|  |  |
| --- | --- |
|  | **TRƯỜNG ĐẠI HỌC TÔN ĐỨC THẮNG**  **KHOA CÔNG NGHỆ THÔNG TIN** |

**BÀI TẬP THỰC HÀNH MÔN HỌC WIRELESS AND MOBILE NETWORK SECURITY**

**LAB 4**

* HỌ TÊN: Tạ Văn Trọng (MSV: 51702048)

**NỘI DUNG BÁO CÁO KẾT QUẢ**

**I. Giới thiệu về mạng LAN không dây**

**Nội dung bài học**

* Mạng LAN không dây SOHO
* Mạng LAN không dây doanh nghiệp
* Kết luận

Ngày nay, có nhiều thiết bị không dây hơn có dây. Khoảng 10 năm trước, hầu hết các văn phòng chỉ có máy tính để bàn và một số thiết bị mạng khác như máy in. Tất cả những thứ này đều được kết nối với dây điện. Ngày nay, rất nhiều người dùng có máy tính xách tay, điện thoại thông minh và máy tính bảng. Đó là ba thiết bị không dây dành cho mỗi người dùng. Tốc độ không dây đã tăng lên đáng kể, tiến gần đến tốc độ Gigabit không dây.

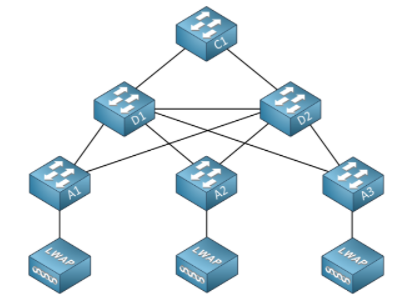
IEEE sử dụng 802.11 cho tất cả các giao thức có liên quan đến không dây. Hầu hết chúng ta đã nhìn thấy hoặc nghe nói về 802.11a, 802.11b, 802.11g, 802.11n và / hoặc 802.11ac trước đây. Chúng tôi cũng có Liên minh Wi-Fi giúp thúc đẩy mạng không dây. Ví dụ: IEEE đã mô tả xác thực và mã hóa theo tiêu chuẩn 802.11i của họ. Liên minh Wi-Fi đã dựa trên WEP, WPA và WPA2 về điều này Tiêu chuẩn. Những tên này dễ làm việc hơn so với việc đề cập đến 802.11i.

**1.1. Mạng LAN không dây SOHO (SOHO: Văn phòng nhỏ / Văn phòng tại nhà)**

Khi chúng tôi xem xét các mạng Doanh nghiệp lớn, một điểm truy cập duy nhất là không đủ. Hãy tưởng tượng một mạng với hàng trăm hoặc hàng nghìn người dùng. Khi bạn đi bộ xung quanh văn phòng, bạn sẽ không muốn bị ngắt kết nối mỗi khi điện thoại của bạn chuyển từ điểm truy cập này sang điểm truy cập khác. Bạn muốn có kết nối không dây ổn định, mọi lúc mọi nơi. Chuyển đổi liền mạch từ một quyền truy cập điểm đến điểm khác được gọi là chuyển vùng.

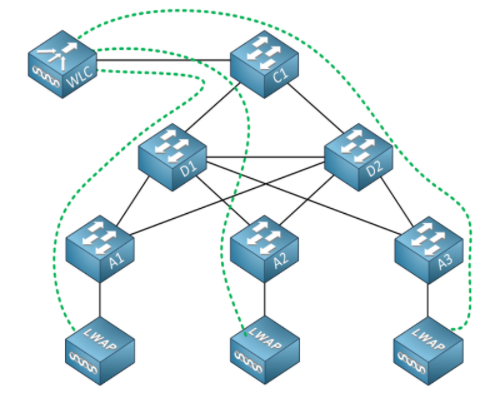
Một điểm truy cập duy nhất cũng có băng thông hạn chế. Nếu bạn có một phòng họp với 100 người dùng thì một điểm truy cập duy nhất có thể không thể cung cấp đủ băng thông cho mọi người.

Vì chúng tôi sử dụng mạng không dây cho người dùng của mình, nó phải gần gũi với người dùng của chúng tôi. Đó là lý do tại sao bạn sẽ tìm thấy các điểm truy cập trên lớp truy cập của mạng của bạn, giống như máy tính và máy in của bạn:



Vẫn còn một vấn đề. Giả sử bạn được kết nối với một điểm truy cập và bạn bắt đầu đi bộ xung quanh văn phòng, điện thoại của bạn sẽ chuyển sang một điểm truy cập khác. Làm thế nào để điểm truy cập thứ hai này biết rằng bạn đã được xác thực vào mạng? Bạn có thể xác thực lại nhưng điều đó sẽ bị hỏng kết nối của bạn ... không phải là một ý kiến ​​hay.

Để giải quyết vấn đề này, chúng tôi làm việc với bộ điều khiển mạng LAN không dây:



Tất cả các tác vụ quản lý được chuyển từ các điểm truy cập sang bộ điều khiển mạng LAN không dây. Nó chăm sóc xác thực, chuyển vùng, tạo mạng không dây mới, v.v. Các điểm truy cập chỉ chịu trách nhiệm chuyển tiếp lưu lượng, chúng tôi gọi đây là các LWAP (Điểm truy cập trọng lượng nhẹ).

Tất cả các quản lý tác vụ đều được chuyển từ các điểm truy cập sang mạng LAN điều khiển không dây. Không xác thực thiết lập, chuyển vùng, tạo mới mạng không dây, v.v. Access Point chịu trách nhiệm chuyển tiếp lưu lượng, chúng tôi gọi đây là LWAP (Điểm truy cập trọng lượng nhẹ).

Bây giờ chúng tôi có một mạng không dây lớn. Nếu bạn tạo một mạng không dây mới (SSID) thì nó sẽ được đẩy đến tất cả các điểm truy cập. Chuyển vùng cũng không có vấn đề gì vì tất cả lưu lượng truy cập được chuyển tiếp đếnWLC.

**II. Bộ dịch vụ LAN 802.11 không dây**

Nội dung bài học

● IBSS

● Chế độ cơ sở hạ tầng

○ Bộ dịch vụ cơ bản (BSS)

■ Hệ thống phân phối (DS)

○ Bộ dịch vụ mở rộng (ESS)

○ Bộ dịch vụ cơ bản lưới (MBSS)

● Chế độ AP

○ Bộ lặp

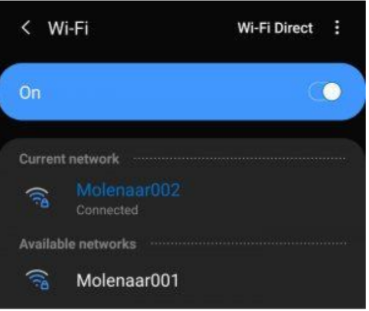
○ Cầu nối nhóm làm việc

○ Cầu ngoài trời

● Kết luận

Giống như mạng có dây, mạng không dây có cấu trúc liên kết vật lý và logic khác nhau. Các chuẩn 802.11 mô tả các bộ dịch vụ khác nhau. Một bộ dịch vụ mô tả cách một nhóm không dây các thiết bị giao tiếp với nhau.

Mỗi nhóm dịch vụ sử dụng cùng một mã nhận dạng nhóm dịch vụ (SSID). SSID là tên "thân thiện" của mạng không dây. Đó là tên mạng không dây mà bạn thấy khi nhìn vào mạng không dây khả dụng mạng trên thiết bị không dây của bạn.

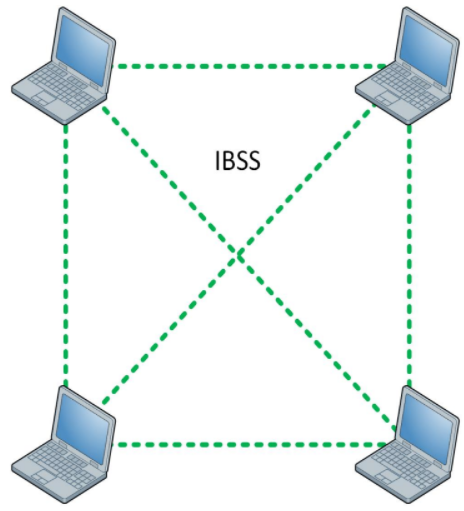


Trong bài học này, tôi sẽ giải thích các nhóm dịch vụ khác nhau và chúng ta sẽ xem xét một số các chế độ AP.

**2.1. IBSS**

Với bộ dịch vụ cơ bản độc lập (IBSS), hai hoặc nhiều thiết bị không dây kết nối trực tiếp không có điểm truy cập (AP). Chúng tôi cũng gọi đây là mạng đặc biệt. Một trong các thiết bị phải khởi động và quảng cáo một SSID, tương tự như những gì một AP sẽ làm. Các thiết bị khác sau đó có thể tham gia mạng.

IBSS không phải là một giải pháp phổ biến. Bạn có thể sử dụng điều này nếu bạn muốn chuyển các tệp giữa hai trở lên máy tính xách tay, điện thoại thông minh hoặc máy tính bảng mà không kết nối với mạng không dây AP cung cấp.



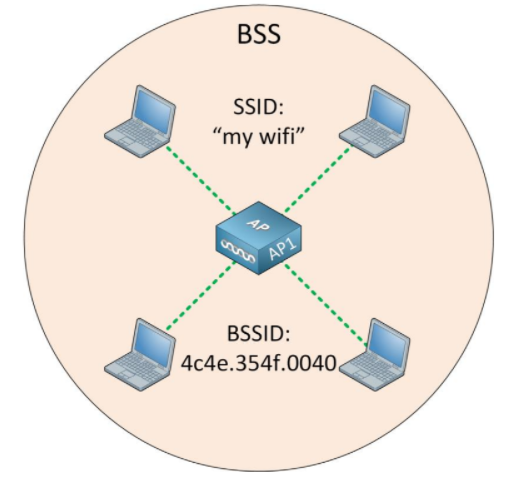
**2.2. Chế độ cơ sở hạ tầng**

Với chế độ cơ sở hạ tầng, chúng tôi kết nối tất cả các thiết bị không dây với một thiết bị trung tâm là AP. Tất cả dữ liệu đi qua AP. Chuẩn 802.11 mô tả các bộ dịch vụ khác nhau.

**2.2.1. Basic Service Set (BSS)**

Với Bộ dịch vụ cơ bản (BSS), các máy khách không dây kết nối với mạng không dây thông qua một AP. BSS là thứ chúng tôi sử dụng cho hầu hết các mạng không dây. Ý tưởng đằng sau một BSS là AP chịu trách nhiệm cho mạng không dây.

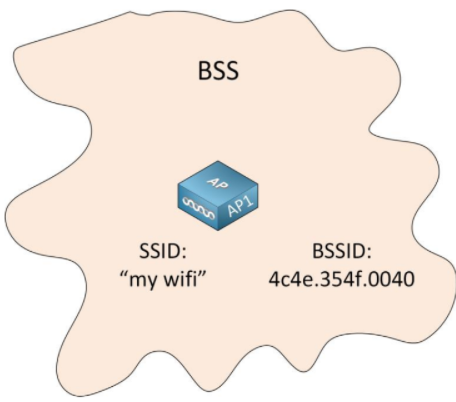
Mỗi máy khách không dây quảng cáo các khả năng của nó cho AP và AP cấp hoặc từ chối quyền để tham gia mạng. BSS sử dụng một kênh duy nhất cho tất cả các giao tiếp. AP và không dây của nó khách hàng sử dụng cùng một kênh để truyền và nhận.



The SSID is the “nice” name of the wireless network, and it doesn’t have to be unique.

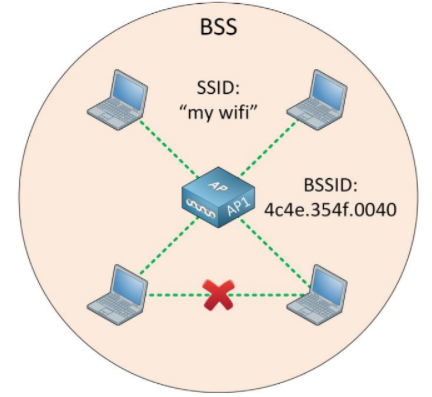
AP cũng quảng cáo Mã nhận dạng nhóm dịch vụ cơ bản (BSSID). Đây là địa chỉ MAC của radio của AP, một địa chỉ duy nhất xác định AP. Tất cả các máy khách không dây phải kết nối với AP. Điều này có nghĩa là phạm vi tín hiệu của AP xác định kích thước của BSS. Chúng tôi gọi đây là Khu vực Dịch vụ Cơ bản (BSA).

Trong hình trên, BSA là một hình tròn đẹp. Đây có thể là trường hợp nếu bạn cài đặt AP ở đâu đó giữa đồng cỏ không có gì xung quanh AP. Trong một tòa nhà, BSA có lẽ trông giống như thế này:



Khi một thiết bị không dây muốn tham gia BSS, nó sẽ gửi một yêu cầu liên kết đến AP. Các AP cho phép hoặc từ chối yêu cầu. Khi thiết bị không dây đã tham gia BSS, chúng tôi gọi nó là máy khách không dây hoặc trạm 802.11 (STA).

Tất cả lưu lượng truy cập từ một máy khách không dây phải đi qua AP ngay cả khi nó được dành cho một máy khách khác máy khách không dây.



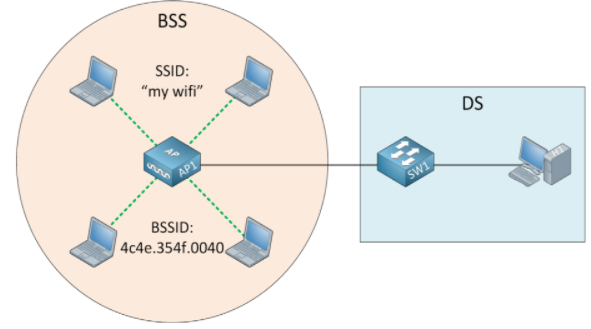
Mọi thứ đều phải thông qua AP vì AP là điểm trung tâm để quản lý của chúng tôi và nó giới hạn kích thước của BSS. Dải tín hiệu của AP xác định ranh giới của BSS.

**2.2.2 Hệ thống phân phối (DS)**

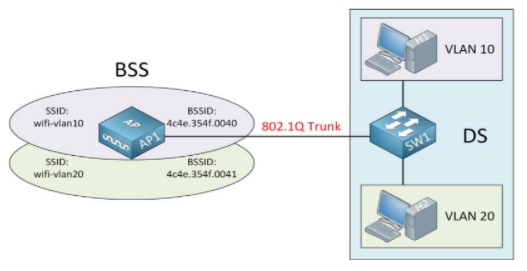
BSS là một mạng độc lập với một AP duy nhất. Trong các hình trên, không có kết nối với mạng có dây.

Tuy nhiên, hầu hết các mạng không dây là một phần mở rộng của mạng có dây. Một AP hỗ trợ cả haikết nối có dây và không dây. Tiêu chuẩn 802.11 gọi mạng có dây ngược dòng là sự phân phối hệ thống (DS).

AP kết nối các khung Ethernet L2 không dây và có dây, cho phép lưu lượng truy cập từ có dây với mạng không dây và ngược lại.



Chúng tôi cũng có thể làm điều này với VLAN. AP kết nối với bộ chuyển mạch bằng đường trục 802.1Q. Mỗi SSID ánh xạ tới một VLAN khác:



Mỗi mạng không dây có một BSSID duy nhất. BSSID dựa trên địa chỉ MAC, vì vậy hầu hết các nhà cung cấp (bao gồm cả Cisco) tăng chữ số cuối cùng của địa chỉ MAC để tạo ra một BSSID duy nhất.

Mặc dù chúng tôi có nhiều mạng không dây nhưng tất cả chúng đều sử dụng cùng một phần cứng cơ bản, radio và các kênh. Nếu bạn có một AP với nhiều bộ đàm, thì bạn có thể chỉ định không dây mạng tới các bộ đàm khác nhau. Ví dụ: bạn có thể sử dụng một mạng không dây trên đài 2,4 GHz và một cái khác trên đài 5 GHz.

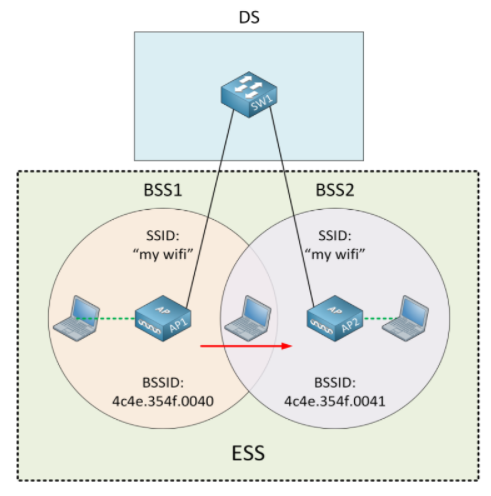
**2.2.3 Bộ dịch vụ mở rộng (ESS)**

Một BSS sử dụng một AP duy nhất. Điều này có thể không đủ vì hai lý do:

Phạm vi phủ sóng: Một tín hiệu của AP không thể bao phủ toàn bộ tầng hoặc tòa nhà. Bạn cần nhiều AP nếu bạn muốn không dây ở mọi nơi.

Băng thông: Một AP sử dụng một kênh duy nhất và không dây là bán song công. Không dây hoạt động nhiều hơn khách hàng bạn có, thông lượng của bạn sẽ càng thấp. Điều này cũng phụ thuộc vào tốc độ dữ liệu mà bạn hỗ trợ. Một ứng dụng khách không dây nằm trên biên giới BSA của bạn vẫn có thể truy cập được AP, nhưng chỉ có thể sử dụng tốc độ dữ liệu thấp. Một máy khách không dây đặt gần AP có thể sử dụng tốc độ dữ liệu cao. Xa máy khách không dây sẽ yêu cầu nhiều "thời gian phát sóng" hơn, giảm băng thông cho mọi người.

Để tạo một mạng không dây lớn hơn, chúng tôi sử dụng nhiều AP và kết nối tất cả chúng với mạng có dây mạng. Các AP làm việc cùng nhau để tạo ra một mạng không dây lớn trải dài toàn bộ một tầng hoặctòa nhà. Người dùng chỉ nhìn thấy một SSID duy nhất, vì vậy họ sẽ không nhận thấy liệu chúng tôi sử dụng một hay nhiều AP. Mỗi AP sử dụng một BSSID khác nhau, vì vậy đằng sau hậu trường, máy khách không dây có thể thấy nhiều AP mà nó có thể kết nối với. Chúng tôi gọi cấu trúc liên kết này với nhiều AP, Bộ dịch vụ mở rộng (ESS).



Các AP hoạt động cùng nhau. Ví dụ: nếu bạn kết hợp với một AP và bạn đi bộ xung quanh tòa nhà, bạn sẽ không ngắt kết nối. Máy khách không dây sẽ tự động "nhảy" từ AP này sang AP khác AP. Chúng tôi gọi đây là chuyển vùng. Để làm cho trải nghiệm này trở nên liền mạch, chúng ta cần có sự chồng chéo giữa các AP.

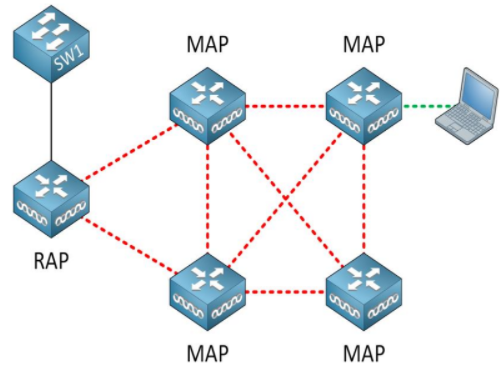
Mỗi AP cung cấp BSS riêng và sử dụng một kênh khác nhau để ngăn nhiễu giữa các AP.

**2.2.4 Bộ dịch vụ cơ bản lưới (MBSS)**

Nếu bạn muốn cung cấp mạng không dây cho một khu vực rộng lớn, chẳng hạn như một thành phố, thì không dễ dàng kết nối mỗi AP với mạng có dây.

Thay vào đó, bạn có thể xây dựng một mạng lưới, còn được gọi là Bộ Dịch vụ Cơ bản Mesh (MBSS).Với mạng lưới, chúng tôi kết nối lưu lượng truy cập không dây từ AP này sang AP khác. Các AP dạng lưới thường có nhiều bộ đàm. Một đài dành cho lưu lượng truy cập backhaul của mạng lưới giữa các AP; đài kia là để duy trì một BSS cho các máy khách không dây trên một kênh khác.

Ít nhất một AP được kết nối với mạng có dây; chúng tôi gọi đây là Root AP (RAP). Cái AP khác là Mesh AP (MAP) và chỉ được kết nối thông qua wireless backhaul.



Có nhiều đường dẫn để MAP đến được mạng có dây thông qua RAP, vì vậy chúng ta cần một giao thức tìm đường dẫn không có vòng lặp tốt nhất. Tương tự như cách thức hoạt động của cây bao trùm đối với L2 hoặc định tuyến giao thức cho L3, có các giải pháp không dây khác nhau. IEEE có tiêu chuẩn 802.11s cho lưới mạng lưới. Các nhà cung cấp đôi khi cũng sử dụng các giải pháp độc quyền. Ví dụ, Cisco có ứng dụng thích ứng giao thức đường dẫn không dây (AWPP).

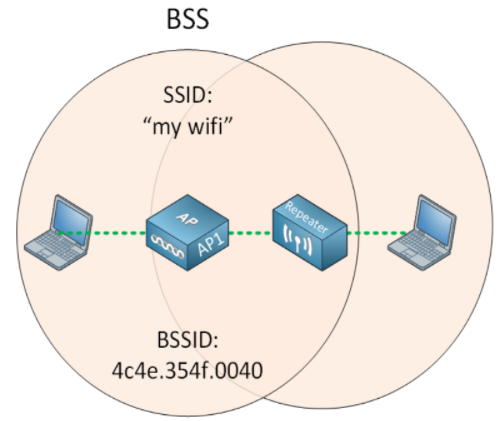
**2.3. AP Modes**

Cho đến nay, chúng ta mới chỉ nói về các bộ dịch vụ. Một số AP cũng hỗ trợ các chế độ cơ sở hạ tầng. Tôi sẽ giải thích các chế độ AP phổ biến nhất bên dưới.

**2.3.1 Bộ lặp**

Nếu bạn cần bao phủ một khu vực rộng lớn với mạng không dây của mình, bạn thường tạo một ESS. Tuy nhiên, ESS yêu cầu kết nối có dây. Nếu không thể kết nối AP của bạn bằng dây, bạn có thể định cấu hình AP ở chế độ bộ lặp.

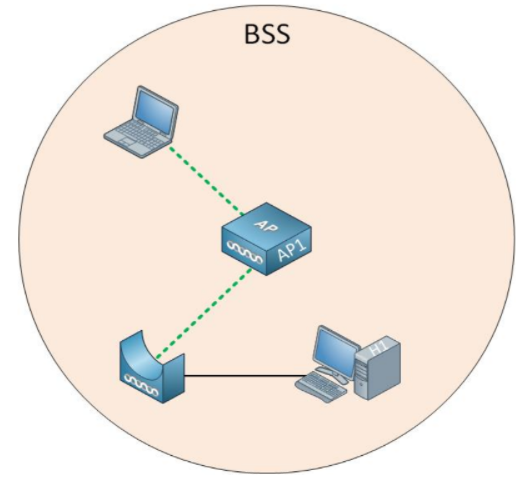
Bộ lặp không dây nhận tín hiệu và truyền lại. Điều này cho phép các thiết bị không dây không đủ gần AP để tham gia mạng.



Phải có sự chồng chéo giữa kích thước ô của AP và bộ lặp. Để tối ưu hiệu suất, nó phải là khoảng 50%. Nếu bộ lặp có một đài duy nhất, thì nó sẽ nhận và truyền trên cùng một tín hiệu với AP. Trong trường hợp này, AP cũng sẽ nhận được tín hiệu được truyền lại. Từ không dây là chế độ bán song công, việc thêm bộ lặp sẽ làm giảm khoảng 50% thông lượng khả dụng của bạn.

**2.3.2 Workgroup Bridge**

Điều gì sẽ xảy ra nếu bạn có một thiết bị có dây cần kết nối với mạng không dây nhưng không có đài? Ví dụ: máy in, máy tính hoặc hệ thống điểm bán hàng (PoS) cũ hơn. Trong trường hợp này, bạn có thể sử dụng cầu nối nhóm làm việc (WGB). WGB có kết nối có dây mà bạn kết nối với thiết bị có dây và kết nối không dây, kết nối này sử dụng để hoạt động như một ứng dụng khách không dây của BSS.



Có hai loại WGB:

● Cầu nối nhóm làm việc chung (uWGB): WGB chung chỉ hỗ trợ một máy khách có dây. Điều này dựa trên các tiêu chuẩn 802.11.

● Cầu nhóm làm việc (WGB): WGB (hoặc Chế độ cầu nhóm làm việc) là độc quyền của Cisco mở rộng cho các tiêu chuẩn 802.11 và hỗ trợ nhiều máy khách có dây.

**2.3.3 Outdoor Bridge**

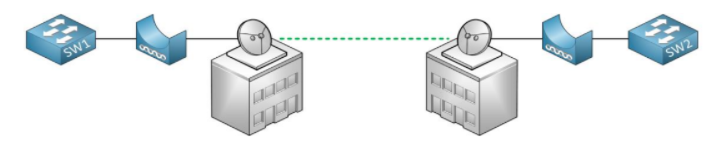
Điều gì xảy ra nếu bạn muốn kết nối hai tòa nhà nhưng không có cáp ở giữa và bạn không muốn sử dụng mạng WAN? Bạn có thể sử dụng một cầu nối không dây ngoài trời. Bạn có thể định cấu hình hai AP để tạo một cầu nối không dây giữa hai mạng LAN trong khoảng cách xa hơn. Cầu nối không dây giữa hai tòa nhà, và thậm chí giữa hai thành phố là có thể.

Có hai lựa chọn:

● Điểm đến điểm

● Điểm đến đa điểm

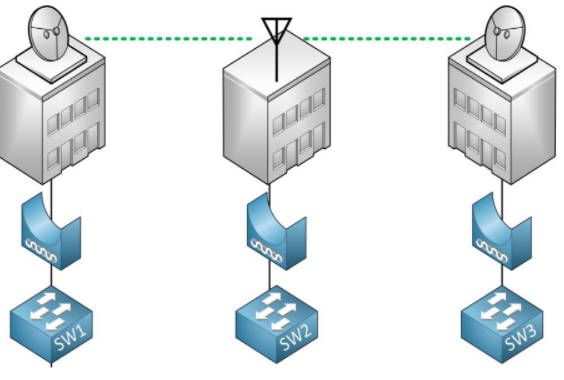
Hãy bắt đầu với point-to-point:



Chúng tôi có hai tòa nhà, mỗi tòa nhà đều có mạng LAN. Các AP đang ở chế độ cầu nối và sử dụng định hướng ăng-ten tập trung tín hiệu của chúng theo một hướng, về phía AP ở phía bên kia.

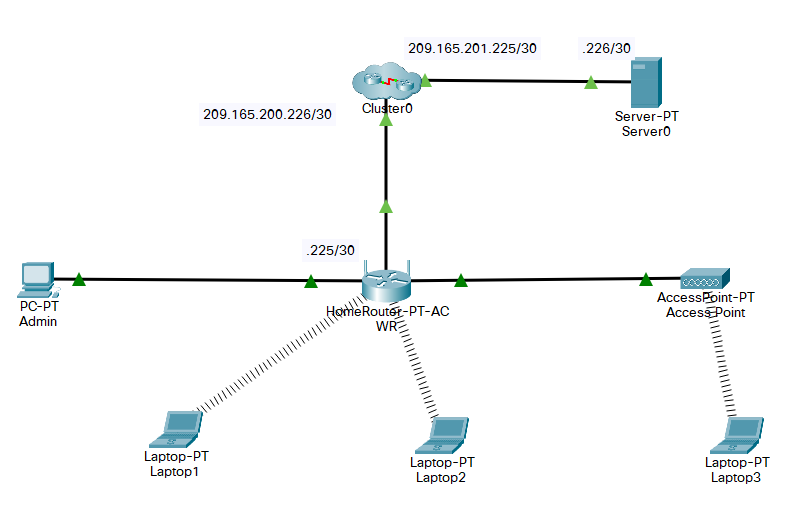
Nếu bạn tự hỏi khoảng cách tối đa của một cầu nối không dây có thể là bao nhiêu: liên kết wifi dài nhất là từ CISAR (Trung tâm Hoạt động Phát thanh của Ý). Đó là 304 km (188 dặm).

Nếu bạn muốn kết nối nhiều hơn hai mạng LAN, bạn có thể sử dụng cầu nối điểm - đa điểm:



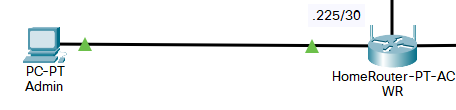
LAN 1 và 3 sử dụng các AP có ăng-ten định hướng. LAN 2 ở giữa sử dụng đa hướng ăng ten để tín hiệu được truyền như nhau theo cả hai hướng.

**Phần 1: Mô hình**

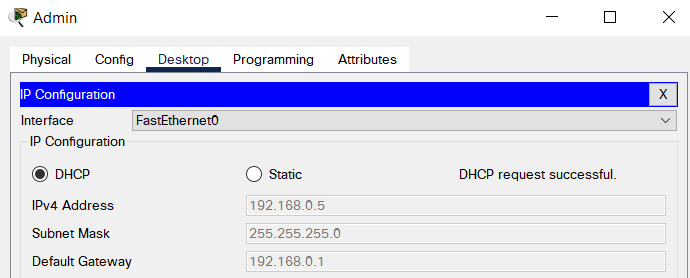


**Phần 2: Kết nối với Bộ định tuyến không dây**

**Bước 1: Kết nối Admin với WR.**



**Bước 2: Cấu hình Admin để sử dụng DHCP.**



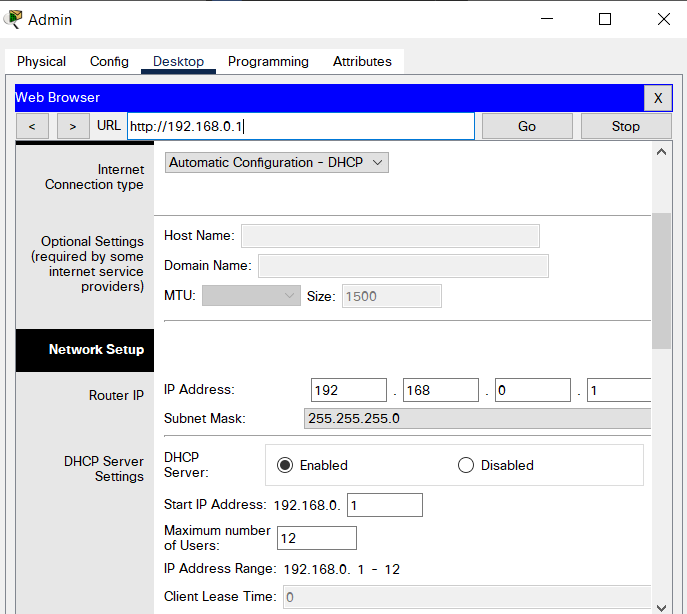
Câu hỏi:

Địa chỉ IP của máy tính là gì? 192.168.0.5

Mặt nạ mạng con của máy tính là gì? 255.255.255.0

Cổng mặc định của máy tính là gì? 192.168.0.1

**Bước 3: Kết nối với Giao diện Web WR.**



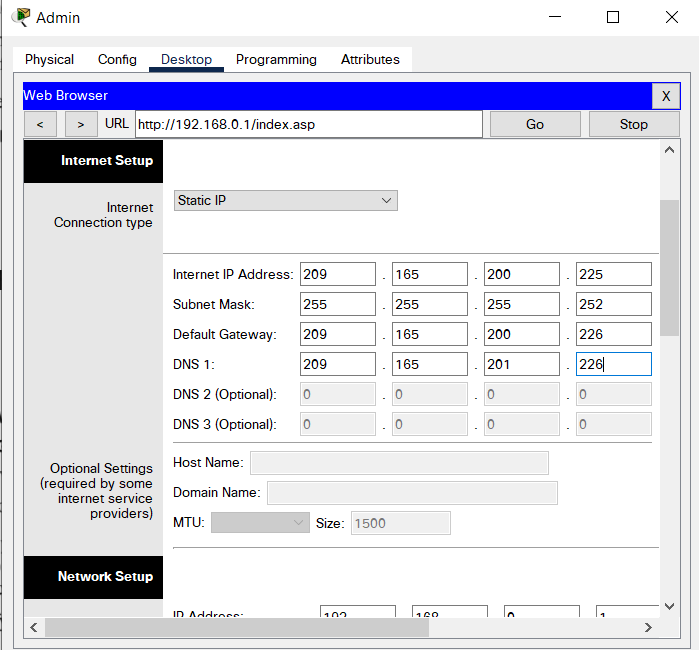
Câu hỏi:

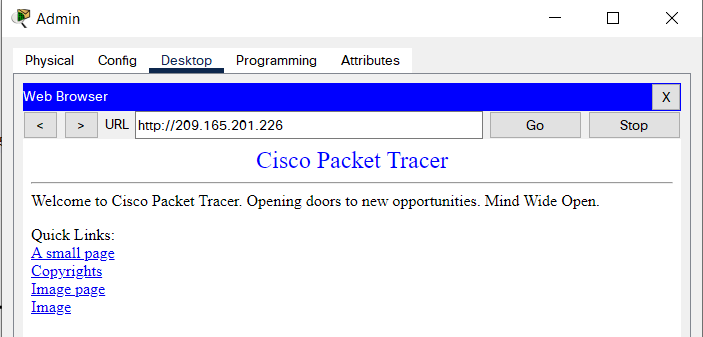
Địa chỉ IP dành cho Quản trị viên có nằm trong phạm vi này không?

192.168.0.1 - 12

Nó có được mong đợi không? Có

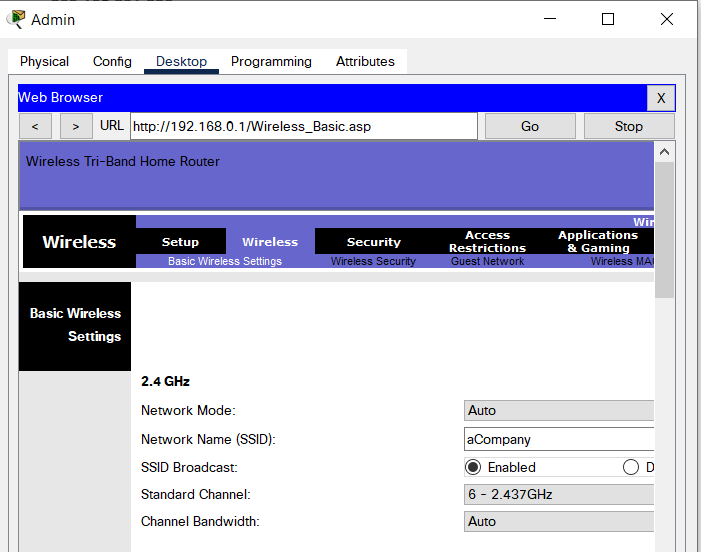
**Bước 4: Định cấu hình Cổng Internet của WR.**



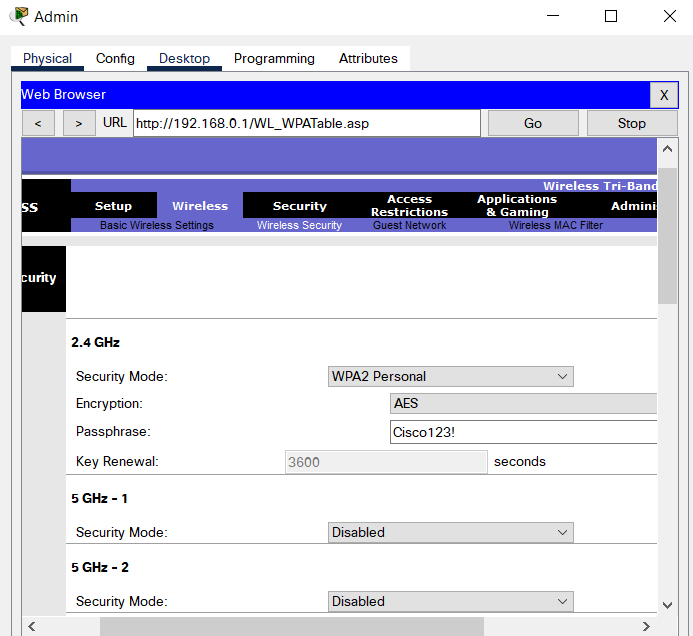


**Phần 3: Cấu hình mạng không dây**

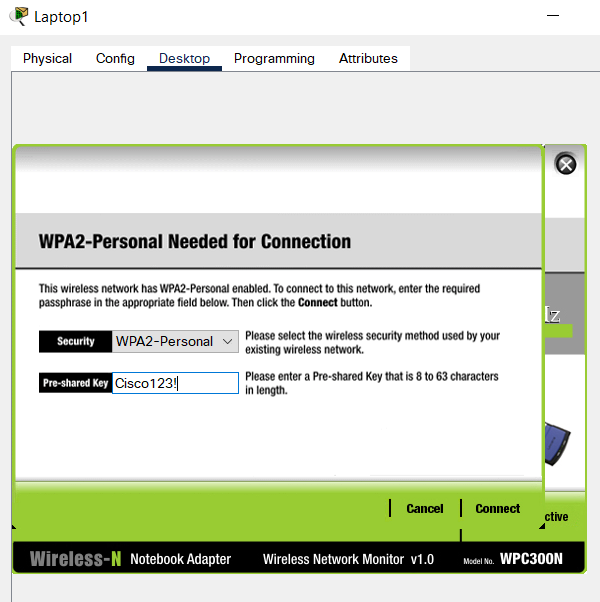
**Bước 1: Định cấu hình WR SSID.**

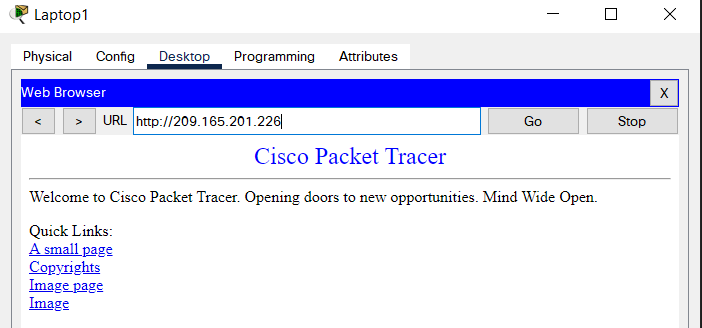


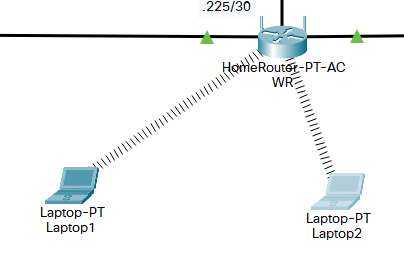
**Bước 2: Định cấu hình cài đặt bảo mật không dây.**



**Bước 3: Kết nối các khách hàng không dây.**

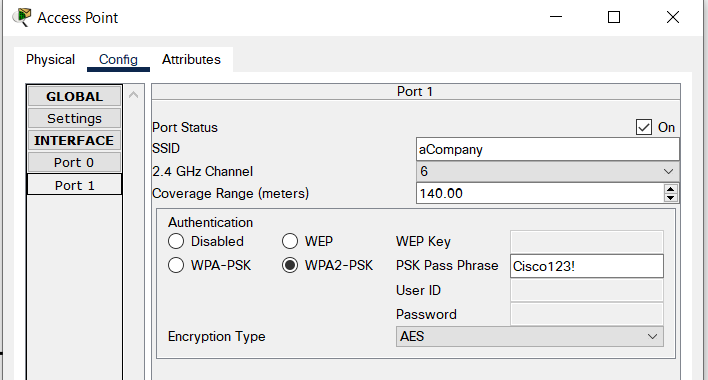




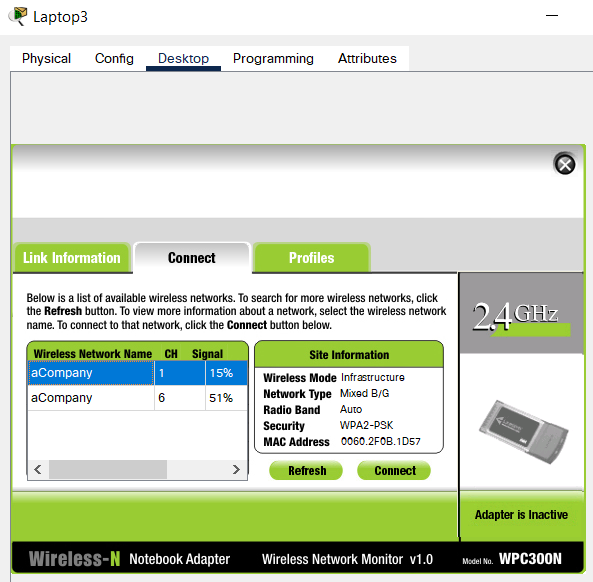


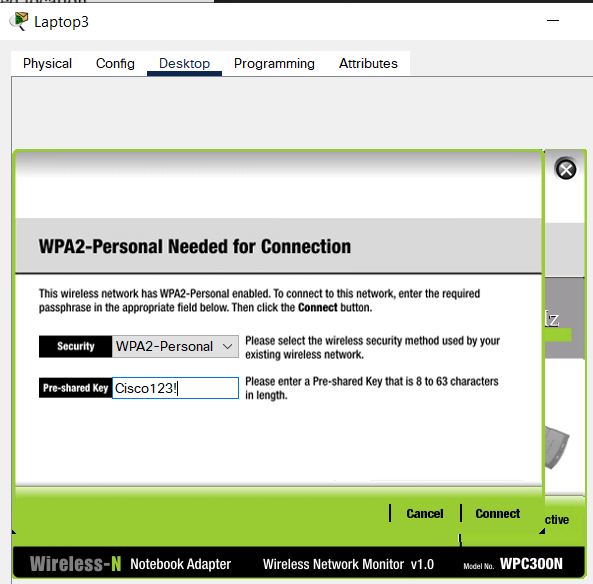
**Part 4: Kết nối khách hàng không dây với một điểm truy cập**

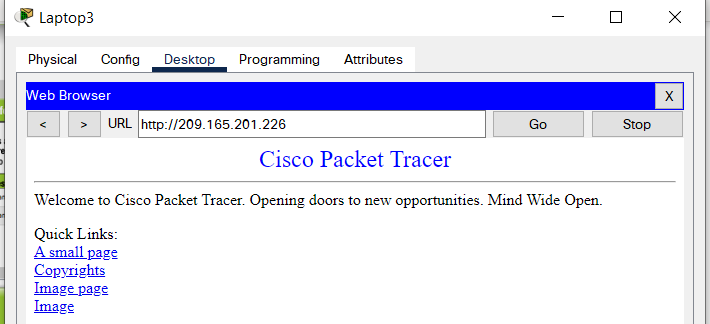
**Bước 1: Định cấu hình Điểm truy cập.**



**Bước 2: Kết nối các khách hàng không dây.**

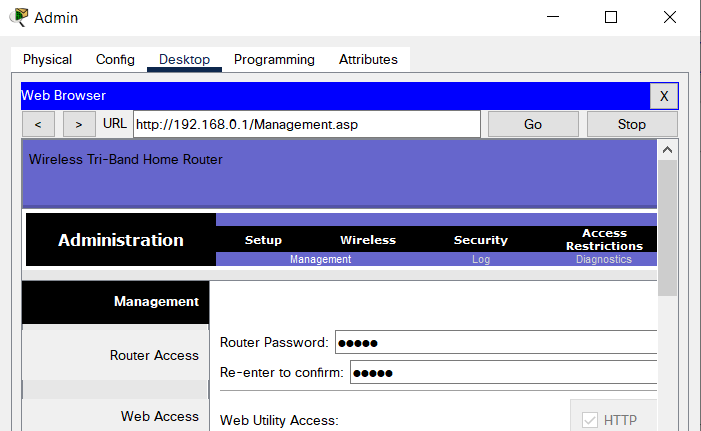


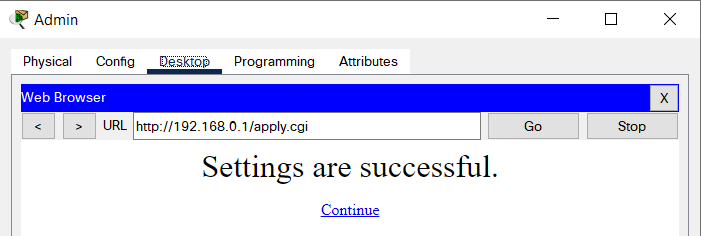


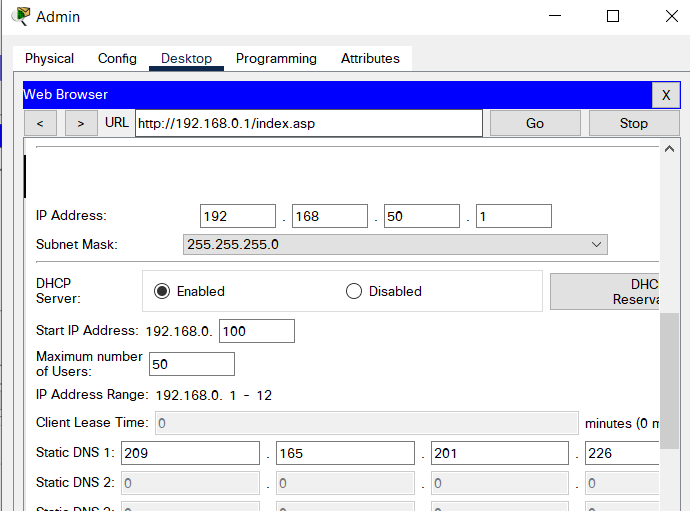


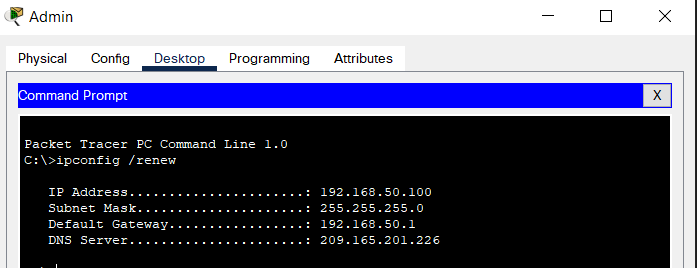
**Phần 5: Các nhiệm vụ quản trị khác**

**Bước 1: Thay đổi mật khẩu truy cập WR.**



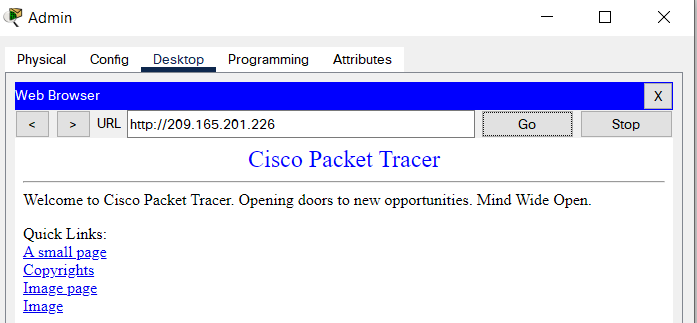


**Bước 2: Thay đổi dải địa chỉ DHCP trong WR.**

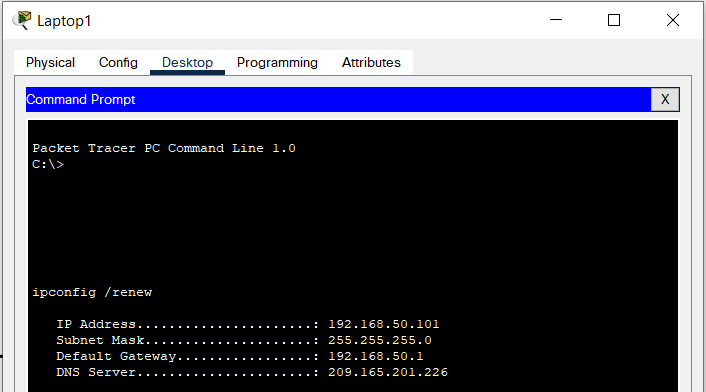


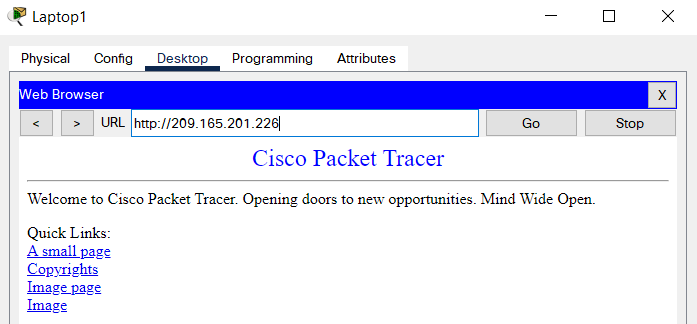
Câu hỏi:

Thông tin địa chỉ IP mới dành cho Admin là gì? 192.168.50.100

Xác minh rằng bạn vẫn có thể điều hướng đến máy chủ 209.165.201.226.

Gia hạn địa chỉ IP trên các máy tính xách tay khác để xác minh rằng bạn vẫn có thể điều hướng đến máy chủ [www.cisco.pka](http://www.cisco.pka).





**Kết luận:**

Sau khi hoàn thành lab4 thì em đã biết các bước cấu hình mạng không dây và chia bộ định tuyến access point.