IETF83-KARP

Key Management and Adjacency Management for KARP-based Routing Systems

J. William Atwood
Revathi Bangalore Somanatha
Concordia University, Montreal

Contents

- Problem Statement
- Architecture and Definitions
- Overview
- Key Scopes
- Place of KARP Proposals
- Context Identifier assignment
- Adjacency
- Our Design
- Questions

Problem Statement

- Ongoing work on key management
  - RKMP – for unicast pairings
  - MRKMP – for multicast associations on a shared LAN
  - GDOI and GDOI-IKEv2 – examples of a group management protocol
- Ongoing work on adjacency management
  - None that we are aware of
  - We will present some ideas and hope for feedback from the WG members

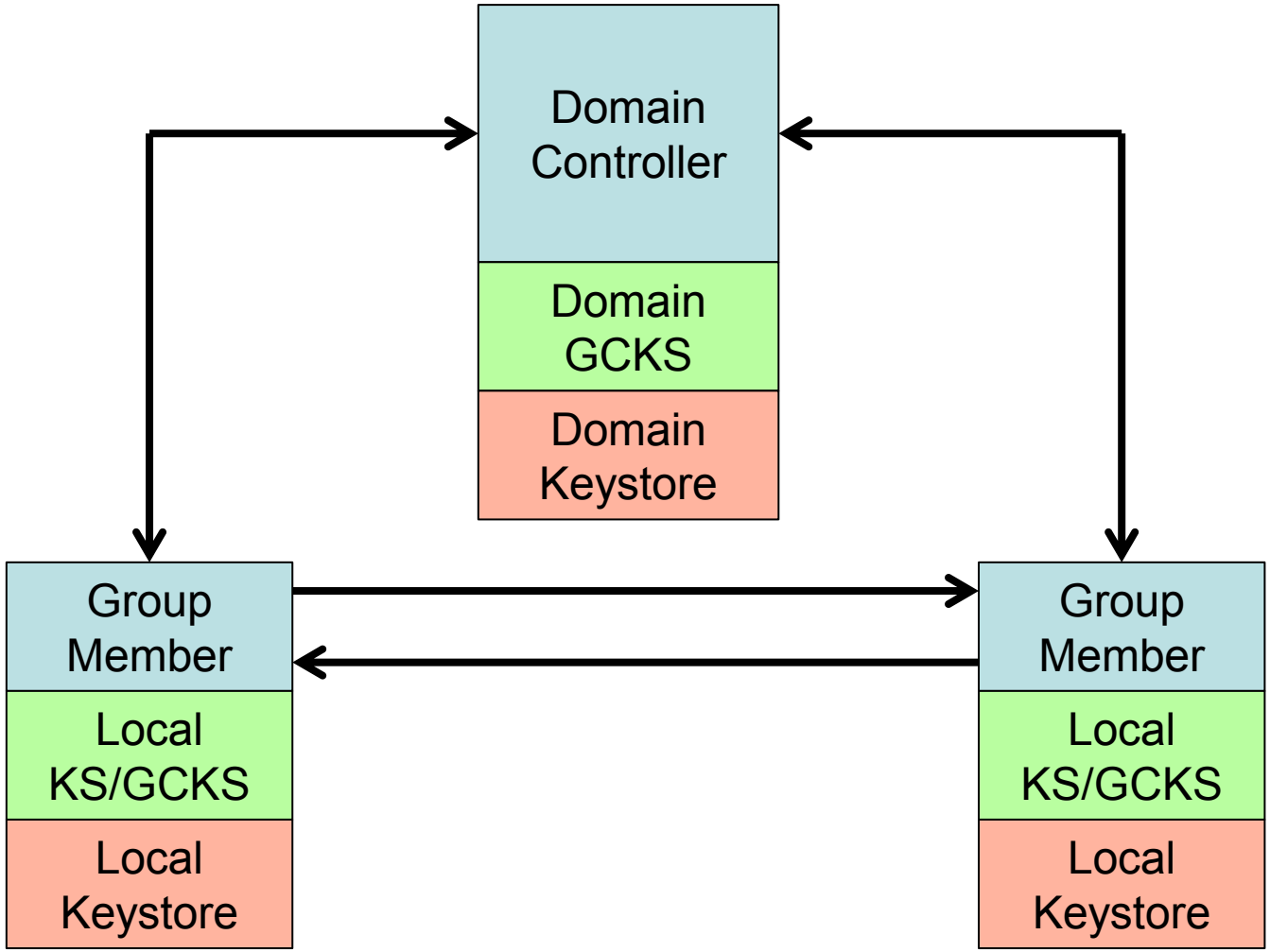
Definitions

- Administrative Domain (AD)
  - Set of routers under a single administration
    - RFC 4375 provides a convenient definition (in the context of Emergency Management)
  - An AD is not bigger than an autonomous system
    - Because we are dealing with Interior Gateway Protocols
- Domain Controller (DC)
  - Specific to a particular routing protocol (RP), because “adjacency” may be defined differently for each RP
    - Rules may be the same for different protocols, but stored data will be different

Definitions..2

- Group Member (GM)
  - Any router within the Administrative Domain
    - Note that depending on the keying model in use, we may form smaller “groups”
- Neighbor
  - The set of routers that are adjacent to a particular router

Architecture



Overview

- Three issues for discussion
  - Key scope
  - Context Identifier assignment
  - Adjacency management

Overview..2

- Key scope
  - The subset of the GMs where a key is valid
  - Two extreme examples
    - One key for whole region
    - Different keys for each interface for each sender
- Context Identifier assignment
  - MUST be centralized for multicast inter-router communication
    - SPI assignment for unicast IPsec contexts is receiver-based
    - SPI assignment in IPsec cannot be receiver-based when there are multiple receivers

Overview..2

- Adjacency control
  - If active, MUST be centrally managed
  - Otherwise, the router MAY use (insecure) neighbor discovery
- This implies that there must be a central (domain) controller
  - Our design tries to minimize the need to communicate with this central controller, especially when re-booting
- We are trying to prepare for adjacency control

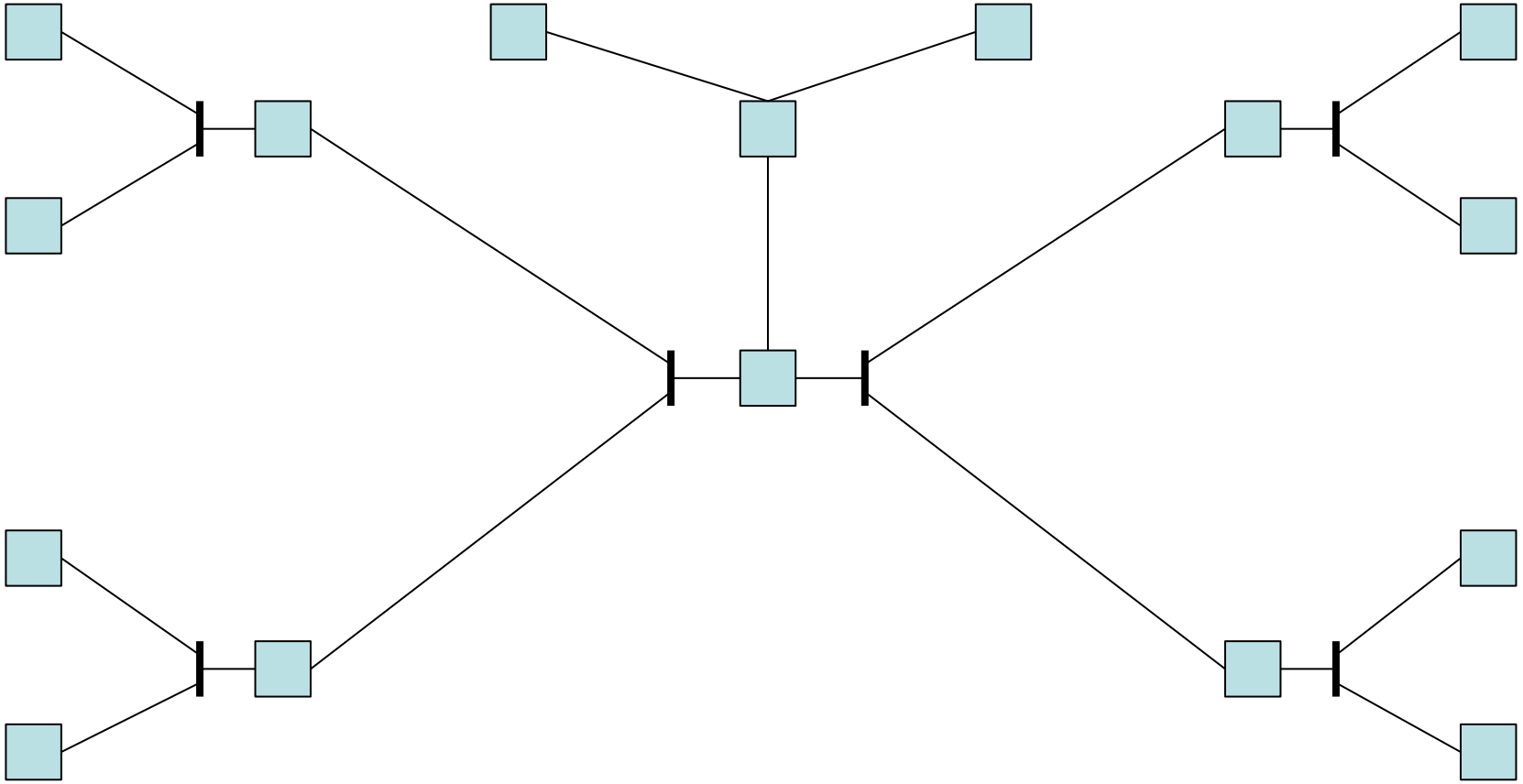
Key scope: 4+1 cases

- One key for the AD
  - Very large attack surface
  - Key must be determined by the Domain Controller
- One key per shared LAN
  - Smaller attack surface
  - Key can be determined locally
    - By mutual agreement
    - By electing a local GCKS for that LAN

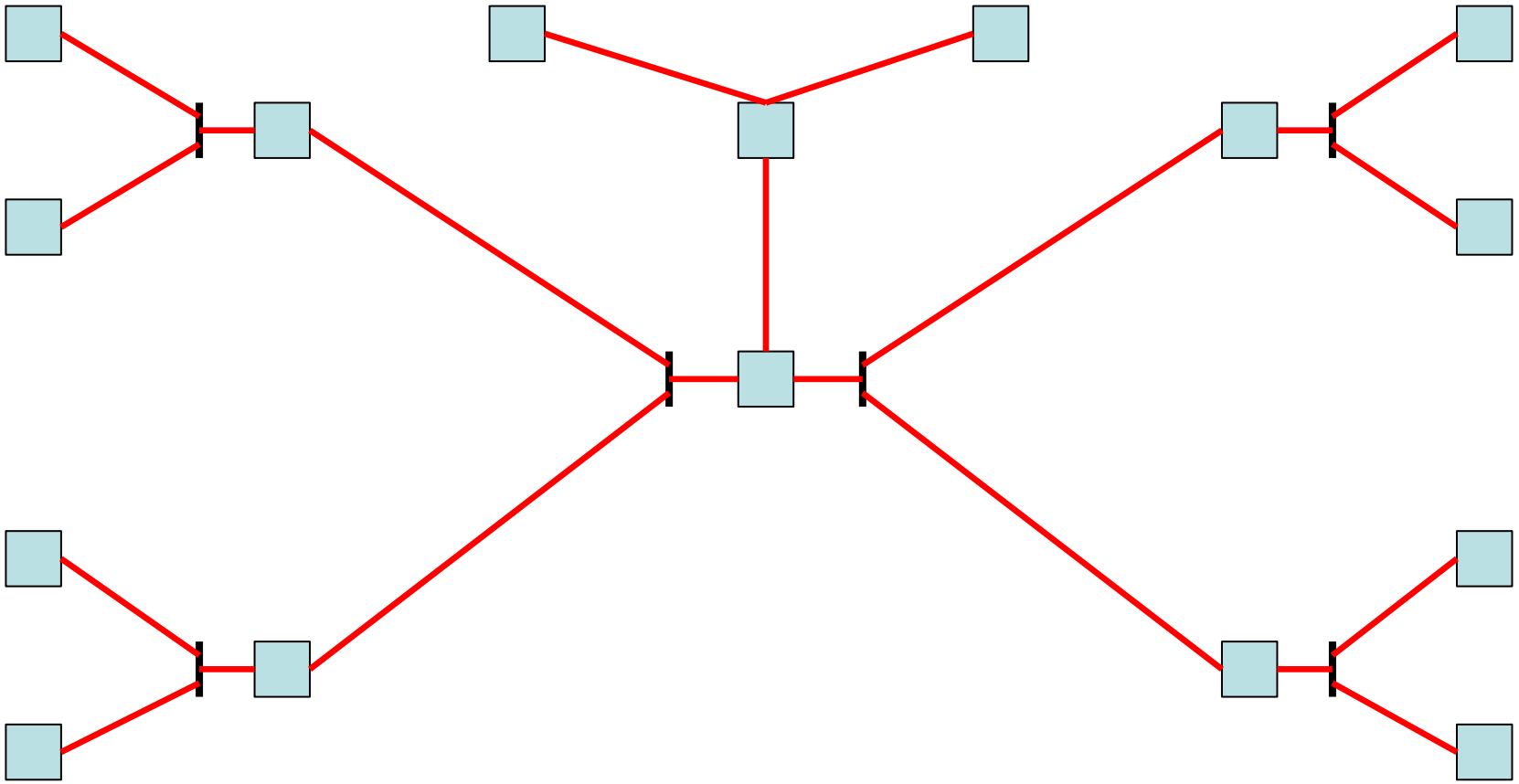
Key scope..2

- One key per sending router
  - Even smaller attack surface
  - Key is determined by sending router, and distributed to its legitimate neighbors
- One key per interface per sending router
  - Smallest attack surface
  - Keys are determined by sending router
- Two keys per pair of routers
  - Unicast IPsec (IKE, IKEv2)
  - Application layer security (TLS)

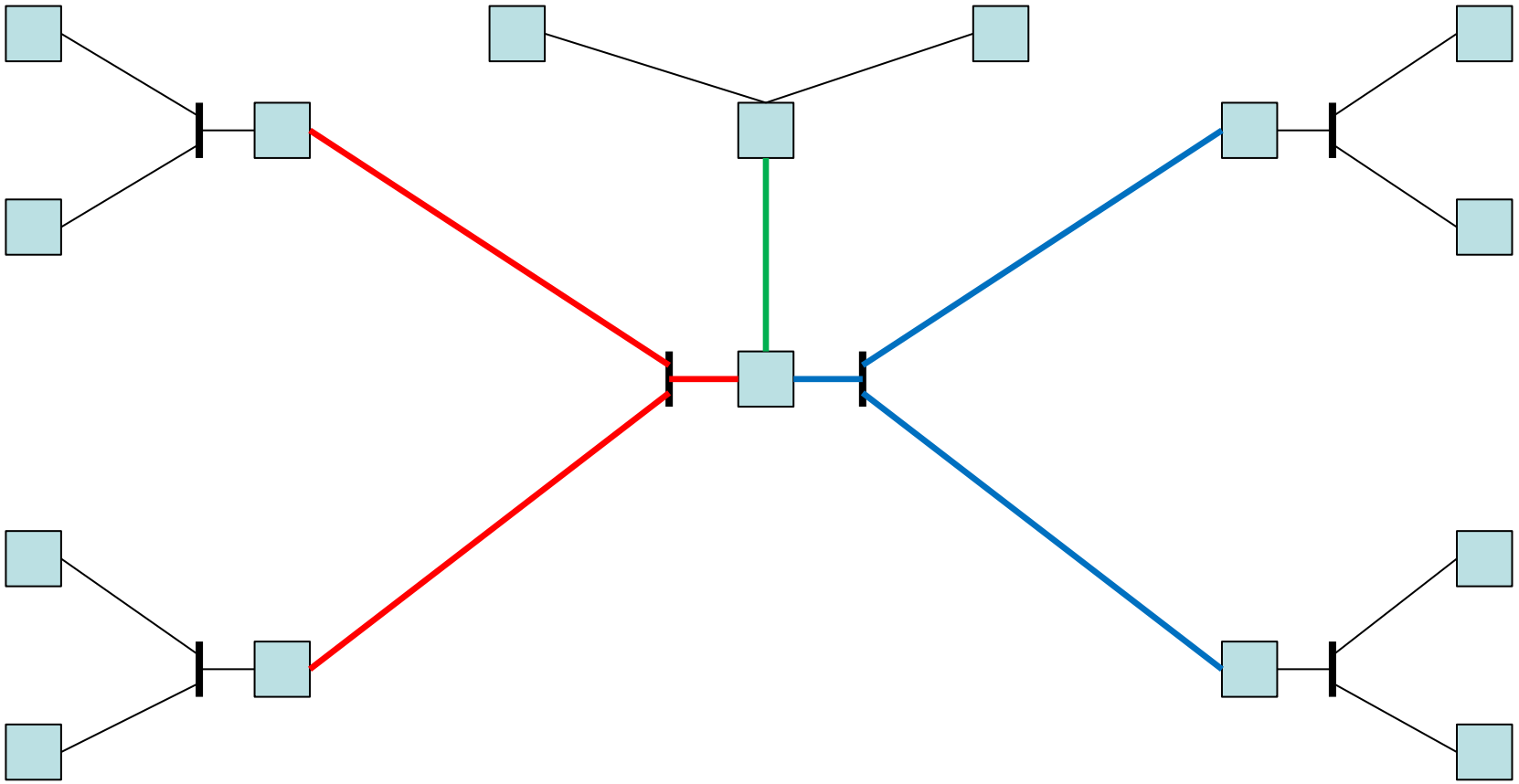
Example network



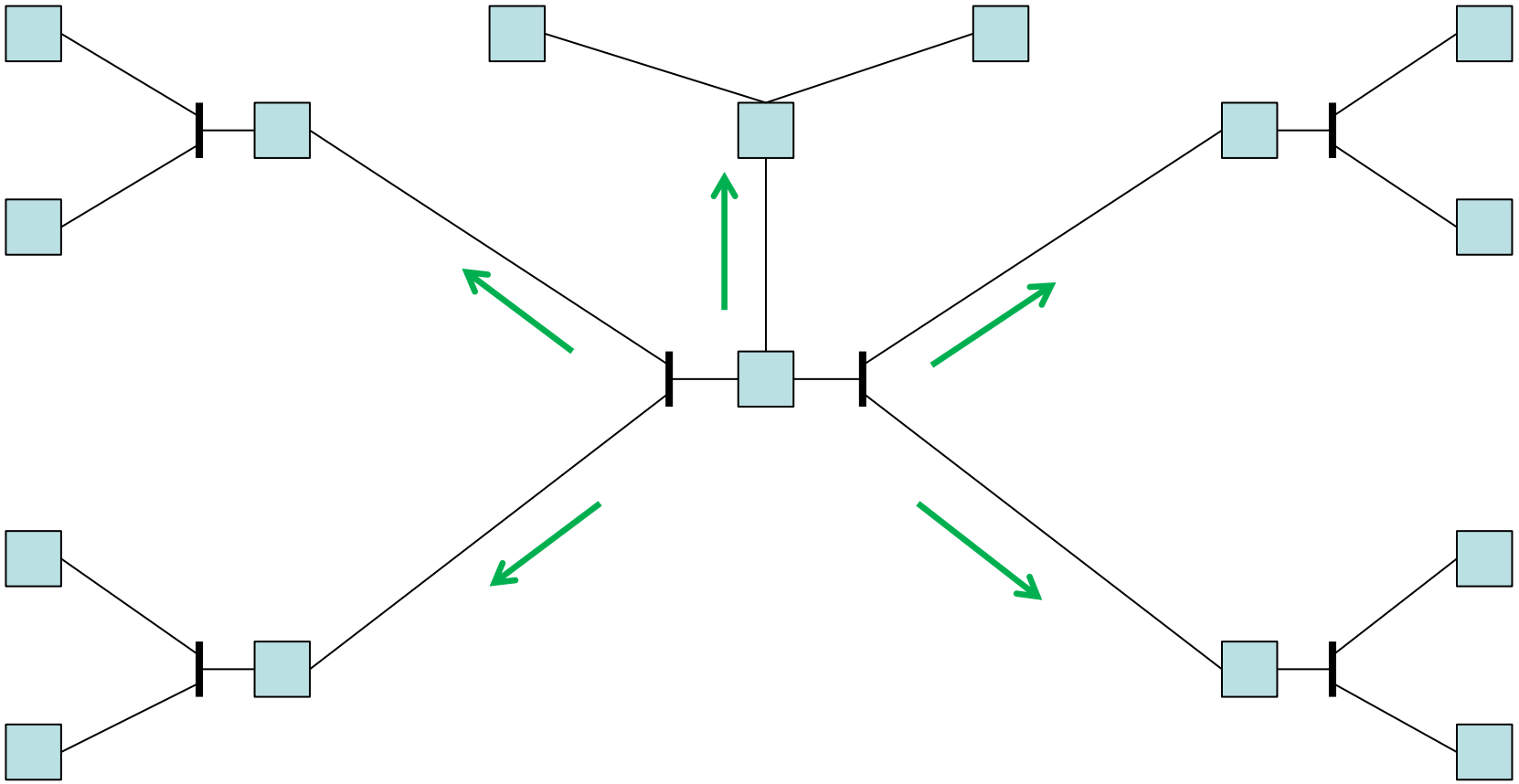
Single Key



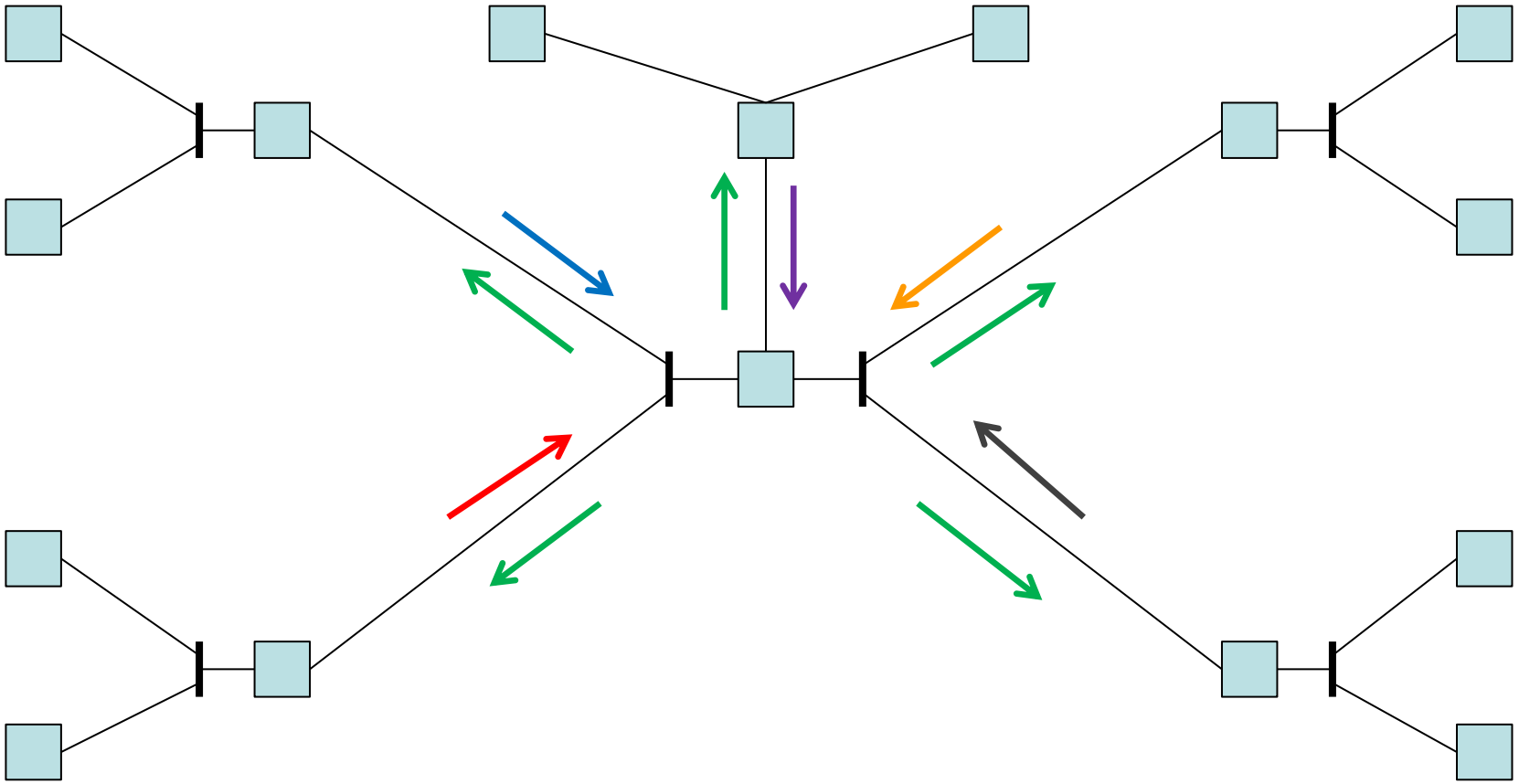
One Key per LAN



One Key per Sender: One Outgoing Key



One Key per Sender: Five Incoming Keys



Place of KARP proposals

- RKMP
  - Used to establish peer-to-peer relationships
  - Assumes a router identification method exists
- KMPRP
  - Additional details of exchanges
  - Deals with key rollover

Proposals..2

- MRKMP
  - Focuses on the election of a local GCKS for the “One Key per LAN” model
  - Assumes a router identification method exists
  - Deals with router reboots
  - Cannot deal with adjacency management
- GDOI/GDOI-IKEv2
  - Does not take into consideration keying groups (key scopes)
  - Does not deal with adjacency management

Context Identifier (CI) assignment

- One key
  - Context Identifier (e.g., SPI) to be used can be defined in the RFC, or by the administrator for the domain
- All other cases
  - Since there will potentially be multiple recipients of the group information, the CIs for each “mini-group” MUST be centrally assigned (i.e., by the Domain Controller)
    - There is probably a very nice graph-coloring problem inside this...

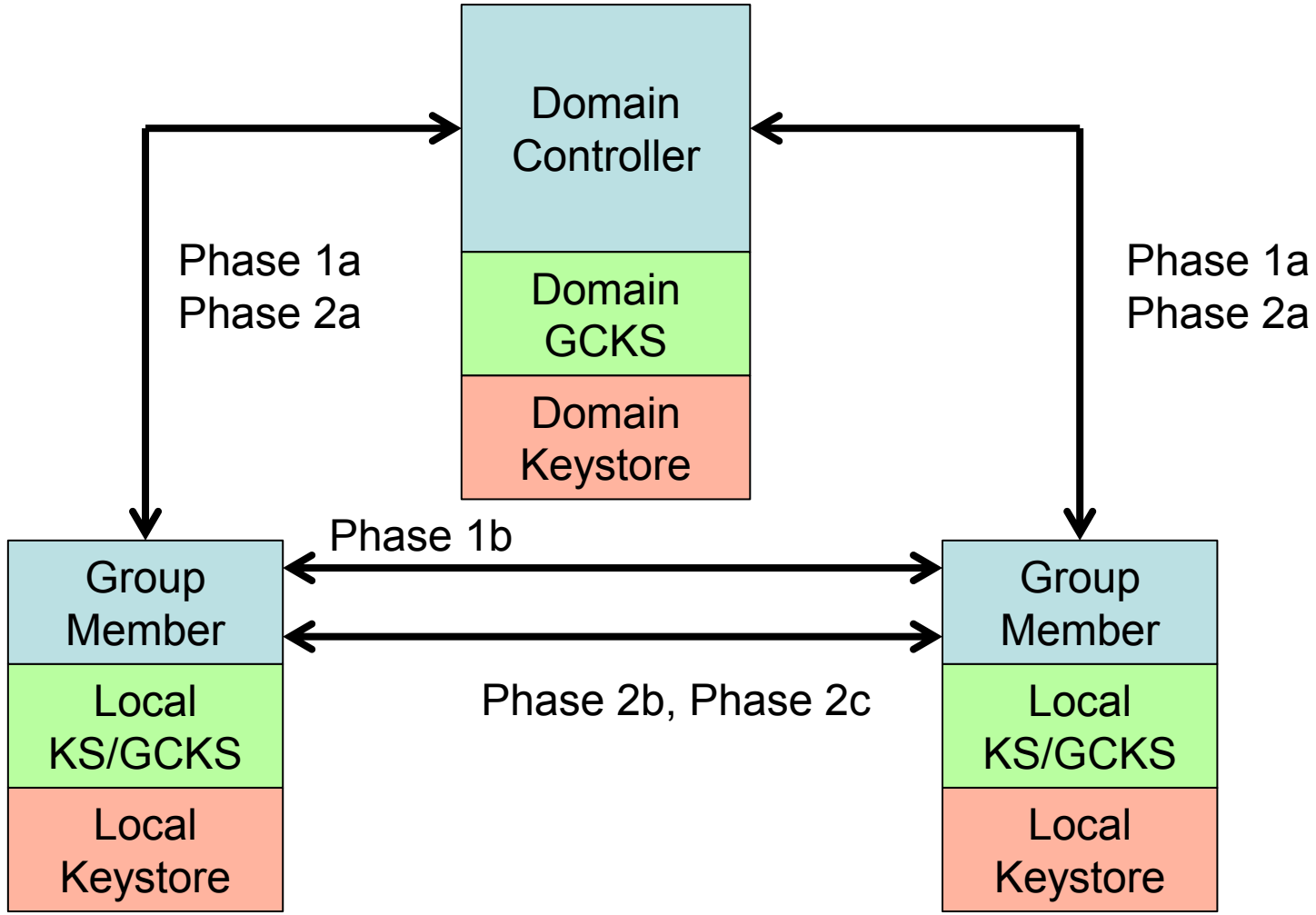
Adjacency

- Each router is assigned an “identity”
  - An FQDN, an arbitrary string, a PKI certificate, etc.
- Adjacency control can take a variety of forms
  - A neighbor is discovered, accept it
  - A neighbor has a valid certificate
    - (it is a valid router, but not necessarily adjacent to me)
  - A neighbor is permitted to be adjacent to me
- The last case MUST be centrally controlled
- The design must not prevent use of the other models (i.e., the disabling of adjacency control)

Our design

- We are exploring a design that
  - allows all of the above key scope models
  - allows us to control adjacency of routers
- Our intention is to specify the actors and the exchanges, and then formally validate the security of these exchanges using AVISPA

Key Management Phases: Between Components



Keying Phases: 1

- Phase 1a
  - Establish secure path and mutual authenticity between Domain Controller and individual Group Members
    - To be used to distribute information for use by the GM to identify and authenticate its neighbors
- Phase 1b
  - Establish secure path and mutual authenticity between adjacent Group Members
    - To be used to distribute parameters that will be used by the GM to send information to its neighbors (i.e., routing protocol control packets)

Phase 1 comments

- A single phase 1 MAY be used for all routing protocols on a particular router (for example, both OSPF and PIM), especially if their concept of “neighbor” is the same
- Phase 1a is the Phase 1 for IKE for the Domain Controller<->GM exchange
- Phase 1b is the Phase 1 for IKE for the GM<->GM exchange
  - It will happen only after the Phase 2a exchange occurs

Phase 1 comments..2

- We may need to find a good way of labeling the "keying group" that is being referenced:
  - How do I differentiate between the group on interface "x" and the group on interface "y"?
  - Is there a way to describe the interfaces that will be stable, and can be understandable to both the GM and the Domain Controller?

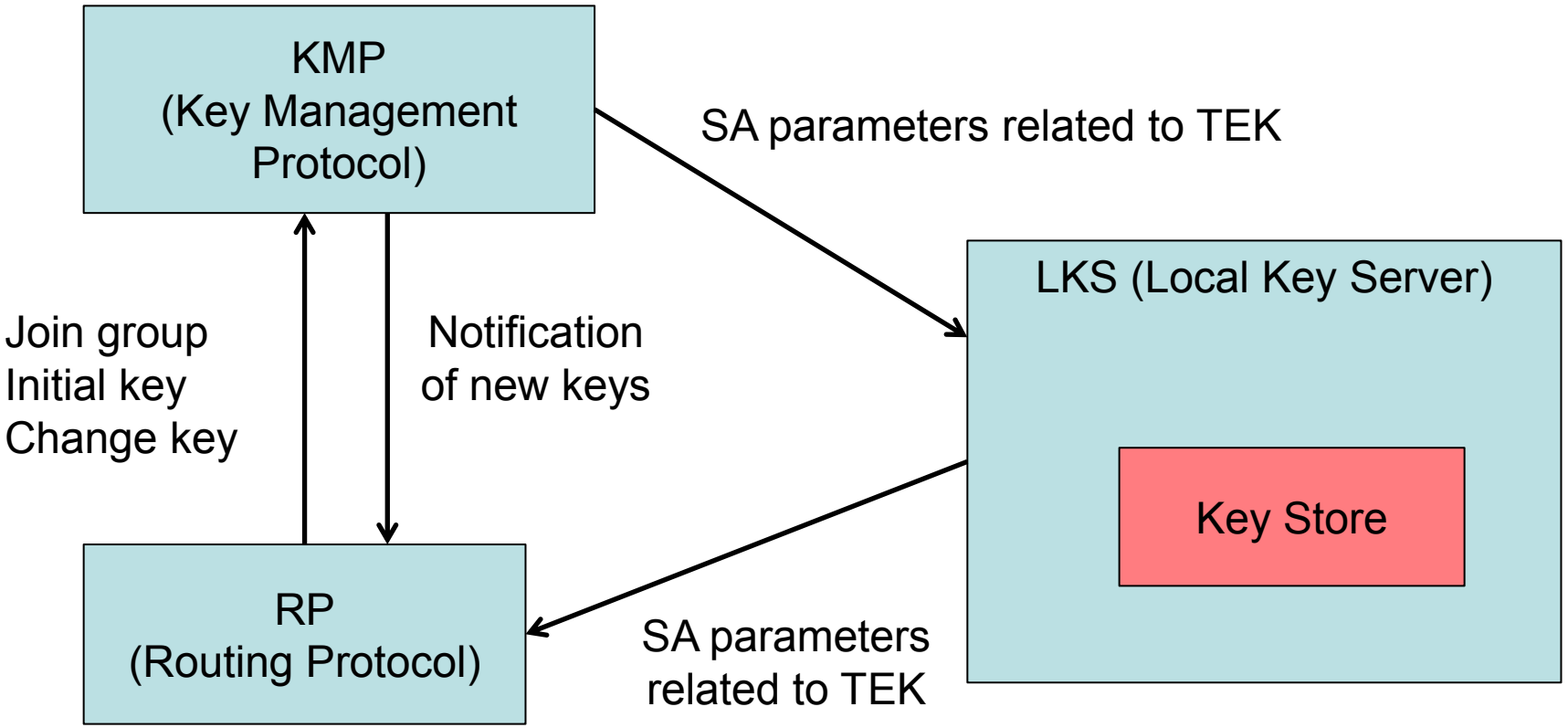
Keying Phases: 2

- Phase 2a
  - Allows a GM to establish the identity of its neighbors (or be given the rules for establishing these identities)
- Phase 2b
  - The GM contacts these identified neighbors
  - Establishes their authenticity and legitimacy
- Phase 2c
  - The GM exchanges the information with its neighbors that will be used to send the routing protocol control packets (e.g., PIM-SM Hello)

Phase 2 comments

- If policy is transferred in Phase 2a, this should be done using standard policy-specification mechanisms
  - We are currently exploring the availability of such mechanisms within the IETF and elsewhere
- Depending on the rules provided in Phase 2a, parts or all of Phase 2b or Phase 2c may be suppressed

Key Management Exchanges: Within GMs



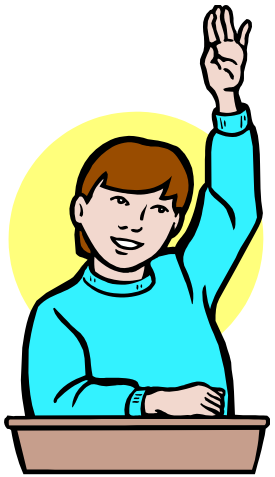
Our questions

- Is this a reasonable model for the interactions that will occur?
- Are there things that we have left out that should be included?
- Any other comments?

Our plan

- There are some details of the interactions still to be worked out
- The modeling is in progress
- We expect to report on progress at IETF 84 in Vancouver

Thank You!



Questions?