Class Capture The Flag Contest

Silvio Biagioni [1]

[1]Department of Information Engineering and Computer Science, University of Trento

May 25, 2017

Outline

Who am I

- PhD Student

Who am I

- PhD Student
- Security Risk Assessment for Attack Surfaceces

Who am I

- PhD Student
- Security Risk Assessment for Attack Surfaceces

For you Opportunity to apply your skills

Who am I

- PhD Student
- Security Risk Assessment for Attack Surfaceces

For you Opportunity to apply your skills

For me Improve my research ☺

Who am I

- PhD Student
- Security Risk Assessment for Attack Surfaceces

For you Opportunity to apply your skills

For me Improve my research ☺

Who am I

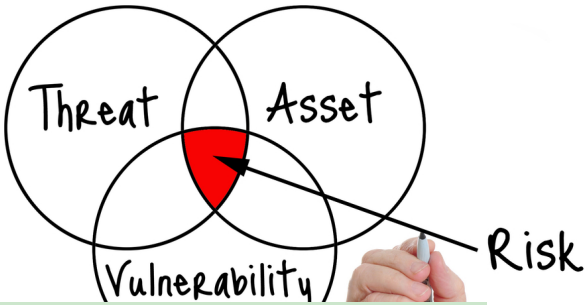
- PhD Student
- Security Risk Assessment for Attack Surfaceces

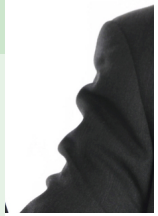
For you Opportunity to apply your skills

For me Improve my research ☺

Who am I

- PhD Student
- Securi... for At...





All Needed Information

Link Link to the student's wiki (TBD)

For you Opportunity to apply your skills

For me Improve my research ☺

cyber DEfense Technology Experimental Research (DETERLab)

- 

  Information Science Institute (ISI)

cyber DEfense Technology Experimental Research (DETERLab)

- 

  Information Science Institute (ISI)
- DETERLab

cyber DEfense Technology Experimental Research (DETERLab)

- USC University of Southern California
  Information Science Institute (ISI)
- DETERLab

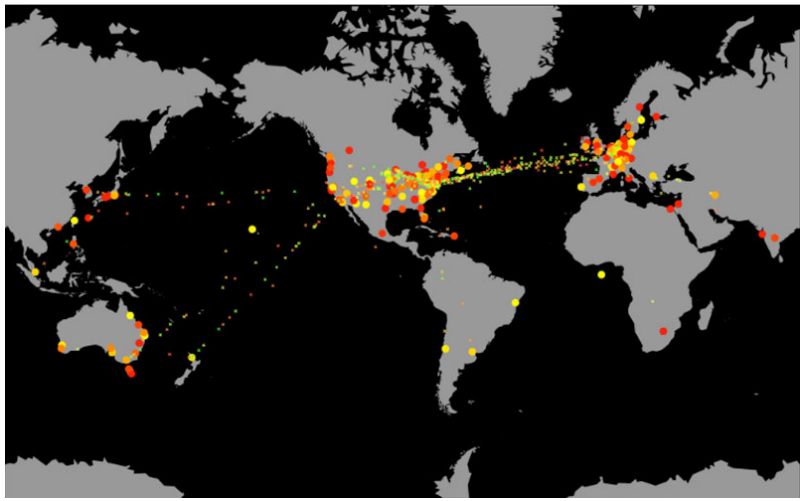
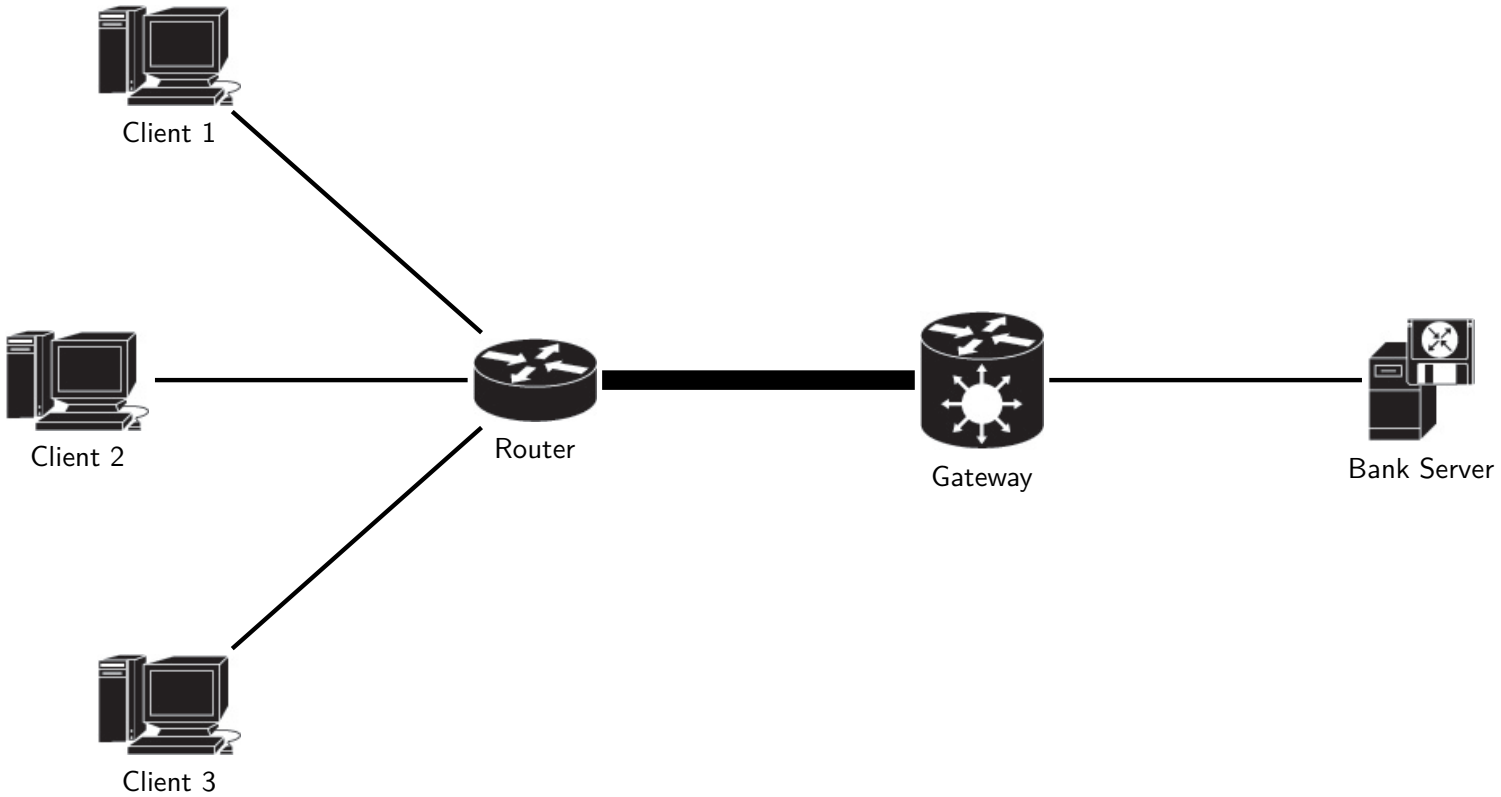
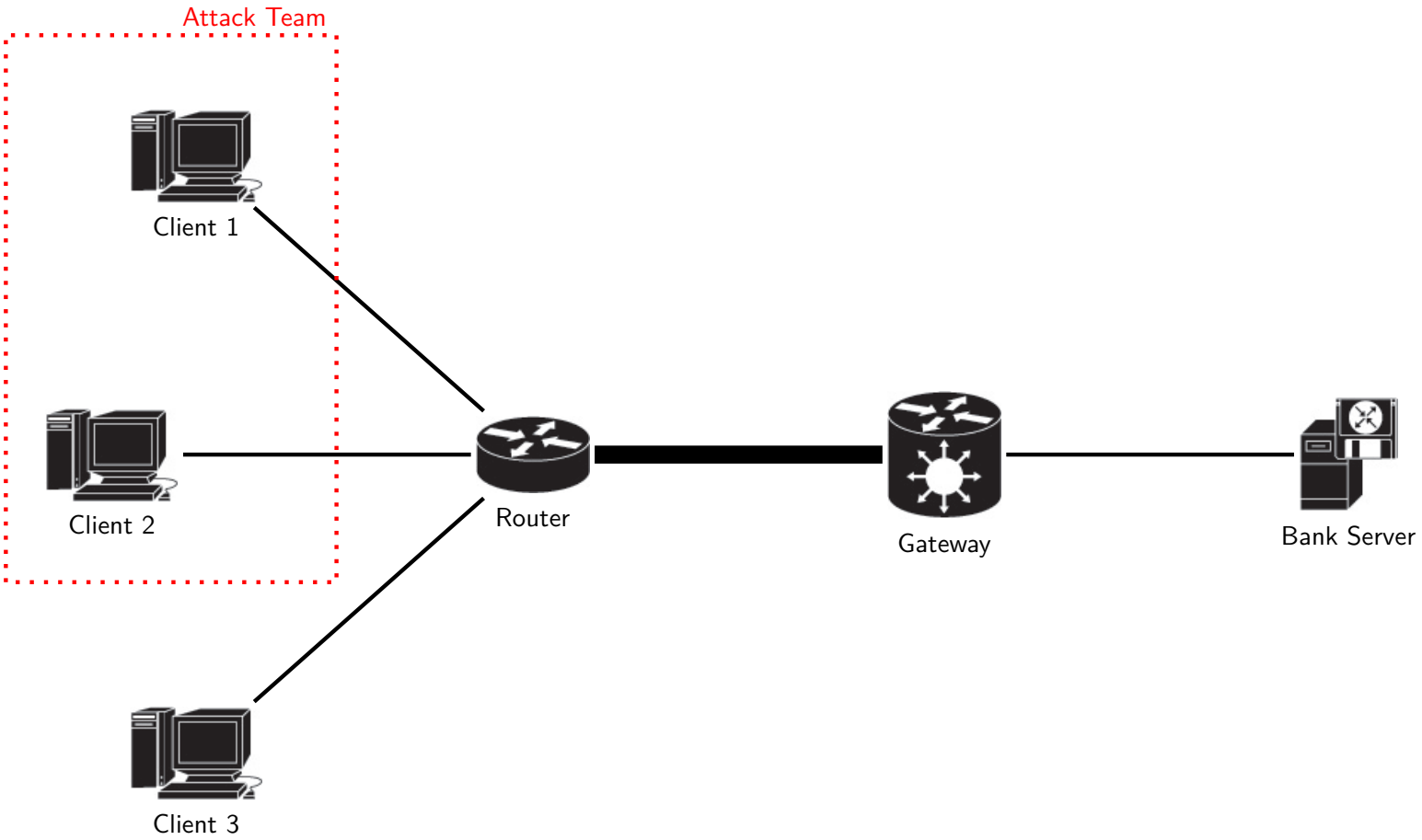


Figure: Global worm DDoS topology on single target

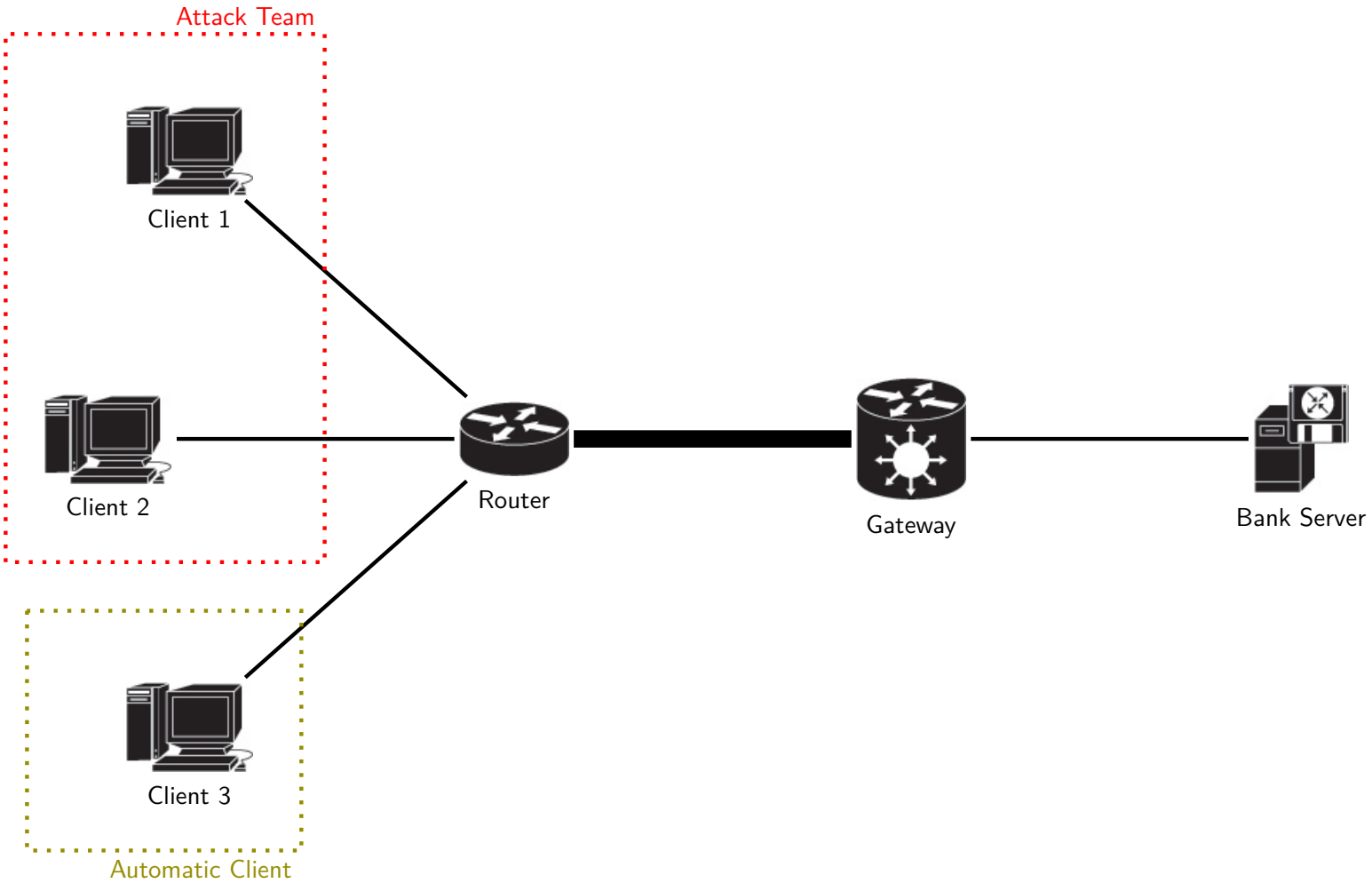
Network Topology



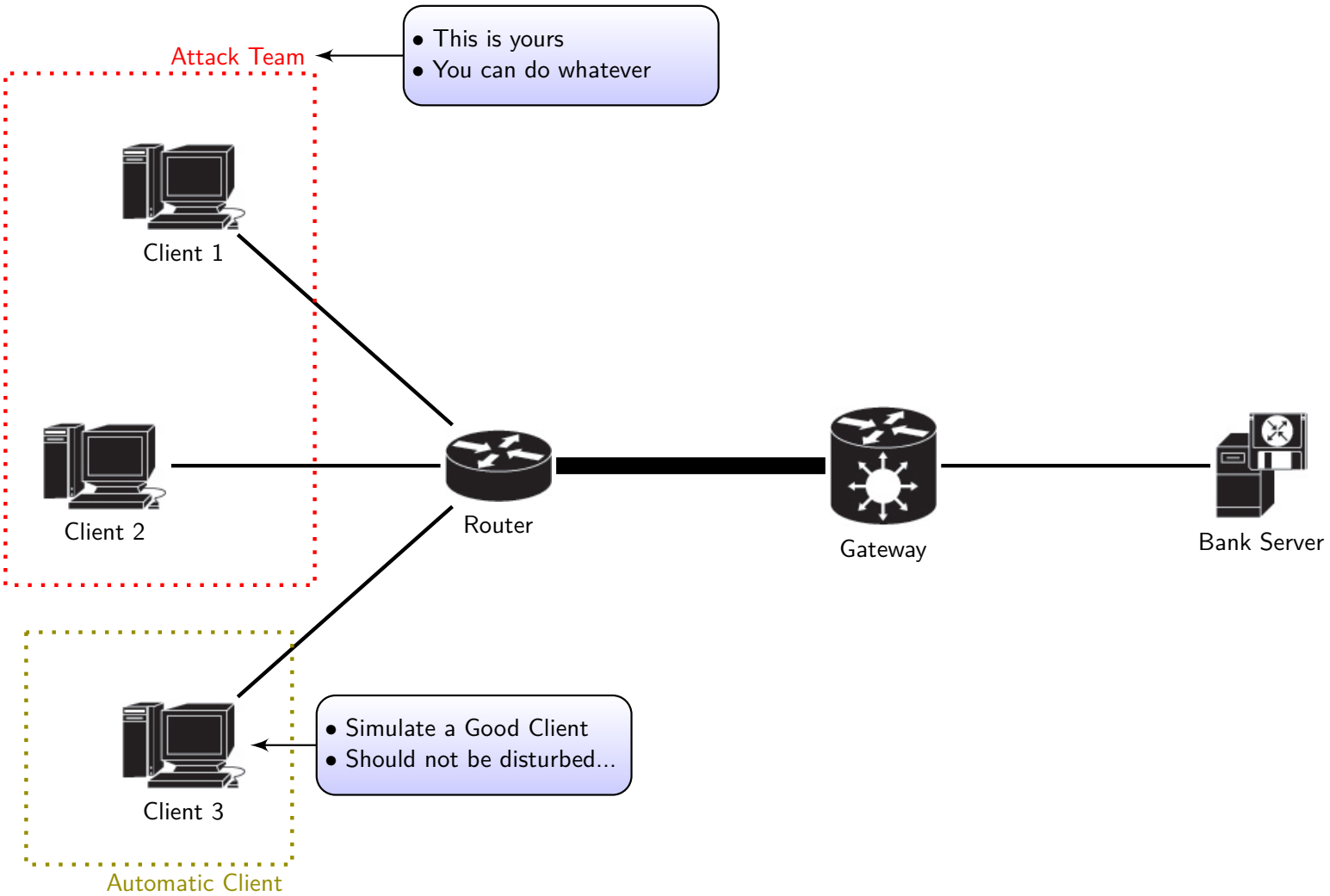
Network Topology



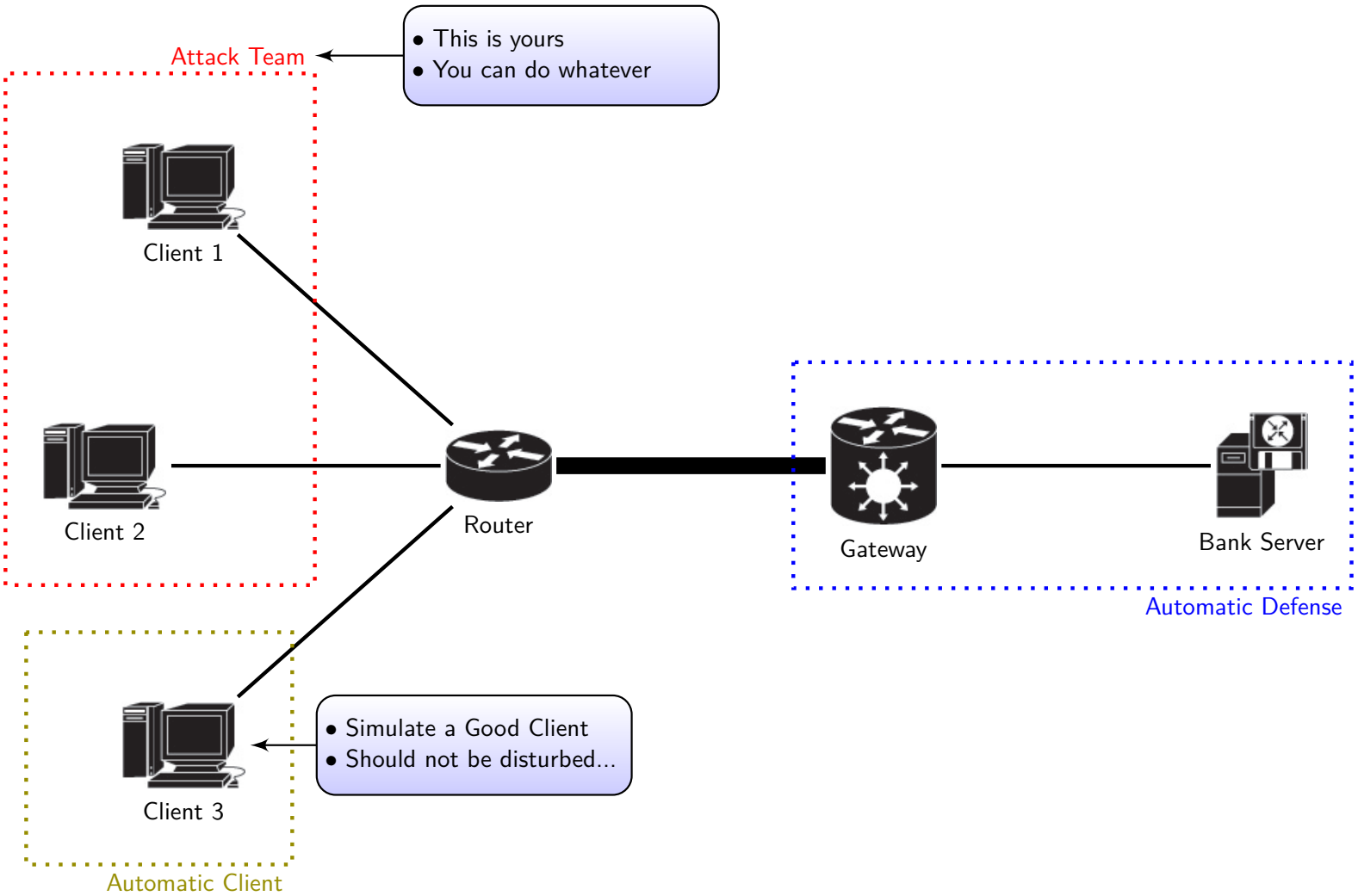
Network Topology



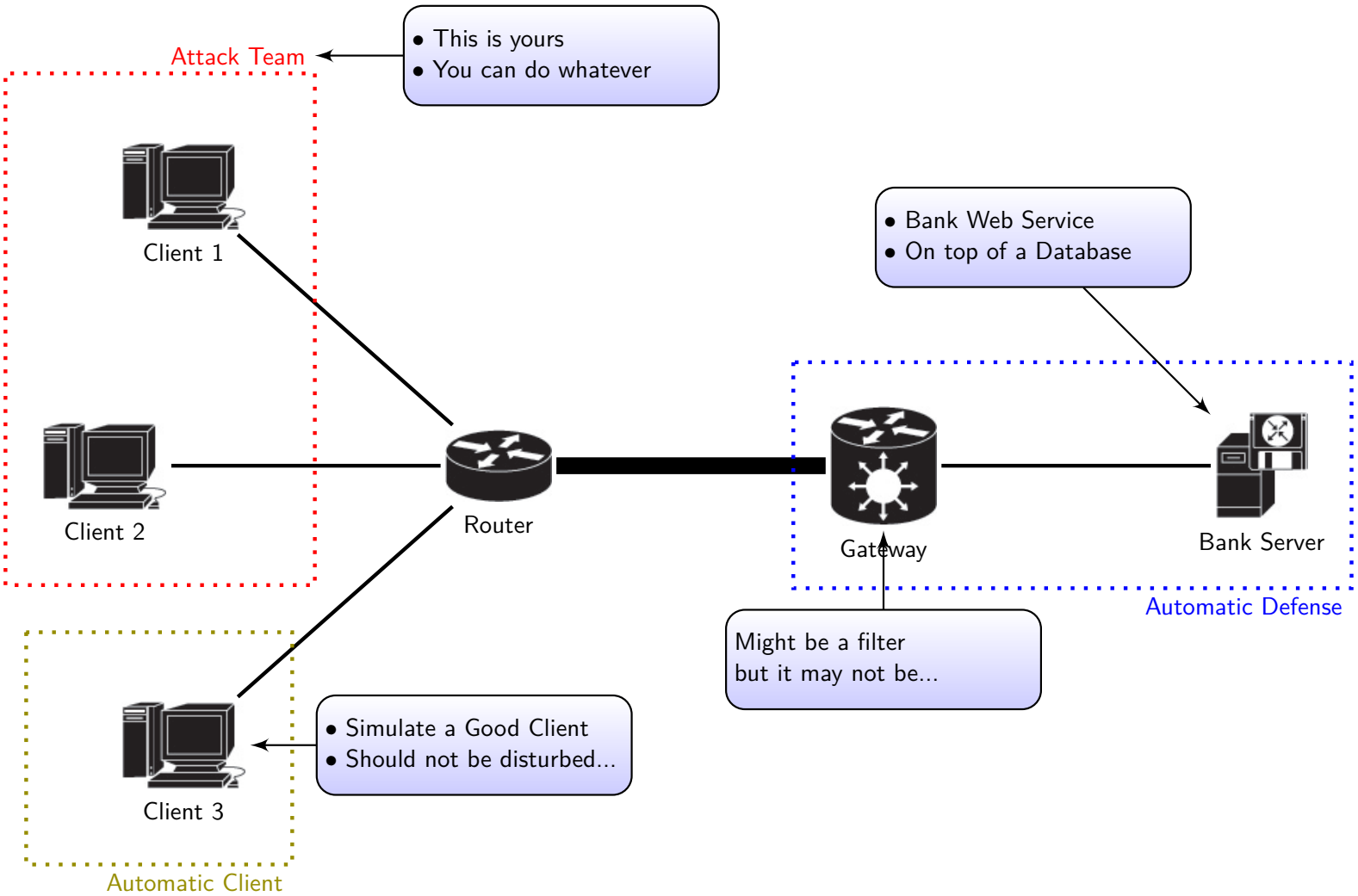
Network Topology



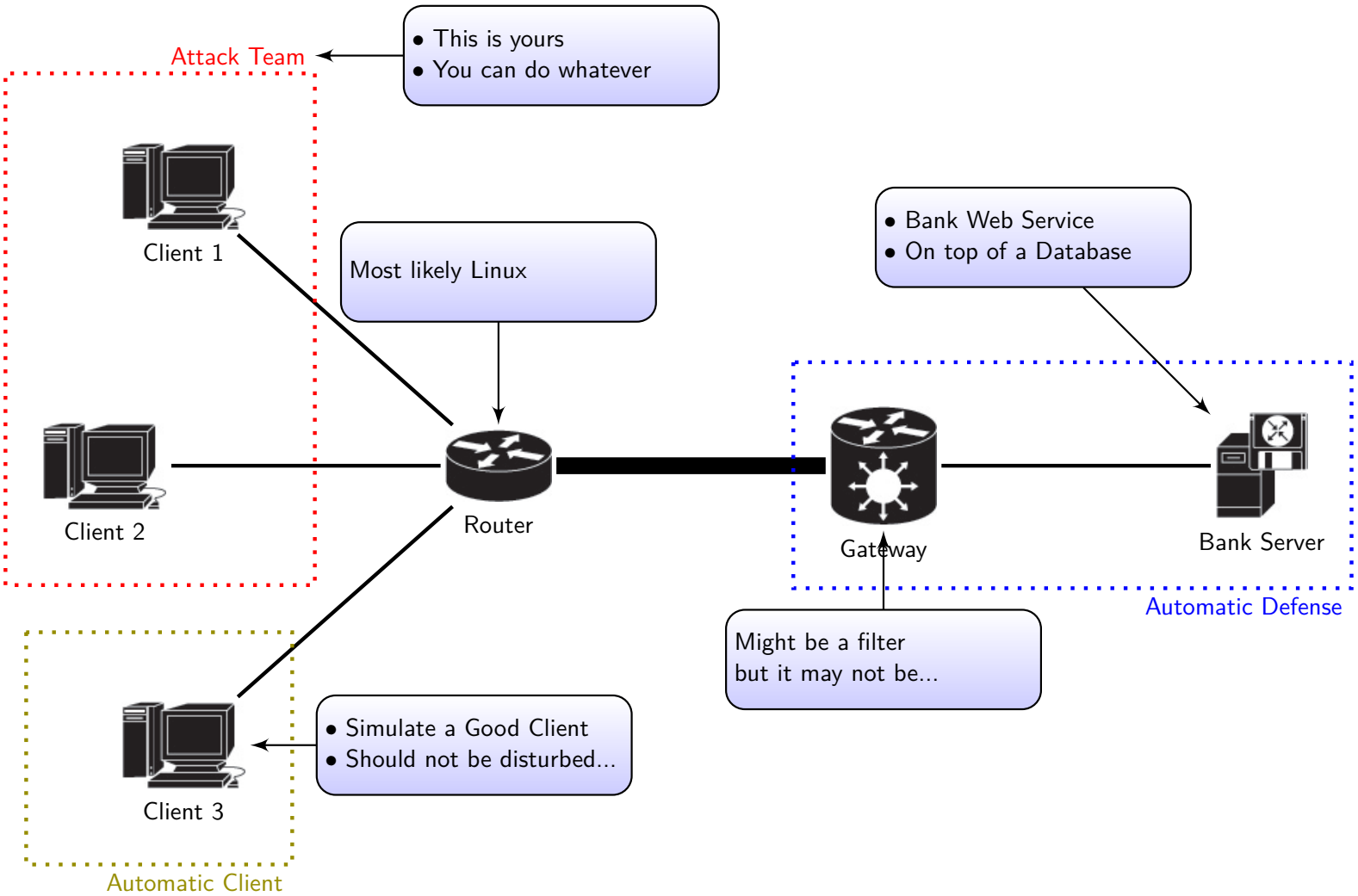
Network Topology



Network Topology



Network Topology



Rounds

Rounds

1. Questionnaire on Web Application Security

Rounds

1. Questionnaire on Web Application Security
   - SQL injection

Rounds

1. Questionnaire on Web Application Security
   - SQL injection
   - XSS

Rounds

1. Questionnaire on Web Application Security
   - SQL injection
   - XSS
   - HTTP misconfigurations

Rounds

1. Questionnaire on Web Application Security
   - SQL injection
   - XSS
   - HTTP misconfigurations
2. 1 Day to compromise a Level 0 config (super-vulnerable)

Rounds

1. Questionnaire on Web Application Security
   - SQL injection
   - XSS
   - HTTP misconfigurations
2. 1 Day to compromise a Level 0 config (super-vulnerable)
3. 5 Days to compromise a Level 1 config (hardening OS, Server)

Rounds

1. Questionnaire on Web Application Security
   - SQL injection
   - XSS
   - HTTP misconfigurations
2. 1 Day to compromise a Level 0 config (super-vulnerable)
3. 5 Days to compromise a Level 1 config (hardening OS, Server)
4. 5 Days to compromise a Level 2 config

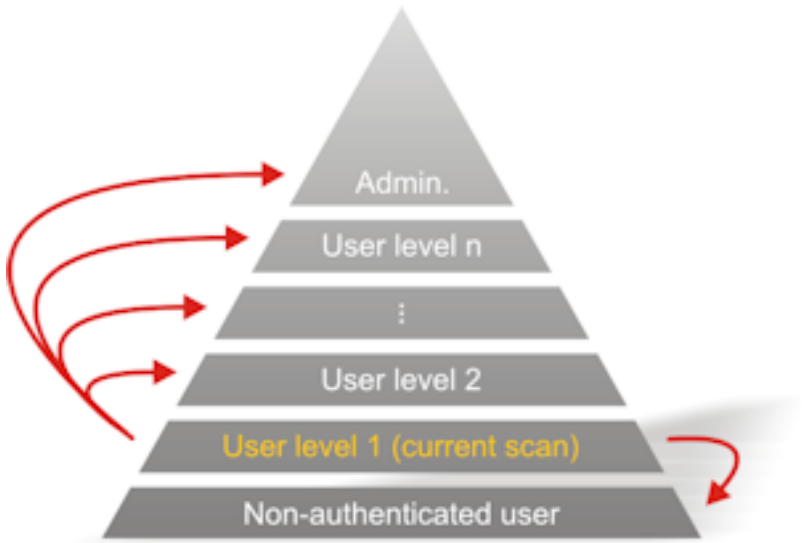
Goal

Goal

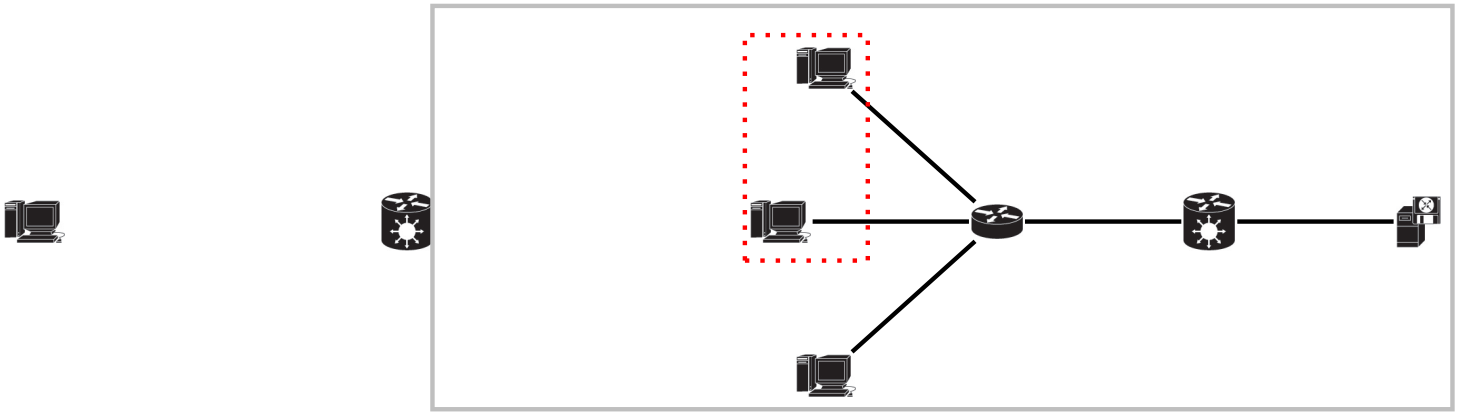
- Confidentiality Exfiltrate all Data on Bank Accounts
  Integrity Modify Bank Accounts
  Availability Provoke a DoS

Goal

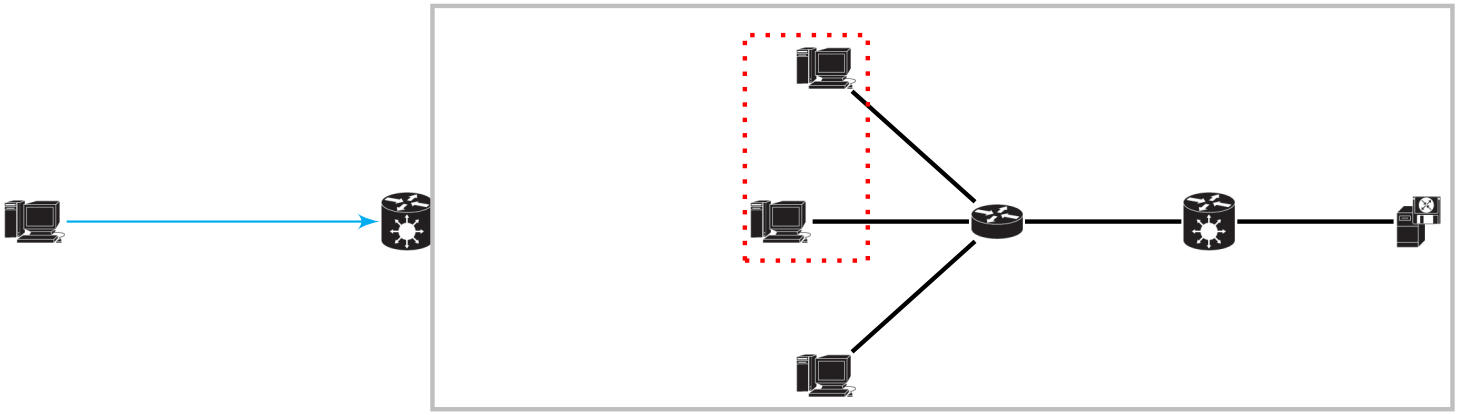
- Confidentiality Exfiltrate all Data on Bank Accounts
  Integrity Modify Bank Accounts
  Availability Provoke a DoS
- Privilege Escalation



Operational Details

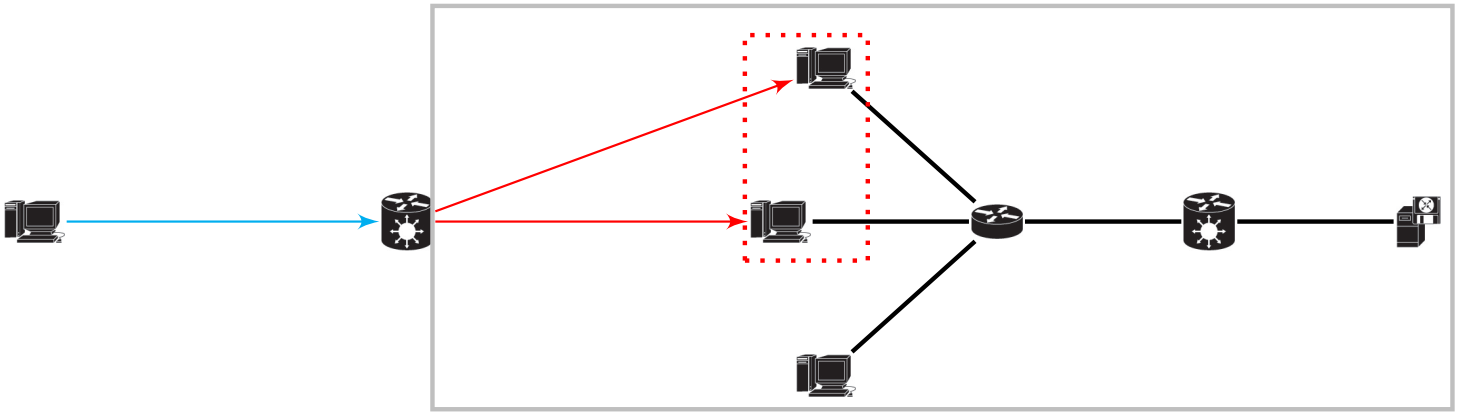


Operational Details



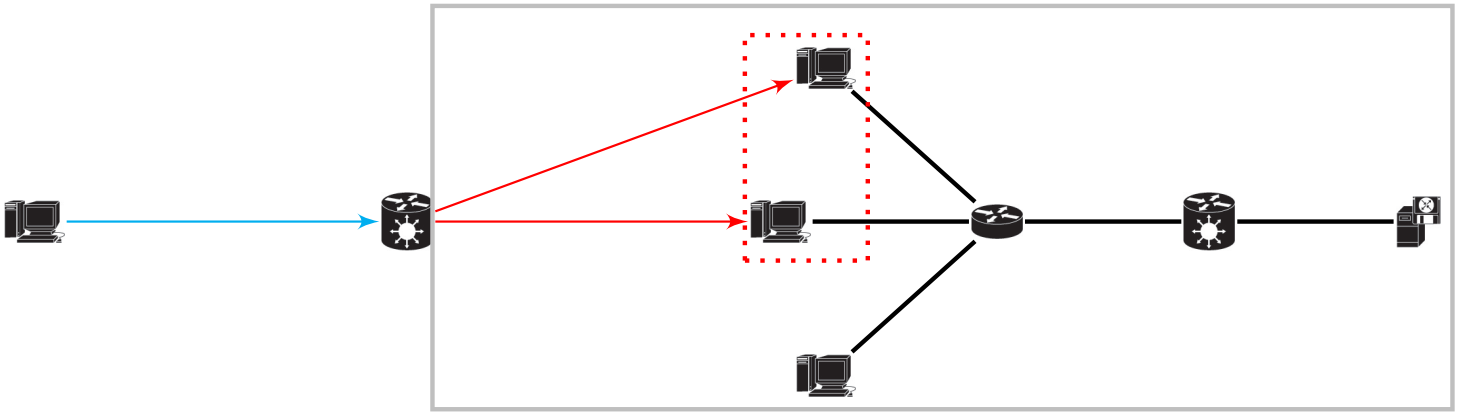
- ssh unitn9ab@users.deterlab.net

Operational Details



- ssh unitn9ab@users.deterlab.net
- ssh client1.exp1.ExperCCTF1.isi.deterlab.net

Operational Details



- ssh unitn9ab@users.deterlab.net
- ssh client1.exp1.ExperCCTF1.isi.deterlab.net
  - same for the other nodes (for you, not yet...)

Bank Server Access

- to GUI or not GUI... waiting Jelena

Forming Groups

- my contact
- how many people per group

Thanks for your Attention!