Middlebox Cooperation Protocol Technical Considerations

Brian Trammell, MAMI Plenary

Berlin - 14 July 2016

mami

measurement and architecture for a middleboxed internet

measurement | architecture | experimentation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 688421.The opinions expressed and arguments employed reflect only the authors' view. The European Commission is not responsible for any use that may be made of that information.

Supported by the Swiss State Secretariat for Education, Research and Innovation under contract number 15.0268. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Swiss Government.

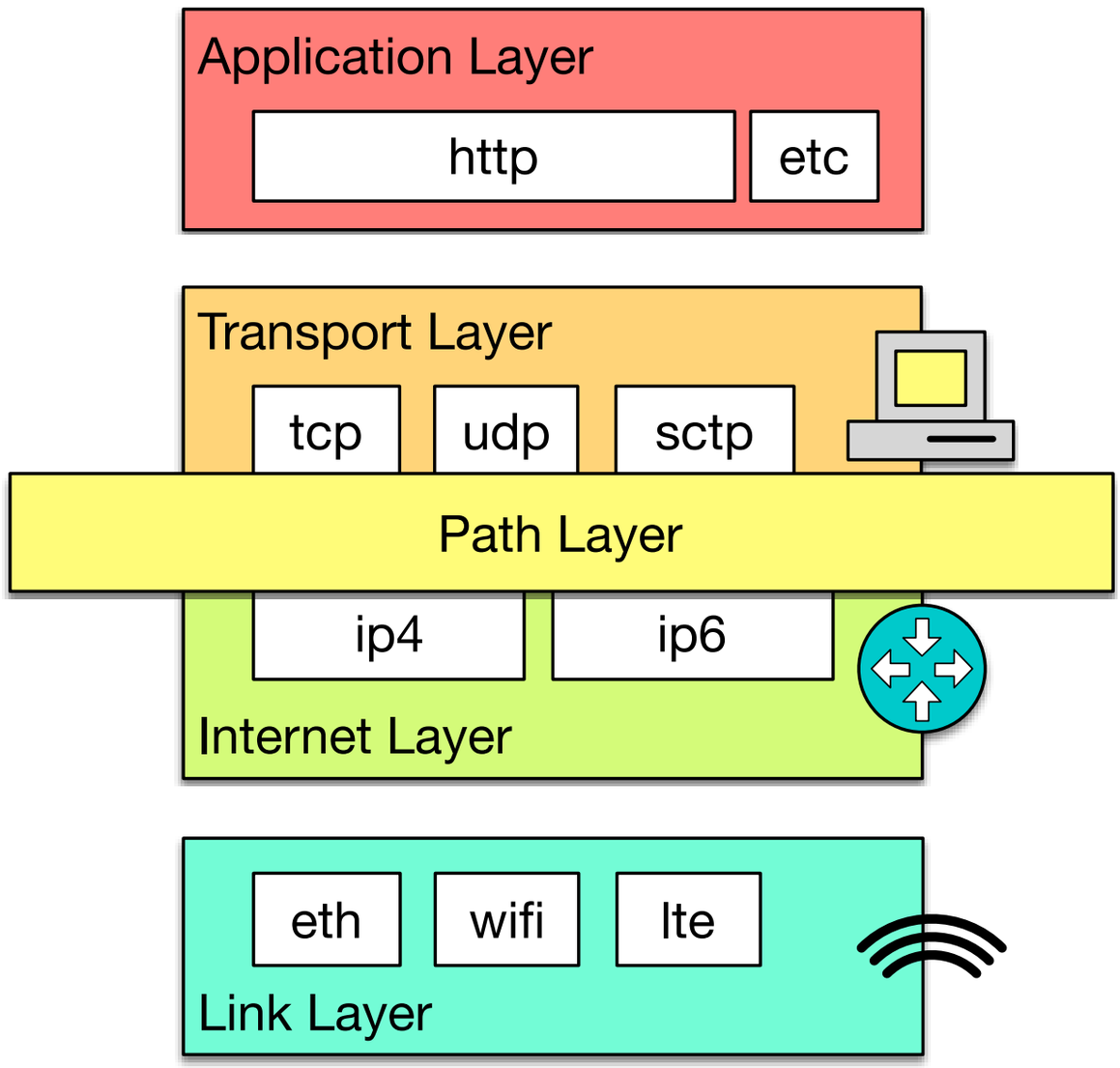

PARENTAL
ADVISORY
EXPLICIT COOPERATION

Explicit Cooperation

- “Implicit cooperation” between endpoints and middleboxes **already widespread in the Internet**,
  - where “cooperation” may be the wrong term:
    some hacks and workarounds are quite hostile.
- **Explicit cooperation** under **endpoint control** may be a way to reduce tension in this tussle
  - Declarative, advisory signaling with no trust required between endpoint and path.
- **Encrypt everything devices on path don’t need to see** (including transport headers), to prevent future unauthorized “implicit cooperation”.

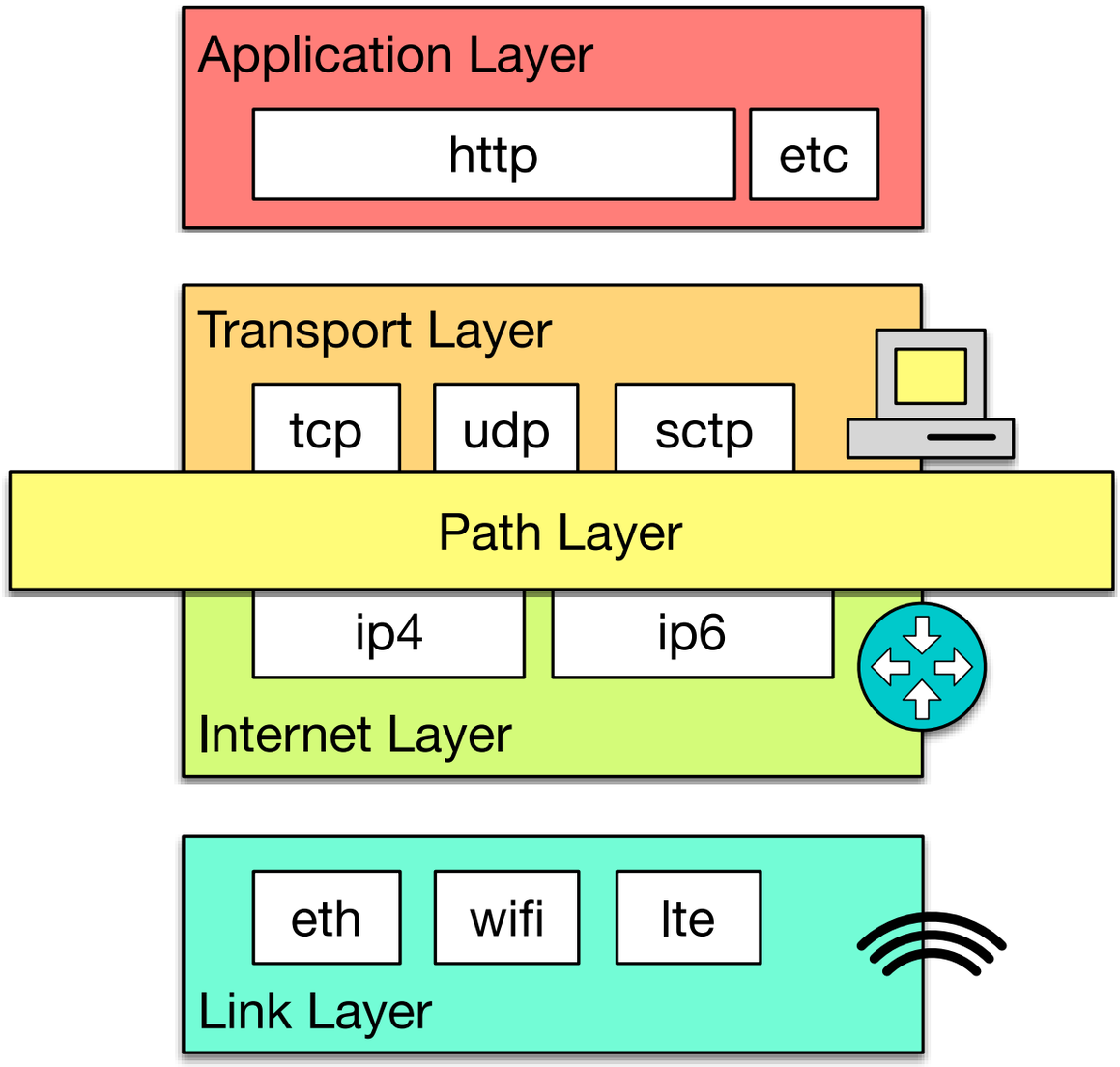
Introducing the Path Layer

- Network: hop-by-hop, no data-plane state.
- Transport: end-to-end, stateful.
- Implicit layer in between where all the state in the network lives.
- MCP makes this explicit.

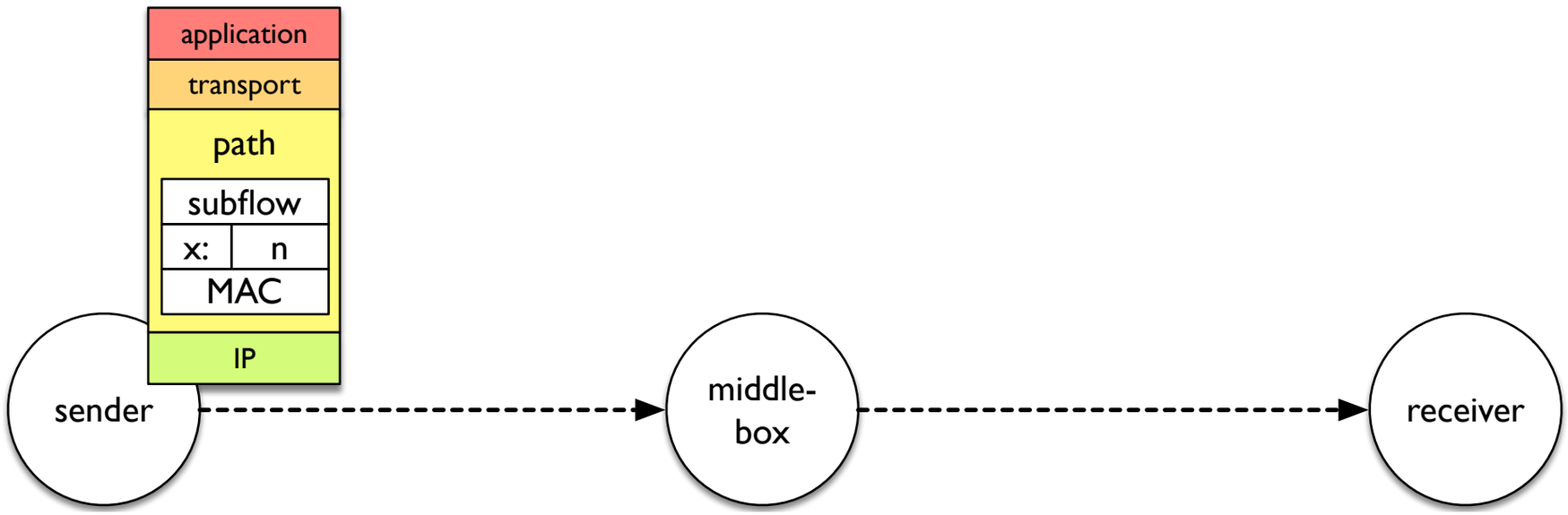


Three and a half mechanisms to make the path layer explicit

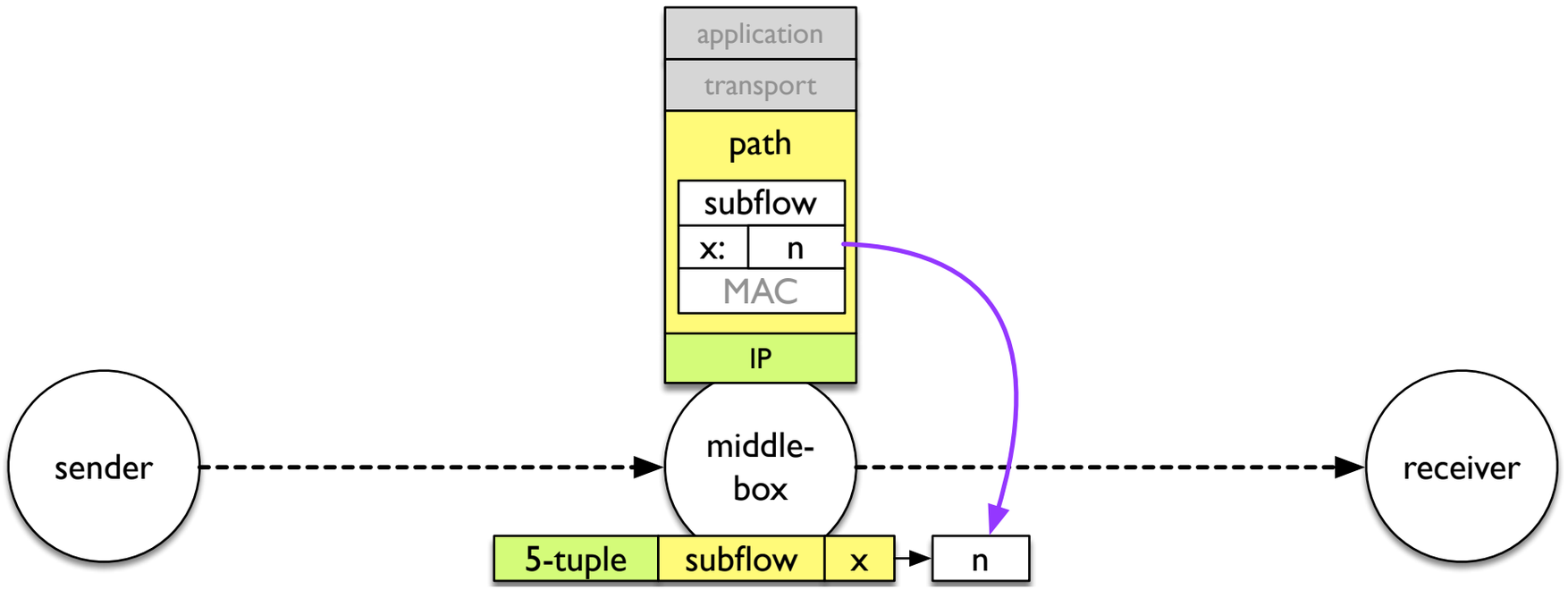
- Sender – Path Signaling
- Path – Receiver Signaling
  - with encrypted feedback to sender
- Direct Path – Sender Signaling



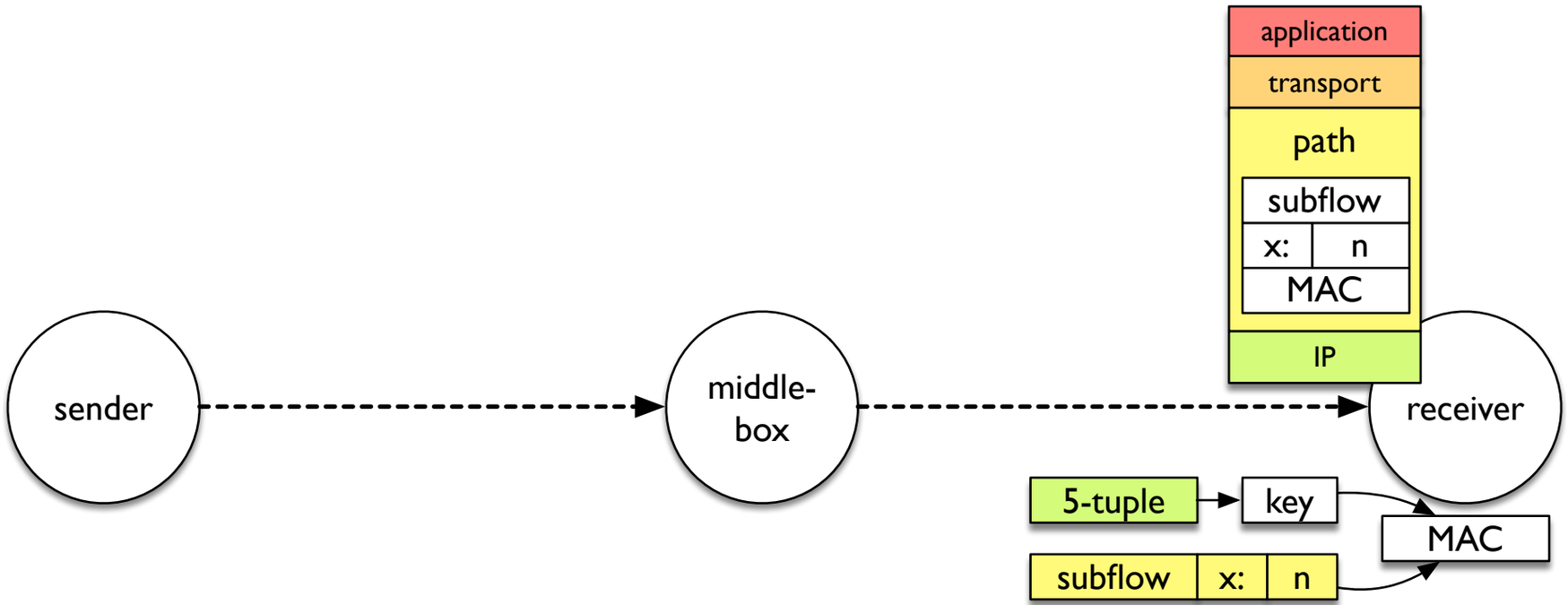
Sender to Path (sender-side)



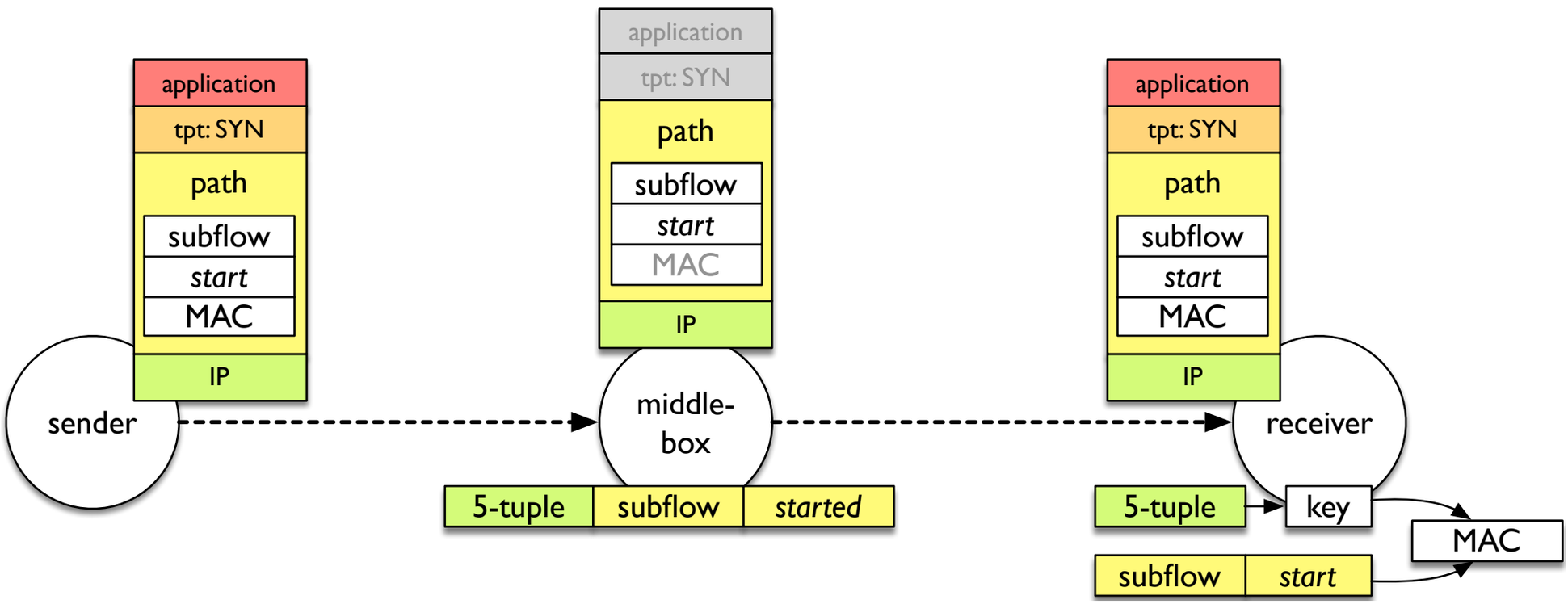
Sender to Path (on-path)



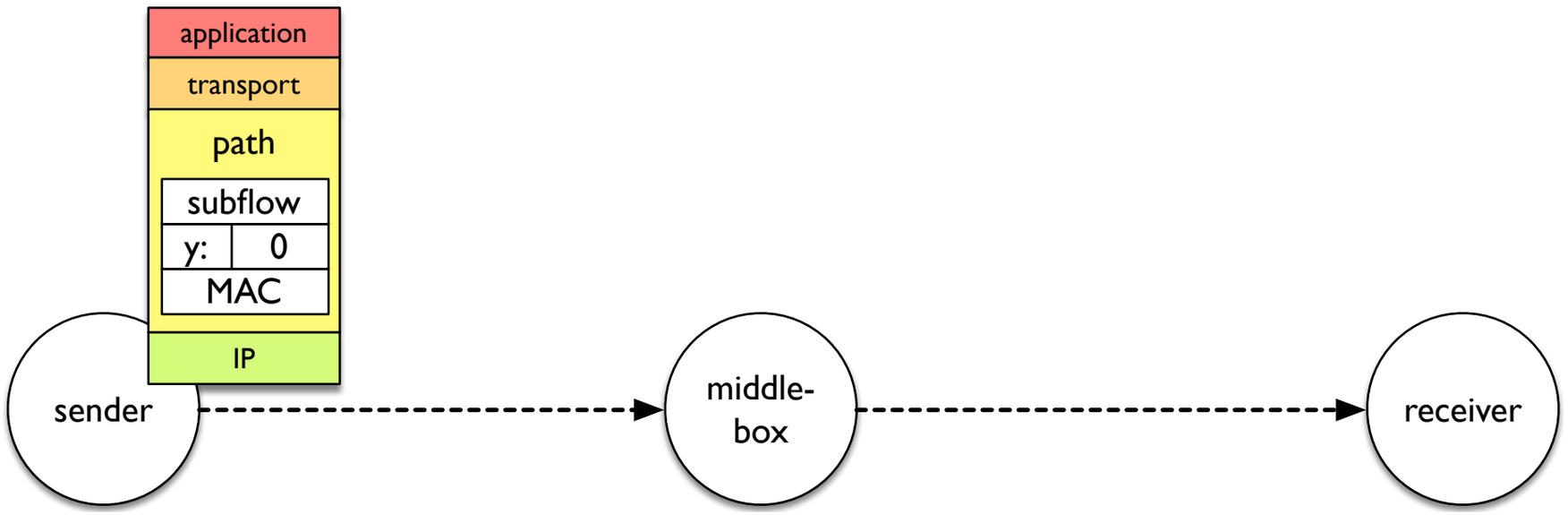
Sender to Path (receiver-side)



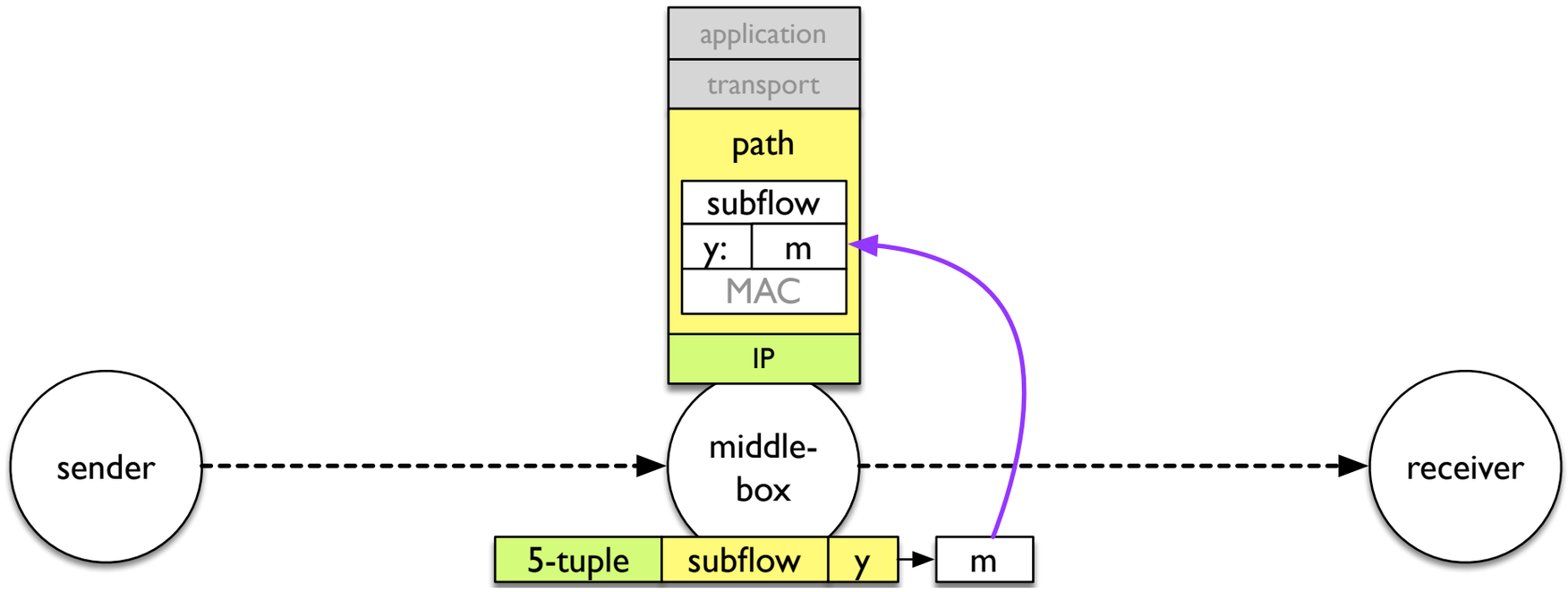
Sender to Path Transport State Signaling



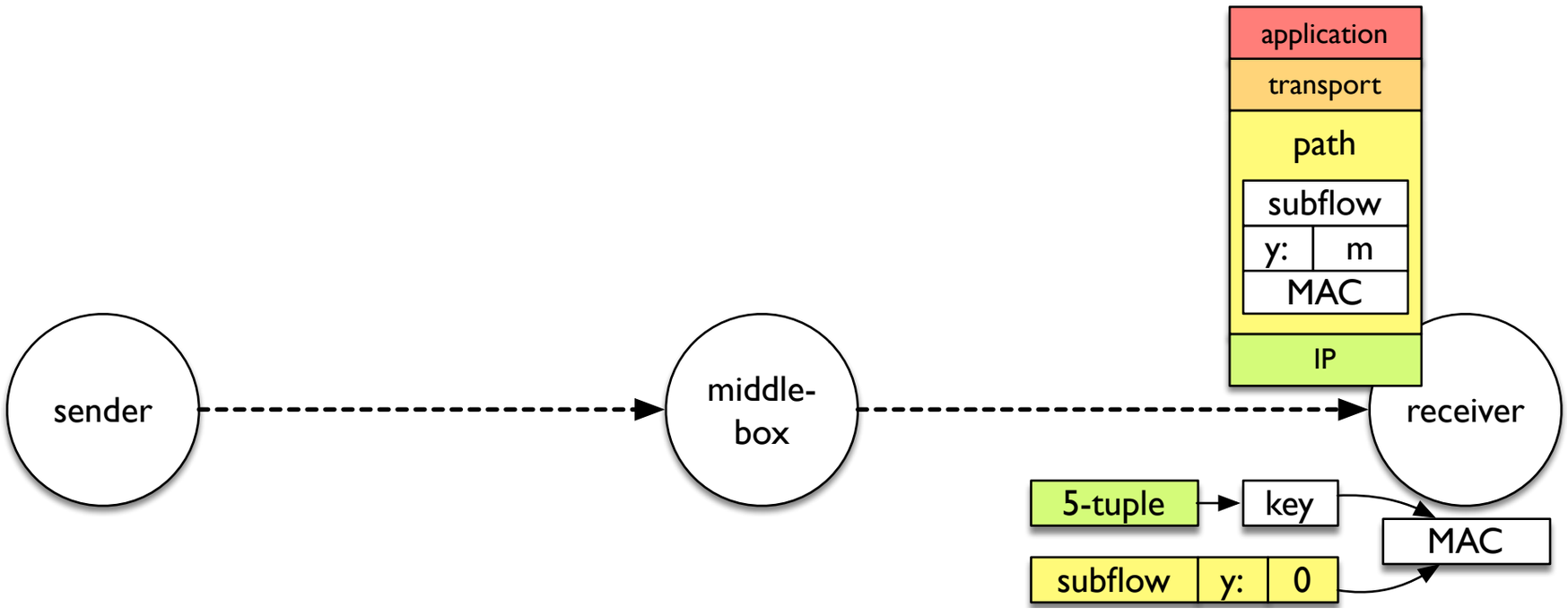
Path to Receiver (sender-side)



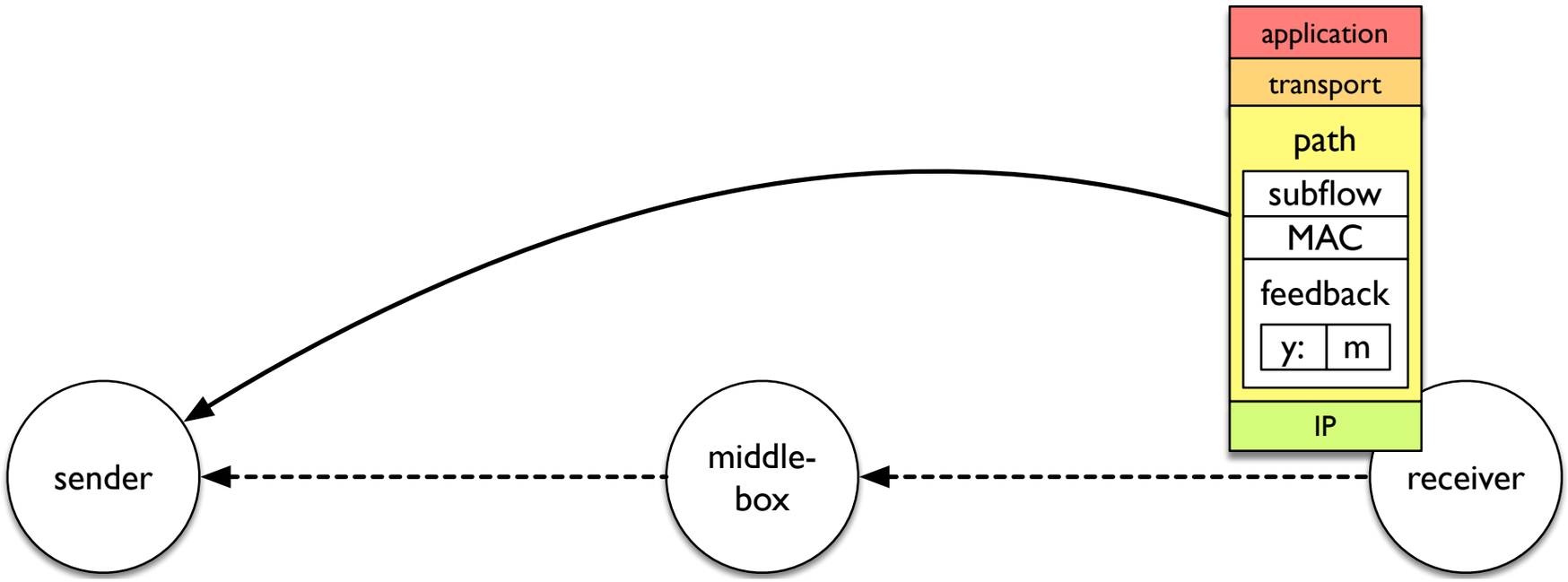
Path to Receiver (on-path)



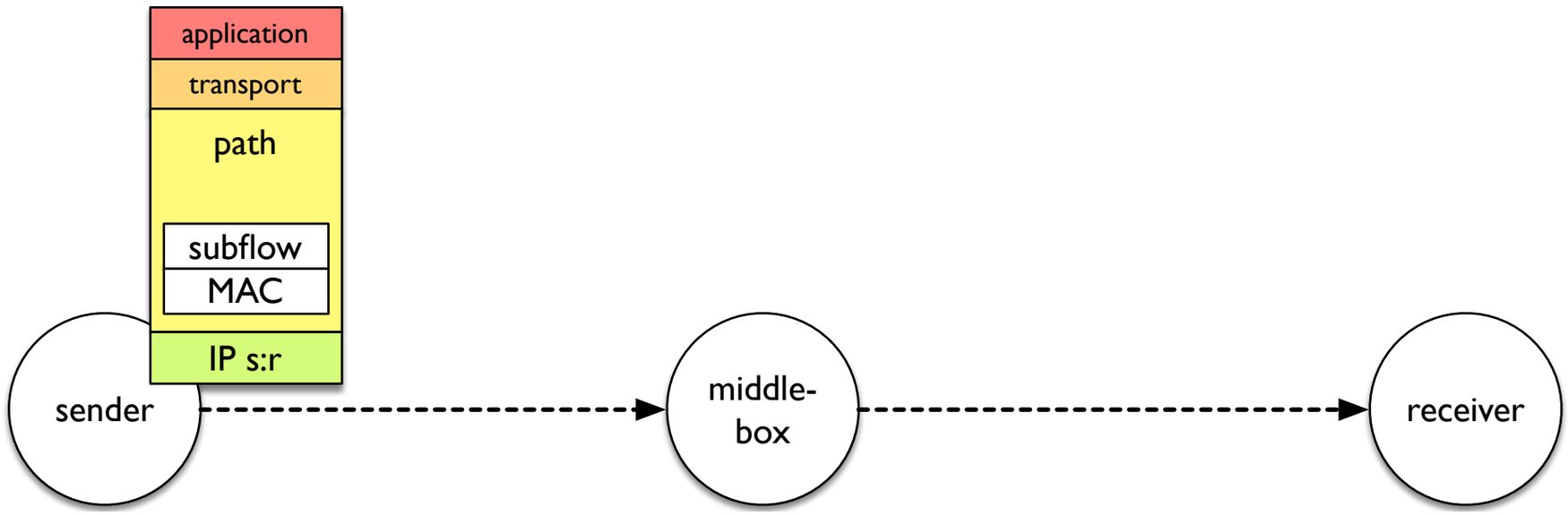
Path to Receiver (receiver-side)



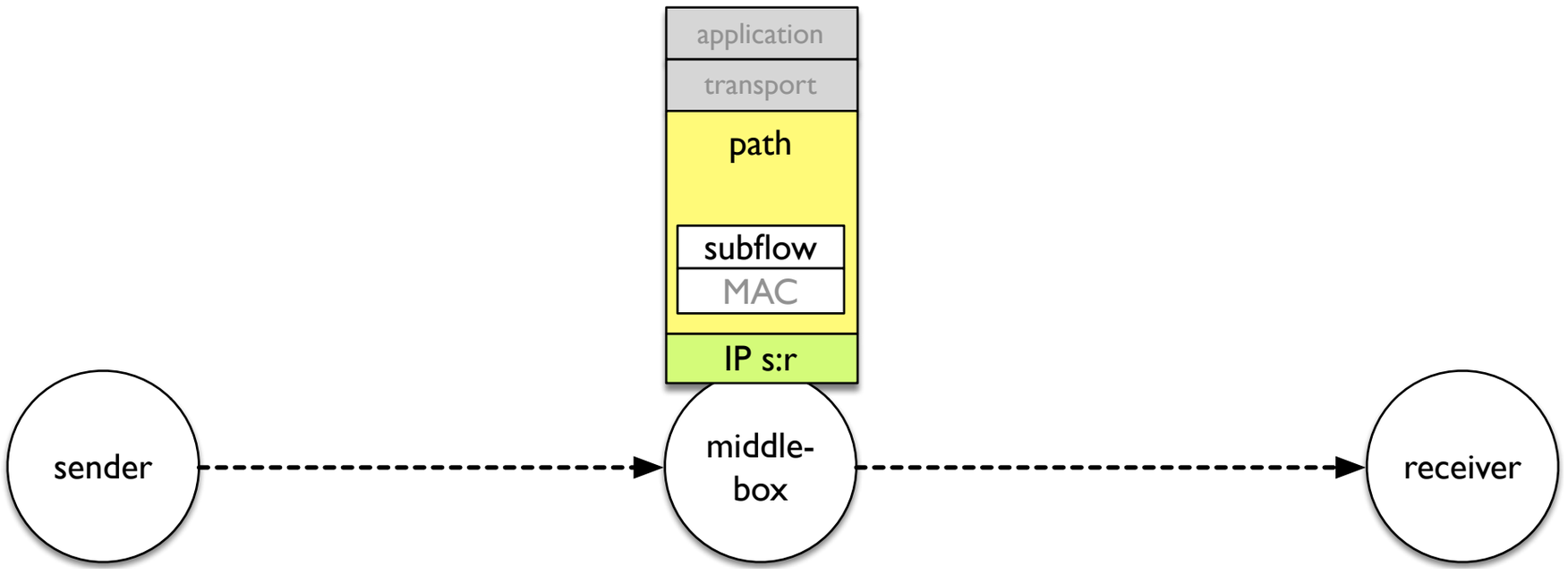
Receiver Feedback



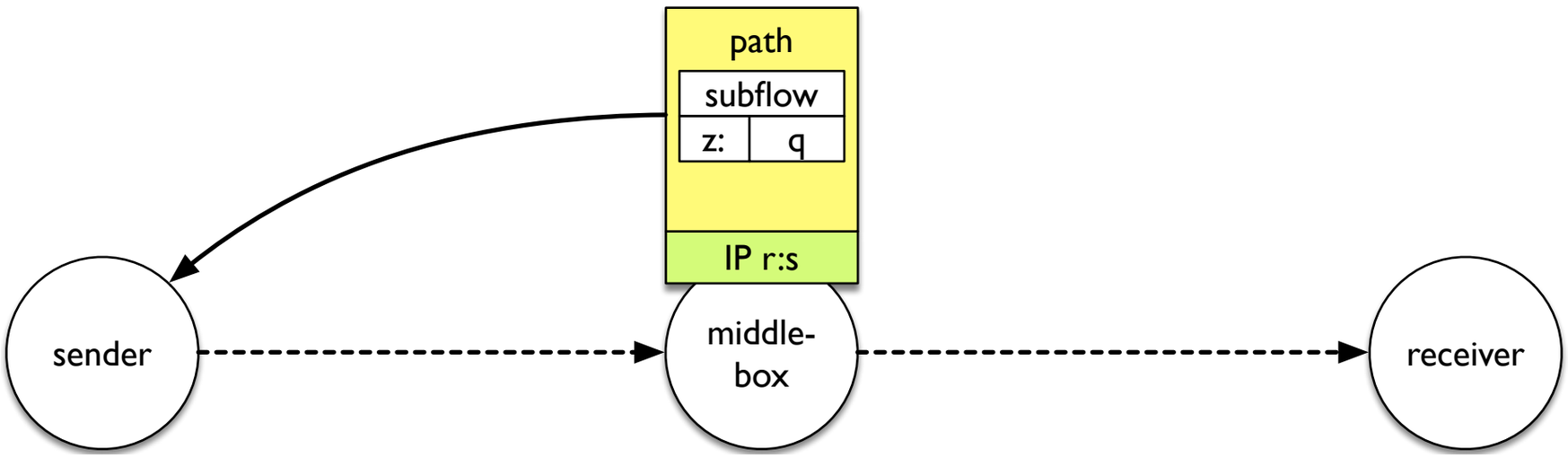
Path Direct to Sender (sender-side)



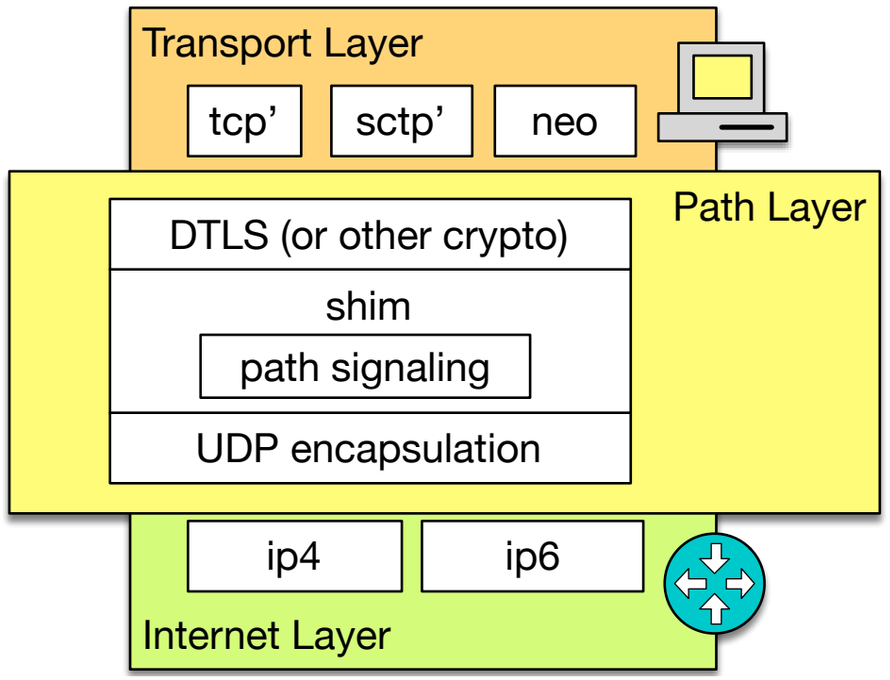
Path Direct to Sender (on-path)



Path Direct to Sender (feedback)



Anatomy of the Path Layer



- UDP encapsulation
  - userspace implementation
  - ports for NAT
  - ~95% deployable today
- encoding for signaling mechanisms
- crypto to protect transport headers and above

Layering Security for Diverse Trust and Authentication Models

- “Core MCP” provides:
  - Signaling as above
  - Integrity protection of sender-provided data
  - Integrity protection of permission for path-provided data
  - Confidentiality and integrity for receiver-feedback data

- Sender-provided data can be encrypted for selected path elements.
- Path-provided data can be encrypted and MAC’d for sender/receiver
- Key negotiation, path element ID, and multiparty crypto protocols can run in-line over “core MCP”