Multicast Routing Key Management Protocol

Sam Hartman

Dacheng Zhang

IETF79

draft-hartman-karp-mrkmp

11/07/10

Objectives

- Provide initial proposal for automated key management for routing protocols such as OSPF and IS-IS
- Support an approach that also works for unicast
- Demonstrate the out-of-band model for KARP

What KARP Learns Now

- Work out long-standing open issues
  - Work through multicast interactions for key table
  - Work through out-of-band key management
- Examine interface between routing protocol and key management

Replay and Protocol Interactions

- Today, manual keying provides no defense against inter-session replay
- Automated key management is one approach:
  - Re-key when a new “session” starts
  - Requires trigger from routing protocol to KMP
- Significant complexity savings if routing protocols solve this themselves

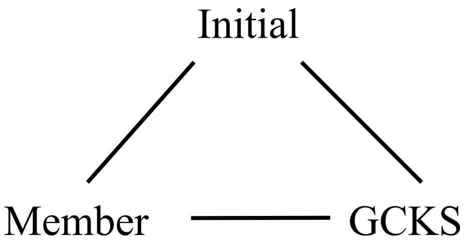
Starting from Known Technologies

- Based on GDOI for multicast operation
- Based on IKEv2 for base key management
- Some changes and alignment are required

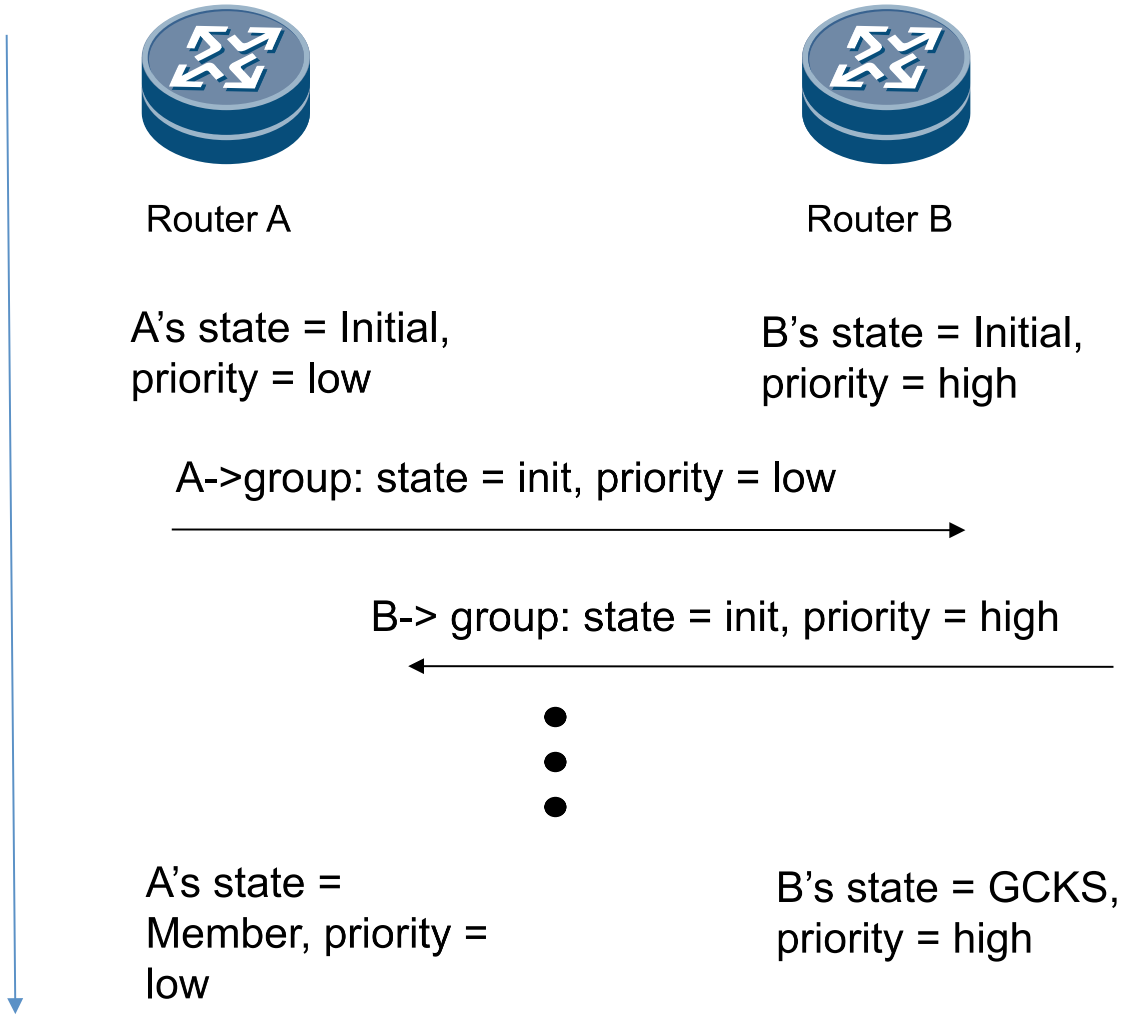
Overview

- Elect a GCKS from available candidates
- All nodes perform unicast authentication to the GCKS and get initial key download
- GCKS may provide periodic updates

Election Protocol



State Machine



t1

A’s state = Initial, priority = low

B’s state = Initial, priority = high

A->group: state = init, priority = low

B-> group: state = init, priority = high

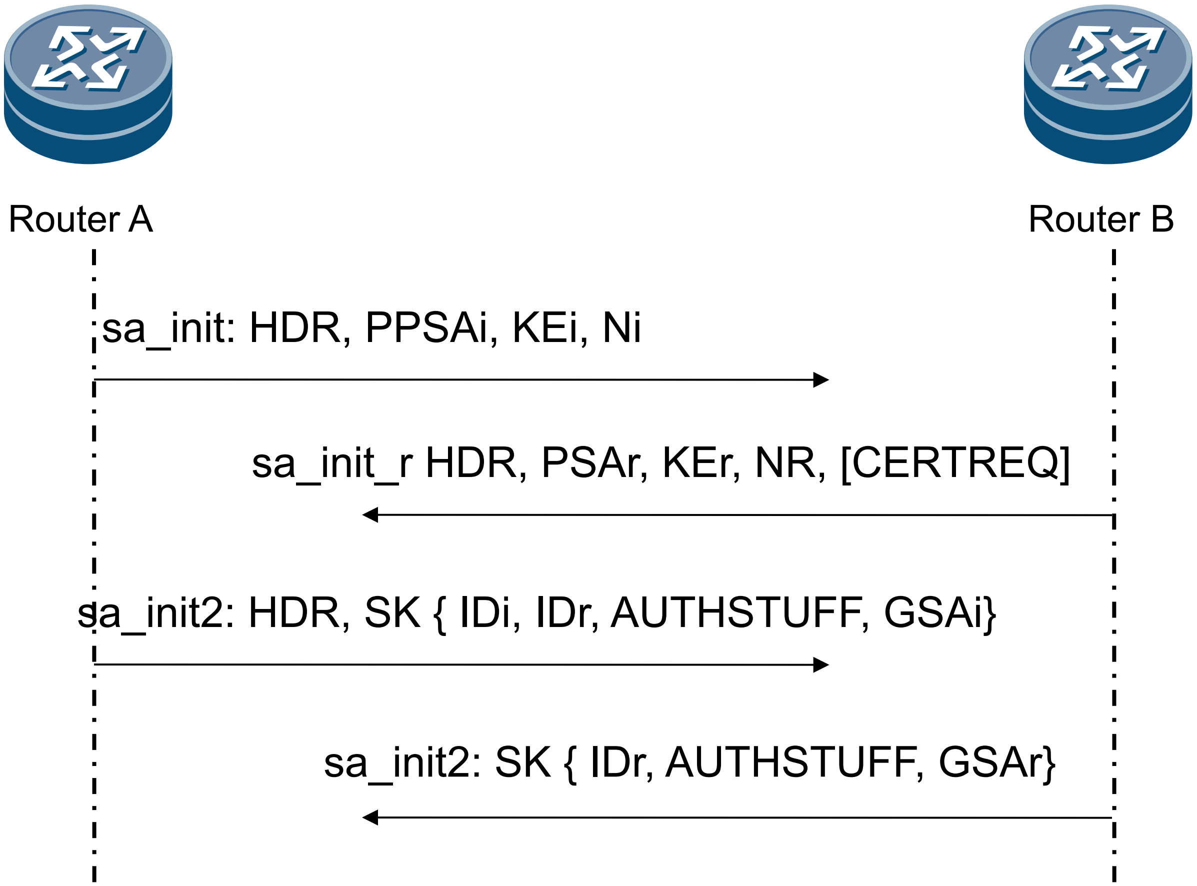
Time Delay

t2

A’s state = Member, priority = low

B’s state = GCKS, priority = high

Initial Exchange



Router A

Router B

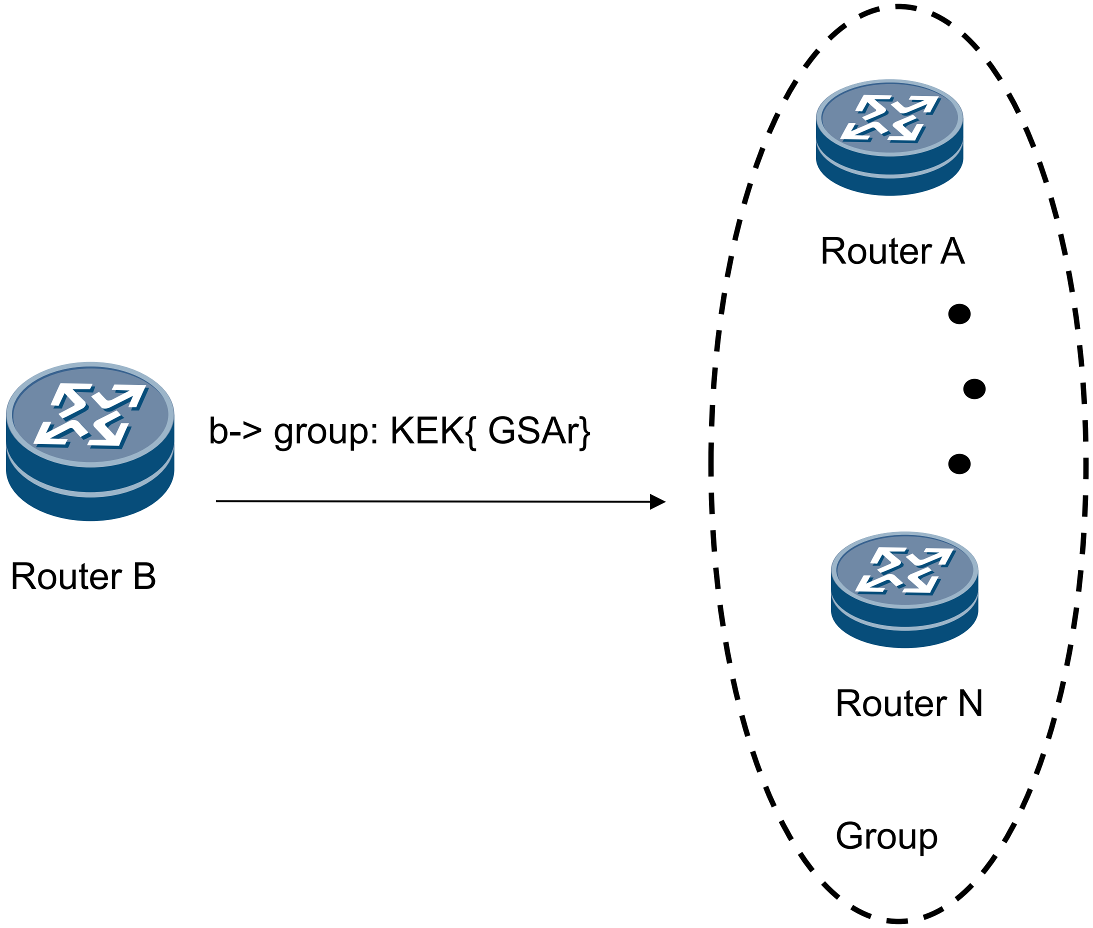
sa_init: HDR, PPSAi, KEi, Ni

sa_init_r HDR, PSAr, KEr, NR, [CERTREQ]

sa_init2: HDR, SK { IDi, IDr, AUTHSTUFF, GSAi}

sa_init2: SK { IDr, AUTHSTUFF, GSAr}

Key Update



Interface to Routing Protocol

- Manipulate election priorities to match DR/ BDR
- Request re-keys to deal with replays