LISP

Kalabalık bir topolojide (dinamik yönlendirme protokolü kullanıldığı varsayılıyor) her bir router bir diğerine erişebilmek için kullanılabilecek rotaların tespit edilmesi ve tespit edilen rotalar arasında en iyi rotanın seçilebilmesi için her router üzerinde ayrı ayrı kaynak tüketmesi gerekecek. Bu durum topolojide gerçekleşen her bir değişimde her router üzerinde yeniden kaynak tüketilmesine nenden olacaktır.

LISP (Location/ID Seperation Protocol), routerlardaki yönlendirme tablolarının sadeleştirilmesi ve daha az kaynak harcanarak yönlendirme işleminin gerçekleştirmesini sağlamak üzerine geliştirilen bir teknoloji olarak tanımlanabilir. Bu teknolojinin işleyişini anlayabilmek için birkaç terimin bilinmesi gerekiyor. Bu terimler;

- **RLOC (Routing Locators),** topolojide tanımımlanan EID'lere ulaşmak için kullanılan ip adreslerine verilen isimdir.
- **EID (Endpoint Identifier),** ulaşılmak istenen nihai network (hedef network) bilgisine verilen isimdir.
- **ETR (Egress Tunnel. Router),** paketlerin EID'lara yönlendirilebilmesi için üzerine ITR'de eklenen ek L3 başlık bilgisinin çıkarıldığı (dekapsüle edildiği / tünellemenin sonlandırıldığı) routerlara verilen isimdir.
- **ITR (Ingress Tunnel Router** paketlerin hedef routera ulaştırılmak üzere enkapsüle edildiği (hedef routera iletilmek üzere L3'de ek bir başlık bilgisinin eklendiği / tünellemenin başlatıldığı) routera verilen isimdir.
- **XTR (X Tunneling Router**), hem ITR hem de ETR işlemini gerçekleştiren routerlara verilen genel isimdir.
- **MS (Map Server)**, hangi networkün hangi router üzerinde olduğunu tutan routerlardır. LISP kullanılan topolojilerde mutlaka en az 1 tane olması gerekir. MS hem veriyi üzerinde tutar hem de gelen istek paketlerine dönüş yapar. MR Server ise MS sunucusundan ayrı bir şekilde konfigüre edilebilir.
- **MR (Map Resolver)**, kendisine gelen istek paketlerindeki bilgileri Map Server üzerinde kontrol ederek yanıt veren sunucudur. Bir tür Proxy Server görevi gördüğü söylenebilir.
    - MR sunucusu kendisine gönderilen istek paketlerini her ne kadar MS sunucusu üzerinden öğrenip yanıtlıyor olsa da bu süreçte öğrendiği networklerin bilgisini belirli bir süre belleğinde tutuyor. Aynı sorgu belirli bir süre içerisinde tekrar sorulursa bu bilgiyi tekrar MS sunucusunda kontrol etmeden yanıtlıyor (Bu durum istismar edilebilir mi?).
- **PETR (Proxy Egress Tunnelling Router),** LISP topolojisi dışında çıkarılacak paketlerin topolojide uğradığı son router olarak tanımlanabilir (LISP topolojisi dışına çıkacak paketlere ETR işlemi uygulayan router). Burada pakete LISP topolojisi kapsamında eklenen ek L3 başlığı çıkarılarak (dekapsüle edilerek) paket topoloji dışına çıkarılır.
- **PITR (Proxy Ingress Tunnelling Router),** dış networklerden LISP topolojisine girerken paketlerin ilk uğradığı router olarak tanımlanabilir LISP topolojisine giriş yapacak paketlere ITR işlemi uygulayan router). Paketler buralarda iletileceği router adresi öğrenildikten sonra ek bir L3 başlığıyla enkapsüle edilerek önce hedef routera, ardından hedef networke ulaştırılır.

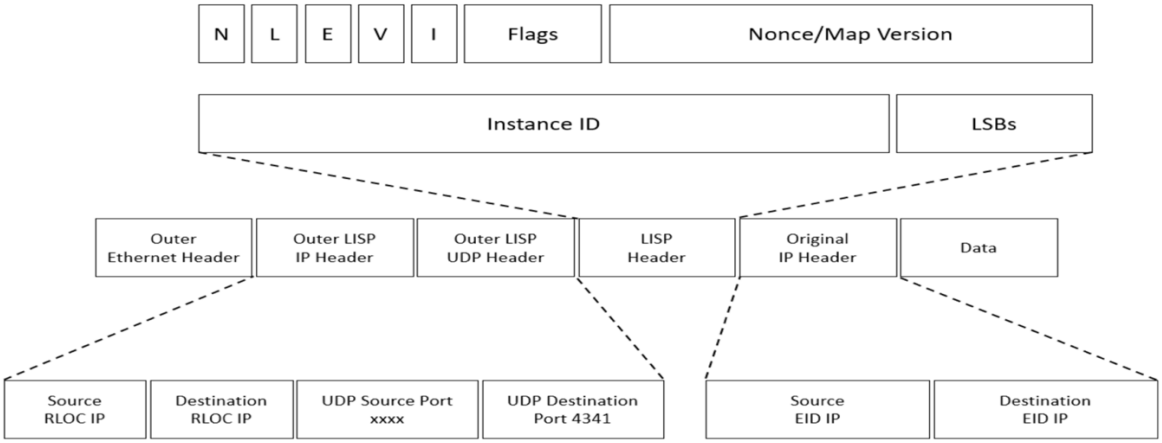
- **PxTR (Proxy X Tunnelling Router),** LISP topolojisi dışına kalan bir networklerle iletişim kurulmasını sağlayan (topolojide gateway görevi görüyor) routera verilen isimdir (Bu routerların bilgisi MS routerda tutulabildiği gibi routerlar üzerinde de tanımlanabilmektedir. Topoloji dışına çıkarılacak paketler yine MS sunucusu üzerinden yönlendirilir). Hem PETR hem de PITR fonksiyonunu yerine getirirler.
    - PITR router ile PETR router iki farklı router üzerinde konfigüre edilebilir. Bu durumda paketler topolojiden çıkış işlemini PETR router üzerinden, topolojiye giriş işlemini PITR üzerinden gerçekleştirecektir. Her iki süreç te tek router üzerinden yapıldığında ise o router PXTR oluyor.
- **LISP Router**, topolojide bulunan bütün routerlara verilen isimdir.

LISP teknolojisinde, öncelikle topolojide bir dinamik yönlendirme protokolü kullanılarak her routerun birbirini öğrenmesi sağlanıyor. Dinamik yönlendirme protokolü oturduktan sonra bir istemci farklı networkteki bir istemciye erişmek istediğinde paket Ingress routera gönderiliyor. Burada paketin hedef adresi LISP topolosindeki network bilgilerinin bir kaydının tutulduğu MS/MR routerdan hedef networkün hangi routera bağlı olduğunu (Engress router) öğreniliyor (Map Request – Map Reply paketleri kullanılıyor). Bu doğrultuda pakete hedef adresi Engress routerun adresi olan ikinci bir L3 başlığı eklenerek paket Engress routera iletiliyor.

Paket Engress routera ulaştığında hedef router üzerinde başlık bilgisi çıkarılarak kendisine doğrudan bağlı hangi networke gönderilmesi gerektiğine karar verip ilgili arayüzüne paket yönlendiriyor. Bu sayede Ingress router Engress routera doğrudan bağlı bütün networkler için (EID) ayrı ayrı kaynak tüketmemiş (yönlendirme tablosunda ayrı ayrı kayıt tutulmuyor, her network için ayrı ayrı en iyi rota hesabı yapılmıyor) oluyor. Sonuç olarak öğrenilen tek bir rota üzerinden birçok networke erişilebilir duruma geliniyor.
|→ Ingress routerda öğrenilen hedef network adresi (EID) ise bir süre bellekte tutuluyor. Kullanılmadığı taktirde bir süre sonra bellekten de siliniyor.
|→ MS/MR server tek bir router üzerinden konfigüre edildiğinde beklenenden büyük miktarda sorgu gelmesi networkte aksamalara neden olacaktır. Bunun için Map Server ile Map Resolver sunucusu ayrı routerlarda konfigüre edilerek trafik yükünün paylaştırılması sağlanabilir.

LISP topolojisi dışında bir networke erişim sağlanması gerekebilir. Bu durumda öncelikle ITR router ilgili network adresini MS sunucuya sorar. MS sunucuda adres kaydı bulunamadığı taktirde paketler PxTR (PITR ve PETR işlemi için tek router kullanılıyor olabilir) veya PETR routera gönderilerek paketi topoloji dışına göndermesini sağlayabilir.

Routerlar MS sunucusundan hedef router bilgisini öğrendikten sonra bu bilgiler doğrultusunda LİSP Data Plane'de paketin orjinal L3 başlık bilgisinin önüne bir LISP başlığı, UDP paket başlığı (4341) ve son olarak da hedef routera yönlendirilebilmesi için LISP protokolüne aitek bir ip başlık bilgisi daha ekleniyor (Buradan LISP teknolojisinin L3 ve üzeri katmanlarda çalıştığı anlaşılıyor). Bu doğrultuda LISP teknolojisi kullanılan bir topolojide enkapsüle edilmiş bir paket yapısına bakıldığında.



|→ Başlık alanları hakkında daha detaylı bilgi için https[:]//www.ciscopress.com/articles/article.asp?p=2992605&seqNum=3#:~:text=When%20an%20xTR%20at%20one,site%20through%20the%20selected%20path.

LISP Konfigürasyonu

NOT: Konfigrasyon için ilk olarak topolojdeki arayüzlere ip adreslerinin atanıp routerlar arasında bu adreslerin statik veya dinamik yönlendirme protokolleri kullanılarak öğretilmesi gerekmetedir.

- LISP konfigürasyonu için "**router lisp**" komutuyla LISP arayüzüne giriş yapılarak devreye alınması sağlanıyor.
- Ardından LISP topolojisine dahil edilmek istene her bir routerda "**database-mapping <Network Address/SM> <Outside Interface Ip Address> priority <Priority> weight <Weight>**" komutuyla routera bağlı her bir neworkün tanımlanması gerekiyor.
- Bağlı her bir network için bu tanım yapıldıktan sonra adres çözümlemesi için "**<IP Address Version> itr**" ve **"<IP Address Version> etr**" tanımlarıyla routerun etr, itr veya xtr görevi görmesi sağlanıyor.
- **"<IP Address Version> itr map-resolver <Map-Resolver Ip Address>"** ve **"<IP Address Version> etr map-server <Map-Server Ip Address> key <Key>**" komutlarıyla MS/MR router tanımlarının yapılması gerekiyor.
- Daha birçok özelleştirme yapılabileceği gibi "**loc-reach-algorithm rloc-probing**" komutuyla da RLOC'a erişilebilirlk sürecinde kullanılması istenen algoritma seçimi yapılabiliyor.

```
router lisp

site site2
description LISP SiteR2
authentication-key Si2Pa
eid-prefix 192.168.10.0/24
eid-prefix 192.168.20.0/24
eid-prefix 20.0.0.0/24
eid-prefix 192.168.30.0/24
eid-prefix 192.168.40.0/24
exit

ipv4 map-server
ipv4 map-resolver
exit
```

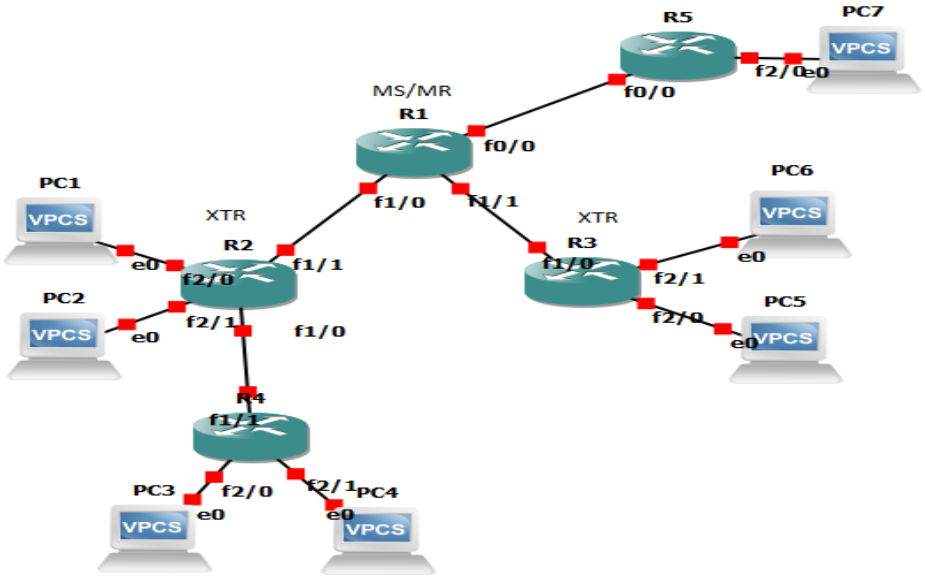
- MS/MR router konfigürasyonu için yine “**lisp router**” komutuyla LISP arayüzüne giriş yapılarak “**site <Site>**” komutuyla topolojide her bir router için tanım yapılıyor.
- Bu tanım içerisinde “**authentication-key <Key>**” komutuyla tanımı yapılan XTR routerda belirlenen Key bilgisi giriliyor.
- Key bilgisi tanımlandıktan sonra “**eid-prefix <Network Address/SM>**” komutuyla XTR routerda tanımlanan her bir network bilgisi bu router üzerinde de tanımlanıyor.
- Son adımda ise routera MS veya MR router olduğunu belirtmek için **“<IP Address Version> map-resolver”** ve **“<IP Address Version> map-server**” komutları kullanılıyor.

```
router lisp
database-mapping 192.168.10.0/24 10.0.0.2 priority 1 weight 100
database-mapping 192.168.20.0/24 10.0.0.2 priority 1 weight 100
database-mapping 20.0.0.0/24 10.0.0.2 priority 1 weight 100
database-mapping 192.168.30.0/24 10.0.0.2 priority 1 weight 100
database-mapping 192.168.40.0/24 10.0.0.2 priority 1 weight 100

ipv4 itr map-resolver 10.0.0.1
ipv4 itr
ipv4 etr map-server 10.0.0.1 key Si2Pa
ipv4 etr

loc-reach-algorithm rloc-probing
exit
```

- Bu konfigürasyon sonunda tanımlı her bir router MS/MR router üzerinden iletişim kurabilecektir.



VXLAN (Virtual Extensible Local Area Network)

Genelde networkleri birbirinden izole edebilmek için L2'de VLAN teknolojisi kullanılır. VLAN teknolojisi bir noktaya kadar izolasyon sağlasa da veri merkezleri gibi networkün yoğun ve kritik öneme sahip olduğu yerlerde yetersiz kalabiliyor. Bunun yanında L2'de STP protokolüne yönelik problemler ve MAC adres tablolarının sınırlı miktarda kayıt tutabilmesi gibi daha birçok problemle de karşı karşıya kalınıyor. Buna istinaden izolasyon sürecinin L2'de değil de L3 üzerinde gerçekleştirilmesini sağlayabilmek için geliştirilen teknolojiye VXLAN denilmektedir. Veri merkezlerinde farklı konumlarda bulunan ama aynı network adresine sahip (VLAN'da olan) sanal cihazlar arasında haberleşme sürecini daha etkili ve ölçeklenebilir hale getirebilmek için geliştirilmiştir.

VXLAN aslında bir Tunnelling protokolüdür. LISP veya GRE gibi Tunnelling protokollerinde L3'den itibaren başlık bilgileri eklenmeye/paket enkapsüle edilmeye başlıyordu. VXLAN teknolojisinde ise bu protokolünden farklı olarak **kapsülleme işlemine L2'den başlamaktadır**. Bu sayede paketin L2'deki başlık yapısında değişim olmadan, L3 üzerinden istenilen networke gönderilebiliyor. Gönderildiği networkte ise (switch üzerinde) L2'ye kadar dekapsüle edileceği için L2'de tanımlı bilgilerinde de değişim meydana gelmiyor (Yani Underlay içerisinde L2 başlık bilgileri değişmiyor – L2'de eklenen VLAN bilgisi de buna dahil). Bu kapsülleme yapısını sağlayan teknolojiye ise VTEP (VXLAN Tunnel End Point) denilmektedir.
|→ Buna ek olarak L2 VLAN numarası bir VNI ile eşleştirilerek (örnek olarak VLA 10 → VXLAN 10010 VNI ile eşleştirilebilir) hedefe ulaştığında dahil olduğu VLAN'da olan cihazlarla iletişim kurabilmesi sağlanabiliyor.
|→ VLAN'lar arası haberleşmeyi sağlamak için VLAN'lar arası yönlendirme işlemi ise paketler VTEP tüneline girmeden hemen önce veya tünelden çıktıktan hemen sonra yapılması sağlanabiliyor.

VXLAN'ın avantajlarına bakıldığında;
- 24 bitlik VXLA Network Identifier (VNI) alanı bulunuyor (16 milyon VXLAN oluşturulabiliyor). Normalde iki cihaz arasında tek bir VTEP tünel kuruluyor. Yani tüm paketler tek bir VTEP tünelini kullanılıyor ama tünel içerisinde trafikleri birbirinden ayırmak için başlık bilgisindeki VNI alanı kullanılıyor.
- L3'de çalıştığı için L2'deki Spanning Tree, CAM tablosunun sınırlı kayıt alabilmesi gibi sınırlamaların aksine L3'deki protokollerin tamamında yararlanıyor olması.

VTEP'ler arası iletişimi sağlamanın üç farklı yolu bulunuyor. Bunlar;
- **HER** (**Head And Replication with static flood-set)**, VTEP'ler arası bağlantı için her iki cihaz üzerinde de bağlantı kuracak VTEP bilgilerinin manuel/elle tanımlanmasıdır.
- **CVX (Ariste)**, VTEP'ler CVX(merkez sunucu)'e kendilerini tanıtır. Böyleçe CVX üzerinde bütün VTEP'lerin bilgisi tutulur ve herhangi bir VTEP başka bir VTEP'e bağlanmak istediğinde bunu CVX üzerinden gerçekleştirir. Cisco'da ise ACI adı verilen bir çözüm bulunuyor (Detaylar için https[:]//www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/L2_config/b_Cisco_APIC_Layer_2_Configuration_Guide/m_layer_2_networking_overview.pdf).
- **BGP-eVPN**,

VXLAN konfigürasyonunu eklenecek.

NOTLAR

- VXLAN destekleyen cihazlar (paketlerin kapsüllenmesini ve kapsülden çıkarılmasını sağlayan cihazlar) Virtual Tunnel Endpoints (VTEPS) olarak isimlendiriliyor.
- Normalde routerlarda yönlendirme tablosu Control Plane dediğimiz kısım tarafından oluşturuyordu. LISP teknolojisinde ise yönlendirme tablosu oluşmuyor, yönlendirme süreci MS server üzerinden gerçekleşiyor. Bu nedenle Control Plane yerine **LISP Control Plane** deniliyor.

TERMİNOLOJİLER

- Private VLAN, Aynı VLAN içerisindeki cihazları birbirinden izole etmeyi sağlayan L2 tekniğidir. Konfigürasyonu ve yönetimi zordur.
- Symetric Directed Routing
- Asymetric Directed Routing,
- Centralized Routing,

Kaynaklar

- https[:]//www.youtube.com/watch?v=yrpfmGnPeGw
- http[:]//tr.opticomfiber.com/info/what-is-nvgre-and-vxlan-52757556.html