Thiết kế mạng IP

Bài 2: Mạng nội bộ (Private network)

Phạm Huy Hoàng
SoICT/HUST
hoangph@soict.hust.edu.vn

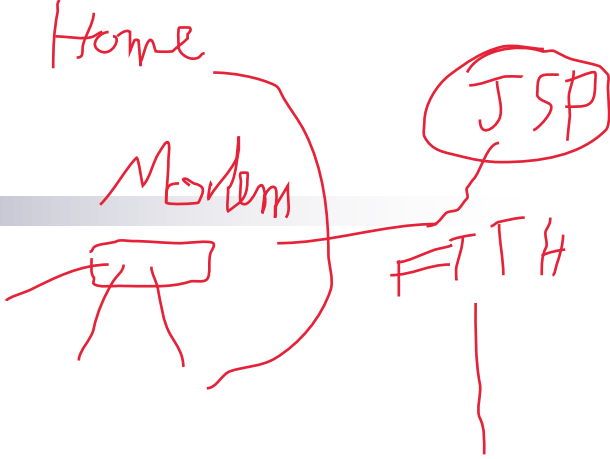
tìm sách: Thiết kế mạng Intranet của thầy

Nội dung

- LAN
- Inter-LAN & Virtual LAN
- Layer 3 switching
- IP cho mạng nội bộ
- Quản lý tài nguyên tập trung trong mạng nội bộ

đơn giản nhất: mạng gia đình cắm vào là xong.
ở BK thì khác-nhiều máy ở nhiều nơi- sd 1 mạng lan ảo
+ ko sd mô hình routing mà sd mô hình Layer 3 switching
+ Có thêm kn qli tài nuyên tập chung, phân biệt là mạng Lan hay ko (chứ kp là sd kích thước)

thường hđ ở tầng 2.
Ở nhà, để rẻ, hđ ở tầng 1 (kp cài phần mềm-mỗi dây ra ngoài cần + ít thiết bị đụng độ thấp => chỉ sd bộ chia HUB hđ ở tầng 1
- Ở Modem sd tầng 2 sd switch



LAN

- Local Area Network
  - Đơn giản nhất
  - Hoạt động tầng 2 (thậm chí là tầng 1)
  - Dễ dàng share resource (thư mục, file, máy in, v.v..)
  - Quản lý tài nguyên tập trung (đây mới là yếu tố xác định LAN)
- Cấu hình địa chỉ
  - IP tĩnh
  - Client plug & play by DHCP
  - DHCP kết hợp static IP – phân vùng địa chỉ IP
  - DHCP với địa chỉ IP đặt trước (reserved IP address)
- Giao thức DHCP
  - Tham khảo giáo trình, mục 3.2 “QUI HOẠCH VÀ GÁN ĐỊA CHỈ IP ĐỘNG VỚI DHCP”
  - Thiếu cơ chế xác thực DHCP ➔ Nguy cơ mất an toàn
- Bài thực hành:
  - Thiết lập DHCP cho LAN

dần bị thay thế bởi share clound

có routing, chỗ này hđ tối thiểu ở tầng 3

cung cấp thong tin IP, GW, DNS

Thường lấy đc thấp nhất 192.168.1.1 và thường cho PC-thiết bị hay kết nối nhất là 192.168.1.2 và 192.168.1.10->... để làm wifi

Thiếu cơ chế xác thực giữa client vs server (h đã đc khắc phục):

xem lại record p30-p33: Dạy về cách kết nối wifi theo kiểu public hay private

Wifi nhiều người sd (đc IP ko đủ) => thêm time tối đa 1 máy có thể giữ đia chỉ IP đó
- TH vẫn sd wifi mà muốn nhiều lần cùng sd 1 địa chỉ IP duy nhất (VD:sd máy in: p44 - đặt luôn tất cả trong 1 cái VLAN đỡ phải cấp cứng bằng tay)

TCP/IP là public ko có khái niệm quản lí tập chung như mạng nội bộ => nhiều công nghệ thiết kế cho TCPIP lỗi => Cisco có chỗ đứng

Inter-LAN & Virtual LAN

1 máy nội bộ bị nhiễm virut. Chạy ctr gì đó:
+Chạy 1 ctr DHCP server T2 (ko thể cấm đc)(học đc server chính, GW vẫn vậy, DNS khác là 1 nơi trỏ tới 1 server chứa 1 web fake) -> có 2 DHCP server, các máy gửi 1 gói tin DHCP discovery, nếu nhận lại 1 DHCP offer giả mạo đầu tiên của thằng virut,

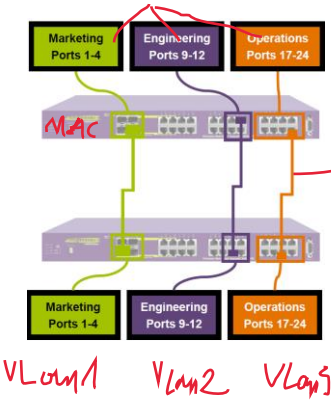
=> cấu hình chặn dhcp offer từ các cổng ngoại trừ tử cổng server thật trên tất cả switch

- LAN ➔ Inter-LAN:
  - Nhu cầu tăng kích thước mạng nội bộ: số host, khoảng cách giữa các host
  - Yêu cầu bảo mật theo từng vùng: phòng ban chia sẻ tài nguyên nội bộ & đảm bảo bên ngoài phòng ban không truy cập được

TH các máy xa về mặt địa lí

  - *Lưu ý:* Yêu cầu bảo mật theo từng vùng có thể xử lý bằng việc kiểm soát tài nguyên tập trung, nhưng phức tạp & cần có sự tham gia của Admin
- LAN ➔ Virtual LAN
  - Có sự phân tán địa lý của vùng bảo mật
  - Phòng ban gồm nhiều địa điểm cách xa nhau nhưng vẫn muốn áp dụng cơ chế bảo mật đơn giản theo broadcast zone (LAN)
  - LAN (VLAN) được khai báo với các host phân tán trên nhiều switch. Các switch phối hợp để vận hành broadcast zone phù hợp
  - Trunk port là cổng đặc biệt, thực hiện vận chuyển các frame của nhiều VLANs
- VLAN technology:
  - Port-based (Untagged) VLAN
  - Protocol-based VLAN
  - 802.1Q Tagged VLAN

các mạng lan ảo



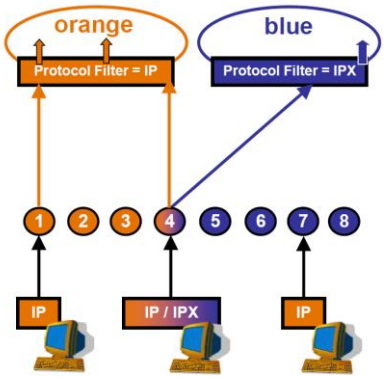
đường trunk

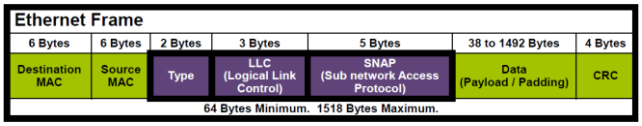
Vlan1 Vlan2 Vlan3

Port-based & Protocol-based VLAN

- Port-based:
  - VLAN được xây dựng bằng cách gán các cổng của switch với số hiệu VLAN.
  - Mỗi cổng switch được gán với duy nhất 1 VLAN
  - Ethernet frame nhận được từ 1 cổng
    ➔ chỉ switch sang các cổng thuộc cùng VLAN
- Protocol-based:
  - Admin khai báo "packet filter" tại switch, dựa trên các tiêu chí matching để xác định frame thuộc VLAN nào.
  - Các tiêu chí matching có thể dựa trên trường Type, LLC hoặc SNAP trong frame
  - Khai báo 1 cổng có thể tham gia nhiều VLAN. Vận hành sẽ xác định ethernet frame hiện tại thuộc VLAN nào để xử lý switch

giải pháp 1L 1 cổng chỉ cắm đc 1 Vlan

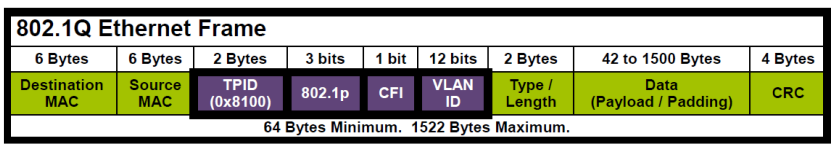




5

802.1Q Tagged VLAN

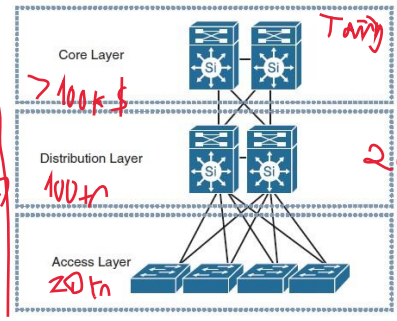
- Hoạt động tương tự cơ chế dựa trên Protocol, nhưng được IEEE chuẩn hóa (802.1)
- 802.1Q VLAN membership is based upon the VLAN ID in the 802.1Q field in the incoming packet.
- The 801.Q Tag contains four fields:
  - Tag Protocol ID (TPID)
  - User Priority
  - Canonical Format Indicator (CFI)
  - VLAN Identifier (VID)



6

Kết nối inter-LAN / inter-VLAN

- Mô hình ISO - TCP/IP
  - Inter-network = kết nối tầng 3
  - Static routing (đơn giản)
  - Dynamic routing khi số lượng LAN tăng lên
- Các khó khắn khi áp dụng internetworking cho mạng nội bộ
  - Mô hình chuẩn TCP/IP ➔ tư tưởng tài nguyên phân tán
  - Mạng nội bộ ➔ quản lý tập trung
    - Phát hiện một host bị bắn gói tin (virus) theo 1 cổng switch ➔ cô lập & cảnh báo trên toàn bộ hệ thống mạng nội bộ
    - Thiết lập các cấu hình phân bổ tài nguyên trên các switch của toàn bộ hệ thống mạng nội bộ
  - Bài toán kiểm soát & điều khiển network traffic:
    - Ưu tiên host/VLAN, hạn chế băng thông host/VLAN, v.v..
    - HUST: hạn chế băng thông kết nối Internet cho wifi VLAN trên tất cả các giảng đường?
    - Thiết lập kênh ưu tiên traffic từ hội trường C2 đến các giảng đường & ra Internet trong khoảng thời gian có buổi tư vấn tuyển sinh trực tuyến?
    - ➔ MPLS: kết hợp routing tại tầng 3 với switching tầng 2 để tối ưu hóa lưu lượng mạng
- Mô hình "de factor" Cisco layer-3 switching



7

7

Quản lý tài nguyên tập trung

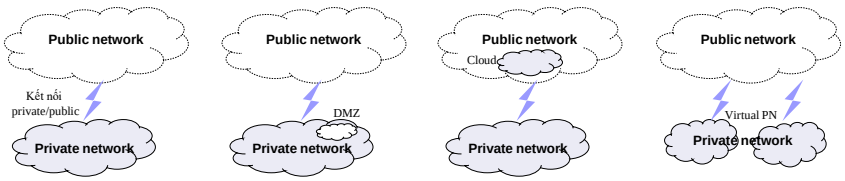
- Lightweight Directory Access Protocol
- Microsoft Active Directory
- Bài thực hành:
  - OpenLDAP
  - PXE & thin client

8

8

Mạng nội bộ/Mạng riêng (private network)

- Techopedia[1]: A private network is any connection within a specified network wherein restrictions are established to promote a secured environment. This type of network can be configured in such a way that devices outside the network cannot access it. Only a selected set of devices can access this type of network depending on the settings encoded in the network routers and access points. On the other hand, a public network is defined as a network that anyone can freely connect to little or no restriction.
- Intranet[2] by Wikipedia: An intranet is a computer network for sharing information, collaboration tools, operational systems, and other computing services only within an organization, and to the exclusion of access by outsiders to the organization. The term is used in contrast to public networks, such as the Internet, but uses most of the same technology based on the Internet Protocol Suite.
- Wikipedia[3]: In IP networking, a private network is a network that uses private IP address space. Both the IPv4 and the IPv6 specifications define private IP address ranges. These addresses are commonly used for local area networks (LANs) in residential, office, and enterprise environments
- Keywords:
  - Private / Public
  - Sharing
  - Access / Exclusion
  - Private IP



[1] https://www.techopedia.com/definition/26423/private-network
[2] https://en.wikipedia.org/wiki/Intranet
[3] https://en.wikipedia.org/wiki/Private_network

Private IP address