CS 547: Foundation of Computer Security

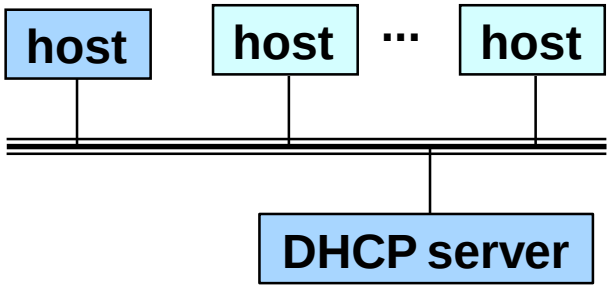
S. Tripathy
IIT Patna

Previous Class

- Security in Networks
  - Threats in Networks
    - Layer 2,

LAN Bootstrapping: DHCP

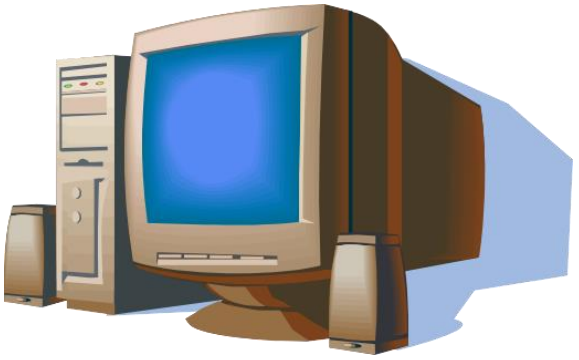
- New host doesn't have an IP address yet
  - So, host doesn't know what source address to use
- Host doesn't know *who to ask* for an IP address
  - So, host doesn't know what destination address to use
- Solution: shout to "**discover**" server who can help
  - Broadcast a server-discovery message (layer 2)
  - Server(s) sends a reply offering an address



Dynamic Host Configuration Protocol

new client

DHCP discover (broadcast)



DHCP server

DHCP offer

"**offer**" message includes IP address, DNS server, "gateway router", and how long client can have these ("lease" time)

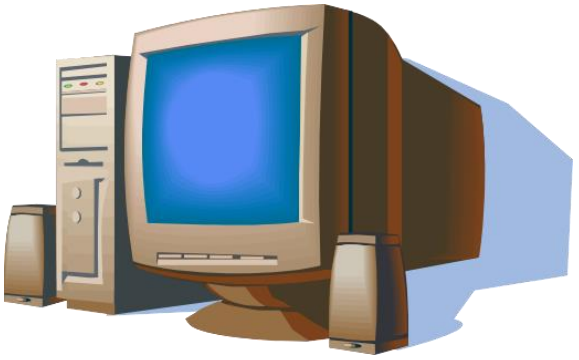
DHCP request (broadcast)

DHCP ACK

Dynamic Host Configuration Protocol

new client

DHCP discover (broadcast)



DHCP server

DHCP offer

"**offer**" message includes IP address, DNS server, "gateway router", and how long client can have these ("lease" time)

DHCP request (broadcast)

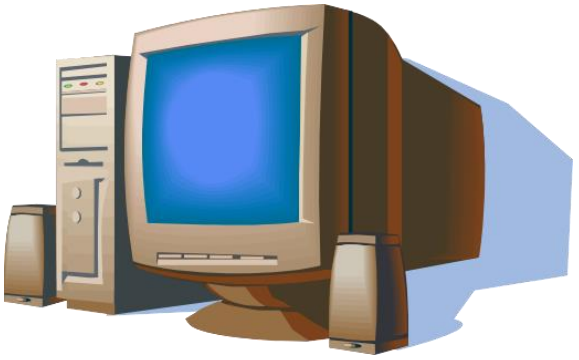
Threats?

DHCP ACK

Dynamic Host Configuration Protocol

new client

DHCP discover (broadcast)



DHCP server

DHCP offer

"**offer**" message includes IP address, DNS server, "gateway router", and how long client can have these ("lease" time)

DHCP request (broadcast)

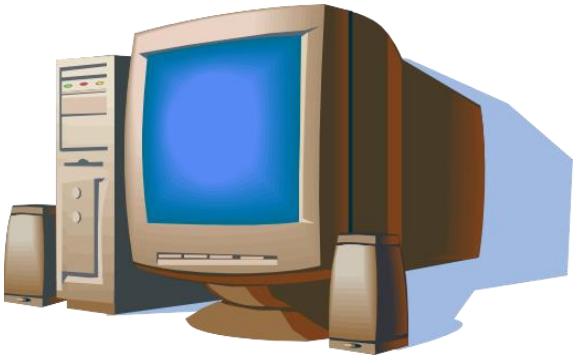
DHCP ACK

Attacker on same subnet can **hear** new host's DHCP request

Dynamic Host Configuration Protocol

new client

DHCP discover (broadcast)



DHCP server

DHCP offer

DHCP request (broadcast)

DHCP ACK

"**offer**" message includes IP address, DNS server, "gateway router", and how long client can have these ("lease" time)

Attacker can **race** the actual server; if they win, replace DNS server and/or gateway router

DHCP Threats

- DHCP Starvation:
  - It is a DOS attack which prevents valid hosts from getting Dynamic IP configuration
    - It works by broadcasting vast numbers of DHCP requests with spoofed MAC addresses simultaneously.
  - A Rogue DHCP server is used to pass invalid IP configuration information to valid hosts

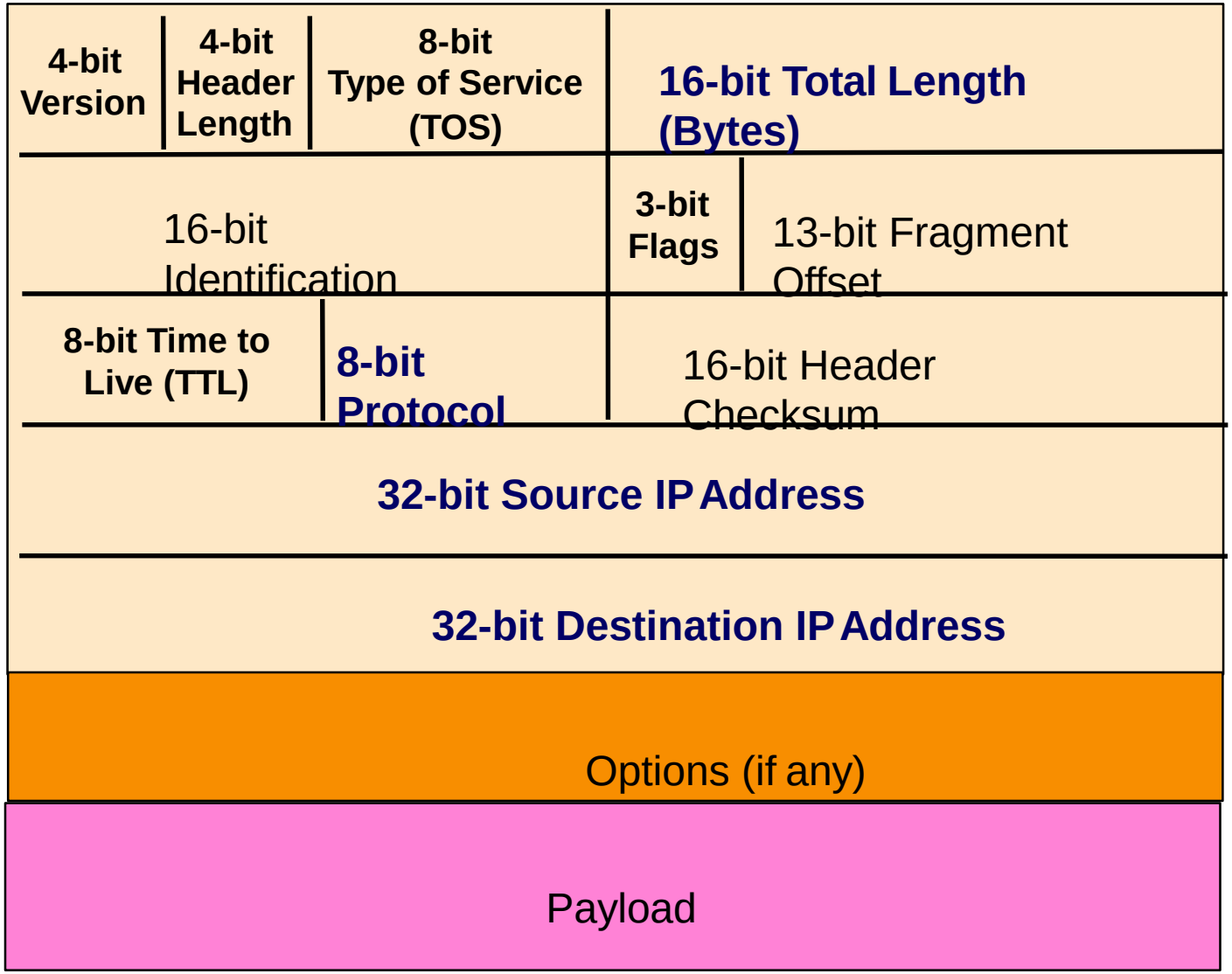
DHCP Threats

- Substitute a fake DNS server
  - Redirect any of a host's lookups to a machine of attacker's choice
- Substitute a fake gateway router
  - Intercept all of a host's off-subnet traffic
    - (even if not preceded by a DNS lookup)
  - Relay contents back and forth between host and remote server and modify however attacker chooses
- An invisible *Man In The Middle* (MITM)
  - Victim host has no way of knowing it's happening
    - (Can't necessarily alarm on peculiarity of receiving multiple DHCP replies, since that can happen benignly)
  - How can we fix this? **Hard**

Attacks in Layer 3

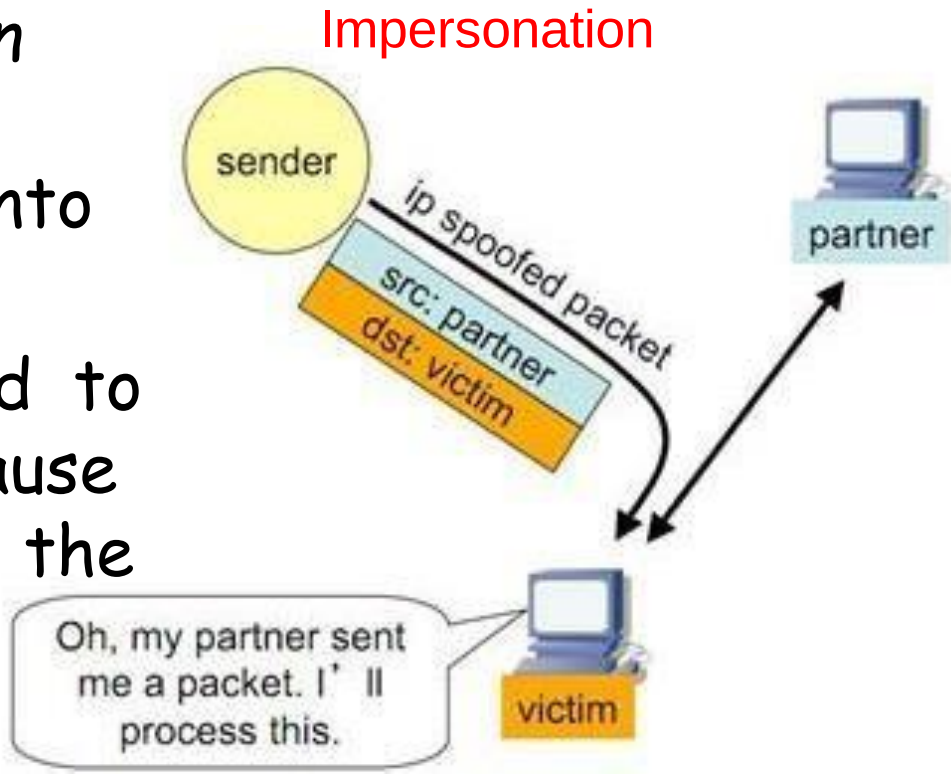
- The Network Layer (L3) is especially vulnerable to many DoS attacks and information privacy problems.
- The most popular protocol used in L3 is IP (Internet Protocol).
- The following are the key risks at L3 associated with the IP:
  - IP Spoofing
  - Teardrop attack
  - ICMP attacks
  - Ping Flood (ICMP Flood)
  - Ping to Death attack
  - Smurf attack

IP Packet Structure



IP Spoofing Attack

- Attacker creates IP packets with a forged *source IP address* to conceal the identity of the sender or to impersonate another computing system.
- The prime goal of an IP spoofing attack is to establish a connection that allows the attacker to *gain root access* to the host and to *create a backdoor* entry path into the target system.
- Spoofing is also sometimes used to refer to ***header forgery*** because attacker forges the header of the packets with fake information.



IP Address Spoofing-Implications

- Many network services use host names or address for identification and authentication
  - Host sends a Req msg to a remote service. Receiver either allows or disallows the service
- Many services are vulnerable to IP spoofing
  - RPC
  - NFS
  - X window system
  - Any service using IP address as authentication method

IP Spoofing Derivative Attacks

- Man in the middle attack: Allows sniffing packets in between
- Routing redirect: Send a packet advertising a false better route to reach a destination
- Source routing: Insert attacker host in the list
  - Strict: Packet has to traverse only through the addresses mentioned
  - Loose: In addition to the list mentioned, packet can traverse additional routers
- Smurf attack: send ICMP packet to a broadcast address with spoofed address
- SYN flooding: Send too many TCP connections with spoofed source address
- Sequence number prediction
- Session hijacking
- Denial of service

How to prevent Spoofing Attacks

1. Avoid using the source address authentication.
   Implement cryptographic authentication system wide.

2. Disable all the r* commands,
   remove all .rhosts files and empty the /etc/hosts.equiv file.
   This will force all users to use other means of remote access.

3. If you allow outside connections from trusted hosts, enable encryption sessions at the router.

4. TTL Value
   - Packet marking
   - Randomized Initial Sequence Number in TCP

5 IPSec.

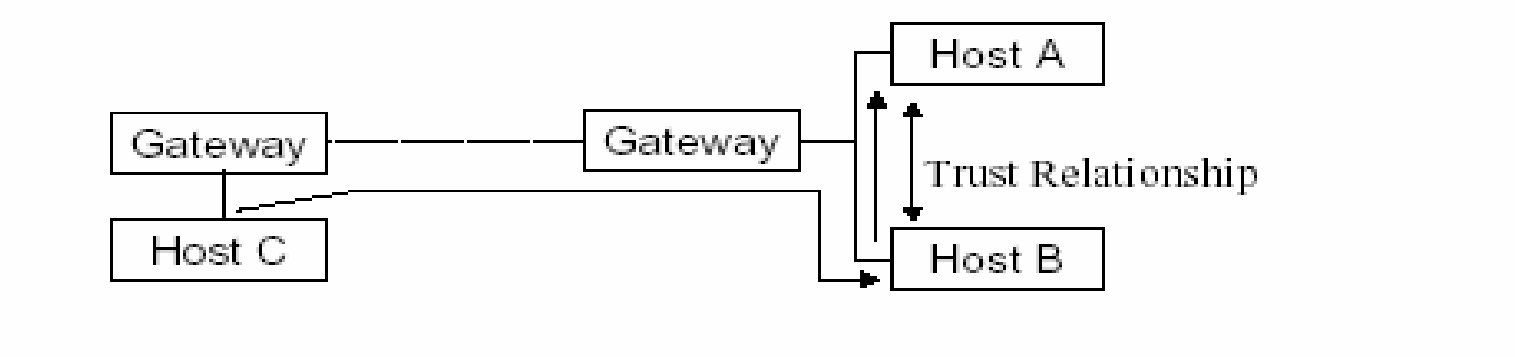
Types of Spoofing attacks (Non_blind)

1. Non-Blind Spoofing

Takes place when the attacker is on the same subnet as the victim. This allows the attacker to sniff packets making the next sequence number available to him.

Types of Spoofing attacks (Blind)

2. Blind Spoofing

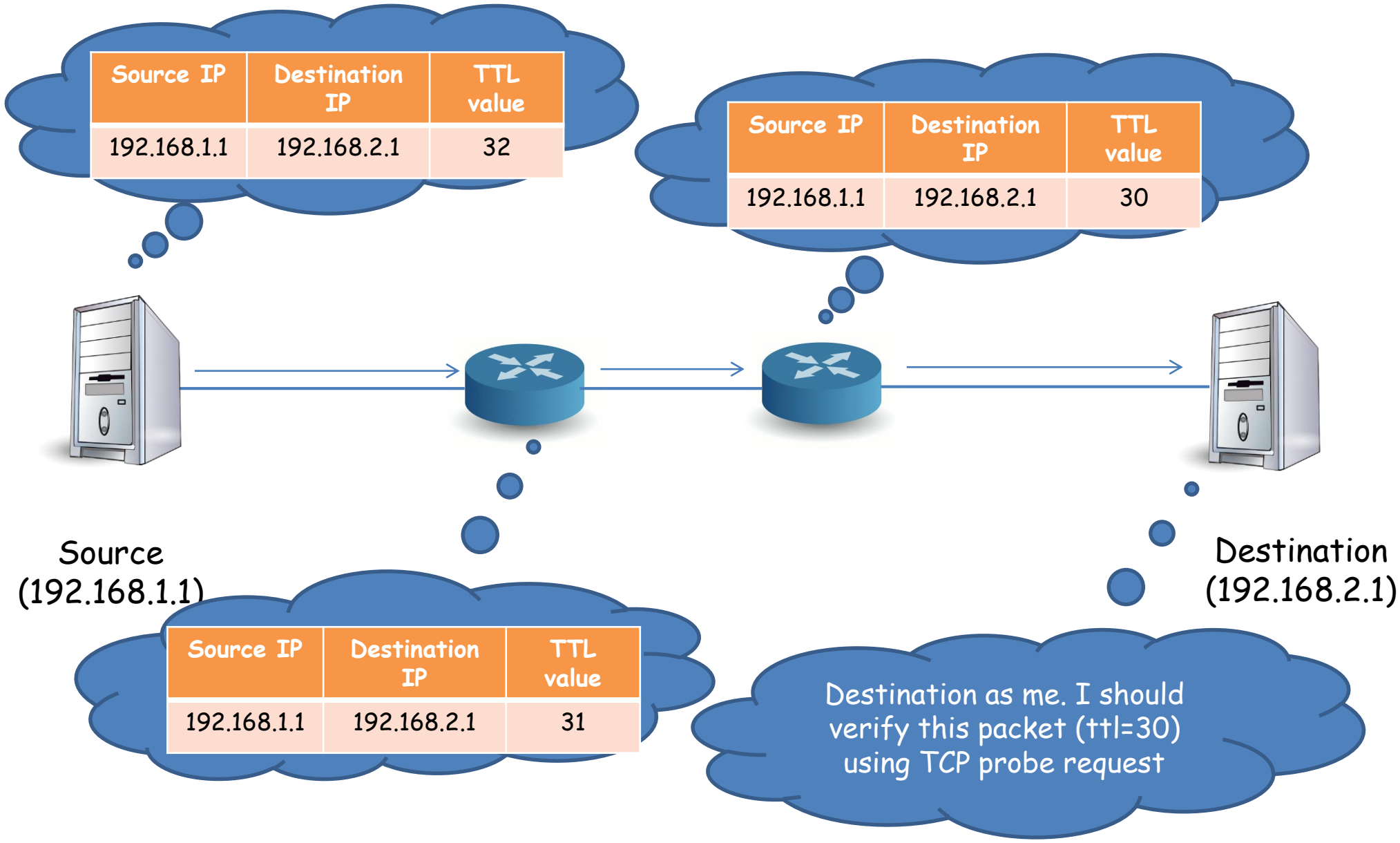


Usually the attacker does not have access to the reply.

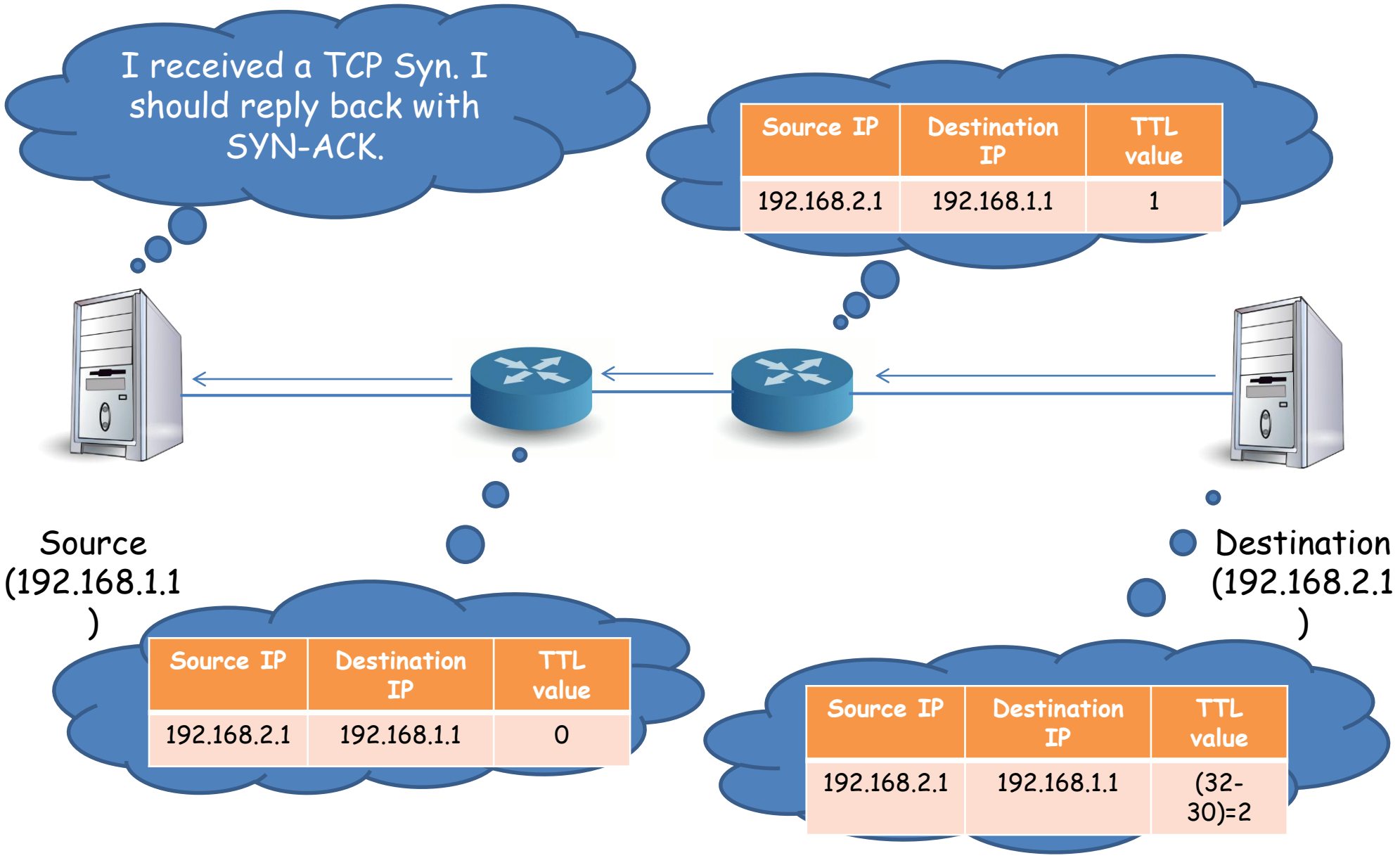
e.g. :Host C sends an IP datagram with the address of some other host (Host A) as the source address to Host B. Attacked host (B) replies to the legitimate host (A)

The sequence and acknowledgement numbers from the victim are unreachable. In order to circumvent this, several packets are sent to the victim machine in order to sample sequence numbers.

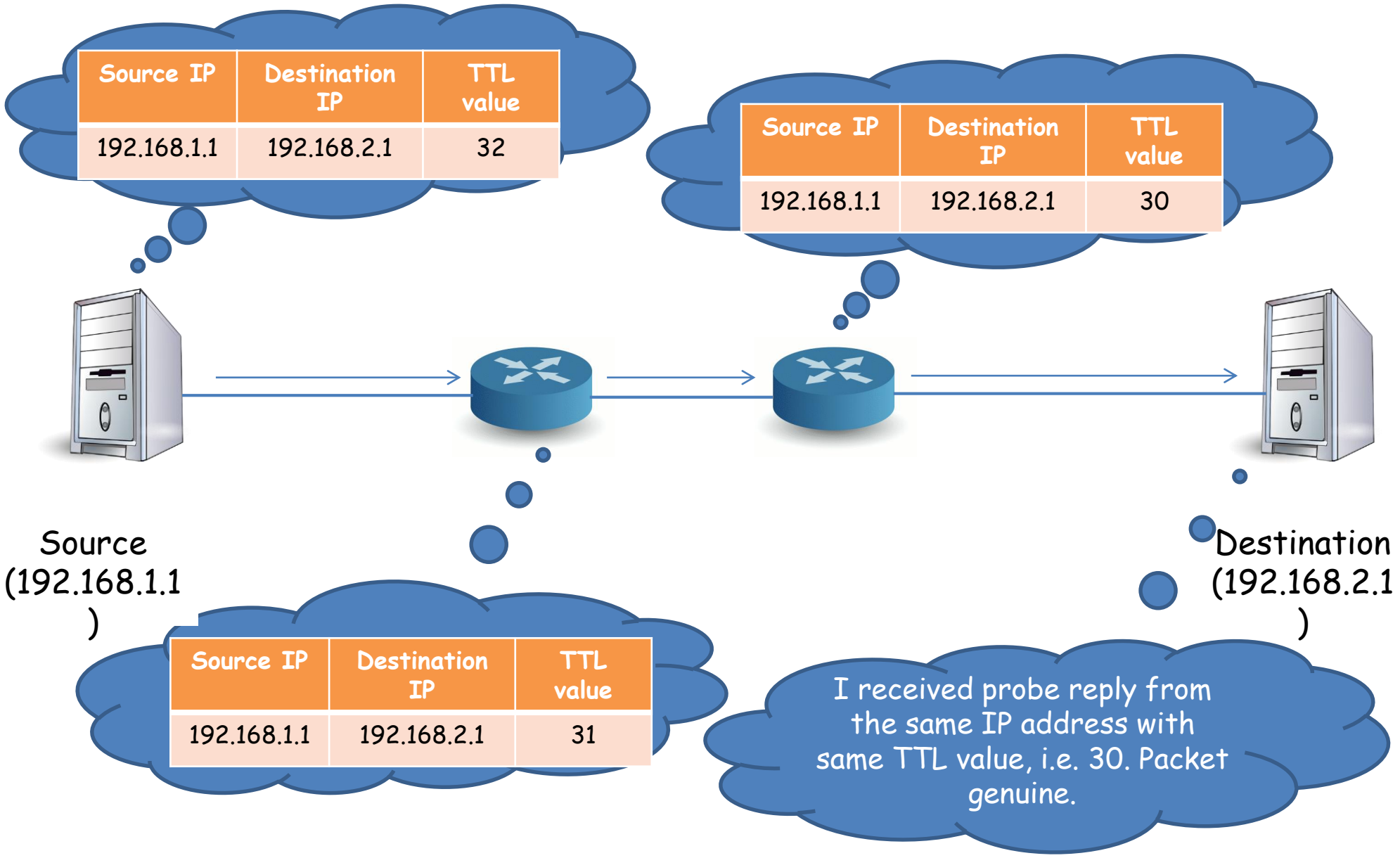
Normal Scenario



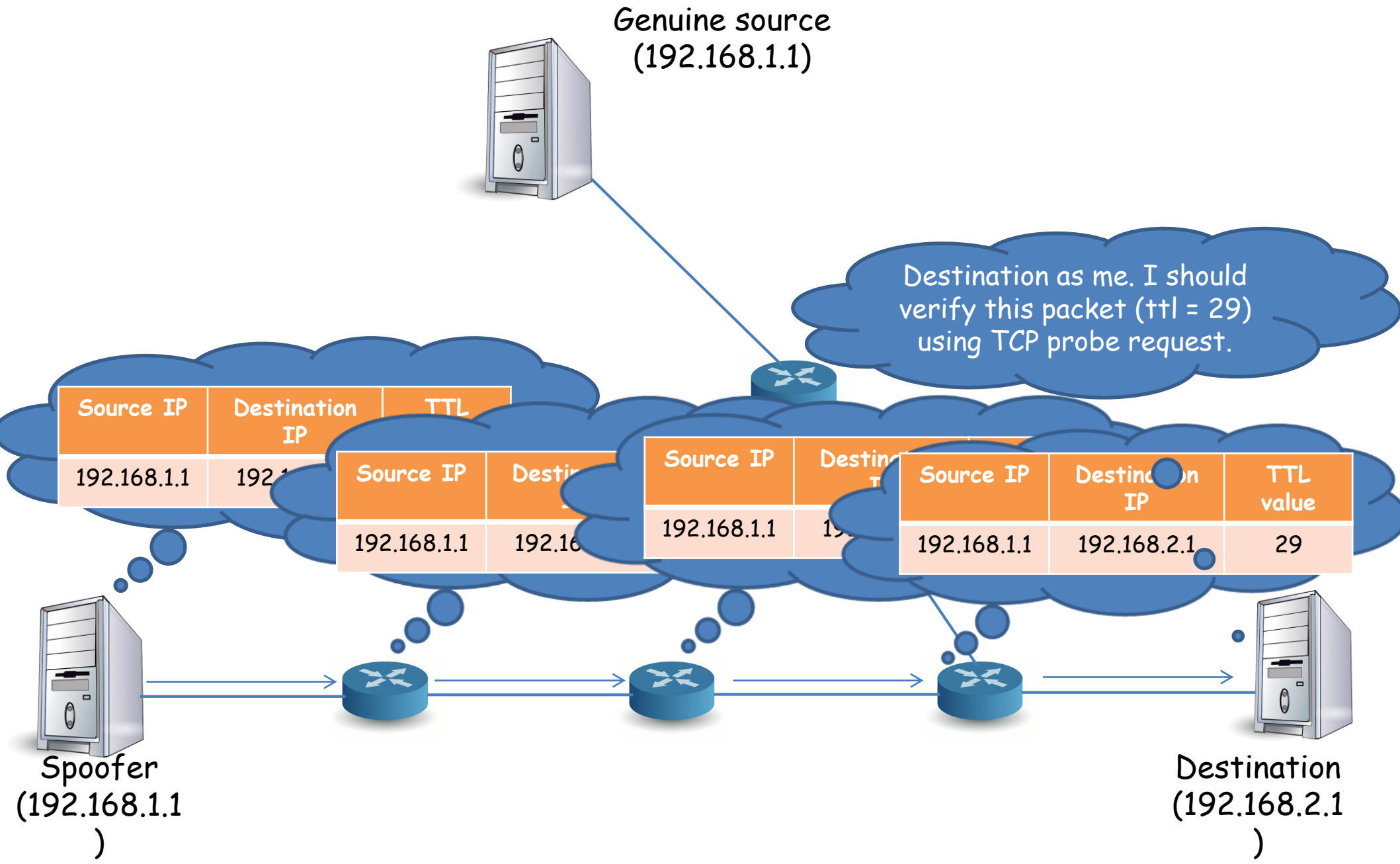
Normal Scenario (contd.)



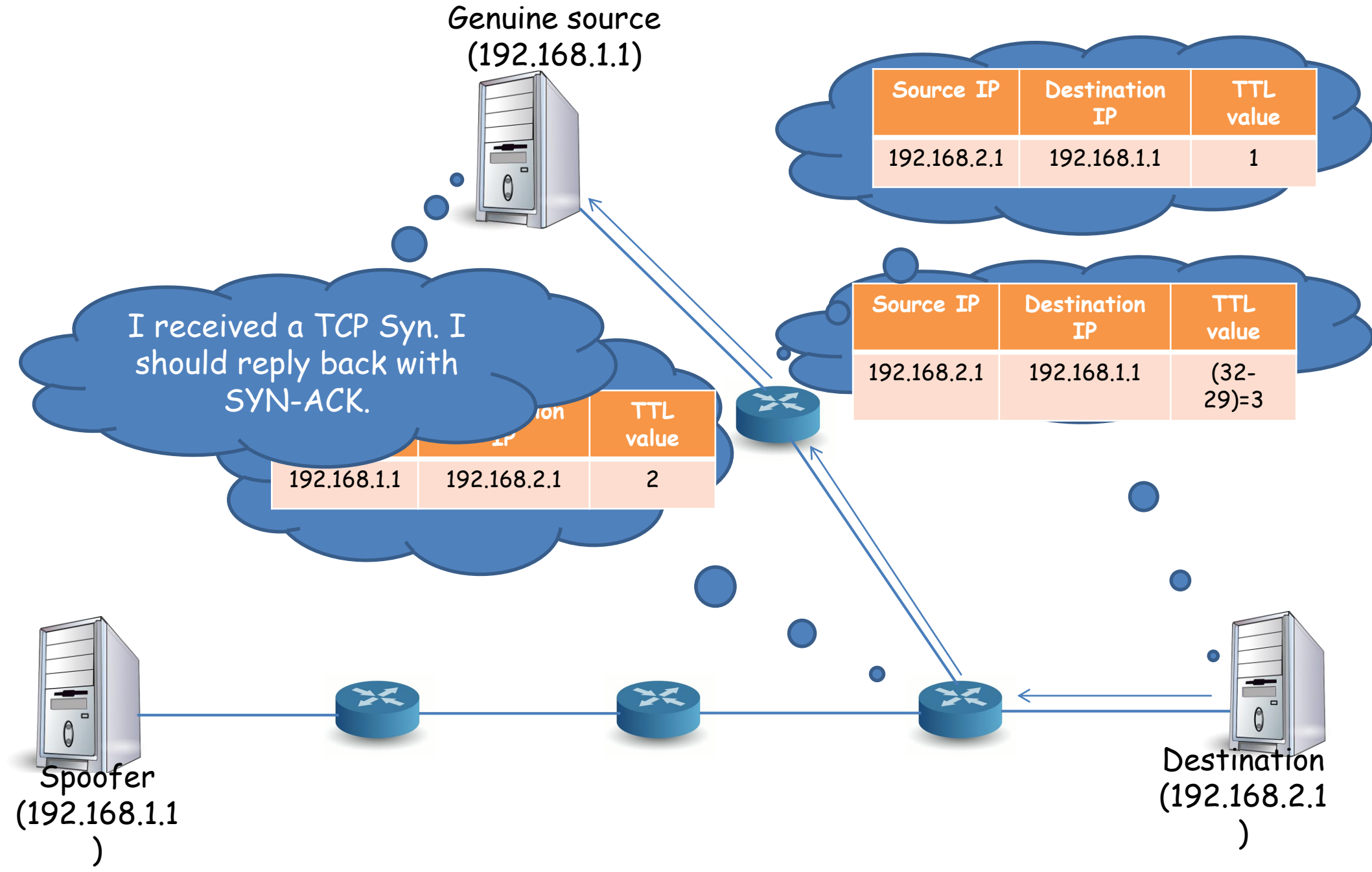
Normal Scenario (contd.)



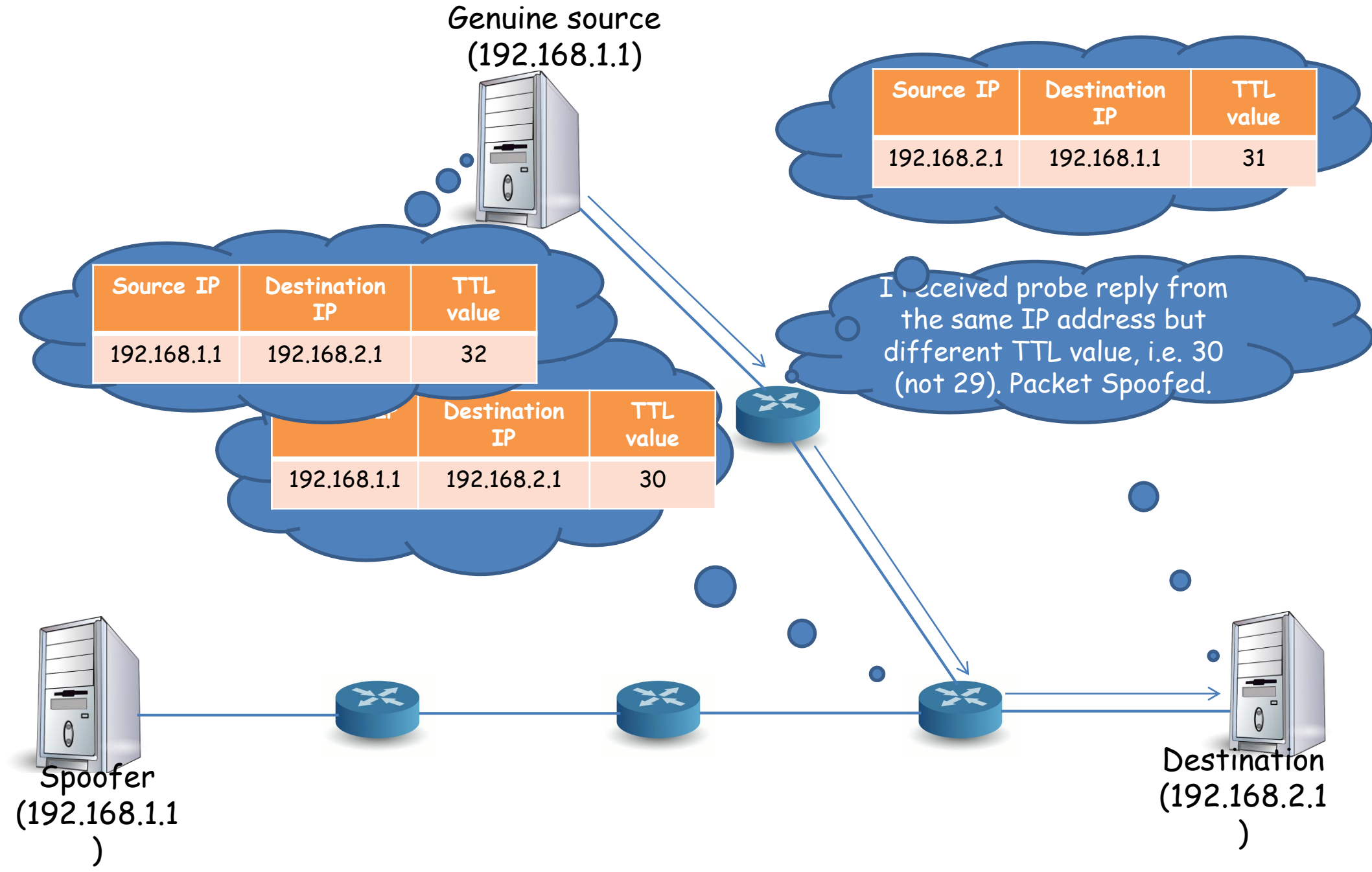
Spoofing Scenario 1



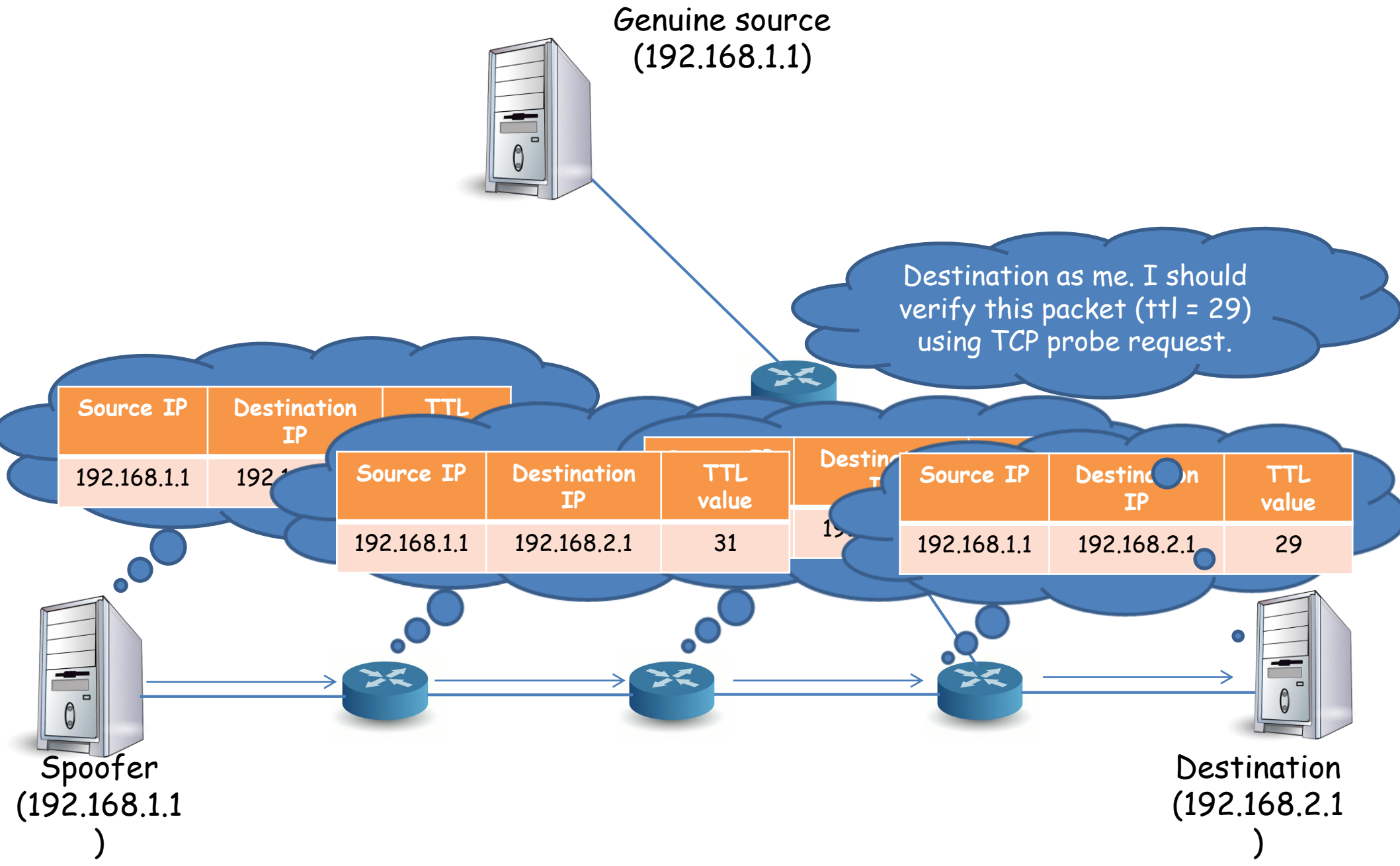
Spoofing Scenario 1 (contd.)



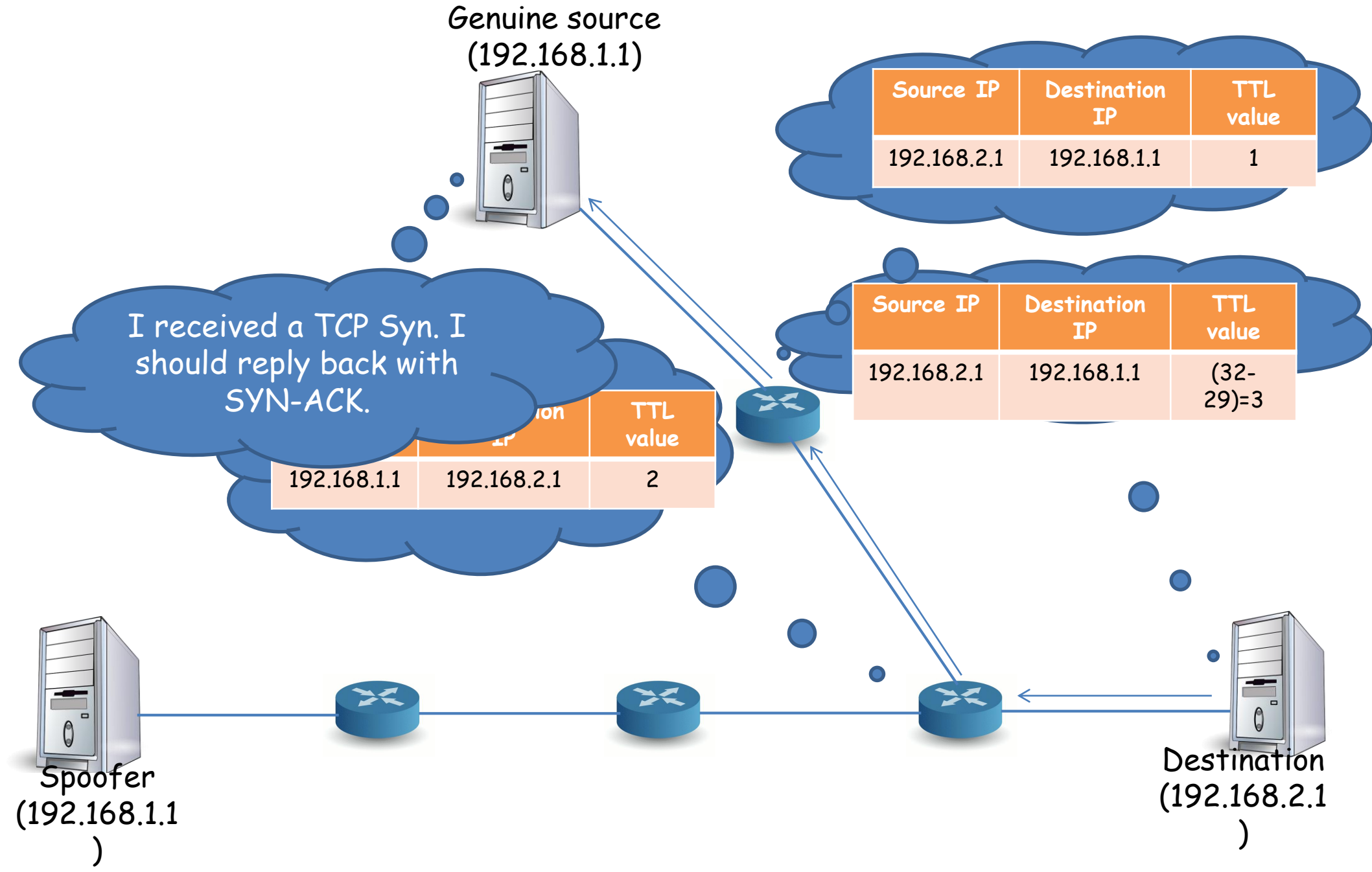
Spoofing Scenario 1 (contd.)



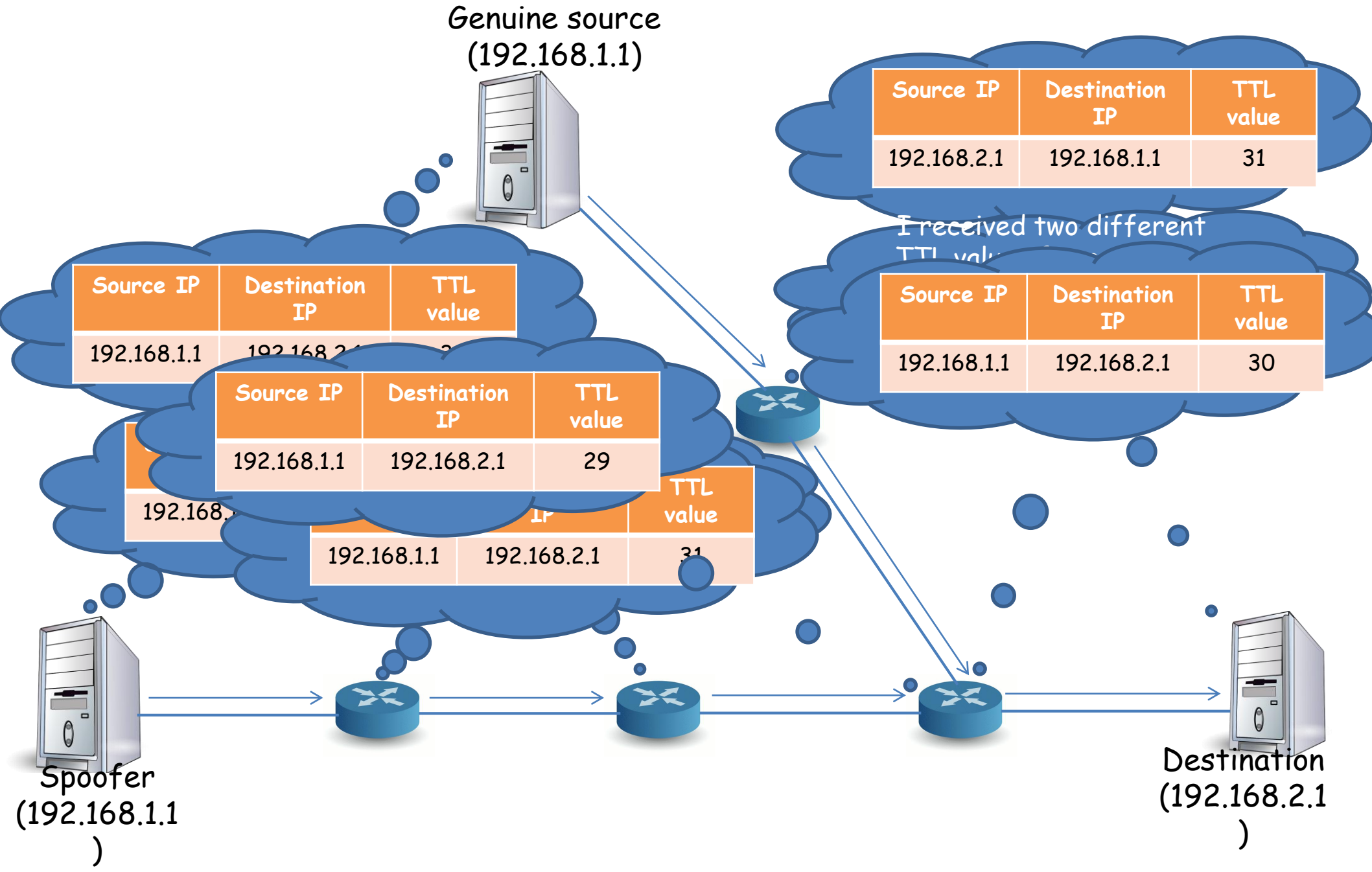
Spoofing Scenario 2



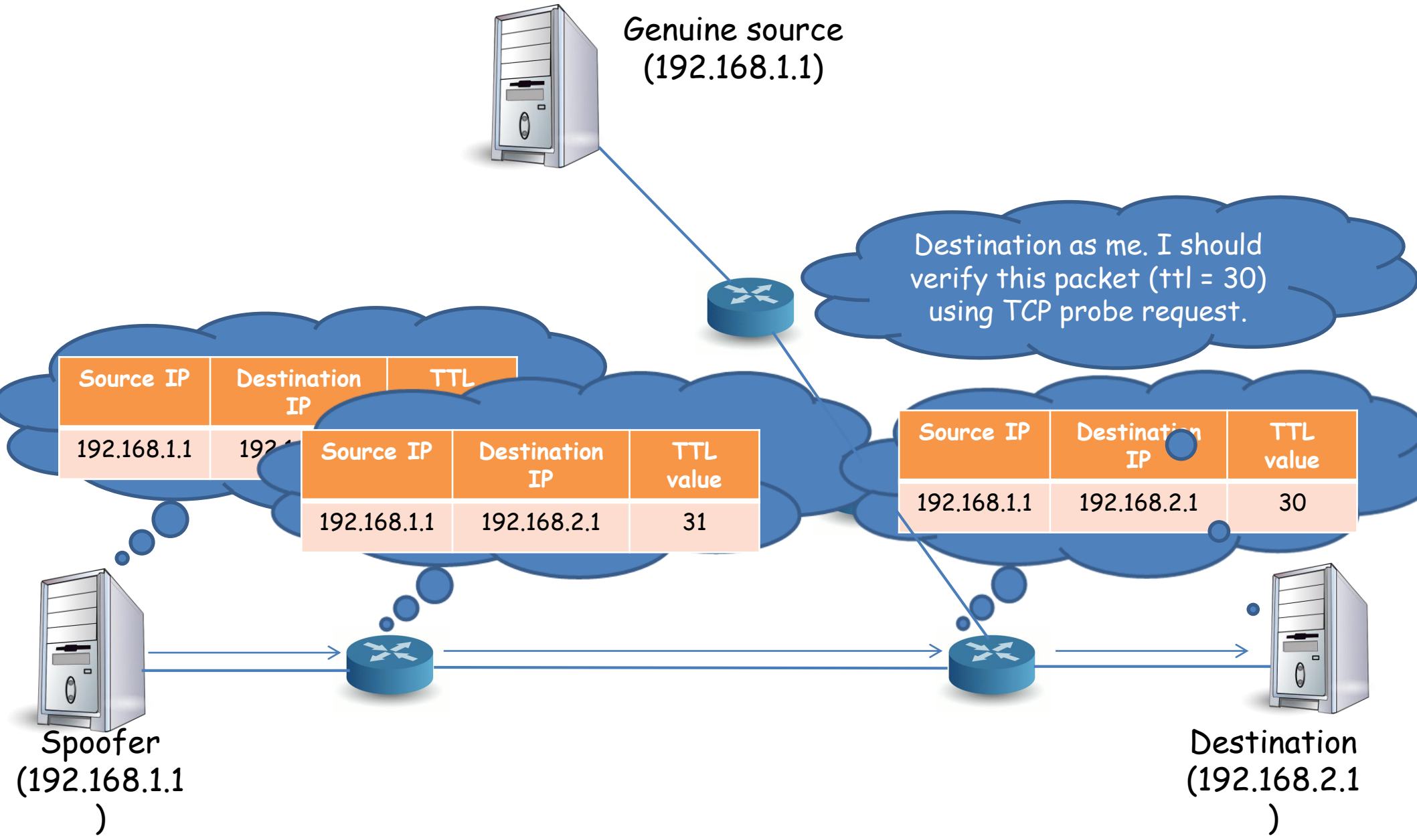
Spoofing Scenario 2 (contd.)



Spoofing Scenario 2 (contd.)

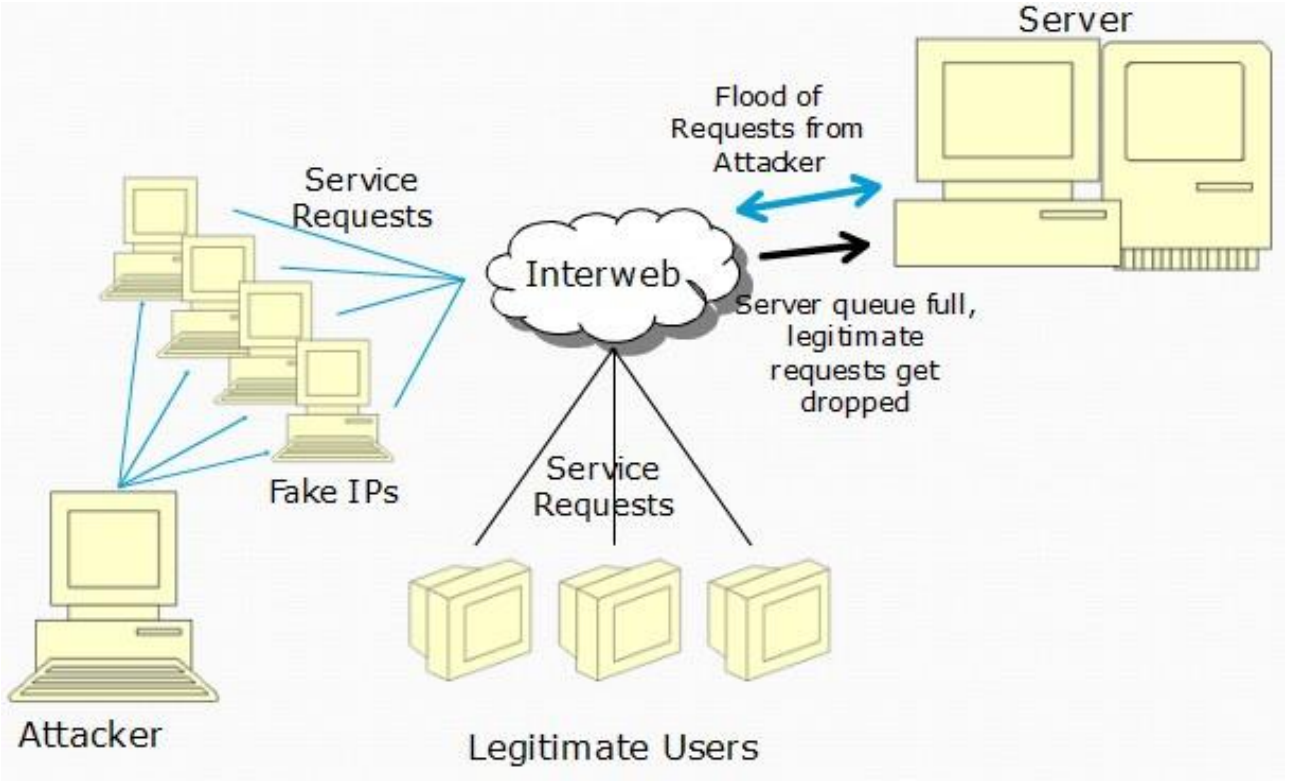


Spoofing Scenario 3



Flooding and DoS attack

- DoS attack with fake IPs
  - Attackers consume *bandwidth* and *resources* by flooding the target with as many packet as possible in a short amount of time.



Teardrop Attack

- Teardrop attack is a type of DoS attack to compromise the *availability* of the target system.
- It consists of an attacker sending a series of *fragmented IP* datagram pairs to the target system, and causes the system crash.