Multicast Routing Key Management Protocol

Sam Hartman

Dacheng Zhang

IETF79

draft-hartman-karp-mrkmp

Objectives

- Provide automated key management for routing protocols such as OSPF and IS-IS
- Use same credentials and similar approach for unicast key management
- Separate key management from actual routing protocols

Threat Model

- Insider attacks are out of scope
- Every member of the group can take on the GCKS role
- Groups are small and eviction rare

Credentials

- Solution should be independent of credential types
- Credentials may be preshared keys, asymmetric keys, PKI or something else
- No assumption of a PKI or any asymmetric keys

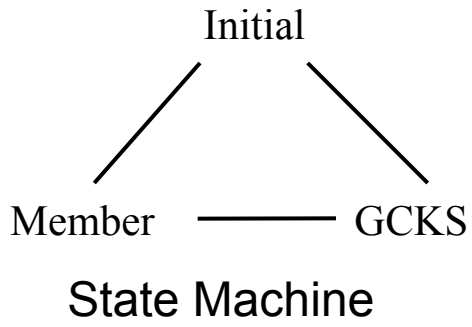
Starting from Known Technologies

- 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

Router A

Router B

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

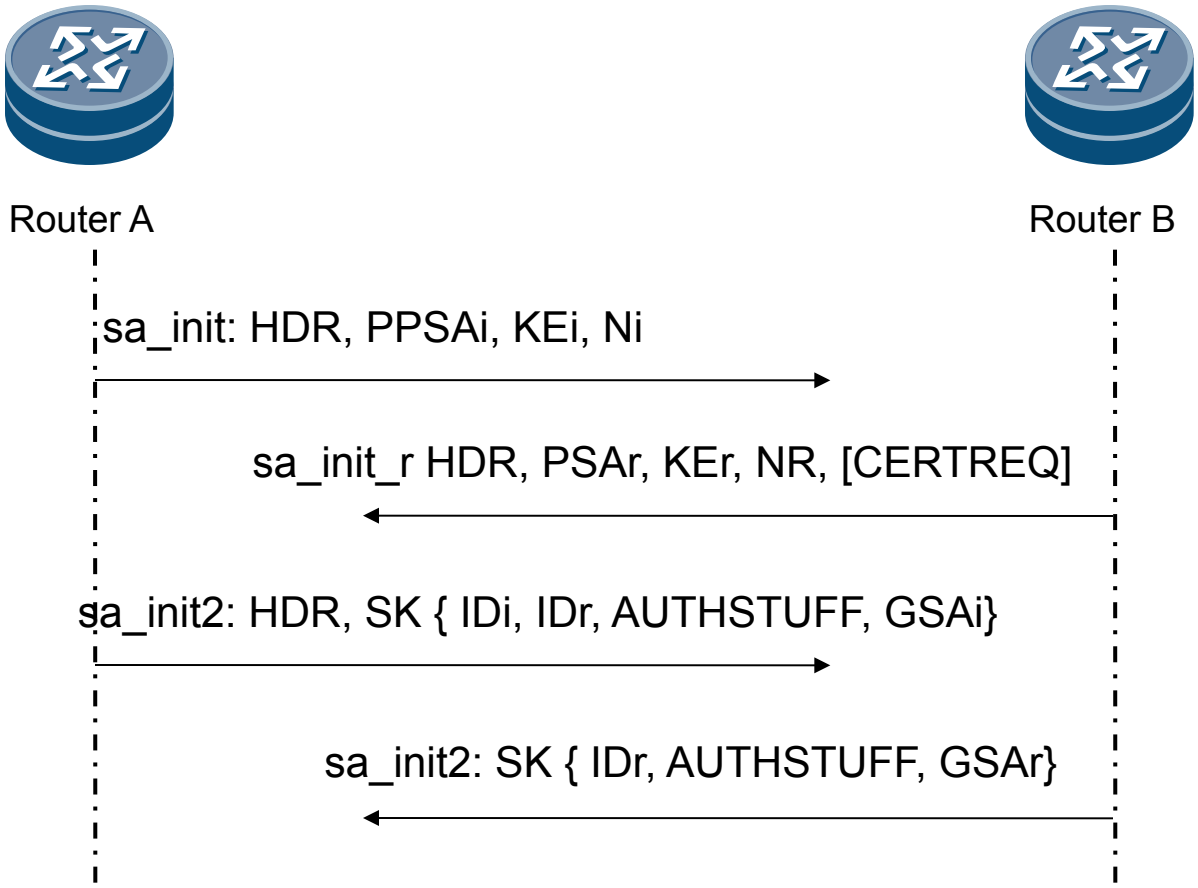
A's state = Member, priority = low

B's state = GCKS, priority = high

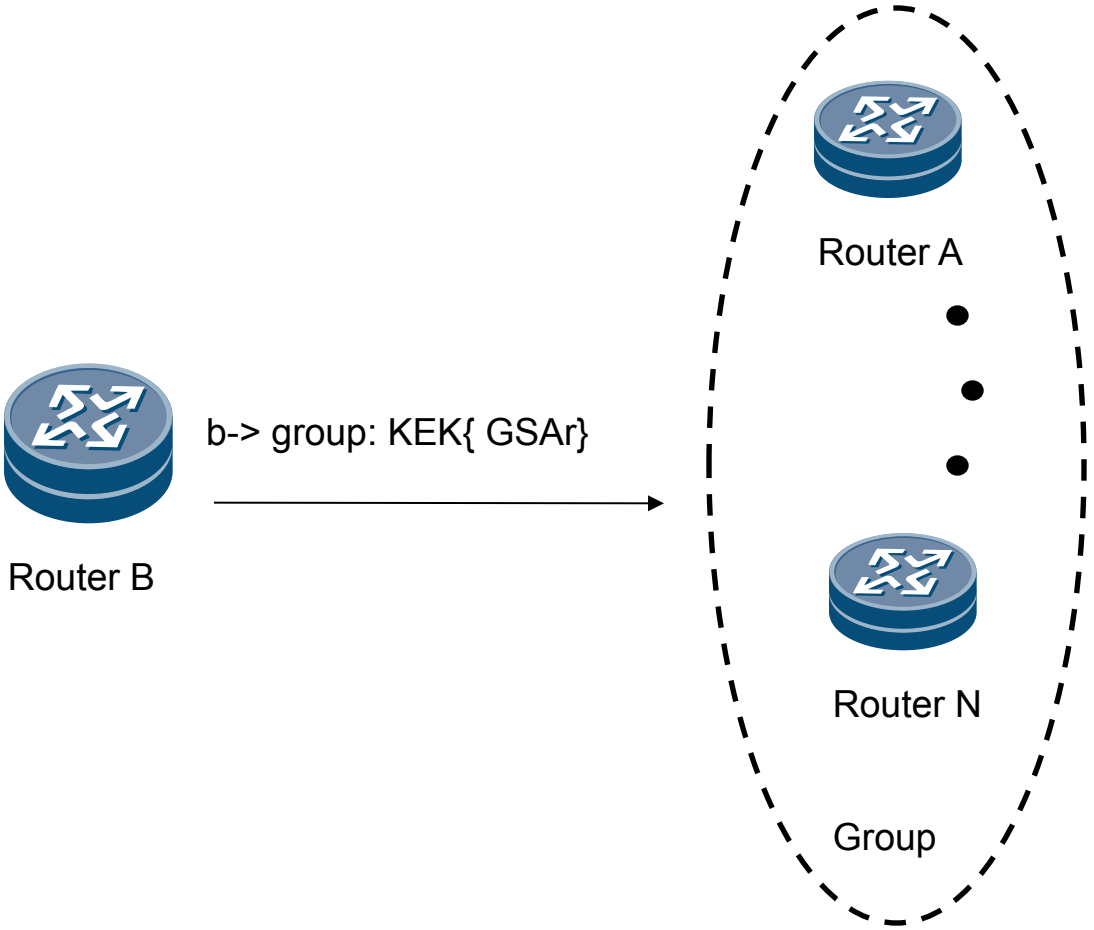
Election Constraints

- Objective: elect a valid member of the group as GCKS
- Attackers may force the outcome of the election
- Attackers should not be able to force a DOS
- Election is insecure; secure confirmation of candidate validity after

Initial Exchange



Key Update



Questions