Họ và tên: Nguyễn Nhật Trường Lớp: CTK45A MSSV: 2111903

Bài 1:

Địa chỉ MAC đích: b0 be 76 df cc 34 OUI: b0 be 76 TP-Link Technologies LTD

Địa chỉ MAC nguồn: 00 08 ca 33 69 fa OUI: 00 08 ca TwinHan Technology LTD

Type của Ethernet frame là: 08 00 = IPv4

Version: 4

IHL: 5

TOS: 00

Total Length: 00 28

Indentifier: 2e b7

Flag: F1 = 010; F2 = 0 0000 0000 0000

TTL: 8016 = 12810

Hệ điều hành: Window XP, 7,8

Protocol: 06 -> TCP

Checksum: 46 0d

Source Add: c0 a8 00 65 -> 192.168.00.101

Destination Add: ac d9 18 25 ->172.217.24.37

Source Port: d2 27 -> 210 39

Destination Port: 01 bb -> 1 187

Sequence Number: 3d 78 3a 68

Acknowledgment number: d4 37 32 bb

Flag: 10 -ACK

Window size: 20 2b

Bài 2:

Địa chỉ MAC đích: b0 be 76 df cc 34 OUI: b0 be 76 TP-Link Technologies LTD

Địa chỉ MAC nguồn: 00 08 ca 33 69 fa OUI: 00 08 ca TwinHan Technology LTD

Type của Ethernet frame là: 08 00 = IPv4

Version: 4

IHL: 5

TOS: 00

Total Length: 00 3d

Indentifier: d1 ad

Flag: F1 = 010; F2 = 0 0000 0000 0000

TTL: 8016 = 12810

Hệ điều hành: Window XP, 7,8

Protocol: 11 -> UDP

Checksum: d8 ba

Source Add: c0 a8 00 65 -> 192.168.00.101

Destination Add: 4a 7d 44 bd->74.125.68.189

Source Port: cc ce -> 52430

Destination Port: 01 bb -> 443 -> HTTPS

Bài 3:

Địa chỉ MAC đích: b0 be 76 df cc 34 OUI: b0 be 76 TP-Link Technologies LTD

Địa chỉ MAC nguồn: 00 08 ca 33 69 fa OUI: 00 08 ca TwinHan Technology LTD

Type của Ethernet frame là: 08 00 = IPv4

Version: 4

IHL: 5

TOS: 00

Total Length: 00 3c

Indentifier: 28 16

Flag: F1 = 000; F2 = 0 0000 0000 0000

TTL: 80 16 = 128 10

Hệ điều hành: Window XP, 7,8

Protocol: 01 -> ICMP

Checksum: 41 8e

Source Add: c0 a8 00 65 -> 192.168.00.101

Destination Add: 08 08 08 08->8.8.8.8

ICMP request

Bài 4:

a) Địa chỉ MAC nguồn là của PCA, địa chỉ MAC của đích là của bộ định tuyến 000D

ethernet được gửi đến công tắc s1, công tắc s1 nhận frame của địa chỉ MAC nguồn có trong bảng địa chỉ MAC của nó sẽ kiểm tra địa chỉ MAC đích và nếu địa chỉ MAC đích đó không có trong bảng. MAC của công tắc s1 nó gửi tới tất cả các cổng. PCB nhận frame ethernet và vì địa chỉ MAC đích không khớp với địa chỉ MAC của chính nó nên nó không chấp phần còn lại của khung switch s2 nhận khung ethernet kiểm tra địa chỉ MAC nguồn nằm trong địa chỉ MAC của nó, nó sẽ kiểm tra địa chỉ MAC đích của frame có trong địa chỉ MAC, vì địa chỉ MAC khớp với địa chỉ MAC nguồn nên sẽ gửi tính hiệu lại .

b) Địa chỉ MAC nguồn là của PCA, địa chỉ MAC của đích là của bộ định tuyến 000D

ethernet được gửi đến công tắc s1, công tắc s1 nhận frame của địa chỉ MAC nguồn có trong bảng địa chỉ MAC của nó sẽ kiểm tra địa chỉ MAC đích và nếu địa chỉ MAC đích đó không có trong bảng. MAC của công tắc s1 nó gửi tới tất cả các cổng. PCB nhận frame ethernet và vì địa chỉ MAC đích không khớp với địa chỉ MAC của chính nó nên nó không chấp phần còn lại của khung switch s2 nhận khung ethernet kiểm tra địa chỉ MAC nguồn nằm trong địa chỉ MAC của nó, nó sẽ kiểm tra địa chỉ MAC đích của khung không có trong địa chỉ MAC của nó để trôi nổi, loại bỏ tất cả các cổng. PCC nhận khung ethernet và vì địa chỉ MAC đích không khớp với địa chỉ MAC của chính nó nên nó không chấp nhận phần còn lại của frame ethernet, bộ định tuyến nhận khung ethernet và vì địa chỉ MAC đích không khớp với MAC của địa chỉ nó chấp nhận phần còn lại của khung bây giờ.

Bài 5:

Địa chỉ đích sẽ là địa chỉ IP đích của PCC 192.168.1.50 vì vậy PCA là cache của chúng cho địa chỉ ip 192.168.1.50 bời vì nó không có trong cache của nó, nó sẽ tạm dừng gói và tạo một người yêu cầu ARP, yêu cầu nghệ thuật chứa địa chỉ ipv4 đích. PCA đang muốn tìm hiểu yêu cầu ARP được gửi dưới dạng broadcast, vì vậy mọi người trên mạng sẽ cần kiểm tra khung ethernet này và xử lý yêu cầu ARP. Để PCA gửi nó đến bộ chuyển mạch vì đó là một bộ chuyển mạch sẽ bị tràn nó rút ra tất cả các cổng ngoại trừ cổng mà nó đi vào trên PCB nhận được broadcast, vì vậy nó phải xử lý nó và quy trình một phần của chúng tôi sẽ kiểm tra yêu cầu ARP, nó so sánh địa chỉ ipv4 của chính nó với địa chỉ ipv4 đích và thông báo rằng chúng không giống nhau vì vậy nó không cần gửi trả lời ARP, bộ định tuyến R1 cũng nhận được yêu cầu ARP này, quy trình của chúng tôi sẽ kiểm tra địa chỉ ipv4 của chính nó và so sánh địa chỉ đó với địa chỉ ipv4 đích và cũng nhận ra đây không phải là địa chỉ ipv4 của nó nên nó không cần gửi trả lời ARP bằng cách các bộ định tuyến sẽ không chuyển tiếp các yêu cầu ARP ra các cổng khác. PCC nhận được yêu cầu ARP so sánh địa chỉ ipv4 của nó với địa chỉ ipv4 đích và thông báo rằng đó là mục tiêu dự định của yêu cầu ARP mà địa chỉ ipv4 đích khớp với địa chỉ của nó. địa chỉ ipv4 riêng nên PCC sẽ cần gửi phản hồi ARP

Bài 7:

Câu 1: 00-60-2F-3A-07-CC

Câu 2: show mac address-tabletpro

-d -> delete

-s -> add

ARP có những phương thức bảo mật an toàn rất cao và được sử dụng khá rộng rãi.

Với giao thức ARP người dùng có thể dễ dàng tìm được địa chỉ MAC nếu đã biết được địa chỉ IP cùng hệ thống.

Không nên cấu hình các end node để "biết" các địa chỉ MAC. Khi nào cần thiết chúng sẽ được tìm thấy.

Mục đích của ARP là enable mọi host trên mạng cho phép người dùng tạo một ánh xạ giữa địa chỉ vật lý và địa chỉ IP.

Bảng ARP hay ARP cache là nơi tập hợp các ánh xạ hay các bảng được lưu trữ trong host