

Thiết kế mạng IP

Bài 2: Mạng nội bộ (Private network)

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

1



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

2

2

LAN

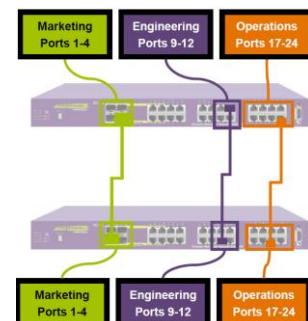
- Local Area Network
 - Đơn giản nhất
 - Hoạt động tầng 2 (thậm chí là tầng 1)
 - Dễ dàng share resource (thư mục, file, máy in, v.v..)
 - Quản lý tài nguyên tập trung (đây mới là yếu tố xác định LAN)
- Cấu hình địa chỉ
 - IP tĩnh
 - Client plug & play by DHCP
 - DHCP kết hợp static IP – phân vùng địa 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

3

3

Inter-LAN & Virtual LAN

- 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
 - 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



4

4

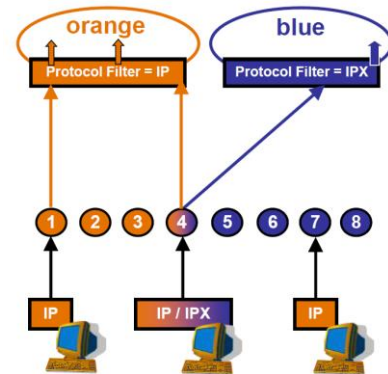
Port-based & Protocol-based VLAN

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



Ethernet Frame						
6 Bytes	6 Bytes	2 Bytes	3 Bytes	5 Bytes	38 to 1492 Bytes	4 Bytes
Destination MAC	Source MAC	Type	LLC (Logical Link Control)	SNAP (Sub network Access Protocol)	Data (Payload / Padding)	CRC
64 Bytes Minimum. 1518 Bytes Maximum.						

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)

802.1Q Ethernet Frame								
6 Bytes	6 Bytes	2 Bytes	3 bits	1 bit	12 bits	2 Bytes	42 to 1500 Bytes	4 Bytes
Destination MAC	Source MAC	TPID (0x8100)	802.1p	CFI	VLAN ID	Type / Length	Data (Payload / Padding)	CRC
64 Bytes Minimum. 1522 Bytes Maximum.								

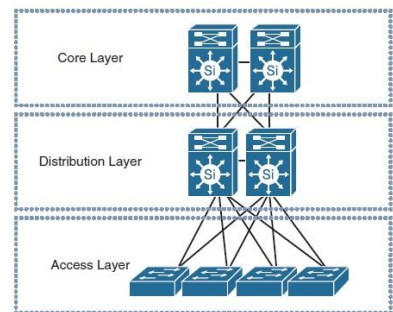
6

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 khăn 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



7

7

Quản lý tài nguyên tập trung

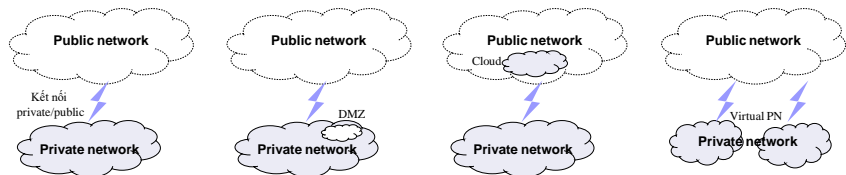
- Lightweight Directory Access Protocol
- Microsoft Active Directory
- Bài thực hành:
 - OpenLDAP
 - PXE & thin client

8

8

Mạng nội bộ/Mạng riêng (private network)

- Techopedia¹: 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.
- Intranet² 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.
- Wikipedia³: 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