Segment Routing with IPv6

Segment Routing Header (SRH)

Eric Vyncke (evyncke@cisco.com)
Distinguished Engineer – Cisco Systems

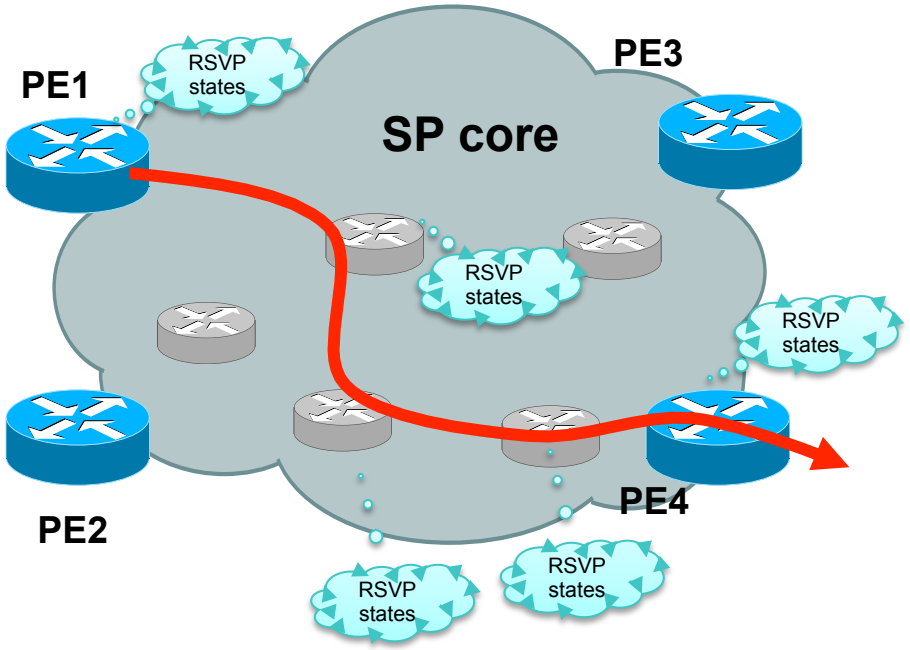
June, 2014

Where is the Internet ?

http://www.google.com/intl/en/ipv6/statistics.html

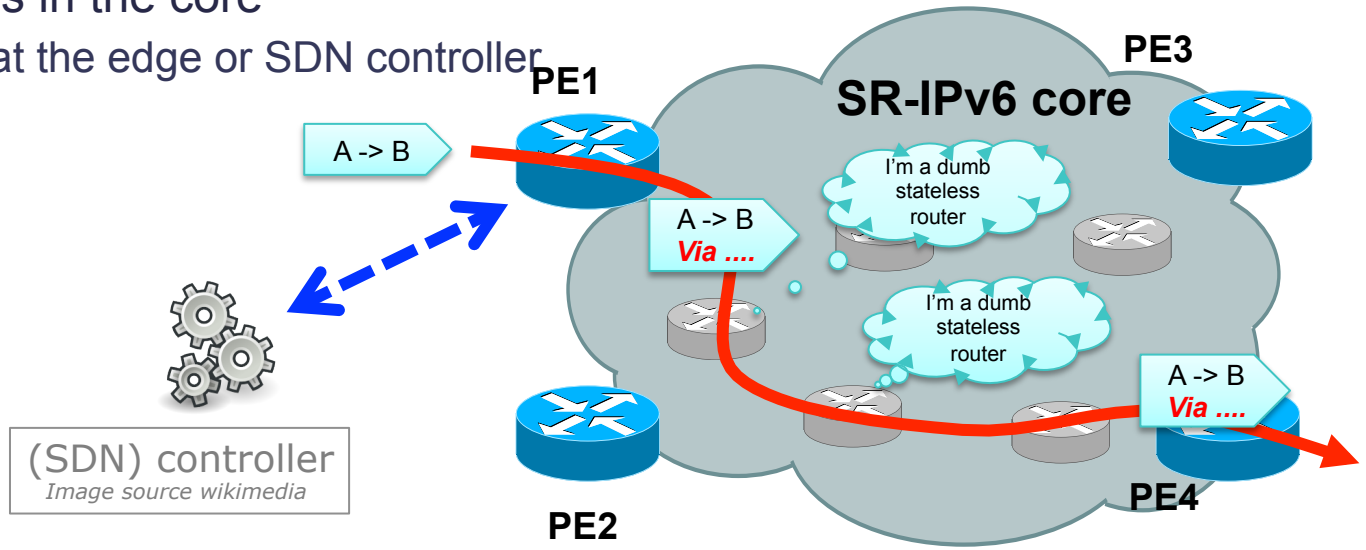
Where is Traffic Engineering (TE) ?

- TE requires RSVP to install states in every the core routers
  - => ‘low’ convergence
  - => TE not widely deployed



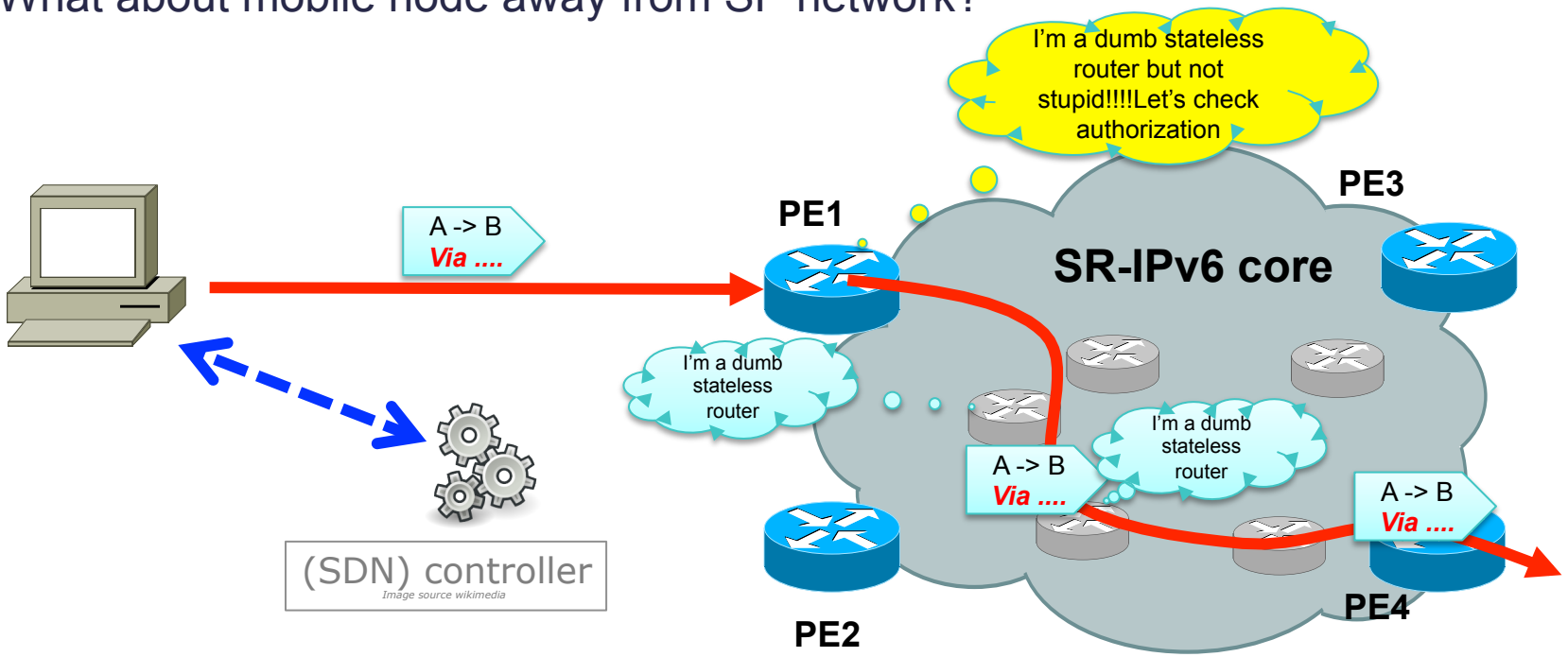
What Can We Do for Efficient/Flexible TE?

- Leverage IPv6 flexibility
  - Overload routing header, i.e. install states in the data packet
- Remove states in the core
  - Push states at the edge or SDN controller



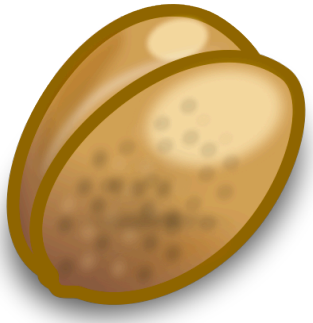
“Extreme Traffic Engineering” from CPE/Set-up Box?

- What about mobile node away from SP network?



Segment Routing in a Nutshell

- Segment Routing:
  - **Source based routing model** where the source chooses a path and encodes it in the packet header as an ordered list of segments
    > Removes routing states from any node other than the source
  - A segment is an instruction applied to the packet.
  - Segment Routing leverages the source routing architecture defined in RFC2460 for IPv6



Source: wikimedia

Segment Routing and the Source Based Routing Model

- Segment Routing technology is extensively explained in
  - http://www.segment-routing.net (includes all published IETF drafts)
- Segment Routing data-planes
  - SR-MPLS: segment routing applied to MPLS data-plane
  - **SR-IPv6: segment routing applied to IPv6**
- SR-IPv6 allows Segment Routing do be deployed over non-MPLS networks and/or in areas of the network where MPLS is not present (e.g.: datacenters)
- Segment Routing backward compatibility
  - SR nodes fully interoperate with non-SR nodes
  - No need to have a full network upgrade

Segment Routing Header

- Segment Routing introduces a new Routing Header Type:
  - The Segment Routing Header (SRH)
  - Contains the list of segments the packet should traverse
  - VERY close to what already specified in RFC2460
  - Changes are introduced for:
    - > Better flexibility
    - > Addressing security concerns raised by RFC5095
- Two SR-IPv6 drafts:
  - draft-previdi-6man-segment-routing-header
  - draft-ietf-spring-ipv6-use-cases

S. Previdi, Ed.
C. Filsfils
Cisco Systems, Inc.
B. Field
Comcast
I. Leung
Rogers Communications
June 9, 2014

IPv6 Segment Routing Header (SRH)
draft-previdi-6man-segment-routing-header-01

J. Brzozowski
J. Leddy
Comcast
I. Leung
Rogers Communications
S. Previdi
M. Townsley
C. Martin
C. Filsfils
D. R. Maglione, Ed.
Cisco Systems
May 9, 2014

Source Packet Routing in Networking

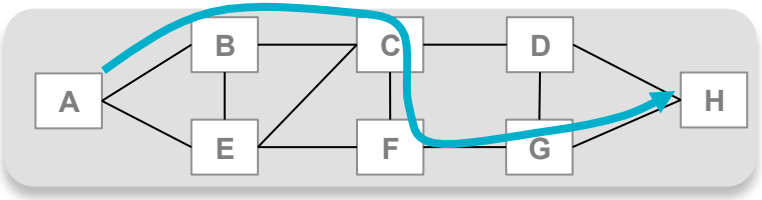
IPv6 SPRING Use Cases
draft-ietf-spring-ipv6-use-cases-00

Segment Routing Model

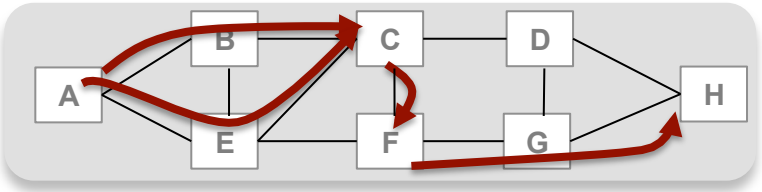
- How to express an explicit (source routed) path knowing that:
  - Nodes may represent routers, hosts, servers, application instances, services, chains of services, etc.
  - A path is encoded into the packet by the originator (or ingress) node
  - A path may be modified by a node within the path
  - The network may have plurality of nodes not all supporting Segment Routing

Segment Routing Model

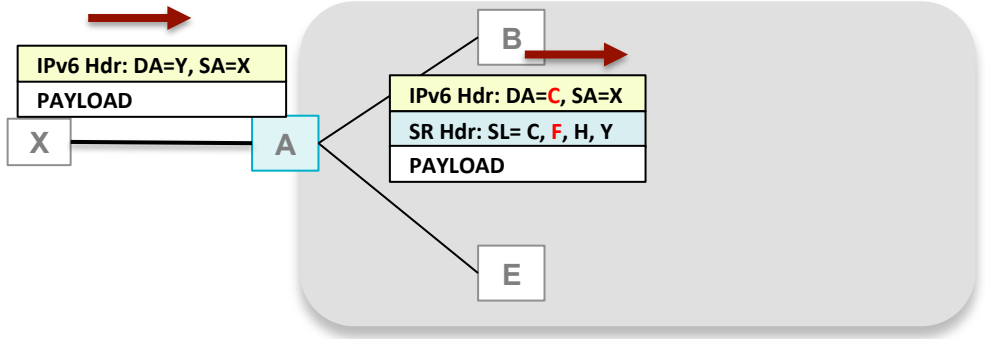
- Assuming following topology:
  - Node A has two shortest paths to C



- How to best express path: [A, B, C, F, G, H]
- Source rooted path with segments: [C,F,H]
  - First segment: set of shortest paths from A to C (ECMP aware)
  - Second segment: adjacency/link from C to F
  - Third segment: shortest path from F to H



Segment Routing Header

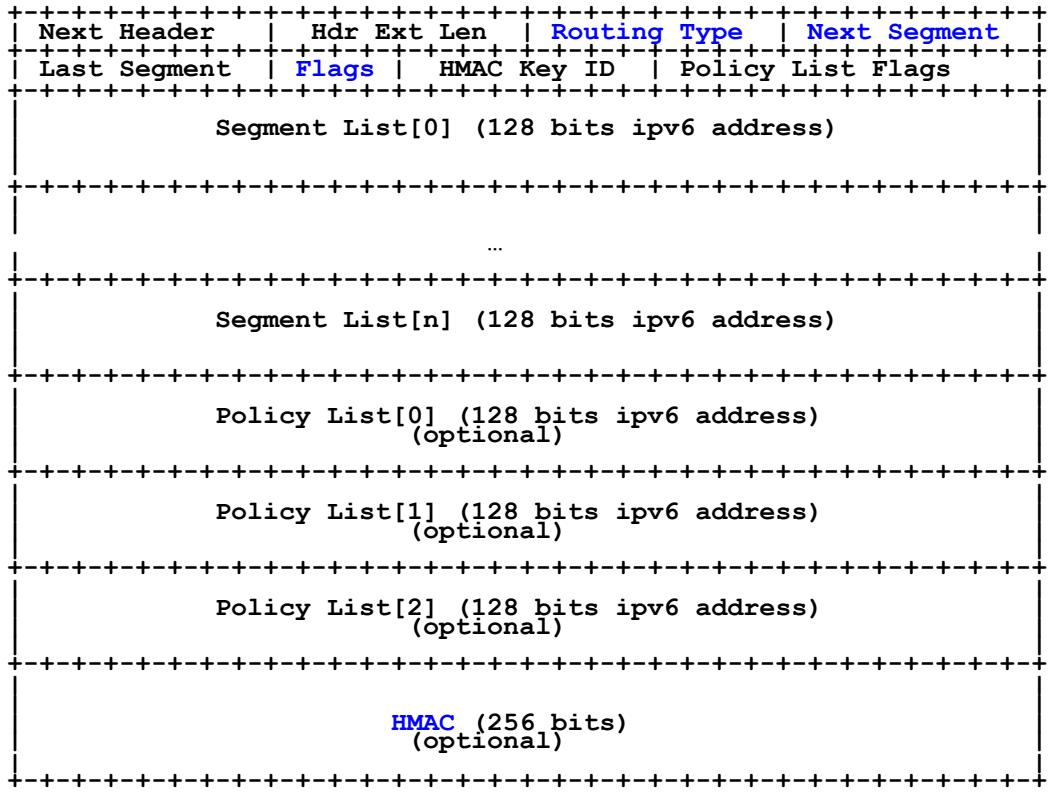


- At ingress:
  - Path is computed or received by a controller (e.g.: SDN Controller)
  - Path is instantiated through a list of segments
  - A SRH is created with the segment list representing the path

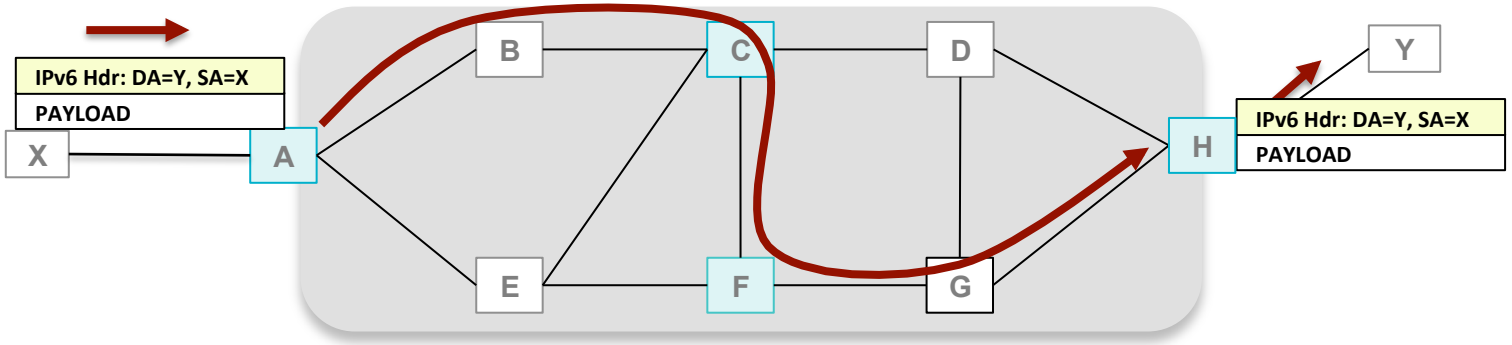
Segment Routing Header

- Segment Routing Header:
  - **Segment List** describes the path of the packet: list of segments (IPv6 addresses)
  - **Next Segment**: a pointer to the segment list element identifying the next segment
  - **HMAC**
  - **Flags** and optional policy information
- The Active Segment is set as the Destination Address (DA) of the packet
  - At each segment endpoint, the DA is updated with the “Next Segment”
  - Compliant with RFC2460 rules for the Routing Header
    > Request to IANA to allocate a new type (probably 4)

Segment Routing Header

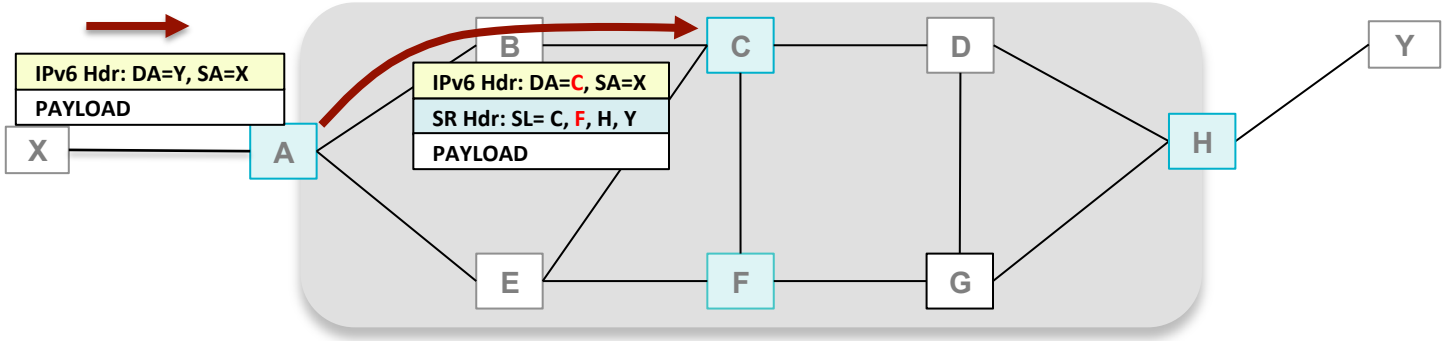


SR-IPv6 Example



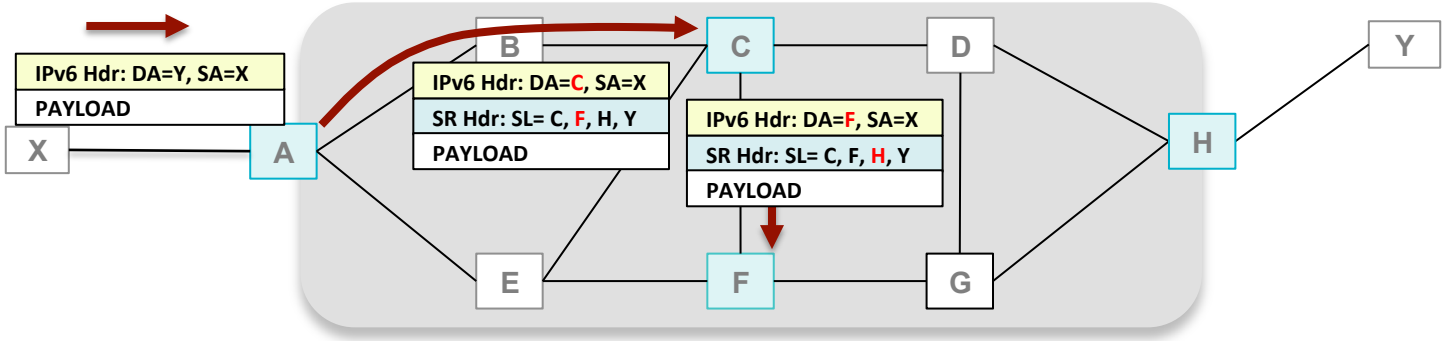
- Example:
  - Classify packets coming from X and destined to Y and forward them across A,B,C,F,G,H path
  - Nodes A, C, F and H are SR capable

SR-IPv6 Example



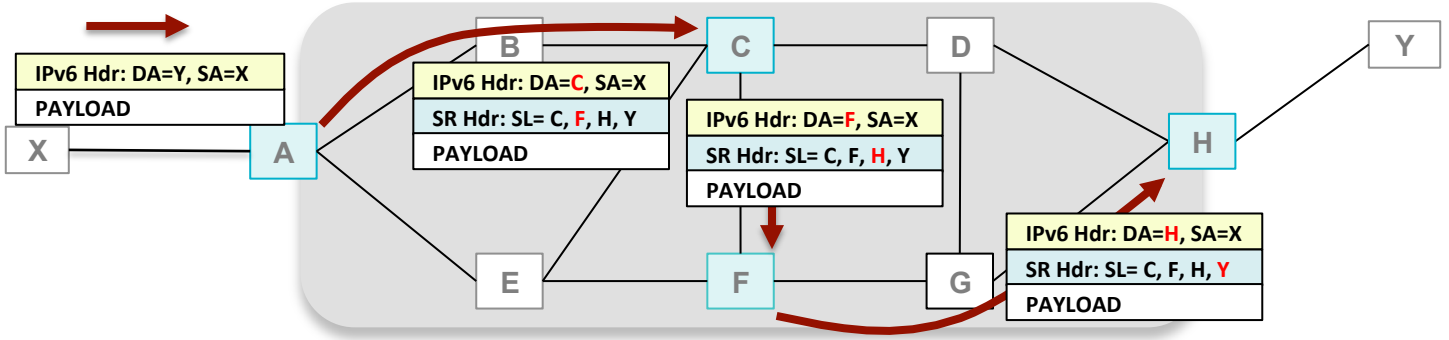
- At ingress, the Segment Routing Header (SRH) contains
  - **Segment List**: C,F,H,Y (original destination address is encoded as last segment of the path)
  - **Next Segment**: points to the next segment of the path (F)
  - **DA** is set as the address of the first segment: C
- Packet is sent towards its DA (C, representing the first segment)
  - Packet can travel across non SR nodes who will just ignore the SRH
  - RFC2460 mandates only the node in the DA must examine the SRH

SR-IPv6 Example



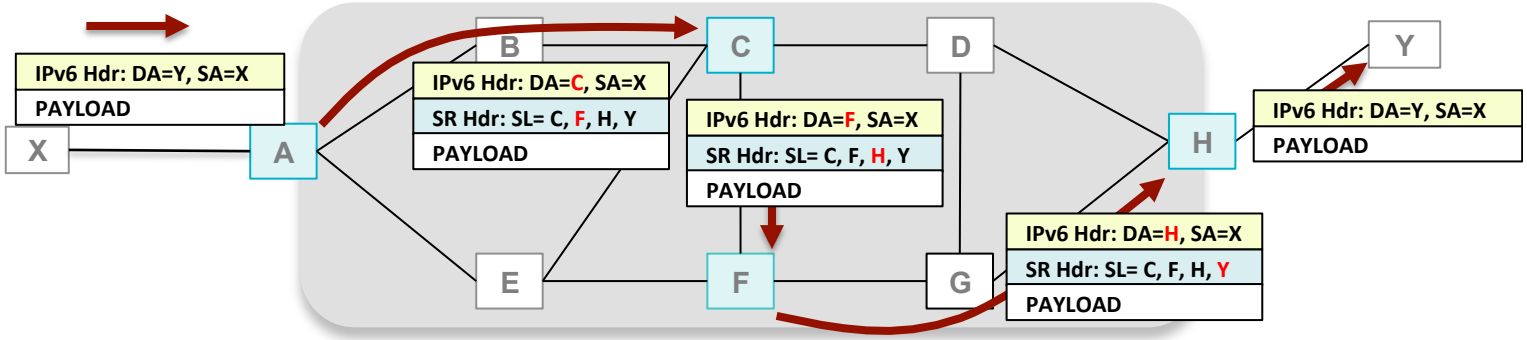
- When packet reaches the segment endpoint C
  - Next Segment is inspected and used in order to update the DA with the next segment address: F
  - Next Segment pointer is incremented: now points to H
  - Packet is sent towards its DA

SR-IPv6 Example



- When packet reaches the segment endpoint F the same process is executed:
  - Next Segment is inspected and used in order to update the DA with the next segment address: H
  - Next Segment pointer is incremented: now points to Y (the original DA)
  - Packet is sent towards its DA

SR-IPv6 Example

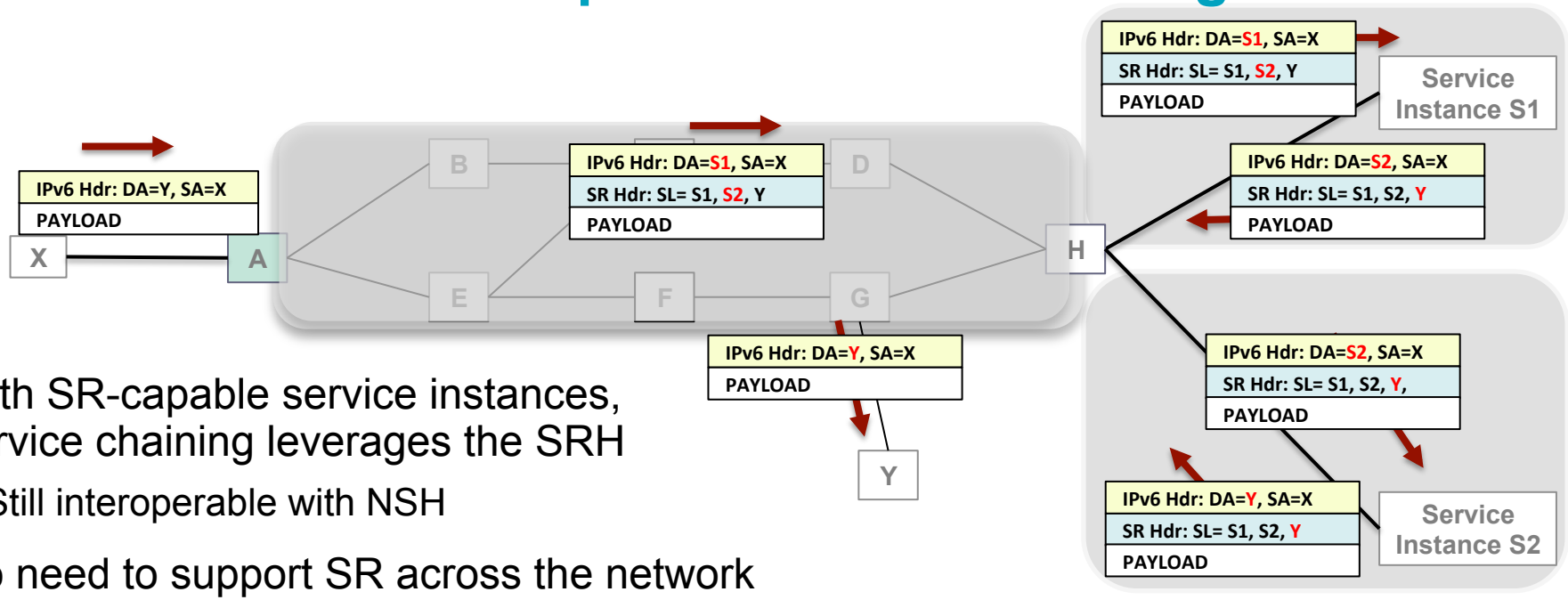


- When packet reaches the segment endpoint H:
  - Next Segment is inspected and used in order to update the DA with the next segment address: Y
  - A flag (cleanup-flag) in SRH tells H to cleanup the packet and remove the SRH
  - Packet is sent towards its DA

Segment Routing Use Cases: Fast Reroute

- Fast Reroute (FRR)
  - Upon failure, the protecting node reroute traffic according to new Segment List
  - Backup path Segment List is pre-computed and pre-instantiated
  - Upon failure, the backup Segment List is inserted

Use Cases: SR-IPv6 Capable Service Chaining



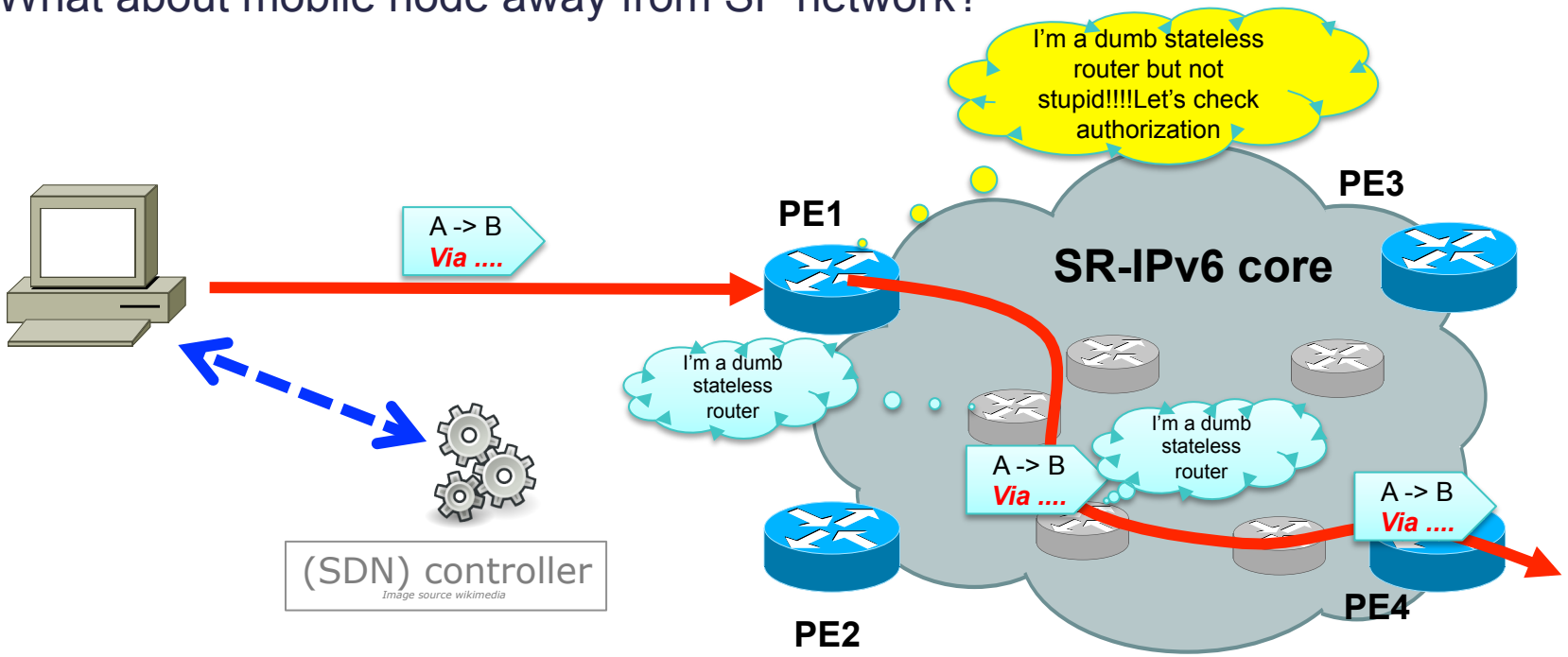
- With SR-capable service instances, service chaining leverages the SRH
  - Still interoperable with NSH
- No need to support SR across the network
  - Transparent to network infrastructure
- Next Step: allow SR service chaining with non-SR applications…
  - Work in progress

Segment Routing Use Cases: Application driven traffic steering

- Impose source-routing semantics within an application or at the edge of a network (for example, a CPE or home gateway)
- CPE gets the SRH from a controller and impose it to outgoing traffic
- SRH includes HMAC that is going to be validated at ingress **only**

“Extreme Traffic Engineering” from CPE/Set-up Box?

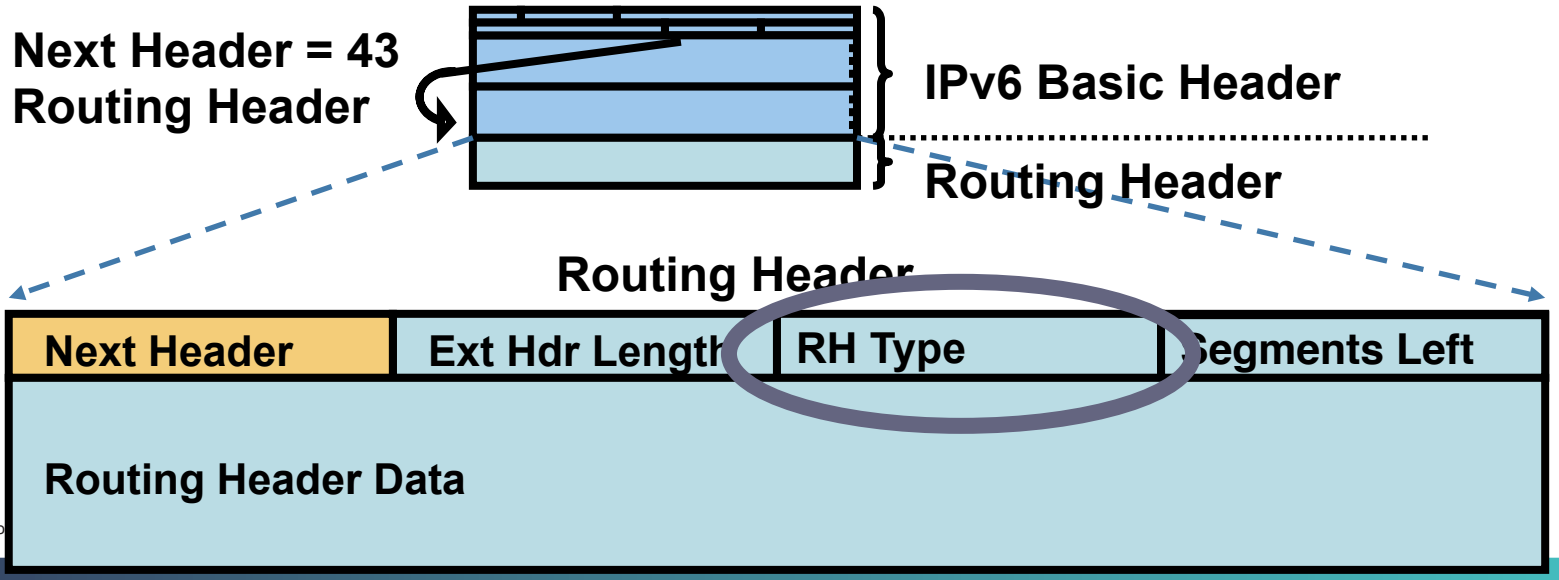
- What about mobile node away from SP network?



Huh??? Source Routing Security? What about RFC 5095?

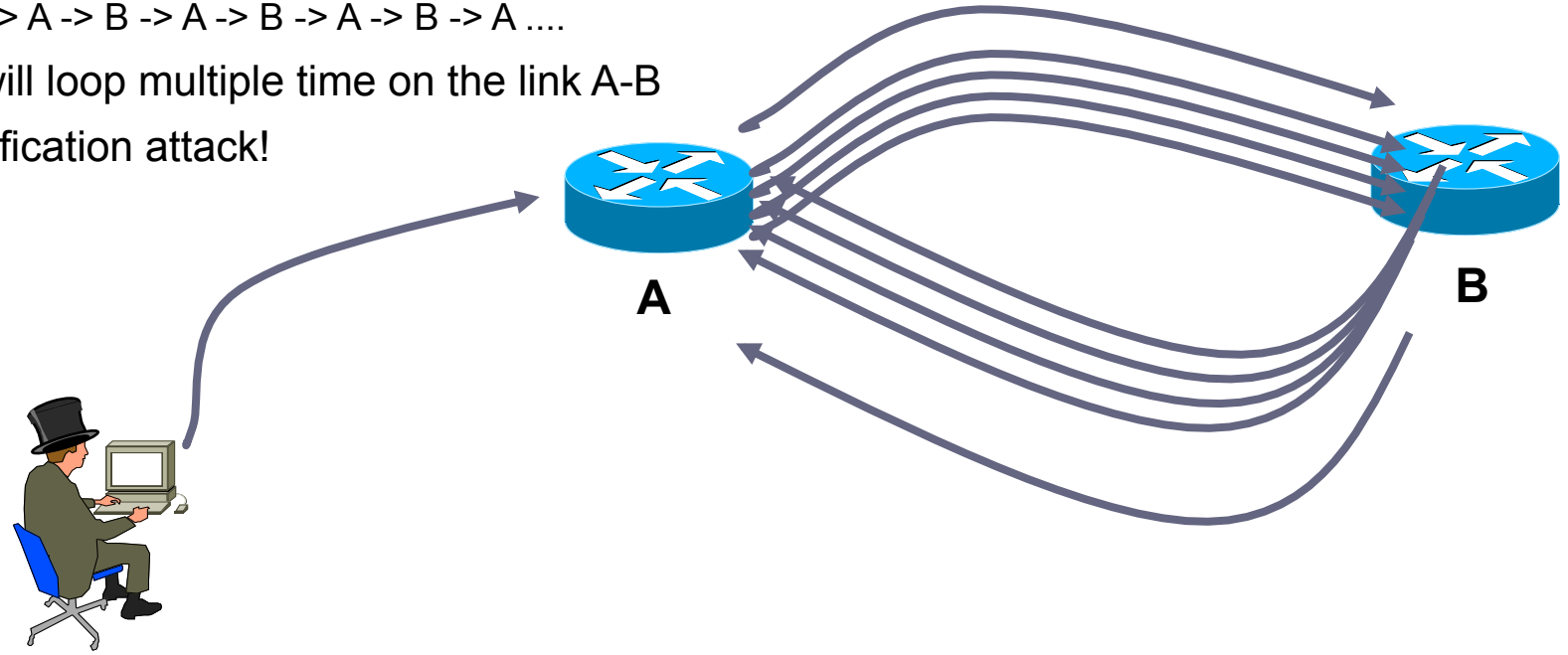
IPv6 Routing Header

- An extension header, processed by **intermediate** routers
- Three types
  - Type 0: similar to IPv4 source routing (multiple intermediate routers)
  - Type 2: used for mobile IPv6
  - Type 3: RPL (Routing Protocol for Low-Power and Lossy Networks)



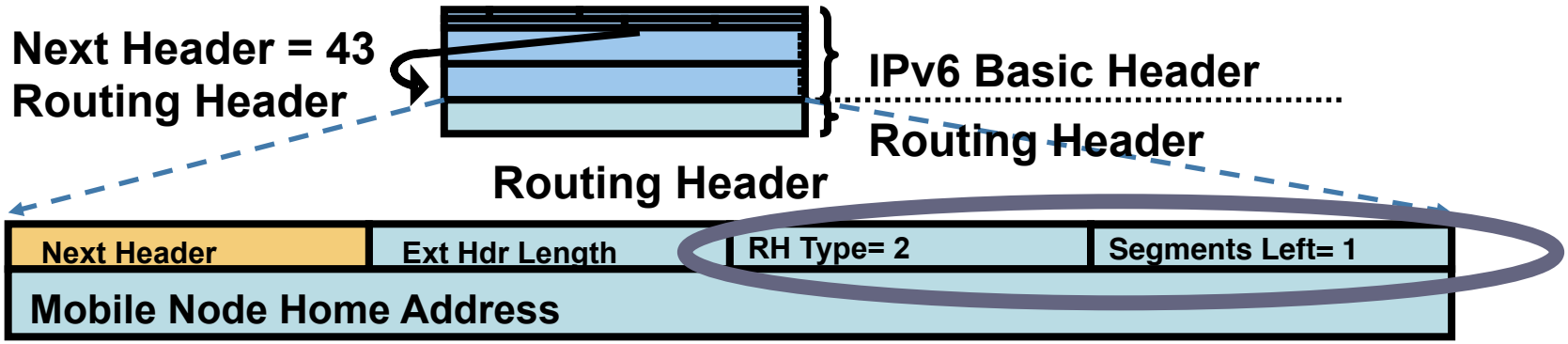
Type 0 Routing Header: Amplification Attack

- What if attacker sends a packet with RH containing
  - A -> B -> A -> B -> A -> B -> A -> B -> A ....
- Packet will loop multiple time on the link A-B
- An amplification attack!



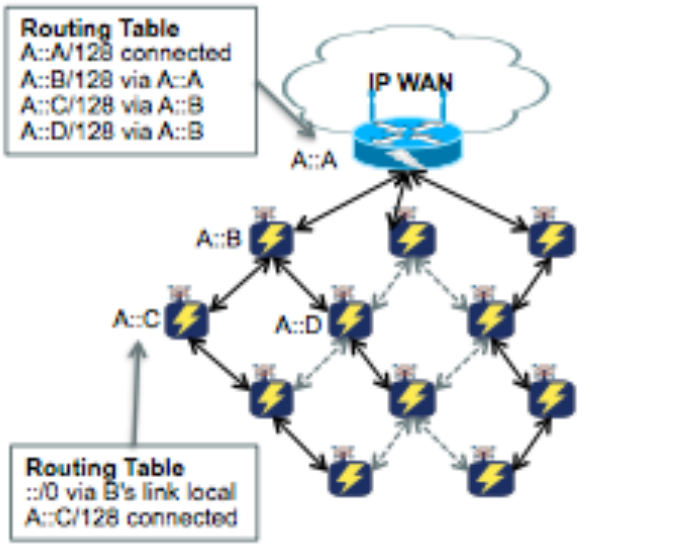
IPv6 Type 2 Routing Header: no problem

- Rebound/amplification attacks impossible
  - Only one intermediate router: the mobile node home address



RH-3 for RPL: no problem

- Used by Routing Protocol for Low-Power and Lossy Networks
- But only **within a single trusted network** (strong authentication of node), never over a public untrusted network
  - Damage is limited to this RPL network
  - If attacker was inside the RPL network, then he/she could do more damage anyway



Segment Routing Security

- Addresses concerns of RFC5095
  - HMAC field to be used at ingress of a SR domain in order to validate/authorize the SRH
  - Inside SR domain, each node trust its brothers (RPL model)

- HMAC requires a shared secret (SDN & SR ingress routers)
  - Outside of current discussions
  - Pretty much similar to BGP session security or OSPFv3 security

SRv6 packets dropped on the Internet

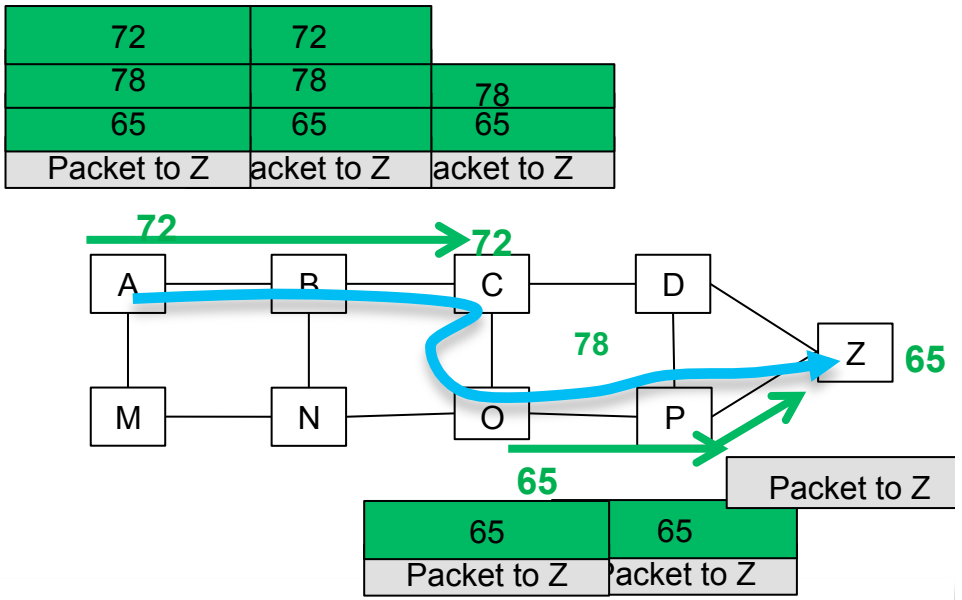
- RFC 5095 deprecates source routing
  - RH-0 only
  - Forwarding based on DA is not prevented even in presence of RH
- Some tests with scapy shows RH-4 (assuming IANA value of 4) => packets are not dropped
- Test on your own: http://www.vyncke.org/sr.php
  - And let us know !

Segment Routing for MPLS

draft-filsfils-spring-segment-routing-mpls

Combining Segments

- ECMP
  - Node segment
- Per-flow state only at head-end
  - not at midpoints
- Source Routing
  - the path state is in the packet header



Wrapping Up

Source: wikimedia

Summary

- Segment Routing implements the source routing model for both MPLS and IPv6
- IPv6 source routing model is already integrated in RC2460 and Segment Routing introduces minor changes through a new routing type header
  - Segment Routing Header
- Segment Routing is very flexible and interoperable with non-SR nodes
  - A SR node can be a router, a server, any appliance, application, …
- Segments are identified by IPv6 addresses, no specific signaling is needed

Conclusion

- Standardization of Segment Routing is in progress at IETF
  - More than 17 drafts
- Running code exists
- Next Step: Segment Routing for Service Chaining
  - More flexible, interoperable with existing applications
- Collaboration with operator on going and very fruitful
  - Join the team !
- Pointers:

  http://www.segment-routing.net

  mailto:ask-segment-routing@cisco.com

Thank you.