IETF84-KARP

Key Management and Adjacency Management for KARP-based Routing Systems

J. William Atwood
Revathi Bangalore Somanatha
Concordia University, Montreal

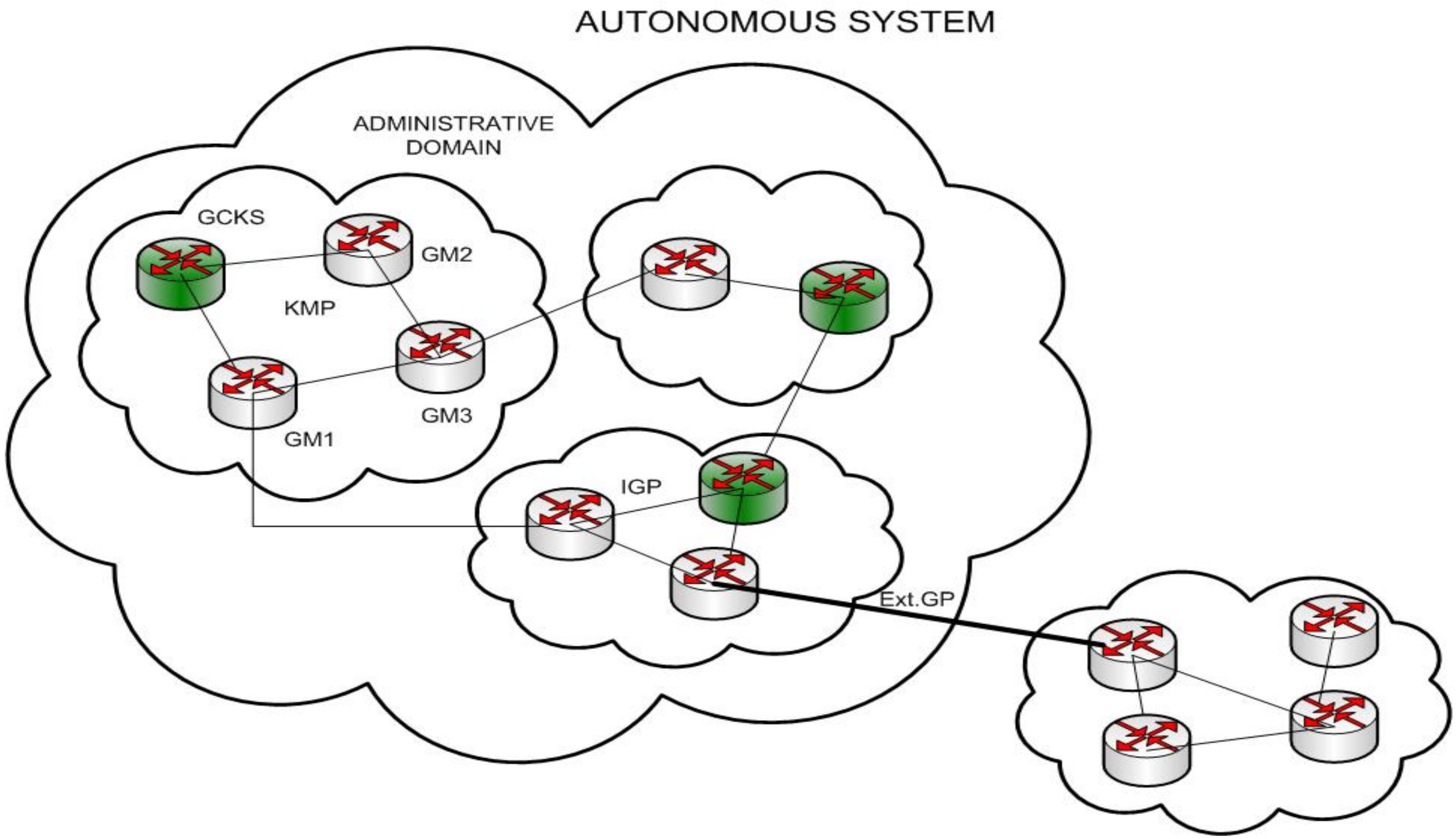
Definitions

- 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
- Group Controller/Key Server (GCKS)
  - 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

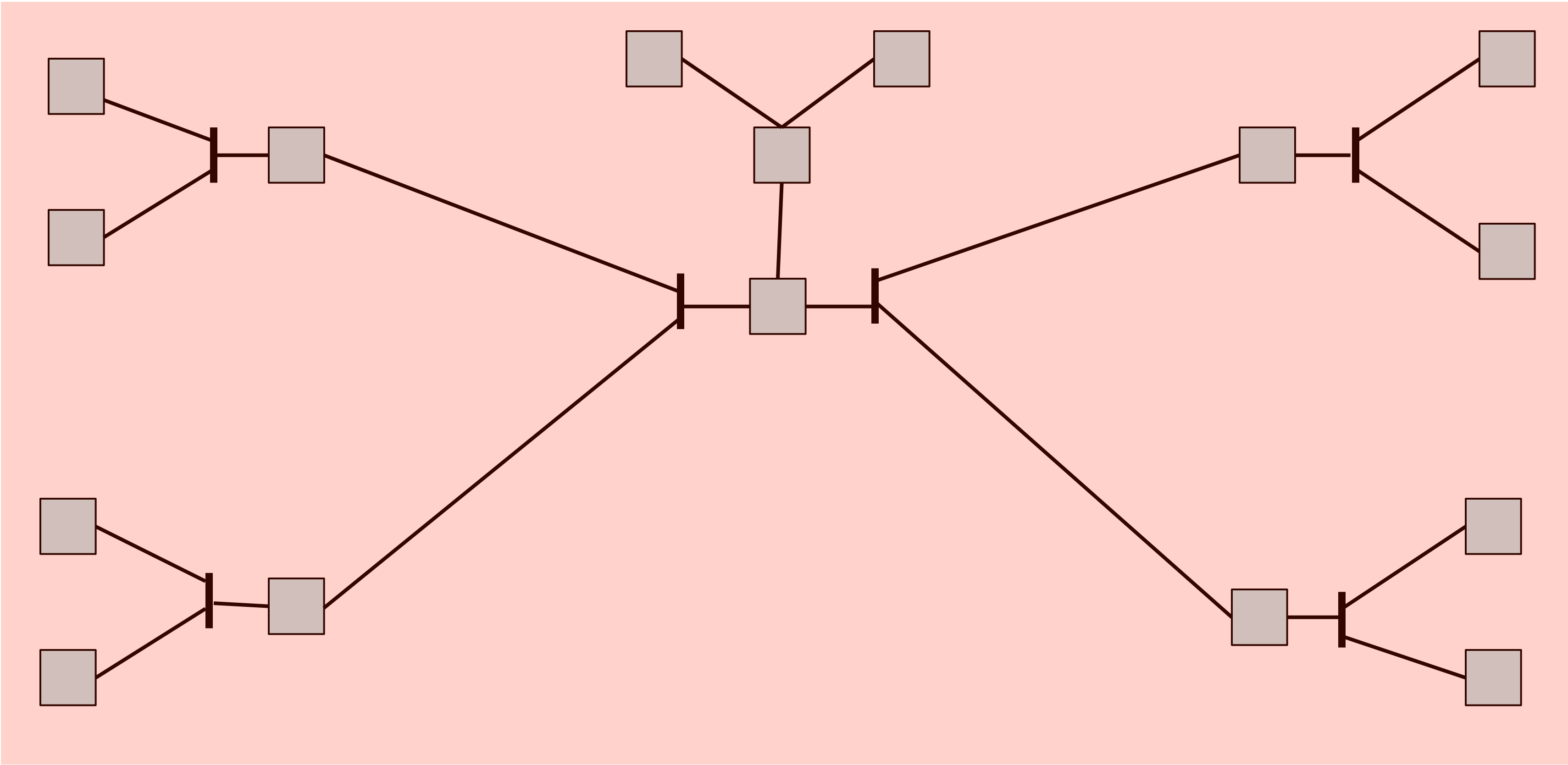
- Group Member (GM)
  - Any router within the Administrative Domain
    - Note that depending on the keying model in use, we may form smaller "groups"
- Neighbor
  - The set of routers that are adjacent to a particular router

AS and AD


AUTONOMOUS SYSTEM
ADMINISTRATIVE DOMAIN
GCKS
GM2
KMP
GM3
GM1
IGP
Ext.GP

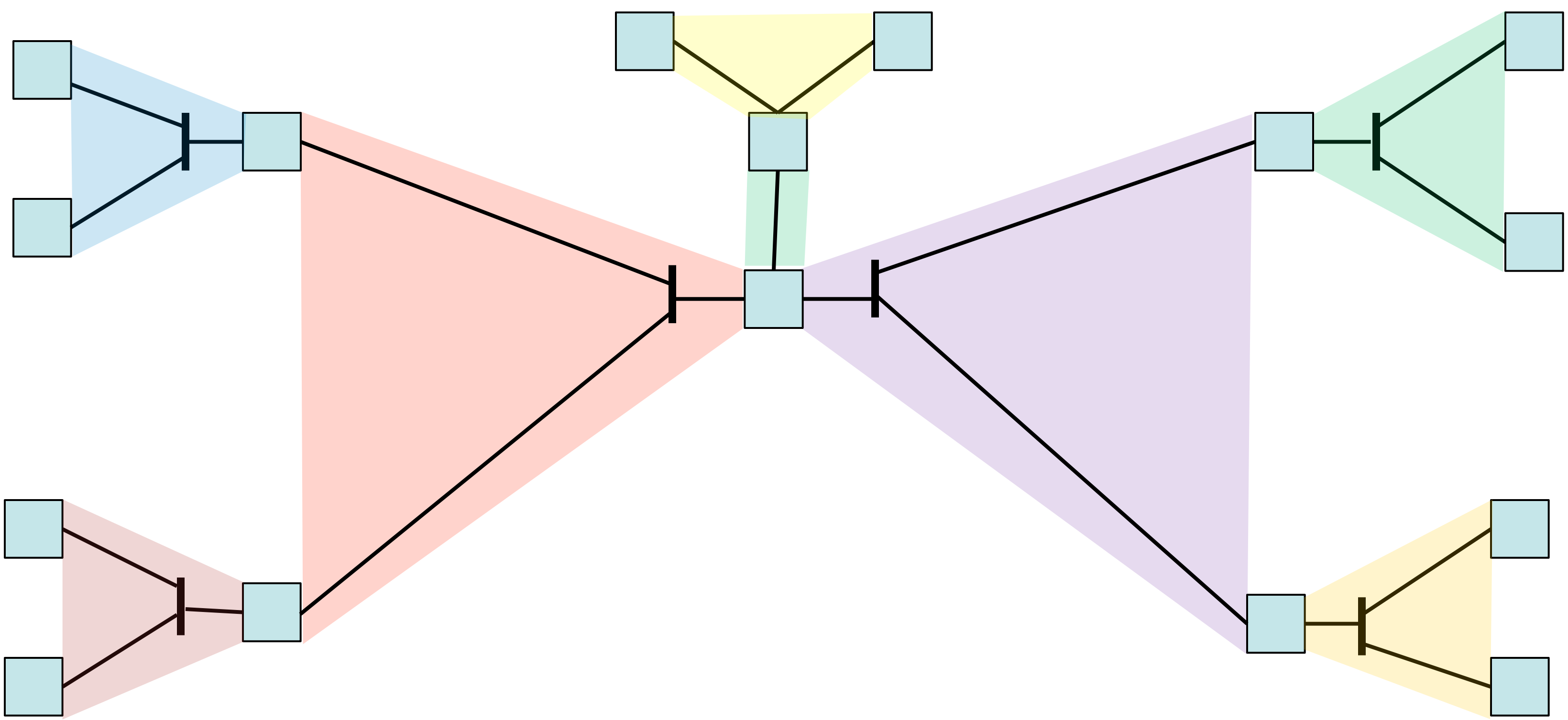
Keying Scopes (1) Whole AD

- Same key for the entire AD



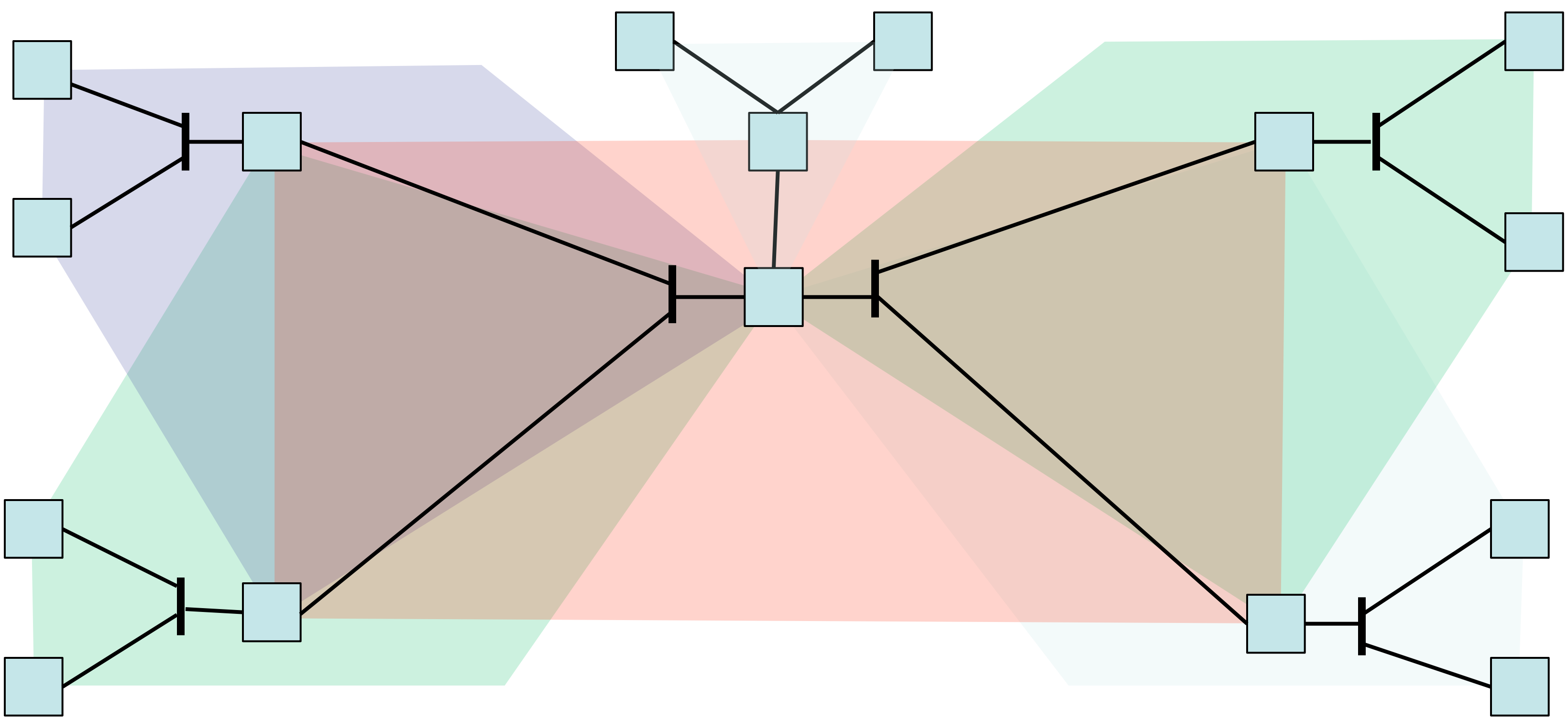
Keying Scopes (2)
All routers on a link

- Key per link



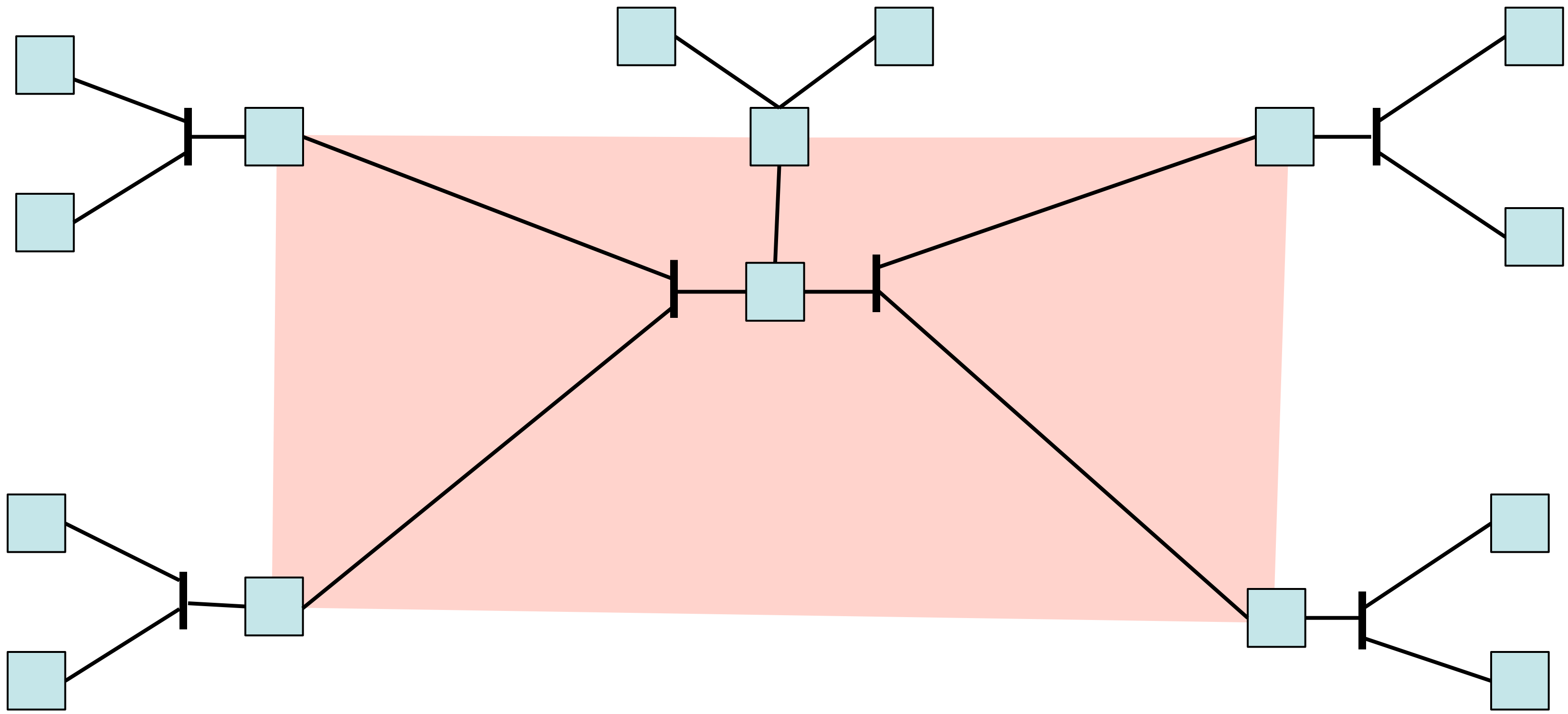
Keying Scopes (3)
Group per sending router

- Separate key per router



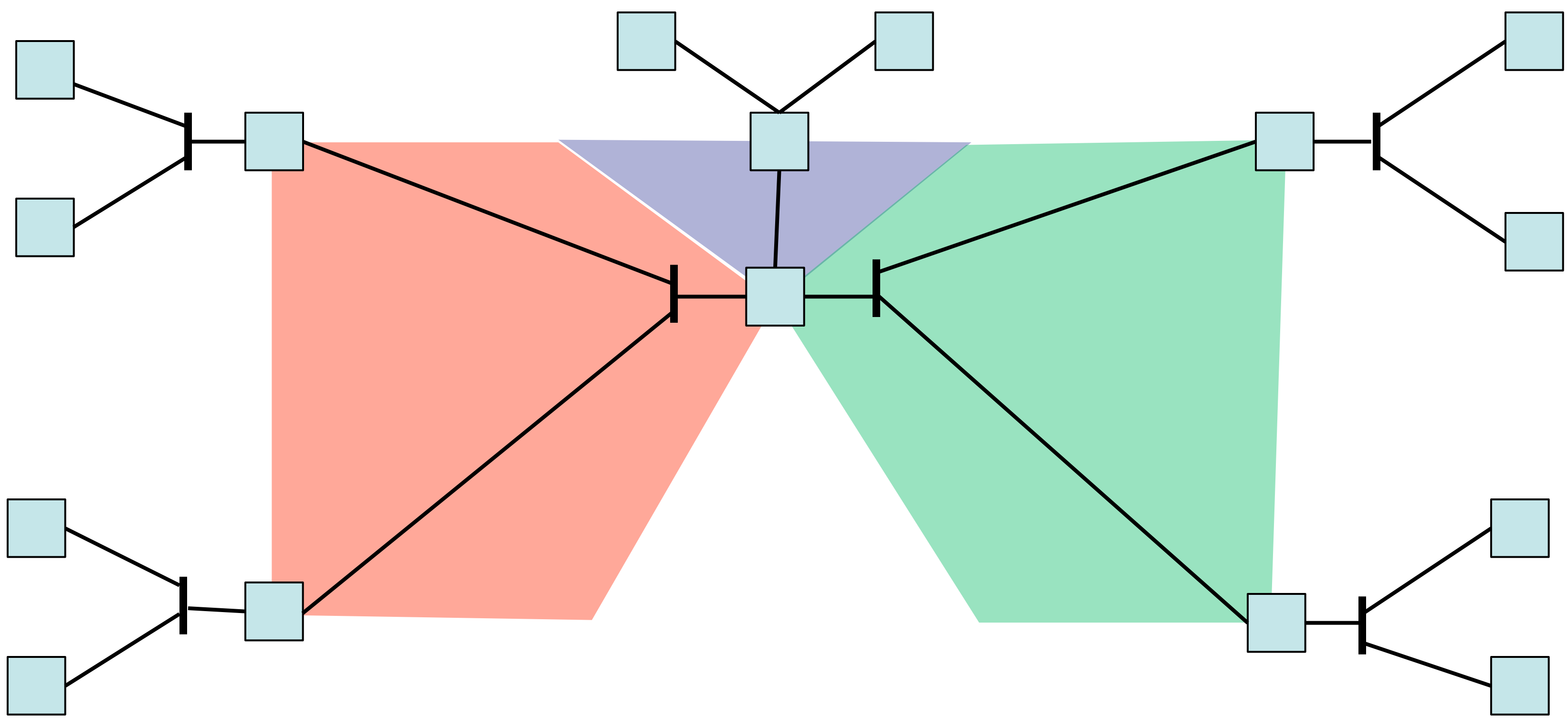
Keying Groups (4)
Group per sending router per interface

- Separate key per router per interface



Keying Groups (4)
Group per sending router per interface

- Separate key per router per interface



Keying Assumptions for RKMP and MaRK

- Both documents make the same statement
  - "Routers need to be provisioned with some credentials for a one-to-one authentication protocol"
  - "Preshared keys or asymmetric keys and an authorization list are expected to be common deployments"

Observations (1)

- To establish the router identities and legitimate adjacencies, this will involve walking to each router and carefully configuring the paired keys and authorization lists
  - Or, at the very least, remotely logging on to each router...
- This seems somewhat error prone to us

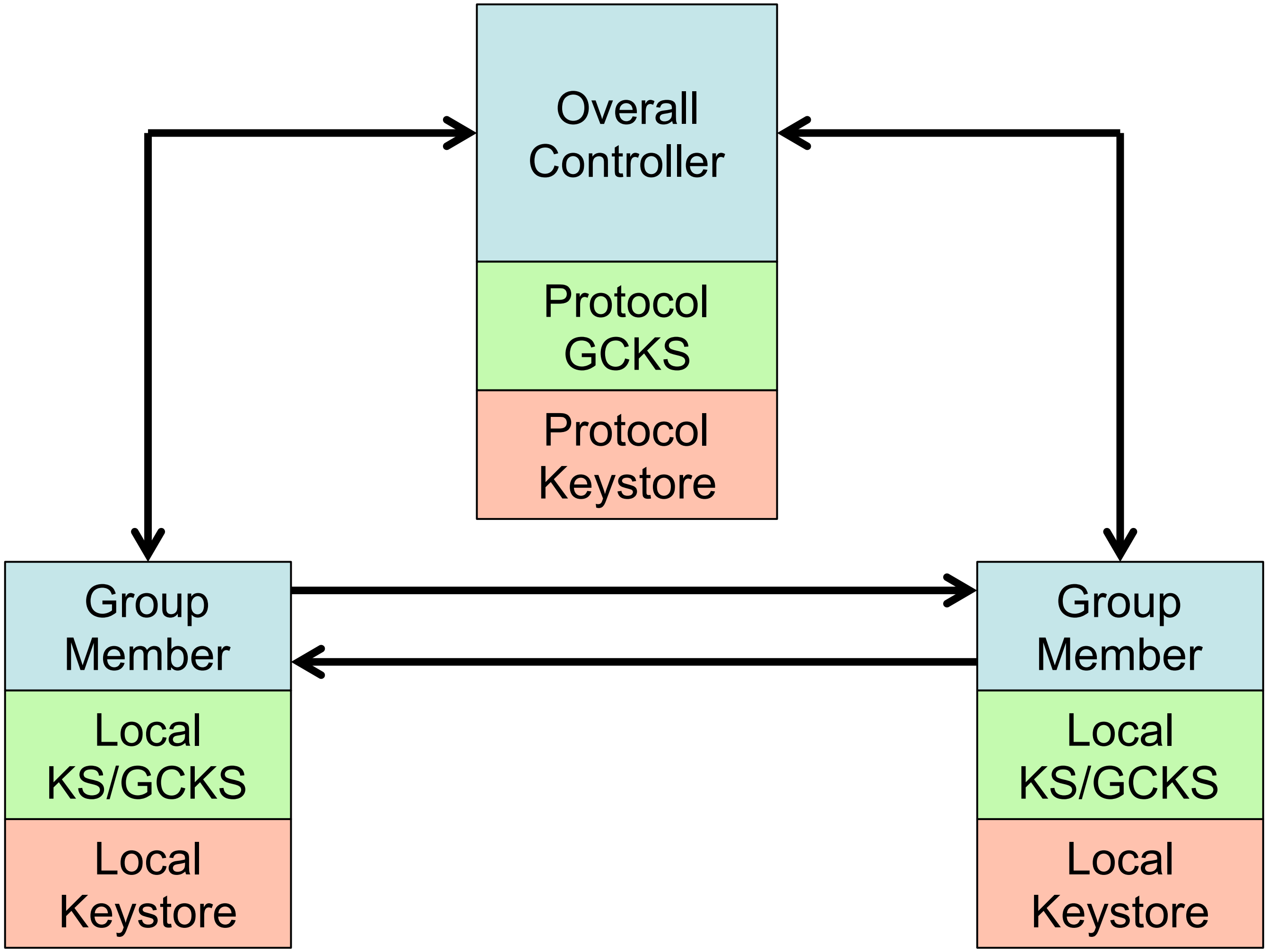
Observations (2)

- Adjacency control has to be centralized
  - No individual router can determine, by itself, who its legitimate neighbors are
- We have explored the issue of key generation in the context of making adjacency management easier.
- The operation of MaRK appears to us to make managing adjacency more difficult
  - Specifically, the election of a GCKS for the routers on a link, which can be different each time it happens.

Our goals

- To explore ways that allow easy adjacency control (which has to be centralized)
- Without depending on a central facility when you have a power failure
- In a manner that works for both the unicast and the multicast cases

Key Management Architecture



Structure

- Two levels for the Automatic Keying Management
  - GCKS ←→ GM Negotiation
  - GM ←→ GM Negotiation
- Four steps
  - Mutual authentication (GCKS ←→ each GM)
  - Push policy and adjacency information on this path
  - Mutual authentication (GM to each adjacent GM)
  - Push or negotiate keying material from GM to/with adjacent GMs

System Goals

- To generate, distribute and update keying materials

- 11 “security goals”
- 6 “non-security goals”

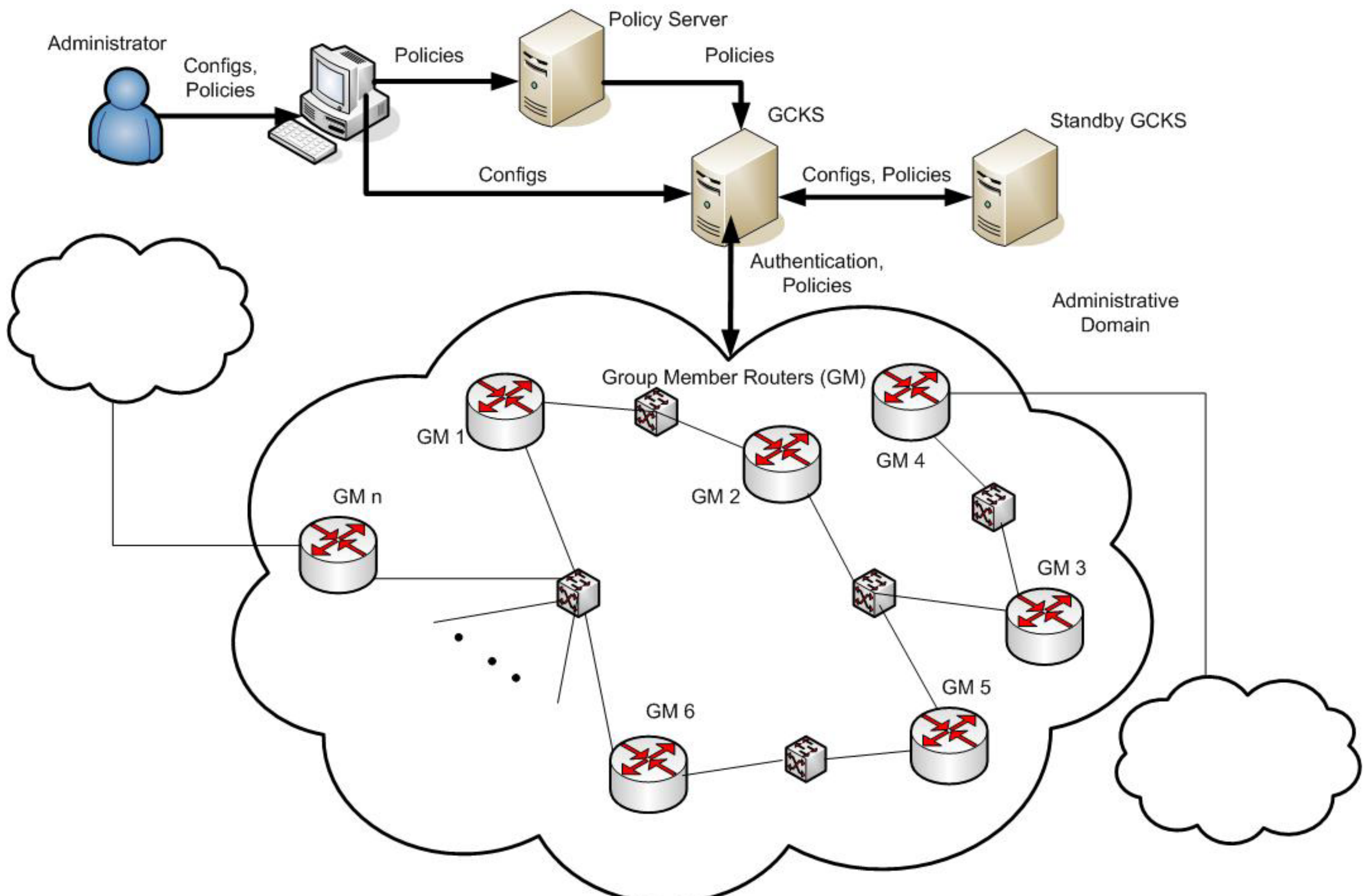
- These were assembled from review of the Design Guide and the Threats and Requirements Guide
- Details are in the draft

Results

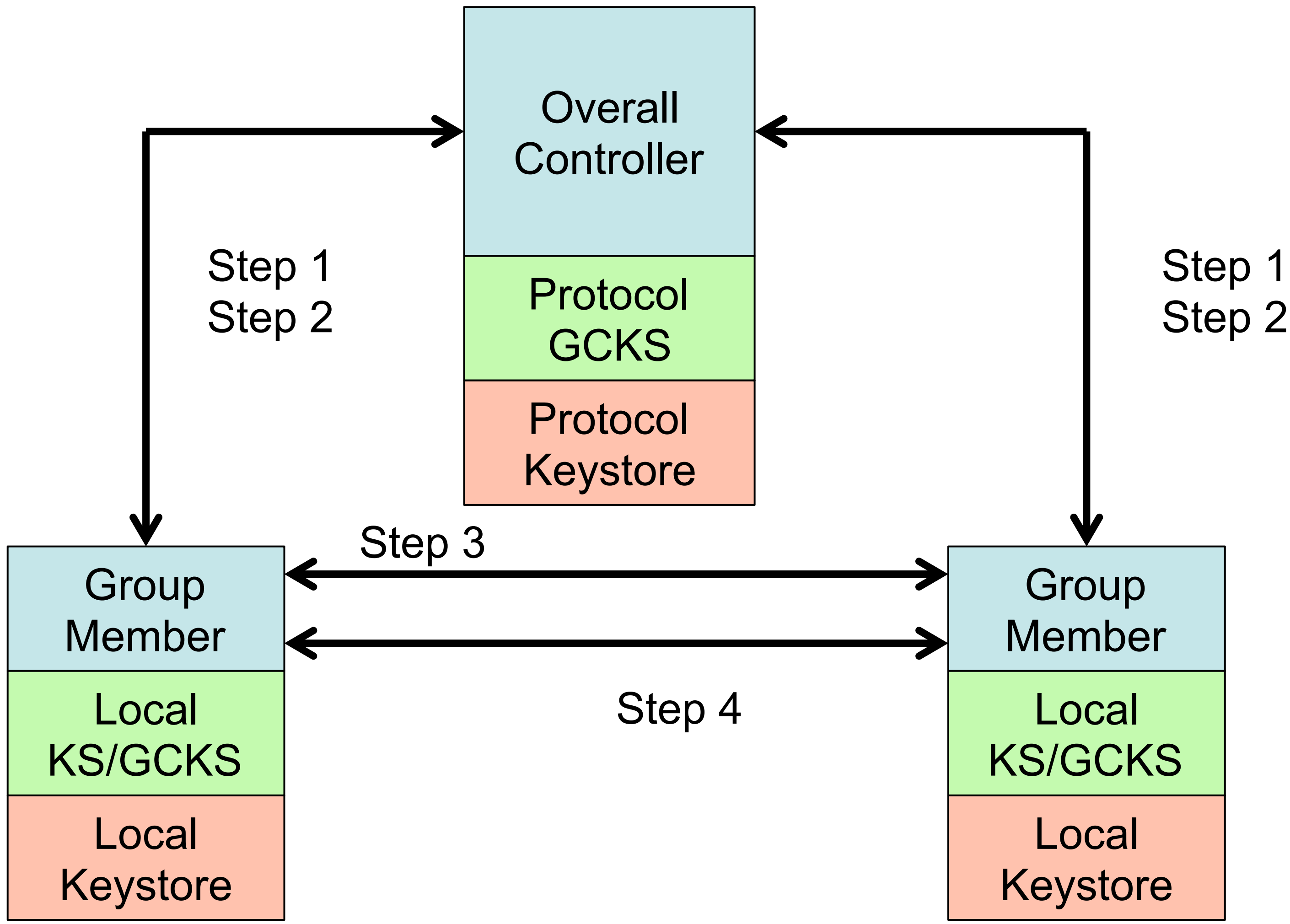
- The framework allows us to simplify the establishment of the pre-shared keys
- Allows us to introduce centralized control of adjacency
- Allows incremental deployment, with different keying models on different interfaces
- Avoids DoS attacks on the central controller after power failure

System architecture

Conforms to the Multicast Group Security Architecture Specification



Key Management Phases: Between Components



System Operation (1)

- Step 1 – Mutual authentication GCKS to GM
  - Establish secure path and mutual authenticity between GCKS and individual Group Members
    - This path will be used to distribute information for use by the GM to identify and authenticate its neighbors
  - Standard IKE or IKEv2 exchange

System Operation (2)

- Step 2 – Push policies to the GM
  - SA policy corresponding to the TEK
  - Signed certificate to identify this router
  - Key scope to be used
  - Policy token
  - Adjacency information
- Plus the necessary hashes and nonces to ensure that the security requirements are met

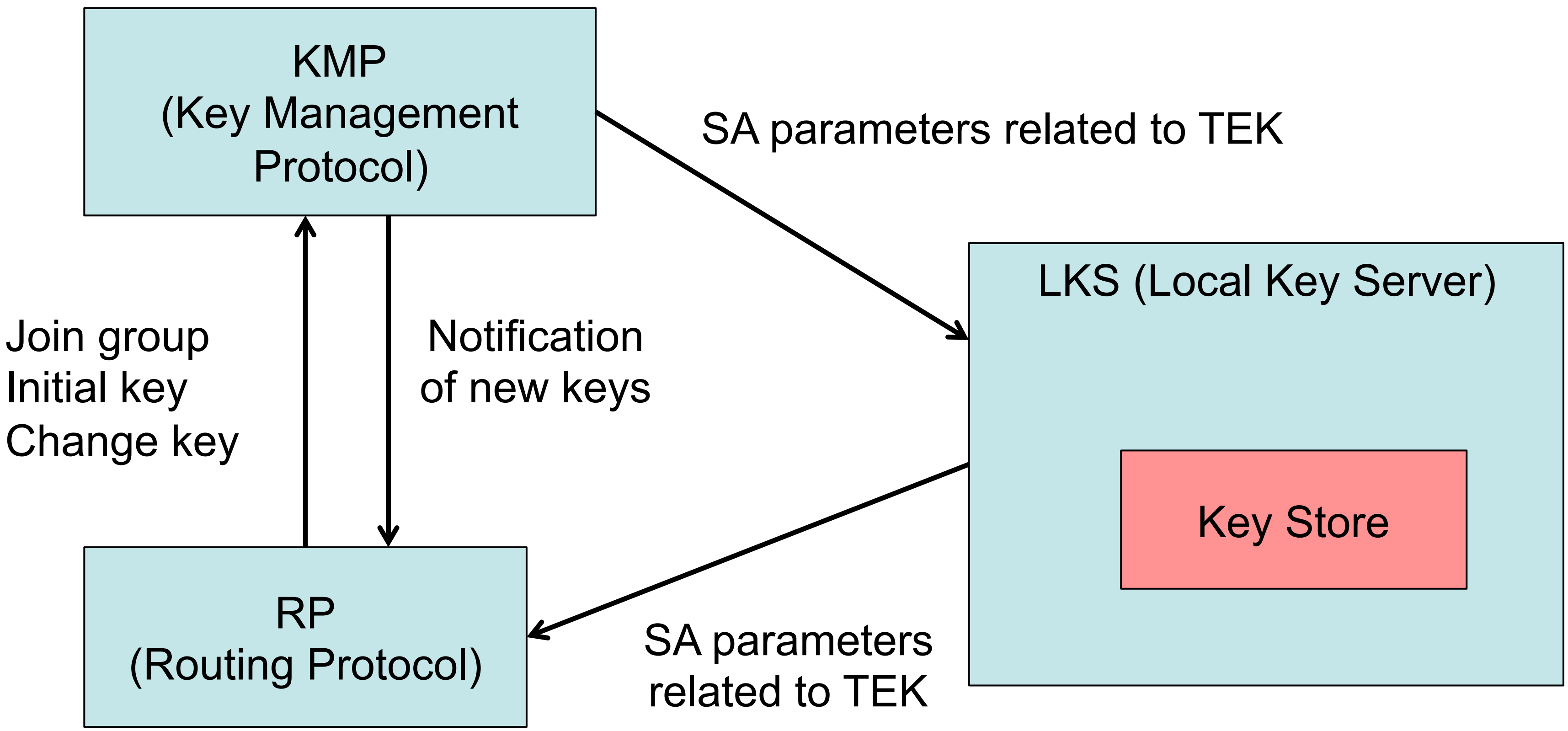
System Operation (3)

- Step 3 – Mutual Authentication between adjacent GMs
  - 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)
  - The identity information pushed in Step 2 is used to identify legitimate neighbors
  - Standard IKE or IKEv2 exchange

System Operation (4)

- Step 4 – Exchange or negotiation of keying materials
  - SA information corresponding to the TEK of the sending router
  - Request for SA information corresponding to the TEK of neighbor routers
- Plus the necessary hashes and nonces to ensure that the security requirements are met

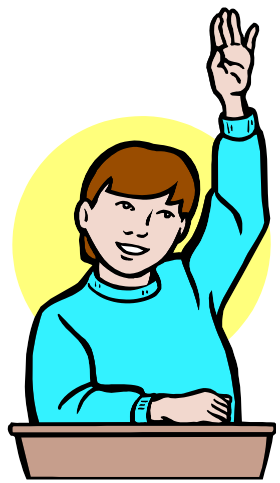
Key Management Exchanges: Within GMs



Academic Aspects

- Formal validation of the security of the protocols has been done, using AVISPA (Automated Validation of Internet Security Protocols and Applications)
- GCKS and GMs are modeled
- Intruder can take any role
- Security goals (for example, secrecy of the generated TEK) can be formulated
- AVISPA reports “safe” for the set of security goals and scenarios explored

Thank You!



Questions?