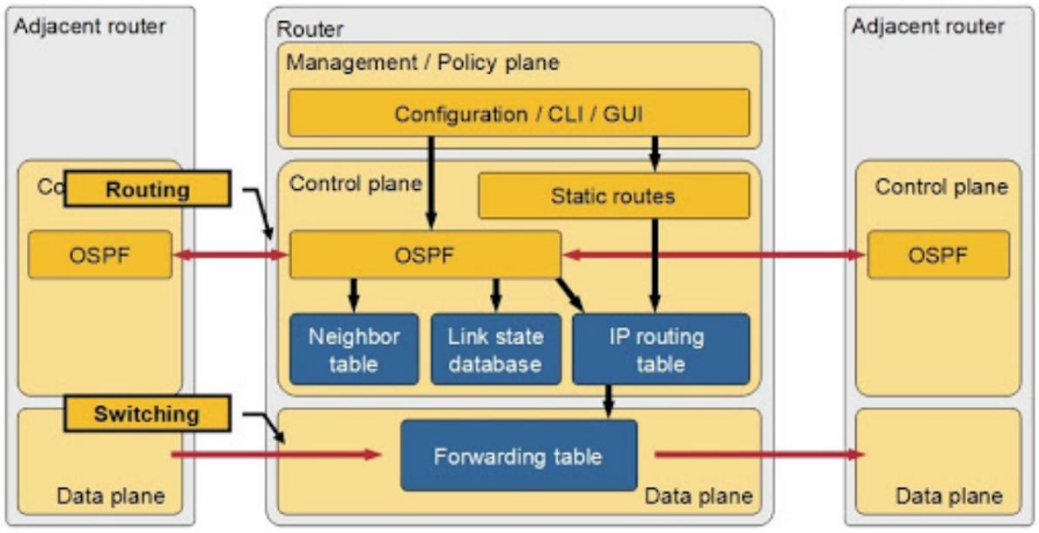
Fabric Technologies

SD-Access (Software-Defined Access)

Cisco'nun kurumsal networklerde yönetimi kolaylaştırmak için geliştirdiği teknolojidir. İçerisinde birçok teknolojiyi barındırmaktadır. Bu teknolojileri daha iyi çözümleyebilmek için ilk olarak fiziksel bir cihazın (switch/router) yapısına bakıldığında cihazlar 3 farklı alandan oluşmaktaydı. Bunlar;

- **Data Plane**, Control Plane tarafından alınan kararların ASIC tabanlı işlemciler ve TCAM adı verilen RAM hafızaları kullanılarak uygulandığı alandır.
- **Control Plane**, cihaz üzerindeki yönlendirme tablolarının hesaplanarak oluşturulması gibi yönetimsel hesaplamaların yapılarak kararların oluşturulduğu alandır. Bu hesaplamalar CPU ve RAM gibi donanımlar kullanılarak gerçekleştirilir.
- **Management Plane**, kullanıcıların cihazı yönetmek/konfigüre etmek için kullandığı alandır. Kullanıcı bu işlemi CLI veya GUI üzerinden gerçekleştirir.
- **Policy Plane**, belirlenen politikaların uygulandığı alandır.



Router (L3 Switchler için de geçerlidir) Control Plane üzerinde en iyi rotaları belirleyip yönlendirme tablolarını oluşturduklarında paketlerin bu tablo doğrultusunda yönlendirilmesi için Data Plane'e kayıt eder. Topolojideki cihaz sayısı arttıkça en iyi rotaların hesaplanması da yönlendirme tablosunun oluşturulması da bu hesaplamaların her router üzerinde ayrı ayrı yapılması da gereksiz yere kaynak tüketimine neden olacaktır. Bu durumu optimize edebilmek adına LISP çözümü geliştirilmişti.

LISP çözümünde özetle, her bir router rota hesaplamalarını ayrı ayrı yapmak yerine her router belirli bir kapsamda bulunan cihazlardan/networklerden sorumlu oluyordu. Topolojide iki istemci aralarında haberleşmek istediğinde kaynak istemci paketi Ingress Routera gönderiyordu. Ingress Router MS server üzerinde paketi göndermesi gereken routerun adresini (Engress Router) öğreniyordu ve bu doğrultuda pakete hedef adresi Engress router olan yeni bir L3 başlık bilgisi ekleyerek gönderiyordu. SD-Access Fabric çözümü de bu yapıya benzer şekilde çalışmaktadır.

SD-Access Fabric çözümünü LISP çözümü üzerinden açıklamak gerekirse LISP çözümünde kullanılan;

- Paketlerin kapsülleme ve dekapsüle etme işleminin gerçekleştirildiği routerlara (LISP -> ITR/ETR routerlar) **Fabric Access/Edge Nodes** deniliyor. Burada kullanılan switchler da dahil olmak üzere topolojideki bütün switchler L3 çalışıyor.
    - Dolayısıyla geleneksel L3 Access Layer Topolojisinde olduğu gibi topolojideki bütün bağlantılar da L3 oluyor.
- Paketlerin L3 üzerinde yönlendirme işleminden sorumlu olan routerlara (LISP -> Underlay görevi gören routerlar – ara routerlar) **Fabric Intermediate Nodes** deniliyor.
- Paketleri yönlendirmek üzere bilgilerin bulunduğu routerlara (LISP -> MS/MR routerlar) **Fabric Control Plane Nodes** deniliyor.
- Paketlerin farklı bir topolojiye geçmesini sağlayan routerlara (LISP -> PITR/PETR) **Fabric Border Nodes** deniliyor.

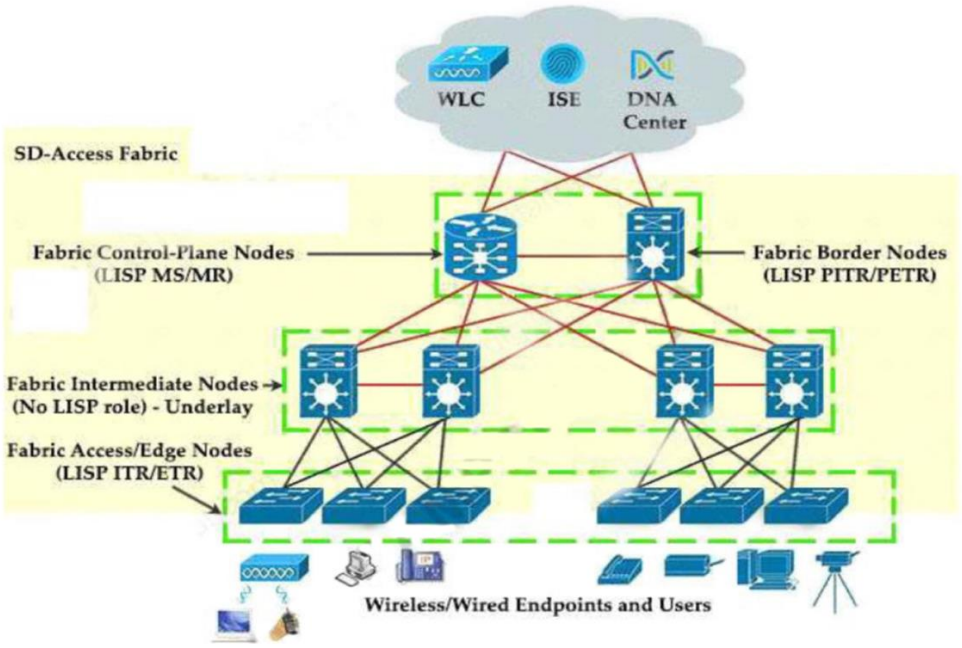
SD-Access Fabric çözümünde istemciler paketi Fabric Edge Node'a gönderir. Burada Fabric Control Plane Node üzerinden hedef Fabric Edge Node adresi öğrenilir ve VXLAN teknolojisini kullanarak paketi hedef Fabeic Edge Node'a gönderilir.
SD-Fabric teknolojisinde routerların en iyi rotayı belirlemek için hesaplama işlemleri yapılmasına gerek kalmadığından üzerlerindeki Control Plane'lere ihtiyaç duyulmadan **Fabric Control Plane Nodes** üzerinden yönetilmesi sağlanıyor.

Unutulmamalıdır ki bu teknolojiler kullanılırken paketlere her seferinde farklı başlık yapıları ekleniyor. Bu durum her pakette taşınabilecek veri miktarının da azalmasına neden oluyor.

Cisco DNA Center gibi çözümlerle entegre edilerek topolojinin yönetimi kolaylaştırılabiliyor. Burada Cisco DNA Center çözümü için harcanacak lisans ücretinin de göz önünde bulundurulması gerekiyor.

Yönlendirme tablolarında network bazlı adresler yerine (IPv4 -> /32, IPv6 -> /128) istemci bazlı adreslerin kayıtları tutulmaya başlanıyor.

ISE Server, SD-Access Fabric topolojisinde topolojiye eklenecek cihazları kimlik denetiminden geçirmek için kullanılan sunucudur.



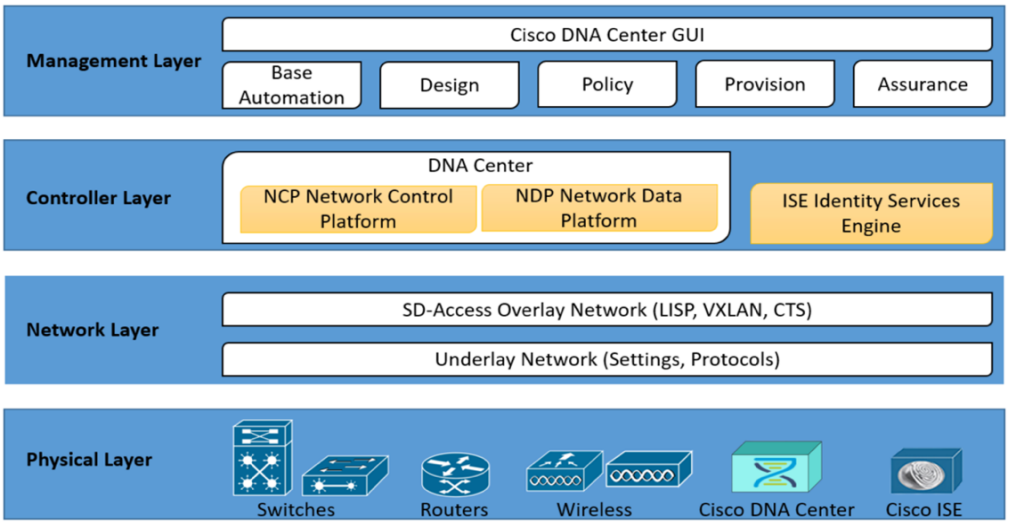
SD-Access Fabric teknolojisinin sağladığı avantajlarına bakıldığında;

- Cisco DNA Center gibi çözümlerle entegre kullanılarak topolojinin tek bir noktadan/merkezden yönetilebilmesi sağlanabiliyor. Yani yönetim sürecini kolaylaştırıyor.
- Topoloji üzerinde sistemin performansını arttırmaya yönelik analizler yapılarak güvenlik riski oluşturan ögeler, oluşabilecek problemler hakkında bilgi sağlayabiliyor. Bu özellik daha çok kablosuz yayınların kullanıldığı durumlarda etkili olabiliyor.
- Bu kısımdan sonraki özellikler geleneksel tasarımlarda da gerçekleştirilebiliyor. Tek farkı SD-Access Fabric bu sürecin daha kolay yönetilmesini sağlıyor.
    - Kablolu bağlantılarda veya kablosuz yayınlarda istemciler yer değiştirse dahi kesinti yaşamadan bağlantılarının devam etmesi sağlanabiliyor.
    - İstemciler networke bağlanırken kimlik denetiminden geçirilebildiği gibi uygulama, istemci veya grup bazlı politikaların uygulanması da sağlanabiliyor.
    - İstemcilerin gruplandırılıp birbirinden izole edilebilmesi gerektiğinde belirli grupların aralarında iletişim kurabilmesi sağlanabiliyor (geleneksel topolojilerde VLAN kullanılarak gerçekleştirilebiliyor).
    - Tek bir router üzerinde birden fazla sanal yönlendirme tablosu (VRF) oluşturulabiliyor.

SD-Access Architecture

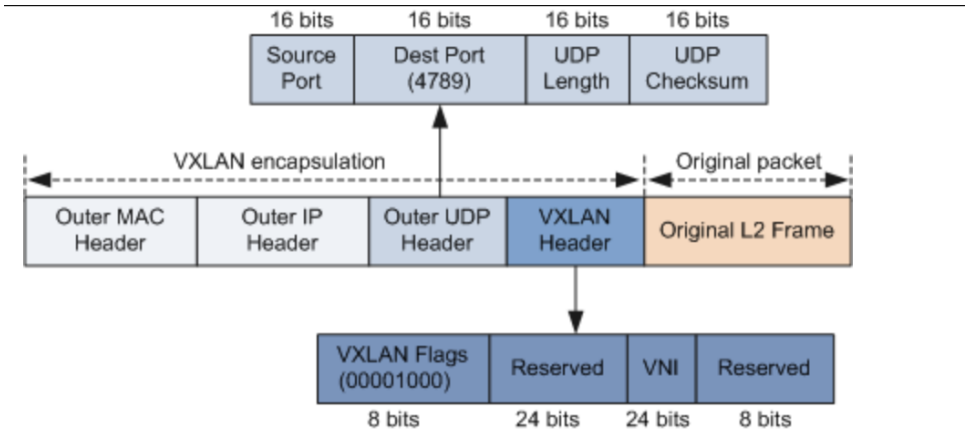
SD-Access mimarisi birkaç katmandan oluşmaktadır. Bu katmanlara bakıldığında;

- **Physical Layer**, Cisco marka router, switch ve AP gibi fiziksel cihazların bulunduğu katmandır.
- **Network Layer**, LISP, VXLAN gibi teknolojiler kullanılarak tünelleme ve yönlendirme (Underlay ve Overlay) işlemlerinin gerçekleştirildiği katmandır.
    - Topolojide Underlay yapı manuel olarak oluşturulabileceği gibi (Dinamik yönlendirme protokollerinden birisi her bir routerda ayrı ayrı konfigüre edilerek ayağa kaldırılabilir. Benzer şekilde Multicast trafiği için de yönlendirme işlemi gerekecektir) **Cisco DNA Center LAN Automation Feature** özelliğiyle (**IS-IS kullanılıyor**) otomatize oluşturulması da sağlanabiliyor. Otomatize oluşturulmasını sağlamak konfigürasyon hatalarının oluşmasını önlemek adına önemlidir. Tek olumsuz tarafı manuel müdahaleye izi verilmemesidir.
    - Topolojide Overlay yapı için VXLAN teknolojisi kullanılıyor.
    - Geleneksel topolojide VLAN'lara dahil istemcilerin farklı networklere çıkabilmesi için bir L3 cihaz üzerinde (SVI-Switch Virtual Interface arayüzünde) default gateway adresi tanımlanır. SD-Access Fabric topolojisinde kullanılan VXLAN teknolojisiyle birlikte her switch arası bağlantı L3 olduğu için tek bir SVI tanımı yeterli olmayacaktır. Bu nedenle **L3 Anycast Gateway** tekniği kullanılarak her Edge Node switchde SVI arayüzüne aynı ip adresiyle tanım yapılarak (ip çakışması olmadan) VXLAN'lar arası haberleşme sağlanabiliyor (Detayları "Notlar" kısmında bulabilirsin).
- **Controller Layer**, Management katmanda belirlenen konfigürasyonların fiziksel cihazlara uygulandığı katmandır. Cisco DNA çözümünün bir kısmı bu katmanda çalışır.
- **Management Layer**, network yönetiminin gerçekleştirildiği katmandır.



SD-Access Fabric teknolojisinde cihaz üzerinde bulunan her Plane dağıtık bir şekilde çalıştırılıyor. Plane'ler üzerinde çalıştırılan teknolojilere bakıldığında;

- **Control Plane (MS/MR router)**, LISP teknolojisi kullanılıyor. LISP teknolojisi sayesinde;
  - Cihazlar üzerinde daha küçük yönlendirme tabloları oluşturuluyor.
  - Cihazlar topolojide yer değişikliği yaptığında LISP teknolojisinde bu değişim otomatik olarak algılanarak Map Server (MS) üzerinde güncellemeler yapılıyor. Bu sayede kullanıcılara yer değiştirme konusunda esneklik sağlanıyor.
    - Yönlendirme tablolarında network adresleri yerine artık istemci ip adresleri bazında kayıtlar tutuluyor. Bu nedenle MS/MR routerun daha fazla kayıt için daha fazla depolama alanına sahip olması gerekir.
- **Data Plane**, VXLAN teknolojisi kullanılıyor. Her ne kadar hedef istemcinin ip bilgisi LISP teknolojisiyle öğrenilse de paketin iletimi VXLAN teknolojisiyle tünellenerek gerçekleştiriliyor (50 bayt başlık bilgisi ekleniyor. Bu durum tek bir paket üzerinde taşınabilecek veri miktarını düşürdüğünü unutma).
- **Policy Plane**, Cisco TrustSec güvenlik çözümü kullanılıyor (Kimlik denetiminden geçtikten sonra). Geleneksel topolojide ip bazlı ACL tanımları üzerinde politikalar uygulanabiliyordu. TrustsSec çözümünde ise kullanıcı veya cihaz bazında gruplar oluşturuluyor ve istemciler bu gruplara dahil ediliyor. Politikalar ise gruplar üzerinden uygulanıyor. İstemcilere uygulanacak politikaları belirleyen grup bilgisi ise VXLAN başlık yapısında 24 bitlik rezerve edilen kısımda **Group Policy Id** bilgisi (16 bit kullanılıyor) olarak taşınıyor.

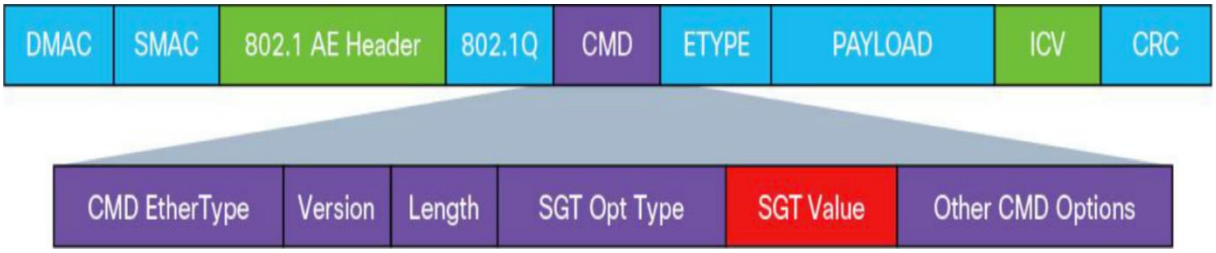


VXLAN başlık bilgisinde TrustSec için kullanılan alanda bulunun bitlere ve anlamlarına bakıldığında;

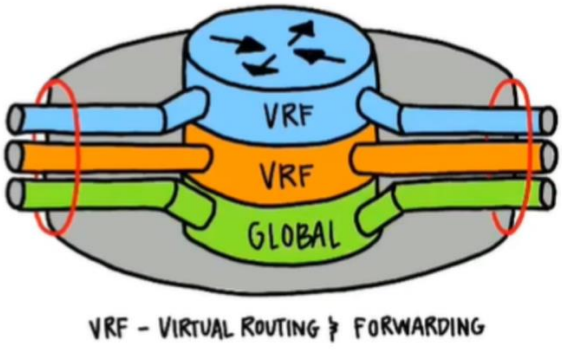
- **Policy Group ID (16 bit)**, istemcinin hangi gruba dahil olduğunu belirlemek için kullanılan alandır.
- **Group Based Policy Extension Bit (G bit – 1 bit)**, istemcinin bir gruba dahil olup olmadığını (politika uygulanıp uygulanmadığını) belirlemek için kullanılıyor /farklı bir ifadeyle bu bit 0 set edilmişse Group Policy Id değeri yok sayılır).
- **Dont't Learn Bit (D bit – 1 bit)**, VXLAN tünelinin sonlanacağı cihazın (VTEP – VXLAN Tunnel Endpoint) MAC adresini öğrenip öğrenmeyeceğini belirleyen bittir.
- **Policy Applied Bit (A bit – 1 bit)**, bir tür Acknowledgement bitidir. İstemcinin dahil olduğu grup politikalarının uygulandığını gösteren bittir. Bu sayede politikaların tekrar tekrar uygulanmasının önüne geçilir.

Geleneksel topolojide adresler üzerinden politika tanımları yapılabiliyordu. Adres değişikliği olduğunda yeniden düzenleme ihtiyacı doğuyordu. TrustSec çözümünde SGT (**Scalable Group Tag**) etiketleri kullanılarak istemcilerden veya kullanıcılardan oluşan gruplar üzerinden politikalar belirleniyor. Bu sayede adres değişimi yaşansa dahi istemciye veya kullanıcıya tanımlanan politikalar uygulanmaya devam ediyor (Günümüzde geleneksel topolojide kullanıcıya ip adresi sabitlenerek de bu özellik sağlanabiliyor).

- Cihaz veya kullanıcı bazlı uygulanan bu politikalar SD-Access Fabric topolojisi dışına çıkarılacak bir pakette **SGT Exchange Protocol** (SXP) özelliği kullanılarak geçiş yapılacak networke aktarılması sağlanabiliyor.



Geleneksel topolojilerde olduğu gibi SD-Access Fabric topolojisinde de routerlar üzerinde sanal yönlendirme tabloları (VRF – Virtual Routing and Forwarding) oluşturularak router arayüzlerine gelen trafiklerin farklı yönlendirme tabloları kullanılarak iletilmesi sağlanabiliyor (Detaylar için "CCNP - 04 - IP Routing Essentials" notlarını inceleyebilirsin).



WLC - SD-Access Fabric Topology

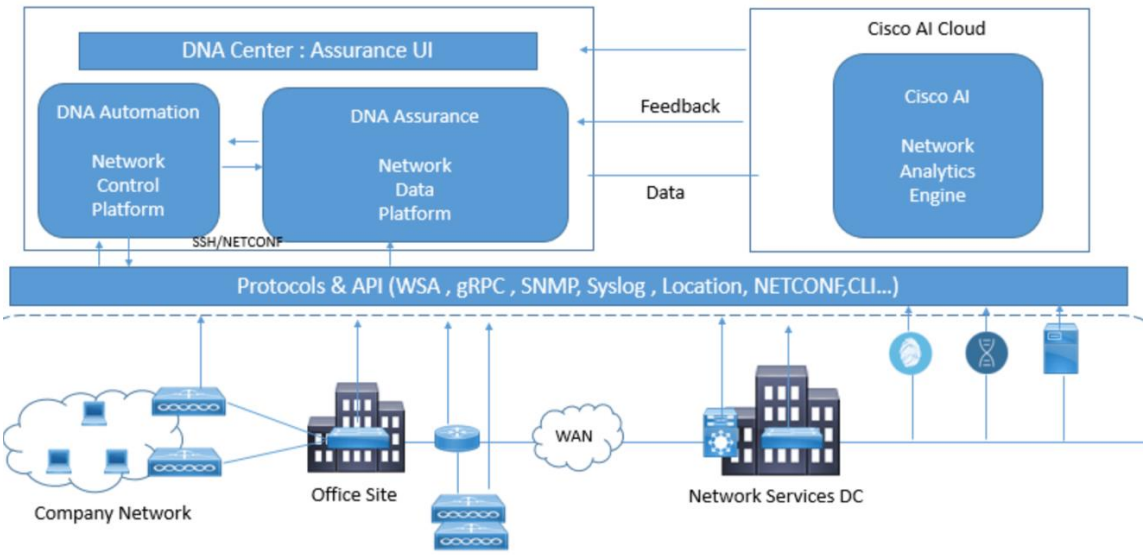
Geleneksel topolojide AP'lerin yönetimi WLC kullanılarak gerçekleştirildiğinde bir AP farklı bir AP'e paketi WLC üzerinden gönderebiliyordu (Bu süreçte paket iki defa tünelleniyordu). SD-Access Fabric topolojisinde WLC kullanıldığında VXLAN protokolüyle paketler doğrudan (CAPWAP tüneline ihtiyaç duyulmadan, paket WLC'ye gönderilmeden) hedef AP'e gönderilebiliyor (Bunu yapabilmek için yine AP'ler üzerinde ek ayarlamaların yapılması gerekiyor).

- Bu sayede iletişim çok daha hızlı gerçekleşmiş oluyor.
- Networkte gereksiz trafik oluşmasının önüne geçiliyor.
- Cihazların kaynakları gereksiz yere tüketilmemiş oluyor (2 kere CAPWAP tünel kuruluyordu).

Cisco DNA Center Appliance

Cisco DNA Center çözümünün hem Managemet Layer'da hem de Controller Leyar'da çalıştığından yazının başlarında bahsedilmişti. Kullanıcıların konfigürasyon yaptıkları arayüz sağlanan kısım (DNS Center Assurance UI) Management Layer olarak tanımlanıyor. DNA Center çözümü içerisinde **Network Control Platform (NCP)** ve **Network Data Platform (NDP)** olmak üzere iki tane alt modül içeriyor. Bu alt modüller ise Controller Layer olarak tanımlanıyor. Bu yapıların görev tanımlarına bakıldığında;

- **DNA Center Assurance UI**, kullanıcının topoloji üzerindeki cihazlara konfigürasyonlar yapabilmesini sağlayan arayüzüdür.
- **NCP**, DNA Center arayüzü üzerinde belirlenen konfigürasyonları SSH, SNMP veya NETCONF protokollerini kullanarak topolojideki cihazlara uygulayan modüldür.
- **NDP**, topolojideki cihazlardan istatistiksel bilgilerin toplandığı modüldür. Bu modül sayesinde network üzerindeki genel durum görüntülenebiliyor.
- **Cisco Identity Service Engine (ISE)**, bu modül ISE sunucusu üzerinde bulunuyor. Kimlik denetimi gerçekleştirip politikaları cihazlara uygulayan modüldür (AAA, Radius, EAPoL).



DNA Center Assurance UI (Management Layer)

DNA Center çözümünün arayüzünde (Managemetn Layer) kullanıcıya sunulan sekmeler ve özelliklerine bakıldığında;

- **Design Workflow,**
    - **Network Hierarchy**, networkün topoloji haritasının çizilebilmesini sağlayan sekmedir (Dünya haritası üzerinde görüntüleniyor).
    - **Network Settings**, networke özel DNS, DHCP, AAA gibi çeşitli ayarlamaların yapıldığı sekmedir.
    - **Image Repository**, cihazların üzerinde çalışan işletim sistemlerinin yüklenmesi veya güncellenmesi sürecinde yüklenecek yazılımları depolamak/yönetmek için kullanılan alandır.
    - **Network Profiles**, LAN, WAN, WLAN veya VXLAN gibi altındaki networklere dair bilgilerin tarif edildiği sekmedir.

- **Policy Workflow**,
    - **Dashboard**, özet bilgilerin görüntülendiği sekmedir.
    - **Group-Based Access Control**, TrustSec çözümüyle cihazların gruplandırılabildiğinde ve grup bazlı politikalar uygulanabildiğinden bahsedilmişti. Grup bazlı uygulanan politikaların yönetim sürecinde kullanılan sekmedir.
    - **Ip-Based Access Contro**l, ip adres bazında uygulanan politikaların yönetimi için kullanılan sekmedir.
    - **Application**, topolojide uygulama bazlı politikaların (QoS, Block ...) belirlenmesi ve yönetilmesi sürecinde kullanılan sekmedir.
    - **Traffic Copy**, Mirrior/Span port olarak da bilinen bir port üzerinden geçen trafiğin kopyasının farklı bir port üzerinden de gönderilmesini sağlayan özellikti. Traffic Copy sekmesi ise bu sürecin yönetildiği sekmedir (ERSPAN desteklemektedir).
    - **Virtual Network**, VRF konfigürasyonunun yapıldığı ve yönetildiği sekmedir.

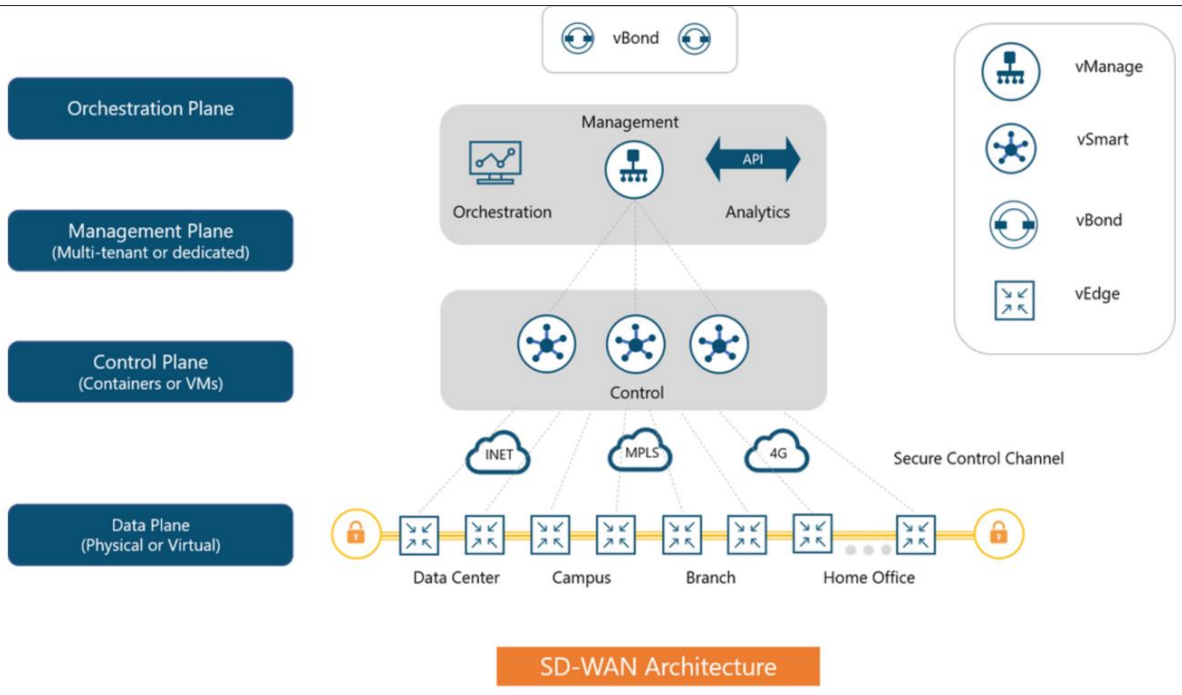
- **Prevision Workflow**,
    - **Devices**, Fabric topoloji üzerinde kullanılan cihazlar üzerine ayarlamaların yapılabildiği ve cihazlar hakkında detaylı bilgilerin görüntülendiği sekmedir.
    - **Fabrics**, Fabric altyapısının oluşturulması için kullanılıyor.
    - **Fabric Devices**, Fabric topolojisine cihazların eklendiği ve rollerinin belirlendiği sekmedir (Edge, Control Plane, Border, WLC…).
    - **Host Onboarding**, Fabric topoloji üzerinde kullanılan istemcilere/Host'lara yönelik ayarlamaların yapıldığı sekmedir (Kimlik denetiminin nasıl gerçekleştirileceği, ip havuzlarının tarif edilmesi gibi işlemler).

Assurance Workflow ve **Platform Workflow** sekmelerinden ayrıca bahsedilecekti.

SD-WAN (Software Defined WAN)

Büyük ölçekli networklere sahip kurumlarda (çok fazla şubesi olan ver her şubesinde ayrı bir network yönetimine ihtiyaç duyan – Bankalar gibi) WAN topolojisi üzerinde kullanılan cihaz sayısının yüksek olması durumunda bu cihazların yönetim ve bakım sürecinin gerçekleştirilmesi de zorlaşıyor. Bu süreci kolaylaştırmak adına SD-WAN çözümü tercih edilebiliyor (SD-Access gibi Cisco'ya özel bir çözüm değildir. Birçok markada SD-WAN çözümü bulunuyor). Cisco, Cisco SD-WAN ve Meraki SD-WAN olmak üzere iki ayrı çözüm sunuyor.

- **Meraki SD-WAN**, Cisco Meraki çözümü AP'lerin Cloud bazlı Controller'lar kullanılarak yönetilmesini sağlayan çözümüydü. Meraki SD-WAN çözümü ise farklı kısımlarda bulunan AP'lerin doğrudan Cloud üzerinden yönetmek yerine topolojide internet çıkışına bir Meraki router konumlandırılarak, bu routerun Cloud üzerinden yönetilmesini sağlayan çözümüdür.
- **Cisco SD-WAN** (based on Viptela), WAN topolojisi üzerinde bulunan cihazların yönetimini merkezi bir arayüz üzerinden gerçekleştirilmesini sağlar. Standart teknolojilerin merkezi bir otomasyon mekanizmasıyla yönetilmesini sağlamayı amaçlayan çözümdür. Bu çözüm 4 Plane/ katmandan oluşmaktadır. Bunlar;
    - **Data Plane**, farklı büyüklüklerdeki (Campus, SOHO, Data Center…) farklı boyutlardaki LAN'ların bağlı olduğu routerların bulunduğu katman olarak tanımlanabilir. Bu katmanda kullanılan routerlara **VEdge (Virtual/Viptela Edge) Routers** denilmektedir.
    - **Control Plane**, Data Plane üzerinde bulunan routerlara konfigürasyonları uygulayan katman olarak tanımlanabilir. Bu katmanda kullanılan yapılara **VSmart (Virtual/Viptela Smart) Controllers** denilmektedir.
    - **Management/ Plane,** SD-WAN üzerindeki routerların yönetiminin gerçekleştirildiği, konfigürasyonları belirlendiği katmandır. Bu katmandaki yazılımlara **VManager** denilmektedir.
    - **Orchestration Plane**, Data Plane'de bulunan routerların Control Plane'deki yazılımlara erişimi sürecinin yönetimini sağlayan katman olarak tanımlanabilir.



SD-WAN Architecture

SD-WAN Routers, SD-WAN Ruterler Viptela marka routerlar ise vEdge, Cisco marka routerlar ise cEdge olarak isimlendiriliyor. Buradaki routerlar üzerinde standart dinamik yönlendirme protokolleri, QoS tanımları gibi daha birçok konfigürasyon manuel olarak yapılabiliyor. SD-WAN mimarisi ise bu konfigürasyonların her cihaz üzerinde tek tek manuel yapılması yerine bütün cihazlara otomatize halde uygulanmasını sağlıyor.

VSmart Controllers, SD-WAN routerlara konfigürasyonları uygulayan kontrol yazılımlarıdır. VSmart Controller yazılımı, VEdge routerları SD-WAN mimarisine dahil edilmeden önce kimlik denetiminde geçirilirler. Kimlik denetiminden geçen routerlar için VSmart Controller yazılımıyla aralarında **DTLS** (Datagram Transport Layer Security) tünel kurulur. Bu tünel üzerinden routera uygulanacak konfigürasyonlar **OMP** (Overlay Management Protocol) protokollü kullanılarak uygulanır.

VManage NMS (Network Managemetn System), SD-WAN topolojisinin yönetiminin bir grafikse arayüz üzerinden gerçekleştirilmesini sağlayan yazılımdır.

VBound Orchestration, SD-WAN topolojisine VSmart Controller ile VEdge routerlar arasında bağlantı kurulmasını sağlayan yazılımdır (bağlantı kurmak isteyen cihazlara kuracağı bağlantı hakkında detayları sağlıyor).

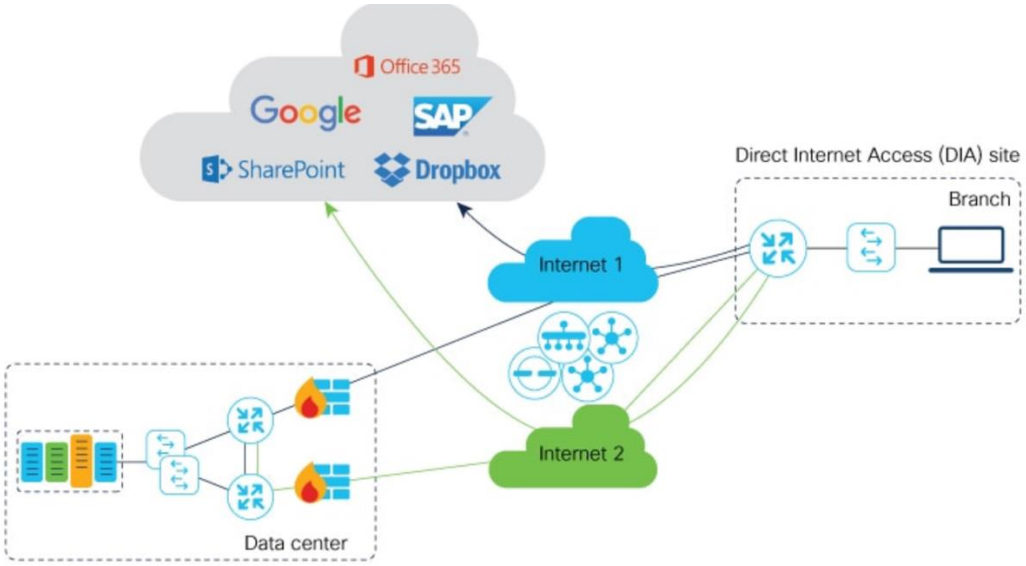
- Topolojiye yeni bir router dahil edileceği zaman routerun kimlik denetiminden geçebilmesi için VSmart Controller'a erişebilmesi gerekiyor. Bu erişim sürecini VBound yazılımı sağlıyor (Topolojiye yeni eklenecek router Public ip adresine sahip olabileceği gibi NAT arkasında da olabilir. NAT arkasından erişilebilmesini de sağlıyor). İlk bağlantı sürecinden de anlaşılabileceği üzere SD-WAN topolojisinde Public Ip adresine sahip olması gereken tek yapıdır.
- VBound yazılımı sadece VEdge routerların ilk bağlantılarında değil bağlantı sonrasında VSmart Controller yazılımlarına erişilmesi gerektiğinde de gerekli erişimi sağlamaktadır (bağlanmak isteyen VEdge Routerları VSmart Controller'lar arasında paylaştırarak yük dengeleme işlemi de yapabiliyor).

VAnalytics, WAN altyapısı üzerinde istatistikler tutularak analiz edilebilmesini sağlayan yazılımdır. Analizlerle birlikte topoloji üzerinde performansı arttırabilecek tavsiyeler de verebiliyor.

Cisco SD-WAN Cloud OnRamp, Cloud tabanlı uygulama trafiklerinin performansını arttırmaya yönelik geliştirilen bir çözümdür. Bu çözümle birden fazla internet çıkışına sahip Edge Router'lar için hangi çıkış kullanıldığında Cloud tabanlı uygulamalara daha hızlı erişilebileceğinin otomatize şekilde tespit edilmesini ve uygulanmasını sağlayan çözümdür (https[:]//www.networkacademy.io/ccie-enterprise/sdwan/cloud-onramp-for-saas).

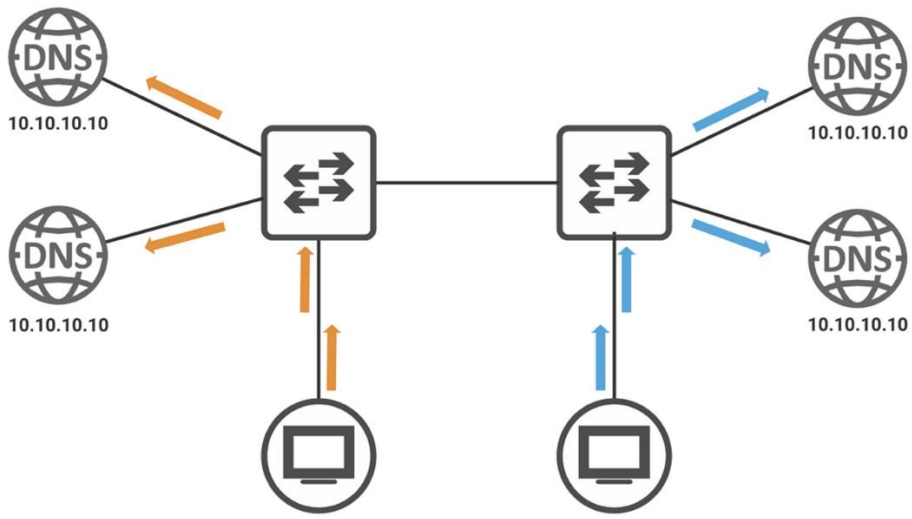
- Örnek olarak bir banka şubesi (Edge Router) zerinden örnek verildiğinde VManager yazılımı, banka şubesinde doğrudan internete çıkıldığında mı yoksa merkez üzerinden internete çıktığında mı Cloud tabanlı uygulamalara daha hızlı erişildiğini test edip hangisi daha performanslı ise Cloud tabanlı uygulamaların o çıkış üzerinden gönderilmesi sağlanabiliyor.
- Türkiye'de 5651 kanunu nedeniyle internete çıkarılan cihazların bağlantı kayıtlarının 1-2 yıl aralığında depolaması gerekiyor (https[:]//www.mevzuat.gov.tr/mevzuat?MevzuatNo=5651&MevzuatTur=1&Mevzuat

Tertip=5). Bu kayıtların tek bir merkezde tutulabilmesi için topolojideki bütün cihazlar tek bir merkez üzerinden internete çıkarılıyor. Bu türden tek çıkışlı topolojier için kullanılabilir bir çözüm değildir.



Notlar

- **Anycast**, IPv4 üzerinde de IPv6 üzerinde de bulunan bir özelliktir. Çalışma prensibine bakıldığında, aynı network içerisinde bulunmadığı durumda (aksi taktirde ip çakışması yaşanacaktır) tek bir ip adresi birden fazla istemci üzerinde kullanılabiliyor. Bu ip adresine yönelik bir trafik oluşturulduğunda dinamik yönlendirme protokolleri paketleri ip adresine sahip en yakın istemciye/sunucuya gönderecektir. Bu durum bir anlamda aynı görevi gören istemci/sunucular arasında yapıldığında yedeklilik de sağlamaktadır. Trafik oluşturulduğunda yakında bulunan (Administrative Distance veya Metric değeri düşük olan) istemcide/sunucuda bir sorun yaşanması durumunda paketler aynı işi yapacak olan daha uzakta bulunan ama aynı ip adresine sahip istemciye/sunucuya gönderilecektir.
    - Günümüzde 13 kök DNS sunucusundan 7 tanesi da Anycast yayını kullanmaktadır.



|→ L3 Anycast Gateway tekniğinde ise switchler arası her bir bağlantı L3 olduğu için tek bir ip adresi her bir switch üzerinde her bir SVI arayüzünde tekrar tekrar tanımlanabiliyor.

SORU: L3 Anycast Gateway kullanıldığında her ne kadar tek bir ip adresi tekrar tekrar kullanılabiliyor olsa da aynı ip adresini kullanan cihazlar arasından sadece birisine gönderiliyor. Peki VXLAN kullanıldığında hangi switch üzerindeki SVI arayüzüne gönderileceği nasıl belirleniyor? https[:]//www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/16-12/configuration_guide/vxlan/b_1612_bgp_evpn_vxlan_9300_cg/configuring_evpn_vxlan_anycast_gateway.pdf

- Aynı switch üzerindeki herhangi bir portlarından geçen trafiğin bir kopyasının farklı bir porttan gönderilmesini sağlamaya **SPAN Port** deniliyordu. L2 üzerinden (aynı network içerisinde) farklı switch üzerindeki bir porttan geçen trafiğin bir kopyasının alınmasına **RSPAN Port** deniliyor. L3 üzerinden (farklı bir networkten) farklı bir switch portundan geçen trafiğin bir kopyasının alınmasına **ERSPAN Port** deniliyor.
- Cisco Meraki, AP'leri topolojide bulunan fiziksel bir WLC ile değil de bulut tabanlı WLC üzerinden yönetilmesini sağlayan çözümüdür.
- SD-Access yapısında kullanılan LISP protokolü aslında ISP protokolü, VXLAN çözümü ise aslında DataCenter çözümüdür.