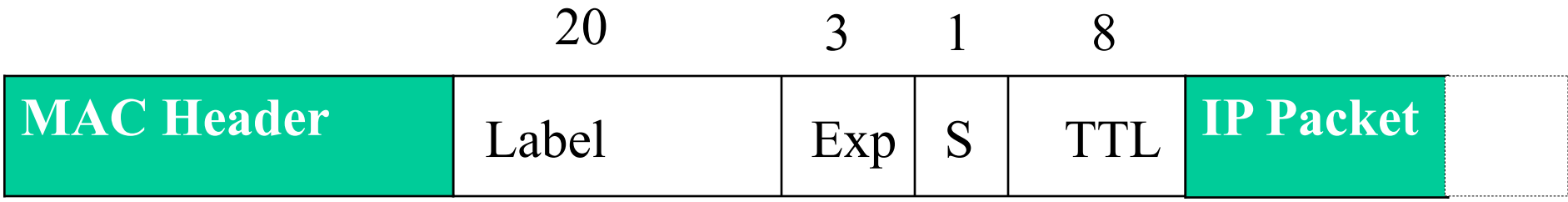
Multi-Protocol Label Switching (MPLS)

MPLS Overview

- A forwarding scheme designed to speed up IP packet forwarding (RFC 3031)
- Idea: use a fixed length label in the packet header to decide packet forwarding
  - Label carried in an MPLS header between the link layer header and network layer header
- Support any network layer protocol and link layer protocol

MPLS Header Format

- Label: 20-bit label value
- Exp: experimental use
  - Can indicate class of service
- S: bottom of stack indicator
  - 1 for the bottom label, 0 otherwise
- TTL: time to live



Forwarding Equivalence Class

- An MPLS capable router is called a *label switching router (LSR)*
- Forwarding Equivalence Class (FEC): A subset of packets that are all treated the same way by an LSR
- A packet is assigned to an FEC at the ingress of an MPLS domain

Forwarding Equivalence Class

- A packet's FEC can be determined by one or more of the following:
  - Source and/or destination IP address
  - Source and/or destination port number
  - Protocol ID
  - Differentiated services code point
  - Incoming interface
- A particular PHB (scheduling and discard policy) can be defined for a given FEC

MPLS Operation

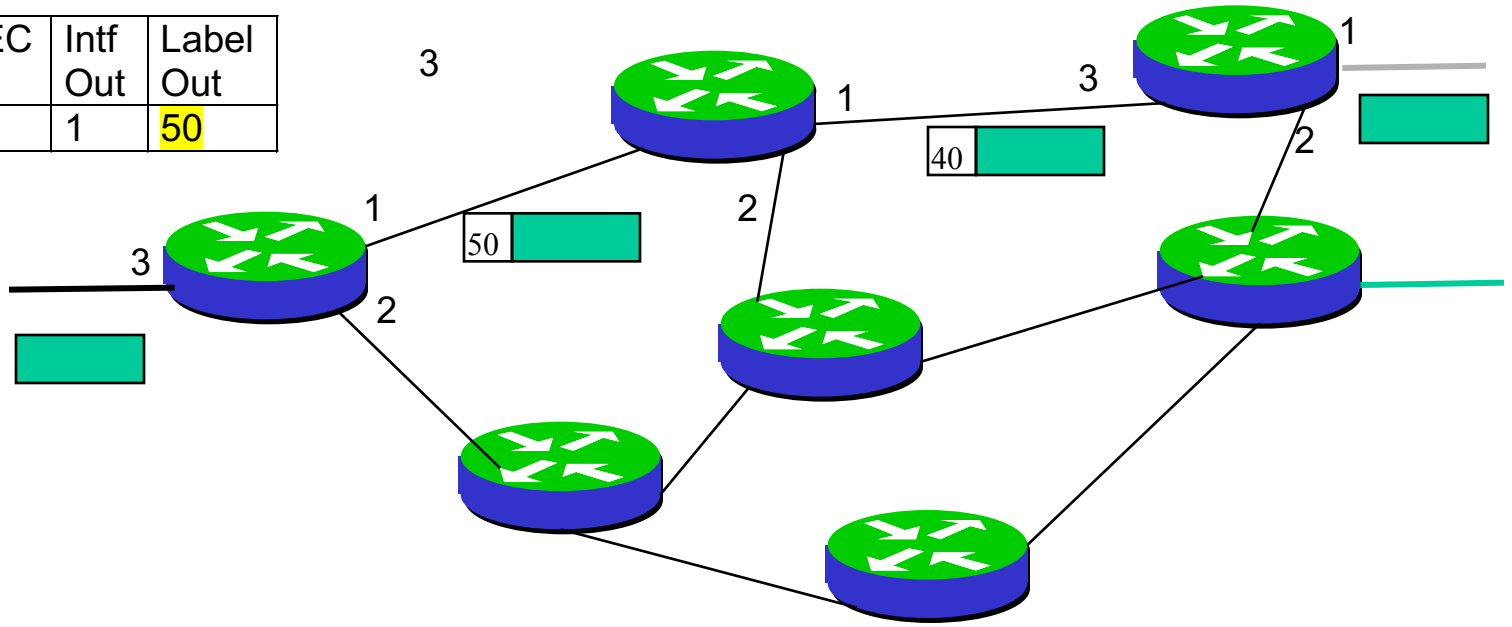
- At ingress LSR of an MPLS domain, an MPLS header is inserted to a packet before the packet is forwarded
  - Label in the MPLS header encodes the packet's FEC
- At subsequent LSRs
  - The label is used as an index into a forwarding table that specifies the next hop and a new label.
  - The old label is replaced with the new label, and the packet is forwarded to the next hop.
- Egress LSR strips the label and forwards the packet to final destination based on the IP packet header

MPLS Operation

Intf In	Label In	Intf Out	Label Out
3	50	1	40

Intf In	Label In	Intf Out
3	40	1

FEC	Intf Out	Label Out
a	1	50



Label Switched Path

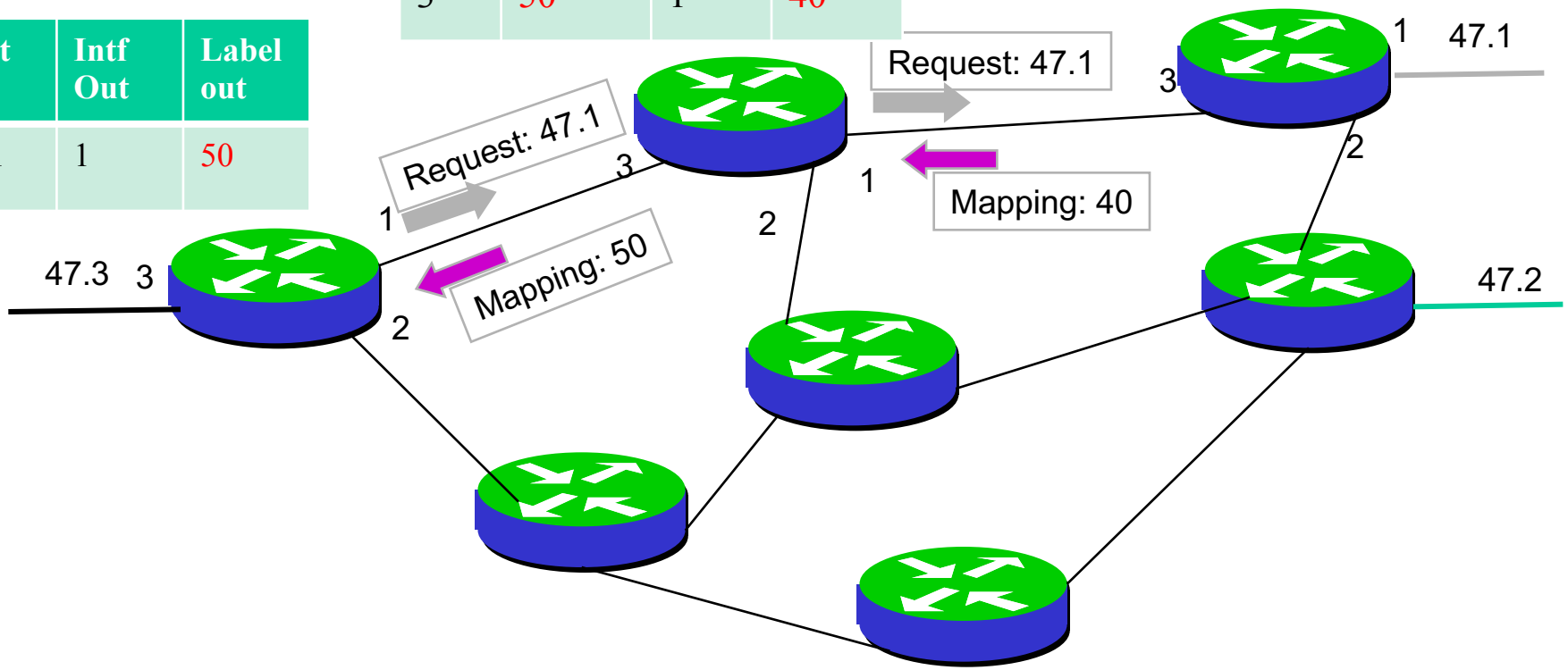
- For each FEC, a specific path called *Label Switched Path (LSP)* is assigned
  - The LSP is unidirectional
- To set up an LSP, each LSR must
  - Assign an incoming label to the LSP for the corresponding FEC
    - Labels have only local significance
  - Inform the upstream node of the assigned label
  - Learn the label that the downstream node has assigned to the LSP
- Need a label distribution protocol so that an LSR can inform others of the label/FEC bindings it has made
- A forwarding table is constructed as the result of label distribution.

Label Distribution

Intf In	Label In	Intf Out	Label Out
3	50	1	40

Intf In	Label In	Intf Out
3	40	1

Dest	Intf Out	Label out
47.1	1	50



LSP Route Selection

- Hop-by-hop routing: use the route determined by the dynamic routing protocol
- Explicit routing (ER): the sender LSR can specify an *explicit route* for the LSP
  - Explicit route can be selected ahead of time or dynamically

Explicitly Routed LSP

- Advantages
  - Can establish LSP's based on policy, QoS, etc.
  - Can have pre-established LSP's that can be used in case of failures.
- Signaling protocols
  - CR-LDP
  - RSVP-TE

Diffserv-Aware MPLS

- MPLS can be used together with Differentiated Services to provide QoS.
- LSPs are configured between each ingress-egress pair.
  - For each ingress-egress pair, a separate LSP can be created for each traffic class, or
  - Can create a single LSP for each ingress-egress pair and use the Exp bits to differentiate packet classes.
- Scalable: as the number of flows increases, the number of LSPs does not increase.

Diffserv-Aware MPLS

- Operations of routers in an ISP network
  - At the ingress router, in addition to policing, a MPLS header is inserted into the packet.
  - Core routers process the packets based on the label and Exp fields
  - At the egress router, the MPLS header is removed.
- Whether a ISP's architecture is DS field-based or MPLS-based is transparent to other ISPs

  ➔ The DS field based architecture and the MPLS based architecture can easily inter-operate.

Diffserv-Aware MPLS

- A customer domain still needs a BB to
  - Allocate services
  - Request for resources on behalf of the customer domain when the SLA is dynamic.
- BBs may not be needed in the MPLS-based ISP networks
  - Ingress router can make the admission control decision
  - If the resource request is granted, ingress router sends a PATH message to egress router through a LSP

Why MPLS Protection?

- IP restoration is very slow
  - OSPF, RIP, etc. require a redistribution of updated link status information in response to a failure.
  - Routing table convergence time on the order of seconds.
  - Looping and packet loss can occur during convergence
- MPLS enables fast failure restoration

MPLS Protection Approaches

- End-to-End protection
  - A backup LSP is set up in advance from the source LSR to the destination LSR of the primary LSP.
    - The backup LSP is link and node disjoint with the primary LSP
    - Need reserve resources for the backup LSP
  - Source LSR responsible for restoration➔sender must be notified of the failure

MPLS Protection Approaches

- Local protection
  - When establishing a primary LSP, a backup LSP for each possible link or node failure is set up
    - Resources reserved for each backup LSP
  - Failure detecting LSR responsible for switching traffic to the backup LSR
  - Faster restoration than end-to-end protection

Local Protection

- Problem: must create a separate set of backup LSPs for every primary LSP
- Can a single LSP backup a set of primary LSPs?
- Yes! Use MPLS label stacking.

Label Stacking

- A packet may carry multiple labels, organized as a last-in-first-out stack
- A label may be added to/removed from the stack at any LSR
- Processing always done on the top label
- Allow the aggregation of LSPs into a single LSP for a portion of the route, creating a tunnel
  - At the beginning of the tunnel, the LSR assigns the same label to packets from different LSPs by pushing the label onto each packet's stack
  - At the end of the tunnel, the LSR pops the top label

Local Protection Using Label Stacking

- Bypass tunnel: a LSP used to protect a set of LSPs passing over a common facility.
- Label stacking allows different primary LSPs to use the same bypass tunnel for failure protection.

Local Protection Using Label Stacking

When a failure occurs:

- LSR at the beginning of the tunnel will
  - Switch packets received on the protected LSP x onto the bypass tunnel
  - Replace the old label with a new label that will be understood by the last node in the bypass tunnel to indicate LSP x
  - Push the bypass tunnel's label onto the label-stack of the redirected packets.
- LSR at the end of the tunnel will
  - Pop the bypass tunnel's label
  - Examine the top label to determine the protected LSP that the packet is to follow.

Summary of MPLS

- Simplify packet forwarding based on a fixed length label
- Enable explicit routing in IP networks
  - Can be used for traffic management, QoS routing
- Enable fast restoration from failures.