Báo cáo bài tập

I, DHCP

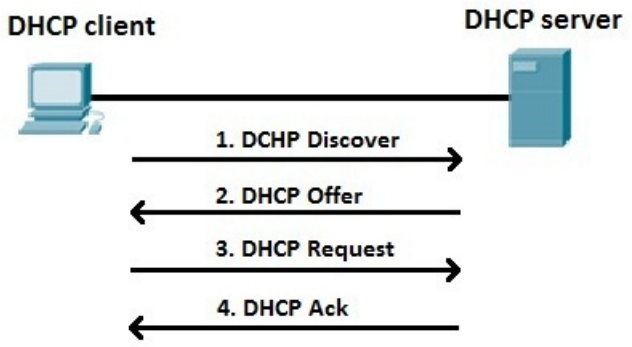
1, Định nghĩa

Dynamic Host Configuration Protocol (DHCP - giao thức cấu hình động máy chủ) là một giao thức cho phép cấp phát địa chỉ IP một cách tự động cùng với các cấu hình liên quan khác như subnet mark và gateway mặc định. Máy tính được cấu hình một cách tự động vì thế sẽ giảm việc can thiệp vào hệ thống mạng. Nó cung cấp một database trung tâm để theo dõi tất cả các máy tính trong hệ thống mạng. Mục đích quan trọng nhất là tránh trường hợp hai máy tính khác nhau lại có cùng địa chỉ IP.

2, Nguyên tắc hoạt động

DHCP là một giao thức Internet có nguồn gốc ở BOOTP (bootstrap protocol), được dùng để cấu hình các Clients không đĩa. DHCP khai thác ưu điểm của giao thức truyền tin và các kỹ thuật khai báo cấu hình được định nghĩa trong BOOTP, trong đó có khả năng gán địa chỉ. Sự tương tự này cũng cho phép các bộ định tuyến hiện nay chuyển tiếp các thông điệp BOOTP giữa các mạng con cũng có thể chuyển tiếp các thông điệp DHCP. Vì thế, DHCP Server có thể đánh địa chỉ IP cho nhiều mạng con.

3, Các bước hoạt động



Bước 1: *Máy trạm khởi động với "địa chỉ IP rỗng" cho phép liên lạc với DHCP Servers bằng giao thức TCP/IP. Nó broadcast một thông điệp DHCP Discover chứa địa chỉ MAC và tên máy tính để tìm DHCP Server .*
Bước 2: *Nhiều DHCP Server có thể nhận thông điệp và chuẩn bị địa chỉ IP cho máy trạm. Nếu máy chủ có cấu hình hợp lệ cho máy trạm, nó gửi thông điệp "DHCP Offer" chứa địa chỉ MAC của khách, địa chỉ IP "Offer", mặt nạ mạng con (subnet mask), địa chỉ IP của máy chủ và thời gian cho thuê đến Client. Địa chỉ "offer" được đánh dấu là "reserve" (để dành).*
Bước 3: *Khi Client nhận thông điệp DHCP Offer và chấp nhận một trong các địa chỉ IP, Client sẽ gửi thông điệp DHCP Request để yêu cầu IP phù hợp cho DHCP Server thích hợp.*
Bước 4: *Cuối cùng, DHCP Server khẳng định lại với Client bằng thông điệp DHCP Acknowledge.*

4, Mô hình lab

5, Cấu hình

- Tải DHCP: Bài hướng dẫn làm trên ubuntu 16.04
  root@cuong:~$ apt-get install isc-dhcp-server
- Vào file cấu hình:
  root@cuong:~$ vi /etc/dhcp/dhcpd.conf
- Sửa lại file configure cho phù hợp:
  option domain-name server2.cuong.vn;
  option domain-name-servers dhcp.server2.cuong.vn, 8.8.8.8, 8.8.4.4;
  authoritative; // Uncomment
- Mô tả IP range:
  subnet 192.168.1.0 netmask 255.255.255.0 {
  option routers 192.168.1.254; // gateway
  option subnet-mask 255.255.255.0; // subnet
  range dynamic-bootp 192.168.1.100 192.168.1.200; // IP range
  }
- Khởi động lại dịch vụ:
  root@cuong:~$ initctl start isc-dhcp-server

II, DNS

1, Định nghĩa

DNS là từ viết tắt trong tiếng Anh của Domain Name System, là Hệ thống phân giải tên được phát minh vào năm 1984 cho Internet, chỉ một hệ thống cho phép thiết lập tương ứng giữa địa chỉ IP và tên miền. Hệ thống tên miền (DNS) là một hệ thống đặt tên theo thứ tự cho máy vi tính, dịch vụ, hoặc bất kỳ nguồn lực tham gia vào Internet. Nó liên kết nhiều thông tin đa dạng với tên miền được gán cho những người tham gia. Quan trọng nhất là, nó chuyển tên miền có ý nghĩa cho con người vào số định danh (nhị phân), liên kết với các trang thiết bị mạng cho các mục đích định vị và địa chỉ hóa các thiết bị khắp thế giới.

2, Nguyên tắc hoạt động

Mỗi nhà cung cấp dịch vụ vận hành và duy trì DNS server riêng của mình, gồm các máy bên trong phần riêng của mỗi nhà cung cấp dịch vụ đó trong Internet. Tức là, nếu một trình duyệt tìm kiếm địa chỉ của một website thì DNS server phân giải tên website này phải là DNS server của chính tổ chức quản lý website đó chứ không phải là của một tổ chức (nhà cung cấp dịch vụ) nào khác.

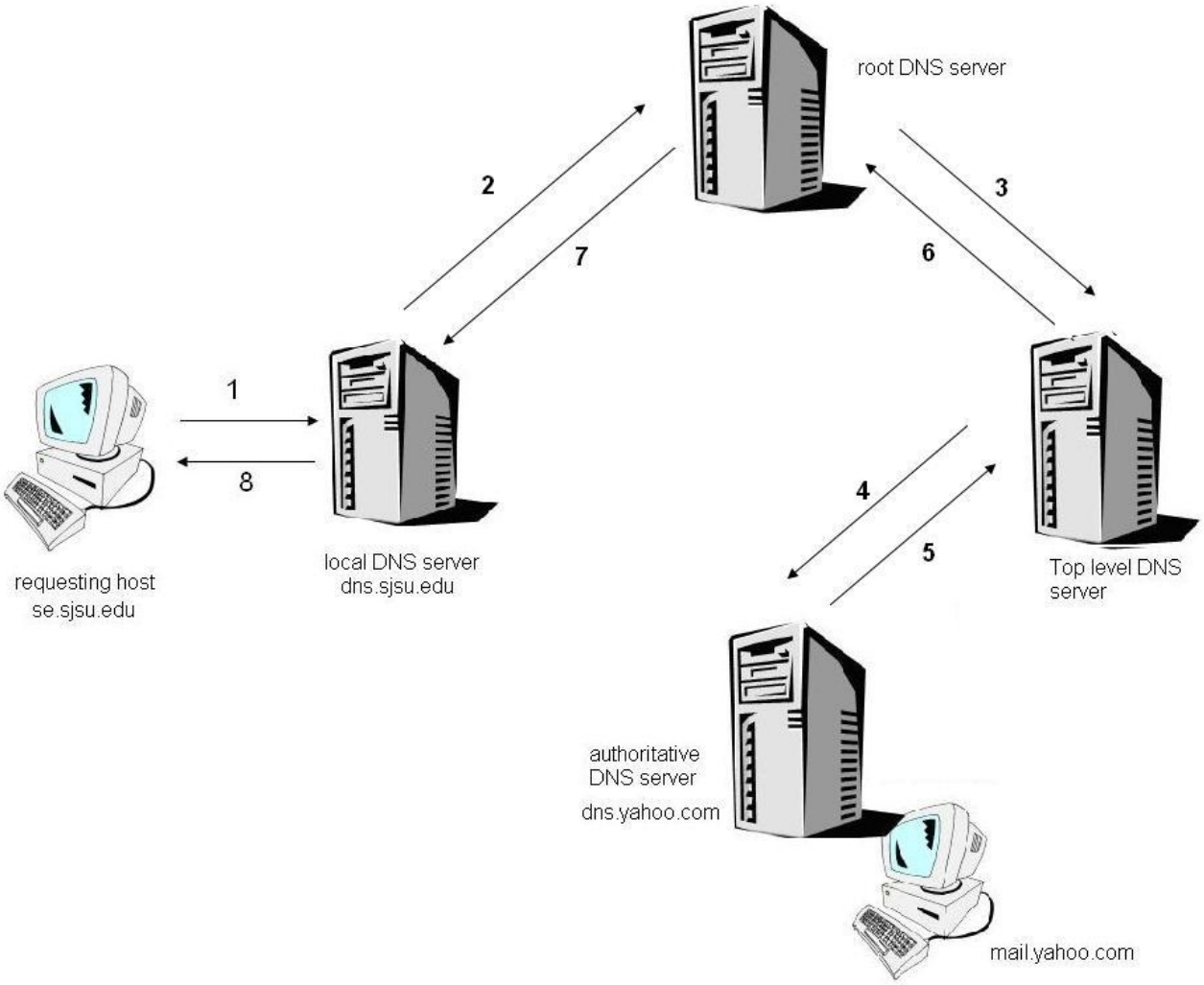
INTERNIC (Internet Network Information Center) chịu trách nhiệm theo dõi các tên miền và các DNS server tương ứng. INTERNIC là một tổ chức được thành lập bởi NFS (National Science Foundation), AT&T và Network Solution, chịu trách nhiệm đăng ký các tên miền của Internet. INTERNIC chỉ có nhiệm vụ quản lý tất cả các DNS server trên Internet chứ không có nhiệm vụ phân giải tên cho từng địa chỉ.

DNS có khả năng tra vấn các DNS server khác để có được một cái tên đã được phân giải. DNS server của mỗi tên miền thường có hai việc khác biệt. Thứ nhất, chịu trách nhiệm phân giải tên từ các máy bên trong miền về các địa chỉ Internet, cả bên trong lẫn bên ngoài miền nó quản lý. Thứ hai, chúng trả lời các DNS server bên ngoài đang cố gắng phân giải những cái tên bên trong miền nó quản lý. - DNS server có khả năng ghi nhớ lại những tên vừa phân giải. Để dùng cho những yêu cầu phân giải lần sau. Số lượng những tên phân giải được lưu lại tùy thuộc vào quy mô của từng DNS.

3, Các bước hoạt động

Bước 1: *Máy client đặt một truy vấn tìm một địa chỉ web với tên miền abc.com cho máy chủ DNS nội bộ.*
Bước 2: *Nếu máy chủ DNS có chứa địa chỉ tên miền đó sẽ trả về kết quả cho client. Nếu máy chủ DNS nội bộ không biết IP của tên miền đó, nó sẽ gửi các truy vấn tới các máy chủ DNS lân cận để tìm ra địa chỉ IP tương ứng với tên miền đã nhận.*
Bước 3: *Máy chủ DNS trả về kết quả cho client.*

Ví dụ:



1, Client yêu cầu máy chủ DNS cục bộ ‘dns.sjsu.edu’ để tìm kiếm một truy vấn DNS 'mail.yahoo.com‘ và cung cấp địa chỉ IP của nó.

2, Máy chủ DNS cục bộ yêu cầu máy chủ DNS root cho địa chỉ IP của 'mail.yahoo.com‘

3, Máy chủ DNS gốc tìm thấy hậu tố ‘com’ trong truy vấn và yêu cầu một trong những máy chủ DNS cấp cao chịu trách nhiệm về miền ".com“

4, Máy chủ cấp cao gửi yêu cầu tới máy chủ đầu cuối, máy chủ có thẩm quyền.

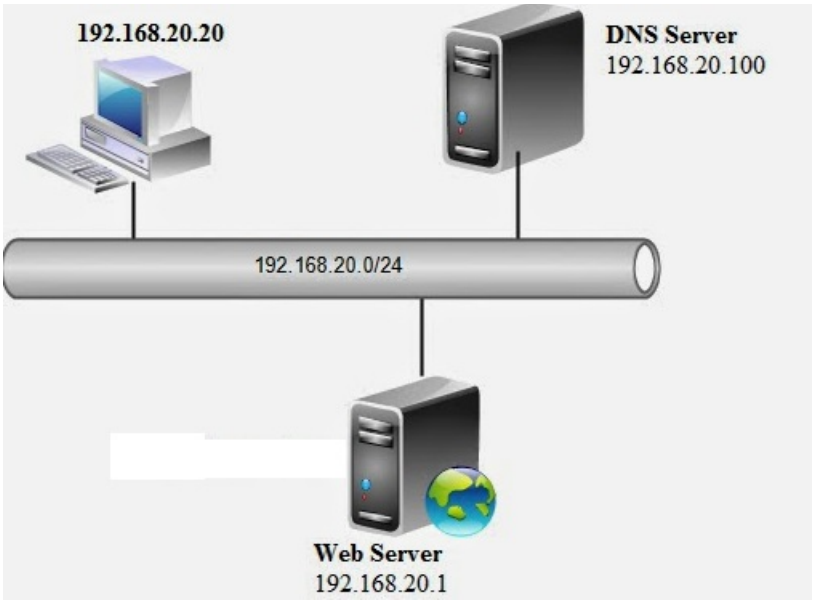
5, Máy chủ DNS có thẩm quyền của Yahoo trả về địa chỉ IP cho máy chủ DNS cấp cao nhất truy cập DNS có thẩm quyền

6, Máy chủ DNS cấp cao nhất trả về địa chỉ IP này tới máy chủ DNS gốc

7, Máy chủ DNS gốc sẽ trả lại địa chỉ IP cho truy vấn DNS cục bộ.

8, Máy client nhận được địa chỉ IP của truy vấn mong muốn của nó.

4, Mô hình lab



5, Cấu hình

- Cài đặt DNS: bài hướng dẫn trên CentOS 6.8
  yum -y install bind caching-nameserver bind-chroot bind-utils
- Cấu hình file named.conf (nằm trong /var/named/chroot/etc/):
  acl mynet (
  192.168.20.0/24;
  127.0.0.1;
)

```
        options {
                allow-transfer {none;};
                directory "/var/named";
                dump-file "/var/named/data/cache_dump.db";
                statistics-file "/var/named/data/named_stats.txt";
                memstatistics-file      "var/named/data/named_mem_stats.txt";
                notify          yes;
        };

        zone "huucuong.vn" IN {
                type master;
                file "huucuong.vn";
        };

        zone "20.168.192.in-addr.arpa" {
                type master;
                file "20.168.192.in-addr.arpa.db";
};
```

- Cấu hình phân giải thuận file /var/named/chroot/var/named/huucuong.vn:

```
- $TTL   86400
- @      IN     SOA    server2.huucuong.vn. root (
-                       42            ; Serial
-                       3H            ; Refresh
-                       15M           ; Retry
-                       1W            ; Expire
-                       1D )    ; Minimum
-              IN     NS     server2.huucuong.vn.
-              IN     MX     10 server3
-        1D    IN     A      192.168.20.3
-
- server3 1D    IN     A      192.168.20.3
- server2 1D    IN     A      192.168.20.2
- server1 1D    IN     A      192.168.20.1
- www           1D     IN     CNAME   server3
- mail          1D     IN     CNAME   server3
- fpt           1D     IN     CNAME   server3
```

- Cấu hình file phân giải nghịch /var/named/chroot/var/named/20.168.192.in-addr.arpa.db

```
@       IN     SOA    server2.huucuong.vn. root (
                      2011030801            ; Serial
                      43200         ; Refresh
                      3600          ; Retry
                      3600000       ; Expire
                      2592000 )     ; Minimum

;       Thiet lap cac record

@       IN     NS     server2.huucuong.vn.
1       IN     PTR    server1.huucuong.vn.
2       IN     PTR    server2.huucuong.vn.
2       IN     PTR    server3.huucuong.vn.
~
```

III, ARP

1, Định nghĩa

Giao thức phân giải địa chỉ (Address Resolution Protocol hay ARP) là một giao thức truyền thông được sử dụng để chuyển địa chỉ từ tầng mạng (Internet layer) sang tầng liên kết dữ liệu theo mô hình OSI. Đây là một chức năng quan trọng trong giao thức IP của mạng máy tính. ARP được định nghĩa trong RFC 826 vào năm 1982, là một tiêu chuẩn Internet STD 37.
ARP được sử dụng để từ một địa chỉ mạng (ví dụ một địa chỉ IPv4) tìm ra địa chỉ vật lý như một địa chỉ Ethernet (địa chỉ MAC), hay còn có thể nói là phân giải địa chỉ IP sang địa chỉ máy. ARP đã được thực hiện với nhiều kết hợp của công nghệ mạng và tầng liên kết dữ liệu, như IPv4, Chaosnet,..
Trong mạng máy tính của phiên bản IPv6, chức năng của ARP được cung cấp bởi Neighbor Discovery Protocol (NDP).

2, Nguyên tắc hoạt động

Trong mạng LAN:

Khi một thiết bị mạng muốn biết địa chỉ MAC của một thiết bị mạng nào đó mà nó đã biết địa chỉ ở tầng network (IP, IPX…) nó sẽ gửi một ARP request bao gồm địa chỉ MAC address của nó và địa chỉ IP của thiết bị mà nó cần biết MAC address trên toàn bộ một miền broadcast. Mỗi một thiết bị nhận được request này sẽ so sánh địa chỉ IP trong request với địa chỉ tầng network của mình. Nếu

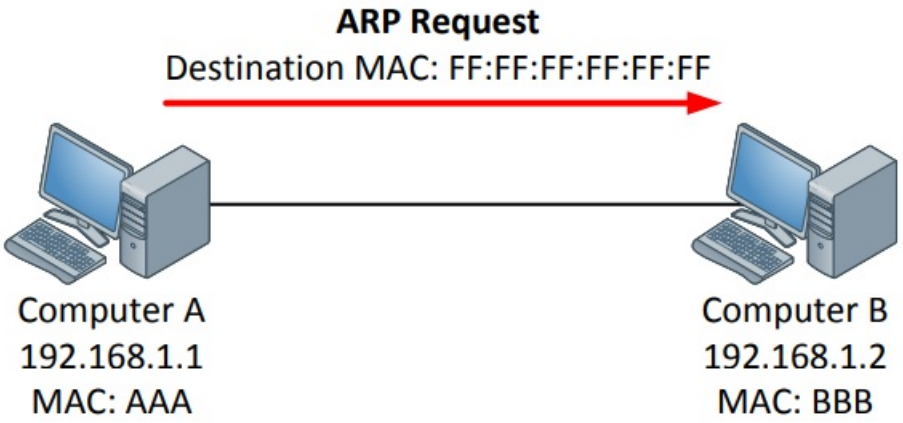
trùng địa chỉ thì thiết bị đó phải gửi ngược lại cho thiết bị gửi ARP request một gói tin (trong đó có chứa địa chỉ MAC của mình).

Trong hệ thống mạng LAN:

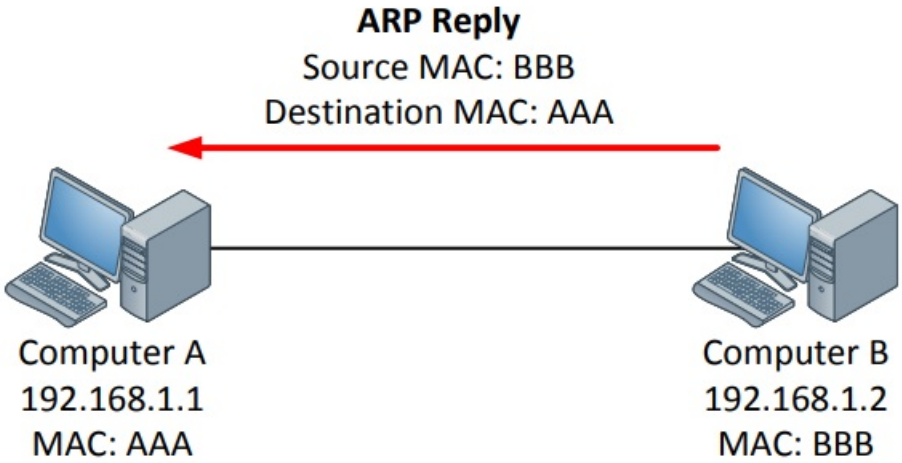
Hoạt động của ARP trong một môi trường phức tạp hơn đó là hai hệ thống mạng gắn với nhau thông qua một Router C. Máy A thuộc mạng A muốn gửi gói tin đến máy B thuộc mạng B. Do các broadcast không thể truyền qua Router nên khi đó máy A sẽ xem Router C như một cầu nối hay một trung gian (Agent) để truyền dữ liệu. Trước đó, máy A sẽ biết được địa chỉ IP của Router C (địa chỉ Gateway) và biết được rằng để truyền gói tin tới B phải đi qua C. Tất cả các thông tin như vậy sẽ được chứa trong một bảng gọi là bảng định tuyến (routing table). Bảng định tuyến theo cơ chế này được lưu giữ trong mỗi máy. Bảng định tuyến chứa thông tin về các Gateway để truy cập vào một hệ thống mạng nào đó.

3, Các bước hoạt động

Trong mạng LAN:

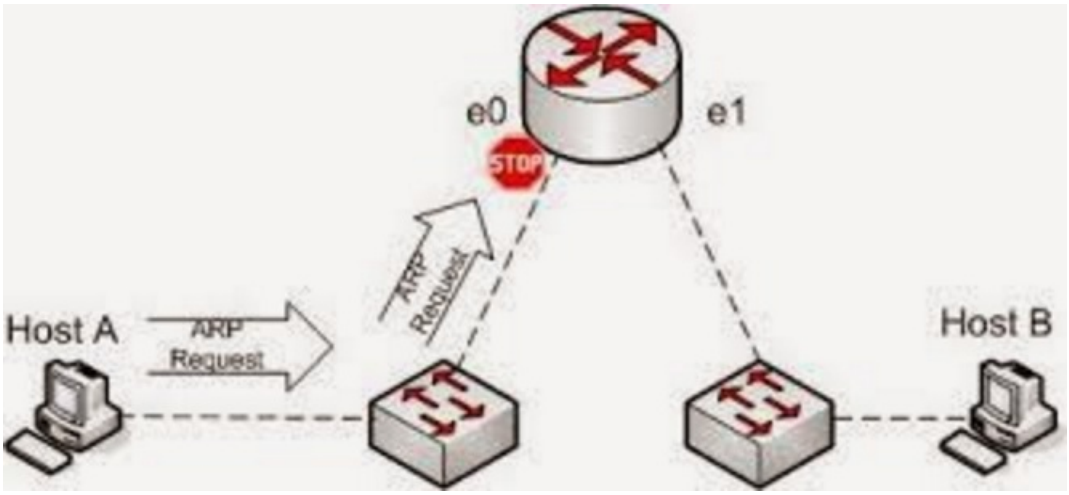


Bước 1: máy A gửi ARP Request để hỏi xem máy nào có địa chỉ IP là x.x.x.x gửi theo kiểu Broadcast tới các máy trong mạng địa chỉ MAC đích là FF:FF:FF:FF:FF:FF



Bước 2: Máy B nhận ra IP mà máy A đang tìm là IP của mình nên gửi lại gói ARP Reply, với nội dung gói có địa chỉ nguồn là MAC của B, đích là MAC của A.
Bước 3: Máy A nhận được địa chỉ MAC của máy B lưu lại bảng ARP và bắt đầu quá trình trao đổi dữ liệu.

Trong hệ thống mạng LAN



Bước 1: Máy A sẽ truyền một ARP Request theo dạng Broadcast để tìm địa chỉ MAC của Port X
Bước 2: Router C nhận được và cung cấp lại cho A một địa chỉ MAC của port X.
Bước 3: Máy A truyền Packet đến port X của router C
Bước 4: Router C nhận được packet. Trong Packet này chứa địa chỉ IP của máy B.
Bước 5: Router C sẽ gửi ARP Request theo dạng Broadcast trong mạng của máy B để tìm địa chỉ MAC của B.
Bước 6: Máy B nhận được và trả lời lại cho router biết địa chỉ MAC của mình.
Bước 7: Sau khi nhận được địa chỉ MAC của máy B thì router sẽ gửi Packet đến máy B.

IV, GRE

1, Định nghĩa

Generic Routing Encapsulation (GRE) là một trong những cơ chế đường hầm có sẵn sử dụng IP làm giao thức vận chuyển và có thể được sử dụng để thực hiện nhiều giao thức khác nhau. Đường hầm hoạt động như các liên kết điểm-điểm ảo có hai điểm cuối xác định bởi đường hầm và địa chỉ đích đường hầm tại mỗi điểm cuối.

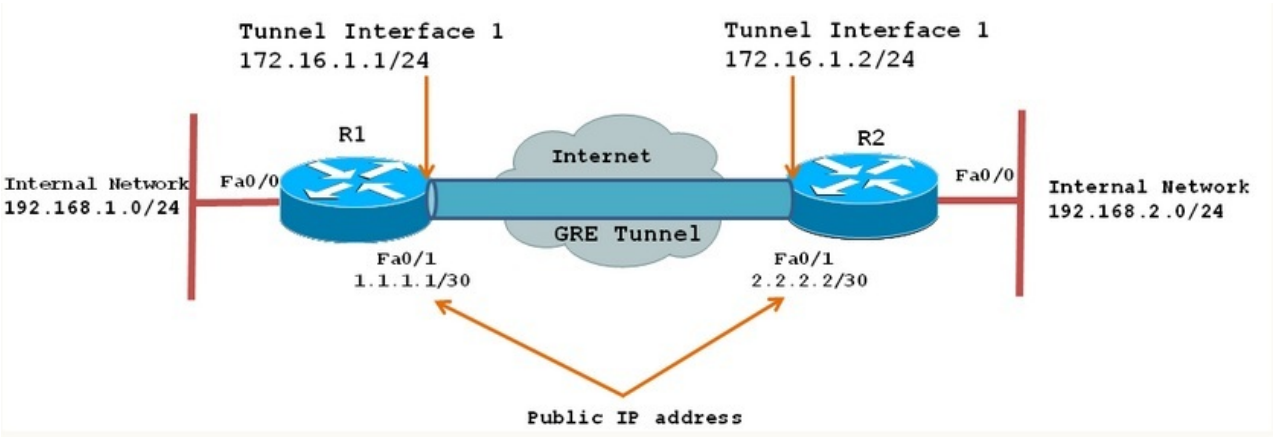
2, Nguyên tắc hoạt động

Đặt gói tin IP vào một gói tin IP khác để di chuyển trong đường hầm.

3, Các bước hoạt động

Bước 1: Gói tin được gửi từ mạng 192.168.1.0/24 đi tới router 1
Bước 2: Gói tin đi từ router 1 tới router 2 qua đường hầm ảo, lúc này gói tin sẽ được đóng gói lại vào một gói khác và được mã hoá. Khi tới đầu bên kia sẽ được mở ra.
Bước 3: Router 2 gửi gói tin tới máy đích sau khi mở gói tin nhận từ tunner.

4, Mô hình lab



5, Cấu hình

- Router 1
  R1(config)# interface Tunnel1
  R1(config-if)# ip address 172.16.1.1 255.255.255.0
  R1(config-if)# ip mtu 1400
  R1(config-if)# ip tcp adjust-mss 1360
  R1(config-if)# tunnel source 1.1.1.1
  R1(config-if)# tunnel destination 2.2.2.2
- Router 2
  R2(config)# interface Tunnel1
  R2(config-if)# ip address 172.16.1.2 255.255.255.0
  R2(config-if)# ip mtu 1400
  R2(config-if)# ip tcp adjust-mss 1360
  R2(config-if)# tunnel source 2.2.2.2
  R2(config-if)# tunnel destination 1.1.1.1

V, VXLAN

1, Định nghĩa

VXLAN là một công nghệ ảo hóa hạ tầng mạng, mang tới hạ tầng mạng được trừu tượng hóa, linh động và có khả năng mở rộng trên toàn datacenter. VXLAN đem lại một cấu trúc có khả năng mở rộng cho các ứng dụng của Doanh nghiệp trên các cluster (chứa nhiều server) và pod mà không cấu hình lại hạ tầng mạng vật lý. Nó sử dụng MAC-in-UDP để đóng gói.
VXLAN giải quyết ba vấn đề chính:
1. 16 triệu VNIs (broadcast domains) so với 4 nghìn được cung cấp bởi các VLAN truyền thống.
2. Cho phép Layer 2 được mở rộng bất cứ nơi nào trong một mạng IP.
3. Tối ưu hoá flooding.

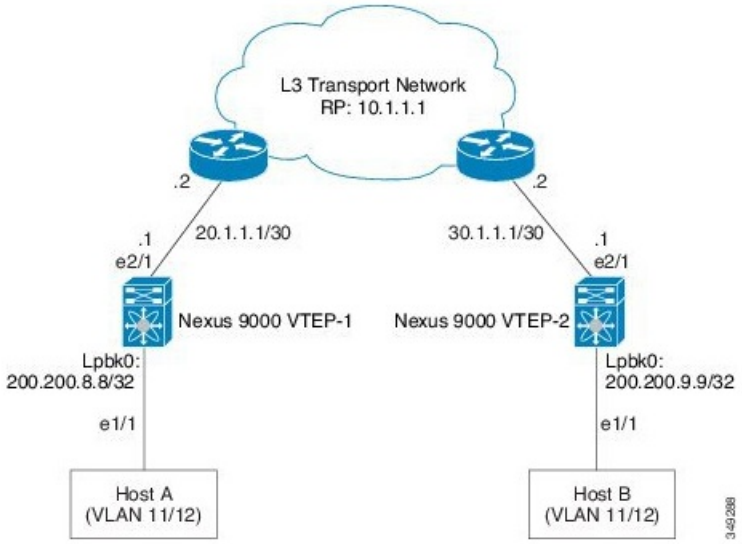
2, Nguyên tắc hoạt động

Mỗi VTEP được cấu hình một cách độc lập. Để học được địa chỉ MAC của máy khác thì quá trình như sau:
● Gửi gói ARP request, chưa biết unicast, multicast và traffic
● Khám phá VTEPs từ xa
● Tìm hiểu địa chỉ MAC máy chủ từ xa và ánh xạ MAC-to-VTEP cho từng phân khúc VXLAN

3, Các bước hoạt động

Bước 1: Host A gửi một ARP request cho IP host B, trên mạng VXLAN lớp 2 của A.
Bước 2: VTEP-1 nhận được gói ARP từ A, nó vẫn chưa có địa chỉ B trong bảng của nó, nó gửi multicast IP tới tất cả các VXLAN mà nó biết. Gói tin gửi đi có địa chỉ nguồn là IP của VTEP-1, đích là VTEP-2
Bước 3: VTEP-2 nhận được gói tin, nó mở gói tin ra kiểm tra VNID của nó trong VXLAN header. Nếu đúng nó sẽ thay đổi VNID và gửi các gói ARP trong mạng của nó, cùng với đó nó lưu lại MAC của máy A.
Bước 4: Máy B nhận được ARP, nhận ra là IP của B nó gửi lại địa chỉ MAC của nó và lưu lại IP-A-to-MAC-A vào bảng của nó.
Bước 5: VTEP-2 nhận được MAC của B, gửi ngược lại gói ARP reply cho VTEP-1. Gói này được đóng trong playload UDP
Bước 6: VTEP-1 nhận được ARP reply từ VTEP-2, nó gửi trả lời lại cho host A đồng thời lưu địa chỉ B lại vào bảng của nó.
Bước 7: Đường truyề giữa host A và host B được thiết lập, và tạo đường hầm VXLAN giữa chúng.

4, Mô hình lab



5, Cấu hình

- VTEP-1
  switch-vtep-1(config)# feature ospf
  switch-vtep-1(config)# router ospf 1
  switch-vtep-1(config-router)# router-id 200.200.8.8
  switch-vtep-1(config)# interface loopback0
  switch-vtep-1(config-if)# ip address 200.200.8.8/32
  switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
  switch-vtep-1(config)# interface e2/1
  switch-vtep-1(config-if)# ip address 20.1.1.1/30
  switch-vtep-1(config-if)# ip router ospf 1 area 0.0.0.0
  switch-vtep-1(config-if)# ip pim sparse-mode
  switch-vtep-1(config)# feature nv overlay
  switch-vtep-1(config)# feature vn-segment-vlan-based
  switch-vtep-1(config)# interface e1/1
  switch-vtep-1(config-if)# switchport
  switch-vtep-1(config-if)# switch port mode trunk

switch-vtep-1(config-if)# switch port allowed vlan 11-12
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config)# vlan 11
switch-vtep-1(config-vlan)# vn-segment 10011
switch-vtep-1(config)# vlan 12
switch-vtep-1(config-vlan)# vn-segment 10012
switch-vtep-1(config)# interface nve1
switch-vtep-1(config-if)# no shutdown
switch-vtep-1(config-if)# source-interface loopback0
switch-vtep-1(config-if)# member vni 10011
switch-vtep-1(config-if)# ingress-replication protocol static
switch-vtep-1(config-if)# peer_ip 200.200.9.9
switch-vtep-1(config-if)# member vni 10012
switch-vtep-1(config-if)# ingress-replication protocol static
switch-vtep-1(config-if)# peer_ip 200.200.9.9
switch-vtep-1(config-vlan)# exit

- VTEP-2
  switch-vtep-2(config)# feature ospf
  switch-vtep-2(config)# router ospf 1
  switch-vtep-2(config-router)# router-id 200.200.9.9
  switch-vtep-2(config)# interface loopback0
  switch-vtep-2(config-if)# ip address 200.200.9.9/32
  switch-vtep-2(config-if)# ip router ospf 1 area 0.0.0.0
  switch-vtep-2(config)# interface e2/1
  switch-vtep-2(config-if)# ip address 30.1.1.1/30
  switch-vtep-2(config-if)# ip router ospf 1 area 0.0.0.0
  switch-vtep-2(config-if)# ip pim sparse-mode
  switch-vtep-2(config)# feature nv overlay
  switch-vtep-2(config)# feature vn-segment-vlan-based
  switch-vtep-2(config)# interface e1/1
  switch-vtep-2(config-if)# switchport
  switch-vtep-2(config-if)# switch port mode trunk
  switch-vtep-2(config-if)# switch port allowed vlan 11-12
  switch-vtep-2(config-if)# no shutdown
  switch-vtep-2(config)# vlan 11
  switch-vtep-2(config-vlan)# vn-segment 10011
  switch-vtep-2(config)# vlan 12
  switch-vtep-2(config-vlan)# vn-segment 10012
  switch-vtep-2(config)# interface nve1
  switch-vtep-2(config-if)# no shutdown
  switch-vtep-2(config-if)# source-interface loopback0
  switch-vtep-2(config-if)# member vni 10011
  switch-vtep-2(config-if)# ingress-replication protocol static
  switch-vtep-2(config-if)# peer_ip 200.200.8.8
  switch-vtep-2(config-if)# member vni 10012
  switch-vtep-2(config-if)# ingress-replication protocol static
  switch-vtep-2(config-if)# peer_ip 200.200.8.8
  switch-vtep-2(config-vlan)# exit
- Sau khi configure 2 router chúng ta có thể kiểm tra kết quả lại bằng lệnh:
  show nve vni ingress-replication

VI, ICMP

1, Định nghĩa

Giao thức ICMP(Internet control message protocol) là giao thức điều khiển của tầng IP, sử dụng để trao đổi các thông tin điều khiển dòng dữ liệu, thông báo lỗi và các thông tin trạng thái của bộ giao thức TCP/IP.
Các loại thông điệp ICMP là các thông điệp ICMP được chia làm hai nhóm: các thông điệp truy vấn và các thông điệp thông báo lỗi. Các thông điệp truy vấn giúp người quản trị mạng nhận được thông tin xác định từ một node mạng khác. Các thông điệp thông báo lỗi liên quan đến các vấn đề mà bộ định tuyến hay trạm phát hiện ra khi xử lý gói IP. ICMP sử dụng địa chỉ IP nguồn để gửi thông điệp thông báo lppox cho node nguồn của gói IP.

2, Nguyên tắc hoạt động

- Ping:
  Lệnh này dùng để kiểm tra một máy tính có thể kết nối với mạng không. Người sử dụng dùng cặp thông báo Echo Request và Echo Reply. Lệnh Ping sẽ gửi các gói tin từ máy tính của bạn đang ngồi tới máy tính đích. Thông qua giá trị mà máy đích trả về đối với từng gói tin, bạn có thể xác định được đường truyền như thế nào.
- Tracerout:
  Là công cụ dòng lệnh được dùng để xác định đường đi từ nguồn tới dích của một gói giao thức mạng Internet. Tracerout tìm đường tới đích bằng cách gửi các thông báo Echo Request Internet Mesage Protocol ICMP tới từng đích. Sau mỗi lần gặp đích, giá trị TTL tức là thời gian cần gửi sẽ tăng đến khi gặp đúng đích cần đến.

3, Các bước hoạt động

- Tracerout: Máy A thực hiện lệnh Tracer tới máy B
  Bước 1: Máy A gửi ICMP với TTL=1 tới máy router 1 và nhận lại gói ICMP Echo Request vì khi đó TTL=0
  Bước 2: Máy A tiếp tục gửi gói ICMP với TTL=2 tới router 1, router 1 sẽ gửi router 2 với TTL=1, tương tự bước 1, máy 2 sẽ gửi lại gói ICMP Echo Request.
  Bước 3: Tương tự như trên máy A sẽ gửi tới được tất cả các router mà nó cần đi qua cho tới khi tới được máy B và nhận lại gói ICMP Echo, khi đó sẽ có được đường đi từ A tới B.
  Tracert đang được chạy trên máy chủ A, và được đi theo con đường đến host B. Tại Router 1 và Router 2, TTL được giảm đến 0, khiến mỗi router để gửi một thông điệp vượt quá ICMP Time. Khi ICMP Echo Request được nhận tại Host B, nó sẽ gửi lại một trả lời ICMP Echo.