Đối với tốc độ dữ liệu nhất định, bạn có thể thay đổi mức công suất hoặc chọn một ăng-ten khác để thay đổi vùng phủ sóng và hình dạng phủ sóng. Một kích thước ô lớn có thể dẫn đến quá nhiều khách hàng chia sẻ băng thông có sẵn. (Các mạng WLAN IEEE 802.11 là các mạng chia sẻ, với tất cả các thiết bị trong cùng một miền băng thông.) Bằng cách giảm cường độ điểm truy cập hoặc tăng anten na, bạn có thể giảm kích thước ô và chia sẻ băng thông với những khách hàng ít hơn. Điều này sẽ dẫn đến nhiều điểm truy cập hơn cho một vùng phủ sóng nhất định nhưng sẽ mang lại hiệu suất tốt hơn cho khách hàng.

**Mạng WLAN và VLAN**

Bạn có thể đặt nhiều điểm truy cập thông qua một bộ phận để cung cấp cho người dùng khả năng chuyển vùng tự do trong một khu vực mở rộng trong khi duy trì truy cập liên tục vào các nguồn mạng. Phương pháp đơn giản nhất để đảm bảo người dùng có thể chuyển vùng là đặt tất cả người dùng vào cùng một mạng con IP và cùng một VLAN. Mặt khác, các thiết bị di chuyển từ subnet này sang subnet khác phải có được một địa chỉ IP mới và có thể bị mất các gói dữ liệu có thể đã được truyền đi trong khi chúng đang yêu cầu một địa chỉ.

Bất cứ khi nào có thể, một mạng WLAN phải là một mạng con riêng biệt để đơn giản hóa việc định địa chỉ trong khi chuyển vùng và cũng để cải thiện quản lý và bảo mật. Giữ tất cả các máy khách không dây trong mạng con của chính họ làm cho nó dễ dàng hơn để thiết lập các bộ lọc giao thông để bảo vệ khách hàng có dây từ một cuộc tấn công đưa ra từ WLAN.

Điểm truy cập không dây dự phòng

Trong cả kiến ​​trúc LAN có dây và không dây, sự dự phòng thường được mong muốn đảm bảo tính sẵn sàng cao. Đối với mạng Campus với mạng WLAN có nhiệm vụ quan trọng, Cisco có một tính năng được gọi là chế độ Hot Standby hỗ trợ hai điểm truy cập được cấu hình để sử dụng cùng một kênh trong một vùng phủ sóng duy nhất. Chỉ có một điểm truy cập hoạt động. Điểm truy cập chế độ chờ thụ động theo dõi mạng và điểm truy cập chính. Nếu điểm truy cập chính có vấn đề, điểm truy cập phụ sẽ tiếp nhận để cung cấp thêm tầm hoạt động như dự phòng.

**Chú ý** Không nhầm lẫn chế độ Hot Standby với chế độ Hot Standby Router (HSRP) của Cisco, được đề cập trong phần "Workstation-to-Router Redundancy" sắp tới. Điểm truy cập Hot Standby gán địa chỉ dự phòng ở lớp 2, trong khi HSRP gán địa chỉ dự phòng ở lớp 3.

Bạn nên đặt điểm truy cập chờ ở gần điểm truy cập mà nó sẽ theo dõi và cung cấp cho nó cấu hình tương tự (trừ một địa chỉ IP khác). Điểm truy cập dự phòng kết hợp với điểm truy cập được giám sát như là một máy khách và truy vấn các điểm truy cập được giám sát thường xuyên thông qua giao diện Ethernet và giao diện RF. Nếu điểm truy cập được giám sát không đáp ứng, điểm truy cập chế độ chờ sẽ trở nên hoạt động, tín hiệu radio điểm truy cập chính sẽ trở nên không hoạt động và mất vị trí điểm truy cập được giám sát trong mạng.

Ngay sau khi phát hiện sự cố điểm truy cập chính, cần phải có sự can thiệp của người dùng. Người dùng nên trả lại điểm truy cập dự phòng sang chế độ chờ. Việc không thiết lập lại điểm truy cập chờ sẽ dẫn đến cả điểm truy cập chính và điểm chờ hoạt động đồng thời trên cùng một kênh khi điểm truy cập chính trở lại trực tuyến.

**Dự phòng và phân bố tải trong mạng LAN có dây**

Trong mạng Campus có dây, thông thường thiết kế các liên kết dự phòng giữa các thiết bị chuyển mạch LAN. Hầu hết các thiết bị chuyển mạch LAN đều sử dụng thuật toán spanning-tree IEEE 802.1D để tránh các vòng lặp mạng. Chuẩn 802.1D là một giải pháp tốt cho dự phòng, nhưng không phải để phân bố tải, bởi vì chỉ có một đường đi hoạt động. Một số nhà cung cấp chuyển đổi, bao gồm cả Cisco, cho phép bạn có một giao thức spannning-tree trên mỗi VLAN, có thể được sử dụng để thực hiện dự phòng. Một bộ chuyển mạch có thể hoạt động như cây cầu gốc cho một VLAN và như một bản sao lưu cho cây gốc cho một VLAN khác.

Cisco Per VLAN Spanning Tree + (PVST +) xây dựng một cấu trúc cây hợp lý riêng biệt cho mỗi VLAN. PVST + cho phép chia sẻ tải bằng cách có các đường dẫn chuyển tiếp khác nhau cho mỗi VLAN.PVST + có khả năng mở rộng thấp hơn phương pháp 802.1D cổ điển, chỉ có một gốc và cây, vì thời gian CPU cần để xử lý BPDU cho mỗi VLAN. Cisco đã vượt qua giới hạn này bằng giao thức đa thức Spanning Tree (MISTP), cho phép một nhóm VLAN được nhóm lại thành một cây đơn.

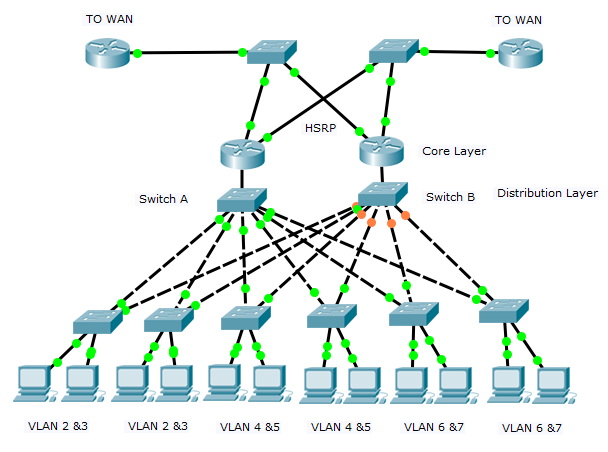
IEEE cũng đã tăng cường thuật toán spanning-tree ban đầu với tiêu chuẩn Cấu trúc Đa cây (MST), được ghi lại trong IEEE 802.1s. Nhiều giao thức Spanning Tree (MSTP) sử dụng RSTP để hội tụ nhanh chóng nhưng cải thiện khả năng mở rộng RSTP bằng cách tập hợp một tập hợp các cây trải rộng dựa trên VLAN vào các trường hợp riêng biệt và bằng cách chạy một thuật toán cây spanning-tree (nhanh) trên mỗi cá thể. Kiến trúc này cung cấp nhiều đường chuyển tiếp cho lưu lượng truy cập dữ liệu, cho phép phân bố tải và giảm số lượng cây trải rộng yêu cầu để hỗ trợ một số lượng lớn các VLAN.

Nếu bạn sử dụng VLAN trong thiết kế mạng trường với các thiết bị chuyển mạch hỗ trợ 802.1s, PVST + hoặc MISTP, các liên kết dự phòng có thể cung cấp khả năng phân bố tải cùng với khả năng chịu lỗi.

Hình 5-11 cho thấy một thiết kế LAN campus dự phòng sử dụng thuật toán spanning-tree và VLAN.

Thiết kế trong Hình 5-11 sử dụng khái niệm một cây lan rộng trên mỗi VLAN. Switch A hoạt động như cây cầu gốc cho các VLAN 2, 4 và 6. (Switch B có thể trở thành cây cầu gốc cho các VLAN nếu Switch A không thành công). Switch B hoạt động như cây cầu gốc cho VLAN 3, 5 và 7. ( Switch A có thể trở thành cây cầu gốc cho các VLAN nếu Switch B không thành công) Kết quả là cả hai liên kết từ một switch lớp truy cập đều mang lưu lượng truy cập, và chuyển đổi dự phòng thành một cây cầu gốc sẽ xảy ra tự động nếu một trong các switch của lớp phân phối thất bại. Cả hai phân bố tải và chịu lỗi đều đạt được.

Thiết kế trong Hình 5-11 có thể mở rộng thành một mạng lưới khuôn viên rộng lớn. Thiết kế đã được thử nghiệm trên một mạng có 8000 người sử dụng, 80 thiết bị chuyển mạch lớp truy cập, 14 thiết bị chuyển mạch(switch) lớp phân phối, và 4 router lớp lõi (không tính các router đi đến WAN).



**Hình 5-11 Cấp bậc dự phòng mạng trong mô hình Campus**

**Dự phòng Server**

Phần này bao gồm các hướng dẫn cho việc dự phòng máy chủ trong một thiết kế mạng trường. File, web, giao thức cấu hình động máy chủ DHCP (Dynamic Host Configuration Protocol), tên và cơ sở dữ liệu là tất cả các ứng viên cho sự dự phòng trong thiết kế mạng campus, tùy thuộc vào yêu cầu của khách hàng. Trong một mạng có hỗ trợ Voice over IP (VoIP), các máy chủ cung cấp ánh xạ giữa một số điện thoại và một địa chỉ IP và xử lý xử lý cuộc gọi cần được cung cấp theo một cách thức dôi dư. Ví dụ: Quản lý Truyền thông Hợp nhất của Cisco hỗ trợ nhóm dự phòng nơi các máy chủ được phân công vai trò của máy chủ chính, thứ hai hoặc thứ ba.

Các máy chủ DHCP có thể được đặt ở lớp truy cập, lớp phân phối hoặc lớp lõi. Đối với các mạng phân phối rộng khắp, các máy chủ DHCP dự phòng thường được đặt trong lớp truy cập. Điều này tránh được lưu lượng truy cập quá nhiều giữa việc lớp truy cập và lớp phân phối hoặc các lớp lõi và cho phép mỗi máy chủ DHCP phục vụ một tỷ lệ nhỏ hơn số người sử dụng. Ví dụ, nếu phần lõi của mạng ở New York, và các lớp truy cập và phân phối được lan rộng trên toàn thế giới, thì có nghĩa là có máy chủ DHCP trong lớp truy cập. Đối với các mạng nhỏ, tuy nhiên, các máy chủ DHCP thường nằm ở trung tâm của mạng để tạo thuận lợi cho việc quản lý bởi một bộ phận CNTT tập trung.

Trong các mạng khuôn viên lớn, máy chủ DHCP thường được đặt trên một phân đoạn mạng khác với các hệ thống cuối sử dụng nó. Nếu máy chủ ở phía bên kia của một bộ định tuyến, router có thể được cấu hình để chuyển tiếp DHCP broadcasts từ các hệ thống đầu cuối. Bộ định tuyến chuyển tiếp các broadcast đến một địa chỉ máy chủ được định cấu hình thông qua lệnh ip helper address trên một bộ định tuyến của Cisco. Router chèn địa chỉ của giao diện nhận yêu cầu vào trường giaddr của yêu cầu DHCP. Máy chủ sử dụng trường giaddr để xác định địa chỉ đến từ đâu để chọn một địa chỉ.

Các tên máy chủ theo lý thuyết ít quan trọng hơn các máy chủ DHCP bởi vì người dùng có thể tiếp cận các dịch vụ theo địa chỉ thay vì tên nếu máy chủ tên thất bại; Bởi vì nhiều người dùng không nhận ra điều này, tuy nhiên, nó là một ý tưởng tốt để lên kế hoạch cho các máy chủ dự phòng. Máy chủ t thực hiện Hệ thống Tên miền Internet (DNS Domain Name System), Dịch vụ Đặt tên Internet của Windows (WINS) và Dịch vụ Tên NetBIOS (NetBIOS Name Service - NBNS). Máy chủ tên có thể được đặt ở cấp truy cập, phân phối hoặc lớp lõi. Đối với các mạng phân phối rộng khắp trên toàn cầu, nên có các máy chủ tên ở lớp truy cập. Đối với các mạng nhỏ, tuy nhiên, phổ biến hơn là đặt các máy chủ trong lõi của mạng.

Trong bất kỳ ứng dụng nào mà chi phí thời gian chết cho các máy chủ tập tin là mối quan tâm lớn, vì thế máy chủ tệp tin được nhân đôi là cách được đề nghị là cách giải quyết vấn đề. Ví dụ: trong một công ty môi giới nơi thương nhân truy cập dữ liệu để mua và bán cổ phiếu, dữ liệu có thể được sao chép vào hai hoặc nhiều máy chủ tệp tin được nhân đôi. Máy chủ tập tin được nhân đôi giữ dữ liệu giống hệt nhau. Cập nhật dữ liệu được đồng bộ hóa qua các máy chủ. Các máy chủ nên được trên các mạng khác nhau và nguồn điện để tối đa hóa tính sẵn có.

Nếu sự dự phòng của máy chủ hoàn thành không khả thi do cân nhắc chi phí, phản chiếu hoặc duplexing của ổ cứng máy chủ tệp là một ý tưởng hay. (Duplexing giống như đối chiếu với tính năng bổ sung mà hai ổ đĩa cứng được điều khiển bởi các bộ điều khiển đĩa khác nhau). Thực hiện một mạng lưu trữ (SAN) là một lựa chọn khác. SAN là một giải pháp phổ biến cho các tổ chức tìm kiếm độ tin cậy cao, không bị gián đoạn truy cập vào một lượng lớn các thông tin được lưu trữ.

Sự dự phòng có cả tính sẵn sàng và hiệu suất. Với máy chủ tệp được nhân đôi, có thể chia sẻ khối lượng công việc giữa các máy chủ. Sử dụng mạng lưới phân phối nội dung (CDN) và các thiết bị dịch vụ nội dung, người dùng có thể được hướng đến một trong nhiều máy chủ được nhân đôi mà tất cả đều giữ cùng một dữ liệu.

Sự dự phòng cũng có thể đạt được bằng cách thêm một số thứ tinh xảo vào DNS. Khi khách hàng yêu cầu truy cập vào một tài nguyên bằng tên DNS của nó, một máy chủ DNS có thể trả về nhiều địa chỉ host trong phản hồi của nó. Cho dù điều này sẽ cung cấp sự dự phòng tốt phụ thuộc vào phần mềm máy chủ lưu trữ. Có một số cài đặt các địa chỉ bổ sung nếu địa chỉ đầu tiên không đáp ứng.

Một khả năng khác là một tính năng gọi là DNS round robin, nơi máy chủ có một danh sách các địa chỉ qua đó nó chu kỳ. Máy chủ đưa ra một địa chỉ khác với mỗi yêu cầu, đi qua danh sách các địa chỉ. Khi nó được vào cuối của danh sách, nó chu kỳ trở lại đầu danh sách. Do bộ nhớ đệm DNS, nơi mà các máy khách và các máy chủ DNS khác nhớ một bản đồ tên-to-địa chỉ trước đó, DNS round robin không hoàn hảo, nhưng khá đơn giản để thực hiện và cấu hình trên một máy chủ DNS điển hình.

Dự phòng và cân bằng tải với DNS cũng có thể làm việc với nhiều máy chủ DNS.Giả sử rằng các máy khách truy cập các máy chủ DNS khác nhau, một máy chủ có thể đáp ứng với một địa chỉ, trong khi các máy chủ khác đáp ứng với các địa chỉ khác nhau. Một lần nữa, bộ nhớ đệm DNS có thể giới hạn hiệu quả của phương pháp này.

**Chú ý** Một lưu ý cần lưu ý là tệp được nhân đôi, DHCP, web và các loại máy chủ khác. Các máy chủ được nhân đôi cung cấp dự phòng cho phần cứng, cáp, kết nối LAN và nguồn điện, nhưng chúng không cung cấp phần mềm hoặc dự phòng dữ liệu. Bởi vì máy chủ được nhân đôi giữ dữ liệu được sao chép, nếu vấn đề nằm trong dữ liệu hoặc khả năng của phần mềm để truy cập vào dữ liệu, tất cả các máy chủ bị nhân đôi đều bị ảnh hưởng.

**Dự phòng từ máy trạm(Workstation) đến Router**

Máy trạm trong mạng campus phải có quyền truy cập vào bộ định tuyến để truy cập vào các dịch vụ từ xa. Vì việc truyền thông qua trạm làm việc với thiết bị định tuyến là rất quan trọng trong hầu hết các thiết kế, bạn nên cân nhắc việc thực hiện dự phòng cho chức năng này.

Một máy trạm có nhiều cách để khám phá một bộ định tuyến trên mạng, tùy thuộc vào giao thức mà nó đang chạy và cũng như việc thực hiện giao thức. Các phần tiếp theo mô tả các phương pháp cho các máy trạm để tìm hiểu về các bộ định tuyến và các tính năng dự phòng để đảm bảo một máy trạm có thể tiếp cận một bộ định tuyến.

Triển khai IP khác nhau về cách chúng thực hiện truyền thông giữa máy trạm với router. Một số máy trạm IP gửi một khung ARP để tìm một trạm từ xa. Một bộ định tuyến chạy ARP proxy có thể đáp ứng yêu cầu ARP với địa chỉ lớp liên kết dữ liệu của router.Cisco routers chạy proxy ARP theo mặc định.

Ưu điểm của ARP proxy đối với các trạm từ xa là một máy trạm không cần phải được cấu hình với địa chỉ của một bộ định tuyến. Tuy nhiên, vì proxy ARP chưa bao giờ được chuẩn hóa, hầu hết các quản trị viên mạng không phụ thuộc vào nó. Ngoài ra, nhiều chuyên gia bảo mật khuyên bạn nên tắt nó đi vì nó giúp kẻ tấn công dễ dàng truy cập vào mạng khác. Thay vào đó, máy trạm IP được cung cấp địa chỉ của một bộ định tuyến mặc định. Điều này có thể được cấu hình bằng tay hoặc cung cấp bởi DHCP. Một router mặc định là địa chỉ của một bộ định tuyến trên phân đoạn cục bộ mà một máy trạm sử dụng để tiếp cận các dịch vụ từ xa. Bộ định tuyến mặc định thường được gọi là cổng mặc định vì lý do lịch sử.

Một máy trạm IP thường chỉ biết địa chỉ của một router: cổng mặc định. Kết quả là một máy trạm không phải luôn luôn sử dụng phương pháp thích hợp nhất để đến một trạm từ xa. Các máy trạm có thể chọn một đường dẫn bao gồm một hop thêm. Hình 5-12 cho thấy các vấn đề ngoài trời. Để có được xung quanh các vấn đề ngoại lệ và để thêm sự dự phòng, một số thực hiện IP máy trạm cho phép một quản trị viên mạng để thêm các tuyến đường tĩnh vào một tập tin cấu hình hoặc để cấu hình máy trạm để chạy một giao thức định tuyến .

**Lưu ý** Trong những môi trường UNIX, các máy trạm đôi khi chạy trình nền RIP để tìm hiểu về các tuyến đường. Tốt nhất là nếu chúng chạy trình nền RIP ở chế độ thụ động thay vì hoạt động. Trong chế độ hoạt động, một máy trạm gửi khung phát RIP mỗi 30 giây. Khi nhiều máy trạm UNIX chạy RIP ở chế độ hoạt động, lượng lưu lượng phát sóng có thể làm giảm hiệu suất mạng. Ngoài ra, có những rủi ro bảo mật trong việc cho phép các trạm không kiểm soát được chạy một giao thức định tuyến trong chế độ hoạt động.