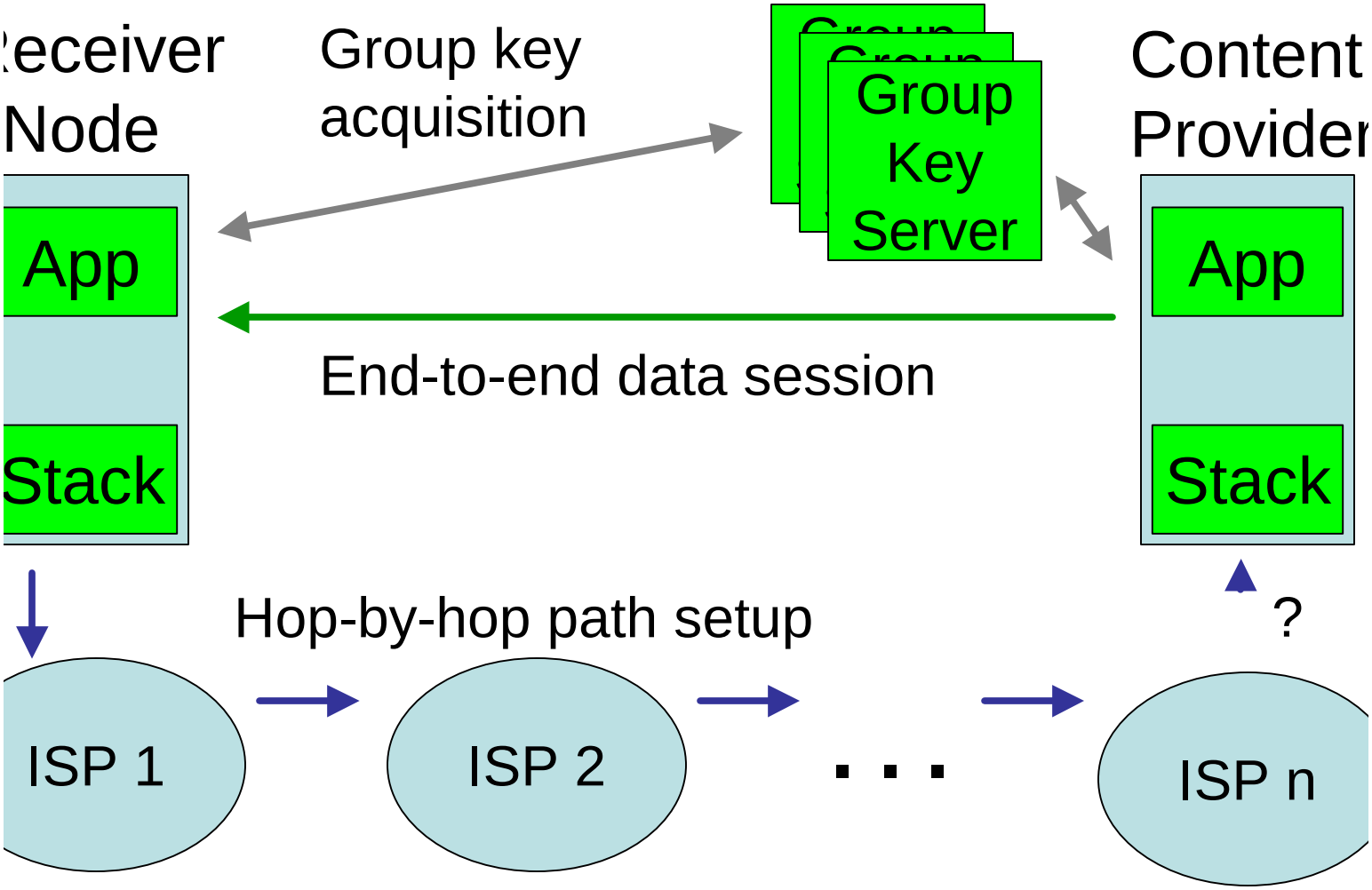
# Non-IGMP-specific security

or “Why not to do security at the IGMP level”

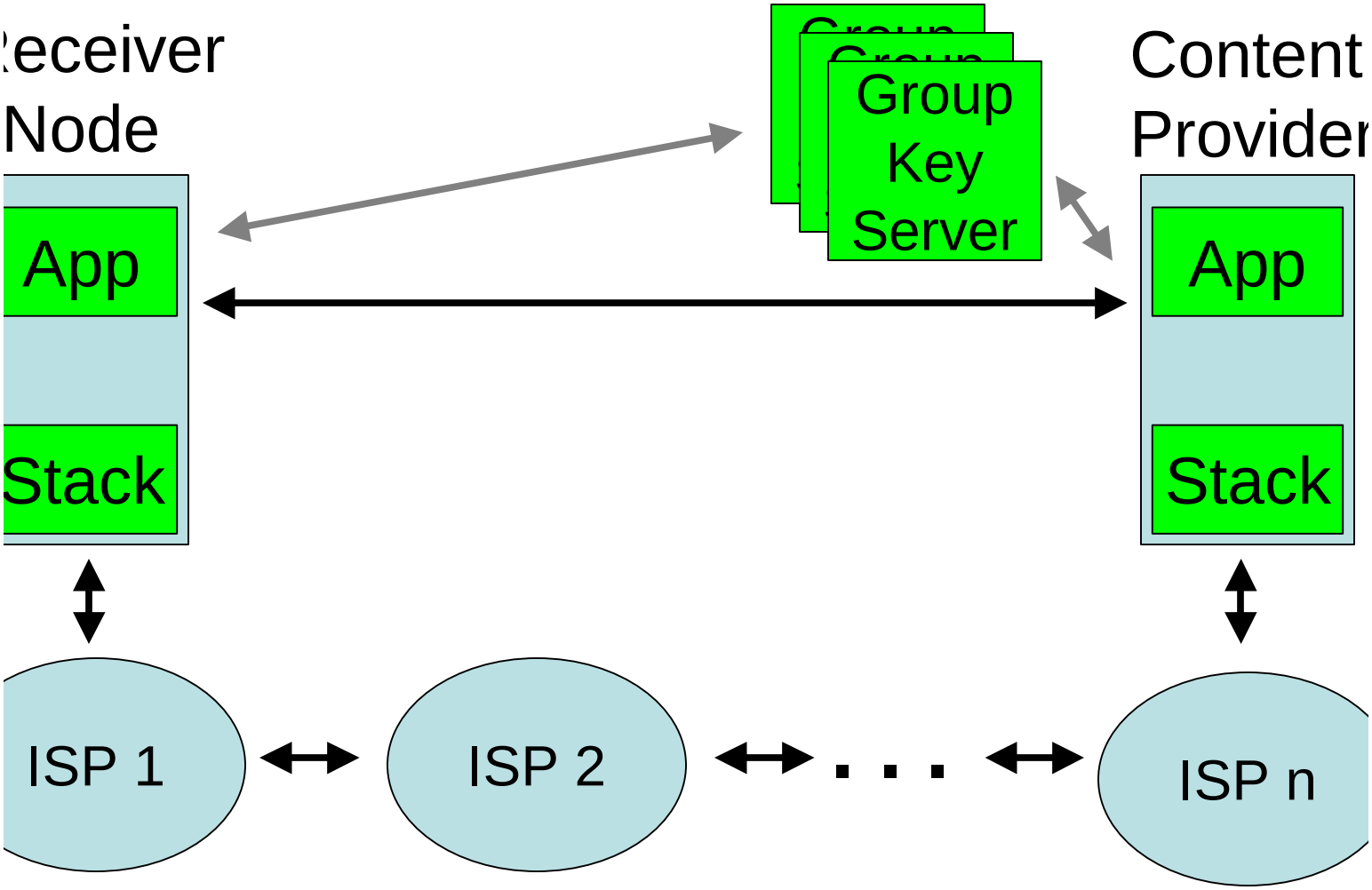
Dave Thaler

dthaler@microsoft.com

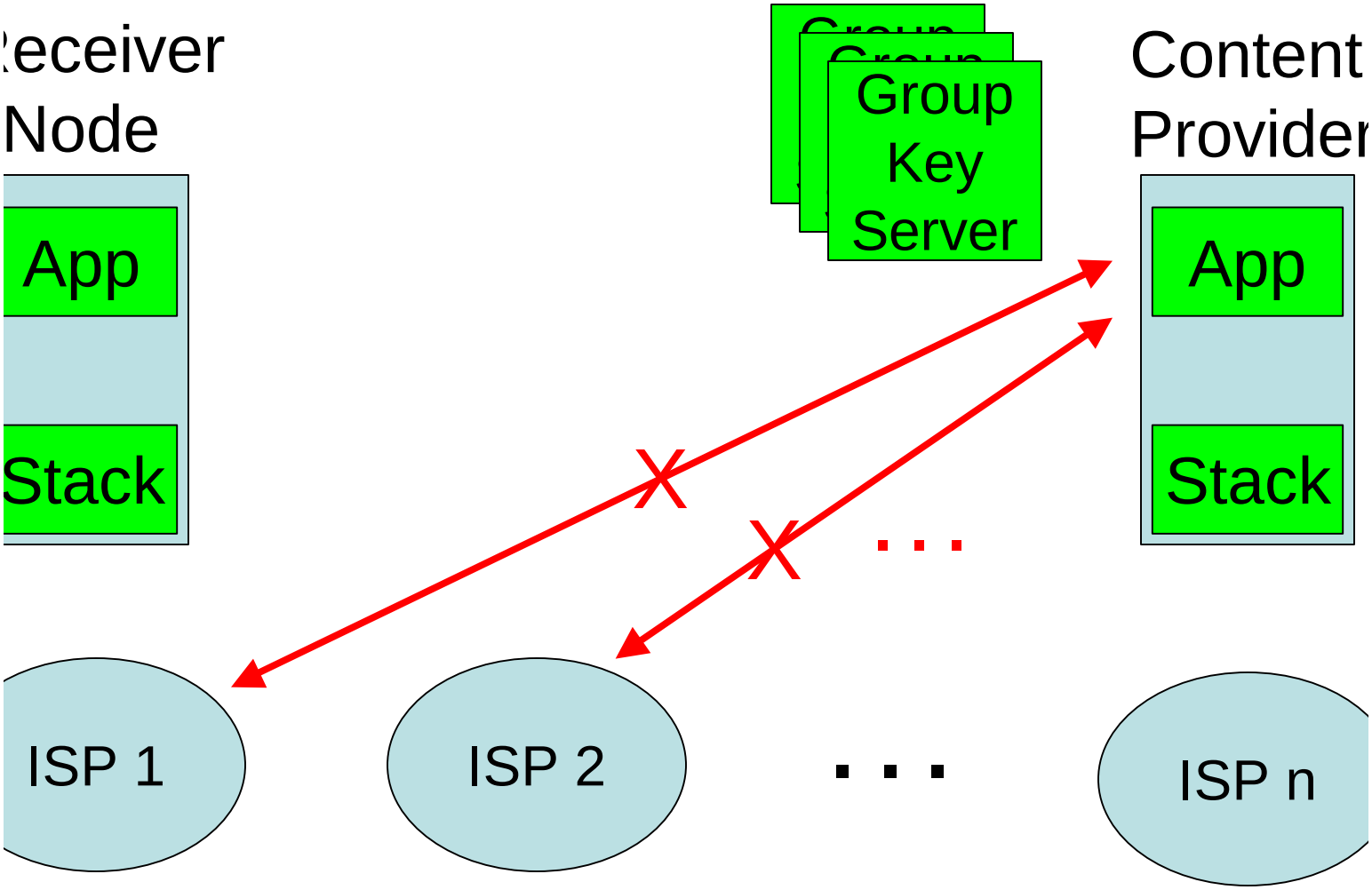
# General Internet Case



# Reasonable Security Relationships



# NOT reasonable in general



# Observations

In general, there is no security relationship between receiver's ISP/network and a content provider

If the content provider and receiver are connected to the same ISP/network, there may be a security relationship

Both problems are interesting

If you solve #1, you also solve #2

# General case needs

ISP/network needs to be able to

- Do accounting per client (port flat rate, per time, per amount of data, whatever)
- Use ACLs (ingress filtering, whatever)

Content provider needs to be able to

- Control who can view content

*hese are not multicast-specific.*

# A solution that matches security relationships

Receiver-edge IP/Link layer:

- ACLs placed on ports based on customer-provider relationship at “connect” time
- Hop-by-hop messages on LANs secured wit same relationship
- Port ACLs may change over time based on ISP/network policy/protocol/whatever

# A solution (cont.)

End-to-end app layer:

- Per-group security/keys done between apps and group key server(s)
- Data can be encrypted in general Internet case
  - If it’s not, then it’s no different from LAN case where other receivers benefit from a legit one

# Protecting bandwidth

General case

- Can just charge requesters
- Same problem occurs with unicast datagram and this is not protected today

When receiver and content provider are o same network

- Content authorizer (e.g. group key server) ca cause port ACL to be updated

# Summary

- Solutions need to match practical security relationships
- Group-specific security in IGMP is not reasonable in general
- Other solutions exist which appear to me the goals
- In the special case, other solutions can d everything IGMP group security does
- Conclusion: don’t do IGMP group security