (Extended Service Area).
•Các chuẩn khuyến nghị rằng giữa các cell trong ESA nên phủ lên nhau
khoảng từ 10% đến 15% để giúp người dùng có khả năng roaming mà
không mất sóng. Trong hệ thống mạng không dây sử dụng cho voice, độ
phủ lấp giữa các cell từ 15% đến 20% được khuyến nghị. Các cell nằm
tại biên nên được thiết lập hoạt động tại những tần số không chồng lấp
nhau được đat dược khả năng vận hành tốt nhất.

Tốc độ dữ liệu 802.11b



•Các client WLAN có khả năng d5ich chuyển tốc độ khi di chuyển. Kỹ thuật này cho phép cùng một client hoạt động ở tốc độ 11 Mbps chuyển sang tốc độ 5Mbps sau đó đến 2Mbps và cuối cùng vẫn có thể giao tiếp ở vùng ngoài cùng với tốc độ 1Mbps. Quá trình dịch chuyển tốc độ này xảy ra mà không làm mất đi kết nối mà người dùng đang có và người dùng không phải can thiệp gì vào quá trình này. Sự dịch chuyển tốc độ xảy ra trên từng quá trình truyền dẫn một, do đó Access point có khả năng hỗ trợ nhiều client hoạt động tại nhiều tốc độ khác nhau tùy vào vị trí đang có của từng client.
•Tốc độ truyền cao yêu cầu tín hiệu mạnh tại ngay đầu nhận, do vậy tốc độ càng thấp thì tầm truyền càng xa.
•Các client không dây luôn luôn cố gắng giao tiếp với tốc độ truyền cao nhất.
•Các client sẽ chỉ giảm tốc độ nếu xảy ra lỗi trong quá trình truyền.
•Quá trình này cung cấp thông lượng truyền dẫn tối đa trong một cell mạng không dây. Hình trên biểu diễn cho chuẩn 802.11b, khái niệm này cũng tượng tự cho chuẩn 802.11a và 802.11g.

Cấu hình Access Point

Thông số cơ bản:

Địa chỉ IP, Subnet mask, và default gateway
Giao thức không dây (chỉ 802.11g, 802.11a/b/g, 802.11a)
Điều chỉnh kênh truyền – kênh 1, 6, hay 11
Điều chỉnh công suất, hay thay thế anten

Thông số bảo mật:

Xác định mạng qua SSID
Phương thức xác thực, thường là WPA hay WPA2 PSK
Phương pháp mã hóa, thường là TKIP, hay AES nếu phần cứng
hỗ trợ

•Access point có thể được cấu hình dùng giao diện dòng lệnh (CLI) hay bằng phương pháp phổ biến hơn là giao diện đồ họa (GUI). Tuy nhiên cách cấu hình Acess point ở những thông số cơ cản là giống nhau cho cả hai phương pháp. Các thông số cơ bãn để cấu hình Access point bao gồm cấu hình SSID, kênh truyền RF đi kèm với các thông số tùy chọn như công suất, xác thực,… Các client cần ít thông số cấu hình hơn vì các card không dây có thể quét tất cả các tần số có thể (những card thuộc chuẩn 802.11b.g không thể quét được sóng ở tần số 5GHz) để định ra nơi cung cấp dịch vụ. Thường thì các client sẽ khởi tạo kết nối với giá trị SSID rỗng. Do vậy với thiết kế của chuẩn 802.11b, nếu sử dụng chuẩn xác thực mở, quá trình sẽ là “plug-and-play”. Khi chuẩn bảo mật được cấu hình dùng kiểu từ khóa chia sẻ (PSK) hay cũ hơn là chuẩn WEP hoặc như hiện tại ở chuẩn WPA, các từ mã buộc phải khớp giữa hai bên (Access point và client) để có thể giao tiếp.
•Tùy vào phần cứng của Access point được lựa chọn mà Access point có thể hoạt động trên cả hai băng tần ISM 2.4 GHz và UNII 5 GHz với sự hỗ trợ của cả ba chuẩn 802.11a/b/g. Khi các client chuẩn 802.11b sử dụng chung với các client chuẩn 802.11g, thông lượng truyền dữ liệu sẽ giảm bởi vì Access point phải duy trì thực thi giao thức RTS/CTS. Do vậy một môi trường chỉ có một loại client sẽ thông lượng truyề dữ liệu sẽ nhanh hơn.
•Sau khi cấu hình cơ bản các thông số không dây cho Access point, một số thông số cơ bản khác liên quan đến môi trường dây dẫn cũng phải được thiết lập như default router hay DHCP server. Với một hệ thống mạng LAN tồn tại sẵn, ta phải có một giá trị default router để ra

Access point đơn giản sẽ đóng vai trò trung gian chuyển các giá trị này
cho các client không dây khi kết nối vào. Và vì hệ thống được mở rộng
thêm như, do vậy phải đảm bảo tầm địa chỉ DHCP đủ rộng để cấp cho
tất cả các client.

Cá bước cấu hình hệ thống mạng không dây

Bước 1: Kiểm tra sự vận hành mạng có dây, DHCP, ISP.
Bước 2: Cài đặt access point.
Bước 3: Cấu hình access point – SSID, không bảo mật.
Bước 4: Cài đặt một client không dây – không bảo mậ.
Bước 5: Kiểm tra sự vận hành mạng.
Bước 6: Cấu hình bảo mật – WPA với PSK.
Bước 7: Kiểm tra sự vận hành mạng

•Quá trình cơ bản để thực thi mộ hệ thống mạng không dây (cũng như
với tất cả các hệ thống mạng cơ bản khác) là từng bước cấu hình và
kiểm tra.
•Trước khi thực hiện bất kỳ cấu hình nào về yếu tố không dây, kiểm tra
hệ thống mạng có sẵn và các thức truy cập vào Internet cho các client
trong mạng dùng dây.Thực thi mạng không dây với chỉ một Access
point, một client và không có bất kỳ chuẩn bảo mật nào. Kiểm tra rằng
client có thể nhận IP từ DHCP server, ping được default gateway và có
thể truy cập Internet. Cuối cùng, cấu hình Access point với các chuẩn
bảo mật WPA. Chỉ sử dụng WEP trong trường hợp phần cứng không
hỗ trợ WPA.

Các client không dây

Wireless Zero Configuration (WZC):

- Mặc định trên hệ điều hành Windows
- Những tính năng hạn chế cho PSK
- Kiểm tra client dùng đúng kiểu mã hóa và password

Cisco Compatible Extensions Program

- Tăng tốc những đặc tính triển khai cho các client bên thứ 3
- Được triển khia bởi nhiều hãng khác nhau

Cisco Secure Services Client

- Chức năng client đầy đủ cho doanh nghiệp
- Cho mạng có dây và không dây

và mã hóa dữ
liệu. Những laptop mới hiện giờ có nhiều hình thức khác nhau giúp truy cập
vào mạng không dây. Những hệ điều hành mới của Windows được trang bị
dịch vụ WZC cho phép khả năng “plug-and-play” bằng cách tìm ra các SSID
và người dùng chỉ đơn giản nhập vào các từ khóa trong trường hợp sử
dụng PSK, WEP hay WPA. Các tính năng cơ bản của WZC thích hợp cho
các giải pháp văn phòng nhỏ.
•Một số hệ thống mạng lớn yêu cầu các client đầu cuối có nhiều tính năng
hơn là những tính năng được cung cấp sẵn trong hệ điều hành. Bảng sau
đây đã tóm tắt một số phiên bản và tính năng mà Cisco đưa thêm vào trong
chương trình chứng nhận của mình từ năm 2000:
Version 1 (Security): Wi-Fi compliant, 802.1x, LEAP, Cisco Key Integrity
Protocol.
Version 2 (Scaling): WPA, access point assisted roaming.
Version 3 (Performance and Security): WPA2, Wi-Fi Multimedia (WMM)

•Cho đến khi Cisco mang lại các tính năng đầy đủ gọi là Cisco Secure
Service Client cho cả các client trong mạng không dây và có dây thì
trước đó quản lý các client không dây và có dây theo những bộ chuẩn
khác nhau. Lơi ích cho người dùng là chỉ sử dụng một chương trình
client duy nhất cho vấn đề kết nối và bảo mật trên mạng không dây và
có dây

Sửa lỗi mạng không dây

Đặt access point ngay tại vị trí trung tâm.
Tránh đặt gần các vật thể kim loại.
Kiểm tra kết nối khi chưa kích hoạt tính năng bảo mật.
Tránh nhiễu sóng với các thiết bị khác (bluetooth, viba,…)
Nếu cầm phát sóng trong phạm vi rộng, cần dùng nhiều hơn một
access point.
Đảm bảo rằng access point sử dụng kênh truyền duy nhất, không
trùng kênh với các thiết bị gầm đó.

radio. Bắt đầu bằng quá trình kiểm tra cơ sở hạ tầng và các dịch vụ
trên môi trường dây dẫn. Đảm bảo rằng các máy trong môi trường
Ethernet có khả năng nhận đại chỉ từ DHCP server và có thể truy cập
Internet.
•Kế tiếp, thực hiện kết nối giữa Access point và client tại cùng một địa
điểm nhằm kiểm tra cấu hình và loại trừ các vấn đề về sóng radio. Luôn
luôn bắt đầu từ chuẩn xác thực mở để thiết lập kết nối. Sau đó thực thi
các chuẩn bảo mật mong muốn.
•Nếu các client có thể kết nối tại điểm này, vấn đề còn lại chỉ liên quan
đến các vấn đề về sóng radio. Trước tiên phải xem xét thử có bất kỳ
vật thể kim loại nào đặt trong khu vực phát sóng hay. Nếu có, ta có thể
chuyển vật thể đi hoặc thay đổi vị trí của Access point. Nếu khoảng
cách truyền là quá lớn, lưu ý là phải dùng thêm các Access point khác
với cùng giá trị SSID nhưng truyền với tần số khác nhau .

•Nếu khả năng vận hành của hệ thống mạng có vẻ như liên quan đến một số khoảng thời gian trong ngày thì nguyên nhân là do hệ thống mạng bị can nhiễu từ các thiết bị khác. Ví dụ như khả năng vận hành của mạng chậm lại vào giờ trưa vì bị ảnh hưởng bởi tần số của lò vi sóng do các nhân viên sử dụng. Mặc dầu hầu hết lò vi sóng chỉ ảnh hưởng đến kênh truyền số 11 thì một số lò vi sóng khác lại ảnh hưởng đến toàn bộ các kênh truyền. Một vấn đề khác ảnh hưởng đến sóng truyền là khi gặp các thiết bị sử dụng công nghệ điều chế kiểu nhảy tần (FHSS) như cordless phone. Do đó, có khá nhiều nguồn nhiễu khác nhau ảnh hưởng đến hệ thống WLAN, bởi vậy ban đầu, luôn luôn đặt Access point và client tại cùng một vị trí, sau đó di chuyển client xa dần cho đến khi có thể phát hiện được nguyên nhân. Hầu hết các phần mềm phía client đều cung cấp khả năng khắc phục sự cố bằng cách thể hiện độ mạnh yếu và chất lượng của sóng đối với các tần số liên quan.