Catching the Middlebox.

A Technique for the Detection of Intermediate Network Devices.

Masters Thesis Defense.

Luis Martín García.

Department of Telematic Systems Engineering.
Higher Technical School of Telecommunications Engineering.
Universidad Politécnica de Madrid (UPM).

ETSIT UPM

TABLE OF CONTENTS

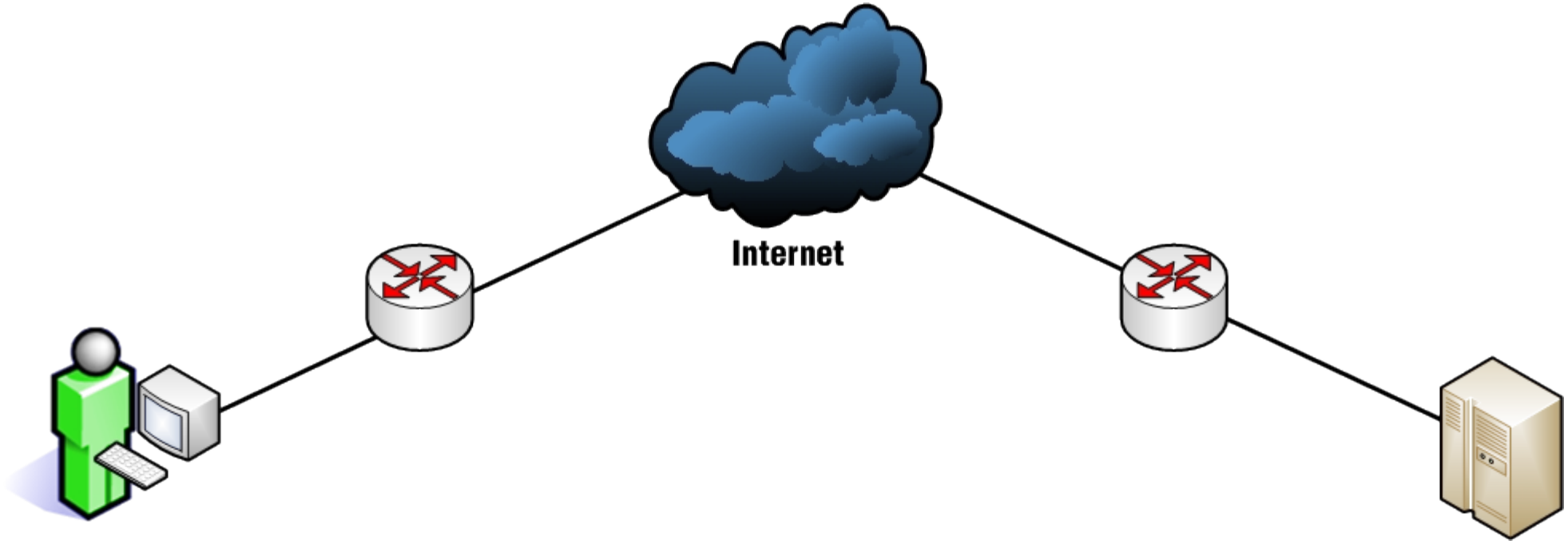
1. Introduction

1. Introduction

- Back in the good old days...
  - When networks where simple.

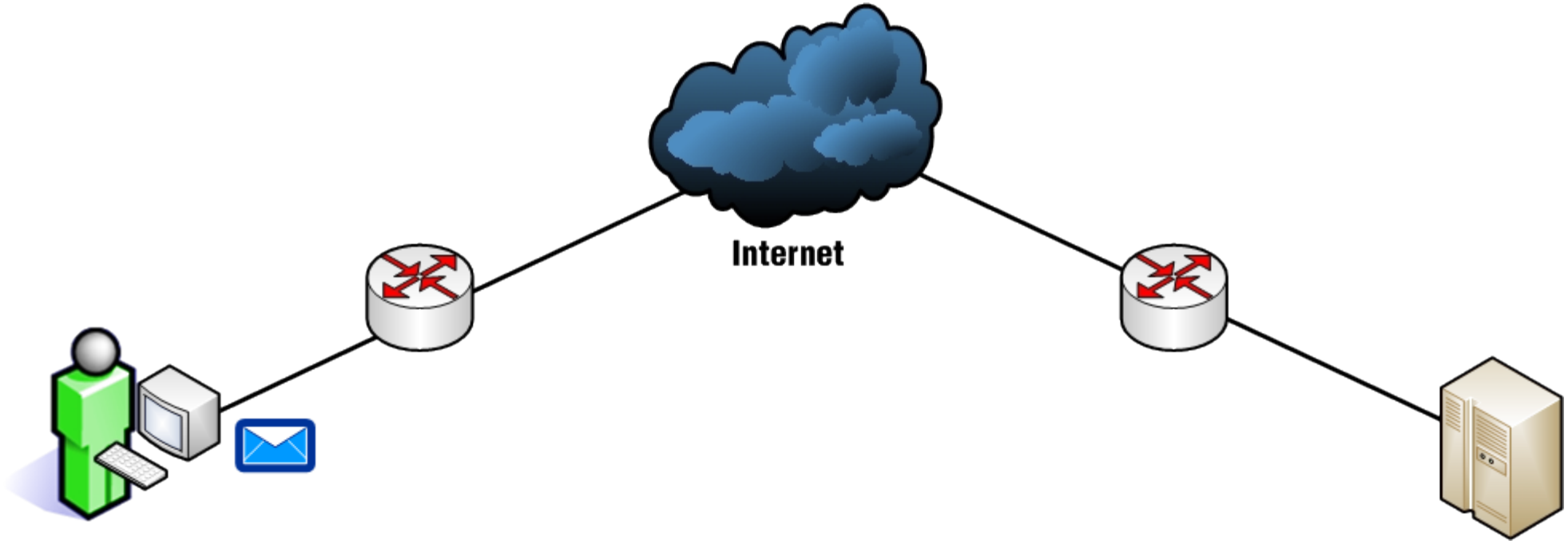
1. Introduction

- Back in the good old days...
  - When networks where simple.



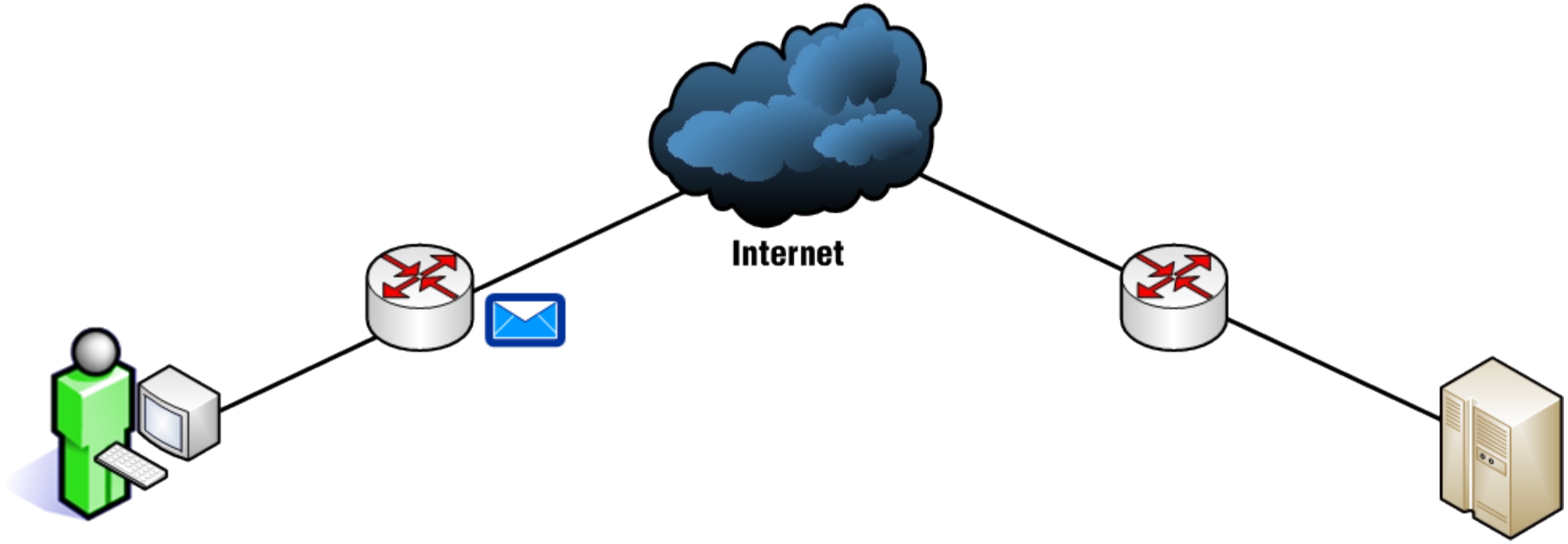
1. Introduction

- Back in the good old days...
  - When networks where simple.



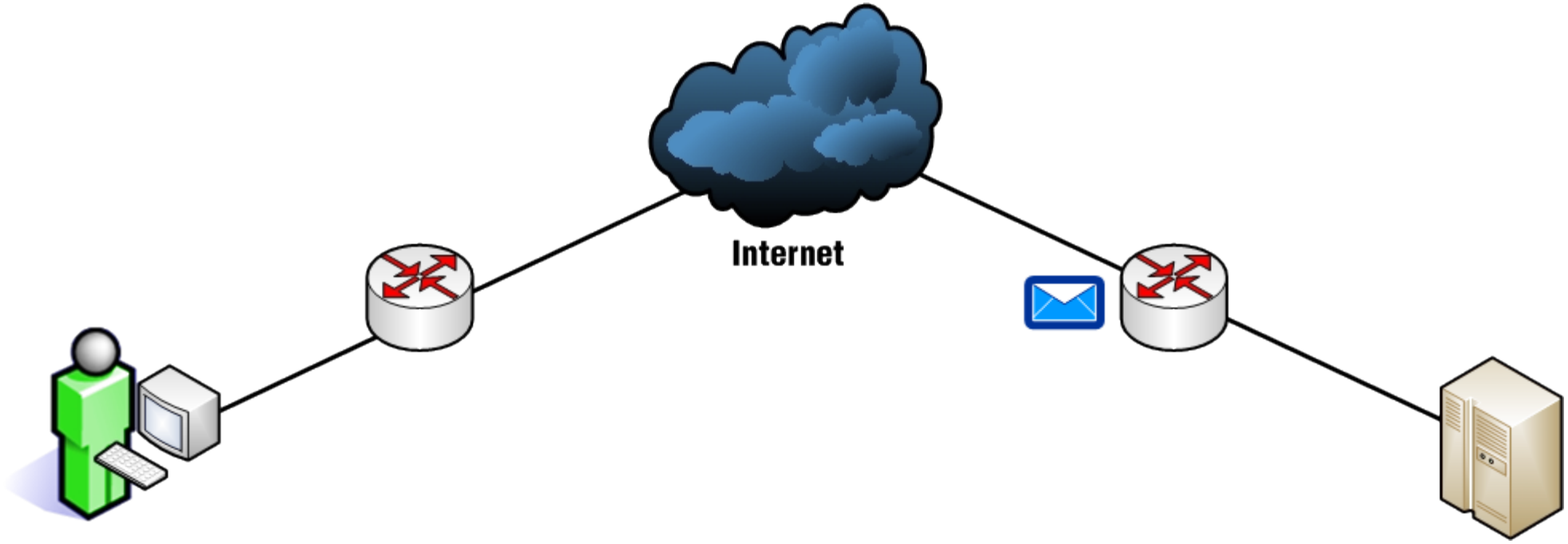
1. Introduction

- Back in the good old days...
  - When networks where simple.



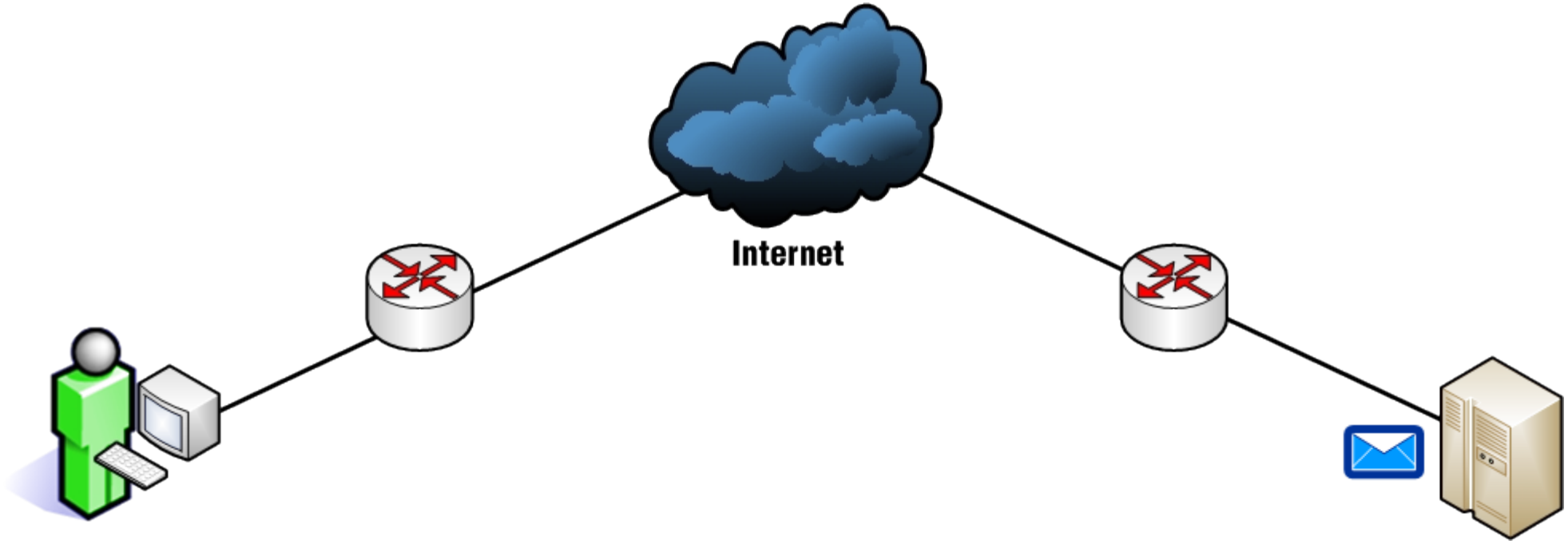
1. Introduction

- Back in the good old days...
  - When networks where simple.



1. Introduction

- Back in the good old days...
  - When networks where simple.

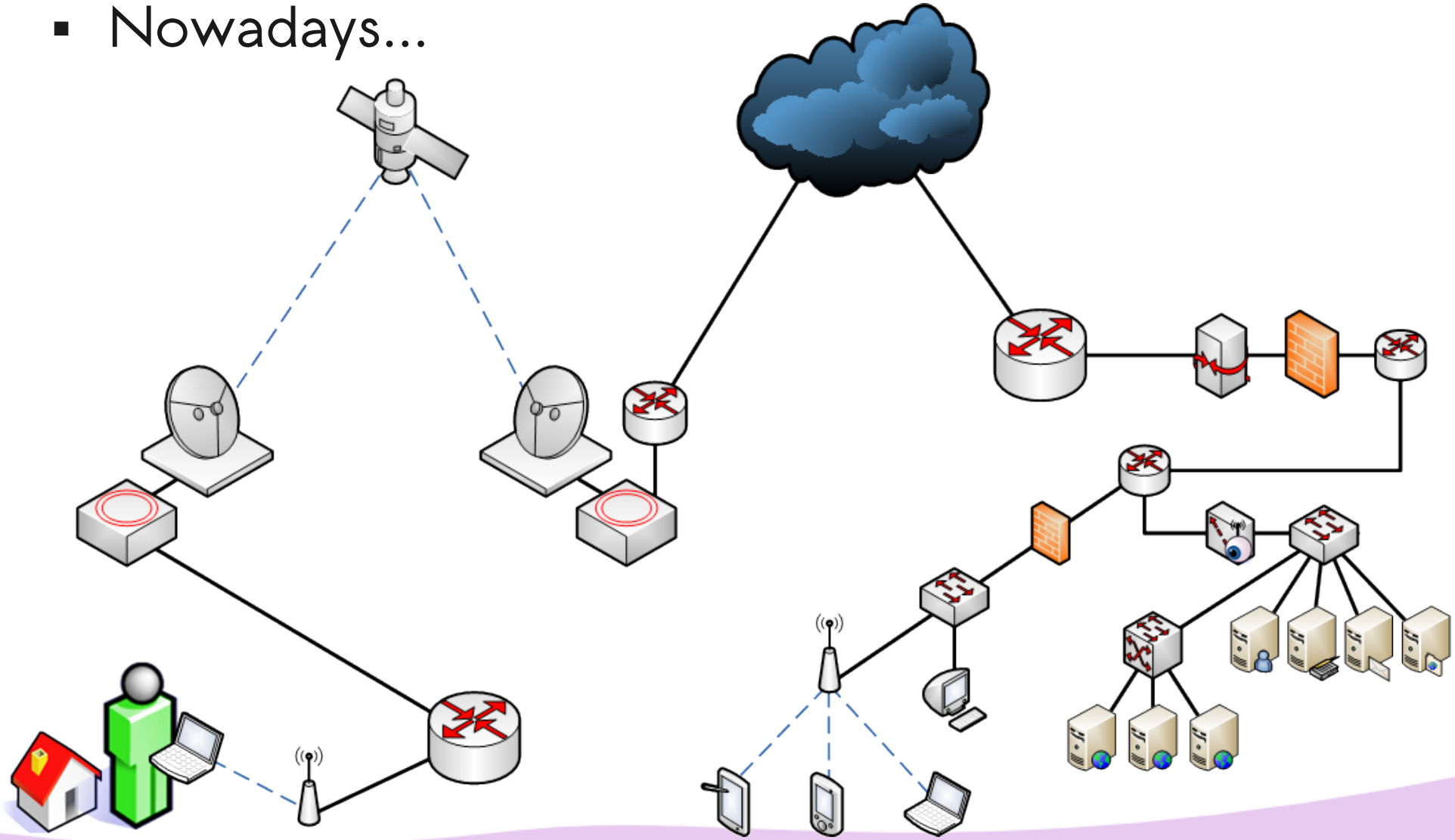


1. Introduction

- Nowadays...

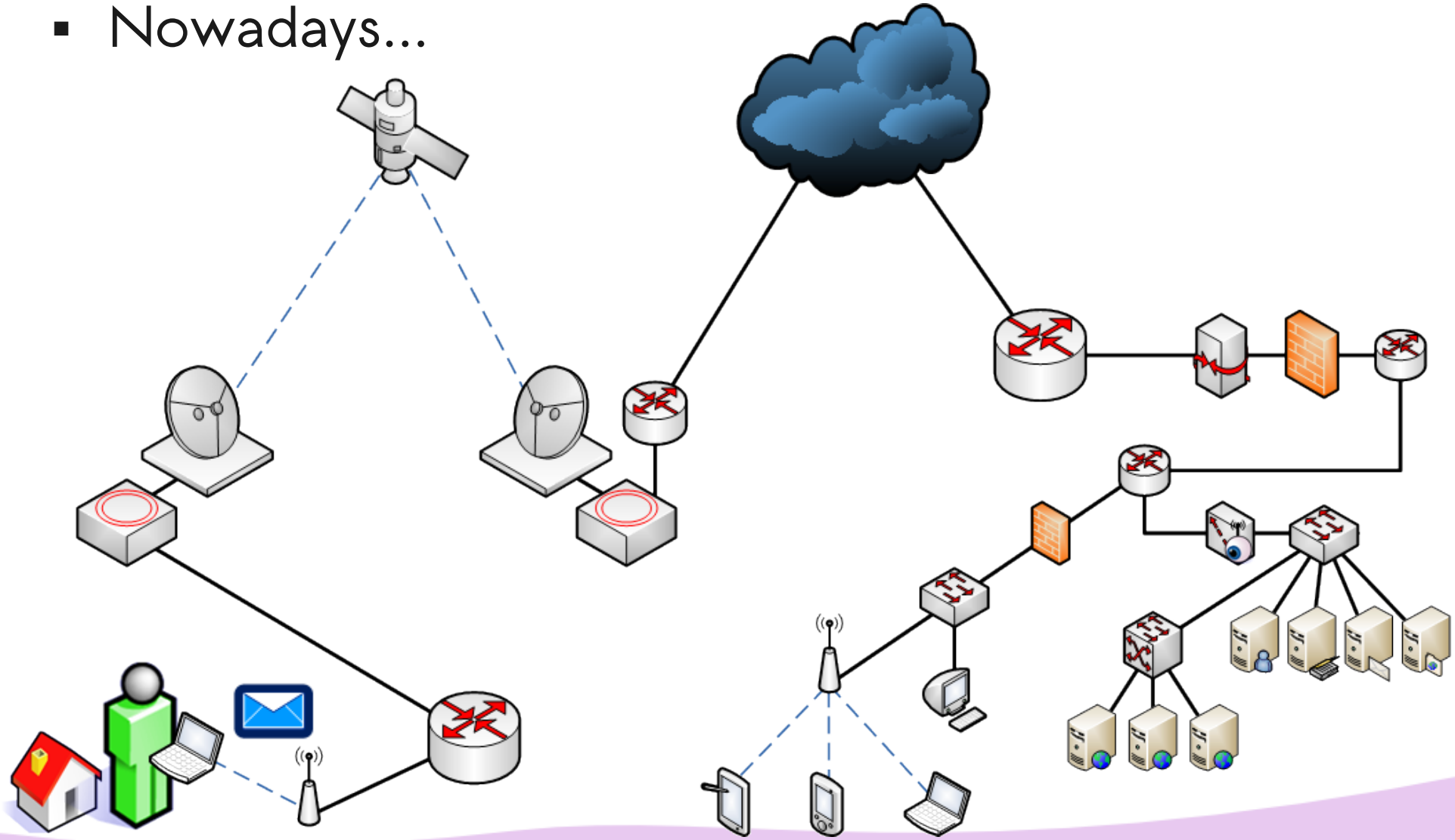
1. Introduction

- Nowadays...



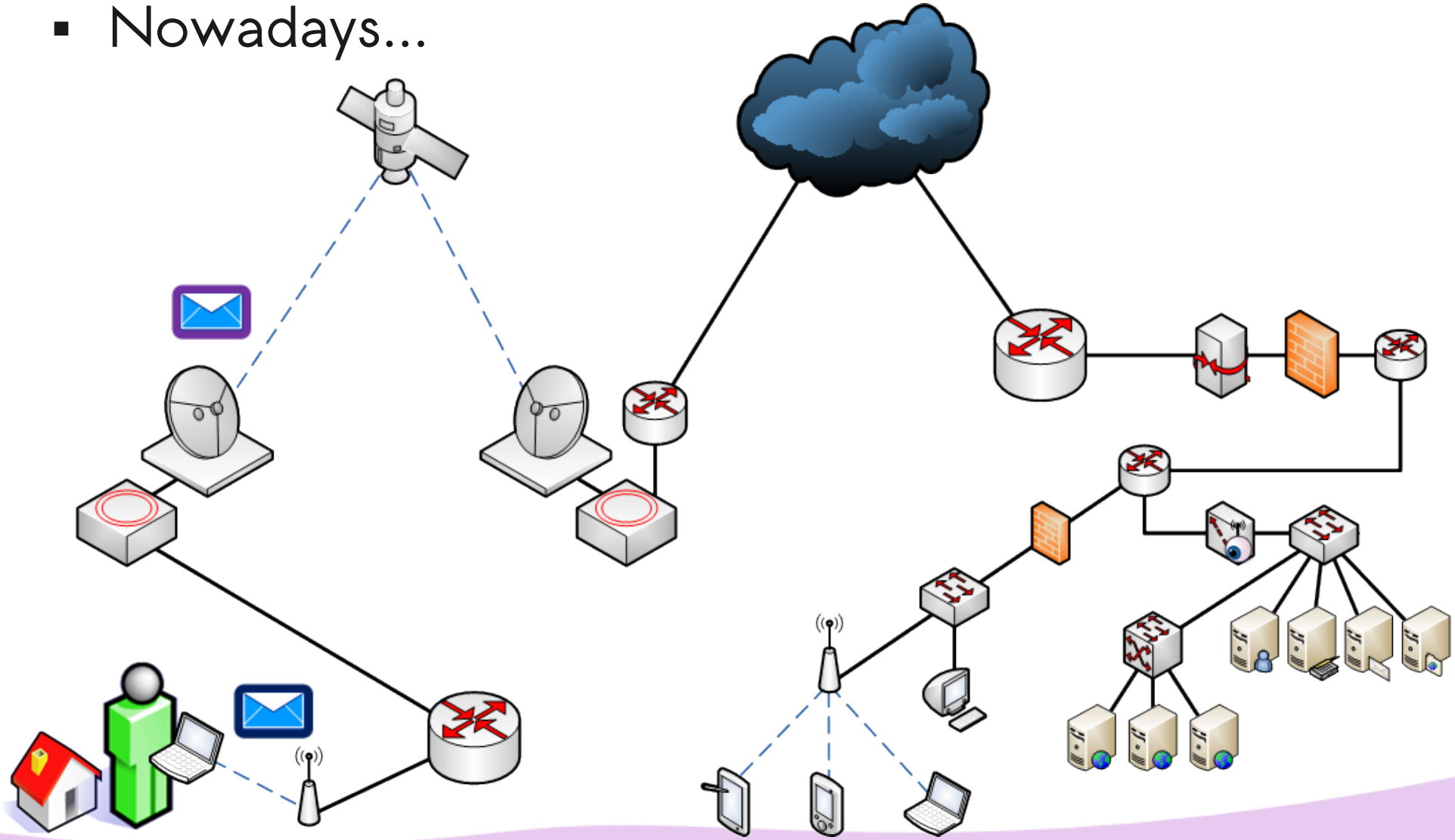
1. Introduction

- Nowadays...



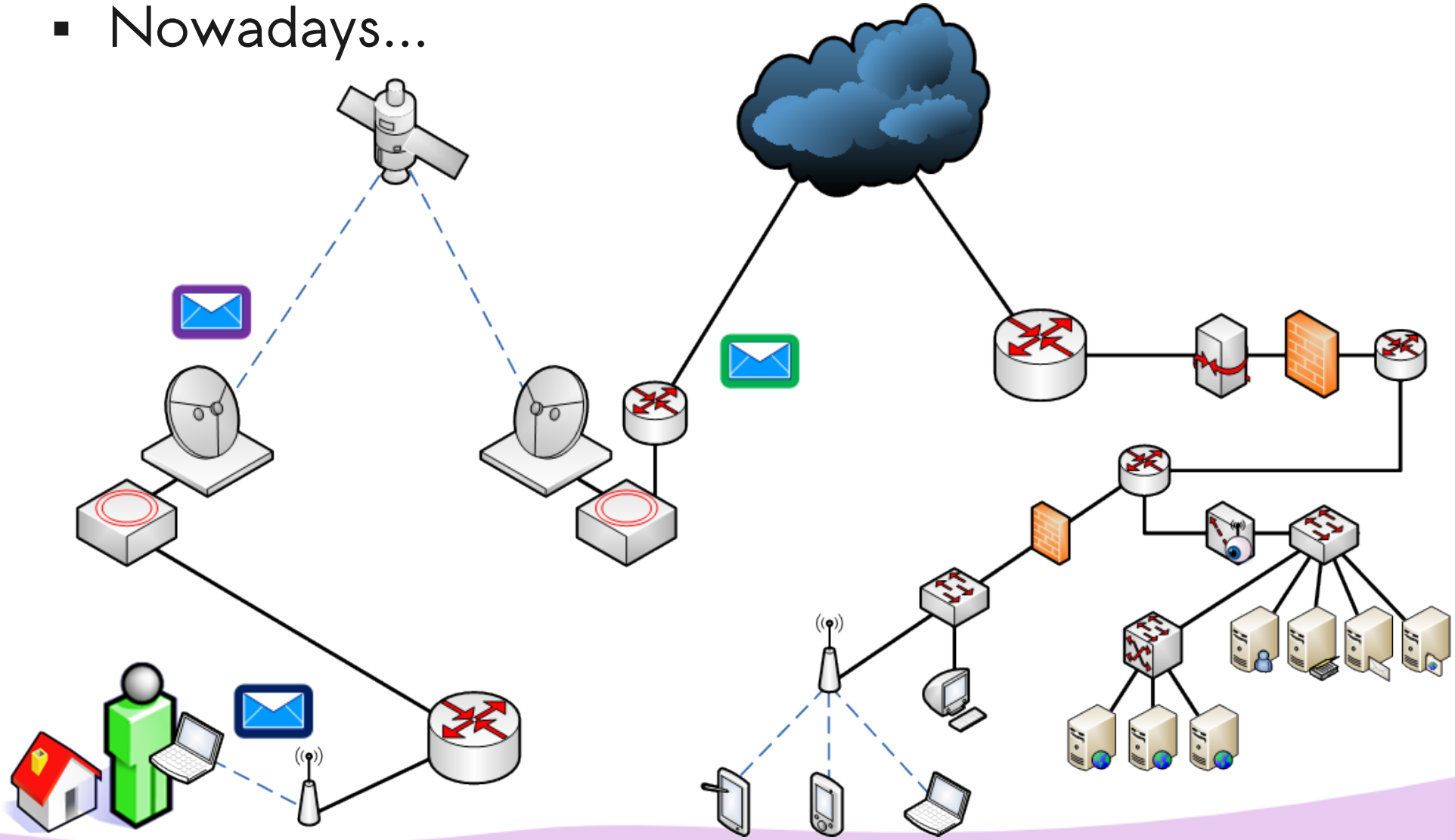
1. Introduction

- Nowadays...



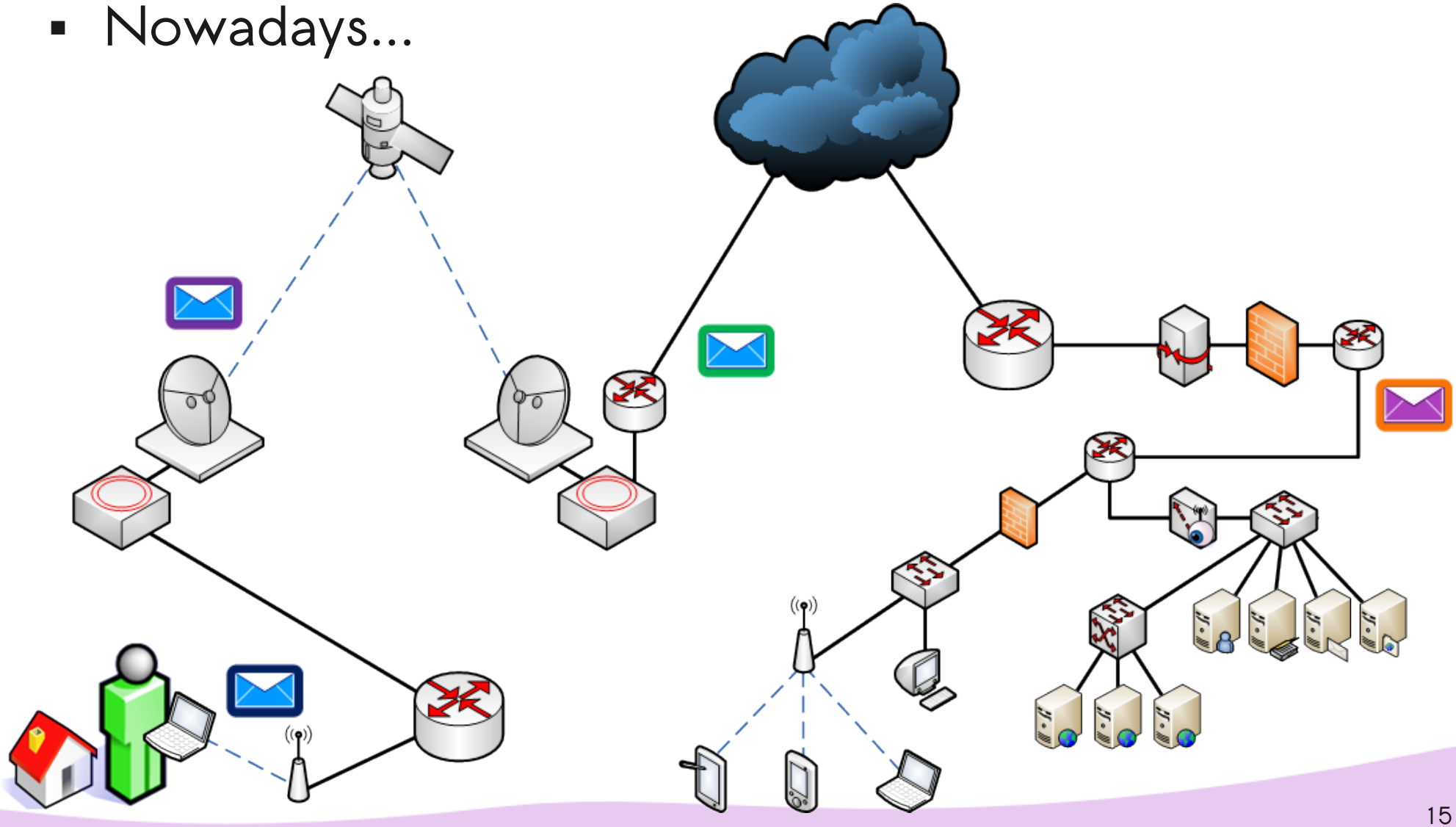
1. Introduction

- Nowadays...



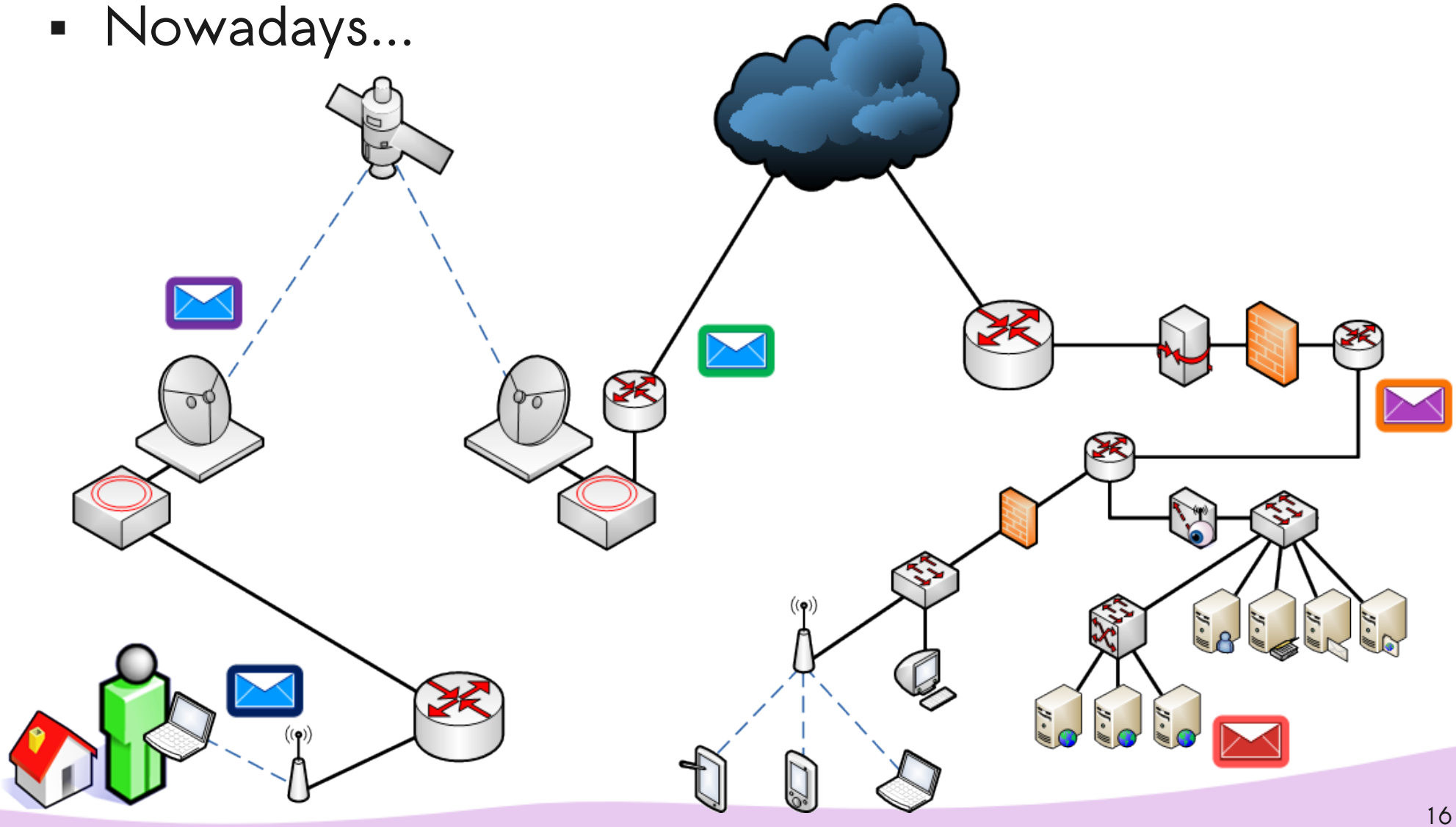
1. Introduction

- Nowadays...



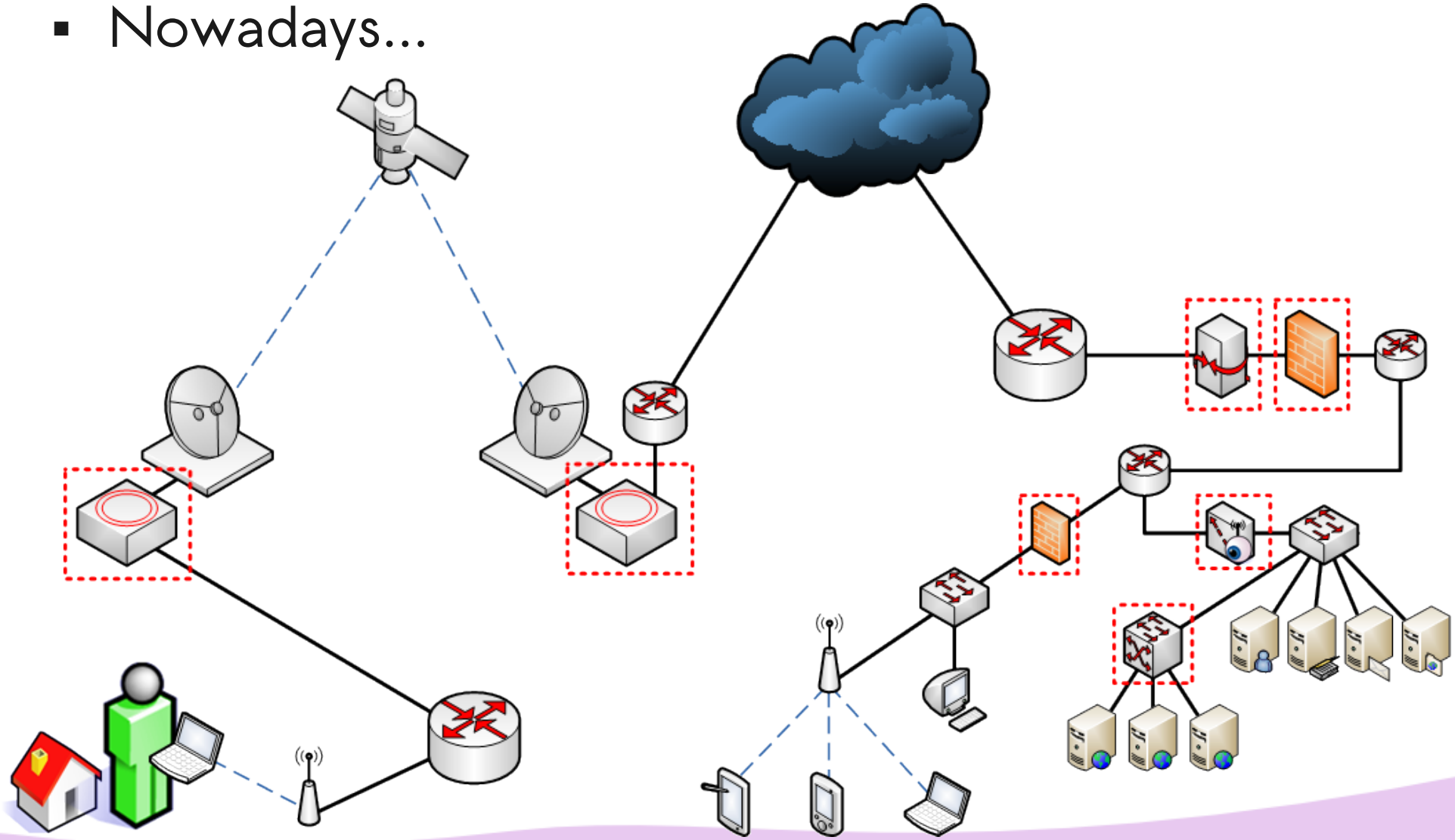
1. Introduction

- Nowadays...



1. Introduction

- Nowadays...

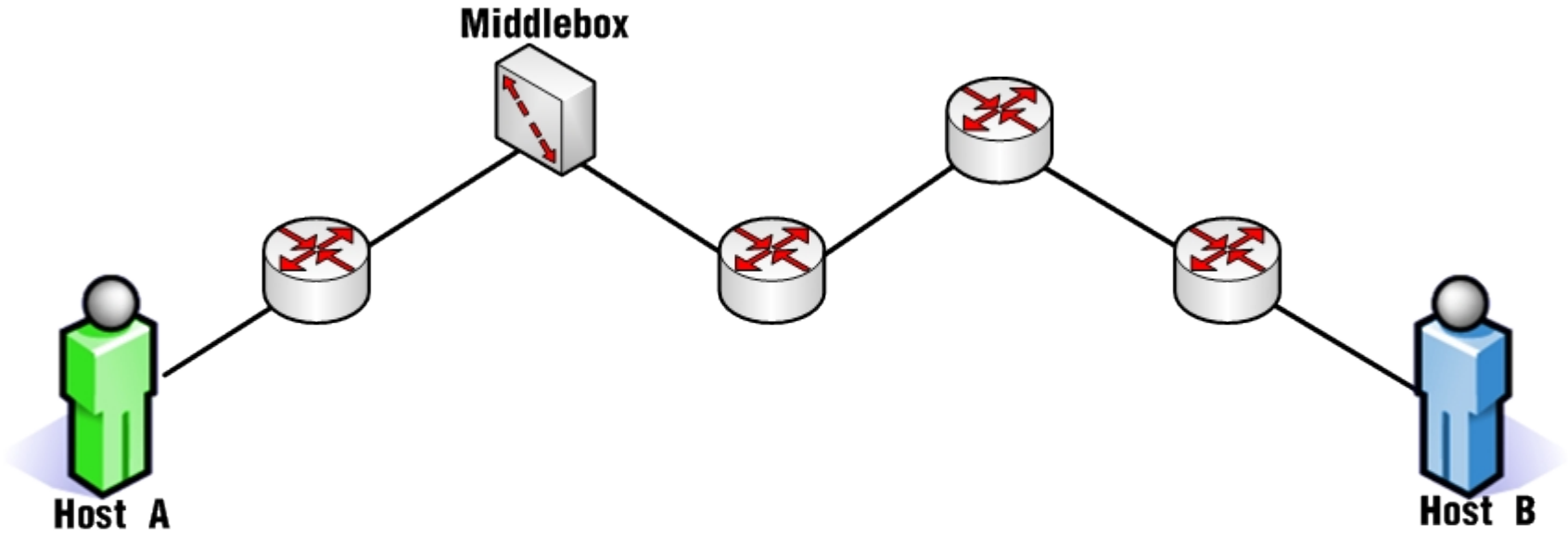


2. Middlebox Detection

- GOAL:

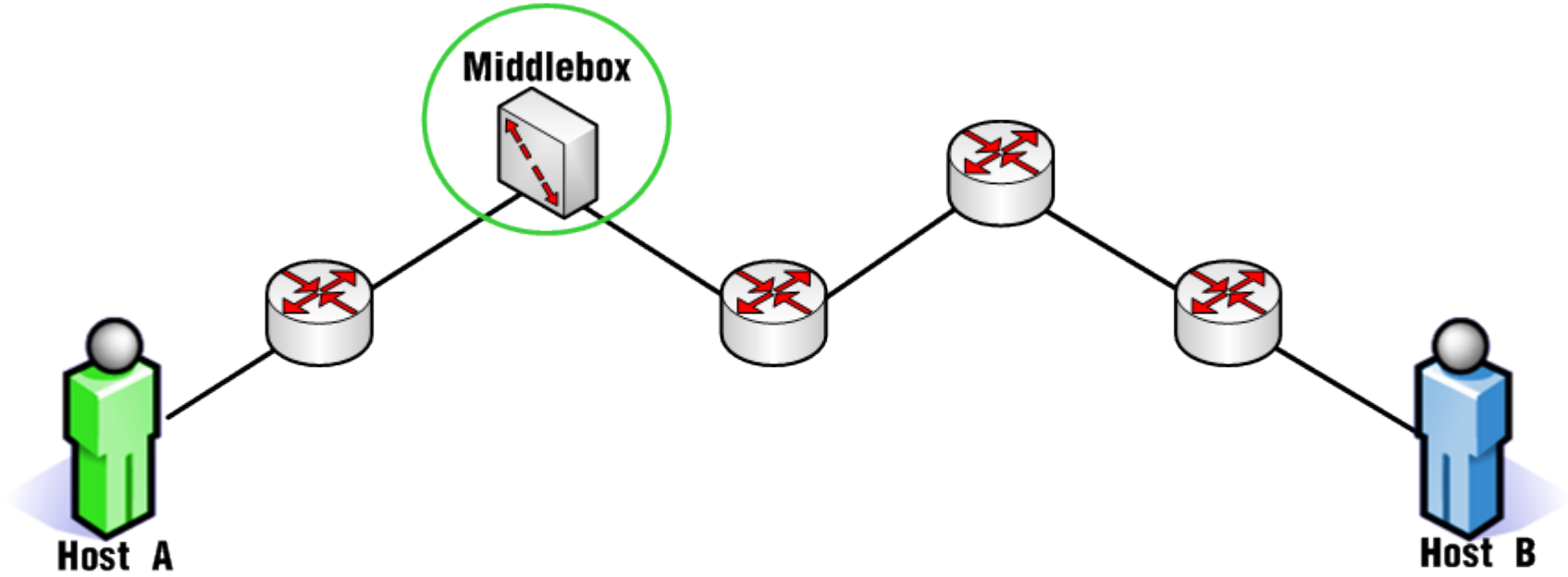
2. Middlebox Detection

- GOAL: Detect intermediate devices in the path between two network hosts.



2. Middlebox Detection

- GOAL: Detect intermediate devices in the path between two network hosts.



2. Middlebox Detection

- What for?

2. Middlebox Detection

- What for?
  - Troubleshoot connectivity issues.

2. Middlebox Detection

- What for?
  - Troubleshoot connectivity issues.
  - Verify that some middlebox works as expected.

2. Middlebox Detection

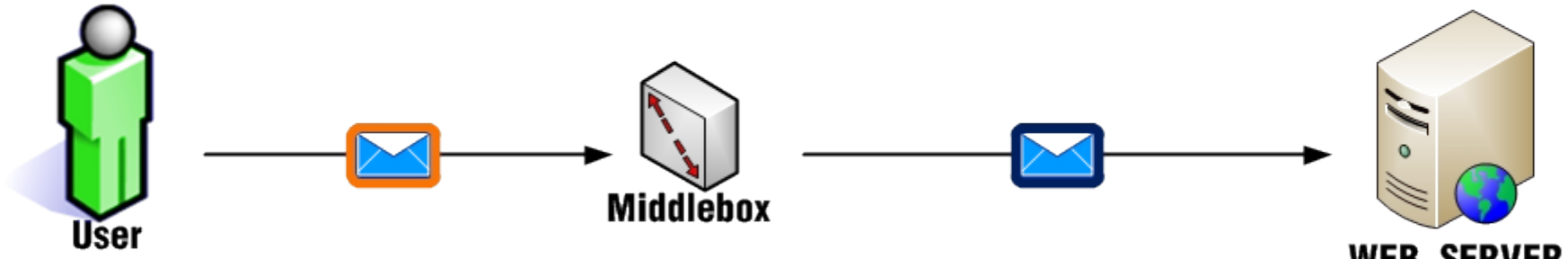
- What for?
  - Troubleshoot connectivity issues.
  - Verify that some middlebox works as expected.
  - Perform network reconnaissance, prior to an attack.

2.1 Basic Operation

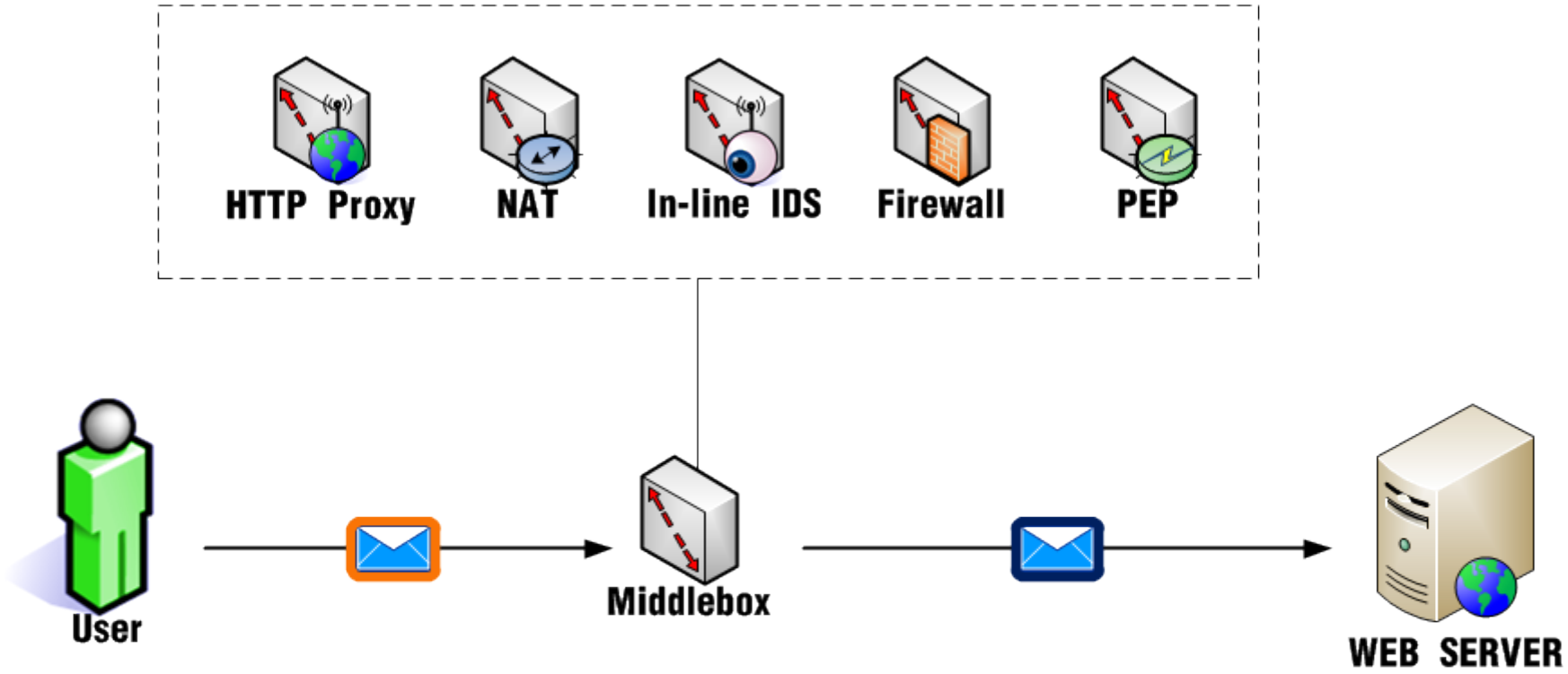
2.1 Basic Operation

2.1 Basic Operation

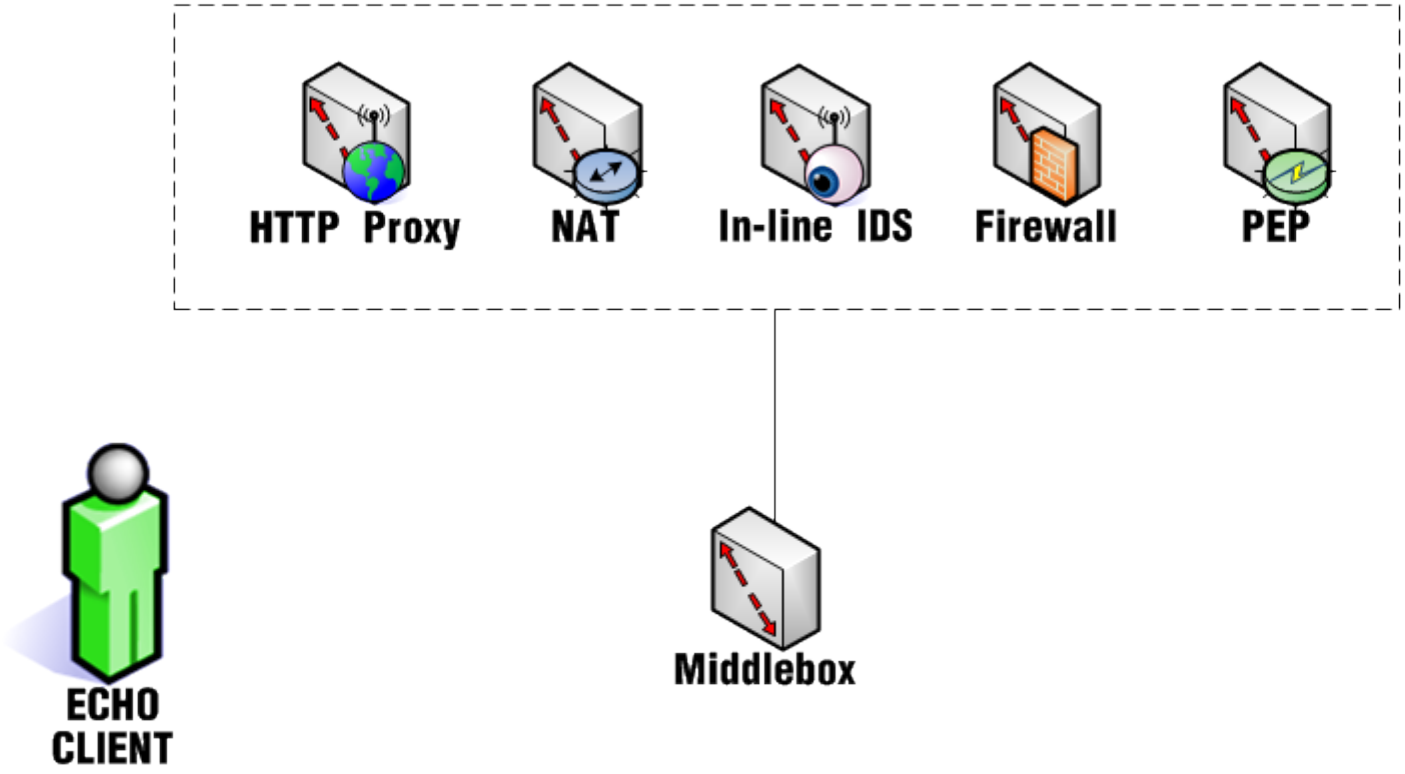
2.1 Basic Operation



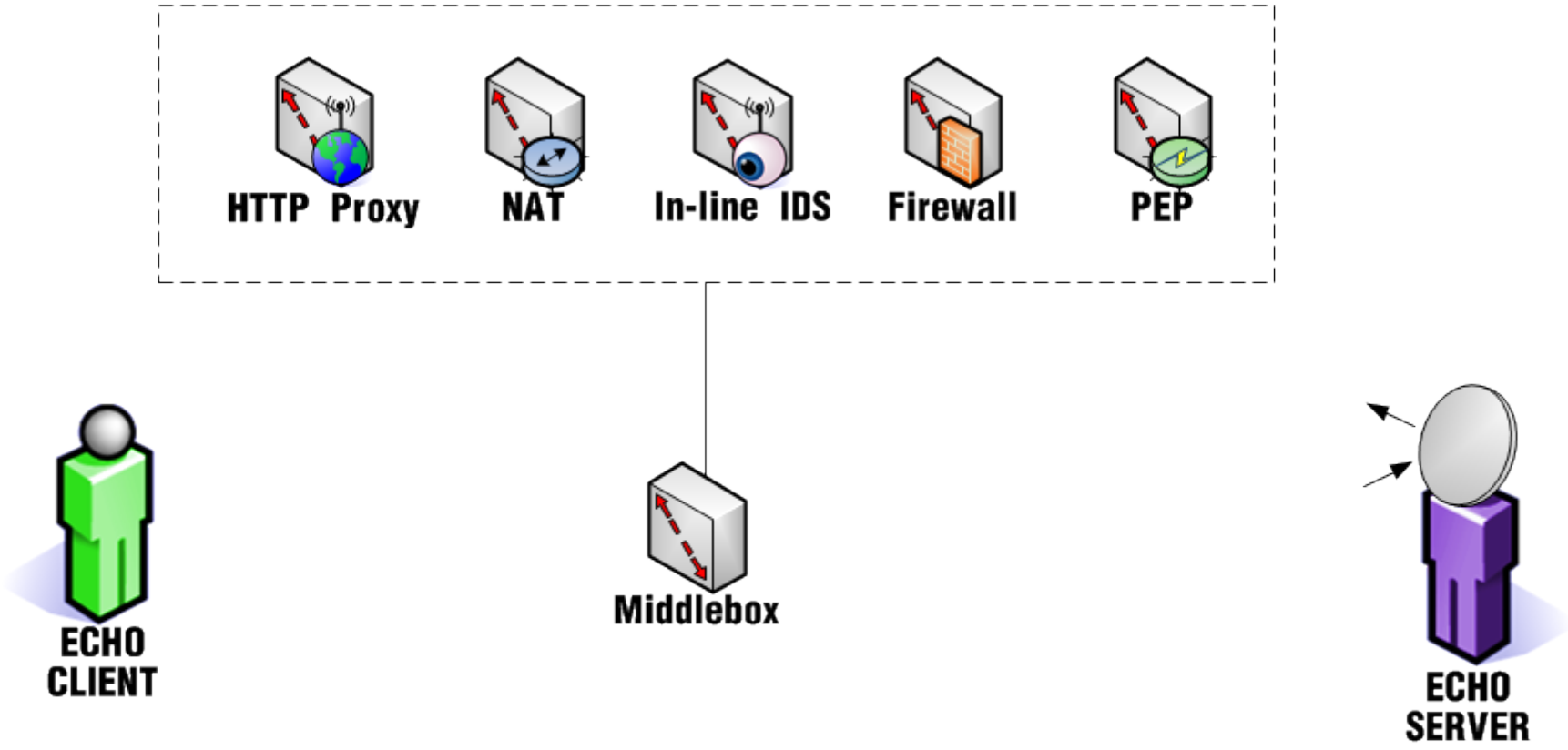
2.1 Basic Operation



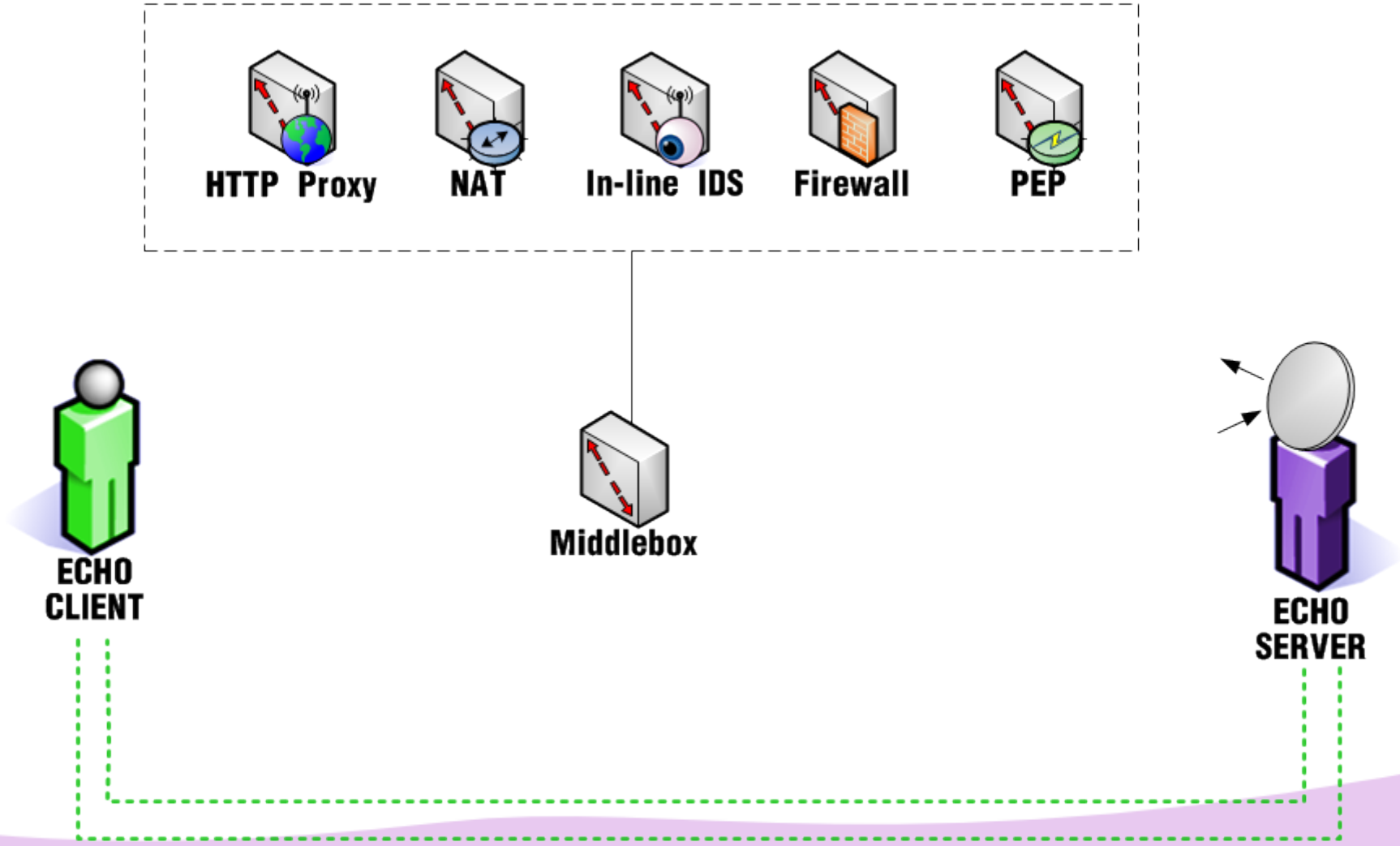
2.1 Basic Operation



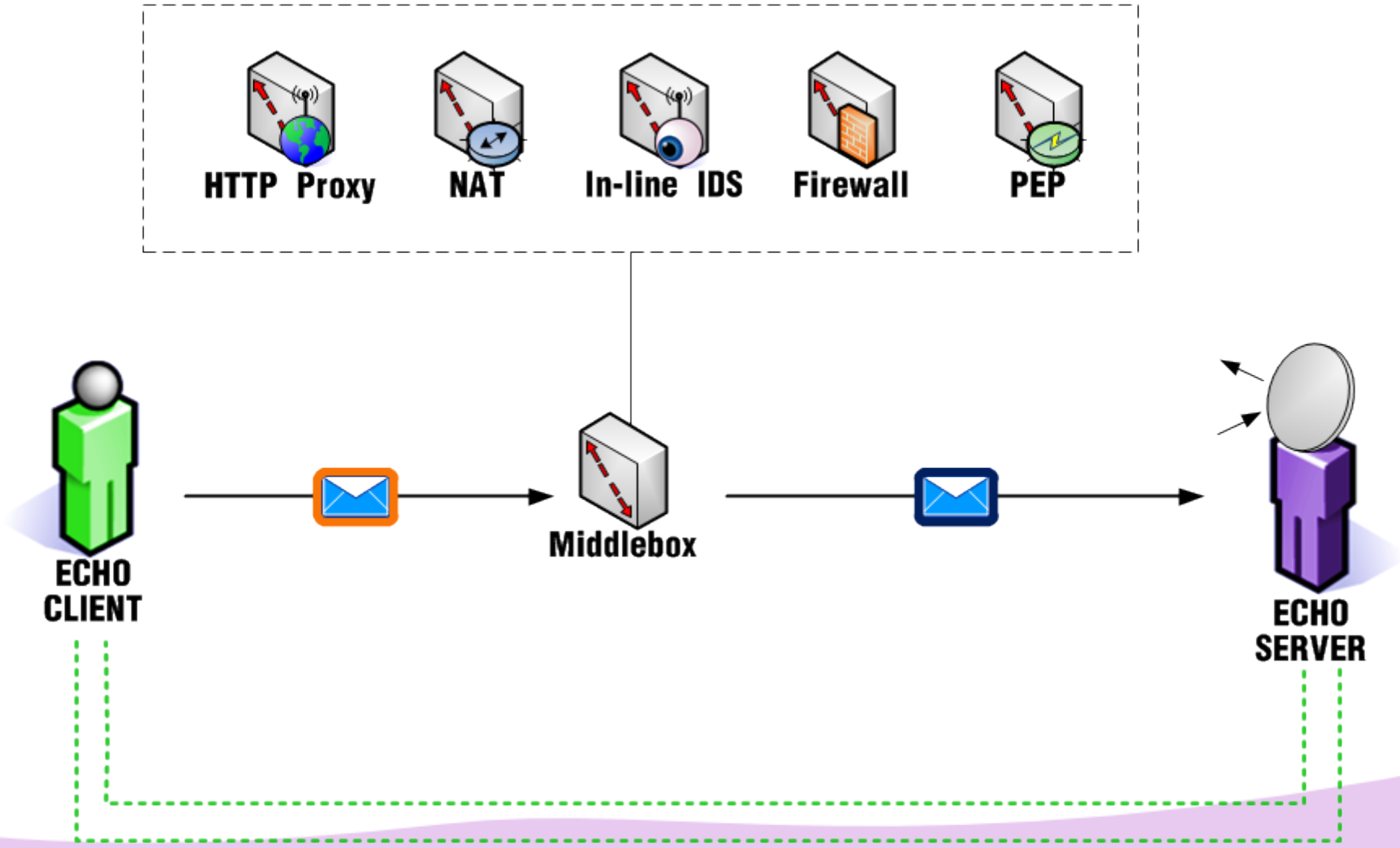
2.1 Basic Operation



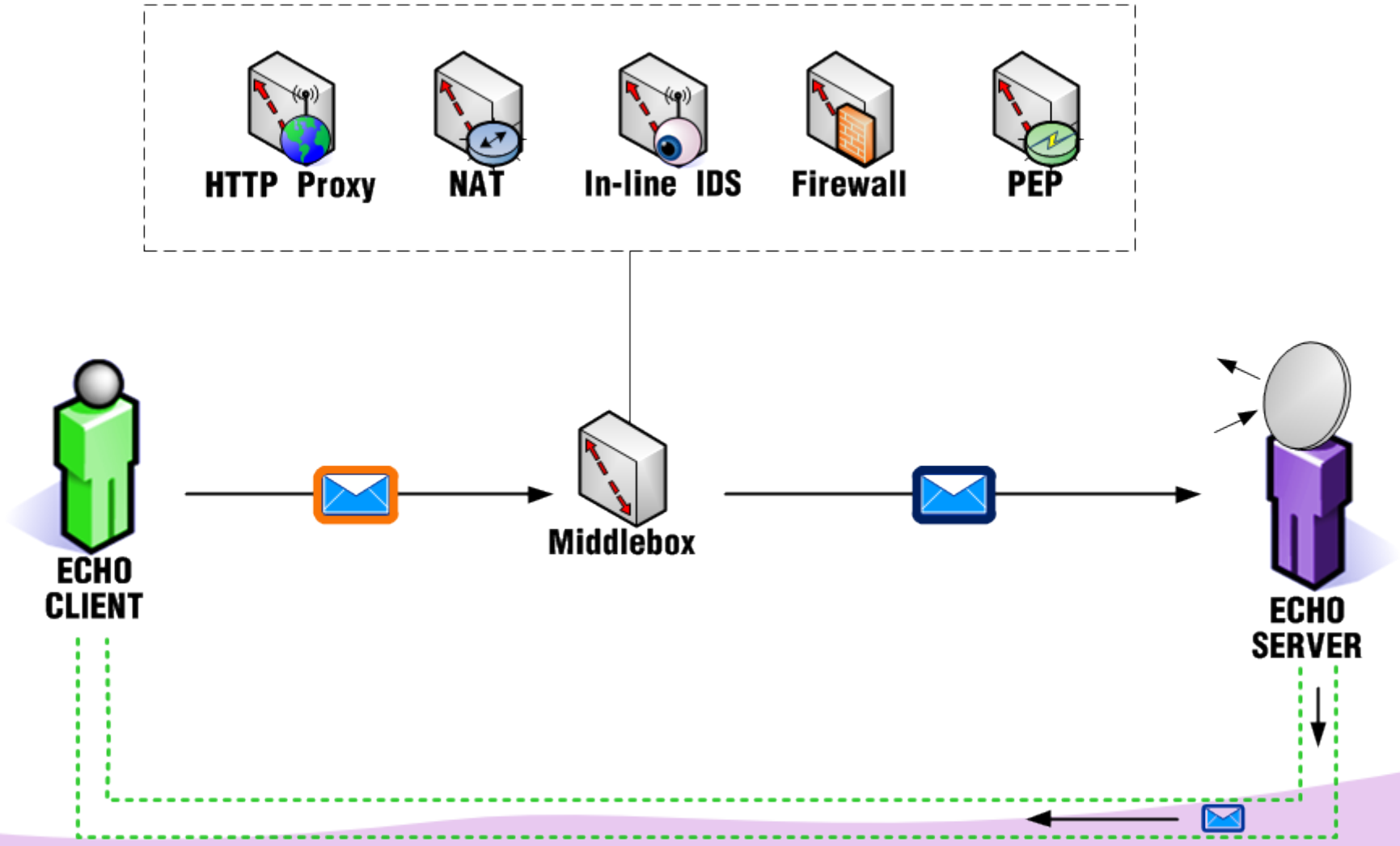
2.1 Basic Operation



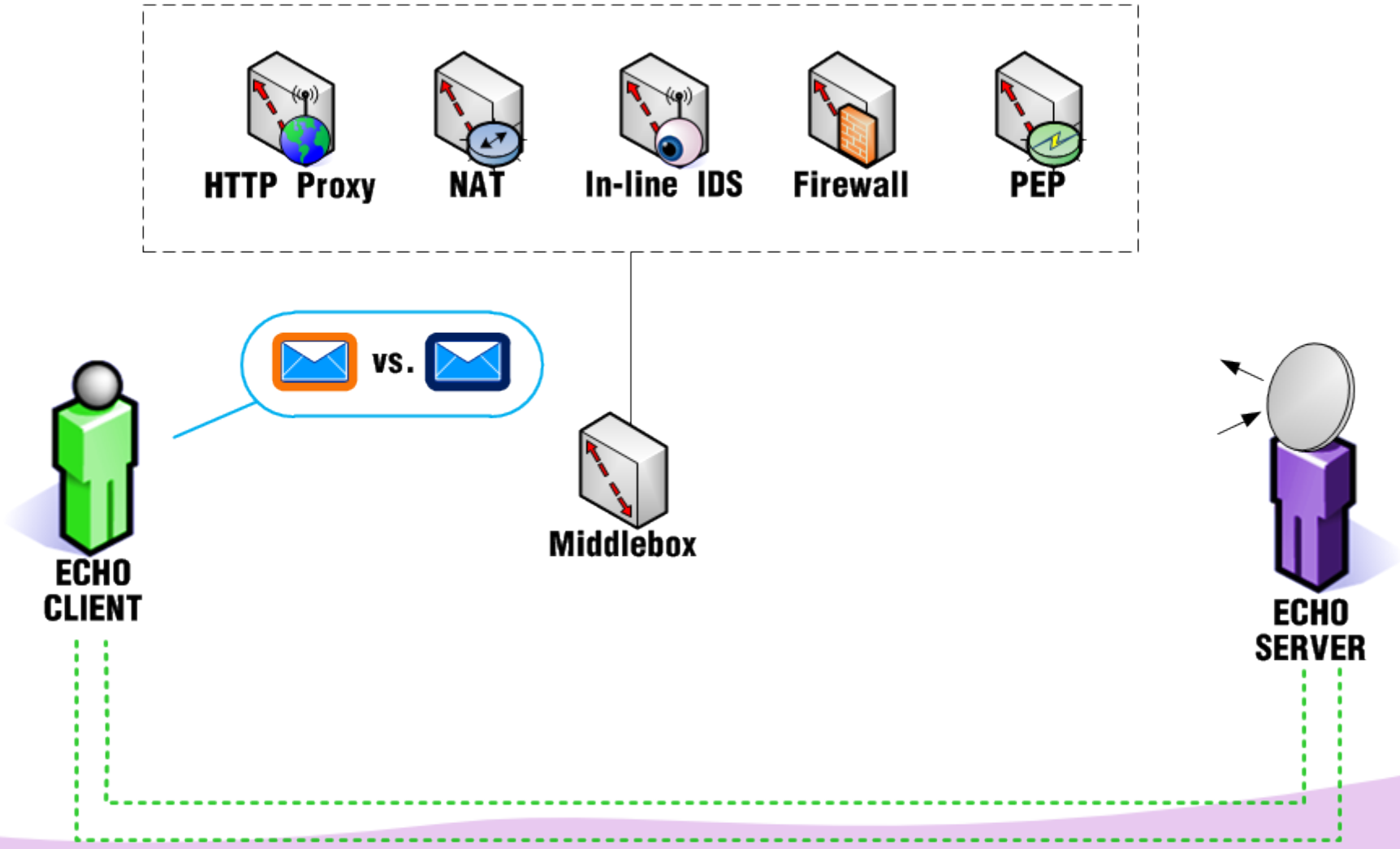
2.1 Basic Operation



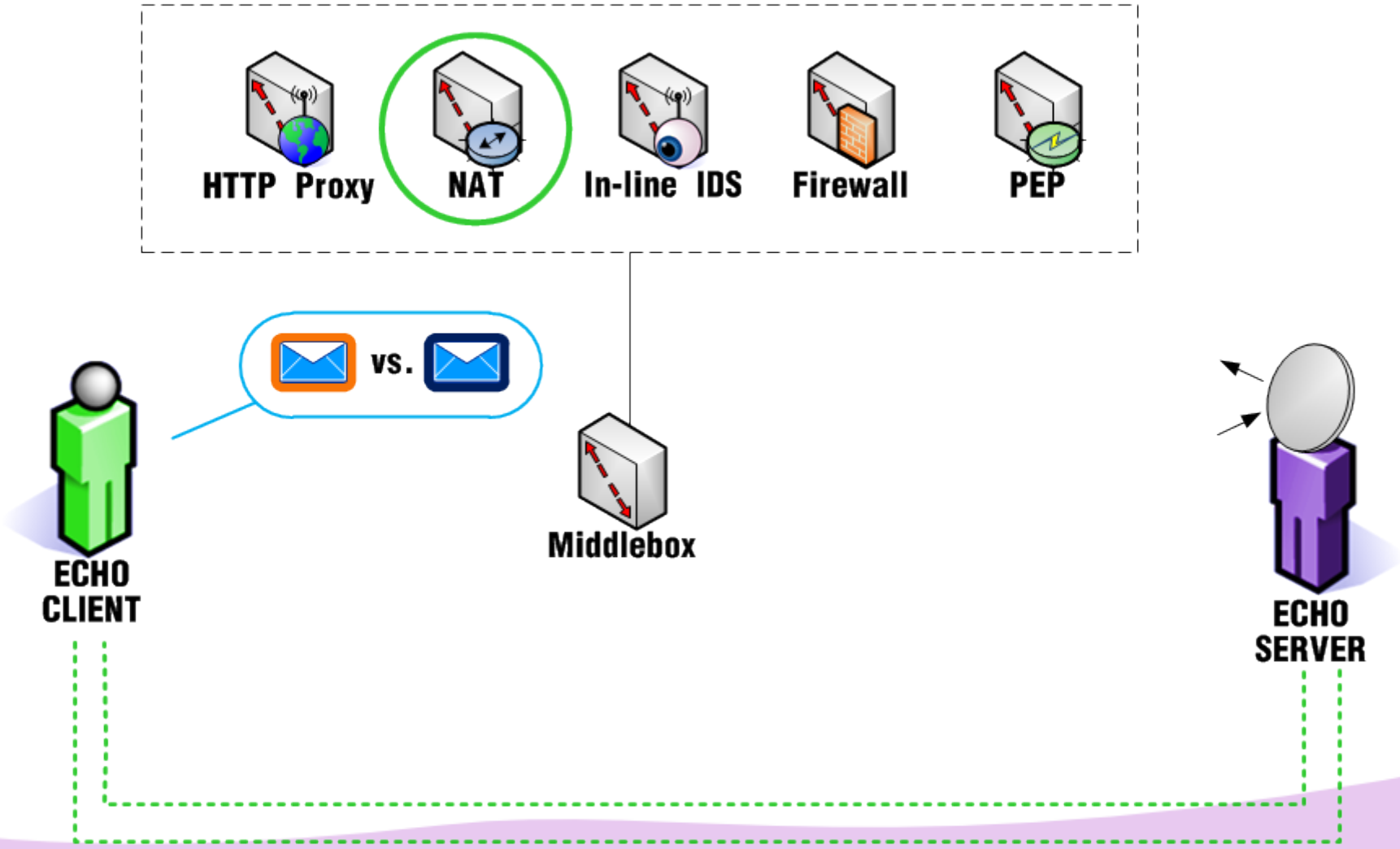
2.1 Basic Operation



2.1 Basic Operation



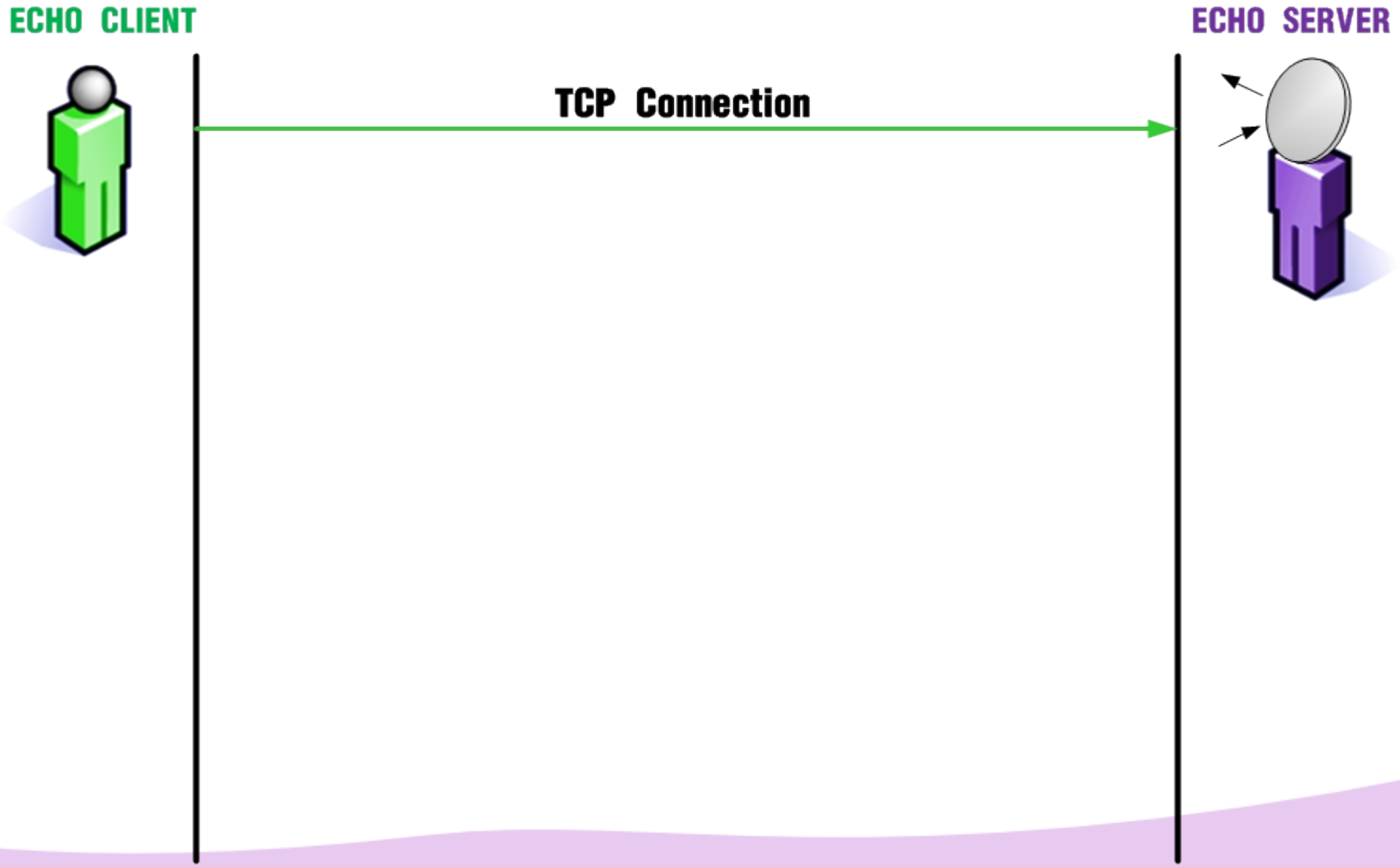
2.1 Basic Operation



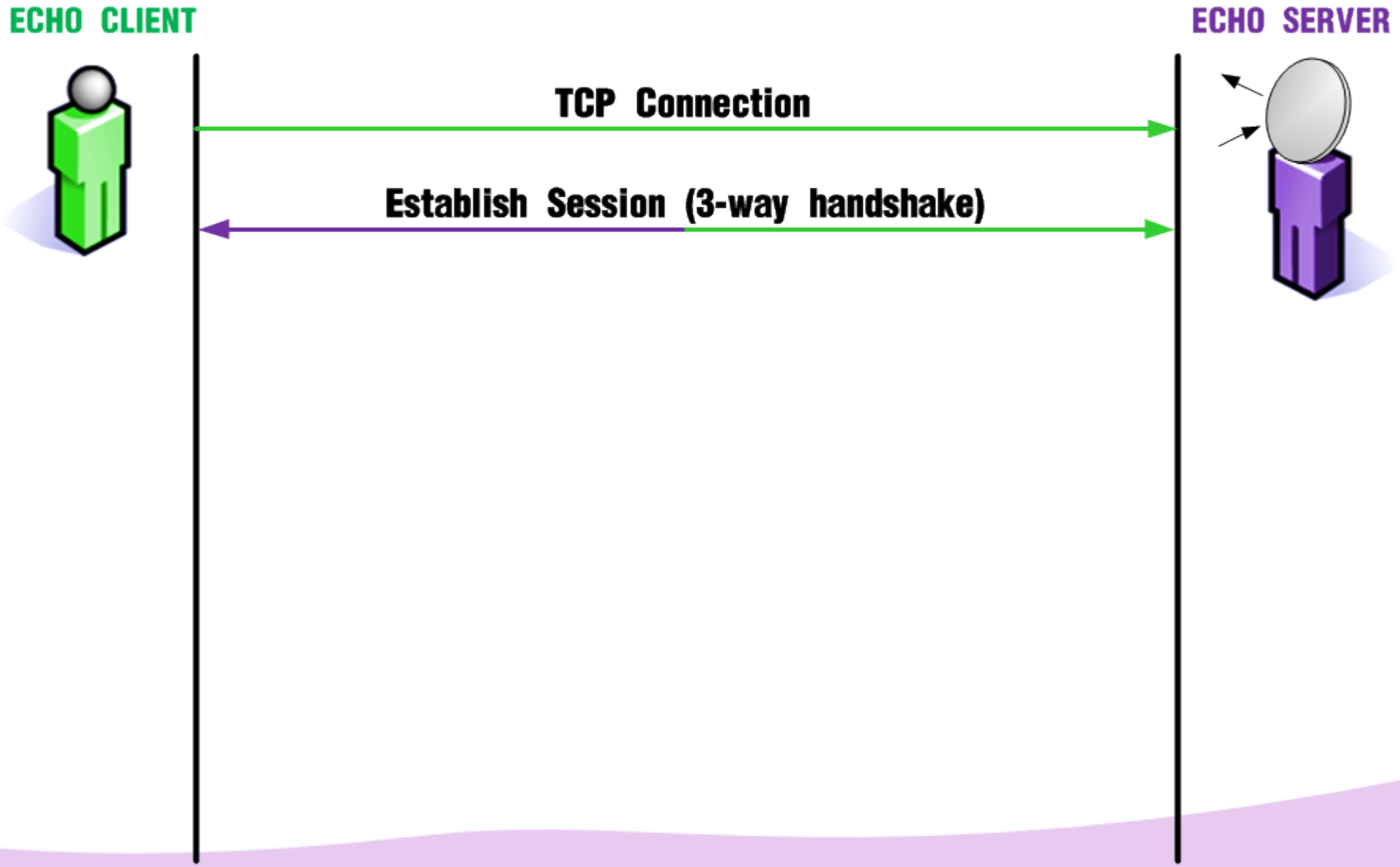
2.2 The Nping Echo Protocol

2.2 The Nping Echo Protocol

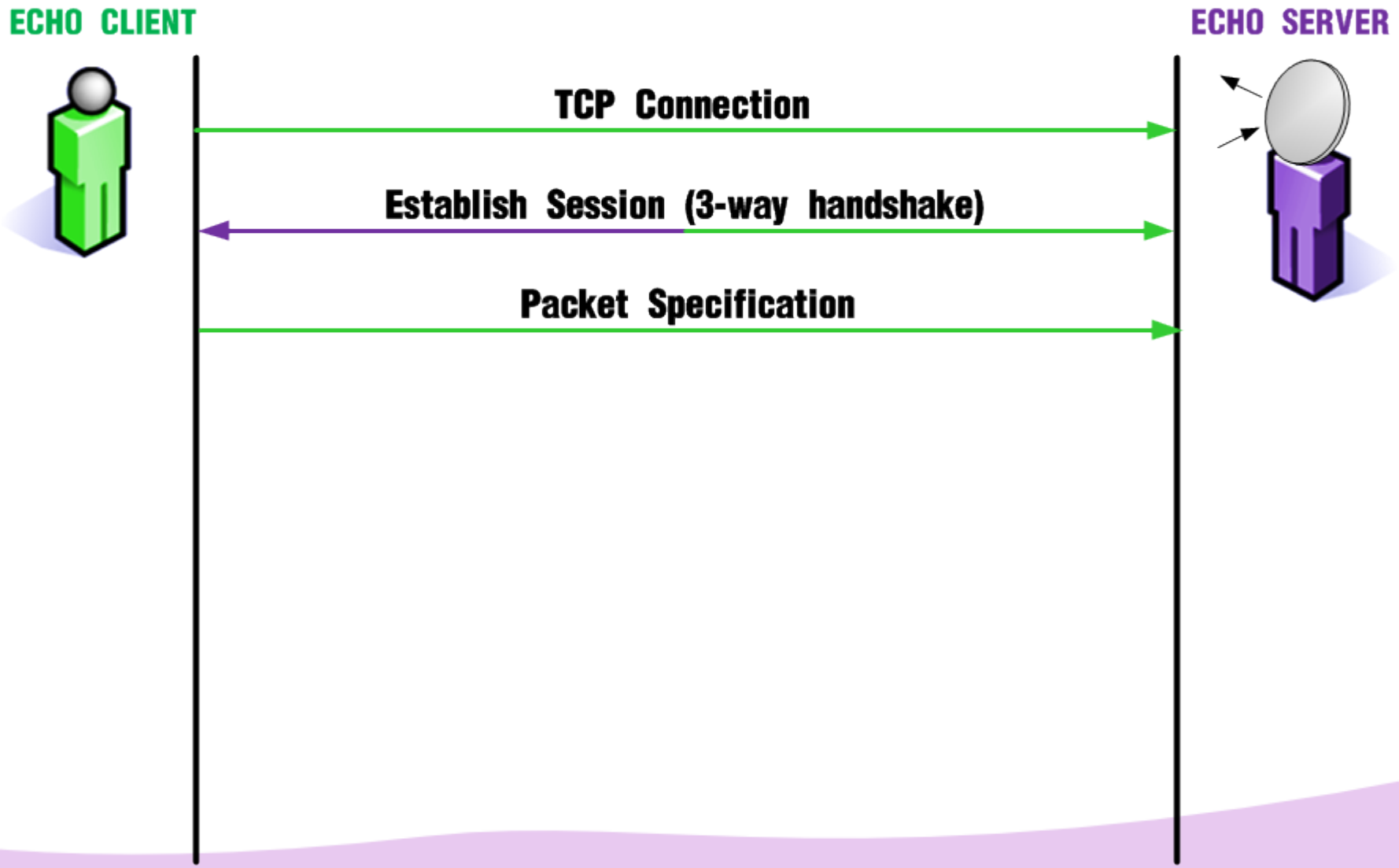
2.2 The Nping Echo Protocol



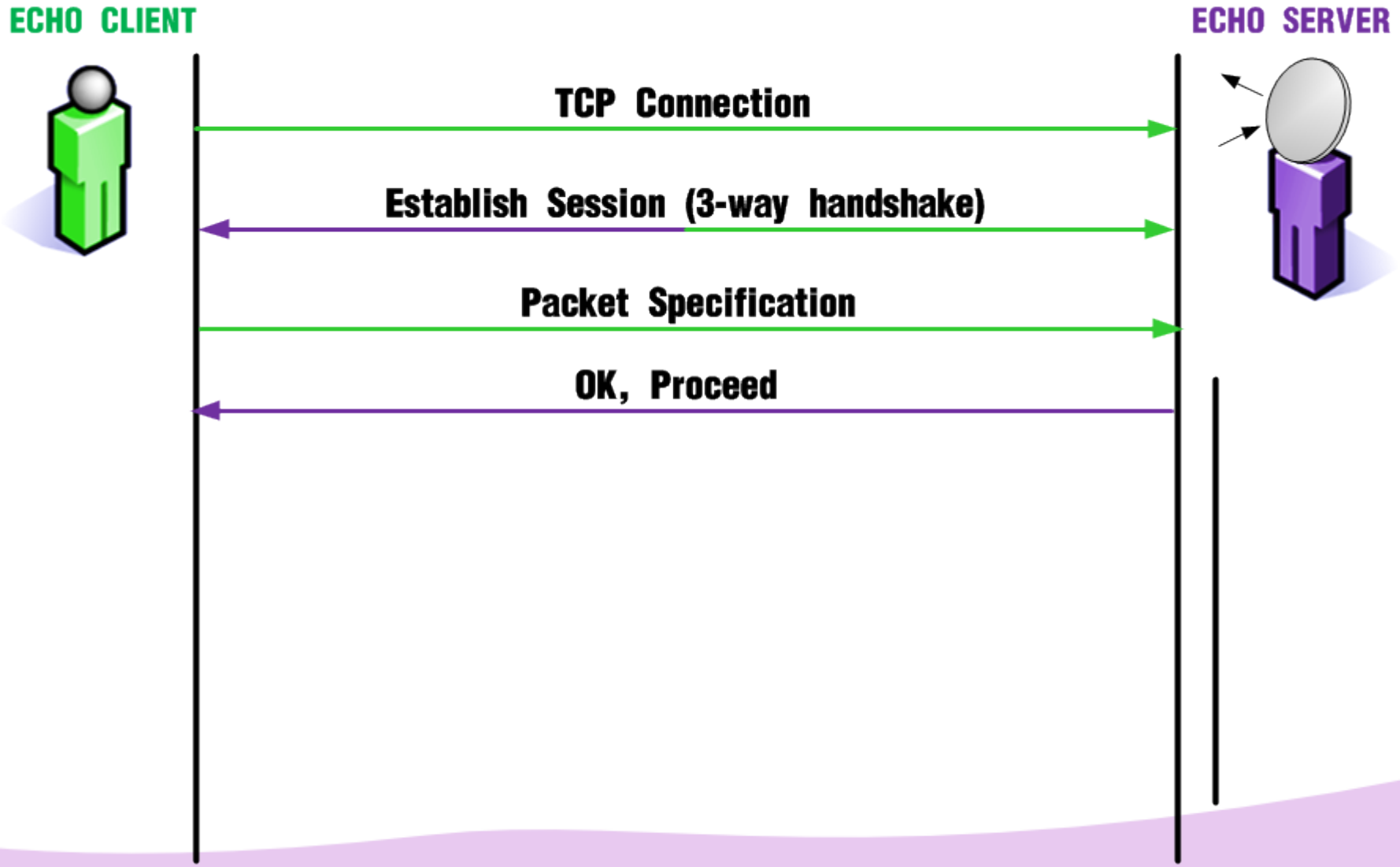
2.2 The Nping Echo Protocol



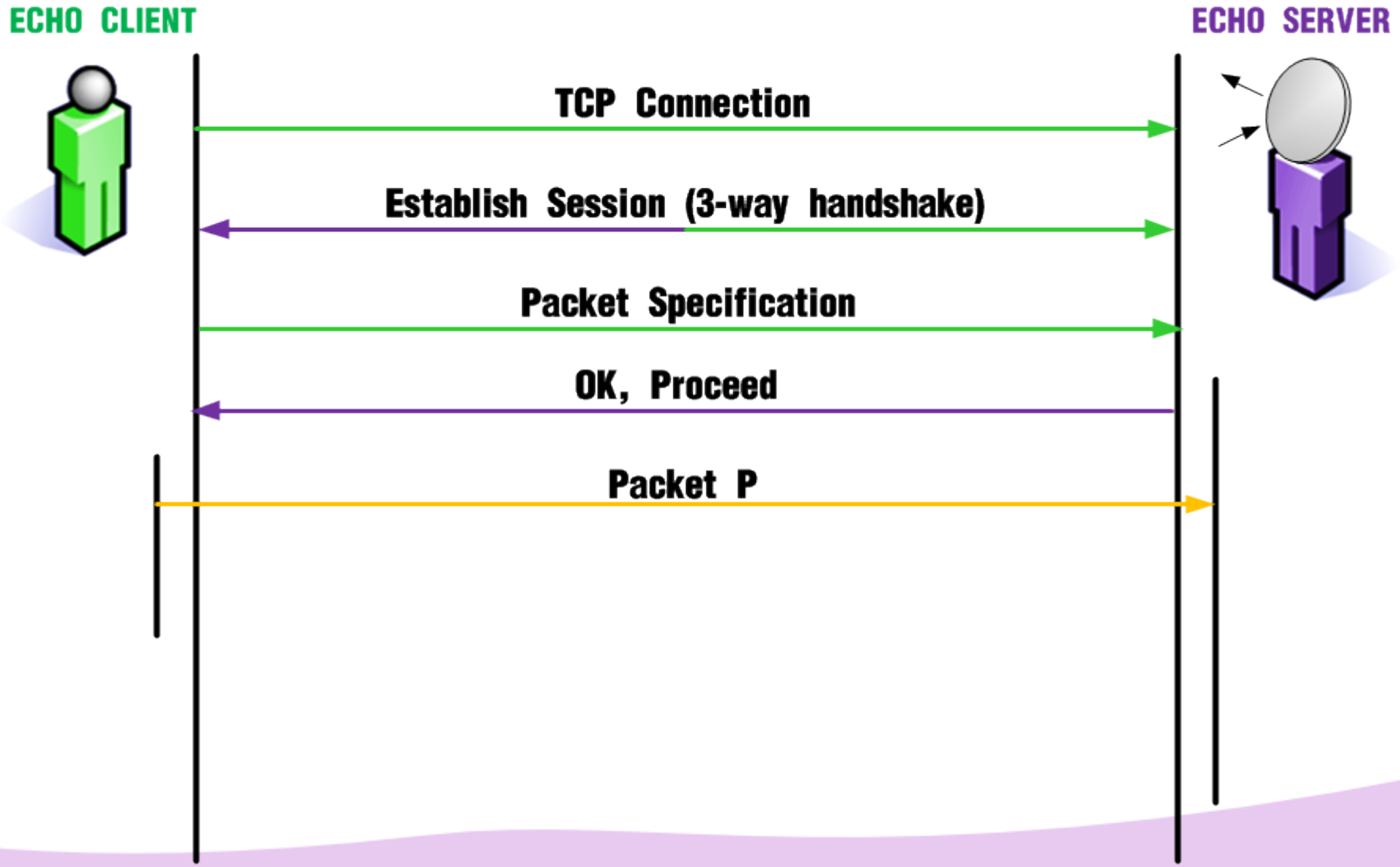
2.2 The Nping Echo Protocol



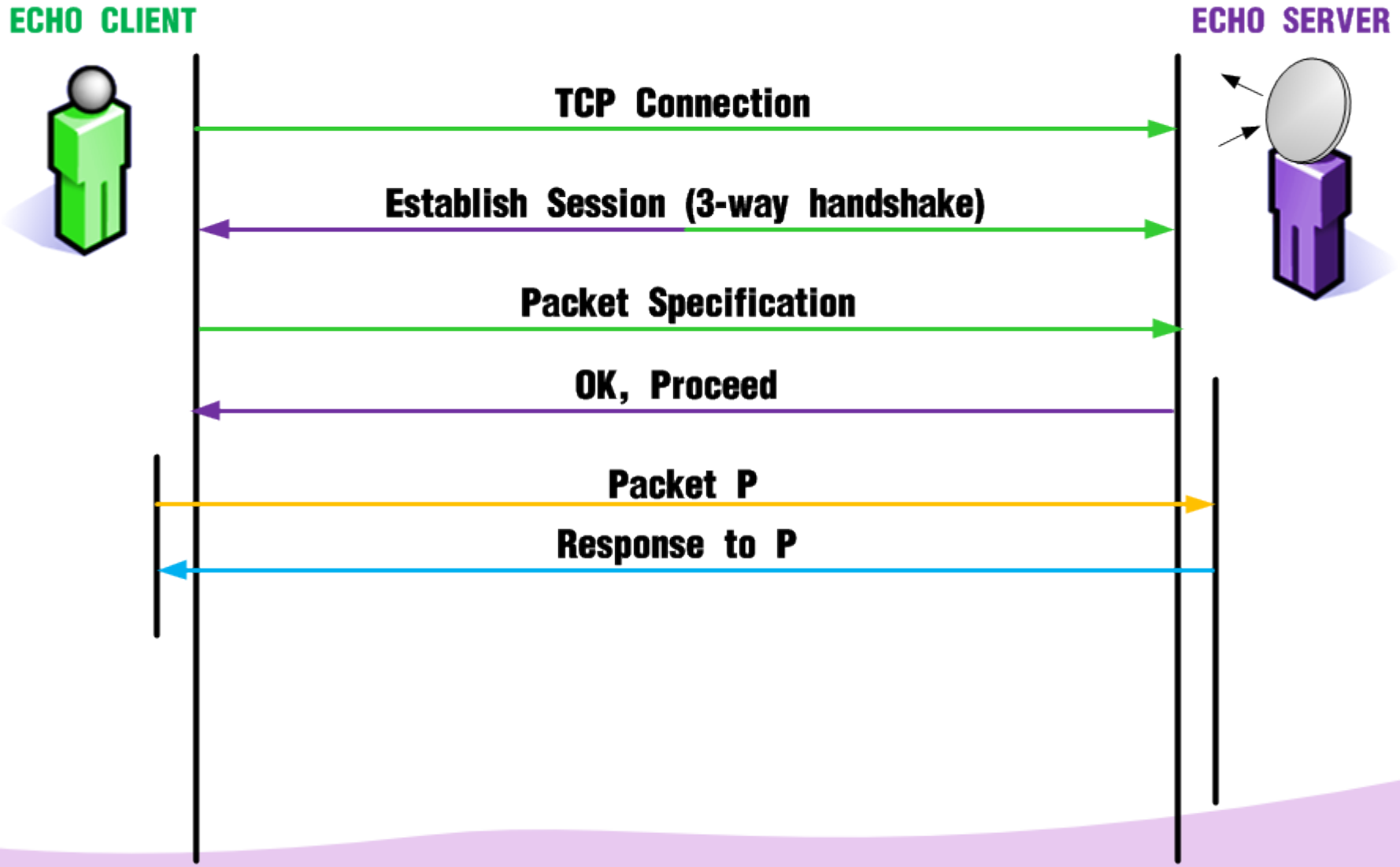
2.2 The Nping Echo Protocol



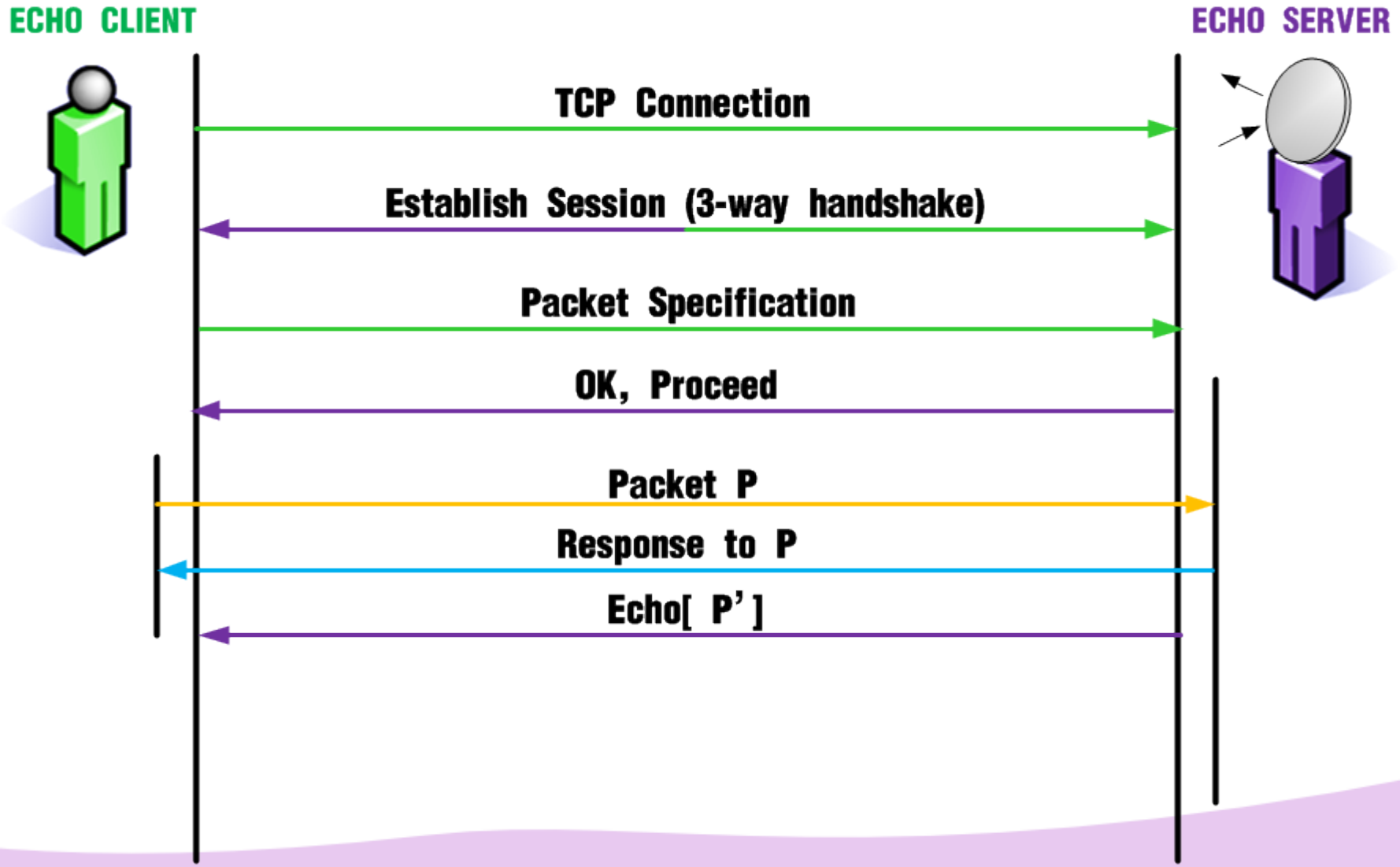
2.2 The Nping Echo Protocol



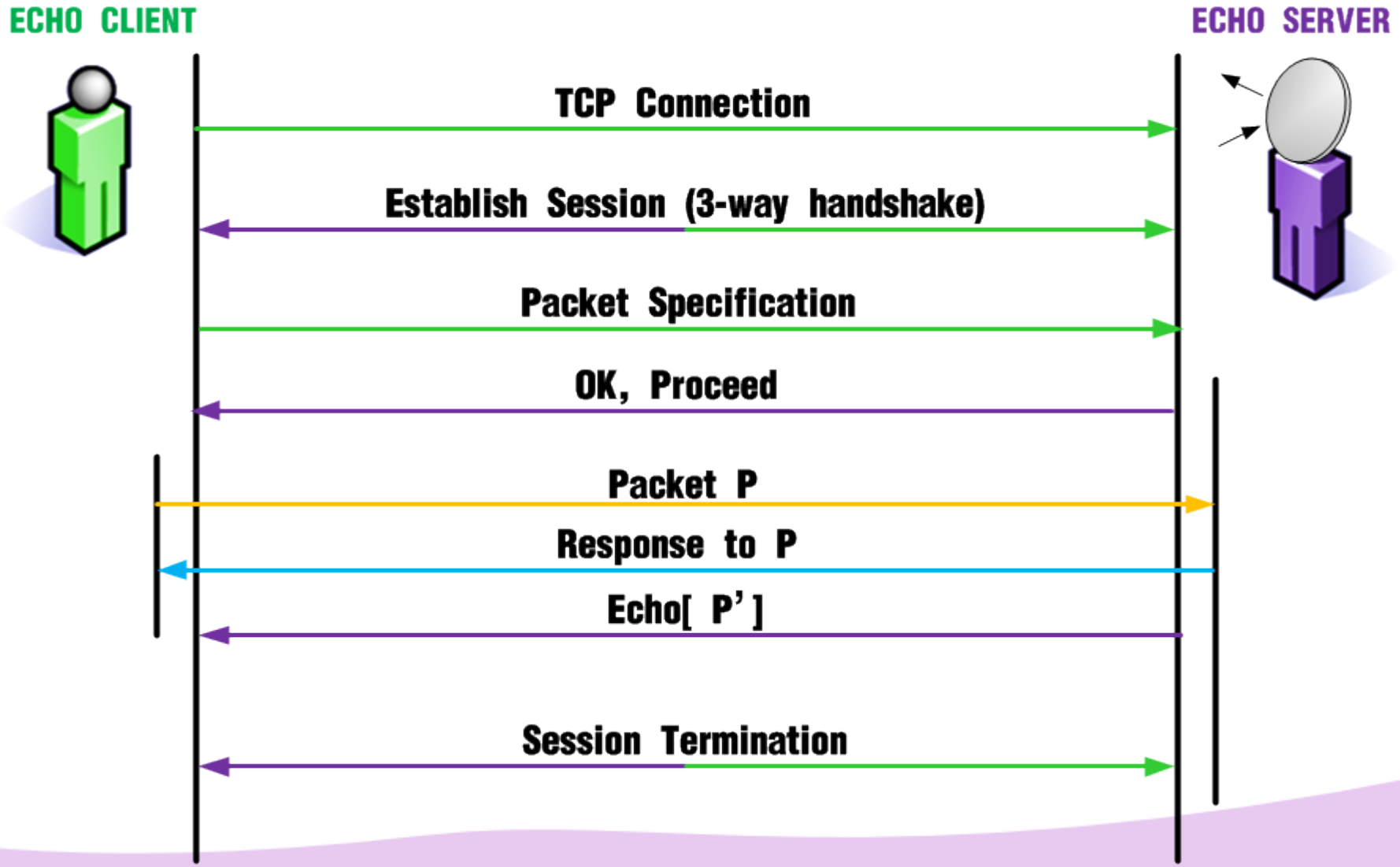
2.2 The Nping Echo Protocol



2.2 The Nping Echo Protocol



2.2 The Nping Echo Protocol

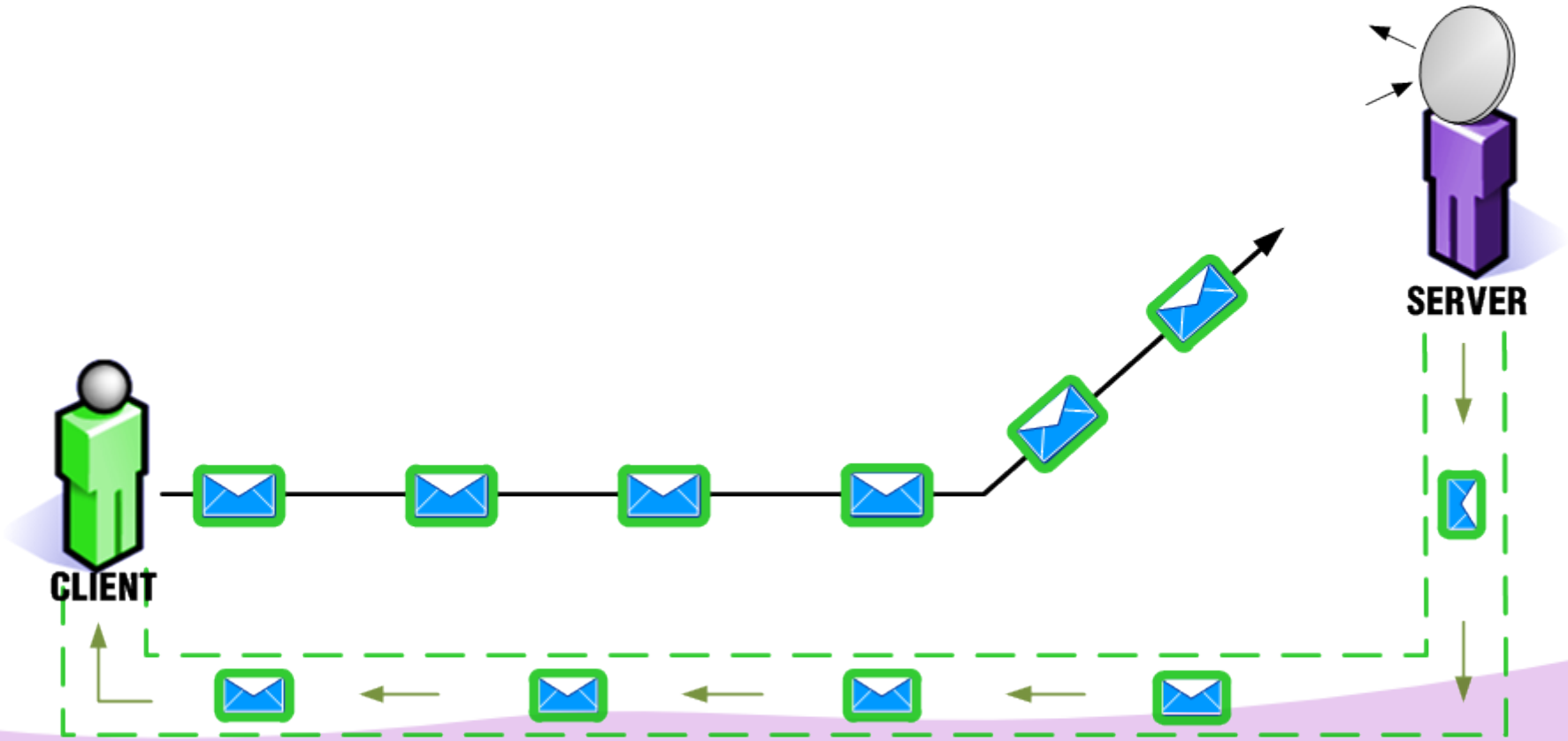


2.3 Security and Implementation Challenges

- Problem: Packet Matching

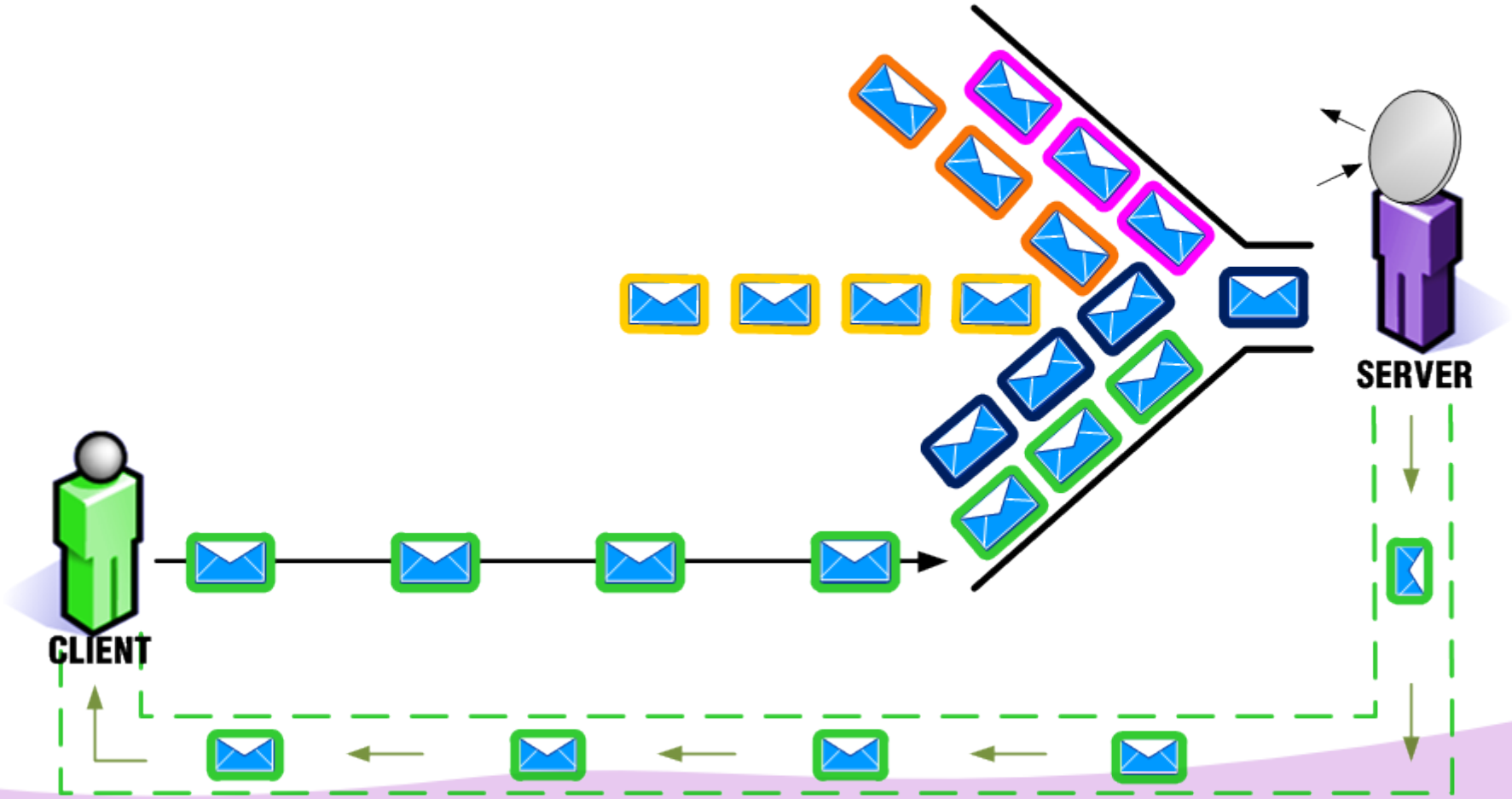
2.3 Security and Implementation Challenges

- Problem: Packet Matching



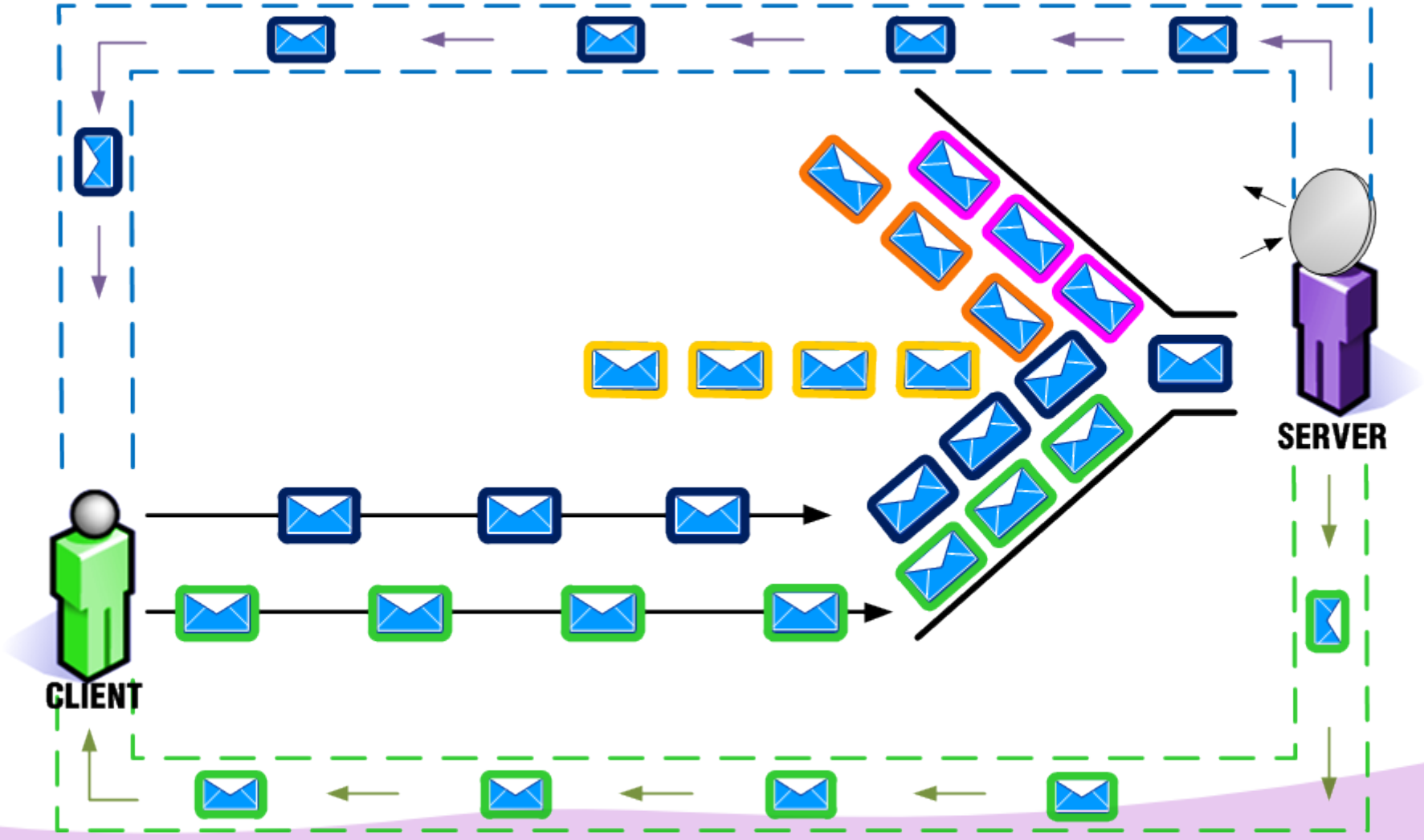
2.3 Security and Implementation Challenges

- Problem: Packet Matching



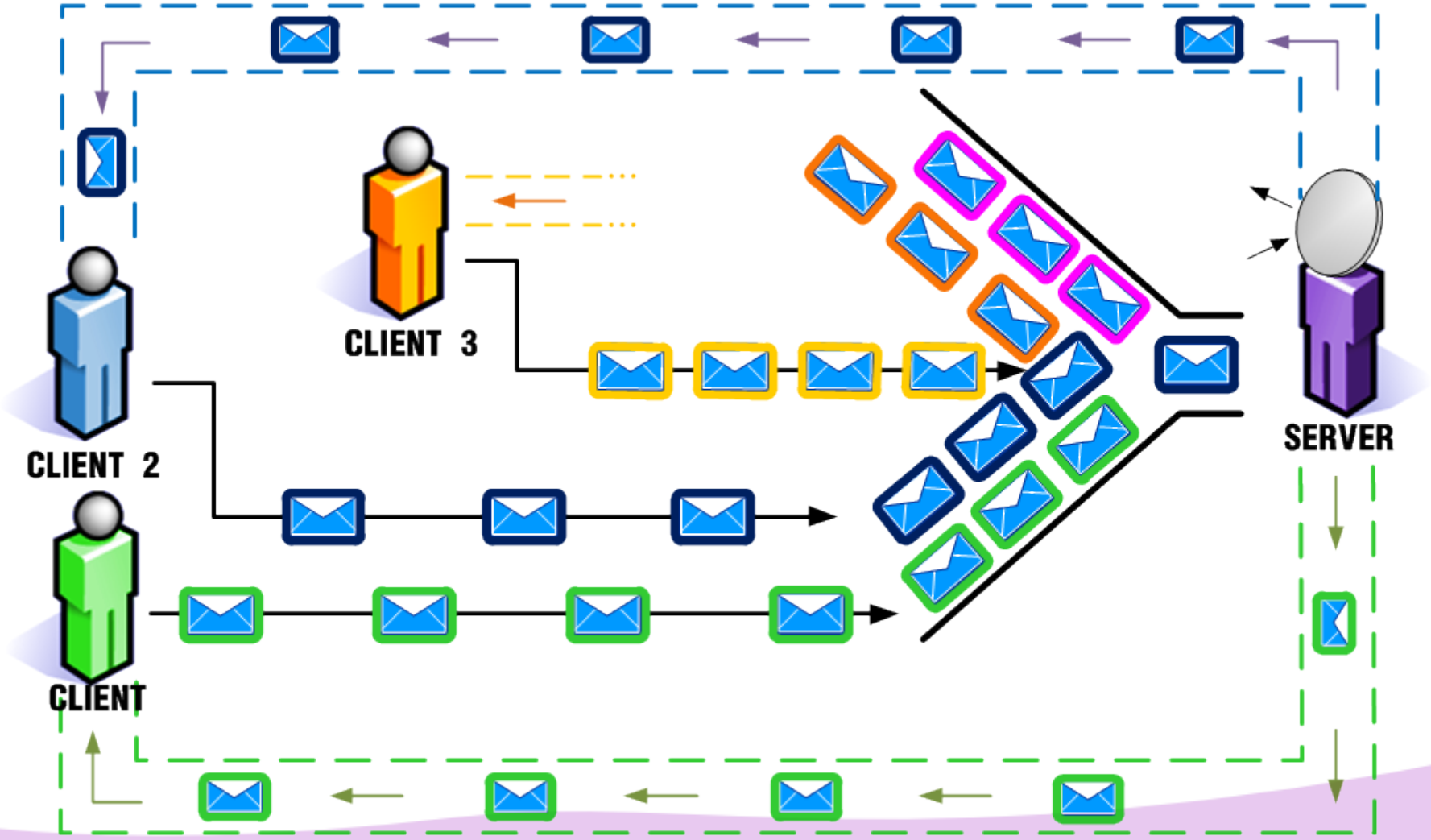
2.3 Security and Implementation Challenges

- Problem: Packet Matching



2.3 Security and Implementation Challenges

- Problem: Packet Matching

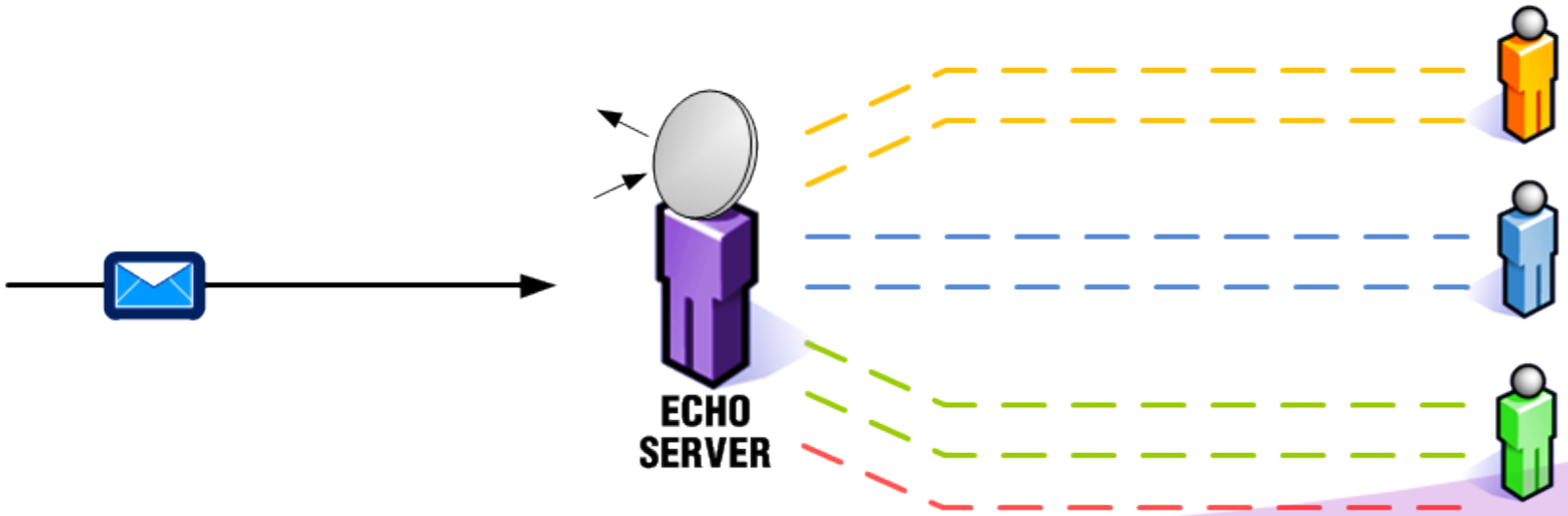


2.3 Security and Implementation Challenges

- Solution: Scoring Algorithm

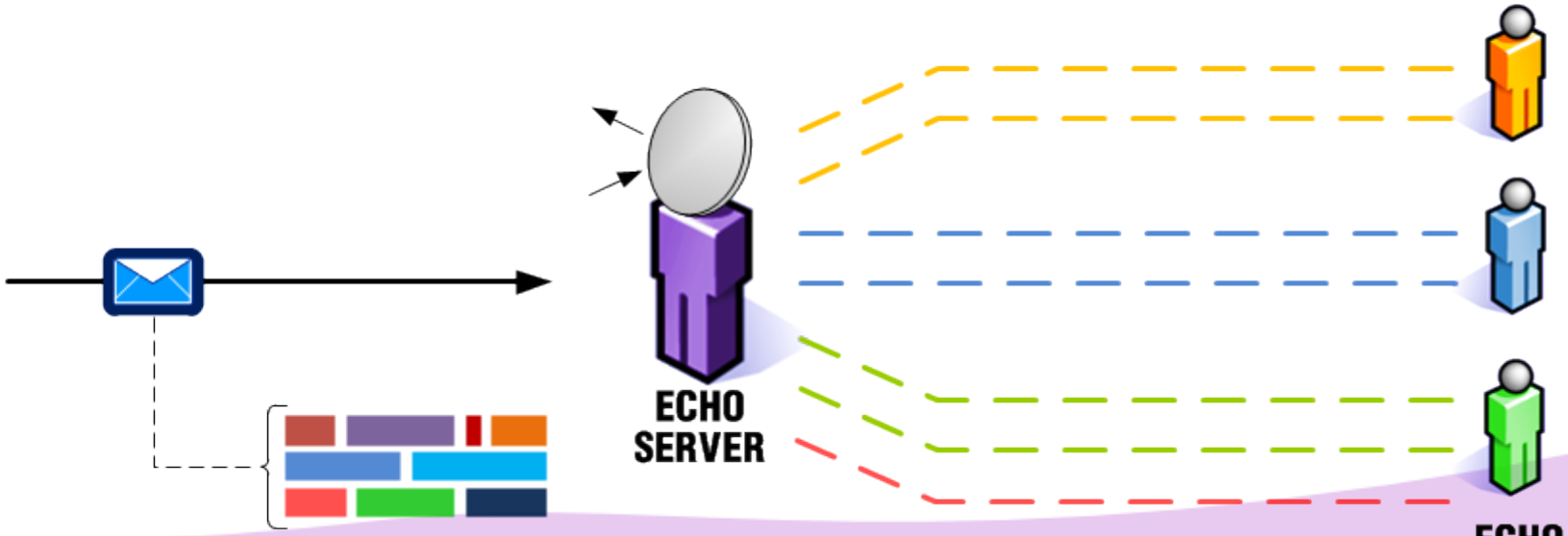
2.3 Security and Implementation Challenges

- Solution: Scoring Algorithm



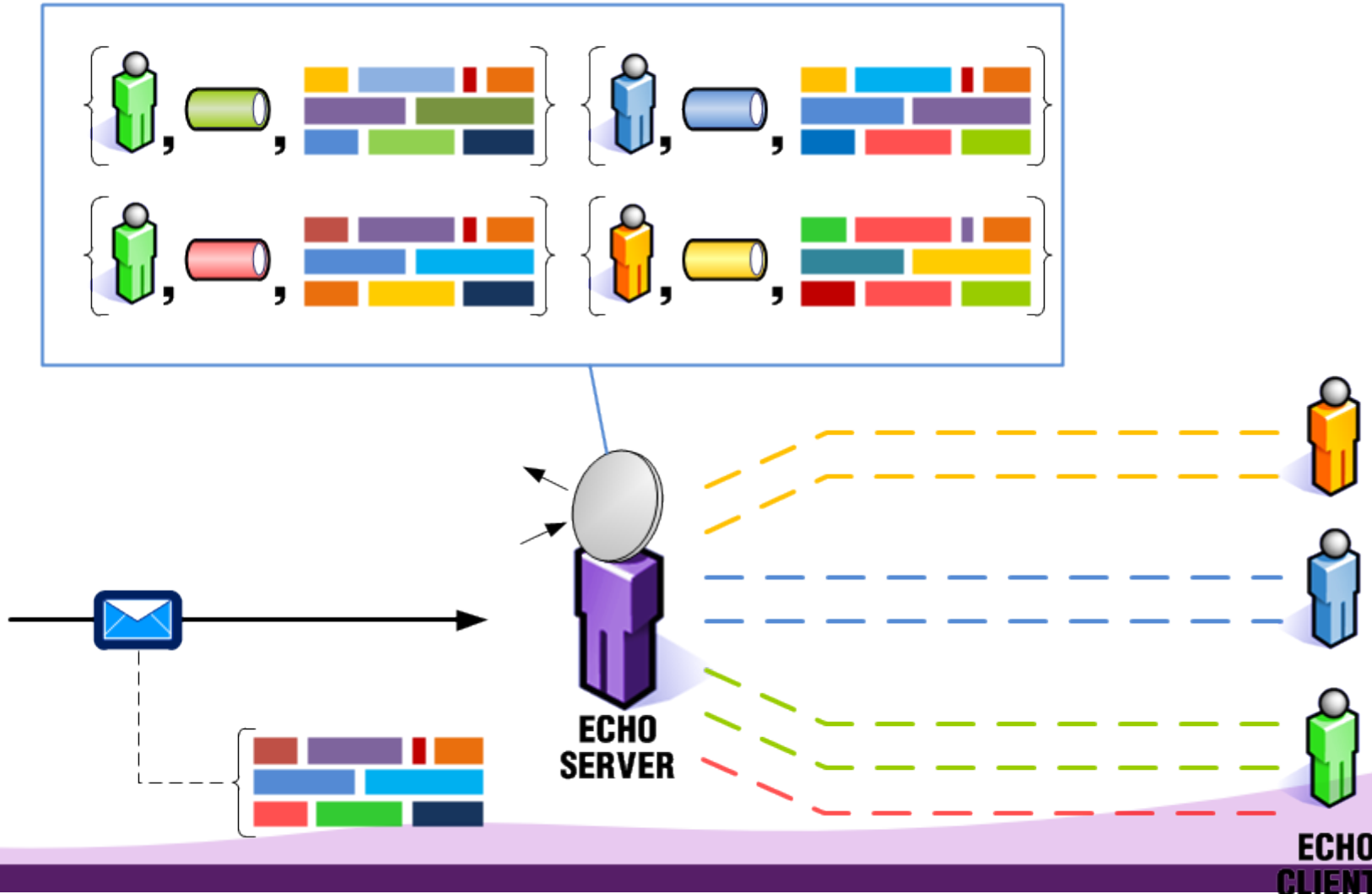
2.3 Security and Implementation Challenges

- Solution: Scoring Algorithm



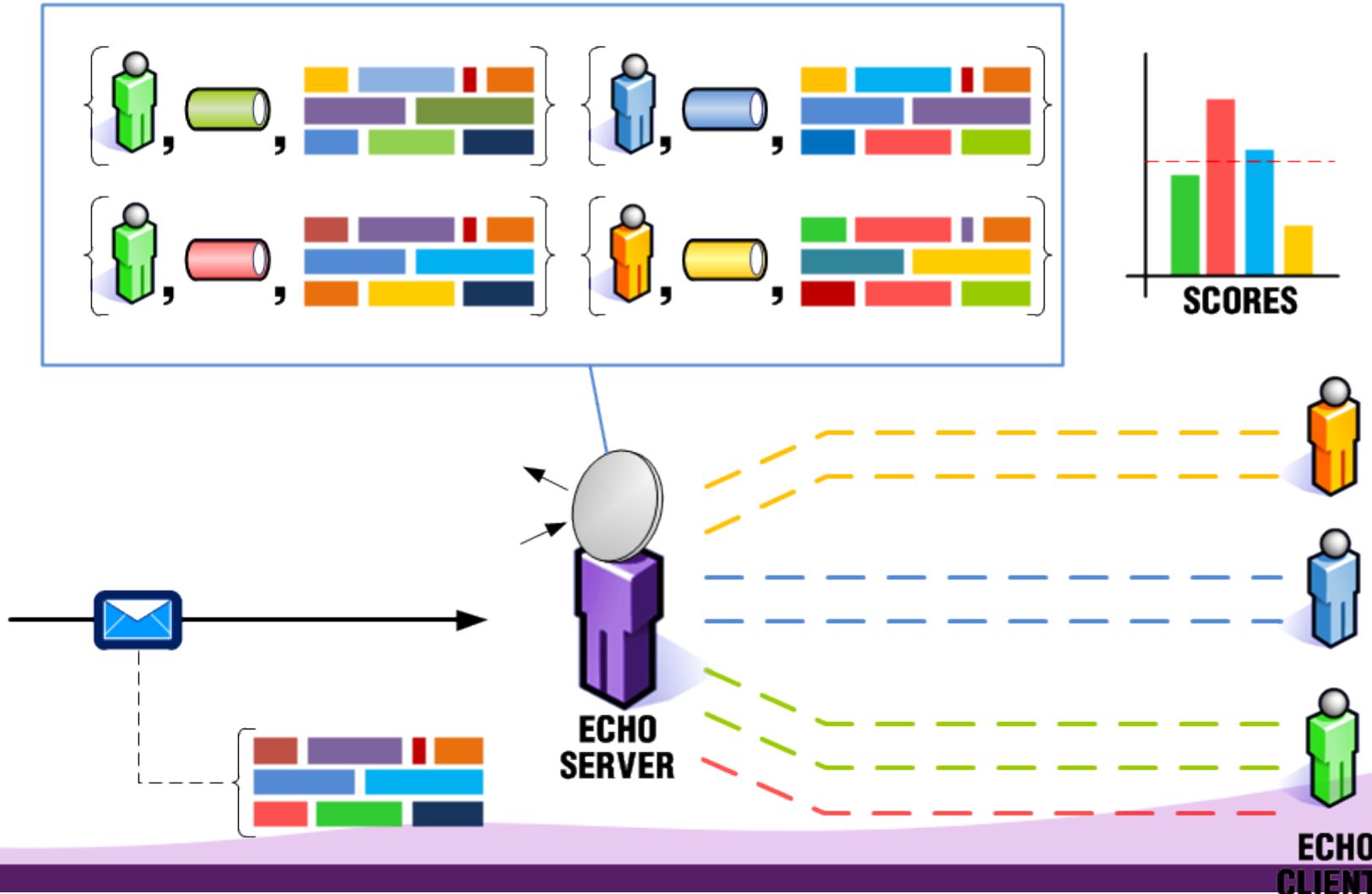
2.3 Security and Implementation Challenges

- Solution: Scoring Algorithm



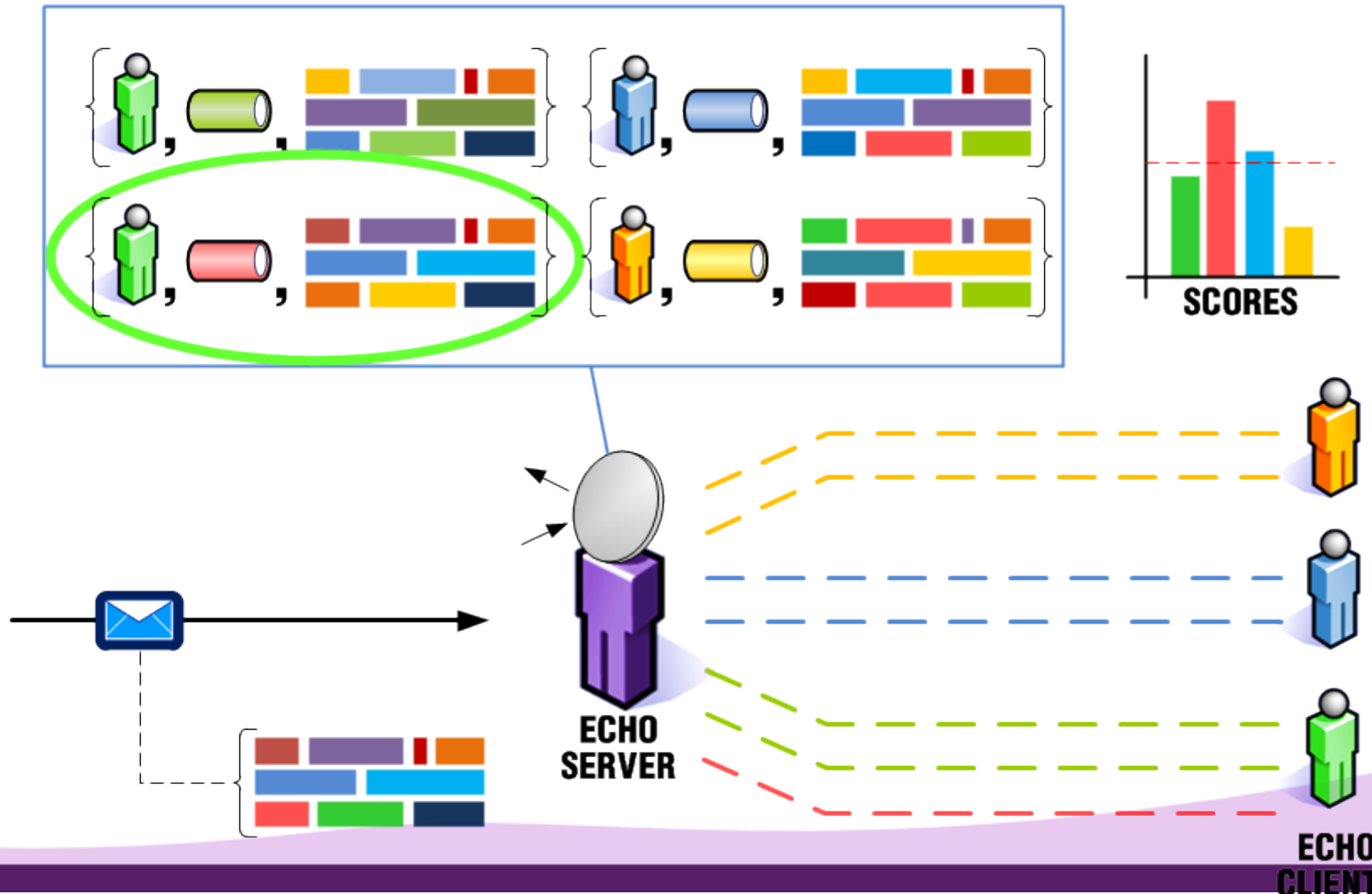
2.3 Security and Implementation Challenges

- Solution: Scoring Algorithm



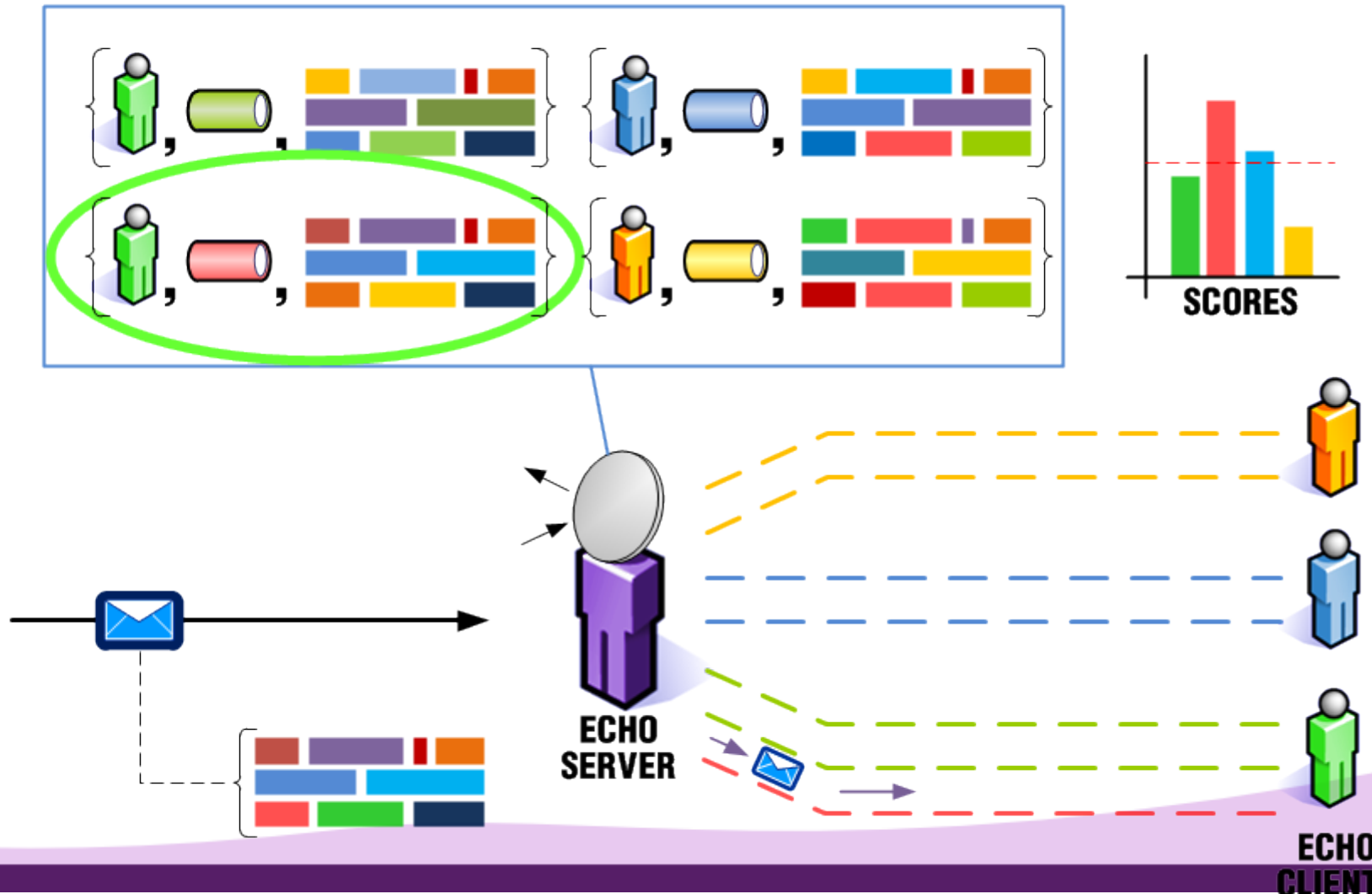
2.3 Security and Implementation Challenges

- Solution: Scoring Algorithm



2.3 Security and Implementation Challenges

- Solution: Scoring Algorithm

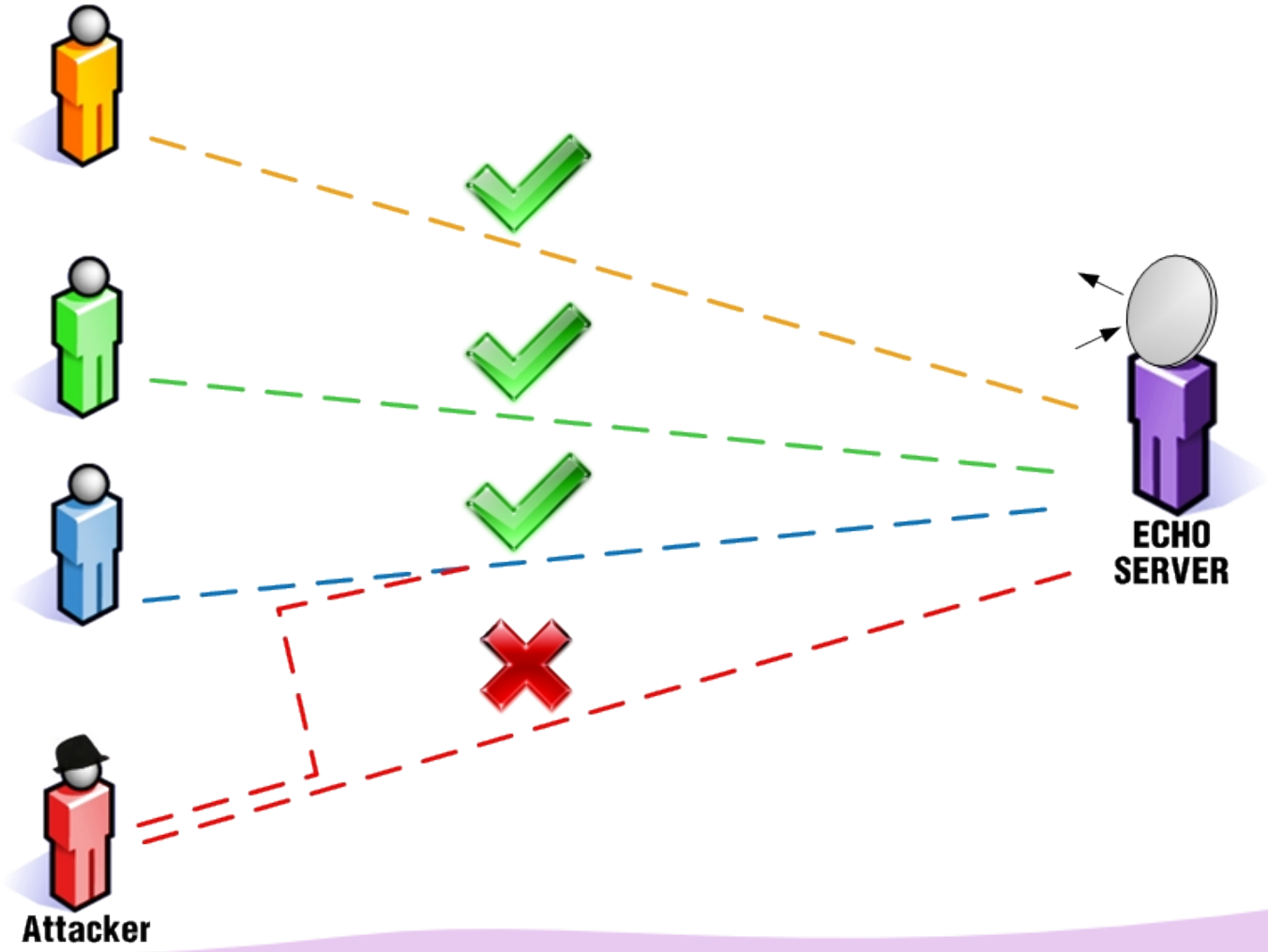


2.3 Security and Implementation Challenges

- Problem: Restricting Access

2.3 Security and Implementation Challenges

- Problem: Restricting Access



2.3 Security and Implementation Challenges

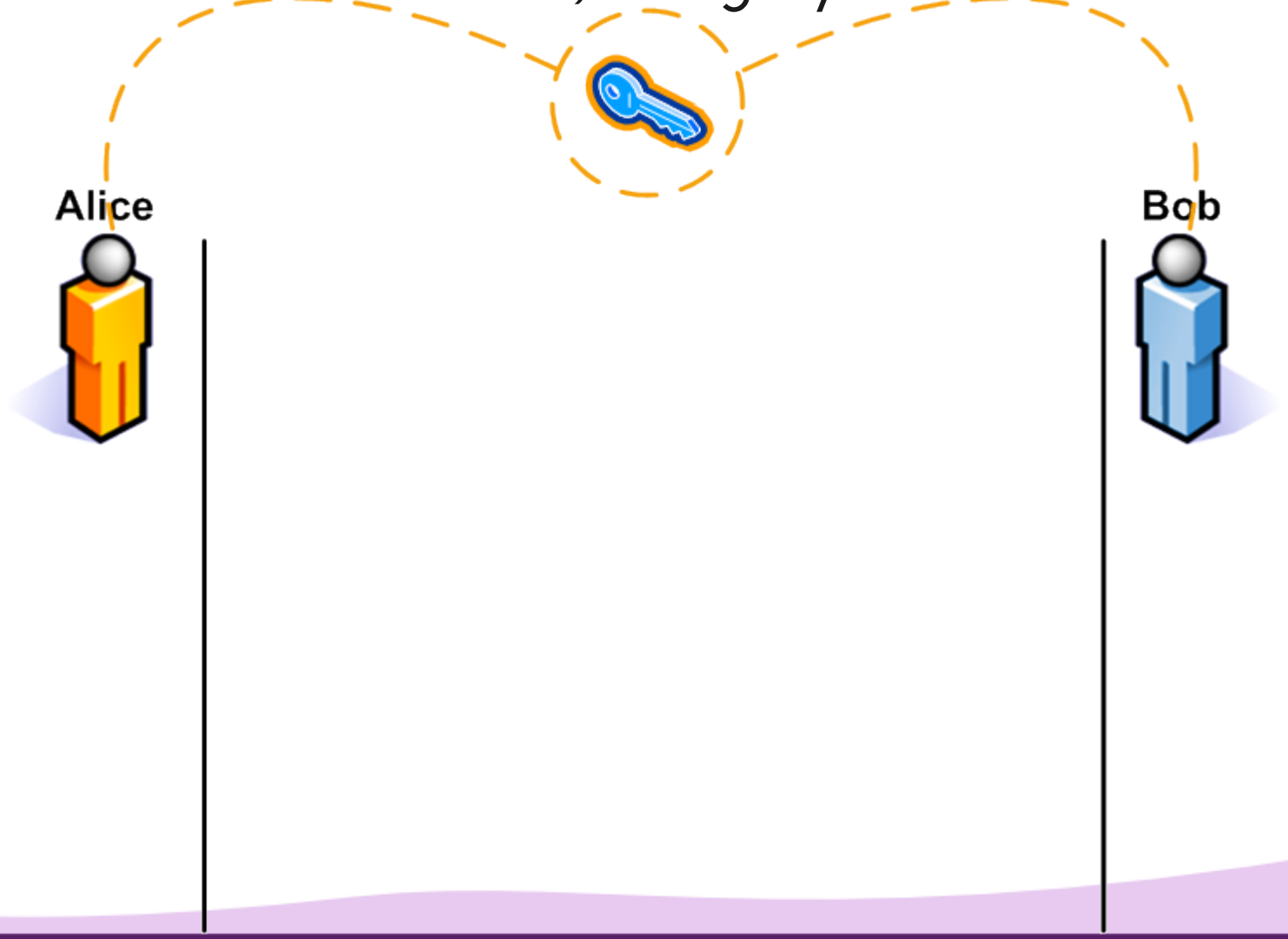
- Solution: Authentication, Integrity and Confidentiality

2.3 Security and Implementation Challenges

- Solution: Authentication, Integrity and Confidentiality

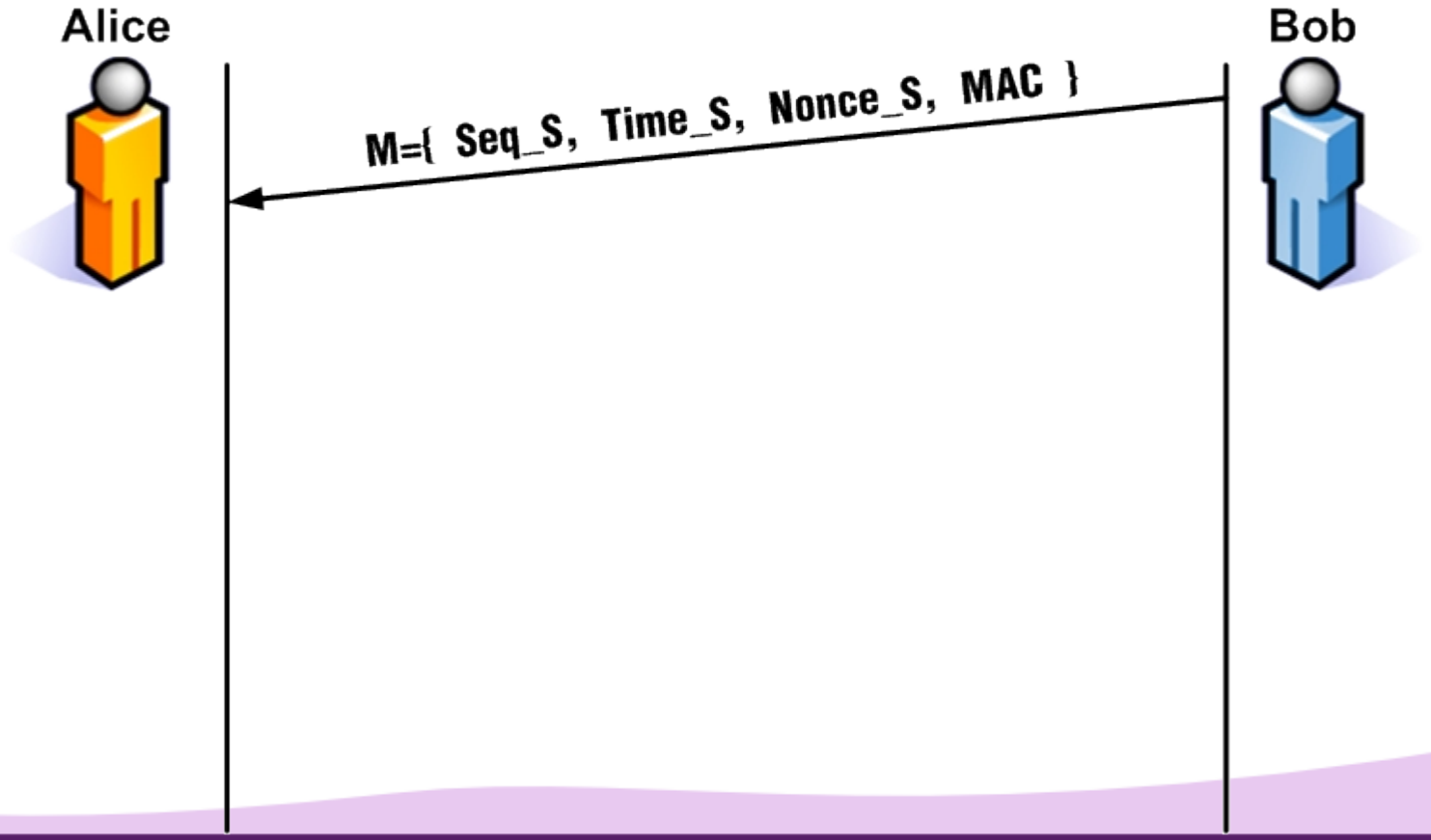
2.3 Security and Implementation Challenges

- Solution: Authentication, Integrity and Confidentiality



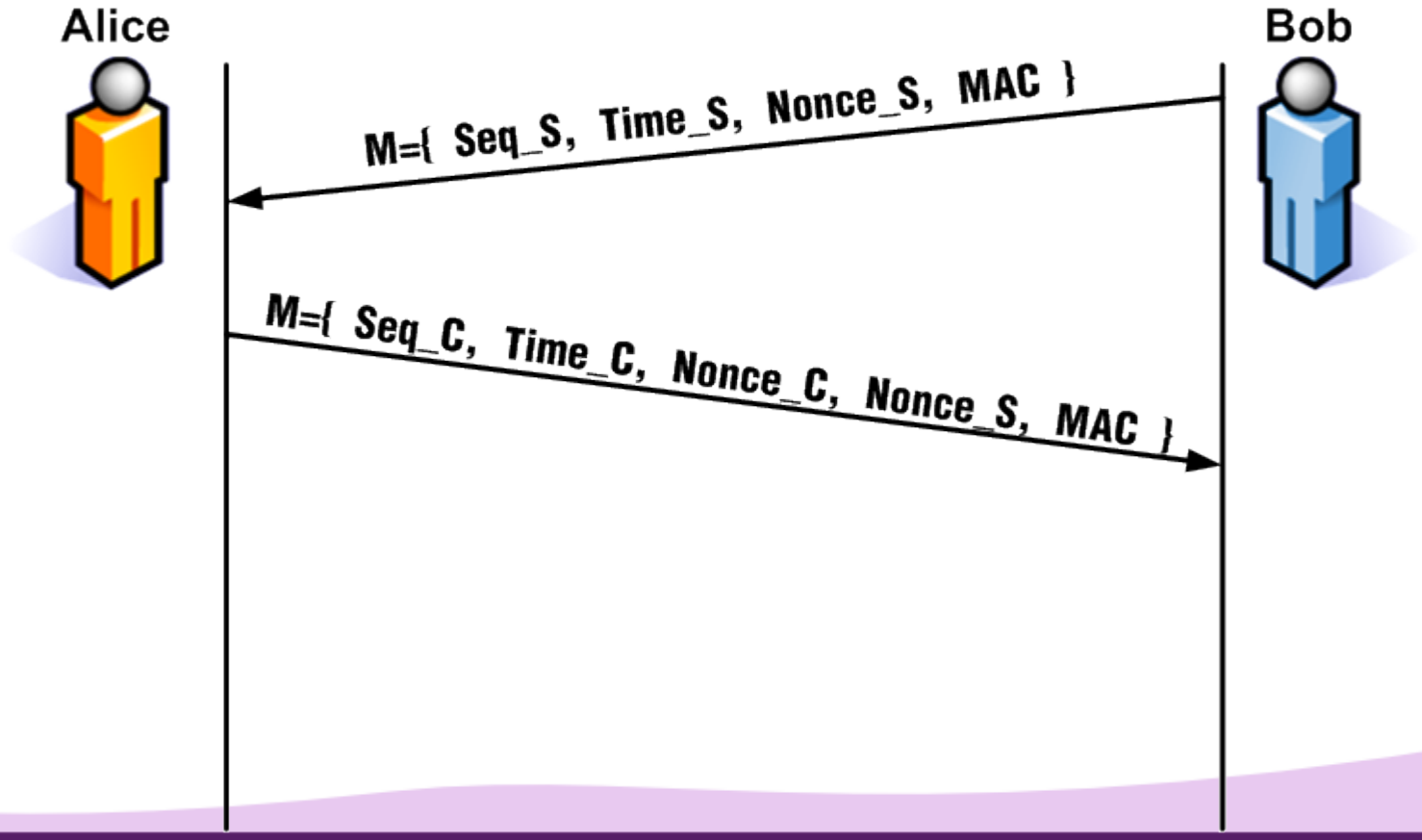
2.3 Security and Implementation Challenges

- Solution: Authentication, Integrity and Confidentiality



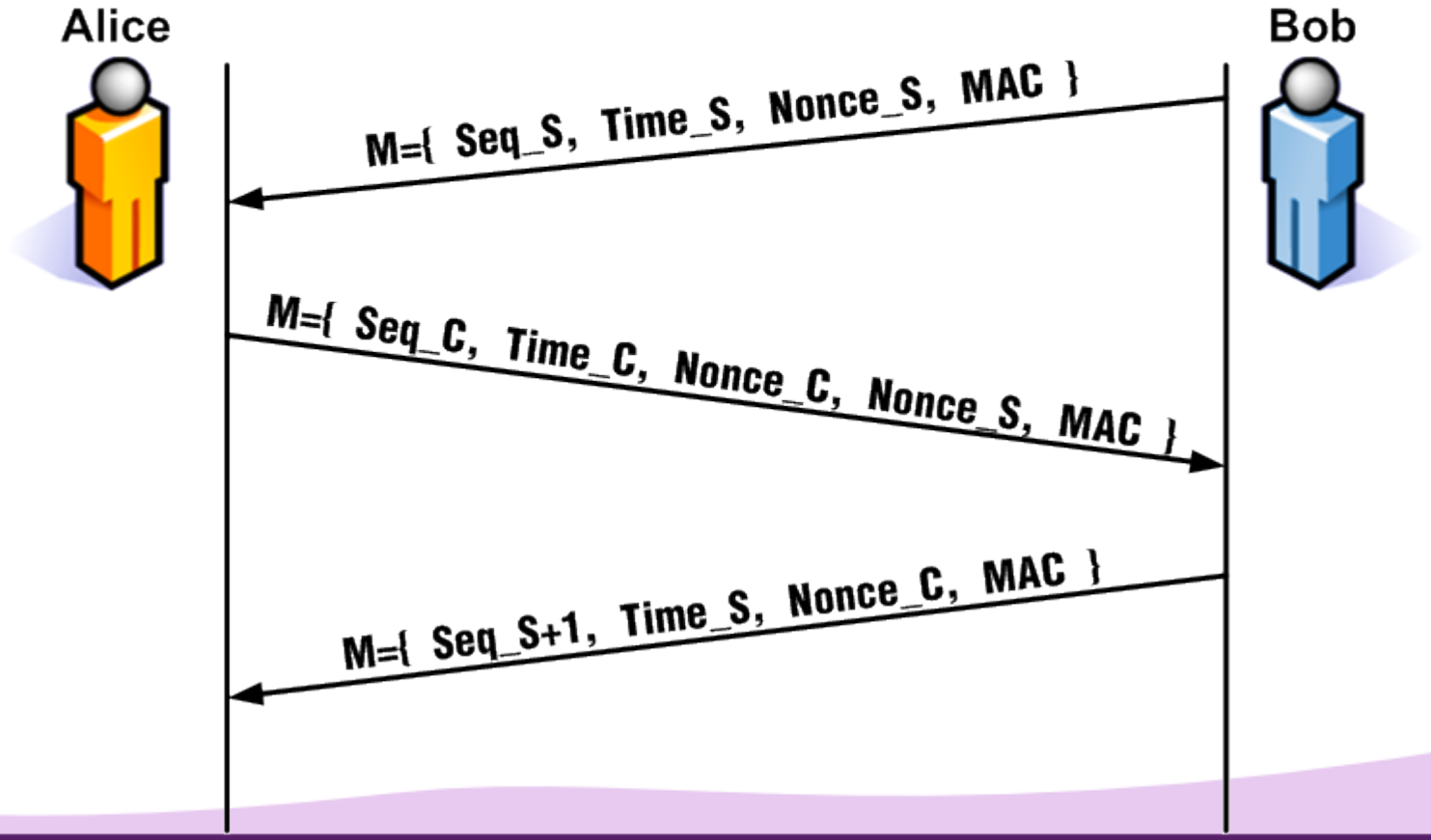
2.3 Security and Implementation Challenges

- Solution: Authentication, Integrity and Confidentiality



2.3 Security and Implementation Challenges

- Solution: Authentication, Integrity and Confidentiality

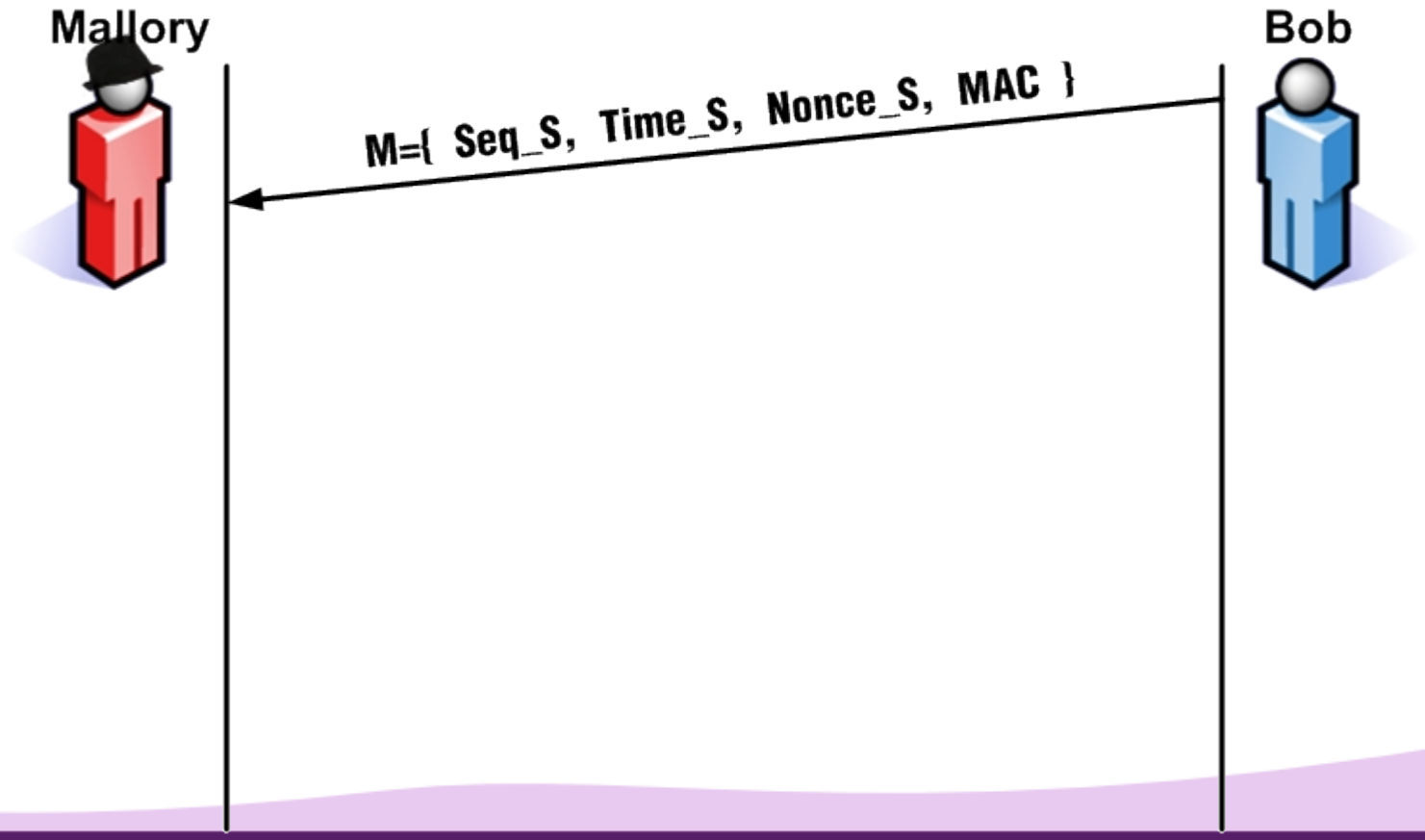


2.3 Security and Implementation Challenges

- Solution: Authentication, Integrity and Confidentiality

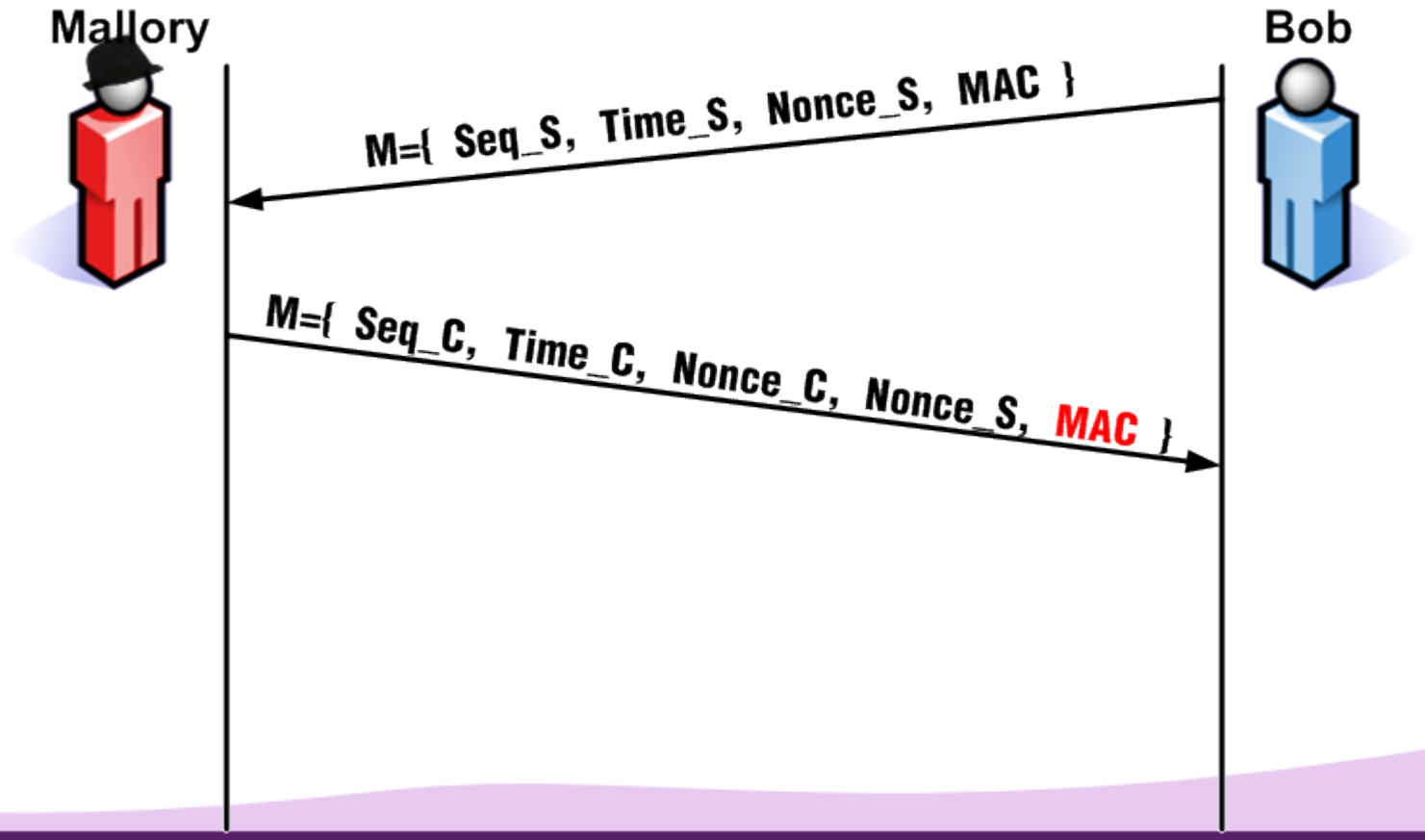
2.3 Security and Implementation Challenges

- Solution: Authentication, Integrity and Confidentiality



2.3 Security and Implementation Challenges

- Solution: Authentication, Integrity and Confidentiality

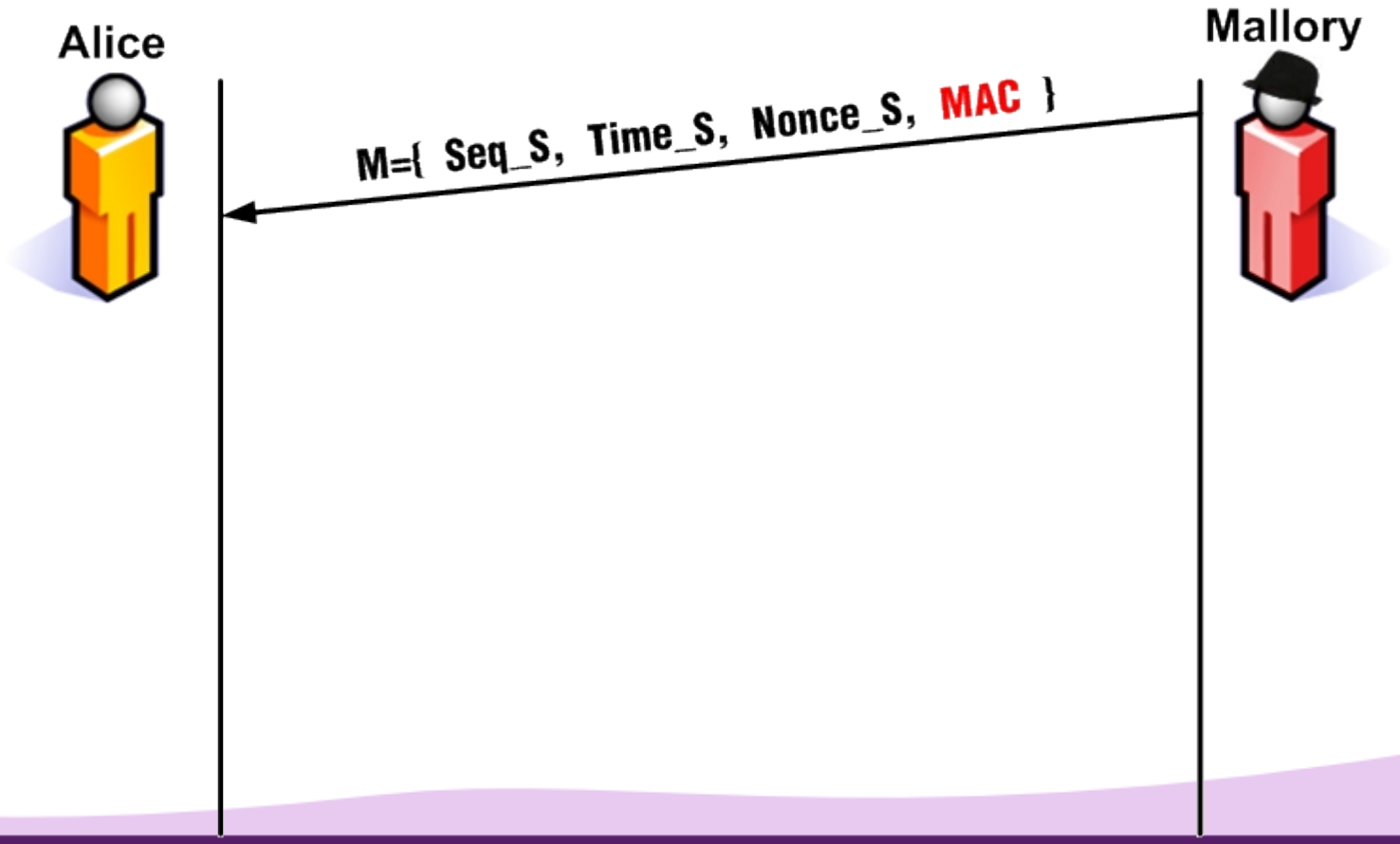


2.3 Security and Implementation Challenges

- Solution: Authentication, Integrity and Confidentiality

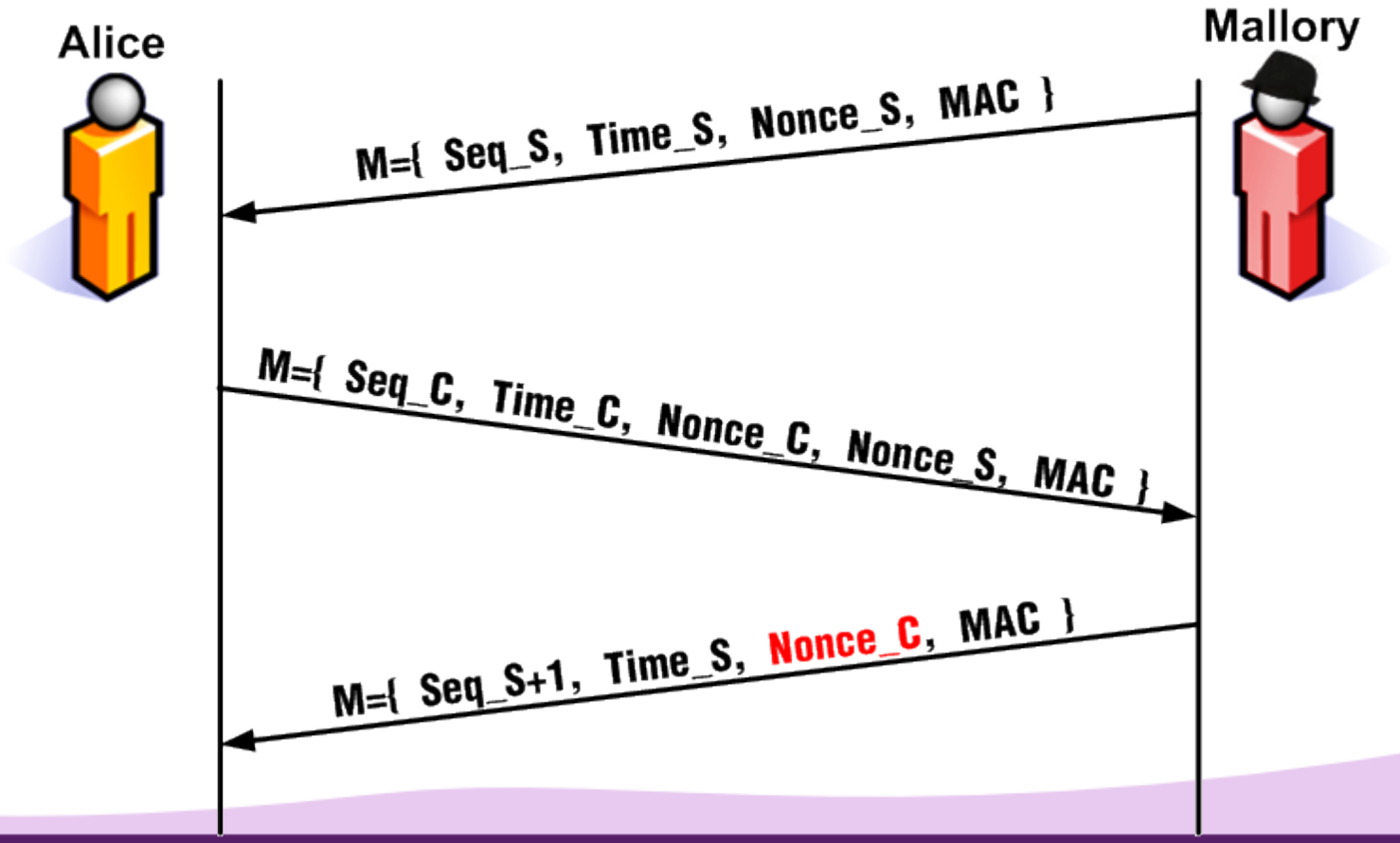
2.3 Security and Implementation Challenges

- Solution: Authentication, Integrity and Confidentiality



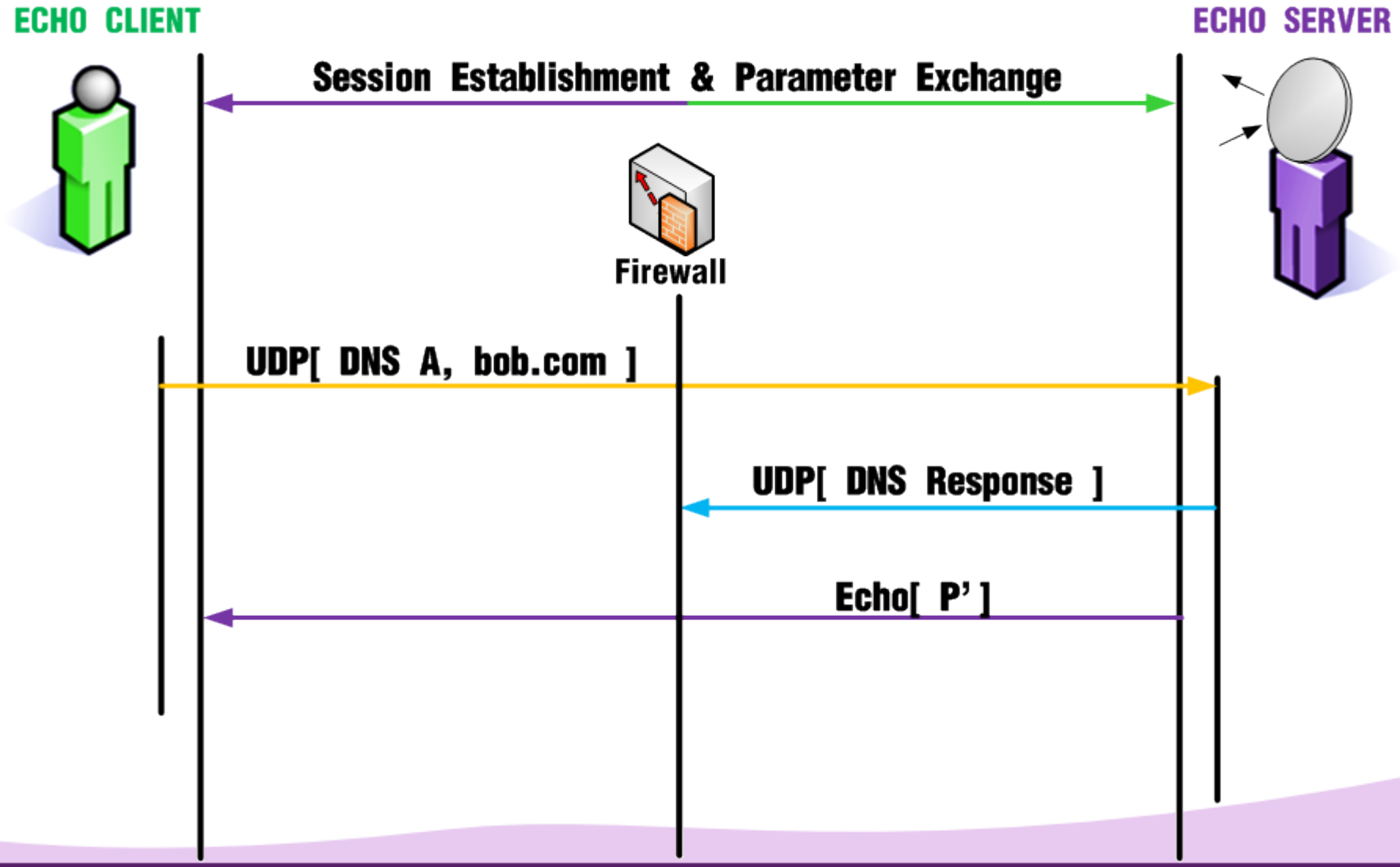
2.3 Security and Implementation Challenges

- Solution: Authentication, Integrity and Confidentiality

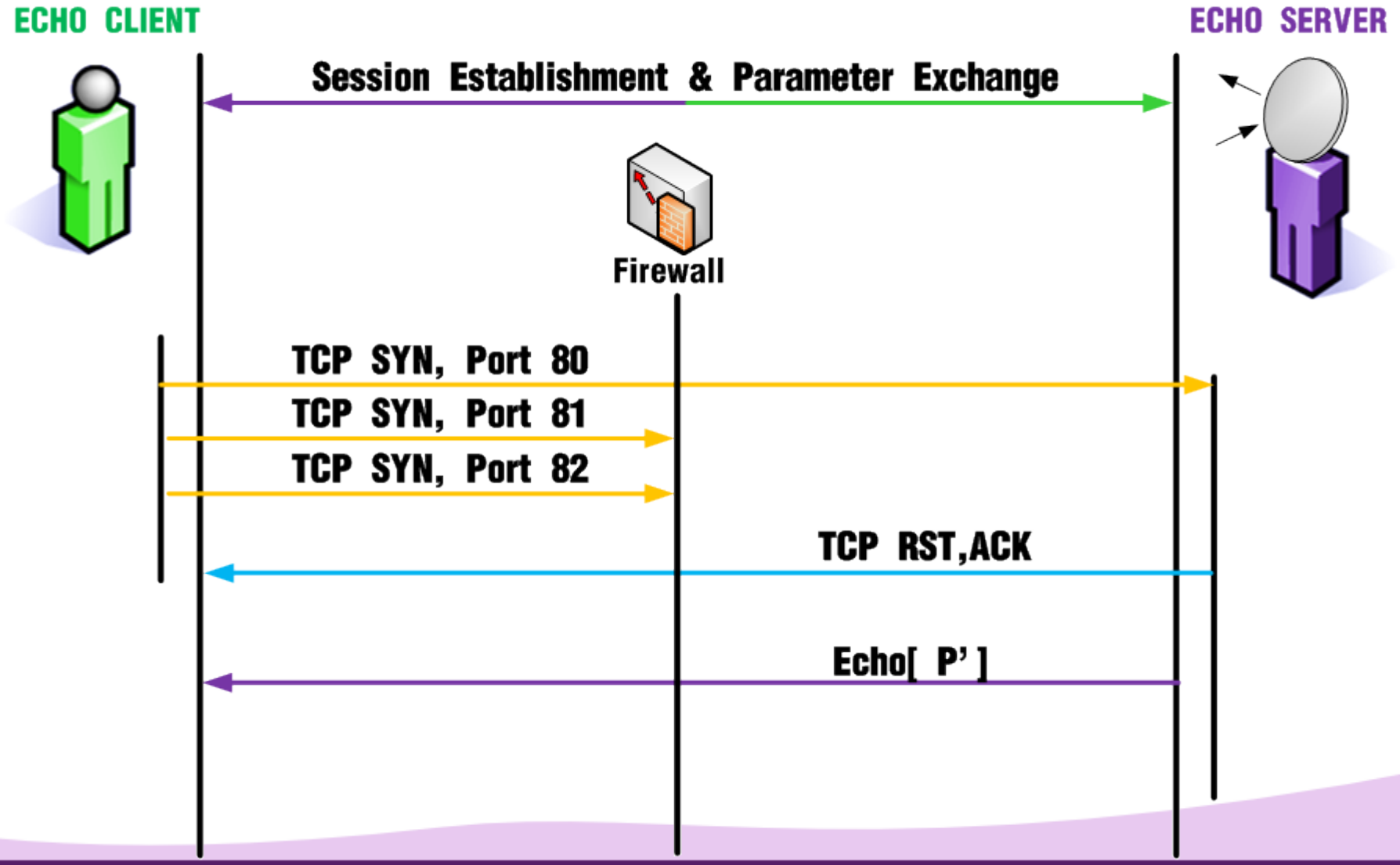


3. Experimental Results and Usage Scenarios

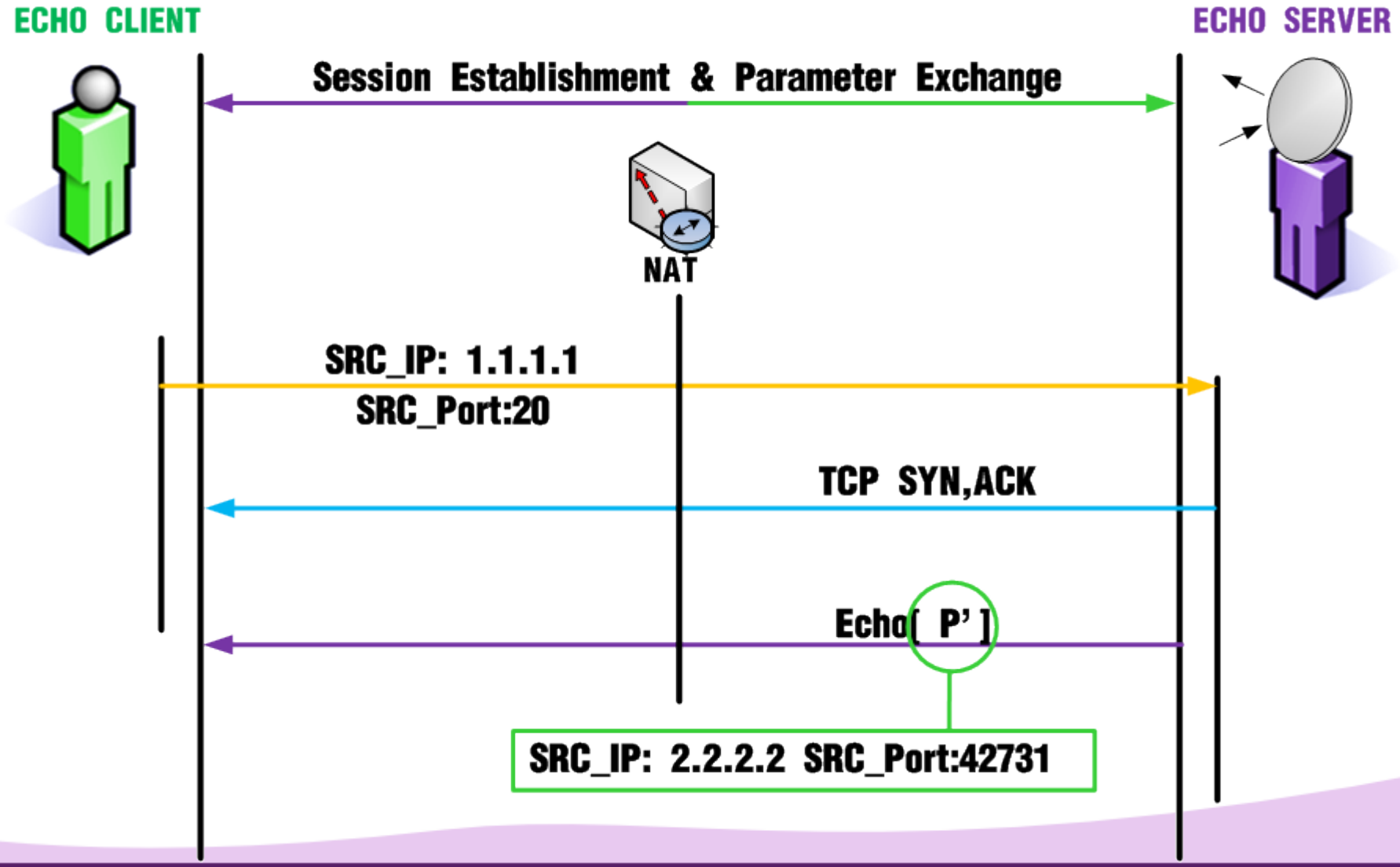
3. Experimental Results and Usage Scenarios



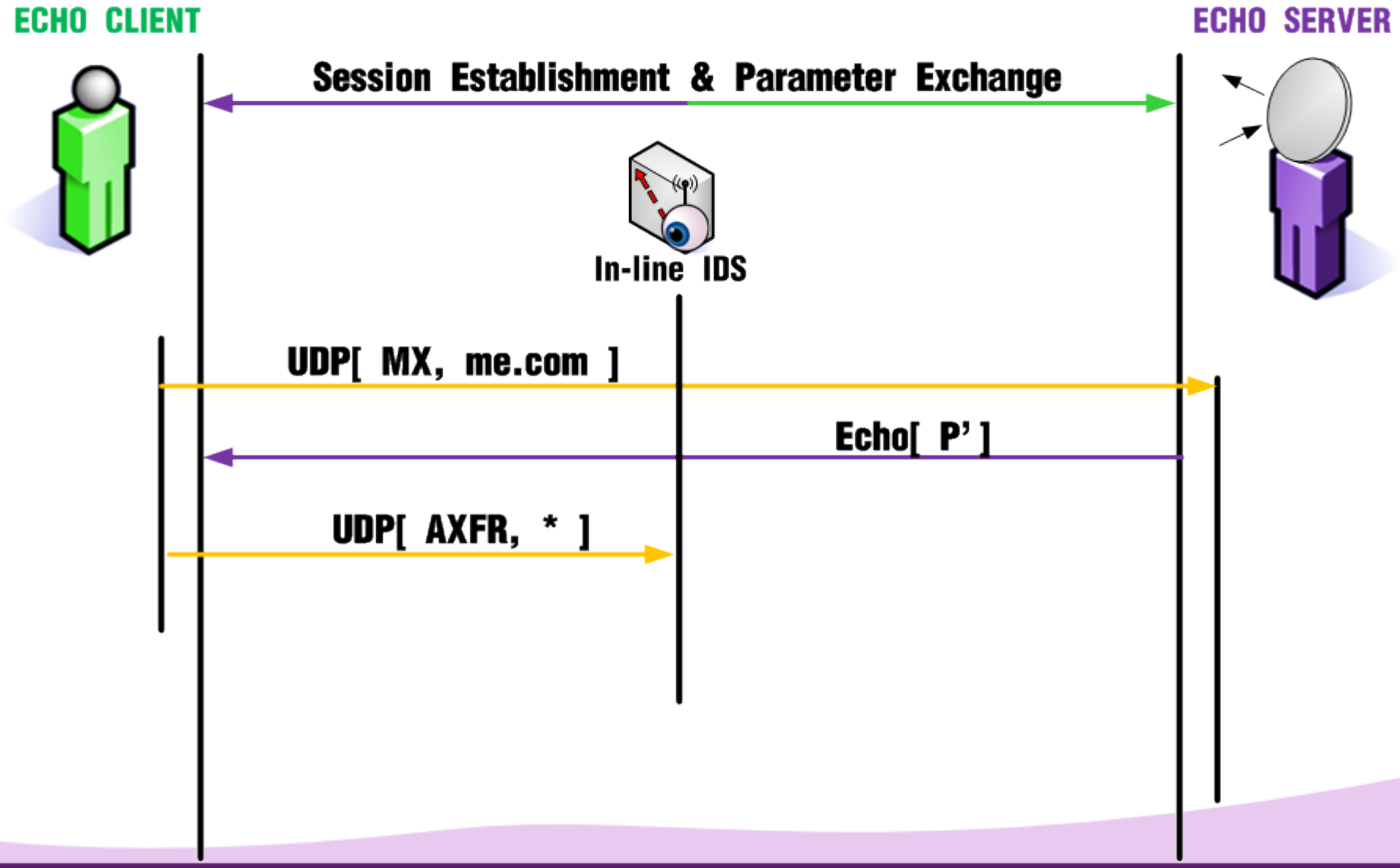
3. Experimental Results and Usage Scenarios



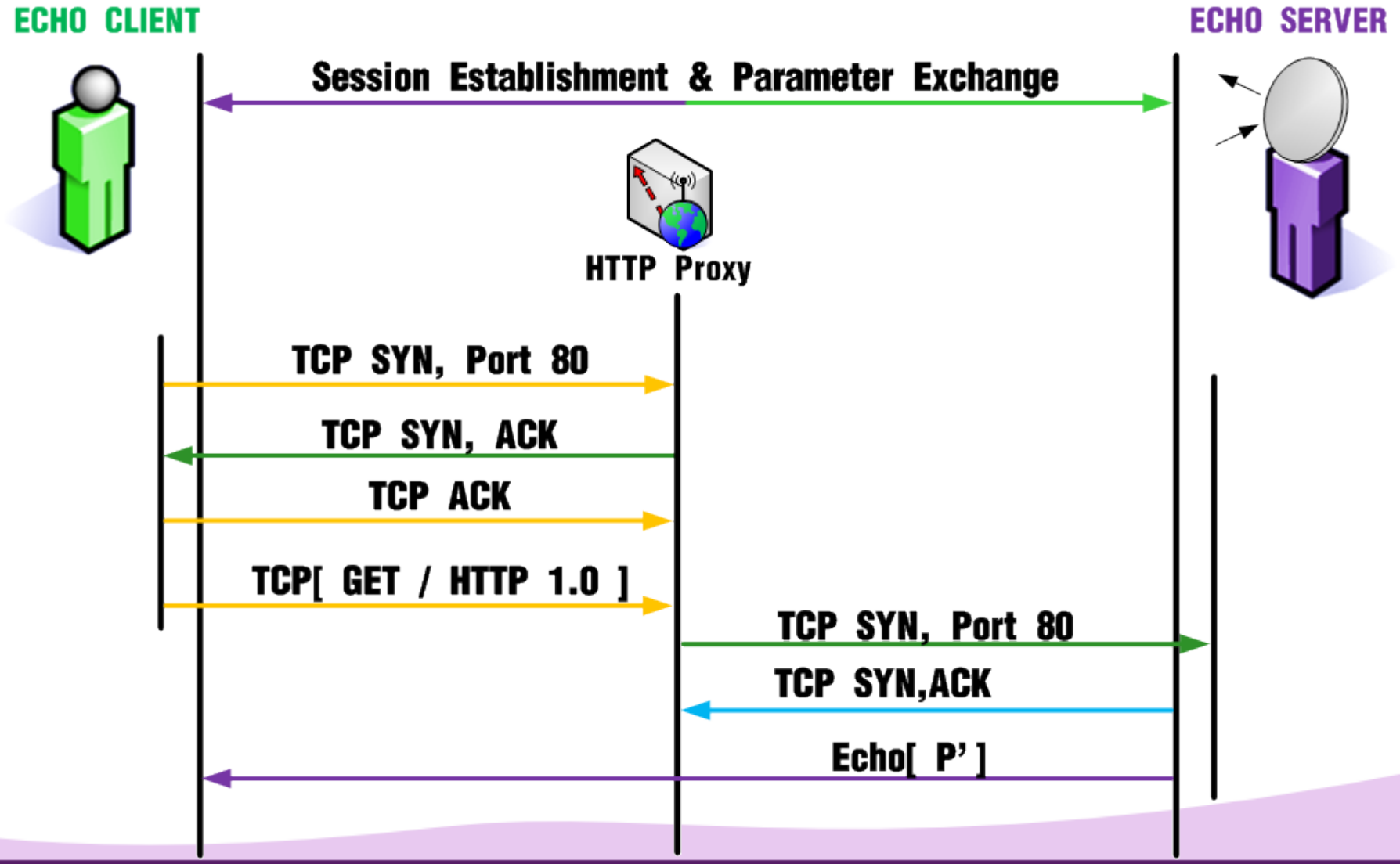
3. Experimental Results and Usage Scenarios



3. Experimental Results and Usage Scenarios



3. Experimental Results and Usage Scenarios



4. Conclusions and Future Work

4. Conclusions and Future Work

- Developed for the Nmap Security Scanner.

4. Conclusions and Future Work

- Developed for the Nmap Security Scanner.
- Sponsored by Google (GSoC Program).

4. Conclusions and Future Work

- Developed for the Nmap Security Scanner.
- Sponsored by Google (GSoC Program).
- Freely available at *http://nmap.org/nping*

4. Conclusions and Future Work

- Developed for the Nmap Security Scanner.
- Sponsored by Google (GSoC Program).
- Freely available at *http://nmap.org/nping*
- Still to be done:

4. Conclusions and Future Work

- Developed for the Nmap Security Scanner.
- Sponsored by Google (GSoC Program).
- Freely available at *http://nmap.org/nping*
- Still to be done:
  - Improve application layer support.

4. Conclusions and Future Work

- Developed for the Nmap Security Scanner.
- Sponsored by Google (GSoC Program).
- Freely available at *http://nmap.org/nping*
- Still to be done:
  - Improve application layer support.
  - Build middlebox fingerprint database.

4. Conclusions and Future Work

- Developed for the Nmap Security Scanner.
- Sponsored by Google (GSoC Program).
- Freely available at *http://nmap.org/nping*
- Still to be done:
  - Improve application layer support.
  - Build middlebox fingerprint database.
  - Implement bi-directionality.

Questions?

Thank you for your attention.