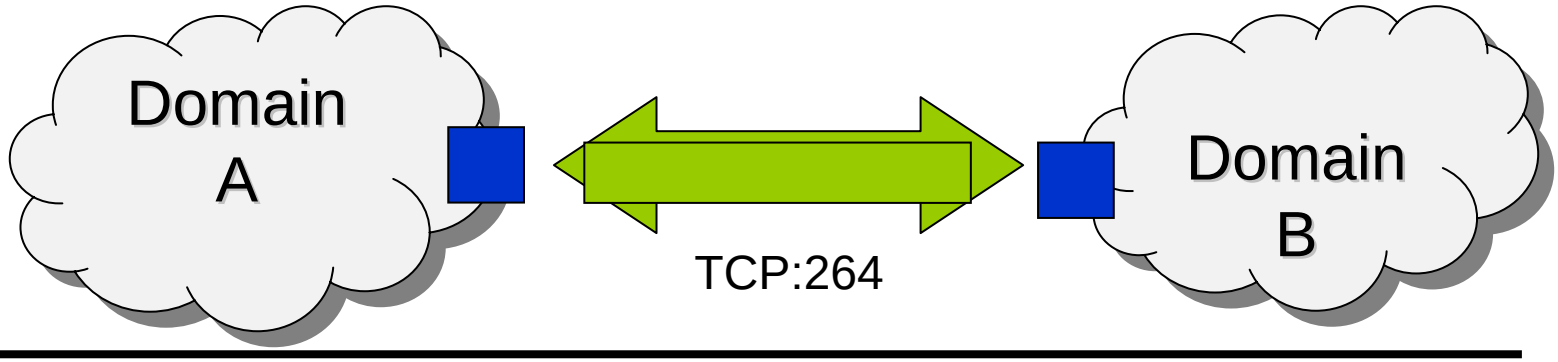
Border Gateway Multicast Protocol

1. Introduction

2. Tasks and Rules of Border Routers

????

- protocol for inter-domain multicast routing
- run by the border routers of a domain
- constructs inter-domain
  bidirectional shared trees
- allows any existing multicast routing protocol
  to be used within individual domains

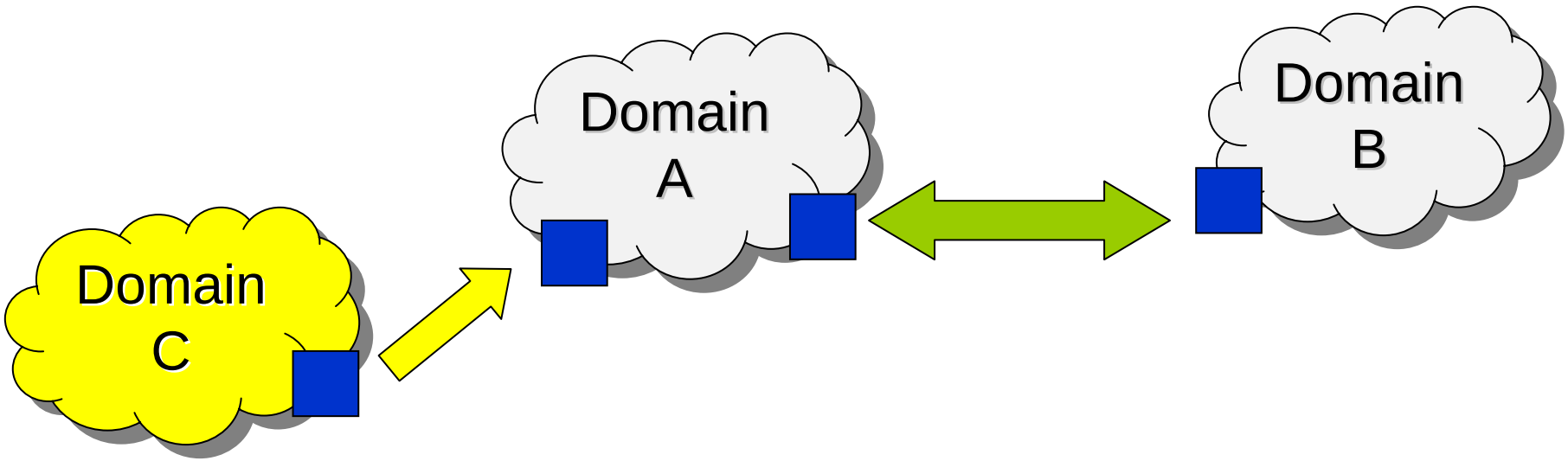


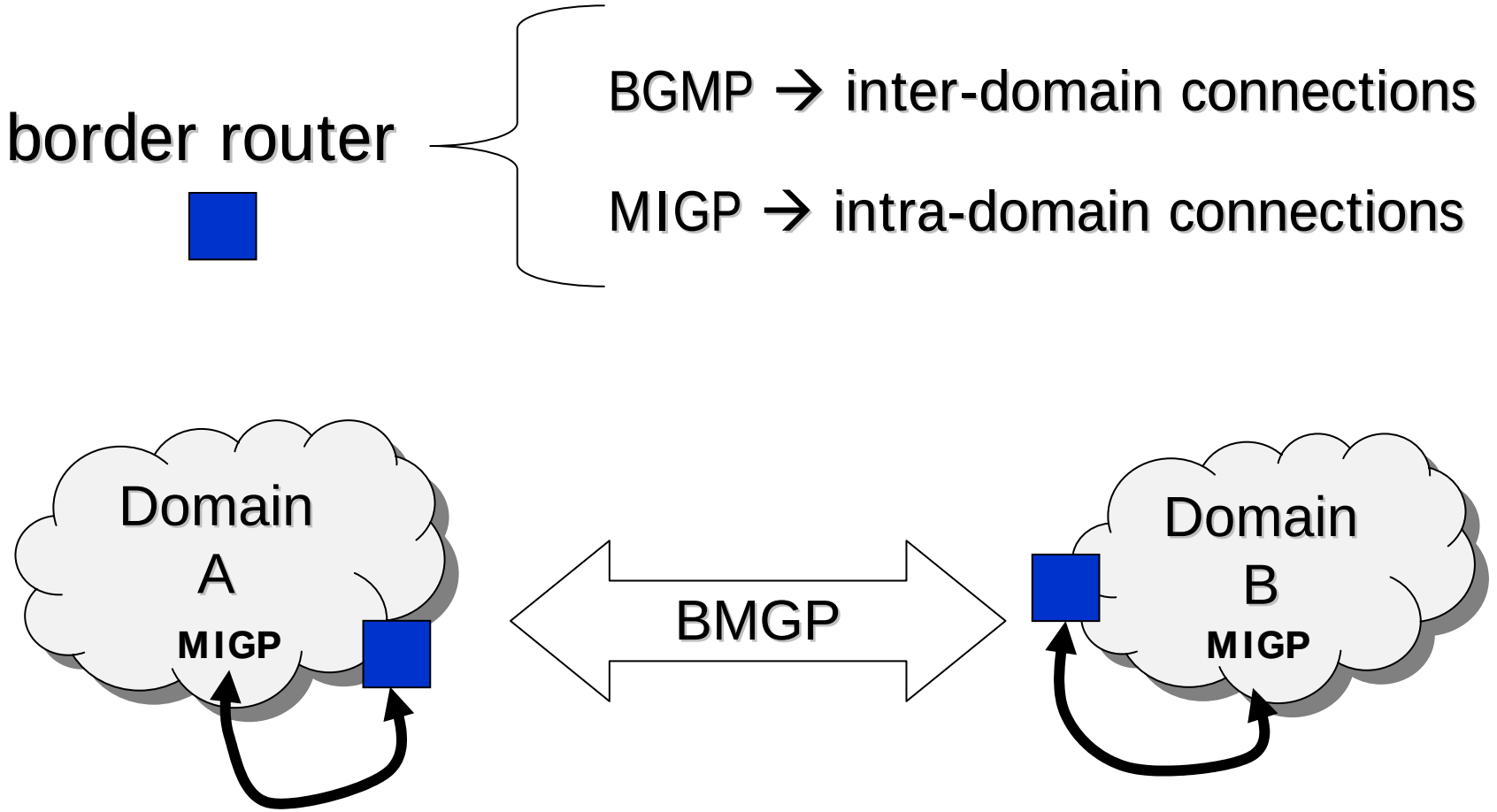
BGMP uses TCP:

→ no need for implementation of:

- message fragmentation
- retransmission
- acknowledgement
- sequencing

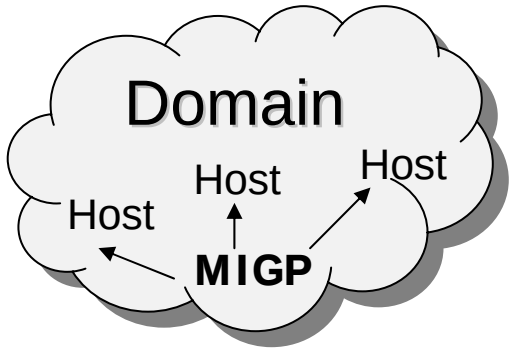
- border routers build:
  - group specific bidirectional branches
  - and source specific unidirectional branches where needed



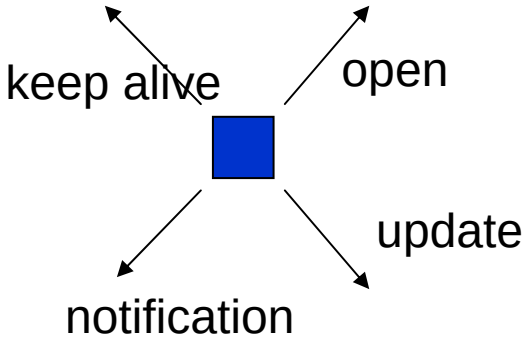

border router
BGMP → inter-domain connections
MIGP → intra-domain connections
Domain A
MIGP
BMGP
Domain B
MIGP

Multicast Interior Gateway Protocol (MIGP):

A generic term for any multicast routing protocol used for tree construction within a domain.
Typical examples are: PIM-SM, PIM-DM, DVMRP, MOSPF and CBT



messages used by border routers:



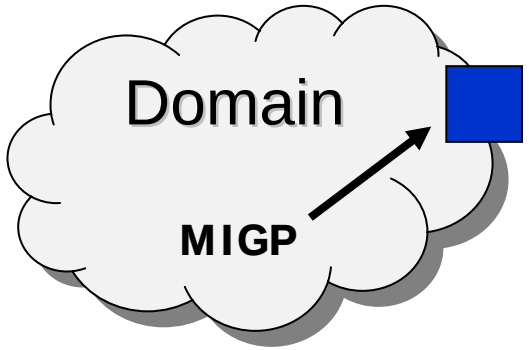
- open
  → first message sent by each side
- keep alive
  → (periodically) to ensure the liveliness
  of the connection and to confirm “open”
- update
  → update if group memberships change
  (via join/prune/source or group messages)
- notification
  → response to errors or special conditions

messages used by border routers:

- processed only after entirely received
- maximum size: 4096 octets
- all implementations are required to support this maximum message size

forwarding-rules used by border routers:

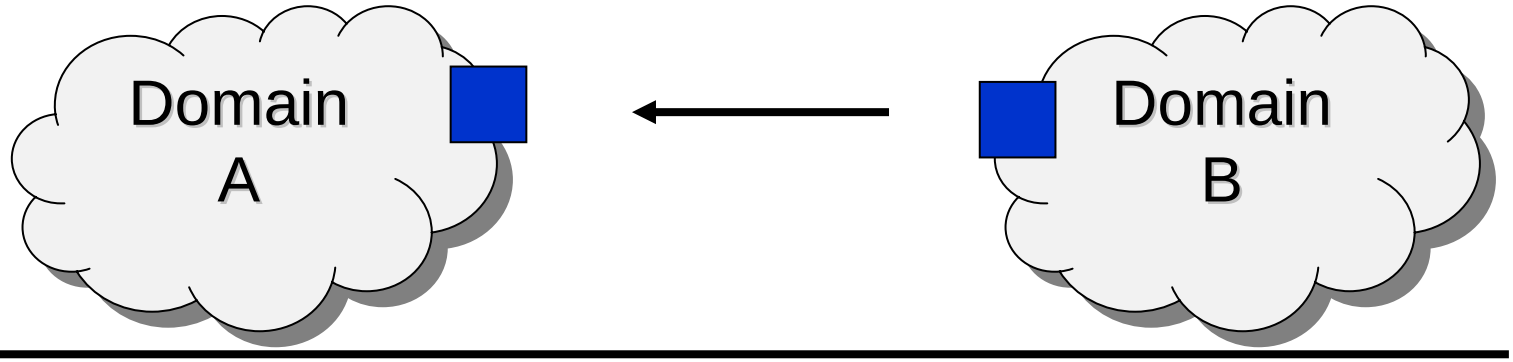
if arrives on an MIGP interface
→ accepted and forwarded according to MIGP rules



forwarding-rules used by border routers:

if arrives over a point-to-point BGMP interface
(and the packet got accepted)

1. targets listed in (S,G) entry (source specific)
2. targets listed in (*,G) entry (bidirectional)
3. next hop towards the group



forwarding-rules used by border routers:

a packet will be dropped if:

- it was not received by the next hop target towards the group or the source

after dropping the packet no further actions are taken.

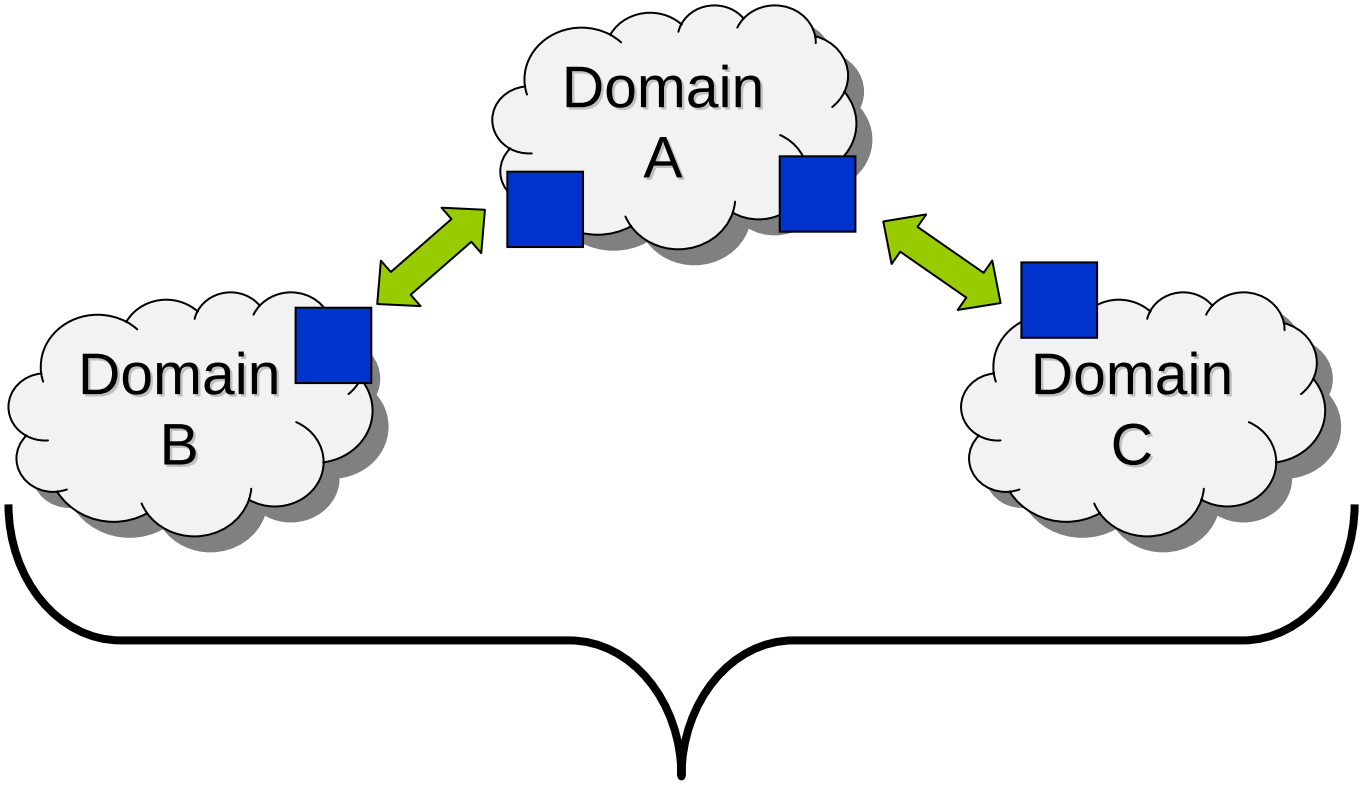
What is this good for??

⇨ IP Multicast

- Multimedia teleconferencing
- Distance learning
- Data replication
- Network games

4. Bidirectional Trees

4.1 Method of choosing the root

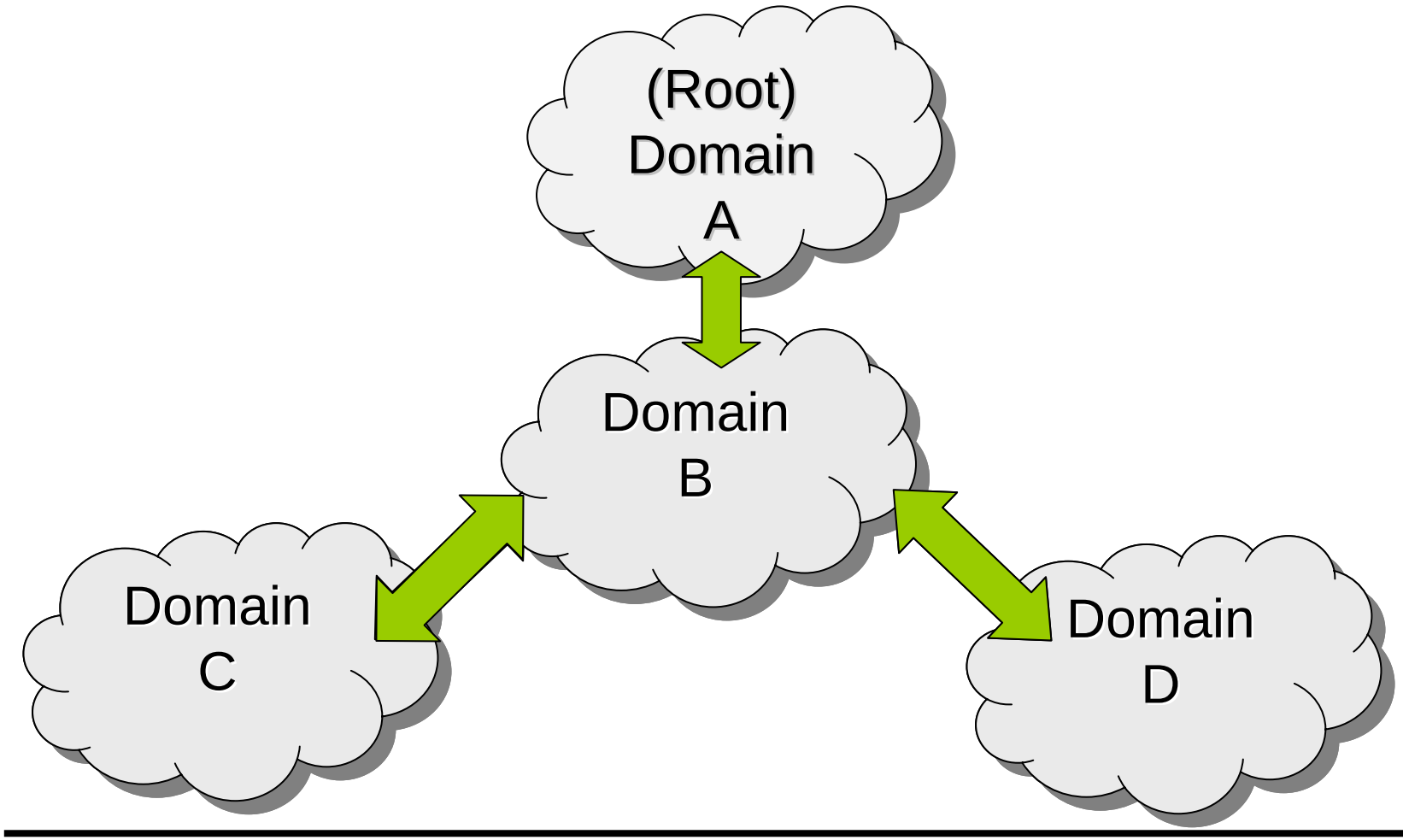


Bidirectional Trees:

- minimize third party dependencies
- improve performance
- more efficient

4.1. Third Party Dependency

4.2 Method of choosing the root



Method of choosing the root for the shared tree:

Intra-domain shared tree protocols:

- all routers are treated as equivalent candidates
- it is a more or less random choice (depending on load sharing and stability)

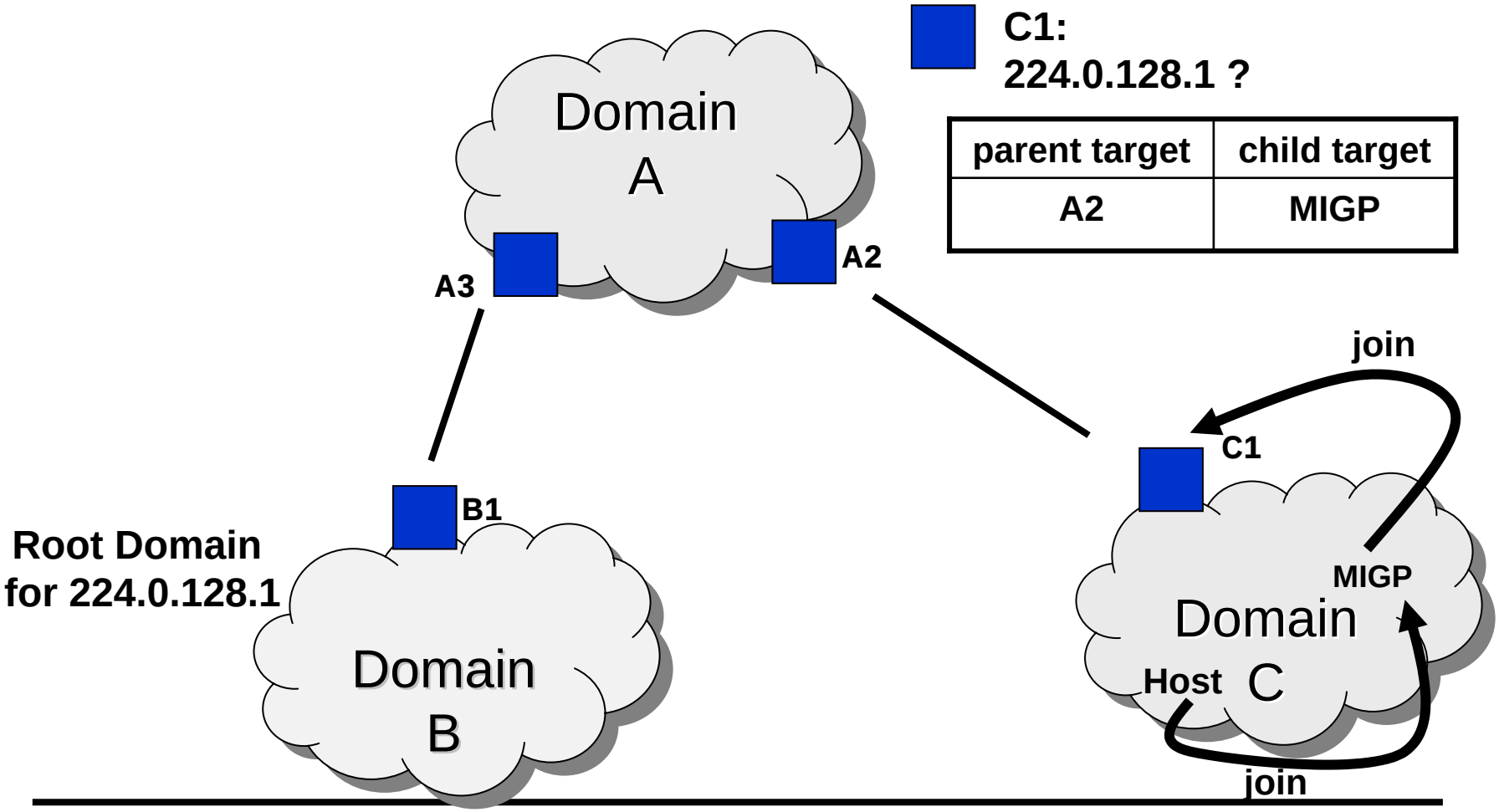
Method of choosing the root for the shared tree:

In BGMP:

- the choice of a group's root is subject to administrative control (depending e.g. on poor locality)
- usually rooted at the domain of the initiator of the group

4.3. Establishing the bidirectional shared tree

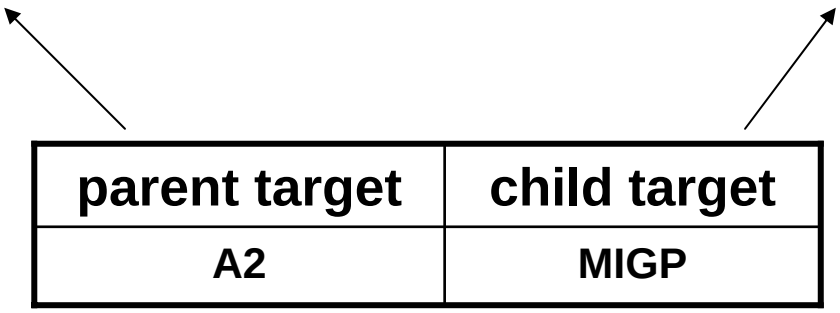
4.4 Data from external domains



4.3. Establishing the bidirectional shared tree

BGMP peer, that is the next hop towards the group's root domain

BGMP peer or MIGP component, from which a join request was received



parent target	child target
A2	MIGP

= target list / multicast-group forwarding entry

C1

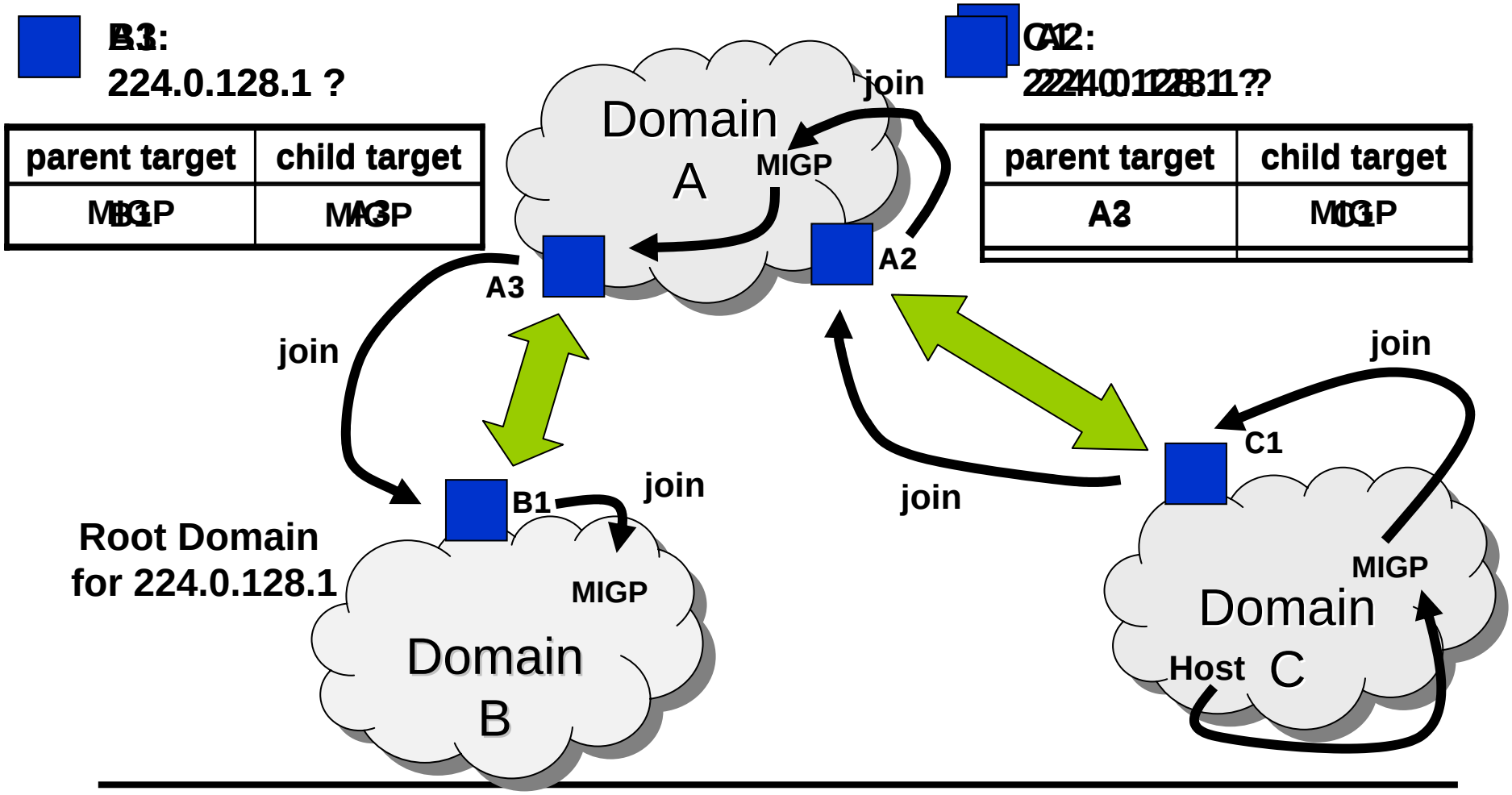
parent target	child target
A2	MIGP

(*,G) entry

Packets from any (*****) source send to the **G**roup
received by the border router
are to be forwarded to all the targets in the list
except to the sender itself.

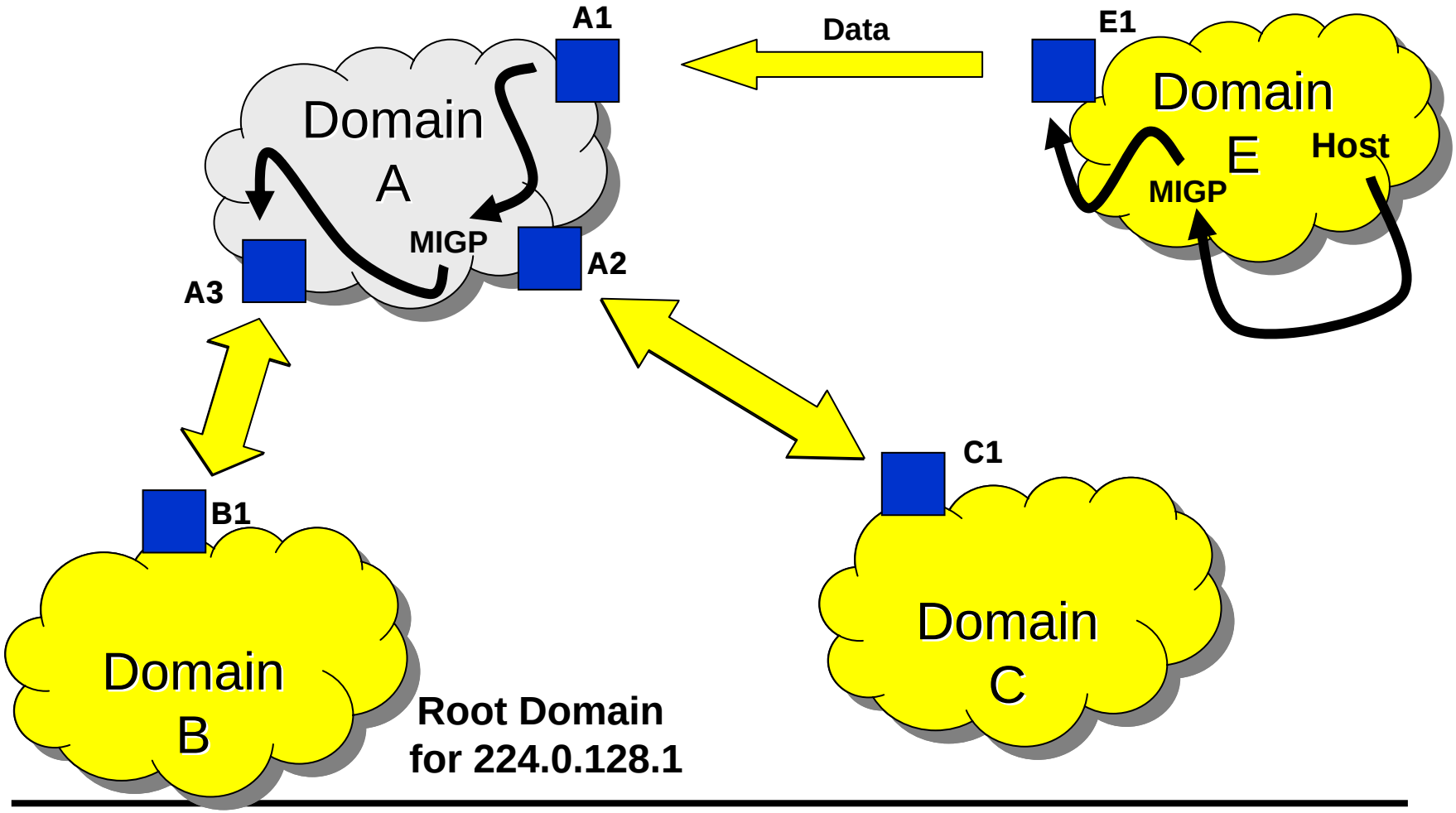
4.3. Establishing the bidirectional shared tree

4.4 Data from external domains



4.4. Data from external domains

5. Source specific Branches/Trees



5. Source Specific Branches/Trees

5.1 Establishing source specific Branches/Trees

source specific trees are used:

- to be compatible with source specific trees used by the MIGP (e.g. source rooted intra domain trees built by DVMRP and PIM-DM)
- or to construct trees for source specific groups

5. Source Specific Branches/Trees

5.1 Establishing source specific Branches/Trees

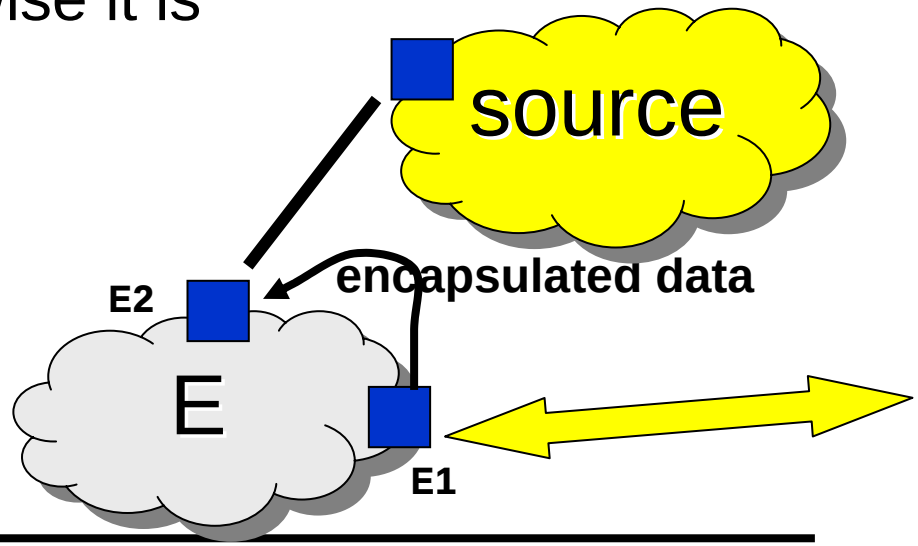
source specific branches/trees are built ONLY when:

- it is needed to pull traffic down to a BGMP router that has a source-specific (S,G) state
- AND it is not yet in the shared tree
- AND the router does not want to receive packets by encapsulation from a router in the shared tree

RPF (**R**everse **P**ath **F**orwarding) check:

Data gets forwarded, if it arrives on a device which the router claims as a part of the shortest path to the source (*E2*). Otherwise it is supposed as duplicate data and gets dropped.

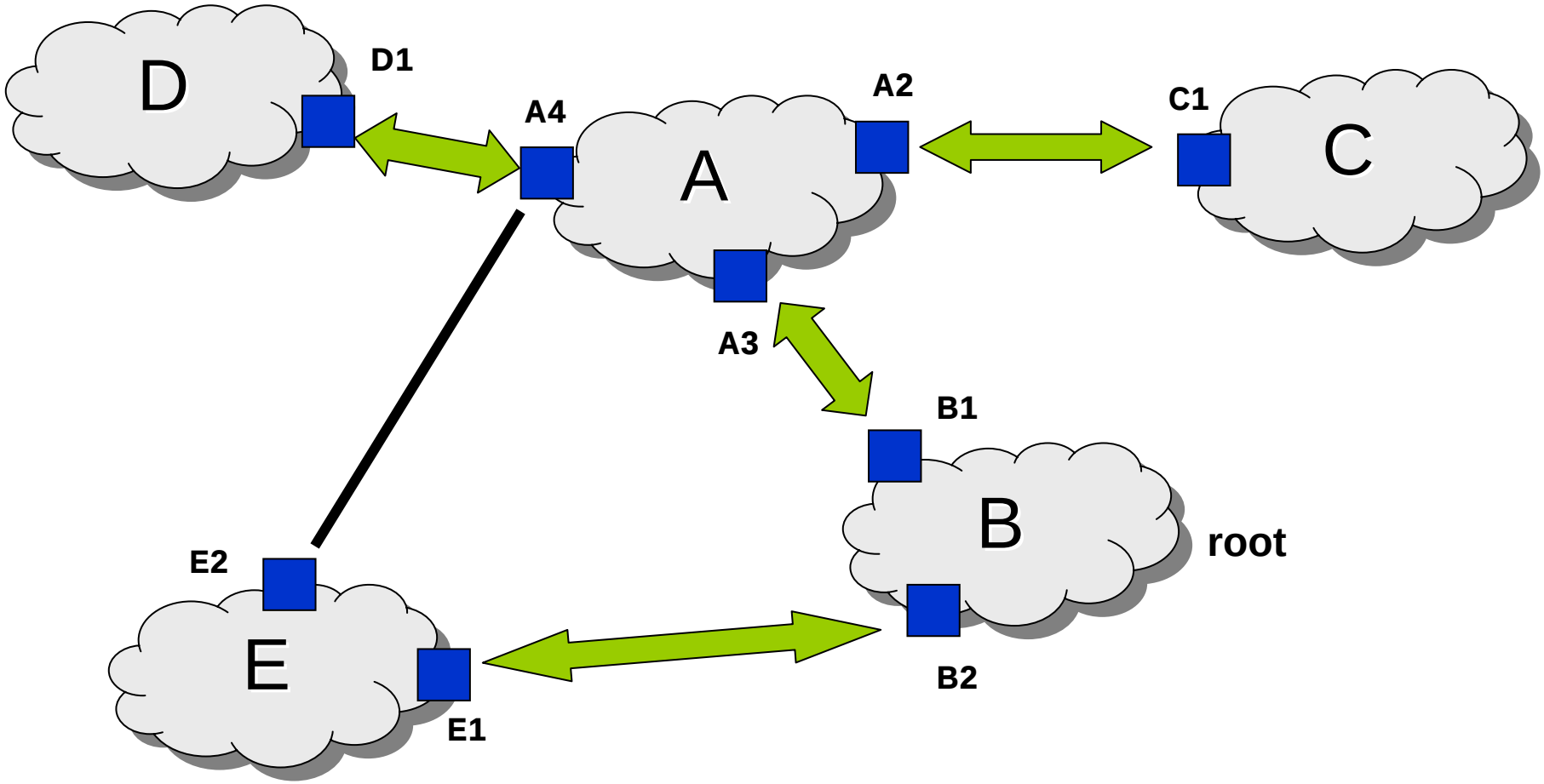
Therefore data packets need to be encapsulated to be accepted by other routers (→ overhead!).



Otherwise not source specific because:

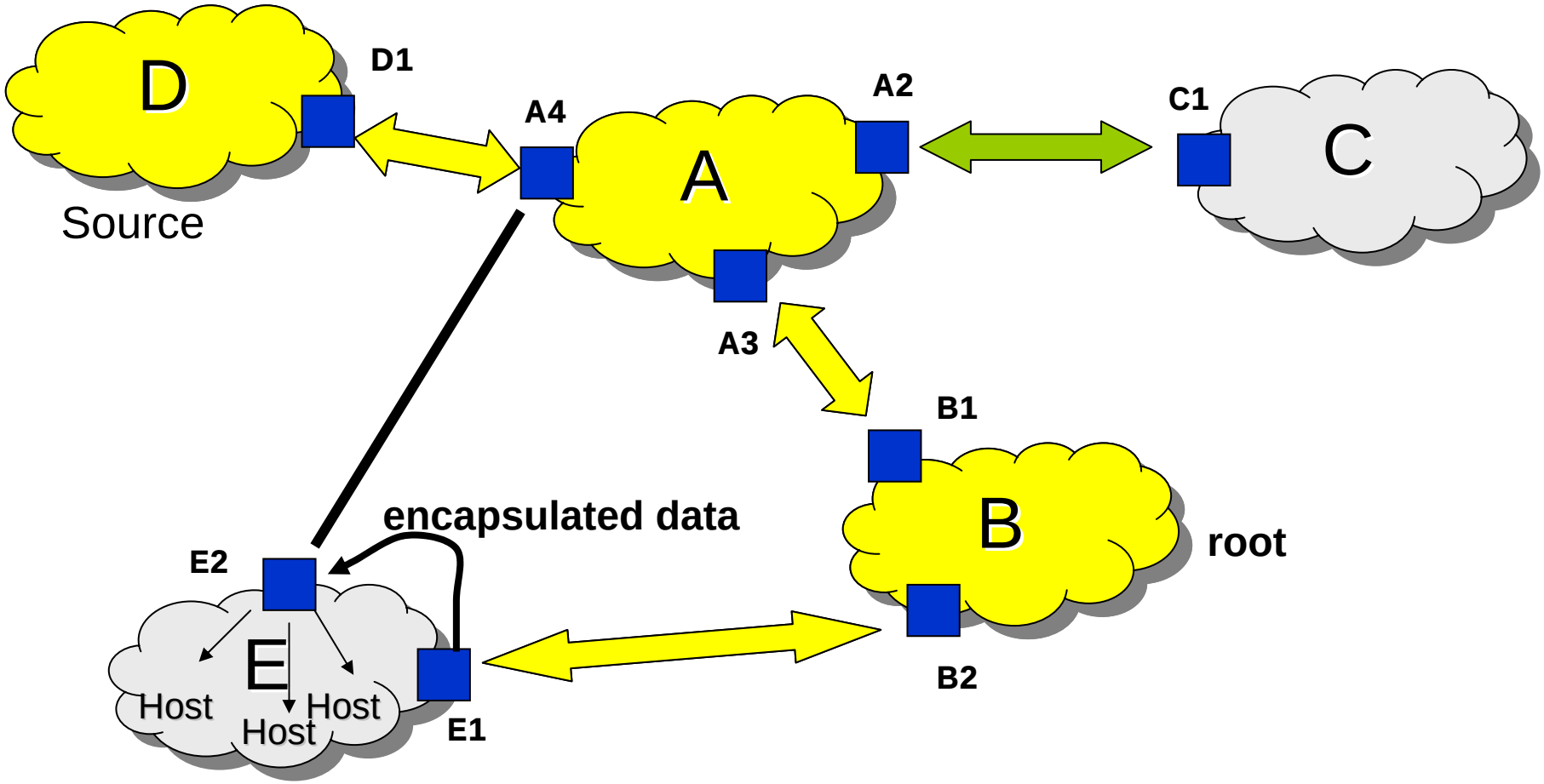
- inter-domain connectivity is small
  → shared distribution trees have acceptable path length and traffic concentration
- by having the shared tree state precedence over the source specific tree, ambiguities are avoided

5.1. Establishing Source Specific Branches/Trees

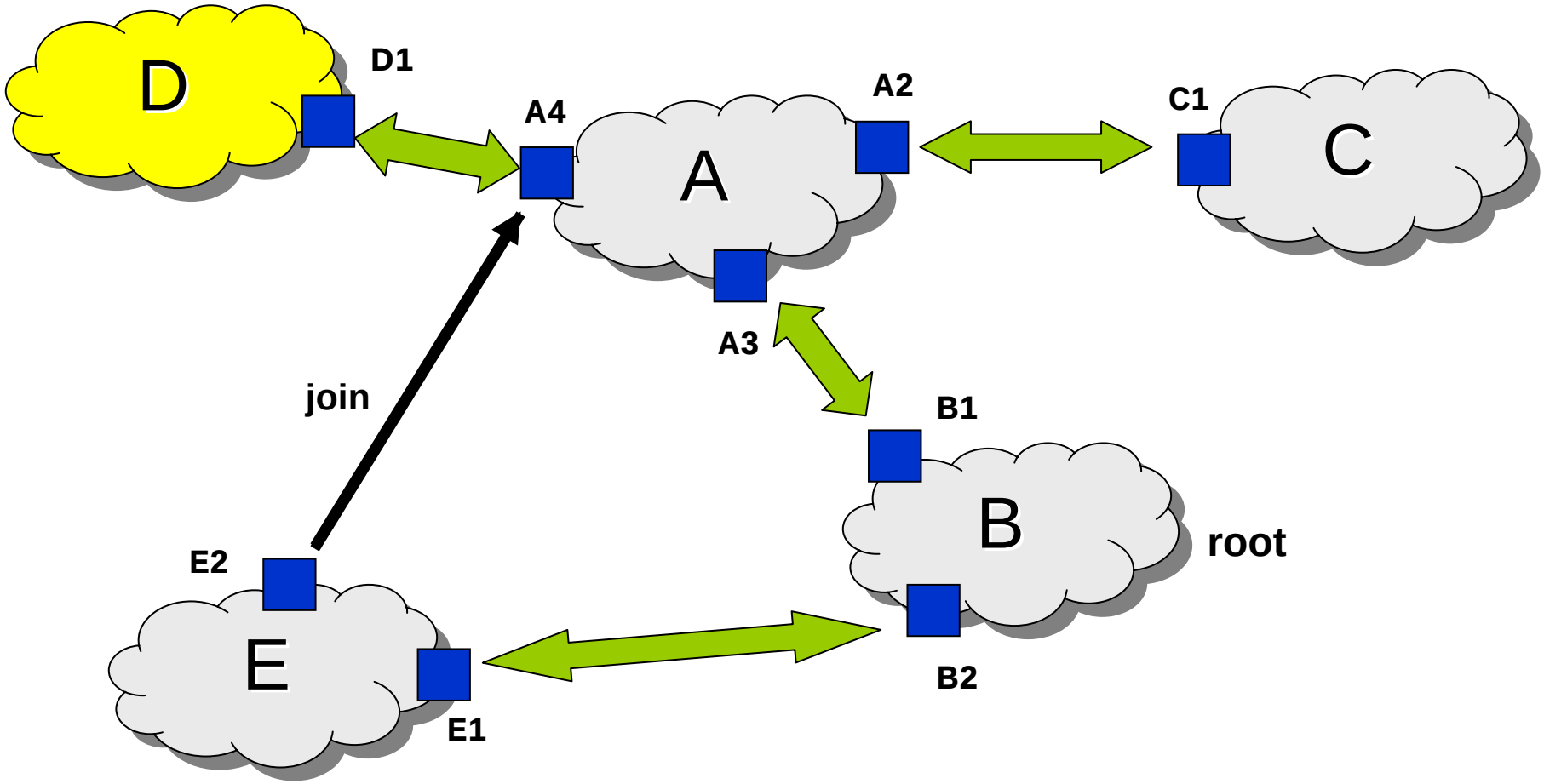


5.1. Establishing Source Specific Branches/Trees

6. Security



5.1. Establishing Source Specific Branches/Trees

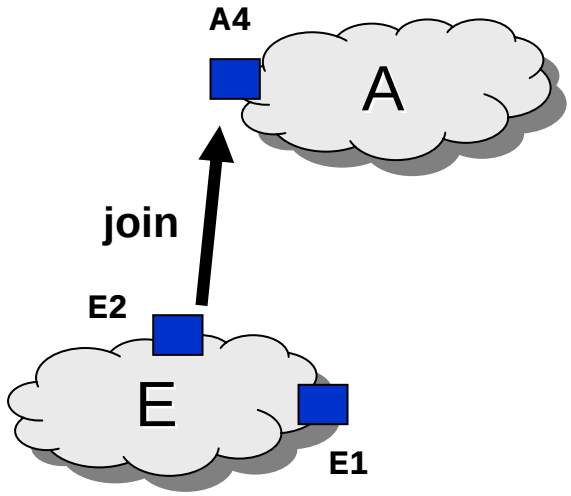


5.1. Establishing Source Specific Branches/Trees

The next hop towards the source S

BGMP peer or MIGP component, from which a join request was received

parent target	child target
A4	MIGP

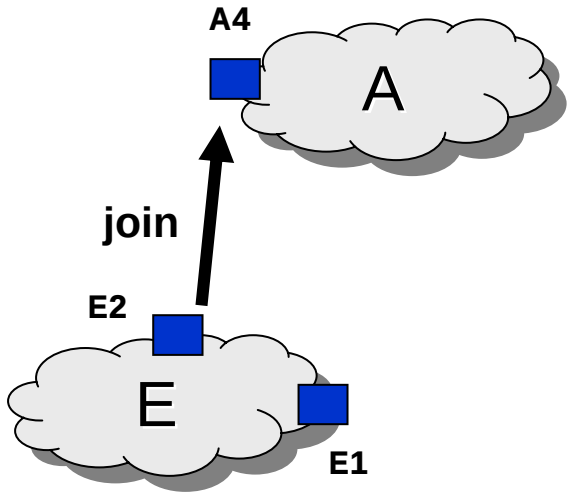


= target list / multicast forwarding entry

E2

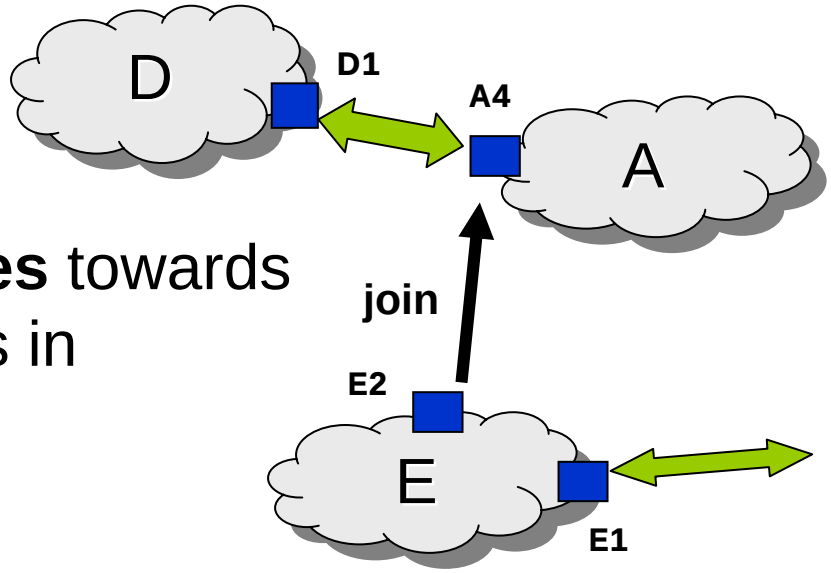
parent target	child target
A4	MIGP

(S,G) entry



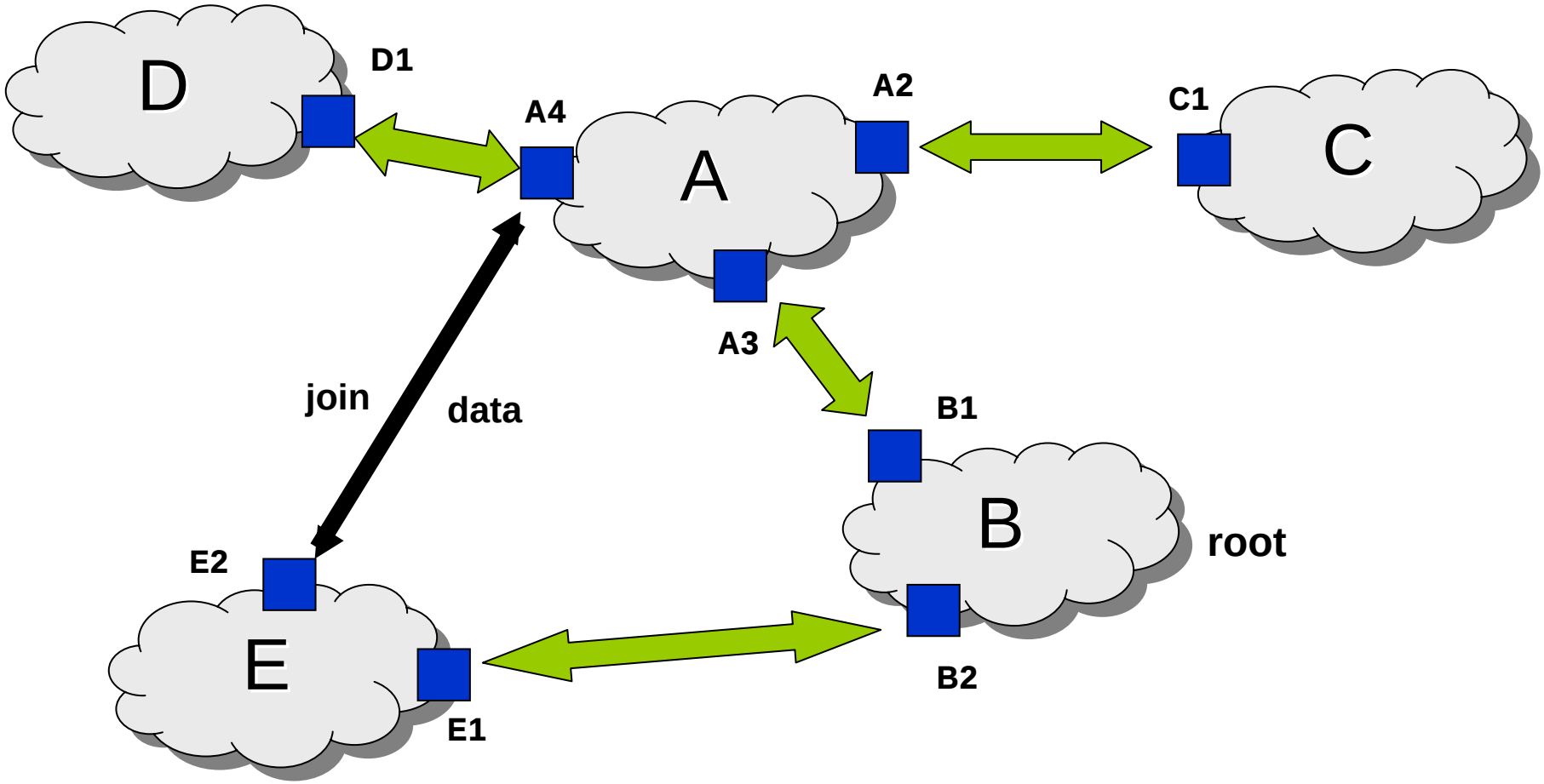
Packets that arrive from the parent target will be accepted and forwarded to all the targets listed in the (S,G) entry (unidirectional)

(S,G) entry

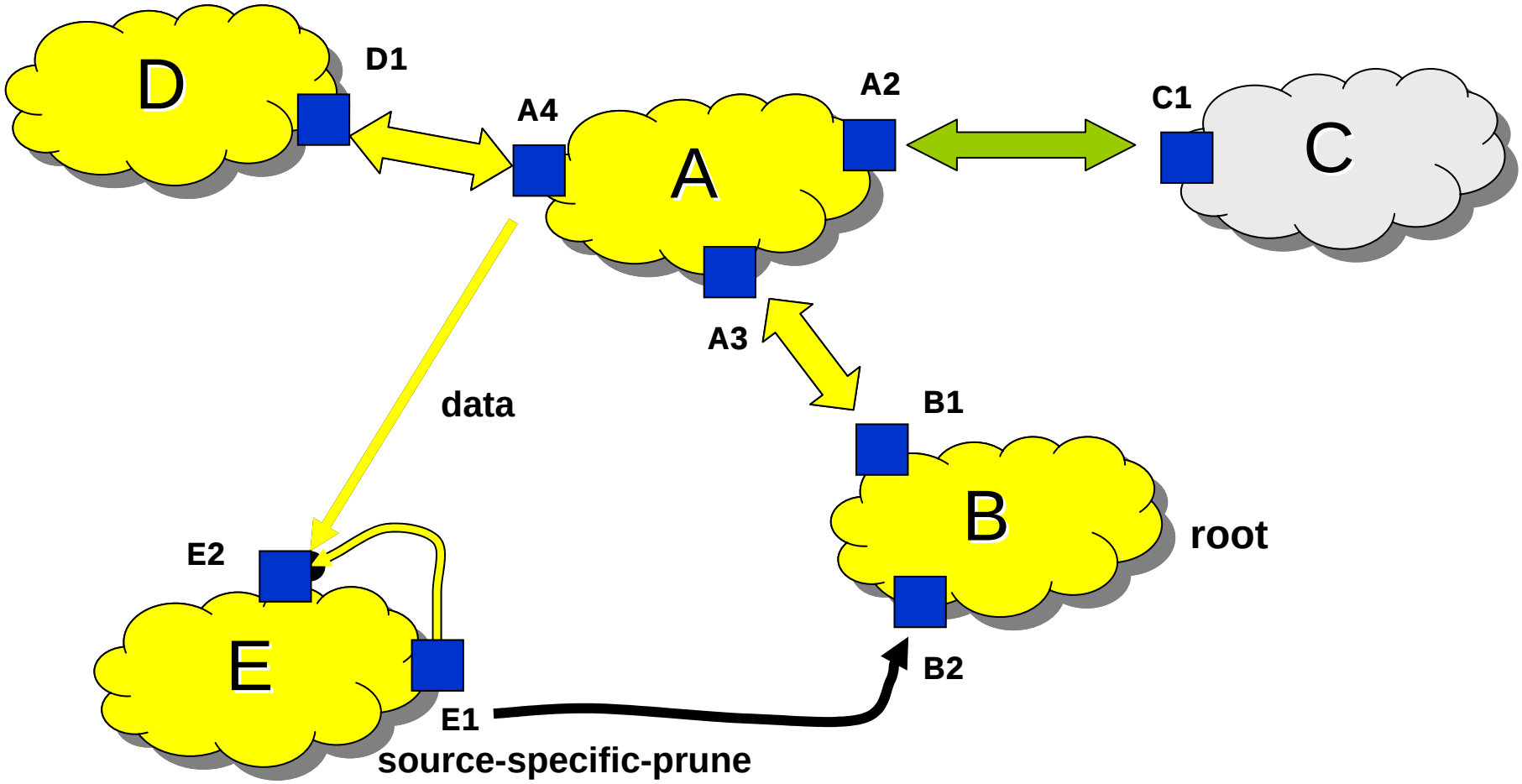


The source specific join **propagates** towards the source setting up (S,G) entries in the border routers **until** it reaches a border router that is in the **shared tree** for the group

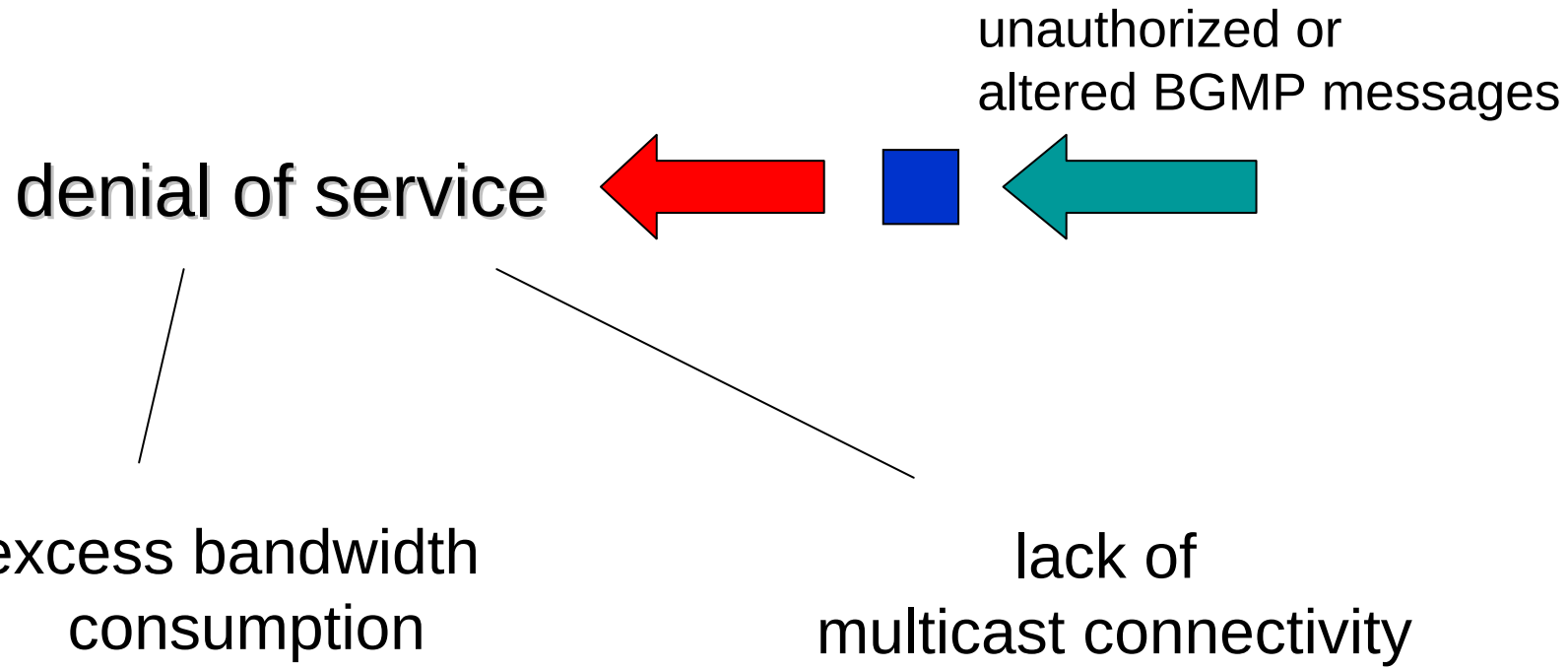
5.1. Establishing Source Specific Branches/Trees



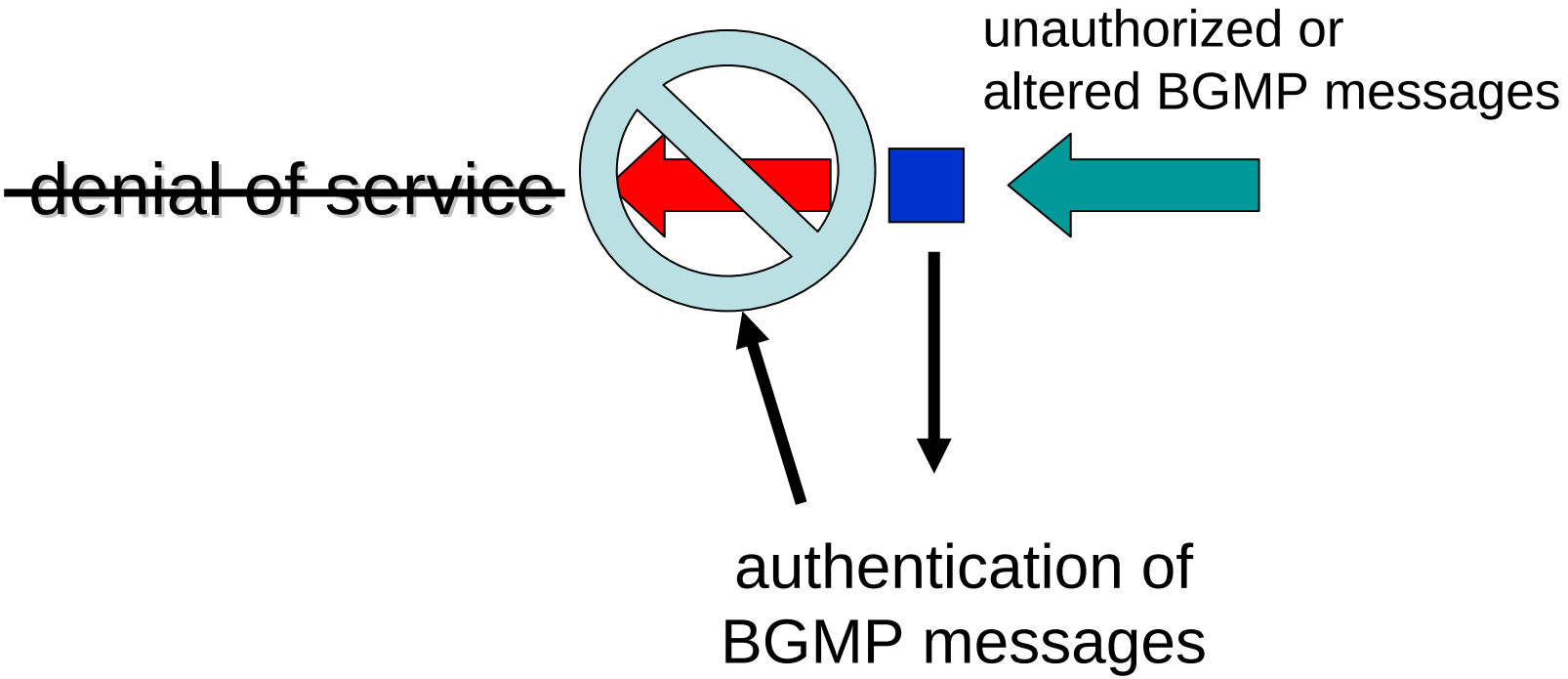
5.1. Establishing Source Specific Branches/Trees



6. Security

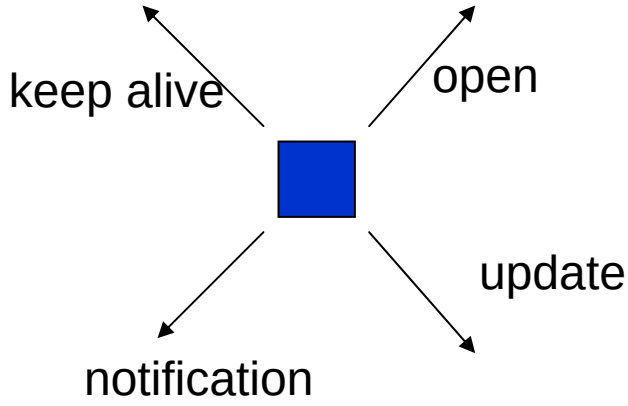

unauthorized or
altered BGMP messages
denial of service
excess bandwidth
consumption
lack of
multicast connectivity

6. Security


unauthorized or
altered BGMP messages
denial of service
authentication of
BGMP messages

6. Security

To secure control messages, keyed MD5 (RFC2385) must be implemented




Thank you!