Openflow switch model

Cos'è SDN?

Software-Defined Networking (SDN) è un nuovo approccio alla programmabilità della rete, ovvero la capacità di inizializzare, controllare, modificare e gestire dinamicamente il comportamento della rete per mezzo di interface aperte. [RFC7426]

In breve gli elementi chiave di SDN sono:

- un livello di astrazione tra il piano utente e il piano di controllo
- interfacce aperte
  - tra piano utente e piano di controllo
  - tra piano di controllo e applicazioni
- possibilità per le applicazioni di programmare il comportamento della rete

Virtualizzazione

La virtualizzazione è una astrazione molto comune.

Virtuale = non esistente come oggetto fisico, ma fatto apparire come tale grazie al software

Qualcosa che si può usare come fosse reale, ma in realtà condiviso con altri.

- facilità d'uso
- condivisione ed uso più efficiente delle risorse

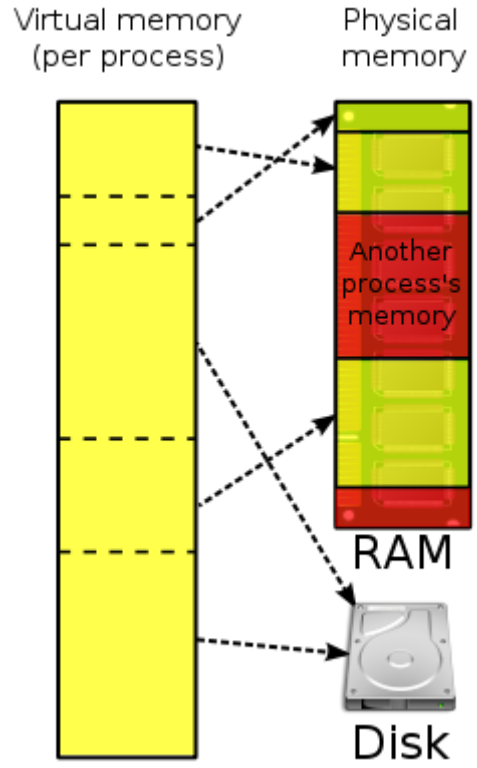
Memoria virtuale

Astrazione della memoria fisica

Il programmatore vede un’unica memoria dedicata al proprio processo

Il software gestisce in modo efficiente l’uso condiviso della memoria fisica

Nasconde la complessità e semplifica lo sviluppo

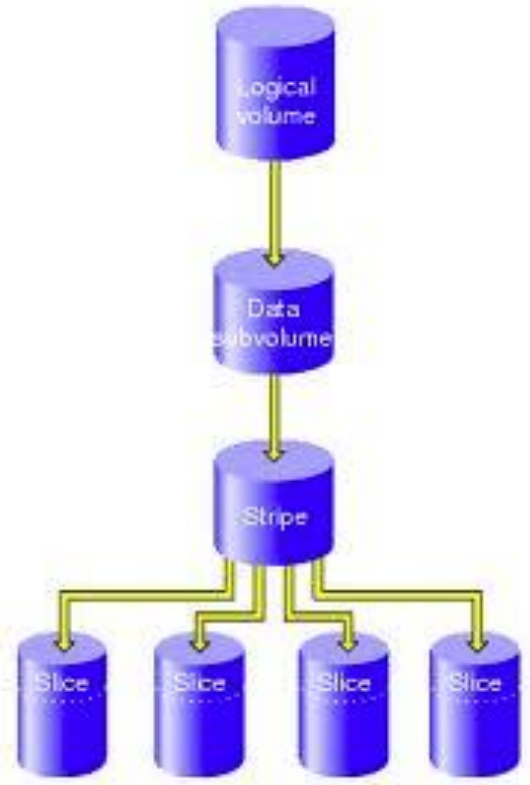


Dischi virtuali

Astrazione dei dischi fisici

Permettono di modificare dinamicamente la din
partizione

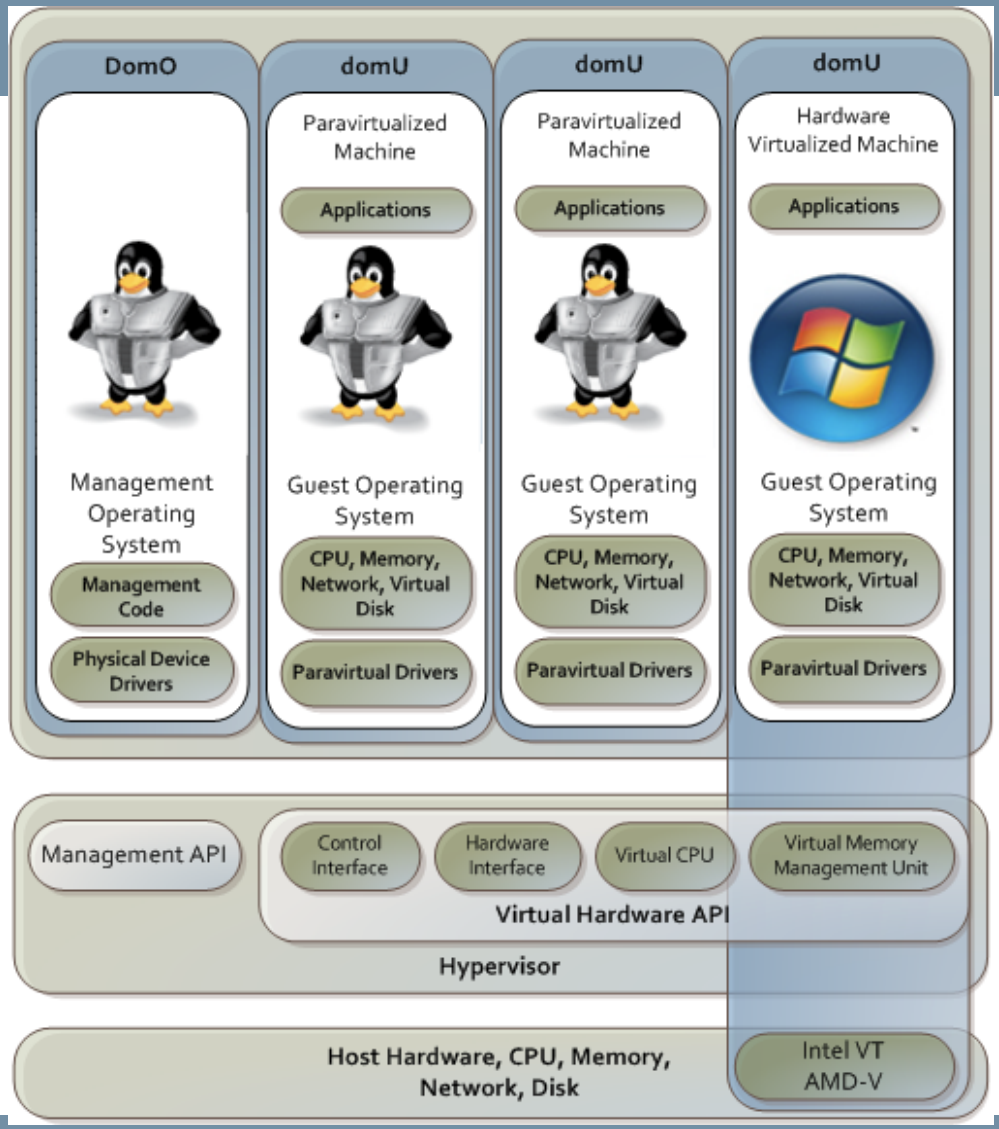
Forniscono servizi aggiuntivi di ridondanza



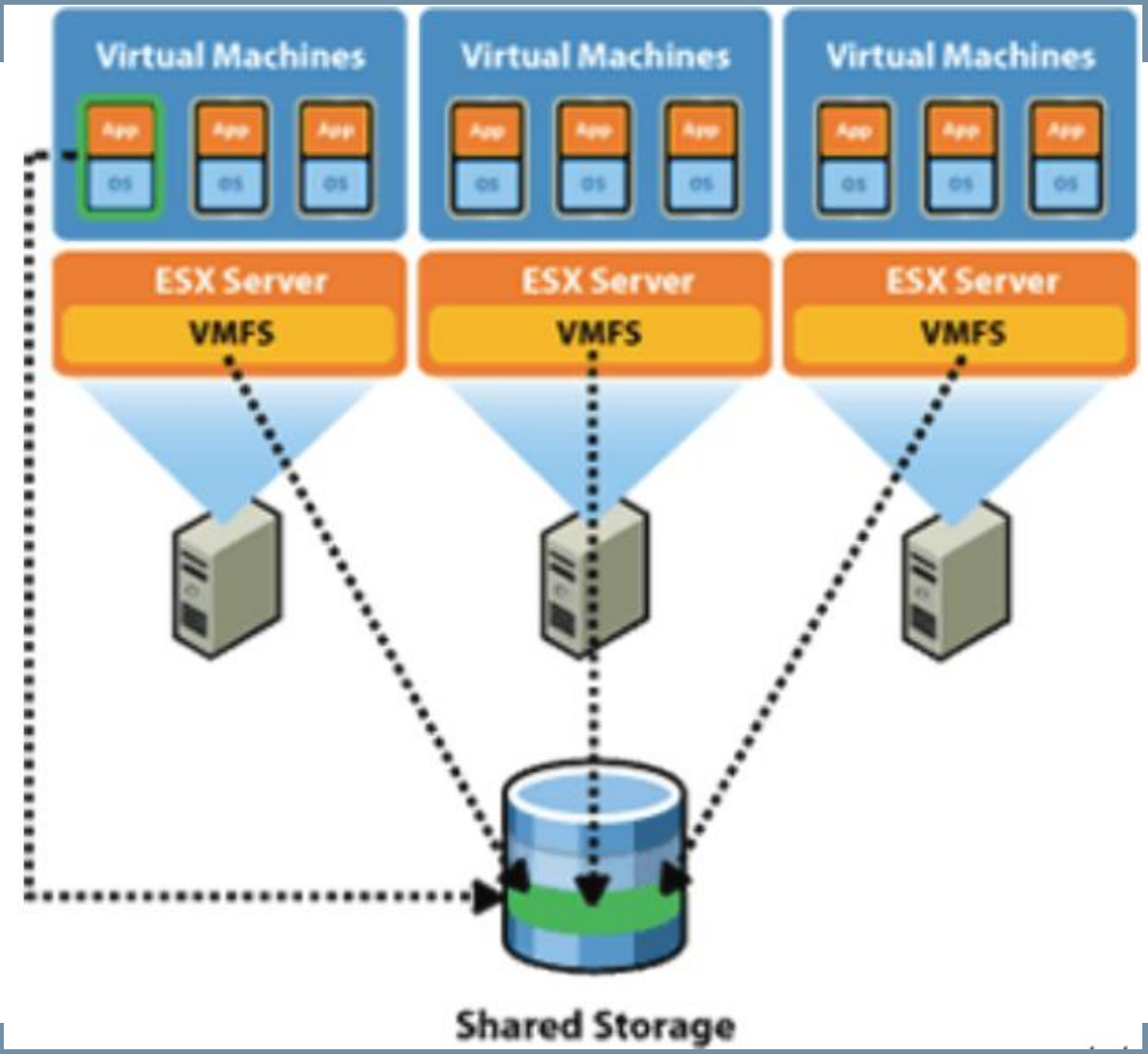
CPU virtuali

Astrazione delle macchine fisiche

Permettono di istanziare facilmente nuove macchine semplificando l'amministrazione



Virtualizzazione combinata



Virtualizzazione di rete?

Reti virtuali sono di uso comune:

- VLAN (L2)
- Tunnel (L2/L3)
- VPN (L2/L3)

Si possono avere astrazioni di livello 2 – 4 che semplifichino la gestione della rete?

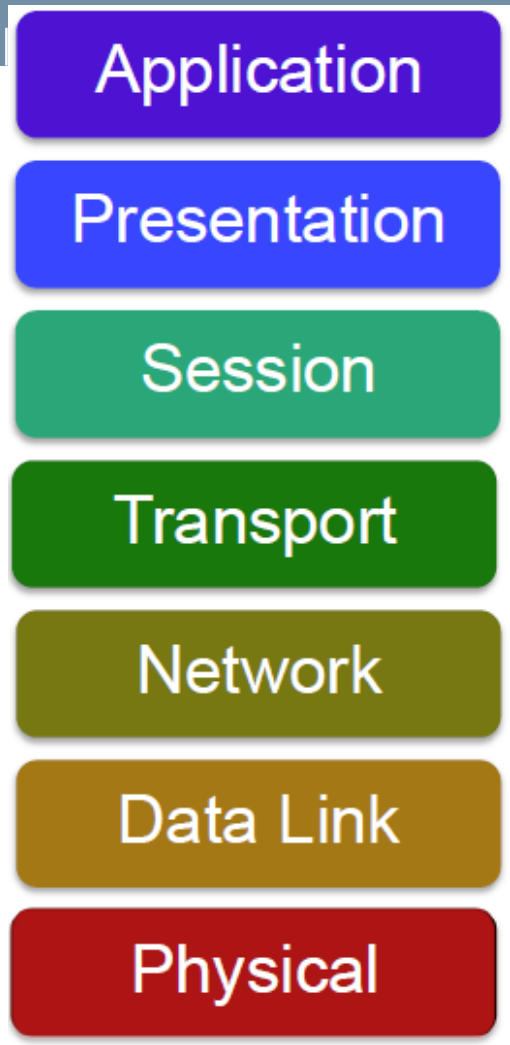
Astrazione nelle reti

Il modello OSI è un'astrazione del piano dati:

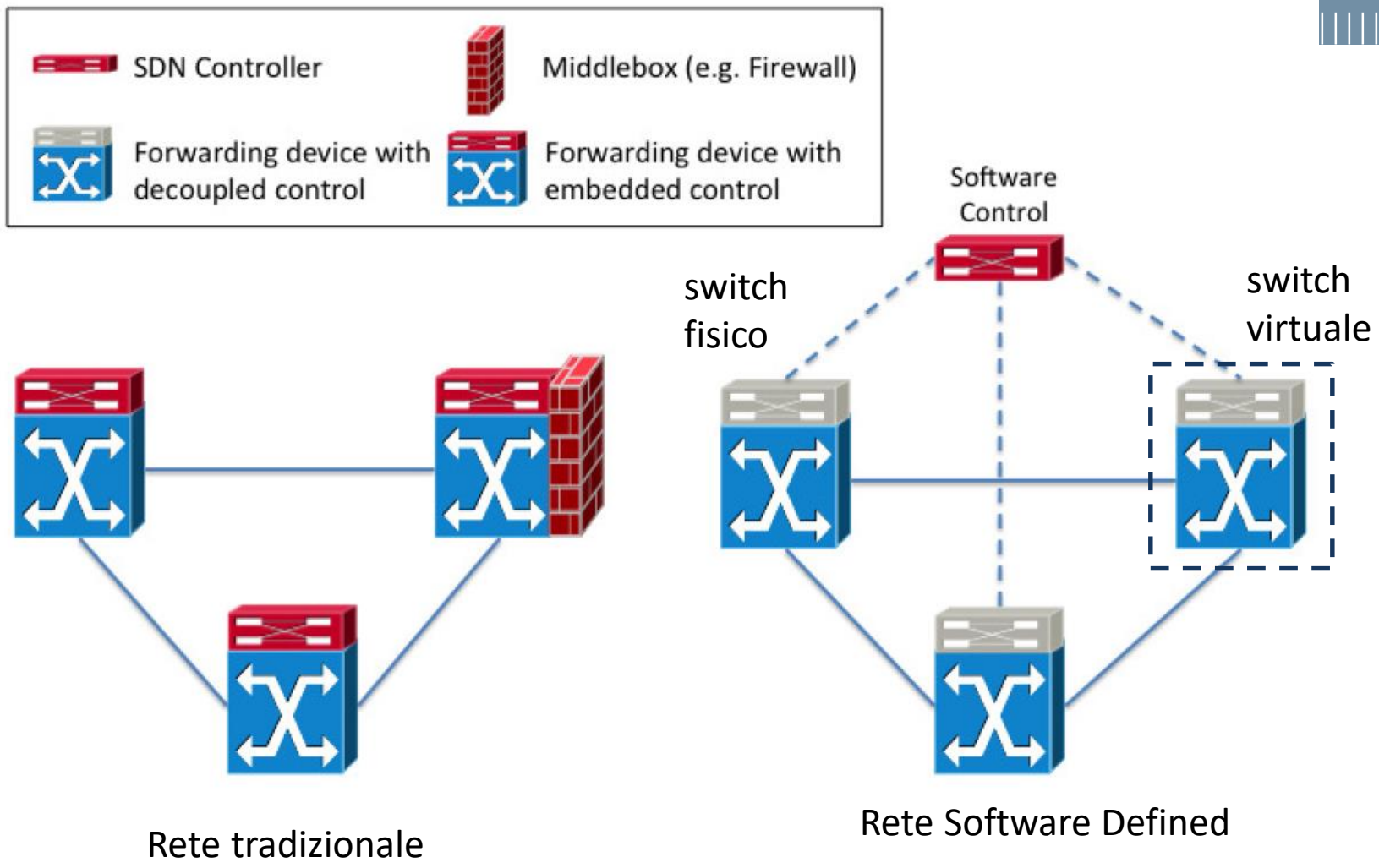
- semplifica il progetto e l'implementazione
- introduce inefficienze.

Software Defined Networking è un'astrazione del piano di controllo

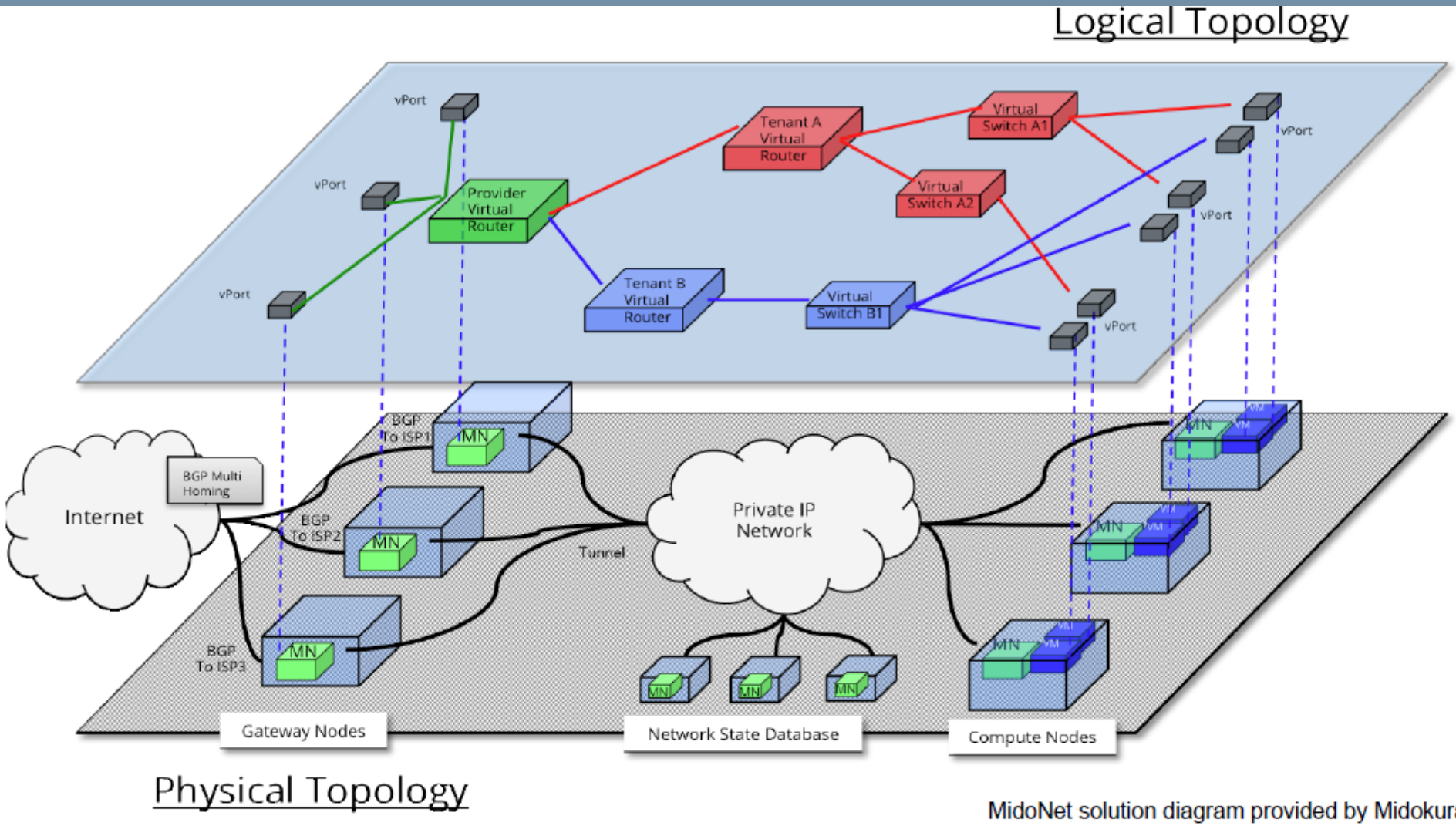
- permette di istanziare reti virtuali per gestire specifici servizi
- si integra con la virtualizzazione delle CPU



Visione uniforme di switch fisici e switch virtuali

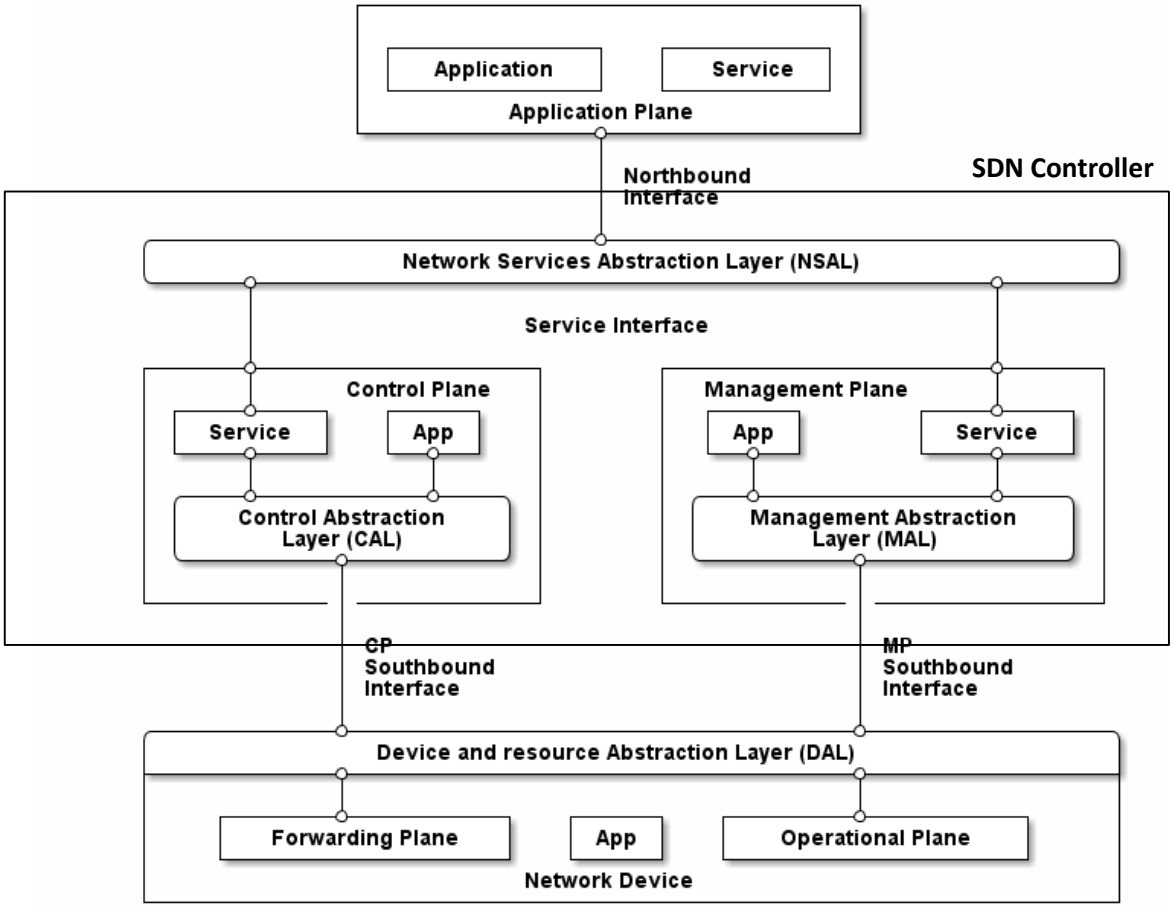


Rete Virtuale

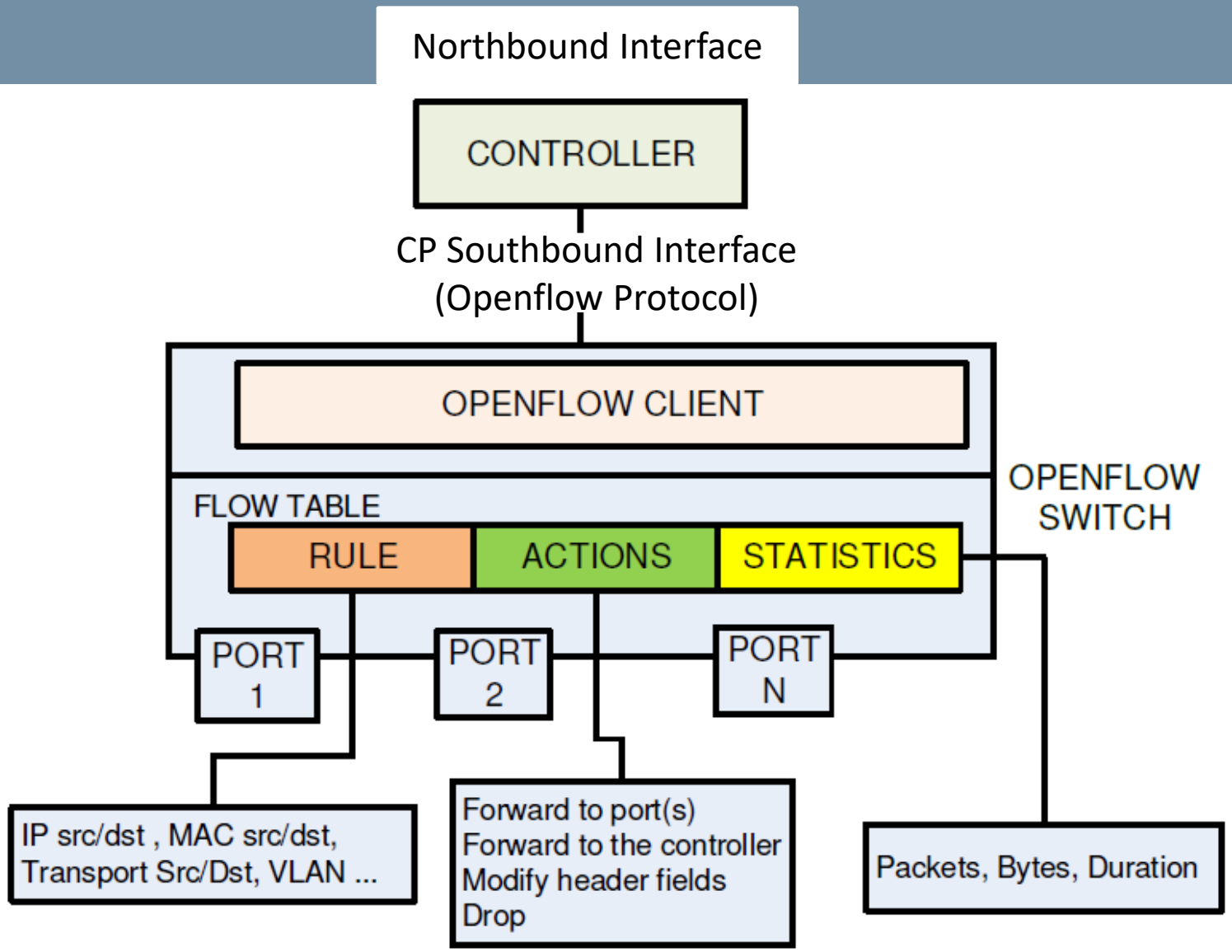


MidoNet solution diagram provided by Midokura

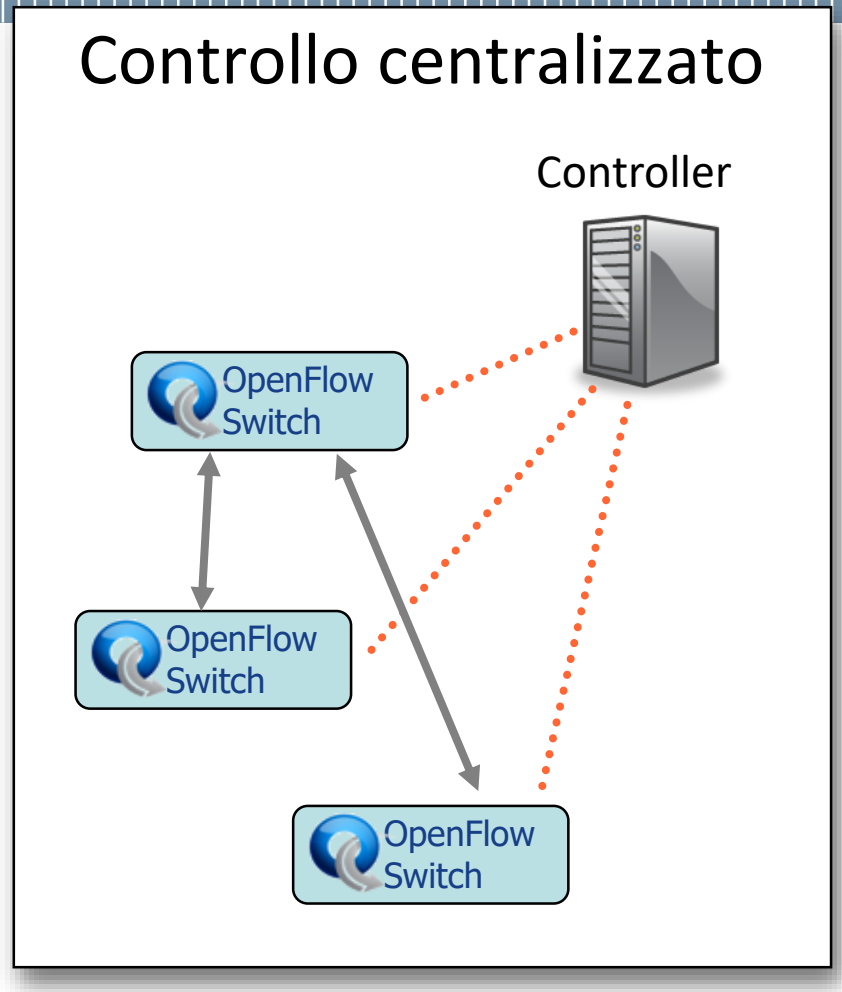
Architettura SDN

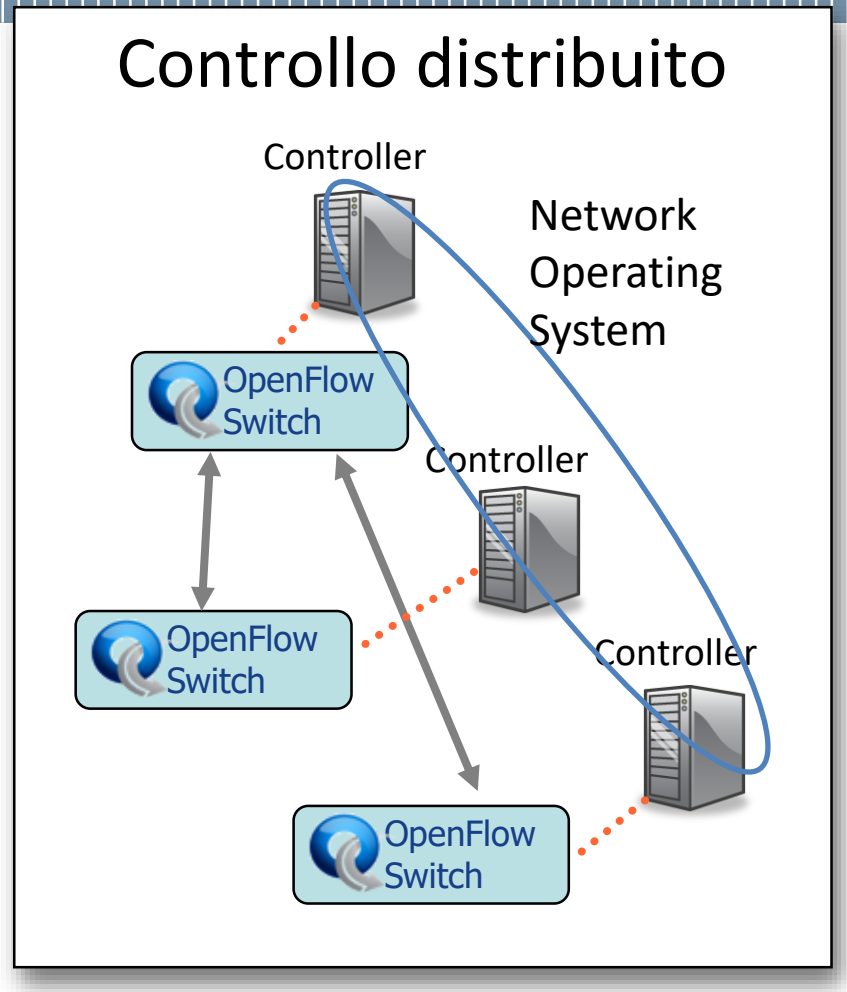


Architettura Openflow



Modelli di controllo
Centralizzato vs Distribuito





Modelli di controllo
Granularità

Pacchetto singolo (modello non SDN)

- decisioni sulla base dell'indirizzo destinazione
- exact match o prefix match

Modello per flusso

- decisioni sulla base di più campi del pacchetto
- tipicamente i campi che definiscono un socket pair
- tutte le regole usano gli stessi campi
- match esatto

Modello per aggregazione di flussi

- decisioni sulla base di più campi del pacchetto
- ogni regola può guardare un diverso insieme di campi
- multifield packet classification

Modelli di controllo
Reattivo vs Proattivo

Modello reattivo

- flow table inizialmente vuota
- al primo pacchetto di un flusso si chiede al controllore
- il controllore installa una regola per il nuovo flusso

Modello proattivo

- all’accensione lo switch chiede le regole al controllore
- il controllore installa tutte le regole

Openflow-only vs Openflow-hybrid

Uno switch Openflow-only elabora i pacchetti esclusivamente usando le regole openflow

Uno switch Openflow-hybrid può elaborare i pacchetti in accordo alle regole openflow oppure in accordo alle regole di un normale switch, router o switch L4

- pacchetto per pacchetto, sulla base della porta fisica o logica lo switch sceglie il modo di funzionamento
- la parte openflow può scegliere di inviare il pacchetto all'elaborazione normale

Openflow

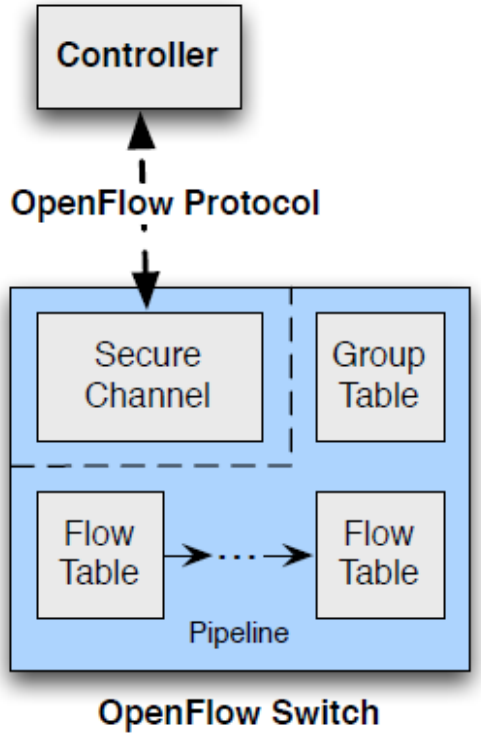
Lo standard Openflow definisce

- un modello astratto di switch
- le azioni che il controller può compiere sullo switch
- un protocollo southbound

Openflow **non** è uno standard IETF

Diverse versioni del protocollo:

- 2008 v. 0.2 (la prima)
- **aprile 2012 v. 1.3 (usata in questo corso)**
- settembre 2016 v 1.6 (più recente)



Switch Openflow
Componenti dello switch

Con riferimento a Openflow 1.3

Lo switch contiene una o più flow table e una group table

Ogni flow table contiene un insieme di flow entries

Ogni flow entry consiste di

- campi di match
- contatori
- insieme di istruzioni da applicare ai pacchetti corrispondenti alla regola di match

Usando il **protocollo openflow** il controllore può aggiungere, modificare o cancellare le flow entries

Verifica delle corrispondenze

La verifica delle corrispondenza tra pacchetto e regole

- inizia con la prima tabella e può continuare sulle tabelle successive (pipeline processing)
- in ogni tabella la verifica segue un ordine di priorità
- ogni tabella può specificare una o più azioni e/o inviare alla tabella successiva
- se non è specificata una tabella successiva il pacchetto è inviato ad una interfaccia oppure alla group table

Se non viene trovata una corrispondenza si esegue la table-miss entry. Se la table-miss entry non è presente il pacchetto è scartato.

Porte Openflow

Rappresentano le interfacce di entrata e di uscita dallo switch

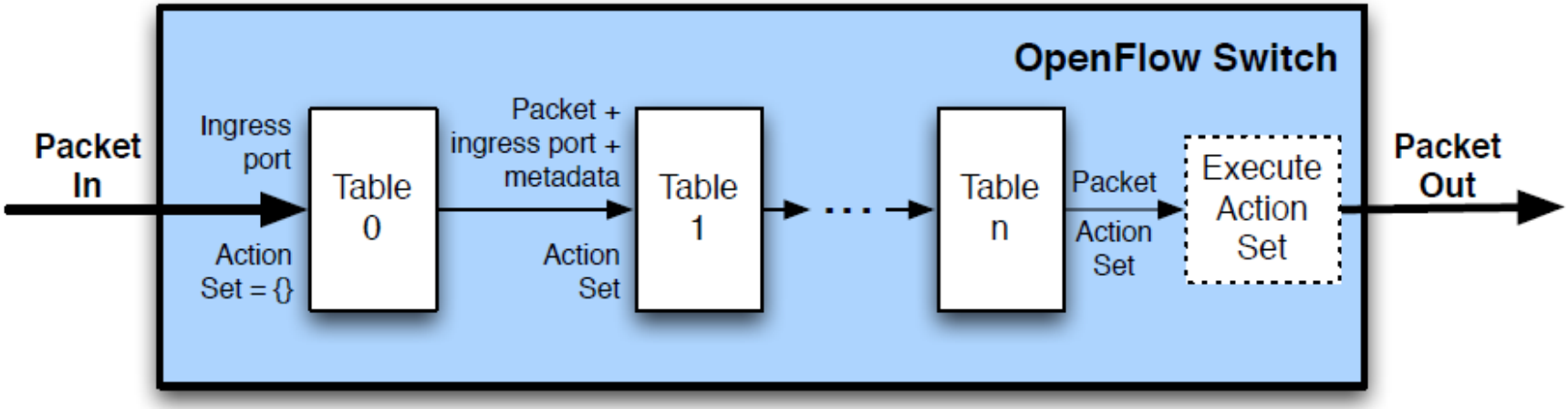
Tipi di porte:

- porte fisiche: sono in corrispondenza con le interfacce fisiche
- porte logiche: sono astrazioni che non corrispondono a un hardware
  - tunnel
  - aggregazioni di link
  - loopback
- porte riservate: definite dalla specifica
  - possono essere porte di solo ingresso o di sola uscita

Porte Openflow riservate

- ALL
  - solo output verso tutte le porte tranne la porta di ingresso del pacchetto
- CONTROLLER
  - in input, il pacchetto è arrivato dal controllore incapsulato in un messaggio di controllo openflow (messaggio packet-out)
  - in output, il pacchetto è spedito al controllore incapsulato in un messaggio di controllo openflow (messaggio packet-in)
- IN_PORT
  - solo input, rappresenta la porta di ingresso del pacchetto
- altre porte riservate: TABLE, ANY, LOCAL, NORMAL, FLOOD

Pipeline openflow



Per ogni tabella

- trova la regola corrispondente a massima priorità
- aggiunge al action set le corrispondenti azioni
- esegue eventuali azioni immediate
- invia alla tabella successiva

Al termine della pipeline

- esegue le azioni nel action set

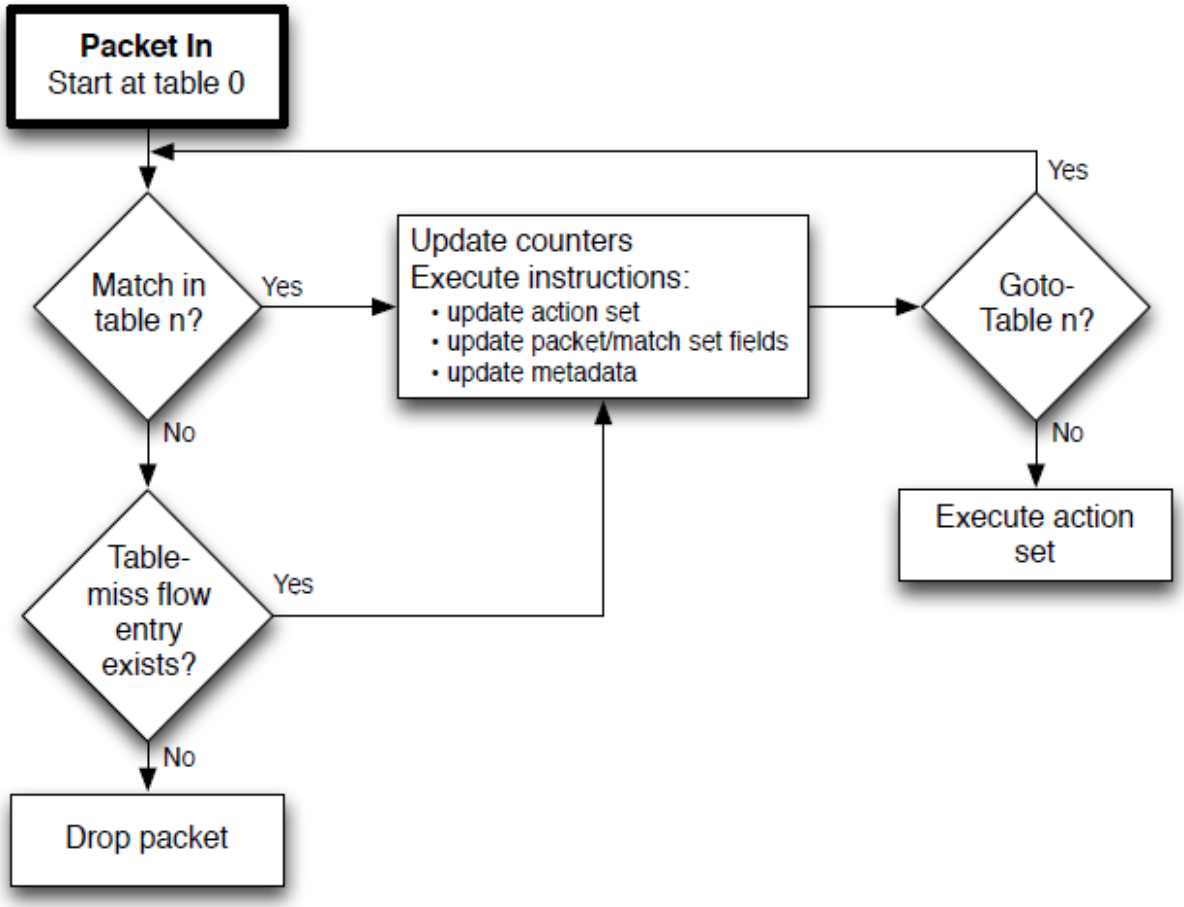
Flow Table

Match Fields	Priority	Counters	Instructions	Timeouts	Cookie

Ogni flow entry consiste in:

- campi di match: porta di ingresso, campi del pacchetto, metadati da una tabella precedente
- priorità di match nella tabella
- contatori aggiornati ad ogni match
- istruzioni
- timeout: tempo massimo o tempo massimo di idle prima che il flusso sia rimosso
- cookie: identificativo univoco scelto dallo switch

Matching
Procedura generale



Matching

La ricerca dei match è esatta su tutti i campi.

Un campo può specificare una wildcard (ANY). Inoltre è possibile specificare bitmask su alcuni campi

La ricerca restituisce solo la flow entry corrispondente a massima priorità

In caso di più flow entry con la stessa priorità, la switch ne restituisce una a sua scelta

Nel caso non ci siano corrispondenze il pacchetto viene inviato alla table-miss entry, se presente

La table-miss entry ha una widcard su tutti i campi e la priorità minima (0)

Se la table-miss entry non è presente il pacchetto è scartato

Group Table

Group Identifier	Group Type	Counters	Action Buckets

Contiene azioni che sono applicate a gruppi. Permette maggiore flessibilità rispetto ai flussi

- Identificativo di 32 bit
- Tipo di gruppo
  - all: il pacchetto è inviato a tutti gli action bucket
  - select: il pacchetto è inviato a uno degli action bucket scelto dallo switch
  - indirect: il pacchetto è inviato all'unico action bucket
    - serve per far puntare tanti flussi a un unico bucket di azioni
  - fast failover: il pacchetto è inviato al primo bucket associato a una porta funzionante

Meter Table

Meter Identifier	Meter Bands	Counters

- Identificativo di 32 bit
- Meter band: lista di velocità associate ad azioni. Il pacchetto è inviato alla meter band di valore più elevato minore della velocità misurata del flusso

Band Type	Rate	Counters	Type specific arguments

Band type:

- drop
- dscp remark: riduce la priorità di scarto nel campo DSCP del pacchetto

Contatori

Molti contatori

- per tabella
- per flow entry
- per porta
- …

Principalmente a 64 bit

- packet count
- byte count
- durata in secondi (32 bit) e in nanosecondi (32 bit)
- errori
- …

Istruzioni

Write-Actions <list>: scrive le azioni nell'action set da eseguire al termine della pipeline

Meter <id>: invia il pacchetto al meter specificato

Apply-Actions <list>: applica le azioni immediatamente

Clear-Actions: azzera l'action set

Write-Metadata <dati/maschera>: scrive i bit specificati nel registro metadati

Goto-Table <tabella>: invia il pacchetto alla tabella specificata

- id nuova tabella deve essere maggiore di id tabella corrente

Azioni

Output <porta>: invia il pacchetto a <porta>

Set-Queue <queue-id>: imposta la queue-id del pacchetto. Viene usato se la <porta> ha più code

Drop: l'azione Drop non è esiste. E' la conseguenza dell'assenza di istruzioni

Group <group-id>: invia il pacchetto al gruppo <group-id>

Push-Tag / Pop-Tag <tag>: aggiunge la <tag> specificata. <tag> può essere VLAN, MPLS, PBB

Set-Field <campo>,<valore>: sovrascrive un campo del pacchetto

Change-TTL: può essere set/decrement/copy outwards/copy inwards

Protocollo OpenFlow

Il protocollo OpenFlow viene usato per scambiare messaggi tra switch e controller. Usa TLS su TCP.

Usa tre tipi di messaggi:

- controller-to-switch
- asincroni (da switch a controller)
- simmetrici (peer-to-peer)

Principali messaggi controller-to-switch «Features»

- inviato all'attivazione del canale tra controller e switch
- richiede allo switch le capabilities
  - datapath ID (~ identificativo dello switch)
  - dimensione buffer
  - numero massimo di tabelle
  - …

Principali messaggi controller-to-switch «Packet-out»

- usato per inviare pacchetti singoli su una porta specifica
- il payload del messaggio può essere un intero messaggio (layer 2-7) oppure un identificativo (buffer-id) di un pacchetto nello switch
- il messaggio deve contenere anche una lista di azioni

Principali messaggi controller-to-switch «Modify-State»

Usato per aggiungere, rimuovere, modificare flow entry e per impostare le proprietà dello switch

Principali messaggi asincroni «Packet-in»

- Usato per inviare pacchetti dallo switch al controllore
- il pacchetto (o parte di esso) è il payload del messaggio
- inviato quando l'azione sul pacchetto è output verso la porta riservata CONTROLLER
- Lo switch può bufferizzare il pacchetto e inviare nella packet-in solo i primi byte del pacchetto e un buffer-id

Principali messaggi asincroni «Flow-Removed»

Informa il controllore della rimozione di una flow entry a seguito di una richiesta esplicita oppure per timeout

Principali messaggi asincroni «Port-status»

Informa del cambio di stato di una porta, per esempio in seguito a un guasto