

BSM 458-AĞ PROGRAMLAMA

Hafta10: Yazılım Tanımlı Ağlar (Software Defined Networks)

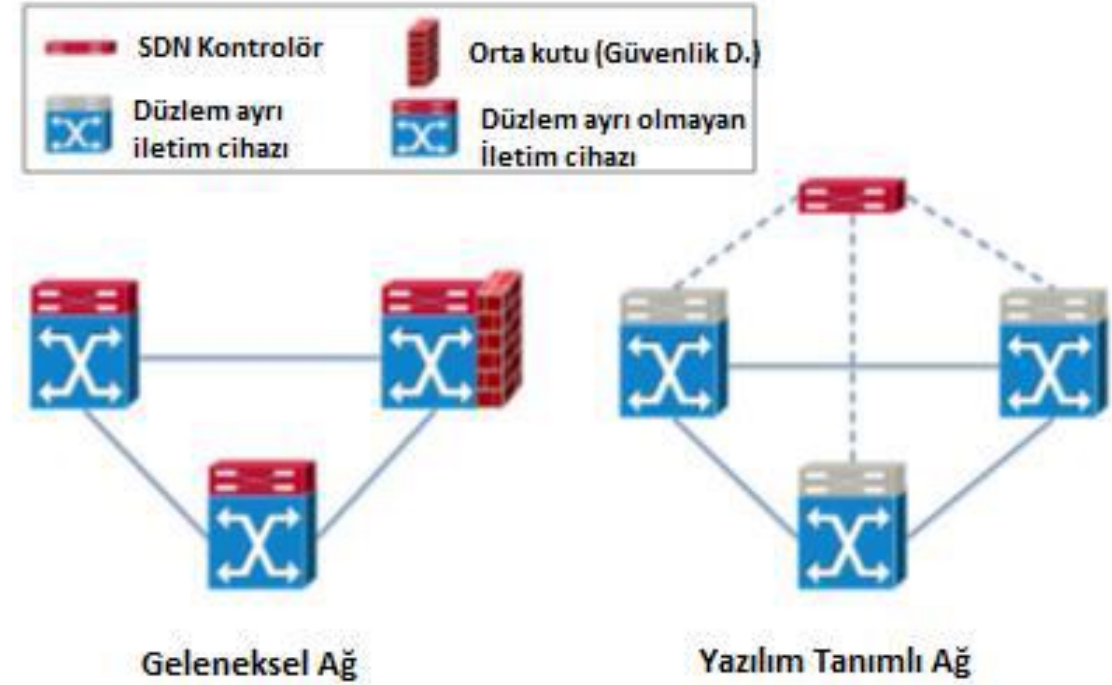
Dr. Öğr. Üyesi Musa BALTA
Bilgisayar Mühendisliği Bölümü
Bilgisayar ve Bilişim Bilimleri Fakültesi

Yazılım Tanımlı Ağ Kavramı

- Günümüz ağ yapıları **dezavantajları**;
 - *Heterojen sistemler*
 - *Farklı protokoller*
 - *Yüksek bant genişliği ihtiyacı*
 - *Kolay ve Dinamik yönetim*
- SDN'nin **avantajları**;
 - *Dinamik ve kolay optimizasyon*
 - *Daha güvenilir ve esnek bir yapı*
 - *Hızlı erişilebilirlik*
 - *Yük dengeleme*
 - *Merkezi Yönetim*

Yazılım Tanımlı Ağlar-Genel Mimari Yapı

- **Veri** ve **kontrol** düzlemleri birbirlerinden ayrılır.
- Ağ kontrolünün doğrudan programlanabilir olmasına ve altyapının uygulamalar ve ağ hizmetleri için soyutlaştırılmasına olanak sağlar.
- **Mimari yapı;**
 - İletim elemanları
 - Kontrolör
 - Uygulama yazılımı



Yazılım Tanımlı Ağlar-Genel Mimari Yapı (devam)

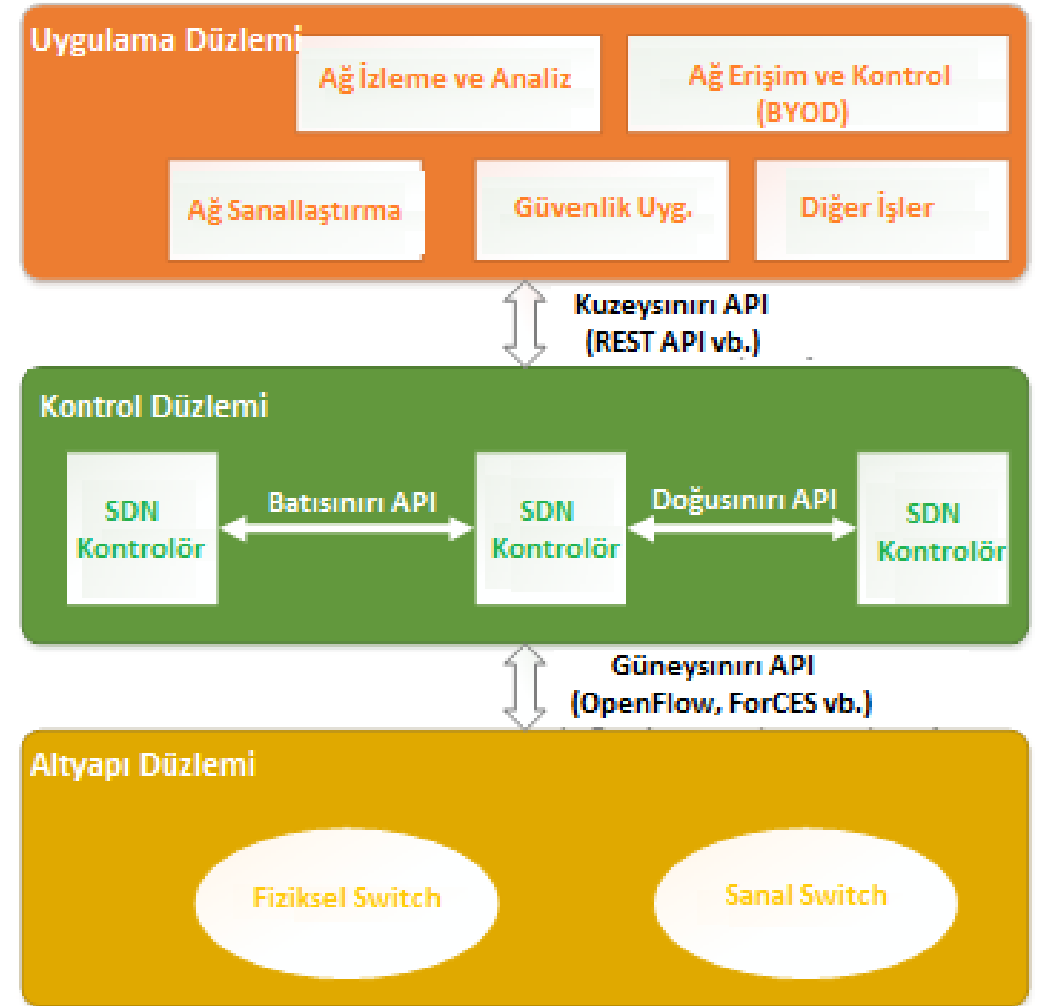
- İletim elemanları önceden tanımlı program mantığına göre kendilerine kontrolörden gelen kurallara göre veri trafiğini iletirler.
- Kontrolör genellikle uzak bir sunucuda çalışır ve bir takım standartlaşmış komutlar kullanarak iletme elemanlarıyla güvenli bir bağlantı üzerinden haberleşir.
- Uygulama yazılımı ise, ağdaki iletim cihazlarını senaryolar gereği nasıl hareket edeceğiyle ilgili yazılan uygulamalardır.
- 2 tip uygulama şekli olabilir.

➤ Interior

➤ Exterior

Yazılım Tanımlı Ağlar-ONF Katmanlı Mimarisi

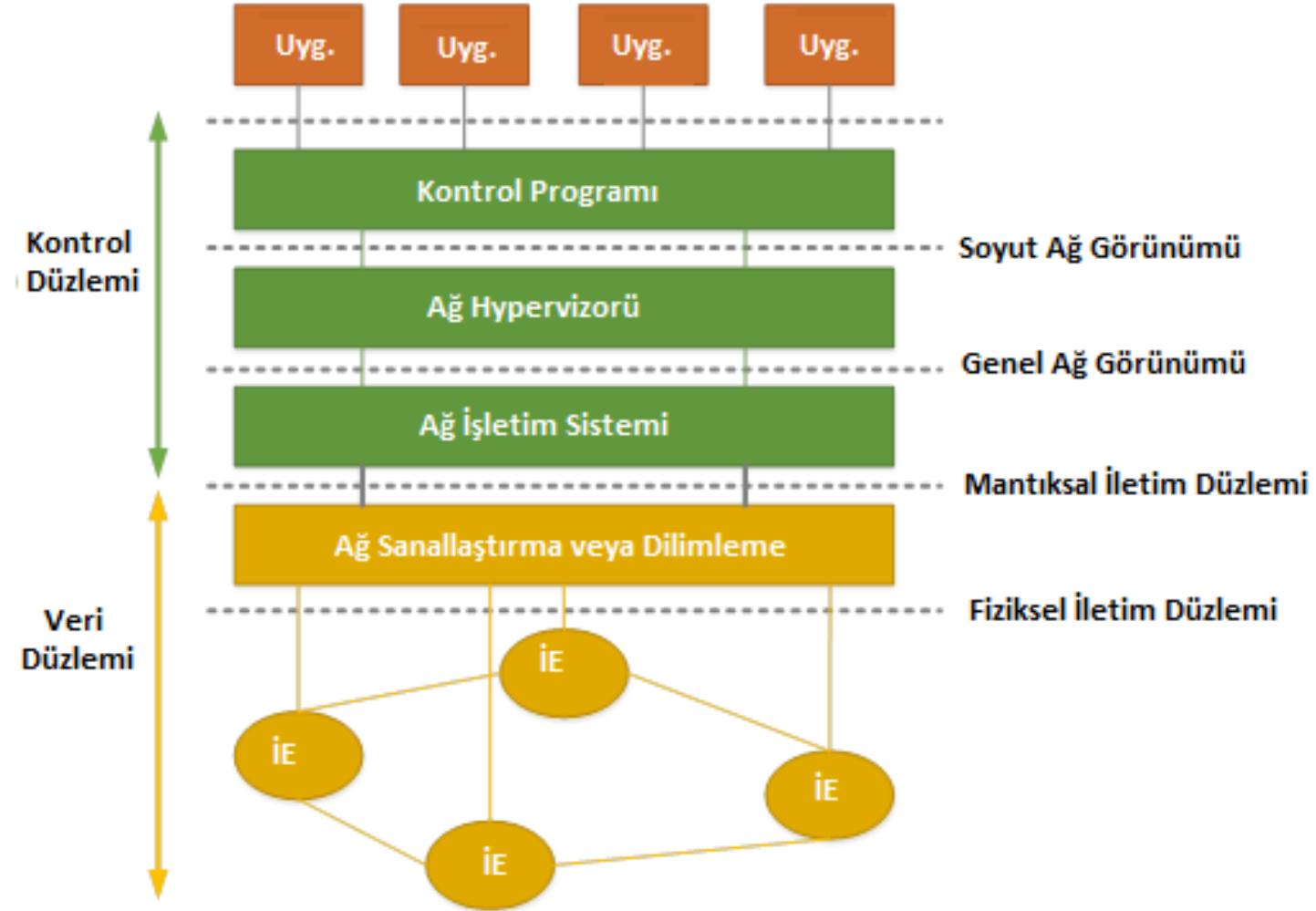
- Literatürde en bilinen SDN mimarisi **ONF** tarafından oluşturulmuş mimaridir.
- 3 temel katmandan oluşur:
 - **Uygulama düzlemi**
 - **Kontrol düzlemi**
 - **Altyapı düzlemi**
- Katmanlar arasındaki haberleşme açık kaynak protokoller/API'ler vasıtasıyla sağlanmaktadır.



Yazılım Tanımlı Ağlar-ONF Mimarisi (devam)

- 1. Altyapı Katmanı:** Veri düzlemi olarak da adlandırılan bu katmanda, bir açık arayüzle/API vasıtasıyla erişilebilen İletme Elemanlarından (fiziksel ve sanal anahtarları) oluşur.
- 2. Kontrol Katmanı:** Bu katman, bir açık arayüz üzerinden ağdaki cihazları yönetmek için çeşitli ağ modüllerinden oluşan kontrolör olarak adlandırılan yazılım bulunmaktadır.
- 3. Uygulama Katmanı (Application Layer):** Bu katman, ana olarak SDN haberleşmesi ve ağ servislerini kullanan yük dengeleme, en kısa yol, güvenlik gibi son-kullanıcı uygulamalarından oluşmaktadır.

Yazılım Tanımlı Ağlar-ONF Mimarisi (Sanal Katmanlar)



Yazılım Tanımlı Ağlar-ONF Mimarisi (Sanal Katmanlar-devam)

- **Fiziksel iletim düzlemi**, ağ içerisinde bulunan iletim elemanlarını ifade ederken, aynı zamanda bu elemanların bir üst katman olan ağ sanallaştırma katmanı ile olan iletişimlerini sağlar.
- **Ağ sanallaştırma katmanı** ağın ihtiyaçlarına göre belirlenen mantıksal iletim düzlemin neticesinde sahadaki iletim elemanlarının nasıl hareket edecekleri ile ilgili bilgi akışı sağlar.
- **Ağ işletim sistemi**; ağdaki cihazların yüklenme işlemleri, cihazların davranışlarını, kısaca ağın programsal kontrolünü sağlar, iletim elemanlarının kontrolünü sağlayabilmesi için genel ağ görüntüsünü alması gerekmektedir.
- **Soyut ağ görünümü düzlemi**; ise genel ağ görünümünün uygulamalar ve kontrol programı tarafından yorumlanabilmesi için oluşturulan bir izdüşüm/tersleme işlemidir.

Yazılım Tanımlı Ağlar-İletim Elemanları

- Ağ altyapıları, yönlendiriciler, anahtar cihazlar, sanal anahtar cihazlar, kablosuz erişim noktaları gibi bir çok iletim cihazı ve ağ ekipmanından oluşmaktadır.
- Yazılım tanımlı ağlarda bu iletim cihazları, kontrol ve yönetim işlevlerini bir kontrolör cihazına devrederek soyutlanmış, açık bir API (openflow, ForCES) ile basitçe erişilebilen iletim elemanları olmuştur.
- İletim elemanlarının kontrolör ve kendi aralarında iletişim halinde olabilmeleri için ONF SDN mimarisindeki güney sınırında gösterildiği üzere bir açık arayüz kullanmaları gerekmektedir.
- Bu açık arayüzlerden literatürde en bilinenleri **ForCES** ve **Openflow** protokolleridir.

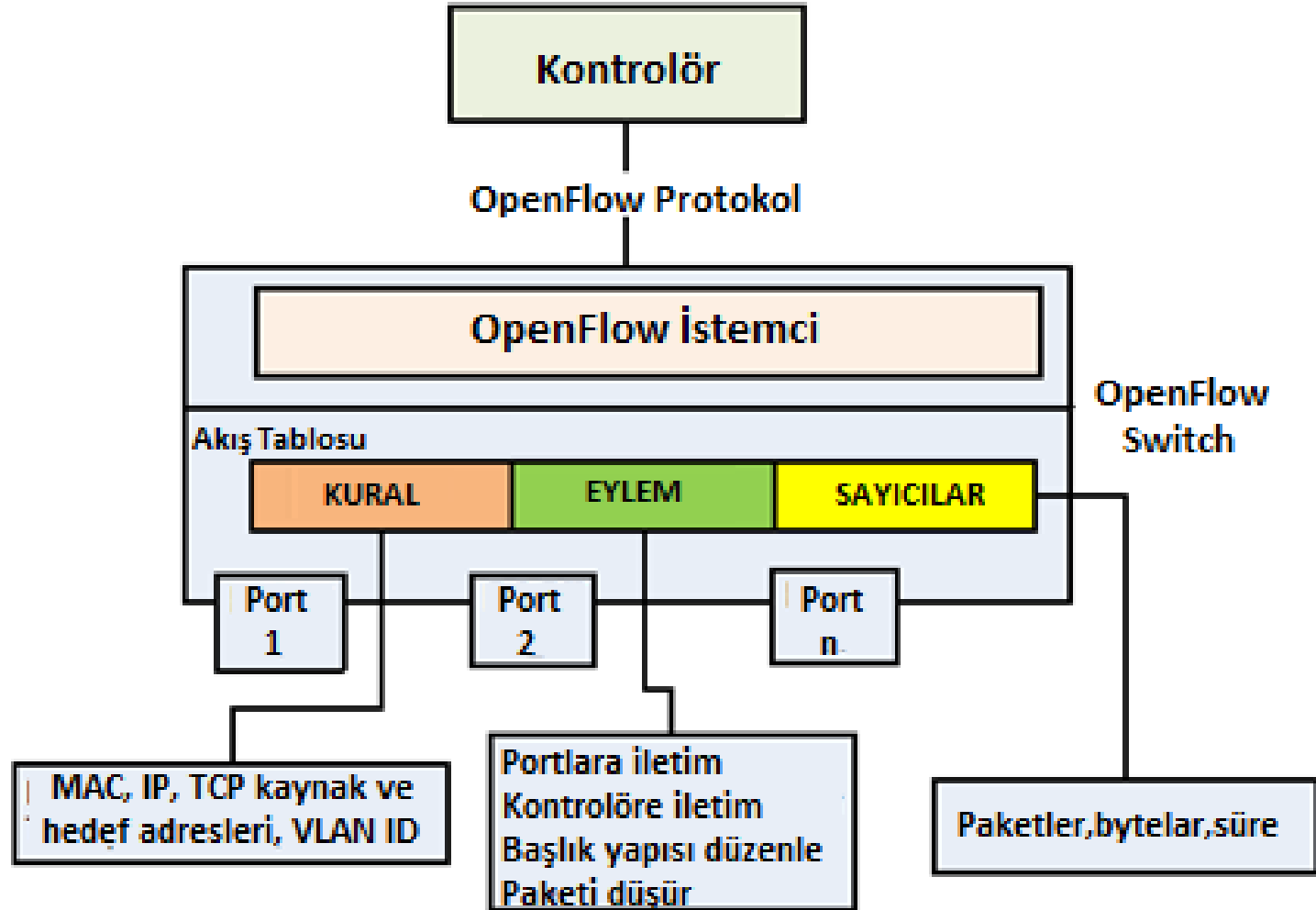
Yazılım Tanımlı Ağlar-Forces

- IETF çalışma grubu tarafından geliştirilen ForCES (Forwarding and Control Element Separation) protokolü ağdaki cihazların kontrol ve iletim işlevlerini birbirinden ayırmayı amaçlasa da, bu cihazların tek bir birimmiş gibi hareket eder.
- İletim cihazları üzerinde, tam anlamıyla Open-flow temelli yazılım tanımlı ağlardaki gibi bir soyutlama yoktur.
- ForCES, iletim elemanları ve kontrol elemanı olmak üzere iki mantıksal birim tanımlamaktadır.
- İletim elemanları kendisine gelen paketleri işlemekten sorumludurlar. Kontrol elemanı ise tüm ağın yönetimi sağlar ve iletim elemanlarının paketleri nasıl işleyeceğine karar verir.
- Bu protokol, iletim elemanlarının köle, kontrol elemanın efendi olarak tanımlandığı master-slave mantığında çalışır. İletim elemanları üzerinde kontrol elemanından gelen komutların tutulduğu ve işlendiği mantıksal fonksiyon blokları bulunur.
- 2003 yılından beri çalışmaları devam eden ilgili IETF çalışma grubu, ForCES protokolü ile ilgili mimari, bileşenler ve çalışma yapısı açısından birçok paylaşım yapmıştır.

Yazılım Tanımlı Ağlar-OpenFlow

- OpenFlow protokolü **Open Network Foundation** tarafından geliştirilmiştir.
- ForCES gibi SDN'nin temel mantığı olan iletim ve kontrol düzlemlerinin ayrıştırılmasına göre çalışmaktadır.
- ForCES'ten farklı olarak OpenFlow protokolünde **akış tabloları** ve **farklı mesaj tipleri** kullanılmaktadır.
- SDN ağlarında en çok tercih edilen Güney Sınırı API'sidir.

Yazılım Tanımlı Ağlar-OpenFlow

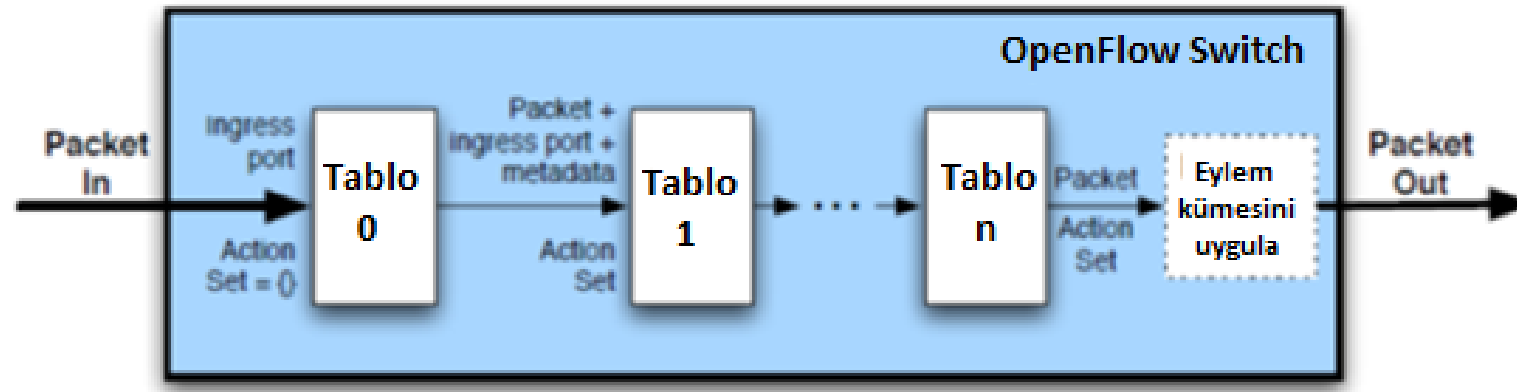


Yazılım Tanımlı Ağlar-OpenFlow

- Bir Openflow destekli iletim elemanı, bir veya birkaç akış tablosundan ve de Openflow vasıtasıyla kontrolör ile haberleşen bir soyutlama katmanından oluşur.
- Akış tabloları, kendilerine gelen her bir paketin nasıl işleneceği ve iletileceği ilgili bilgileri tutan akış girdilerinden oluşmaktadır.
- Akış girdileri genellikle, eşleşme alanı, sayıcılar ve komut kümeleri olmak üzere 3 alandan oluşmaktadırlar.
 - 1. Eşleşme alanı;** SDN temelli anahtar cihazı, kendisine gelen paketleri akış girdilerine göre, paket başlığı, ingress portu ve meta veriye bağlı olarak karşılaştırmasını yapar.
 - 2. Sayıcılar;** Anahtar cihaza gelen paket sayısı, boyutu, akış süresi gibi verileri tutarak düzenli akış istatistik toplar.
 - 3. Komut/eylem kümeleri;** Gelen paketlerin nasıl işleneceği ve eşleştirilmesi ile ilgili işlemlerin yapıldığı kısımdır.

Yazılım Tanımlı Ağlar-OpenFlow (Akış tablosu)

- Openflow temelli bir anahtar cihaza bir paket geldiği zaman, paket başlığı çıkartılarak, anahtar üzerindeki akış tablosundaki akış girdileri ile bir eşleşme var mı bakılır.
- Eğer bir eşleşme var ise, anahtar kümesi eylem kümesindeki işleme göre paketi iletir veya iletmez.
- Bir eşleşme olmaması durumunda paket ile ilgili anahtar cihaz üzerinde **tablemiss akış girdisi** oluşturulur.



Yazılım Tanımlı Ağlar-OpenFlow (Mesajlar)

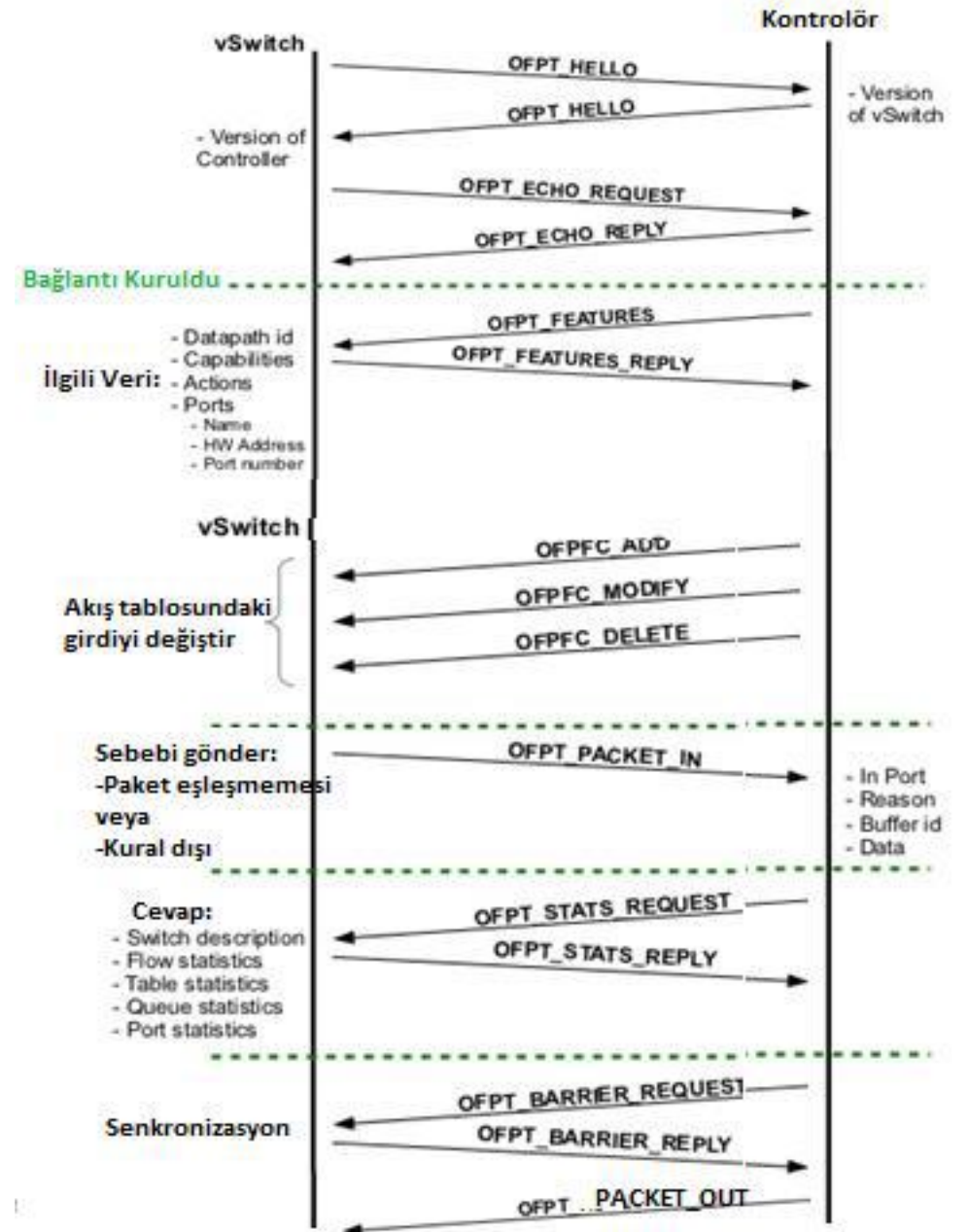
- OpenFlow mesajları üç ana tipte kategorize edilebilir. Bunlar;
 1. **Kontrolör-anahtar arası mesajlar;** Kontrolör tarafından başlatılan ve anahtarların durumunu gözetlemek veya yönetmek için kullanılan mesaj tipleridir.
 2. **Asenkron mesajlar;** Bir anahtar ağ olaylarında kontrolörü güncellemek için asenkron mesajlar başlatabilir ve anahtarın durumunu değiştirir.
 3. **Simetrik mesajlar;** Herhangi bir istek olmadan anahtar ya da kontrolör tarafından başlatılan mesaj tipleridir. Örneğin, kontrolör-anahtar bağlantısı canlılığını kontrol etmek için bu tip mesaj kullanılır.

Yazılım Tanımlı Ağlar-OpenFlow (Mesajlar)

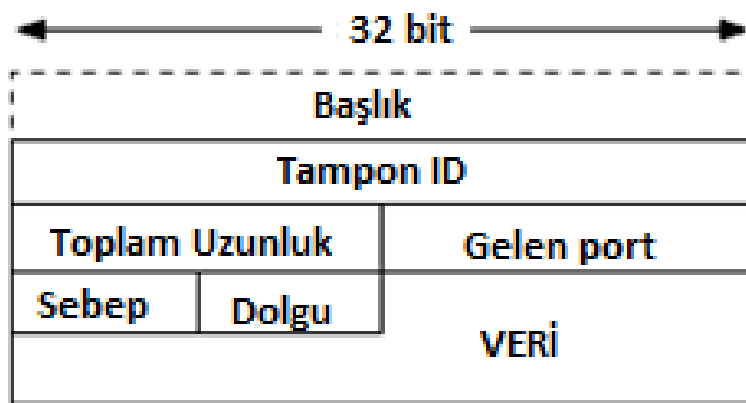
- Openflow protokoku (sürüm 1.4) haberleşme, bağlantı kurulumu, durum bildirimi, yapılandırma bilgisi gibi birçok işleve sahip mesaj tipleriyle birlikte toplam 32 çeşit mesaj tipi vardır.
- Fakat bu mesaj tiplerinden en önemlileri yazılım tanımlı ağlardaki, veri ve kontrol düzlemlerini soyutlama mantığına dayalı akış tablolarındaki akış girdileriyle alakalı olan “packet_in” ve “packet_out” mesaj tipleridir.

SDN-(OpenFlowBağlantı Kurulumu)

- Bir anahtar cihaz kendisine gelen paketi, kendi üzerindeki akış tablosunda eşleştiremediği zaman bu paketi, kontrolör ile bağlantı kurulumu işlemlerinden sonra bir **packet_in** mesajı içerisinde kontrolöre iletir.
- Kontrolör kendisine gelen packet_in mesajını ayrıştırarak, önceden tanımlı kural veya kendi iç modüllerine göre hedefe en uygun yol üzerinden **packet_out** veya **flow_mod** mesajı içerisinde yollar.
- Yol üzerindeki ilgili anahtar cihazlar kendilerine gelen bu mesajı ayrıştırarak, akış tablolarına yeni girdi olarak ekleme yaparlar ve kaynak-hedef arası yol belirlenir.

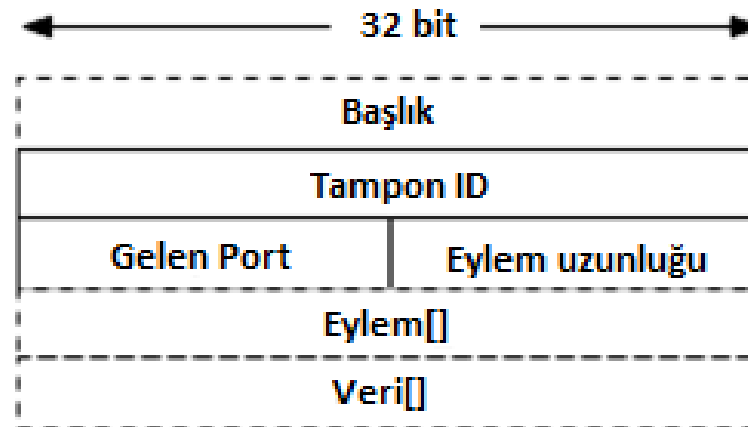


Yazılım Tanımlı Ağlar-(OpenFlow Mesaj Başlık Yapıları)



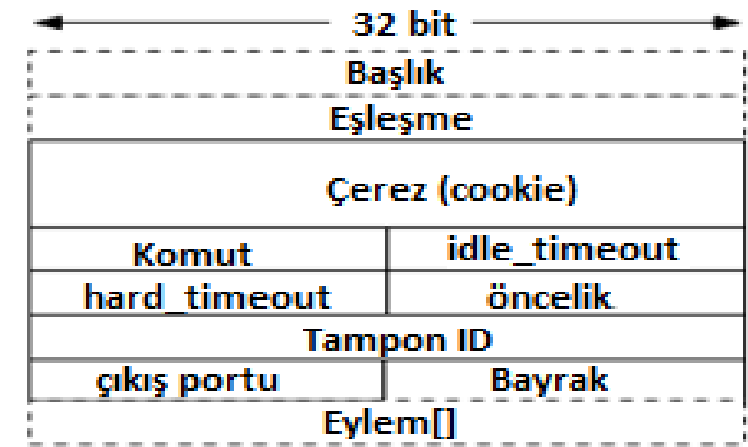
Paket byte dizilimi

Packet_in



Paket byte dizilimi

Packet_out



Paket byte dizilimi

Flow_mod

Yazılım Tanımlı Ağlar-Kontrolör

- Kontrolör, katmanlı mimaride ağ işletim sistemlerinin ana parçası olmasının yanı sıra SDN ağların da kontrol ve yönetim merkezinde yer alır.
- Ağdaki iletim elemanlarını, gerek uygulama temelli gerekse kendi iç modülleri kullanarak akış girdileri vasıtasıyla yönetmek zorundadır.
- Kontrolörler tarafından;
 - **Proaktif**
 - **Reaktif**
- olmak üzere iki farklı akış kurulum modu vardır.

Yazılım Tanımlı Ağlar-Kontrolör (devam)

1. Proaktif akış kurulumlarında, paketlerin nasıl işleneceği ve iletileceği ile ilgili akış kuralları anahtar cihazlar üzerindeki akış tablolarına önceden yüklenir.

Bu atip akış kurulumlarının ana amacı ve avantajı, iletim cihazları ve kontrolörün bağlantı kurulum sıklığının azaltılması ve gecikme, jitter gibi servis kalitesi kriterlerinin iyileştirilmesidir.

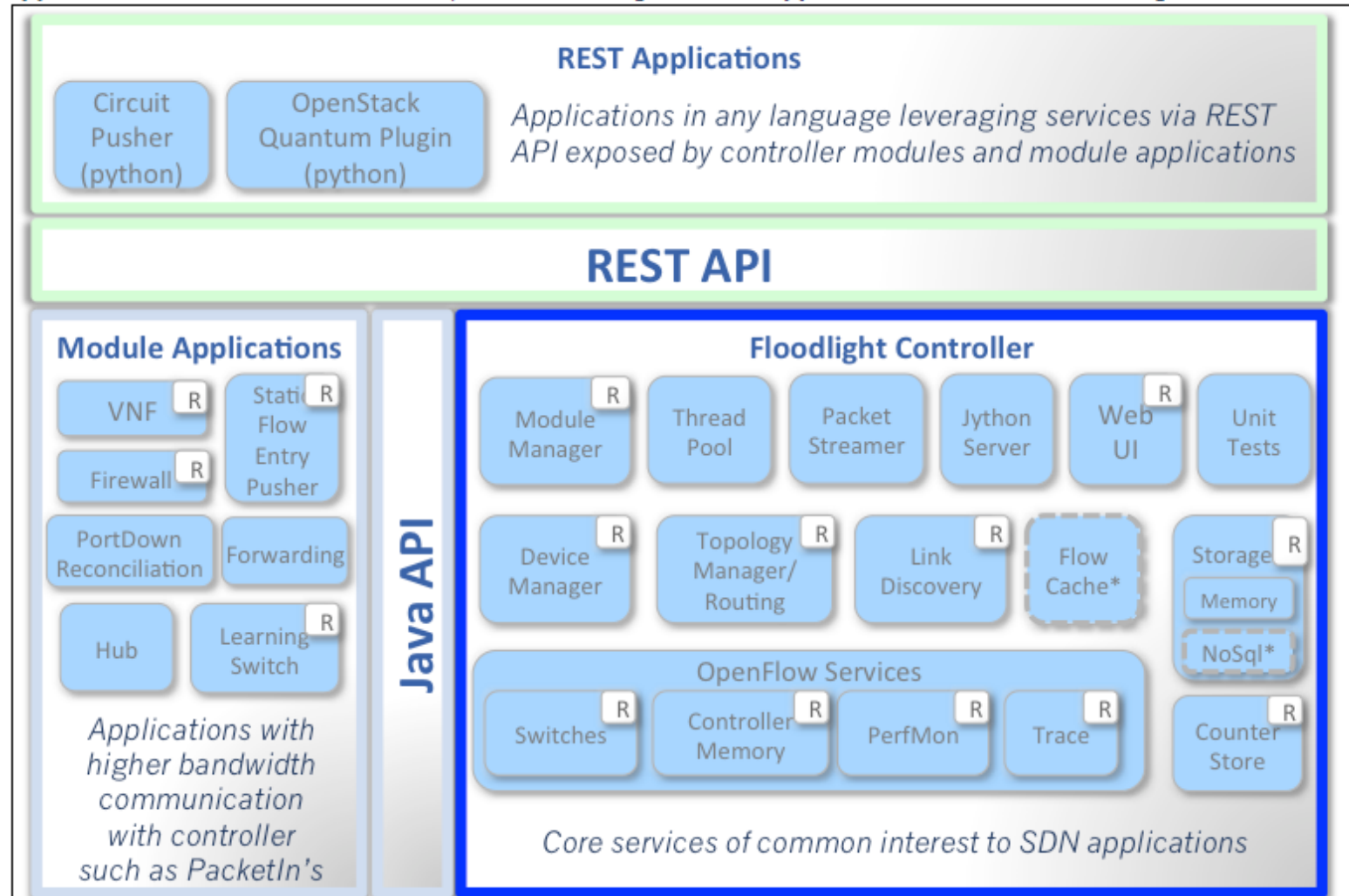
2. Reaktif akış kurulumlarında ise, Openflow destekli anahtar cihazların akış tabloları üzerinde gelen paketlerle ilgili bir akış girdisi olmadığı zaman (table-miss) iletim elemanlarının kontrolör ile bağlantı kurulumu yapılır.

Bu akış girdileri, önceden tanımlı bir durgunluk süreaşımından sonra geçersiz kılınır ve tablodan silinir. Reaktif akış kurulumu yüksek bir Gidiş-Geliş Süresinden (Round Trip Time) muzdarip olsa da, QoS gereksinimleri ve trafik yük şartları dikkate alındığında akış seviyesinde kararlar vermek için belirli esneklik derecesi sağlar.

SDN Kontrolör Karşılaştırma

Özellik	NOX	POX	Beacon	Floodlight	OpenDaylight
Geliştirilen/ Desteklenen Dil	C++, Python	Python	Java	Java, Python	Java
Projenin Durumu	Devam	Tamam	Bakım	Tamam	Tamam
Kurulum/Programl ama Kolaylığı	H	E	E	E	E
Dökümantasyon	Kötü	İyi	İyi	İyi	Orta
REST API Desteği	Yok	Sınırlı	Var	Var	Var
Kullanıcı Arayüzü	Python +QT4	Python+Q T4, Web	Web	Java, Web	Web
Çoklu Düğüm Desteği	Yok	Yok	Yok	Var	Var
Döngü Teknoloji Desteği	Yok	Yok	Yok	Var	Var
non-OF island Bağlantı Desteği	Yok	Yok	Yok	Var	Var
Güney Sınırı Protokollerinde Soyutlama Desteği	Yok	Yok	Yok	Yok	Var
OpenStack Quantum Desteği	Yok	Yok	Yok	Var	Var

Yazılım Tanımlı Ağlar-Floodlight Kontrolör



Yazılım Tanımlı Ağlar-Uygulama Yazılımları

- Yazılım tanımlı ağ paradigmasının iletim elemanları üzerindeki kontrol ve veri düzlemlerini soyutlanmasıyla, ağ ihtiyaçları ve servis kalitesini arttırmak için özellikle;
 - adaptif yönlendirme,
 - yük dengeleme,
 - katmanlar arası geçiş,
 - ağ sanallaştırma
 - sınırsız iletişim/dolaşım,
 - kolay ağ yönetimi ve bakımı, ağ güvenliği,
- gibi genel konularda yeni protokol ve servisler üzerinde çalışmalar hızlanmıştır.

SDN-Uygulama Yazılımları (Adaptif Yönlendirme)

- Adaptif yönlendirme; Paket anahtarlama ve yönlendirme, bir ağın temel fonksiyonlarıdır.
- Bu kavramlar, geleneksel ağlarda sağlamlığı sağlayabilmek için farklı ve dağıtık yaklaşımlar üzerine oturtulmuştur.
- Bu farklı yaklaşımlar/tasarımlar;
 - karmaşık implementasyon,
 - yavaş yakınsama,
 - sınırlı yönetim gibi birçok problemi beraberinde getirmiştir.
- Buna karşın yazılım tanımlı ağlar, uygulamalara genel ağ durum bilgilerini elde etme ve ağı adaptif kontrol etmelerine izin vermişlerdir.

SDN-Uygulama Yazılımları (Yük Dengeleme)

- Yük dengeleme; Yük dengeleme, ağ yapılarında daha iyi kaynak kullanımı sağlamak amacıyla uzun süredir çalışılan bir konudur.
- Özellikle veri merkezi gibi ağlarda kullanıcıların isteklerine karşılık verebilmek için;
 - **işlem hacmini artıran,**
 - **cevap süresini azaltan,**
 - **ağdaki overload** dan kaçınan atanmış yük dengeleyiciler kullanılır.
- Bu sistemlerin pahalı olması ve yazılım tanımlı ağ kontrolörlerinin yük dengeleme modülleri sayesinde veri merkezlerinde geleneksel sistemlerin yerini yazılım tanımlı ağlar almaya başlamıştır.

SDN-Uygulama Yazılımları (Katmanlar Arası Geçiş)

- Katmanlar arası geçiş tasarımı; OSI referans modelindeki katmanlı mimarideki farklı katmanlardaki birimlerin entegrasyonun arttırılması üzerine kurulu bu yaklaşım, yazılım tanımlı ağların uygulamalara ağ durum bilgilerine kolay erişim ve servis kalitesi desteği vermesiyle birlikte daha da gelişmiştir.

SDN-Uygulama Yazılımları (Sınırsız Dolaşım)

- Sınırsız dolaşım; Akıllı telefon ve tabletler internet erişiminde baskın cihazlar haline gelmişlerdir.
- Bu cihazların internete erişimleri kablosuz olarak sağlandığından, bir konumdan başka bir konuma hareket halindeyken sürekli bağlantının sağlanabilmesi için, istasyonlar arasında iletişimlerin değiştirilmesi gerekmektedir.
- Farklı teknolojiler ve farklı taşıyıcılar ile kontrol düzleminde yapılacak uygulamalar bu tip ağlarda da yazılım tanımlı ağların gerekliliğini ortaya koyacaktır.

SDN-Uygulama Yazılımları (Ağ Yönetimi/Bakımı)

- Ağ yönetimi/bakımı; Ağ üzerinde yapılan her hangi bir yapılandırma hatası, ağdaki veri trafiğini olumsuz etkilemektedir.
- Yapılan araştırmalar neticesinde ağ kesintilerinin %60'lık gibi büyük bir oranının ağ operatörleri tarafından yapılan yanlış cihaz yapılandırmalarından kaynaklandığı belirtilmektedir.
- Merkezi ve otomatik yönetim ile ağdaki iletim elemanlarına ilke göndererek yazılım tanımlı ağlar, ağ yapılandırmalarındaki hata oranını büyük ölçüde düşürerek kesintisiz ve verimli bir ağ hizmeti sunabilmektedirler.

SDN-Uygulama Yazılımları (Ağ Güvenliği)

- Ağ güvenliği; Ağ güvenliği, siber güvenliğin en önem arz eden bir alt konusudur.
- Geleneksel ağlarda güvenlik için, güvenlik duvarları, vekil sunucular gibi fiziksel ve yazılımsal çözümler kullanılmaktadır.
- Ağ altyapıları ve uygulamalarının heterojen ve karmaşık yapılarından dolayı bu cihazlar üzerinde her ağ durumu için ayrı ayrı ilke ve yapılandırmalar yapılmak zorundadır.
- Bu sebepten ötürü yazılım tanımlı ağlar ağ güvenliği konusunda, gerek kontrolörlerin güvenlik modül uygulamaları, gerekse ağın merkezi kontrolü sayesinde geleneksel ağlara göre daha avantajlı durumdadırlar.