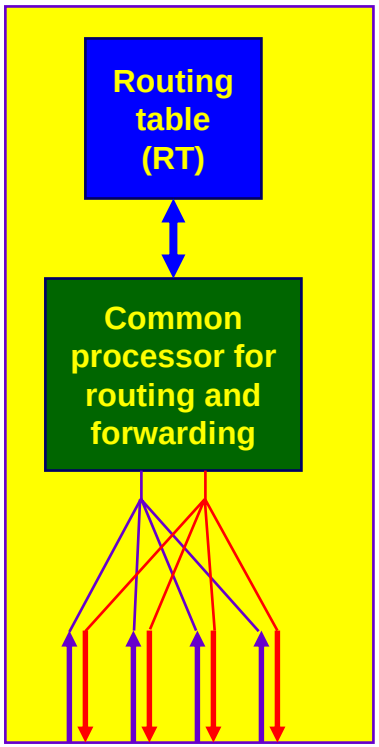
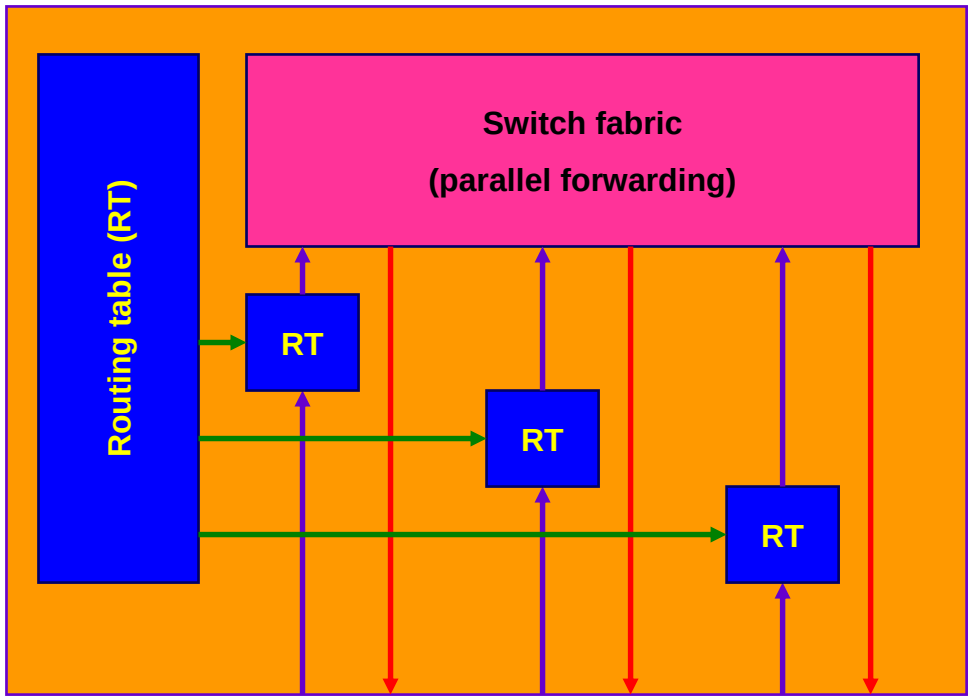
ROUTING vs. FORWARDING

ROUTERS EVOLUTION

Serial processing (S/W based routing)



Parallel processing (routing / forwarding separation)

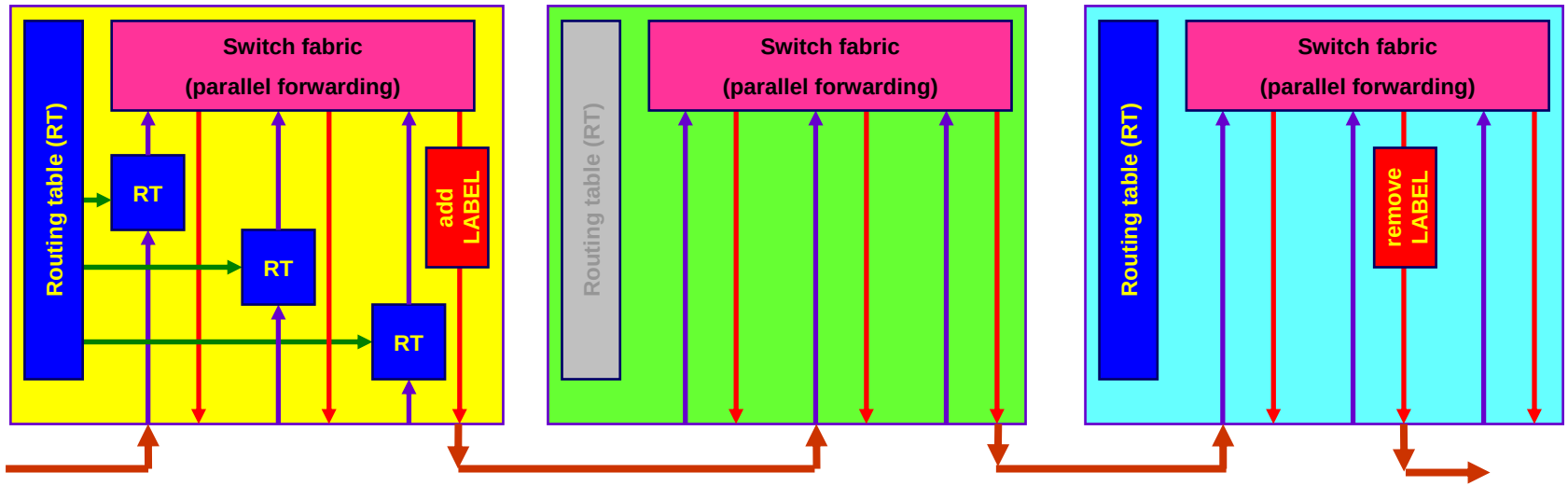


The routing table is replicated at each port. Routing decisions are taken simultaneously. A switch fabric has to be present, to allow simultaneous data transfer from port to port.

ROUTING vs. FORWARDING

ROUTERS EVOLUTION

Label switching



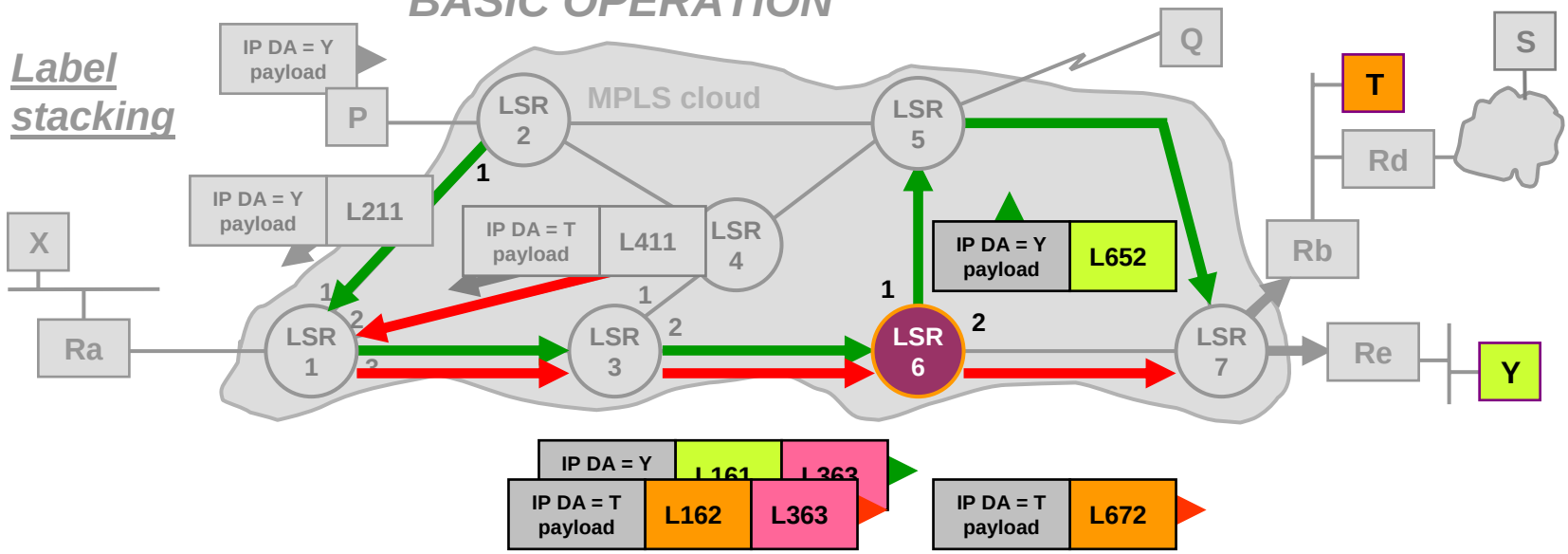
Concepts

- Ingress router adds a label
- Core routers identify the label and forward to apriori decided port (next hop)
- Egress router removes the label
- Assumptions
  - The route to be followed has been decided in an independent process that occurred before the network operation
  - Routers have bindings between specific labels and specific, apriori decided routes to be followed by packets marked with that labels

MULTIPROTOCOL LABEL SWITCHING (MPLS)

BASIC OPERATION

Label stacking



LSR6 tables

FTN (FEC-To-NHLF)	
FEC	NHLFE (Next Hop Label Forwarding Entry)
-	(-)
-	(-)

ILM (Incoming Label Map)	
label	NHLFE (Next Hop Label Forwarding Entry)
361	(1)
362	(2)
363	(3)
161	(4)
162	(5)

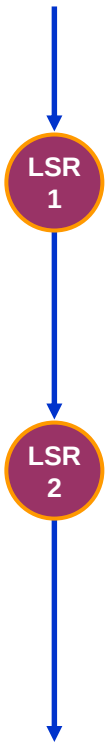
NHLF (Next Hop Label Forwarding)				
NHLFE	operation	label	next hop	physical interface
(1)	label swap	L651	LSR5	1
(2)	label swap	L671	LSR7	2
(3)	label pop	L363	-	-
(4)	label swap	L652	LSR5	1
(5)	label swap	L672	LSR7	2

MULTIPROTOCOL LABEL SWITCHING (MPLS)

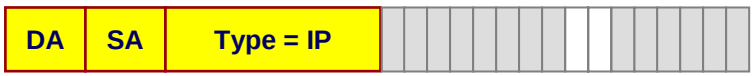
LABEL ENCODING

Identifying labeled packets

- Layer 2 header is written following the rules in effect between the sending LSR and the receiving next hop LSR
- The receiving LSR should identify the packet as a "labeled" one, as opposed to a non-labeled packet which could arrive on the same link



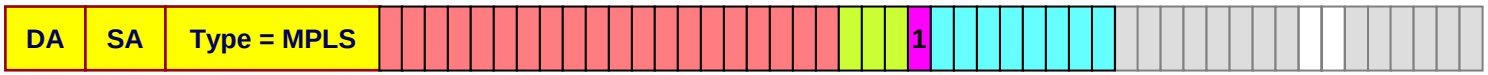
Layer 2 header Ethernet Layer 3 header IP + …



MPLS label presence is indicated by new Ethertypes
- hex 8847 (dec 34,887) - MPLS unicast
- hex 8848 (dec 34,888) - MPLS multicast

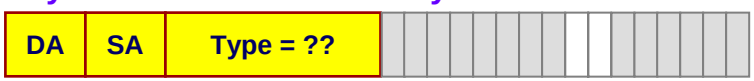
(To be used with LLC/SNAP/OUI 000000, too)

Layer 2 header Ethernet LABEL EXP S TTL Layer 3 header IP + …



After removing the last label, the packet should be processed based on its original layer 3 header, but the information related to layer 3 protocol in the original packet is lost!
LSR should be able to identify original layer 3 protocol for internal processing and for the generation of the packet to be sent to the next hop.

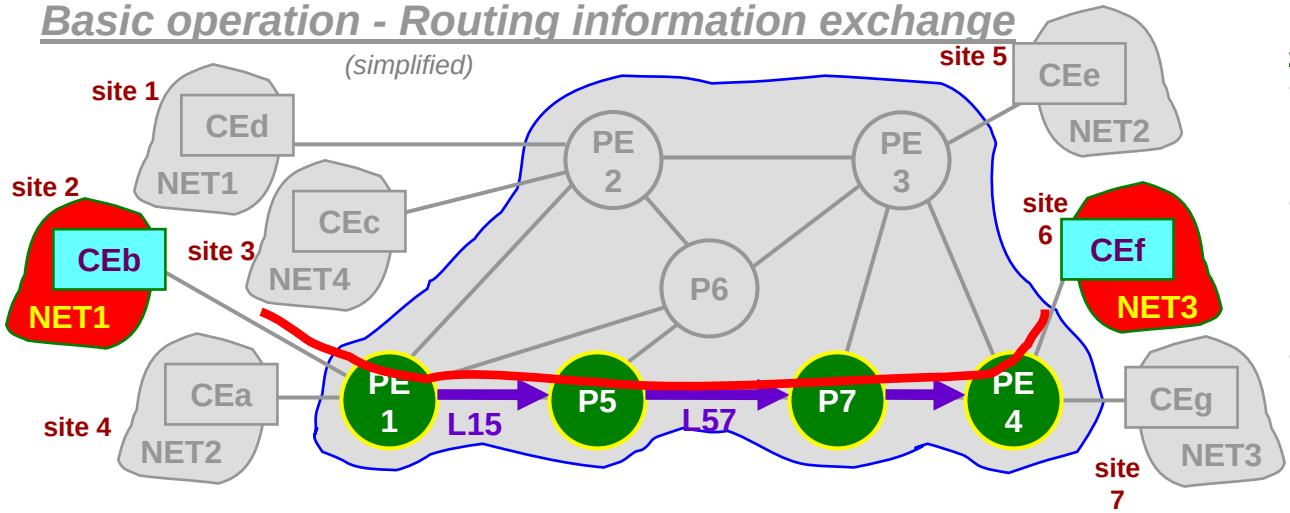
Layer 2 header Ethernet Layer 3 header ?? + …



Virtual Private Networks

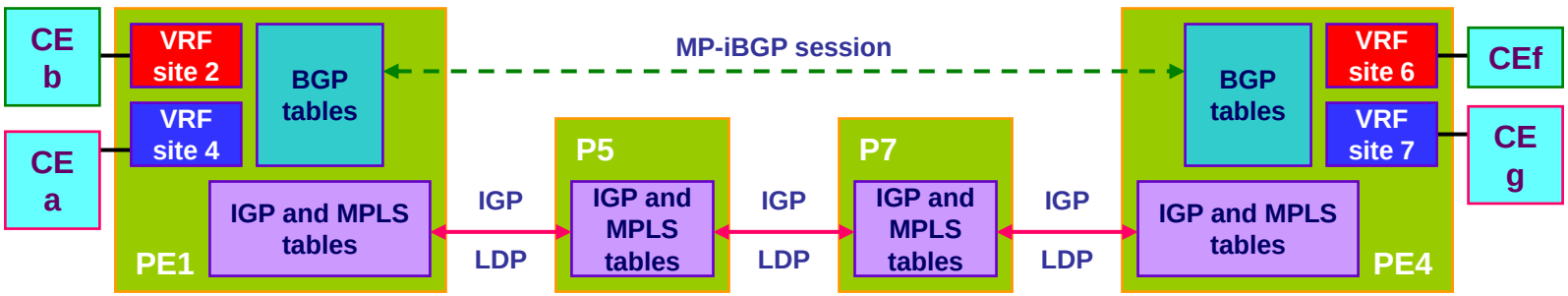
LAYER 3, BGP/MPLS based VPN

Basic operation - Routing information exchange



Step 6

- PE4 has “VRF site6” export route target “VPN RED”
- PE1 has “VRF site2” import route target “VPN RED”, so it will accept the MP-iBGP update arriving from PE4
- PE1 updates its “VRF site2” table



PE1 “VRF site2” routing table

To destination	Deliver to router	int’f
net3	PE4	FEC site6:net3 (L63)

PE1 BGP routing table

To destination	Deliver to router	int’f
site6:net3	PE4	FEC site6:net3 (L63)

PE1 IGP routing table

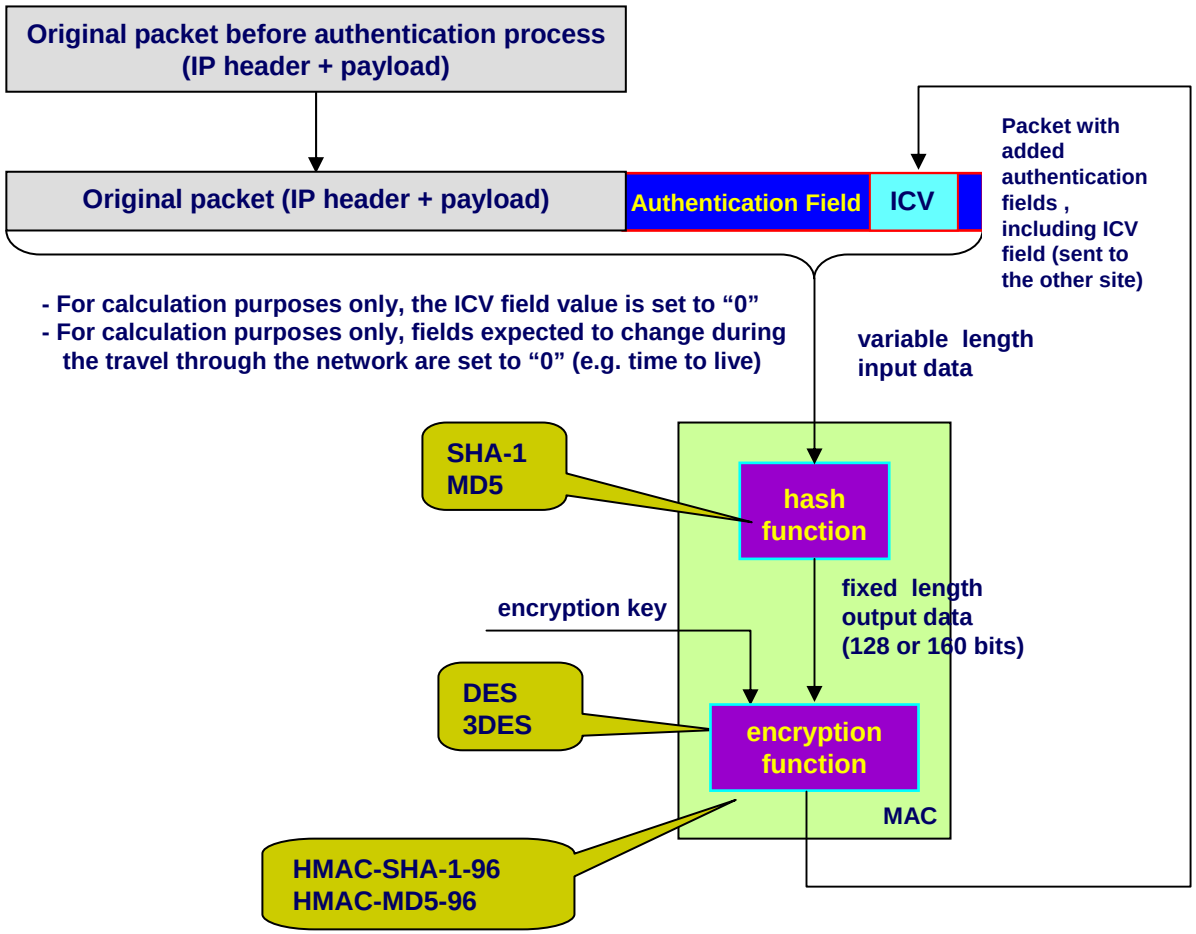
To destination	Deliver to router	physical interface	nr of hops
PE4	PE4	FEC a / L15	0

Virtual Private Networks

IP Sec based VPN

Authentication and Integrity Check principles

Generating and Using the ICV - Transmission process



ICV (Integrity Check Value) is the result of two consecutive processes executed over the packet to be protected:

- step 1 - A hash value is calculated for the packet to be protected. The hash function is not a secret.

- step 2 - The hash value obtained in step 1 is encrypted using a secret key, generating the ICV value to be added to the packet.

The encrypted hash value (the MAC) can be correctly decoded ONLY by the SAME secret key, at reception side.