Routing Header Is back... Should We Panic?

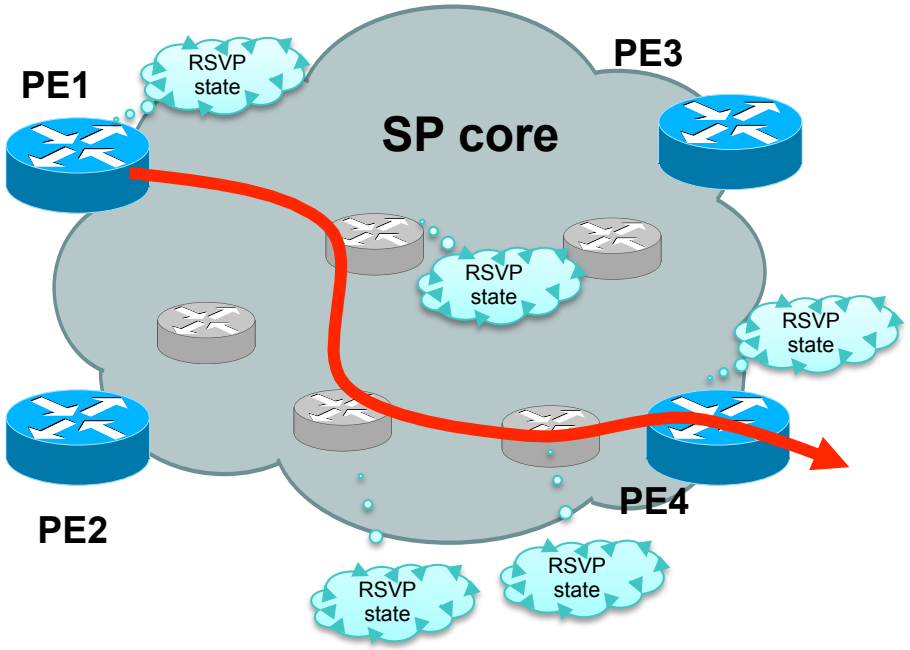
Leveraging IPv6 extension header for traffic engineering

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

March, 2015

Where is Traffic Engineering (TE) ?

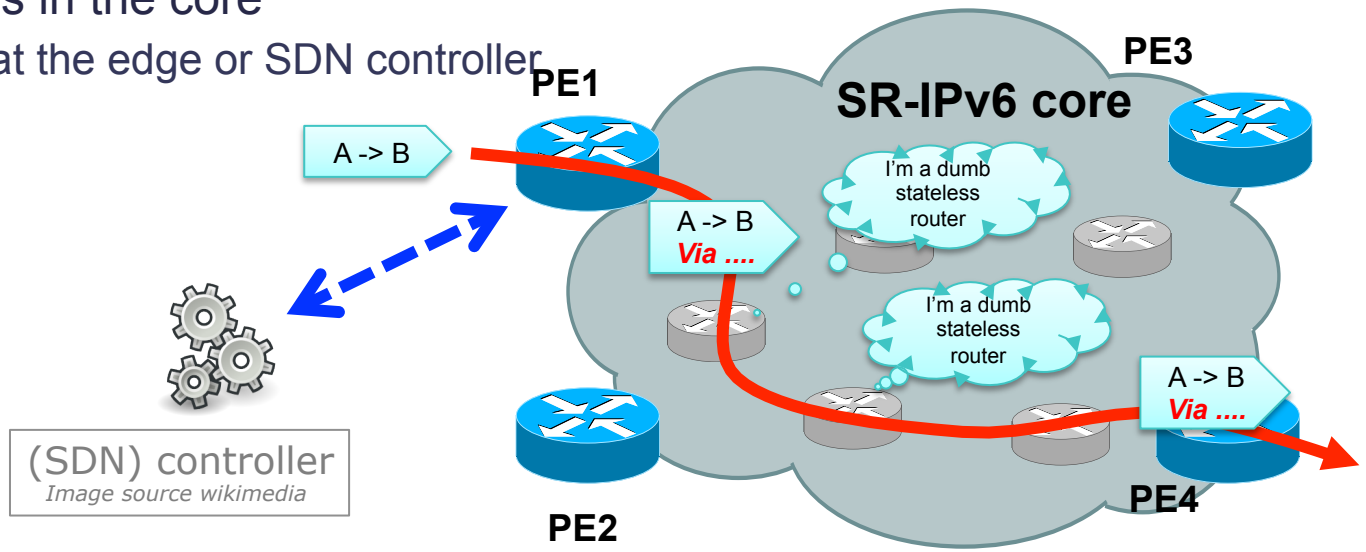
- TE requires RSVP to install state in every the core routers
  - => ‘low’ convergence
  - => TE not widely deployed



© 2015 Cisco and/or its affiliates. All rights reserved.

What Can We Do for Efficient/Flexible TE?

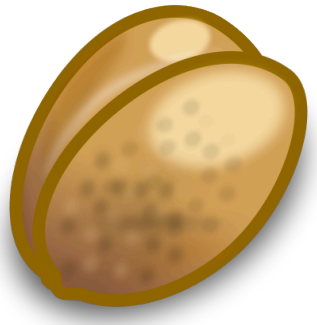
- Leverage IPv6 flexibility
  - Overload routing header, i.e. install state in the data packet
- Remove states in the core
  - Push states at the edge or SDN controller



© 2015 Cisco and/or its affiliates. All rights reserved.

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

© 2015 Cisco and/or its affiliates. All rights reserved.

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

© 2015 Cisco and/or its affiliates. All rights reserved.

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
- Three SR-IPv6 drafts:
  - draft-previdi-6man-segment-routing-header
  - **draft-vyncke-6man-segment-routing-security**
  - draft-ietf-spring-ipv6-use-cases

S. Previdi, Ed.
C. Filsfils
Cisco Systems, Inc.
B. Field
Comcast
I. Leung
Rogers Communications
January 12, 2015

IPv6 Segment Routing Header (SRH)
draft-previdi-6man-segment-routing-header-05

J. Brzozowski
J. Leddy
Comcast
I. Leung
Rogers Communications
S. Previdi
M. Townsley
C. Martin
C. Filsfils
D. R. Maglione, Ed.
Cisco Systems
November 12, 2014

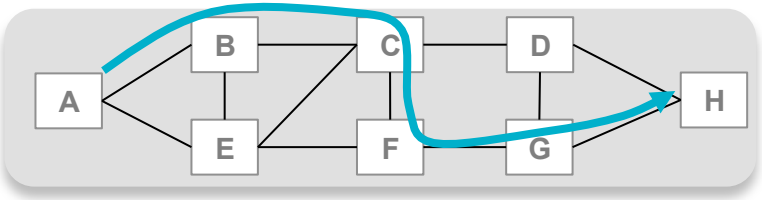
Source Packet Routing in Networking

IPv6 SPRING Use Cases
draft-ietf-spring-ipv6-use-cases-03

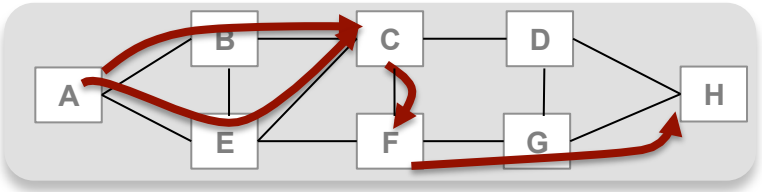
© 2015 Cisco and/or its affiliates. All rights reserved.

Segment Routing Model

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

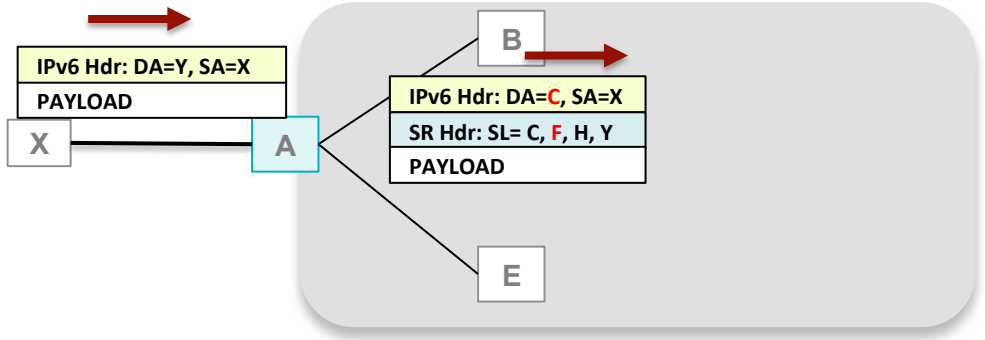


- How to best express path: [A, B, C, F, G, H]
- Source routed path with segments: [C,F,H]
  - First segment: set of shortest paths from A to C (ECMP aware)
  - Second segment: adjacency/link from C to F
  - Third segment: shortest path from F to H



© 2015 Cisco and/or its affiliates. All rights reserved.

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

© 2015 Cisco and/or its affiliates. All rights reserved.

Segment Routing for IPv6 Dataplane

- A Segment is identified through its IPv6 address
  - No mapping needed between Segment IDs (SIDs) and node's addresses
    - >As there are identical ☺
- New Routing Extensions Header type
  - Segment Routing Header (SRH)
  - Contains Segment List, Policy List, and a few other bits…

© 2015 Cisco and/or its affiliates. All rights reserved.

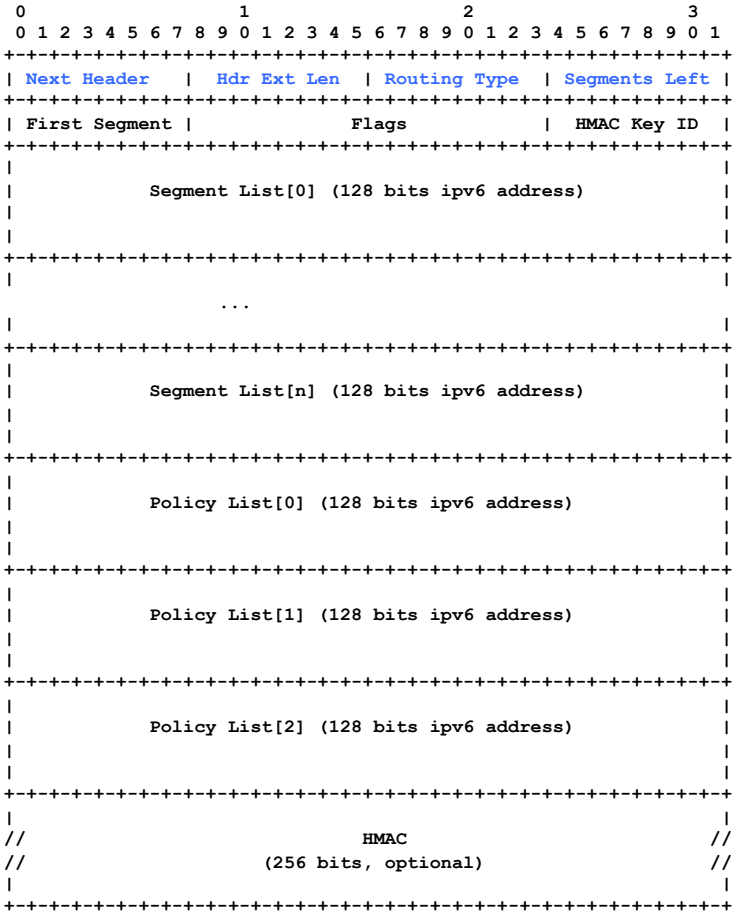
Segment Routing Header

- Segment Routing Header:
  - **Segment List** describes the path of the packet: list of segments (IPv6 addresses)
  - **First Segment**: a pointer to the segment list element identifying the first 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)

© 2015 Cisco and/or its affiliates. All rights reserved.

SRH: identical to RFC 2460

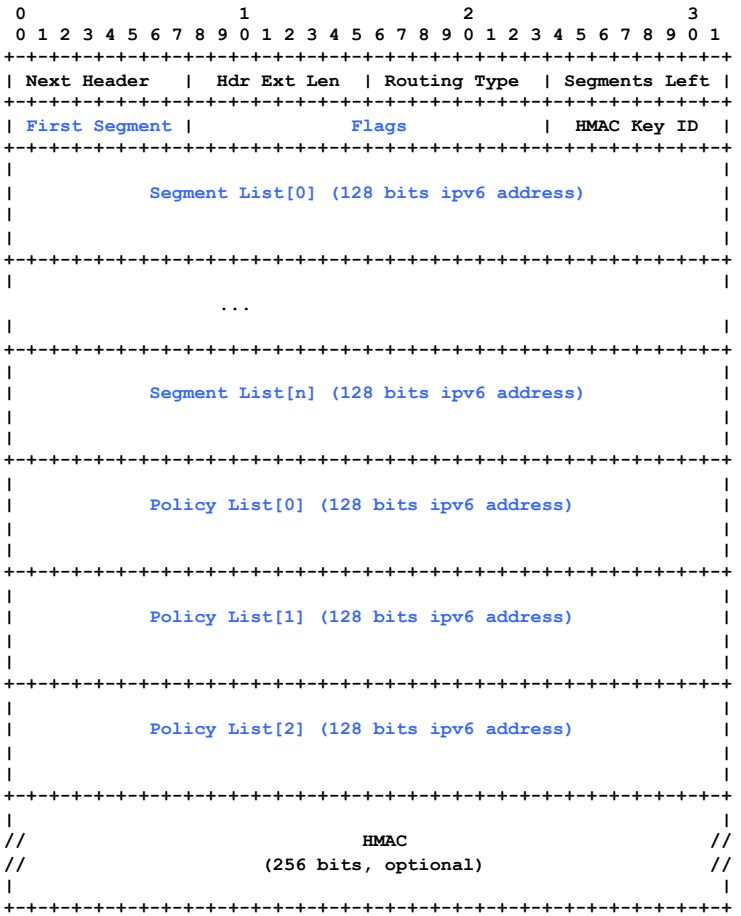
- Next Header: 8-bit selector. Identifies the type of header immediately following the SRH
- Hdr Ext Len: 8-bit unsigned integer. Defines the length of the SRH header in 8-octet units, not including the first 8 octets
- Routing Type: TBD by IANA (SRH)
- Segment Left: index, in the Segment List, of the current active segment in the SRH. Decremented at each segment endpoint.



© 2015 Cisco and/or its affiliates. All rights reserved.

SRH: New

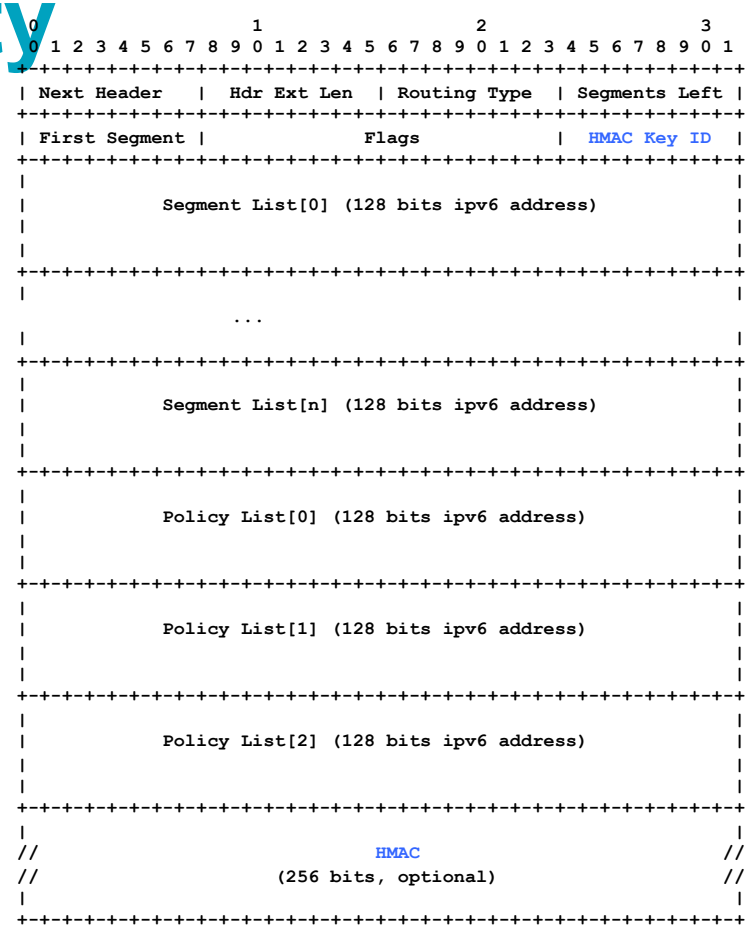
- First Segment: offset in the SRH, not including the first 8 octets and expressed in 16-octet units, pointing to the last element of the Segment List
- Flags:
  - bit-0: cleanup
  - bit-1: rerouted packet
  - bits 2 and 3: reserved
  - bits 4 to 15: policy flags
- Segment List[n]: 128 bit IPv6 addresses representing each segment of the path. The segment list is encoded in the reverse order of the path: the last segment is in the first position of the list and the first segment is in the last position
- Policy List[n] (optional): to mark ingress/ ingress SR address, to remember original source address



© 2015 Cisco and/or its affiliates. All rights reserved.

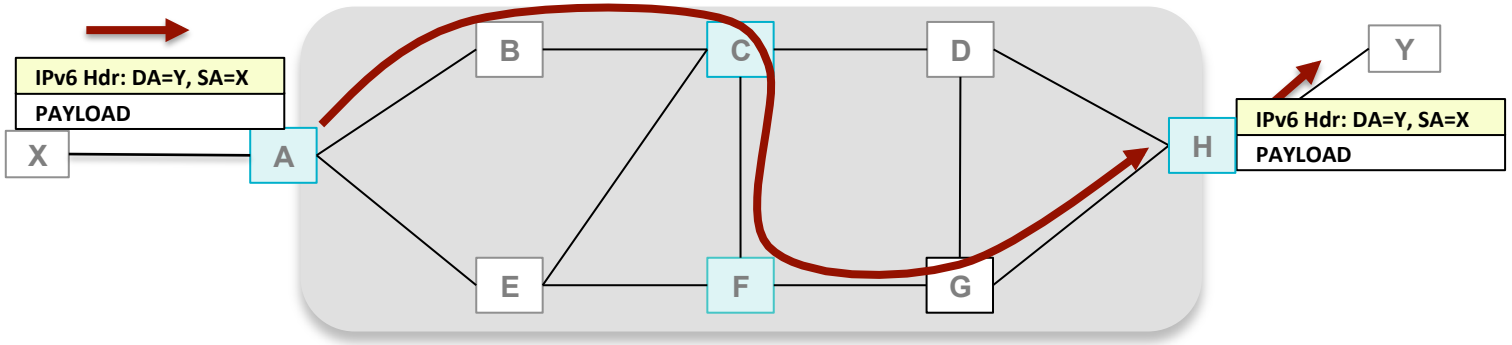
SRH: New for Security

- HMAC Key-id: identifies the shared secret used by HMAC. If 0, HMAC field is not present
- HMAC: SRH authentication (optional)



© 2015 Cisco and/or its affiliates. All rights reserved.

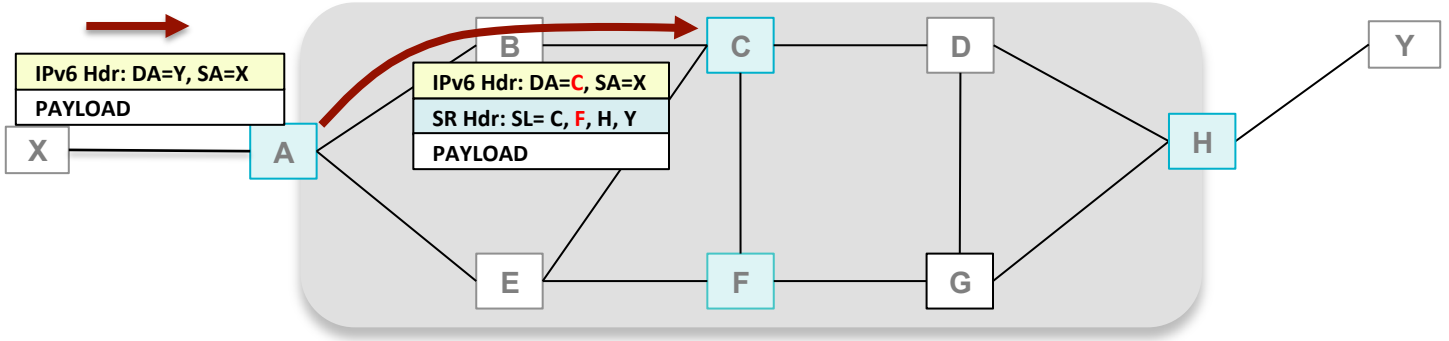
SR-IPv6 Example



- 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

© 2015 Cisco and/or its affiliates. All rights reserved.

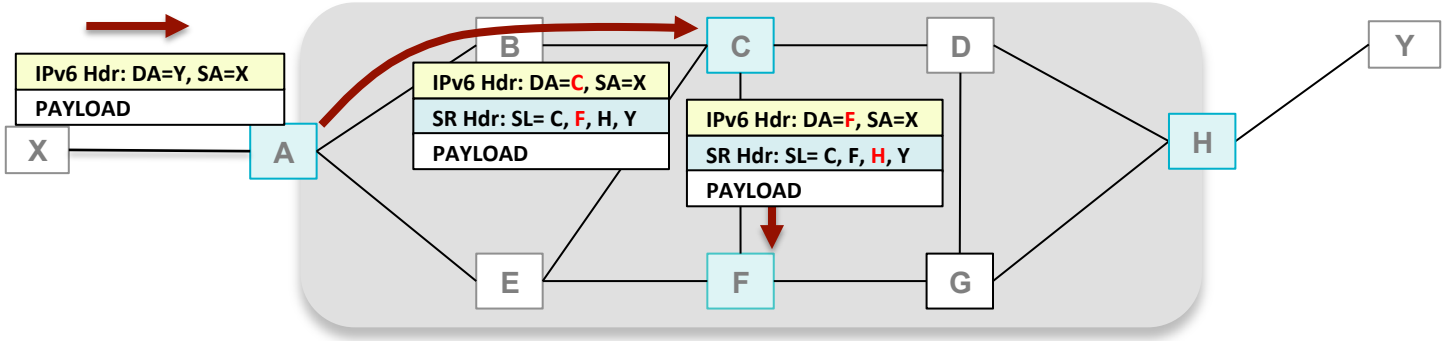
SR-IPv6 Example



- 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)
  - **Segments Left**: identities 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**

© 2015 Cisco and/or its affiliates. All rights reserved.

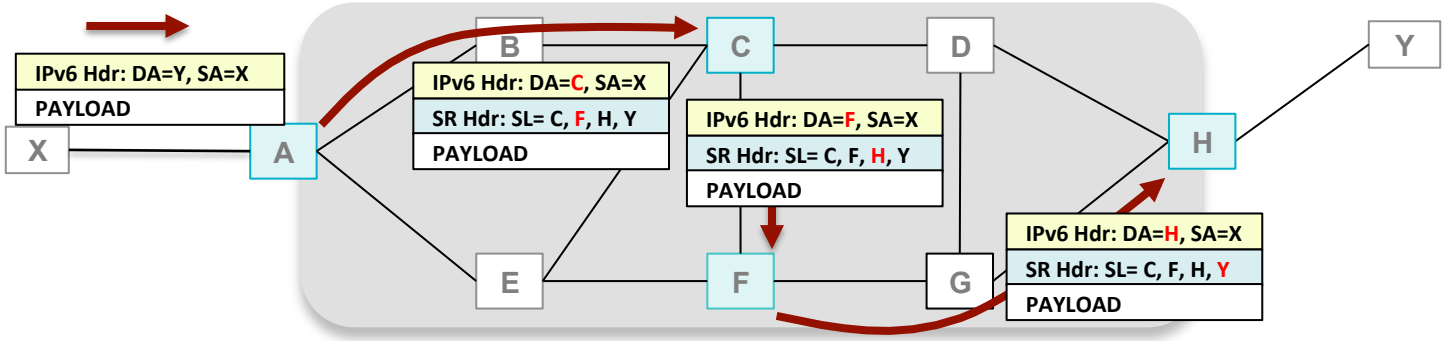
SR-IPv6 Example



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

© 2015 Cisco and/or its affiliates. All rights reserved.

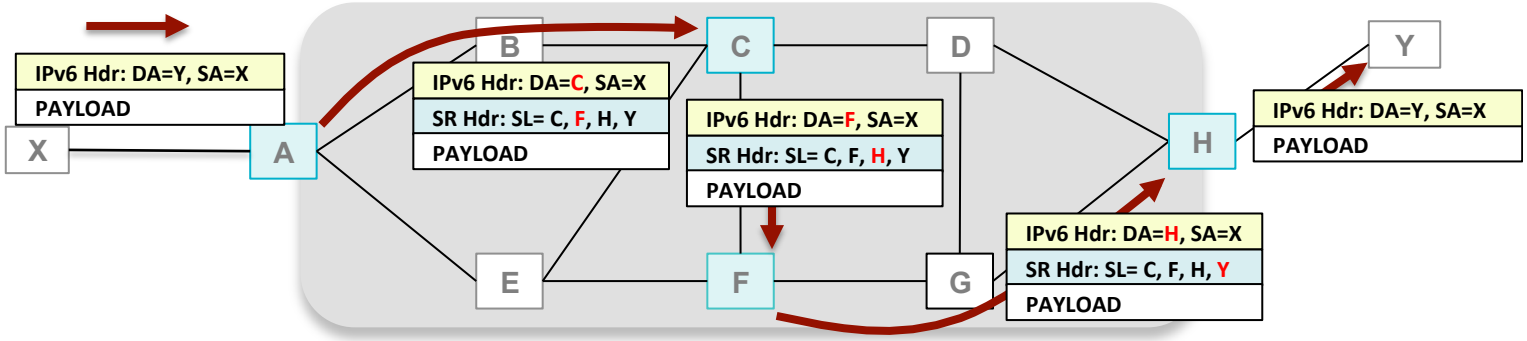
SR-IPv6 Example



- When packet reaches the segment endpoint F the same process is executed:
  - Segment Left is inspected and used in order to update the DA with the next segment address: H
  - Segment Left is decremented: indicated next as Y (the original DA)
  - Packet is sent towards its DA

© 2015 Cisco and/or its affiliates. All rights reserved.

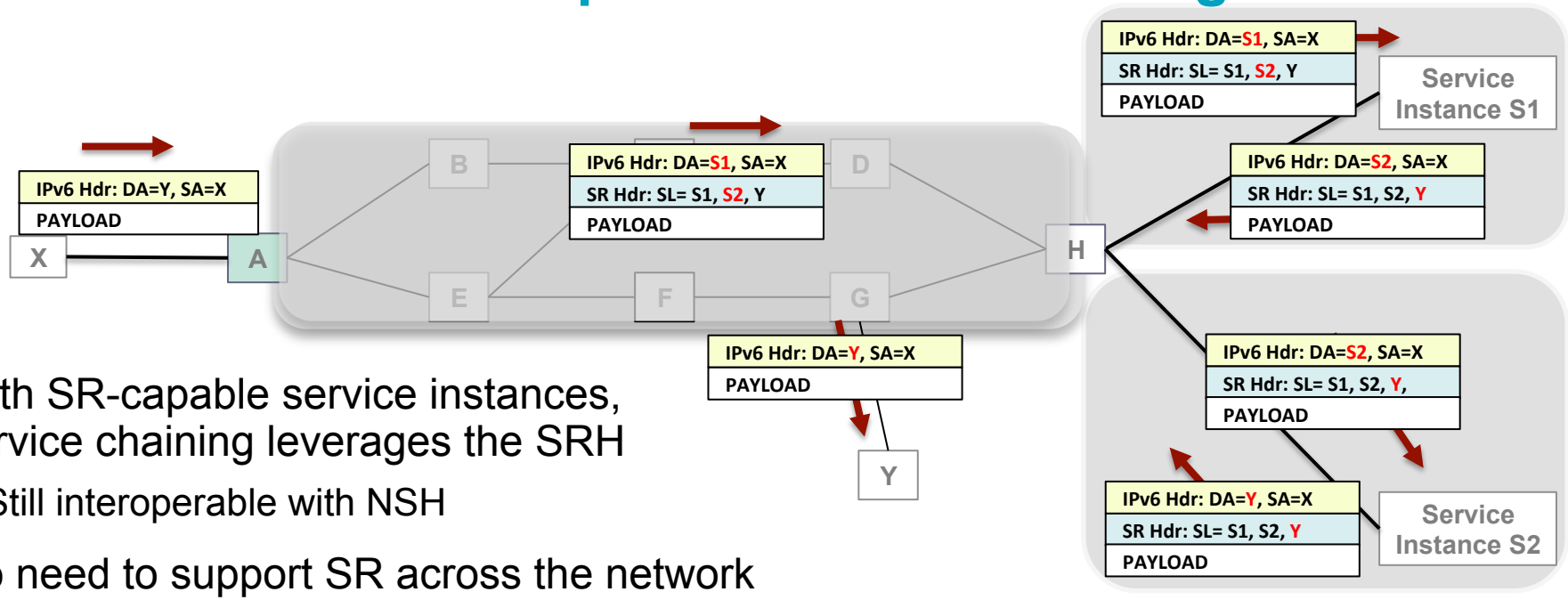
SR-IPv6 Example



- When packet reaches the segment endpoint H:
  - Segment Left is inspected (== 0) and used in order to update the DA with the next segment address: Y
  - An optional flag (cleanup-flag) in SRH tells H to cleanup the packet and remove the SRH
  - Packet is sent towards its DA

© 2015 Cisco and/or its affiliates. All rights reserved.

Use Cases: SR-IPv6 Capable Service Chaining

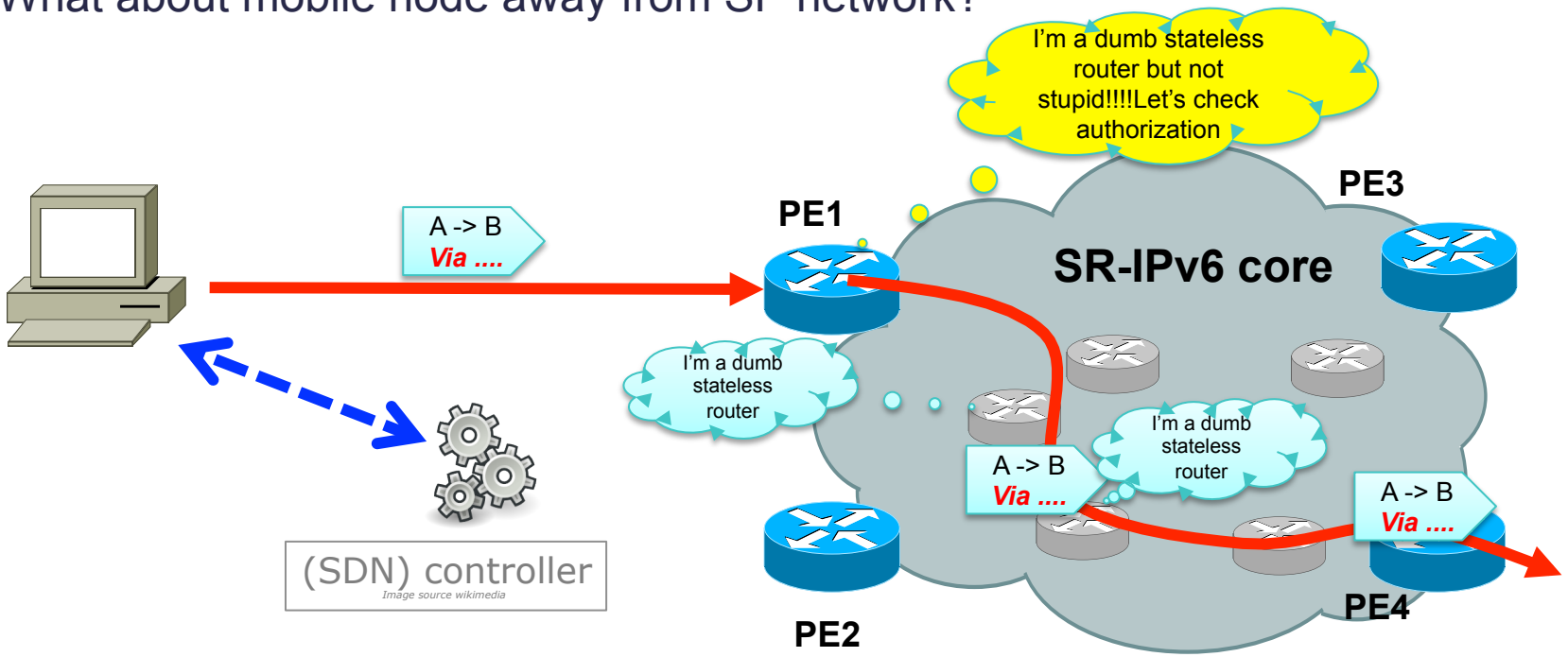


- With SR-capable service instances, service chaining leverages the SRH
  - Still interoperable with NSH
- No need to support SR across the network
  - Transparent to network infrastructure
- Next Step: allow SR service chaining with non-SR applications…
  - Work in progress

© 2015 Cisco and/or its affiliates. All rights reserved.

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

- What about mobile node away from SP network?



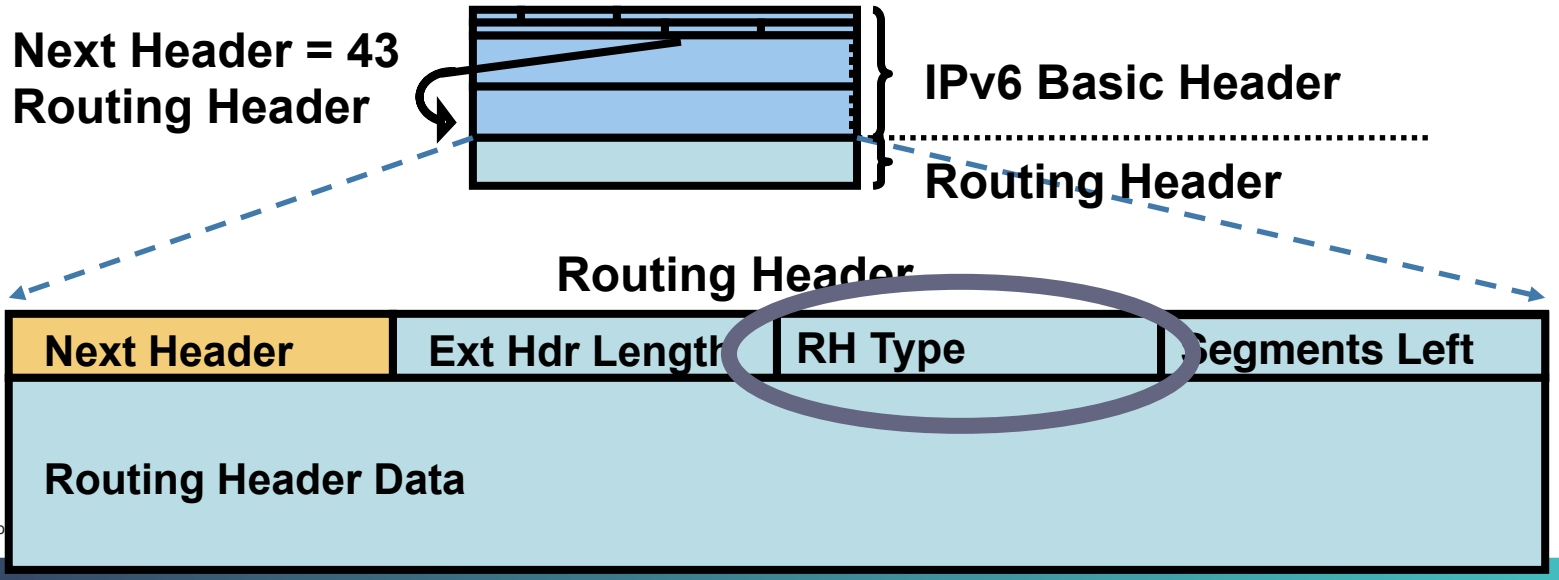
© 2015 Cisco and/or its affiliates. All rights reserved.

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

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

IPv6 Routing Header

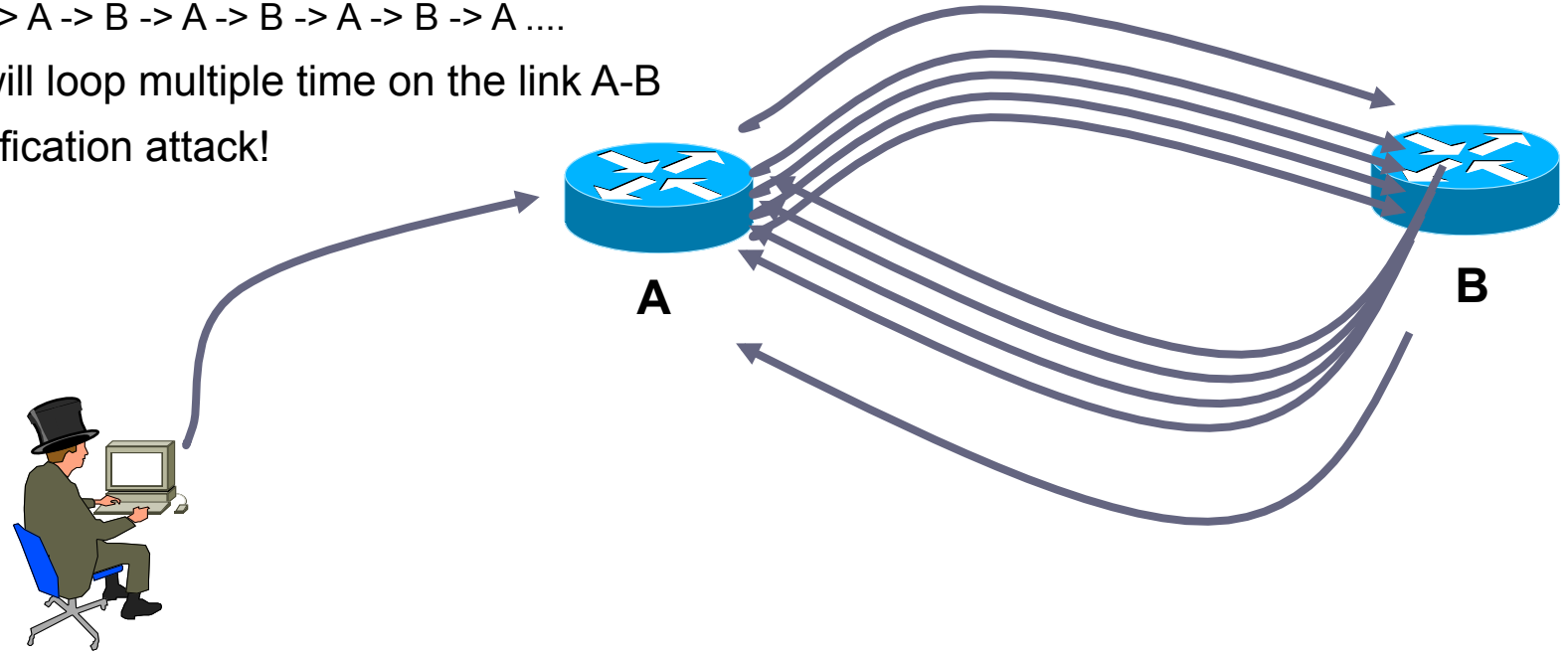
- An extension header, processed by **intermediate** routers
- Three types
  - Type 0: similar to IPv4 source routing (multiple intermediate routers)
  - Type 2: used for mobile IPv6
  - Type 3: RPL (Routing Protocol for Low-Power and Lossy Networks)



© 2015 Cisco and/o

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!



© 2015 Cisco and/or its affiliates. All rights reserved.

What RFC 5095 Says

J. Abley
Afilias
P. Savola
CSC/FUNET
G. Neville-Neil
Neville-Neil Consulting

December 2007

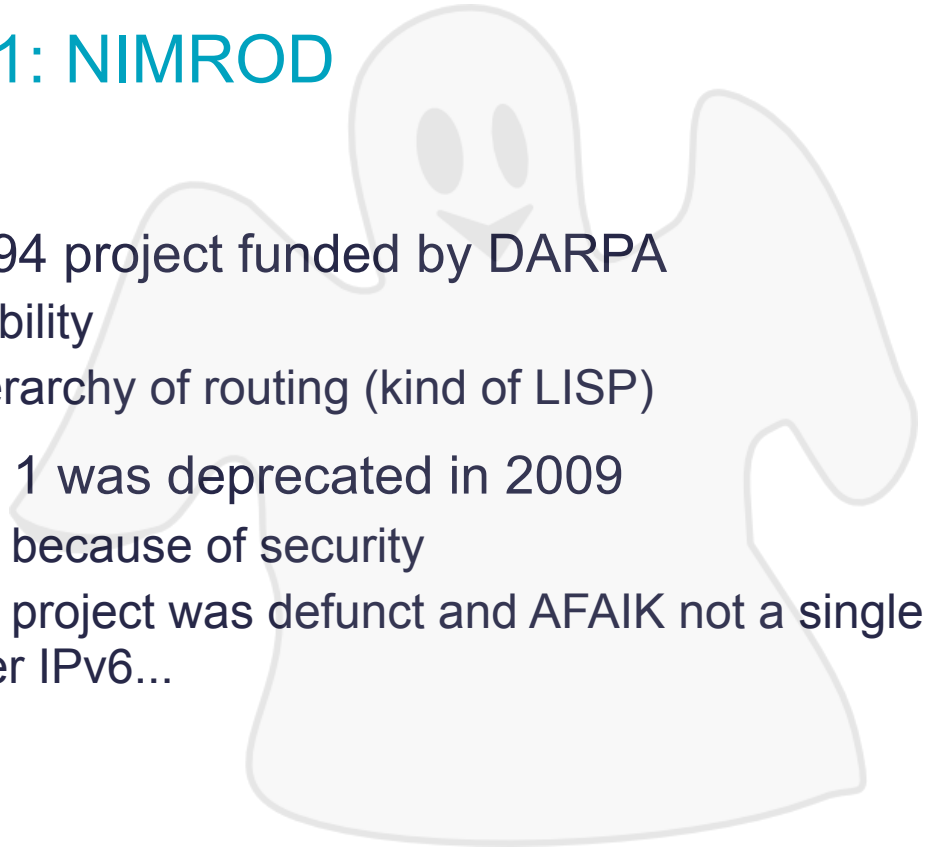
Deprecation of Type 0 Routing Headers in IPv6
RFC 5095

"The severity of this threat is considered to be sufficient to warrant deprecation of RH0 entirely. A side effect is that this also eliminates benign RH0 use-cases; ***however, such applications may be facilitated by future Routing Header specifications****."*

© 2015 Cisco and/or its affiliates. All rights reserved.

Type 1: NIMROD

- A 1994 project funded by DARPA
  - Mobility
  - Hierarchy of routing (kind of LISP)
- Type 1 was deprecated in 2009
  - not because of security
  - but project was defunct and AFAIK not a single NIMROD packet was sent over IPv6...

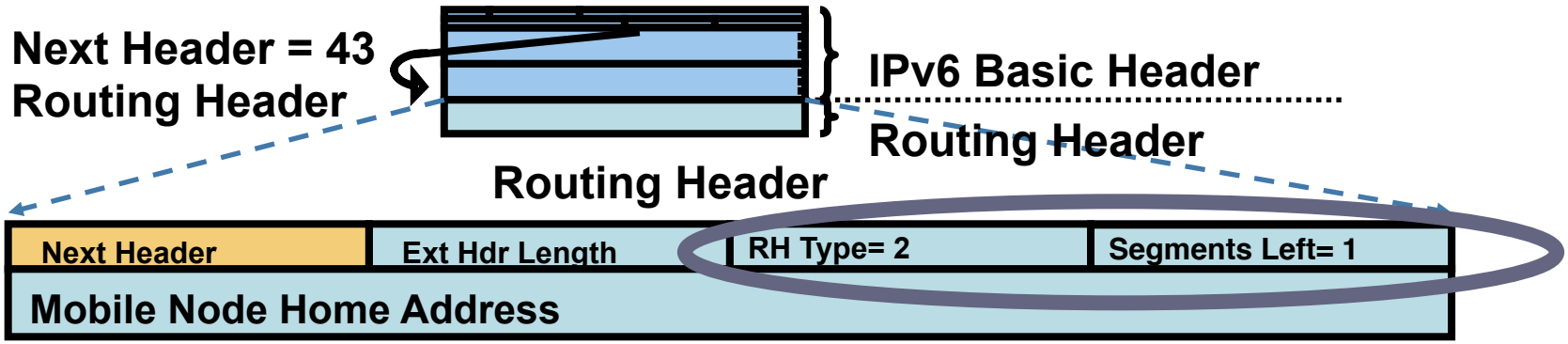


Source: Clipartpanda.com

© 2015 Cisco and/or its affiliates. All rights reserved.

IPv6 Type 2 Routing Header: no problem

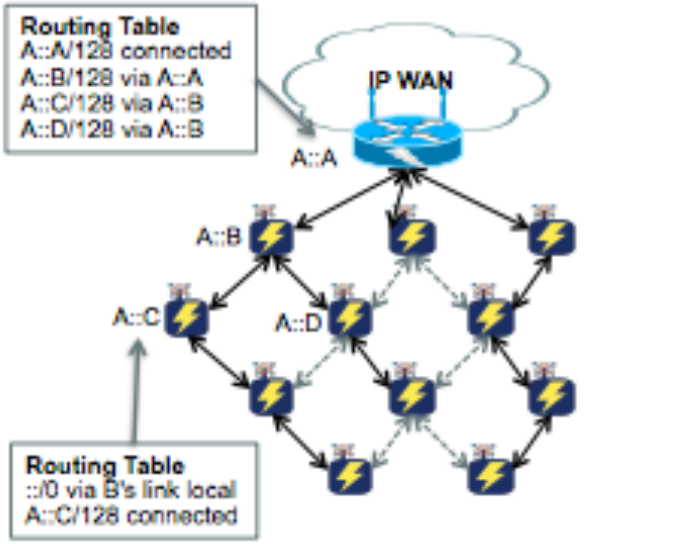
- Rebound/amplification attacks impossible
  - Only one intermediate router: the mobile node home address



© 2015 Cisco and/or its affiliates. All rights reserved.

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



© 2015 Cisco and/or its affiliates. All rights reserved.

Segment Routing Security

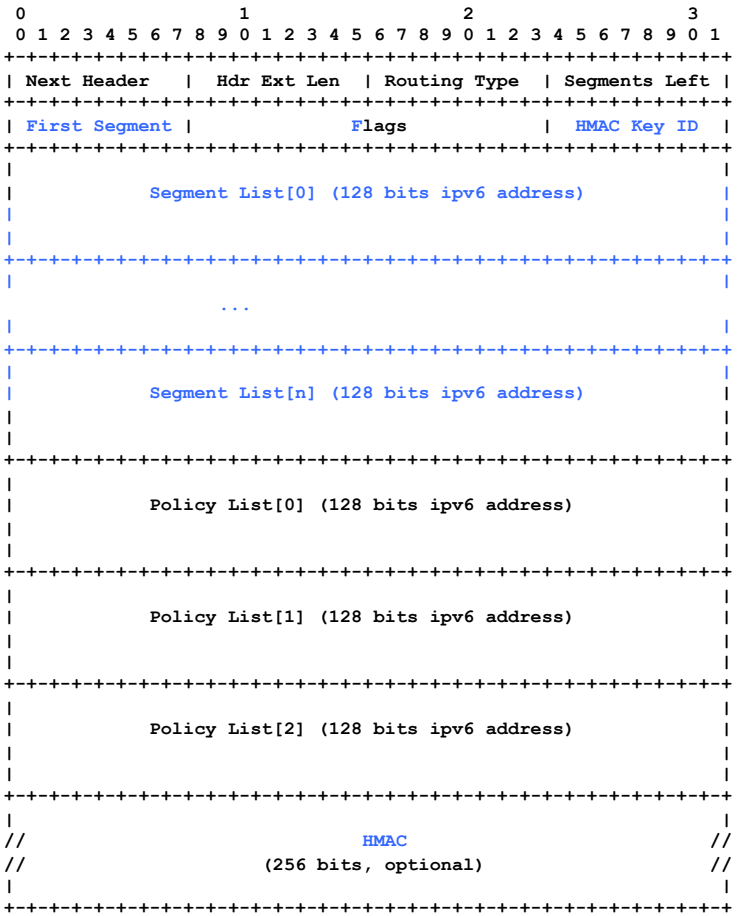
- Addresses concerns of RFC5095
  - HMAC field to be used at ingress of a SR domain in order to validate/authorize the SRH
  - Inside SR domain, each node trust its brothers (RPL model)

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

© 2015 Cisco and/or its affiliates. All rights reserved.

SRH: HMAC Coverage

- Source Address (not shown): as it is immutable and to prevent SR service stealing
- First Segment: offset in the SRH, not including the first 8 octets and expressed in 16-octet units, pointing to the last element of the Segment List
- Flags:
  - bit-0: cleanup
  - bit-1: rerouted packet
  - bits 2 and 3: reserved
  - bits 4 to 15: policy flags
- HMAC Key ID:
- Segment List[n]: all segments



© 2015 Cisco and/or its affiliates. All rights reserved.

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 !

© 2015 Cisco and/or its affiliates. All rights reserved.

Myth: Ext Hdr are dropped on the Internet

- draft-gont-v6ops-ipv6-ehs-in-real-world
  - About 20-40% of packets with Ext Hdr are dropped over the Internet
- SRH works only within one administrative domain
  - => not an issue as operator set the security/drop policy
- Test on your own: http://www.vyncke.org/sr.php
  - And let us know !

© 2015 Cisco and/or its affiliates. All rights reserved.

Running Code BnB @ IETF-90

Source: wikimedia

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

Implementations

- Multiple implementations exist and interoperability has been demonstrated during IETF-90
  - Cisco,
    Comcast,
    Ecole Polytechnique (Paris),
    UCLouvain (LLN, Belgium)
- Demonstrated interoperability between multiple, independent IPv6 Segment Routing implementations (routers and hosts)
- Illustrate interoperability between SR and non-SR capable routers and hosts
- Illustrate how SR can be leveraged for video content delivery through SR capable caches

© 2015 Cisco and/or its affiliates. All rights reserved.

Wrapping Up

Source: wikimedia

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

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
- SRH does not suffer from the same security issues of RH-0
  - Not enabled by default
  - Only within one autonomous system
  - Else, protected by HMAC

© 2015 Cisco and/or its affiliates. All rights reserved.

Thank you.