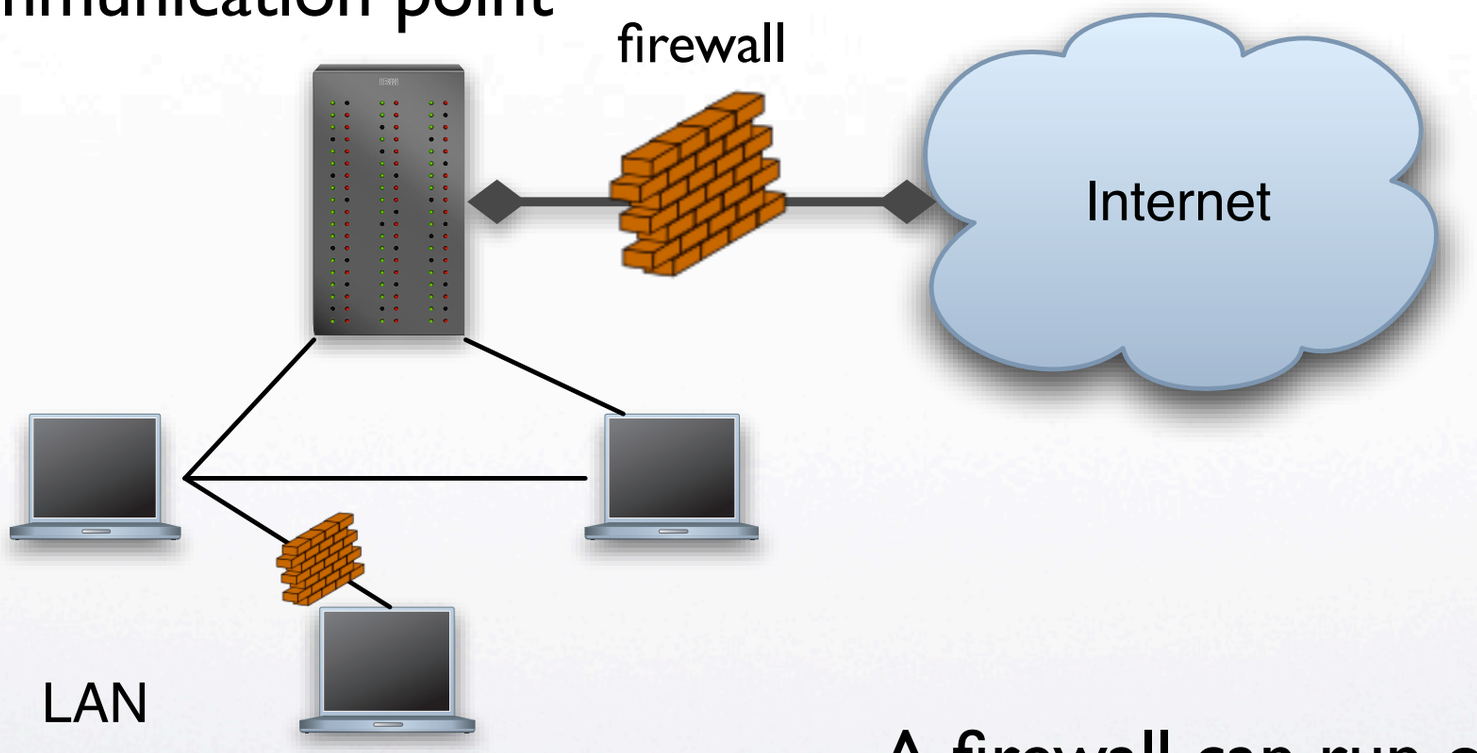
Firewalls

Aggelos Kiayias
University of Connecticut

Firewall

Idea:
Monitor inbound/ outbound
traffic at a communication point



A firewall can run on any host of a network

Firewall Basics

- Transmission control mechanism
  - It blocks traffic that matches a certain pattern.
  - It permits traffic that matches a certain pattern.
- Provides forensic data regarding malicious activities.

Network Layer

- A network layer firewall makes decisions regarding the forwarding of TCP/IP packets. The decisions are based on:
  - Source & Destination IP addresses and ports.
  - Protocol type.
  - Packet type.

    also known as packet filtering

Packet Filtering

- *Stateless*: it is based only on information available from the currently inspected packet. E.g., Drop all packets directed to a local host port 25 (SMTP).

- Shortcomings: without using state it is impossible to judge legitimacy of packets in many cases.

  - Example: FTP clients listens to a random port > 1024. Given any incoming packet to a such port a stateless firewall must accept it.

Stateful Packet Filtering

- Firewall maintains a state of all connections.
- Filtering decisions are based on the state of connections.
- Work load is different depending on packet:
  - Connection initialization packets are more carefully scrutinized.
  - Established connection packets are let through.

Circuit Level Gateway

Client

Pass : update connection state table

SYN

Pass : based on table/ update table

SYN+ACK

Pass : based on table/ update table

ACK

Pass : based on table

Application layer data

Server

Rationale:

The only thing that will be allowed in is data requested.

Server thinks it talks to the firewall.

Circuit Level Gateways

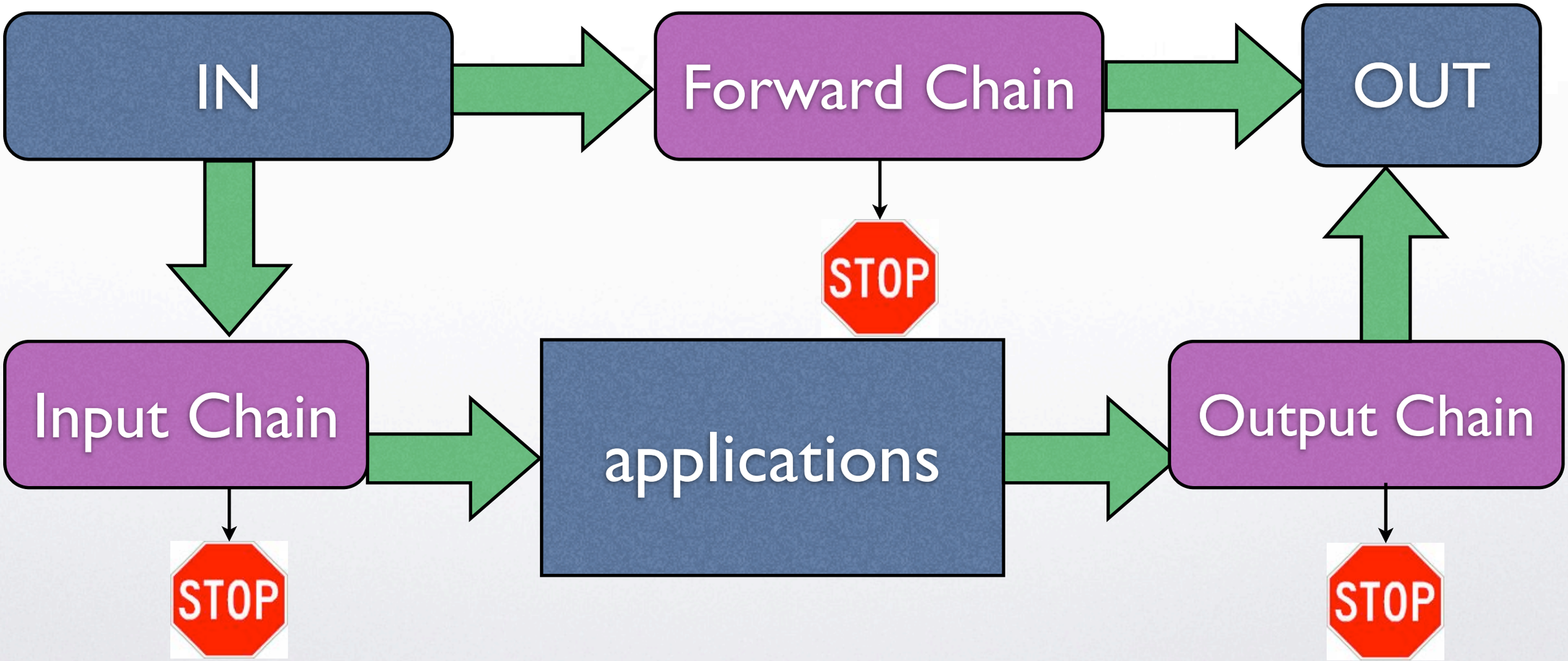
- Advantages:
  - only requested data are allowed (all ports are closed by default).
  - They also facilitate Network Address Translation for Internet sharing.
- Disadvantages:
  - once a connection is initiated all data pass.
  - additional methods are required to handle servers within the firewall's LAN. (i.e., incoming traffic)

Combination

- Packet filtering and Circuit level gateway.
- Allows to open ports for servers within the firewalled LAN and at the same time block unsolicited incoming traffic at other ports.
- Shortcomings:
  - You cannot prevent the existence of a rogue server on a port/host (that may be legitimately open for another purpose).
  - Any open port is a danger if the server sitting on the other side is misconfigured/unpatched.

IPtables

- (Linux 2.4) high level diagram

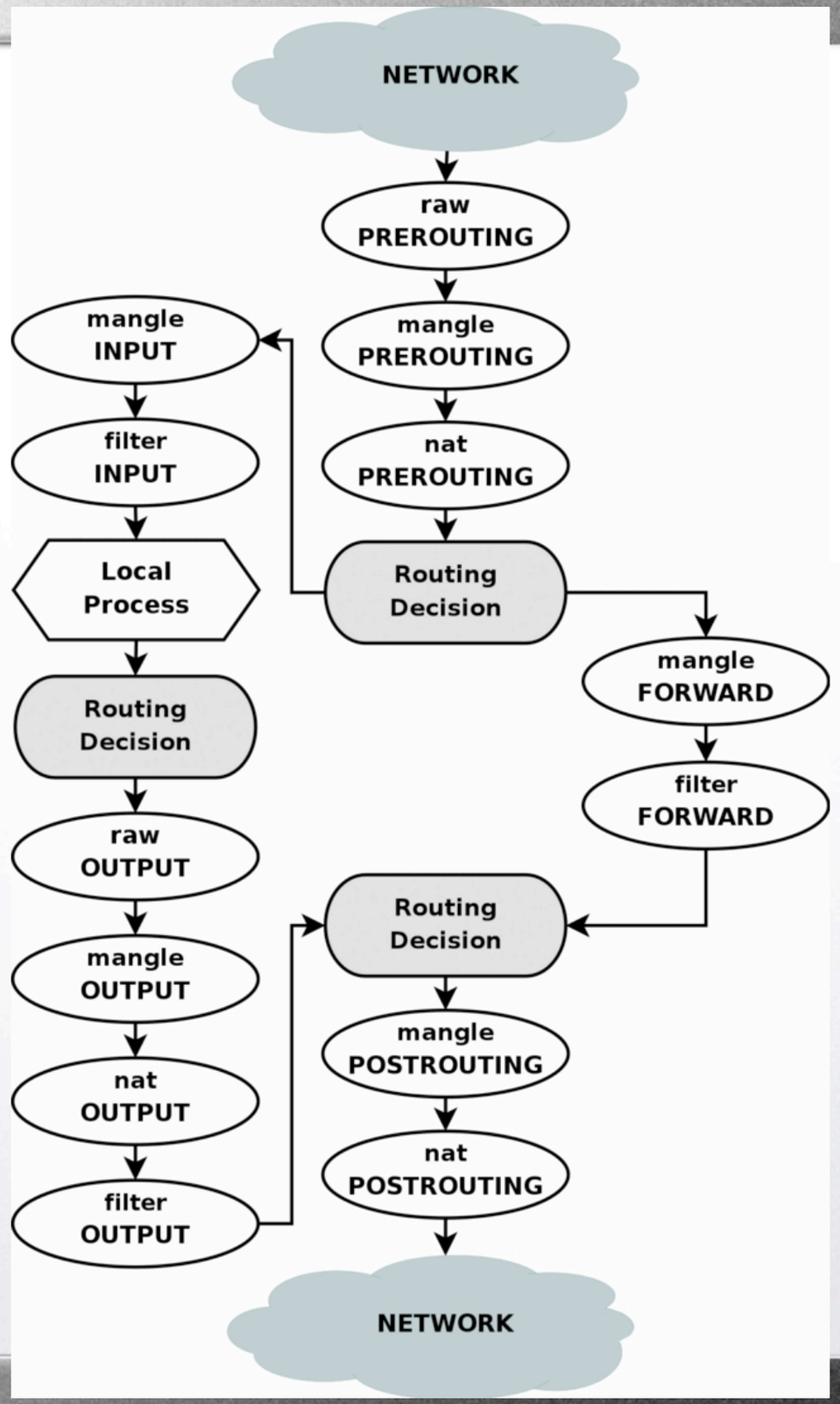


In more detail

Mangling packets:
small intentional
header modifications that
assist in routing and other
network service decisions
(example : modify the TTL)

NAT = network address translation

raw = used to turn off connection tracking



picture from:
http://iptables-tutorial.frozentux.net/iptables-tutorial.html

Examples

drop all incoming TCP packets to destination port 23

```
iptables -A INPUT -p tcp --dport 23 -j DROP
```

drop all incoming packets from eth0 directed to addresses that start with 10

```
iptables -A INPUT -d 10.0.0.0/8 -i eth0 -j DROP
```

drop all incoming packets that have no existing state and they are not suitable for opening a new state.

```
iptables -A INPUT -m state --state NEW, INVALID -j DROP
```


IPtables options

- -t specify the type of tables
  -A Append to a specific chain
  -p specify the protocol
  -i specify the incoming interface
  -d specify the matched destination IP address in packet
  -j specify the "target" or operation to be performed.
  --to-destination substitute the destination IP address.

Throttling

- Applies to stateful firewalls.
- The amount of packets of a specific kind that the firewall will allow is bounded.
  - Useful for protocols such as ICMP that you want to allow them but may be used for malicious purposes.

example:

(ping packet)

```
iptables -A INPUT -p icmp -d 156.123.4.10 --icmp-type 8 -m
limit --limit 10/s -j ACCEPT
```



Calibrating Throttling

- In this setting the firewall changes the throttling behavior depending on the traffic.

Example: allow 10 SYN packets and after the first 10 limit to six per minute

```
iptables -A INPUT -m limit --limit 6/m --limit-burst 10
 --syn -j ACCEPT
```


Forensics

- Firewalls can keep various logs of packets that can be used afterwards to analyze the type of traffic that passes through a router.

```
iptables -A INPUT -s 154.34.0.0/16 -p udp -j LOG
--log-prefix “check this:”
```

Note: packet will continue to transcend the chain of rules after the LOG

Application Level Gateways

- Similar to circuit level gateways but it is application specific.
  - A gateway will have an algorithm for each service that is allowed to be used and will drop connections/packets that are unwanted.
  - Advantages: can tailor your traffic exactly how you want it. Disadvantages: hard to configure; possibility of high overhead.

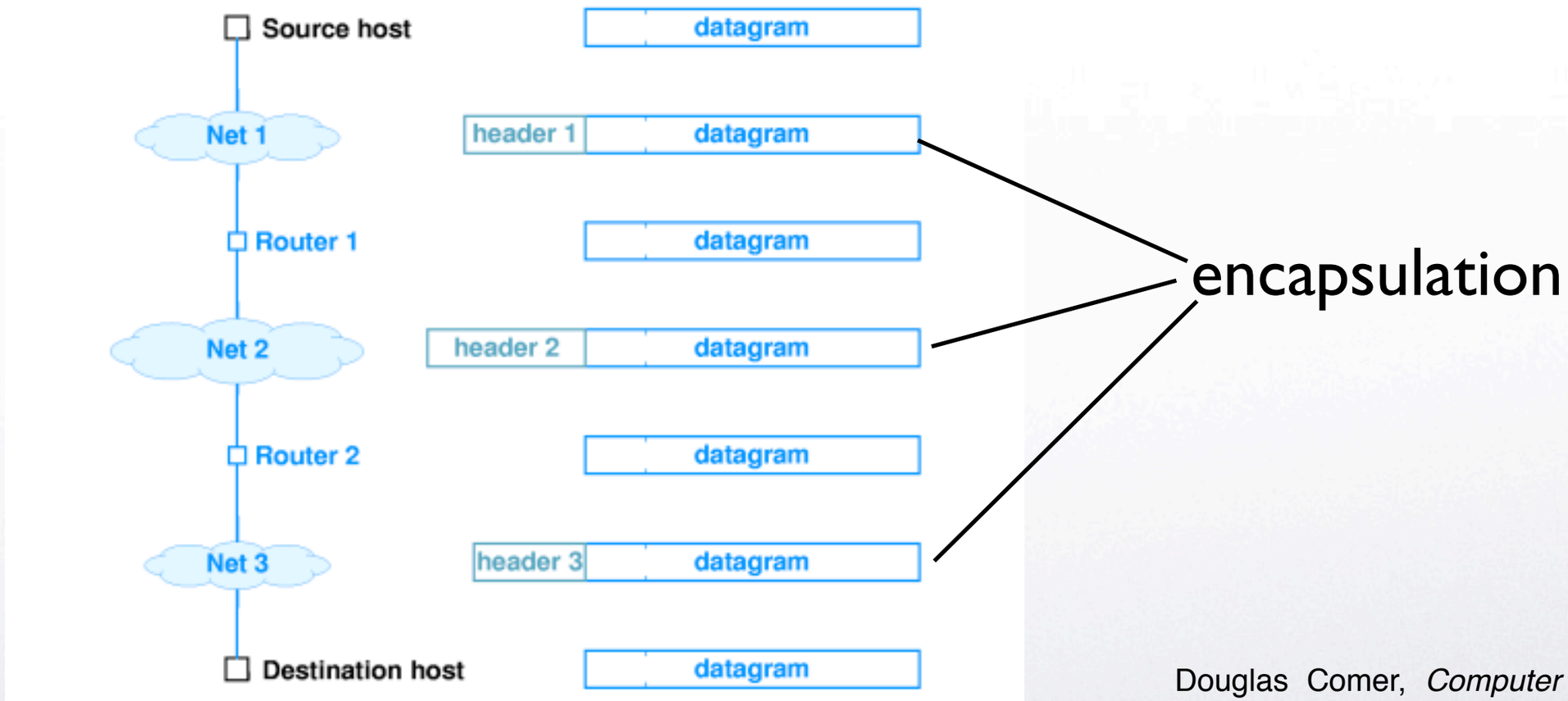
Example: *A web browser proxy service.*

Fragmentation

- Disassembling of IP datagrams so that they can be transmitted over different types of network interfaces.
- An integral component of the IP protocol.
- **MTU**: the maximum transmission unit.
- The problem: forward a datagram from a network interface with larger MTU to a network interface with smaller MTU

Traversing Networks

Traversing different networks



Douglas Comer, *Computer Networks and Internets with Internet Applications (fourth edition)*, Prentice Hall, 2004, ISBN 0-13-143351-2.

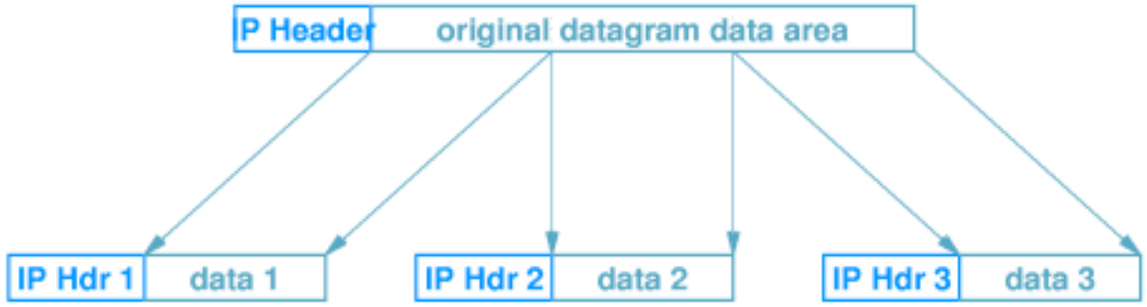
Fragmentation

heterogenous MTU

fragmentation

Characteristics:

```
MORE flag
OFFSET position
CHECKSUM
```



Fragmentation Attacks

Bypassing firewalls

- Tiny fragment attack: create fragments so tiny that they miss information used by a firewall to drop a packet [assuming the firewall examines only first packet]
- Overlapping fragment attack: using overlapping offsets overwrite TCP header information during reassembly. It may be used to change the destination port!

Firewalls Pros and Cons

- They do prevent straightforward attacks and information leakages.
- They can be surpassed though.
- Increasing their effectiveness increases their operational cost substantially (overhead/configuration).
- May give false sense of security.
- **Bottom-line**: you have to have one but do not count on it for much.

