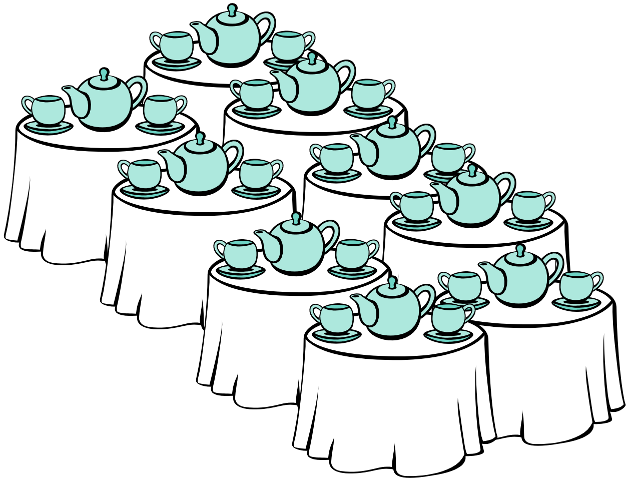
Denial of Service

- Understanding Denial of Service
- Some important DoS attacks
- Defense mechanisms

Dr. Yeonjoon Lee

How to take down a restaurant

Restauranteur



Saboteur

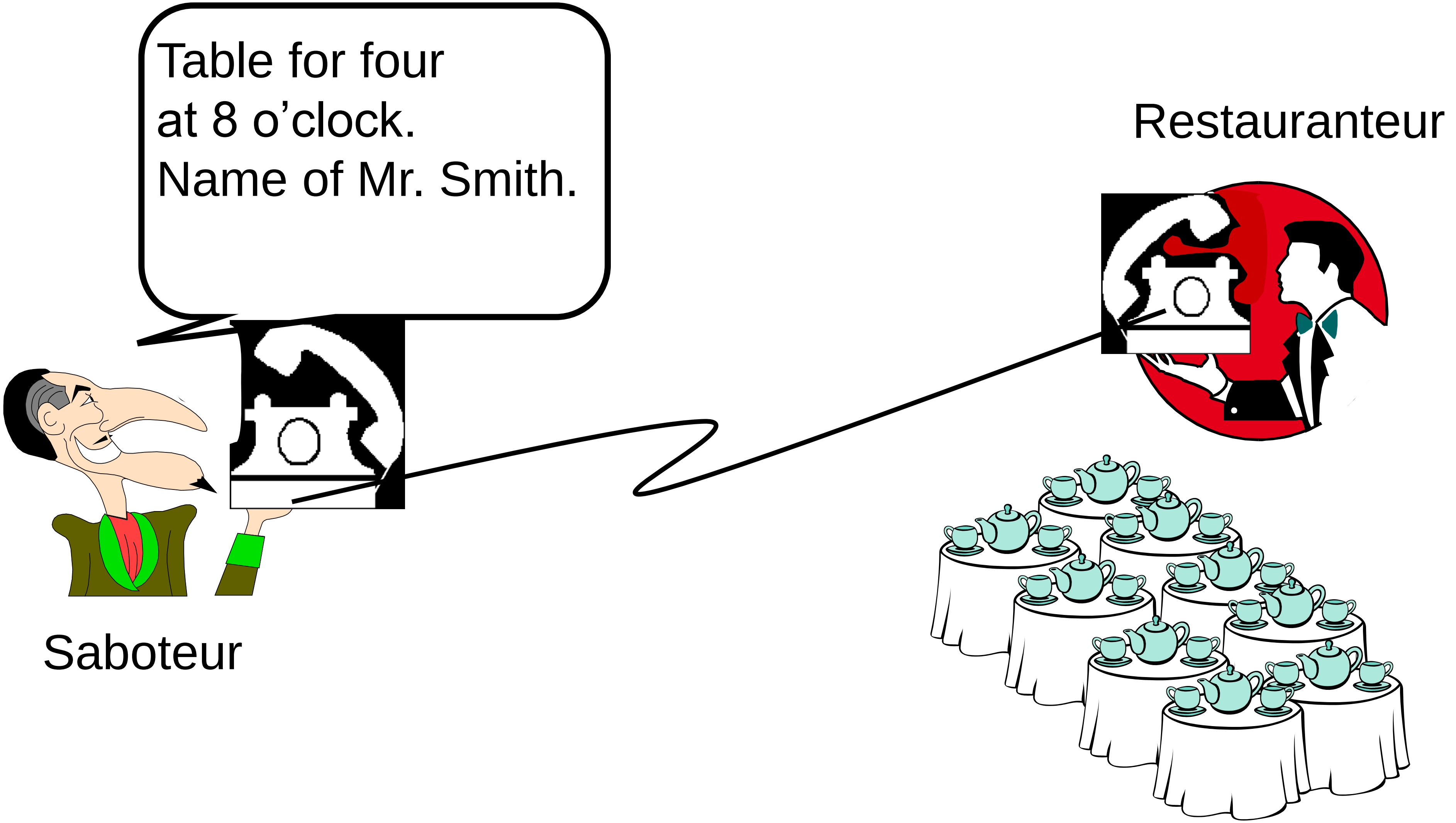
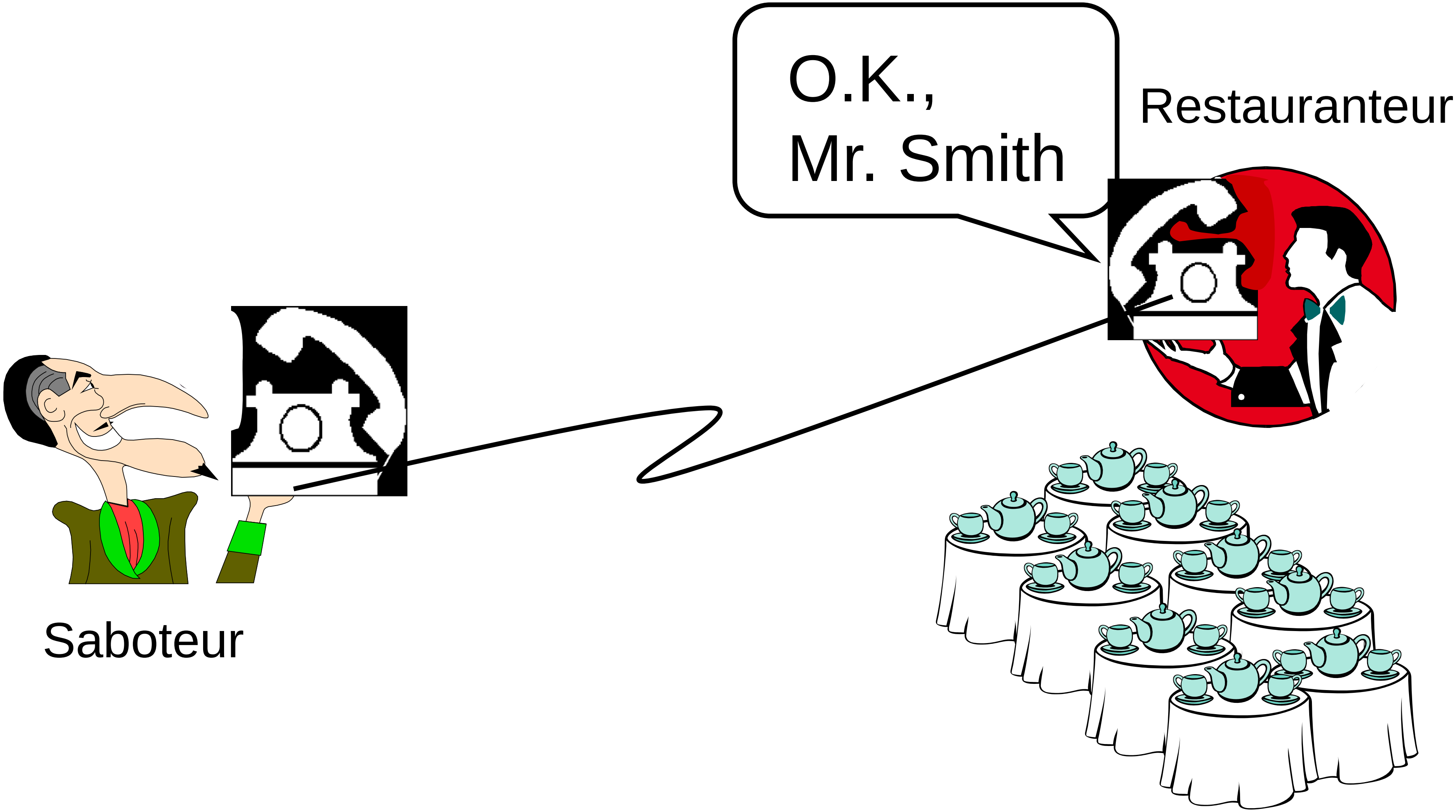


Table for four
at 8 o’clock.
Name of Mr. Smith.

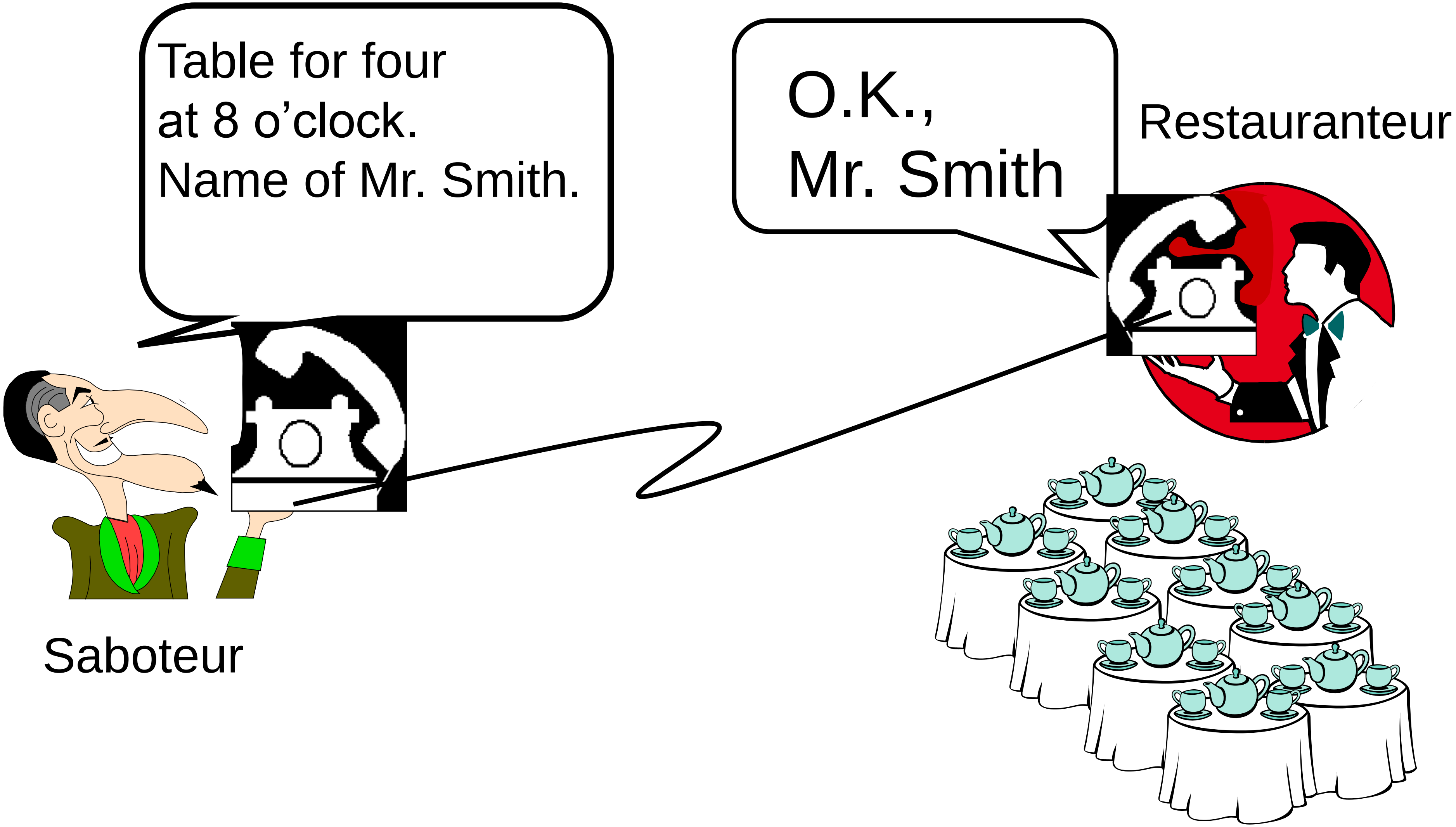
Restauranteur

Saboteur

Saboteur vs. Restauranteur



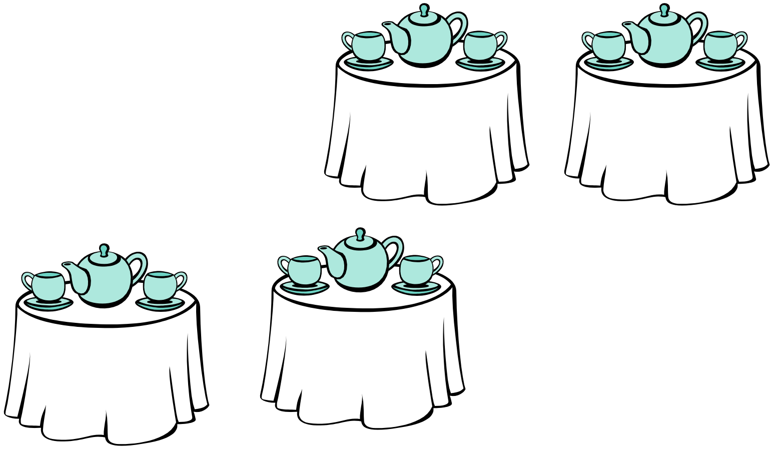
Saboteur vs. Restauranteur



Saboteur vs. Restauranteur

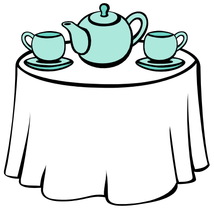
Restauranteur

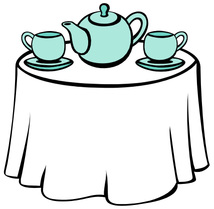
Saboteur

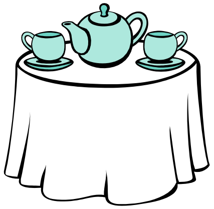


Restaurateur

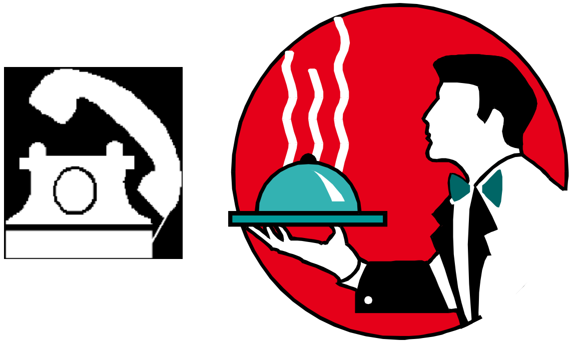
Saboteur



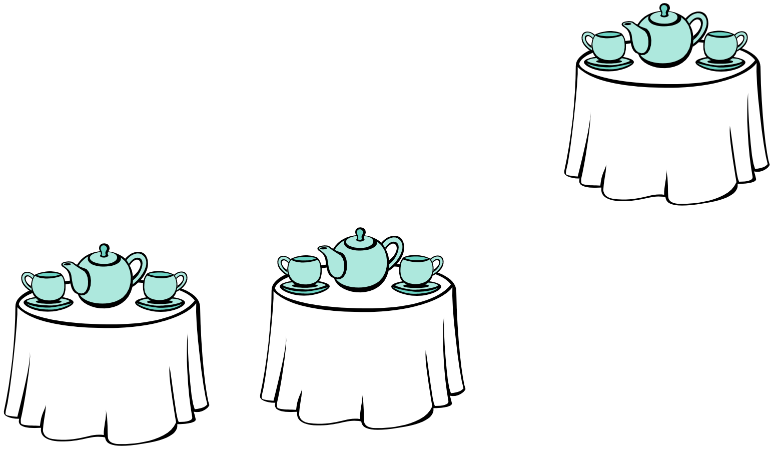




Restaurateur

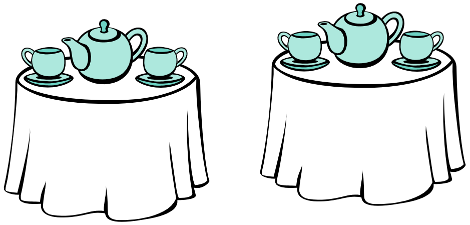


Saboteur



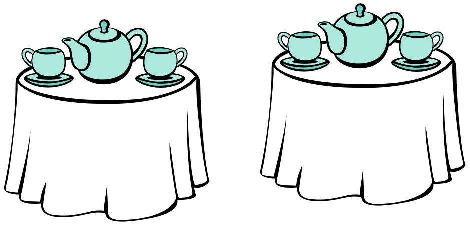
Restaurateur

Saboteur



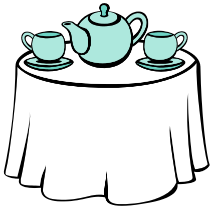
Restauranteur

Saboteur



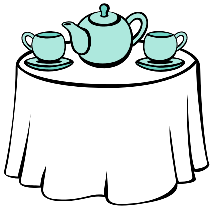
Restauranteur

Saboteur



Restauranteur

Saboteur



Restauranteur

Saboteur

Restauranteur

Saboteur

No More Tables!

Denial-of-service (DoS) attacks

- A general definition:

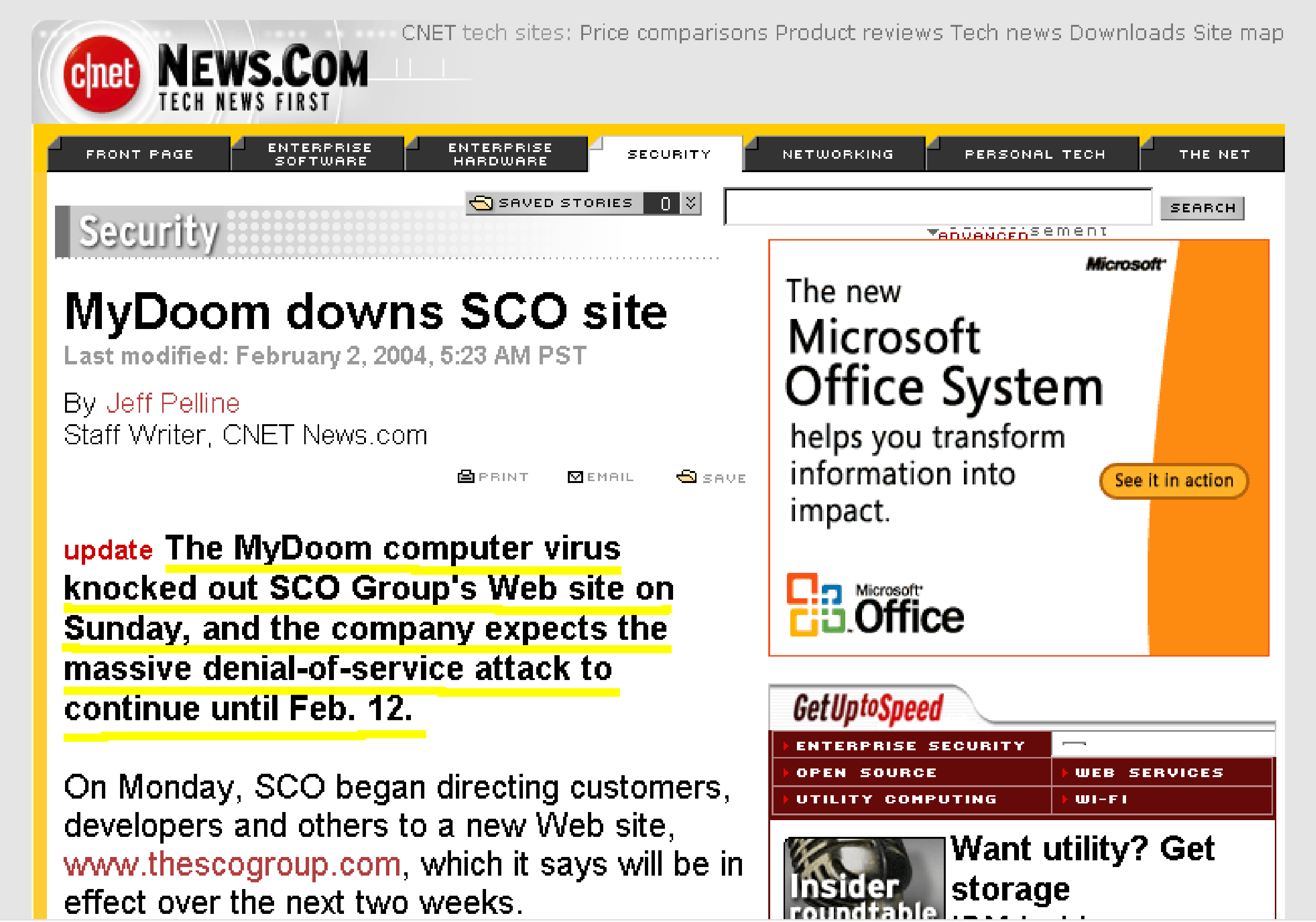
  An attack which prevents legitimate users from accessing a service from a computing system

- DoS is often interpreted as a resource exhaustion attack, an attack which causes the loss of network connectivity and services by
  - consuming the bandwidth of the victim network or
  - overloading the computational, memory resources of the victim system

Typical types of attacks

- Consumption of computational resources, such as bandwidth, disk space, or CPU time
  - Most frequently happen and most difficult to defend against
- Disruption of configuration information, such as routing information
  - Proper authentication mechanism will work
- Disruption of physical network components
  - Call the cop!!!

A real story



Security

MyDoom downs SCO site

Last modified: February 2, 2004, 5:23 AM PST

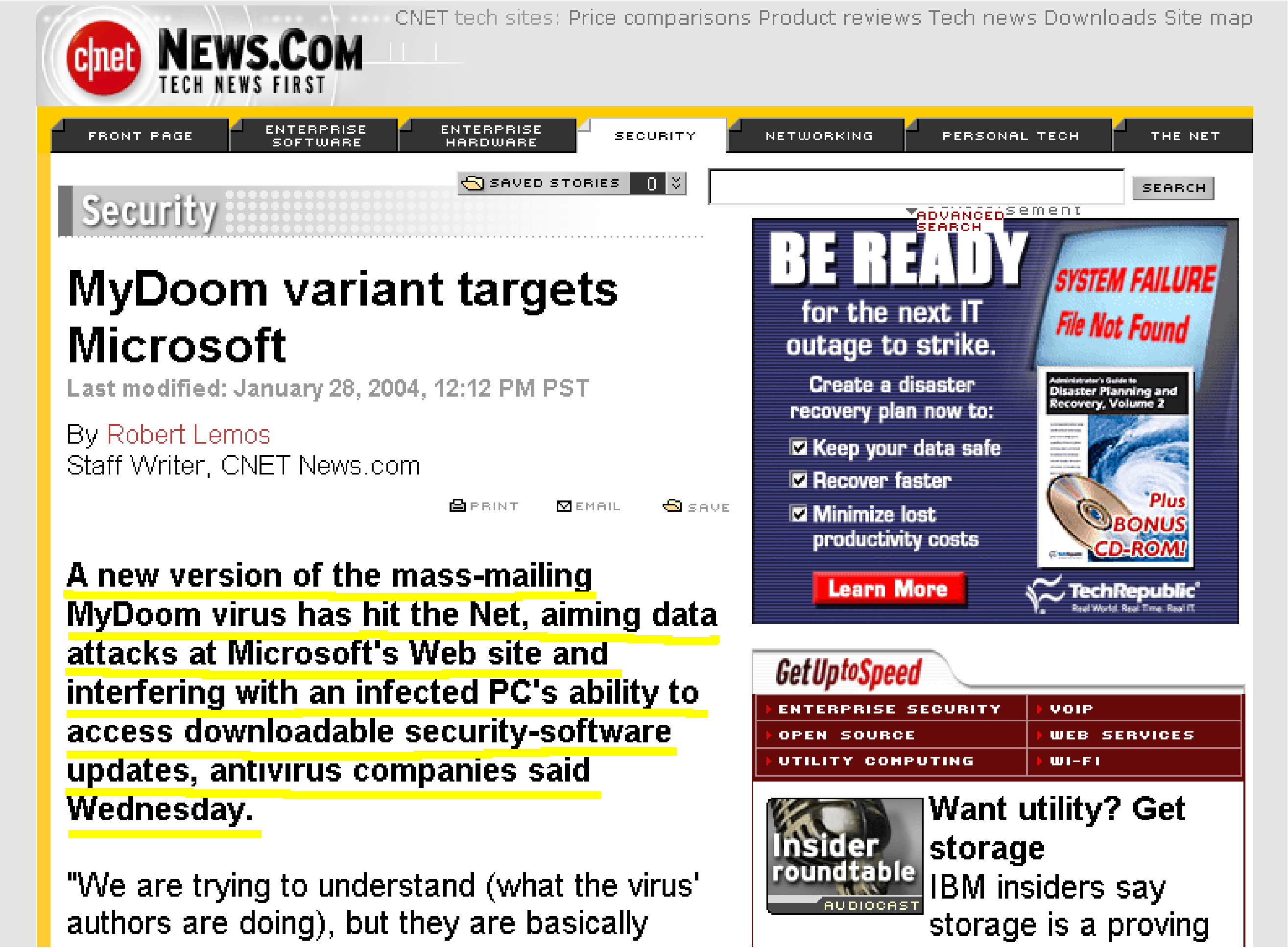
By Jeff Pelline
Staff Writer, CNET News.com

update **The MyDoom computer virus knocked out SCO Group's Web site on Sunday, and the company expects the massive denial-of-service attack to continue until Feb. 12.**

On Monday, SCO began directing customers, developers and others to a new Web site, www.thescogroup.com, which it says will be in effect over the next two weeks.

Want utility? Get storage

A real story (cont’d)



MyDoom variant targets Microsoft

Last modified: January 28, 2004, 12:12 PM PST

By Robert Lemos
Staff Writer, CNET News.com

A new version of the mass-mailing MyDoom virus has hit the Net, aiming data attacks at Microsoft's Web site and interfering with an infected PC's ability to access downloadable security-software updates, antivirus companies said Wednesday.

"We are trying to understand (what the virus' authors are doing), but they are basically

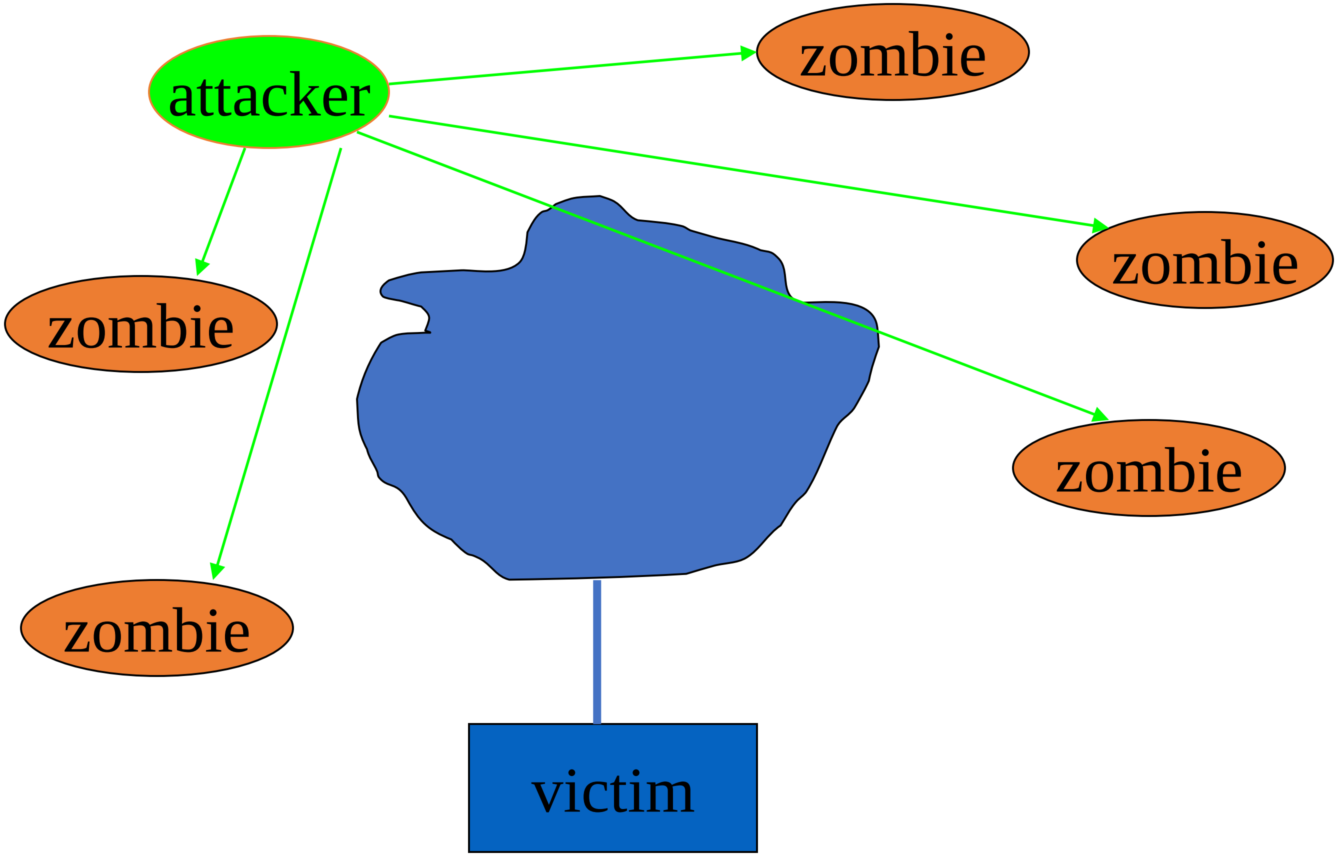
Get Up to Speed
- ENTERPRISE SECURITY
- VOIP
- OPEN SOURCE
- WEB SERVICES
- UTILITY COMPUTING
- WI-FI

Insider roundtable AUDIOCAST

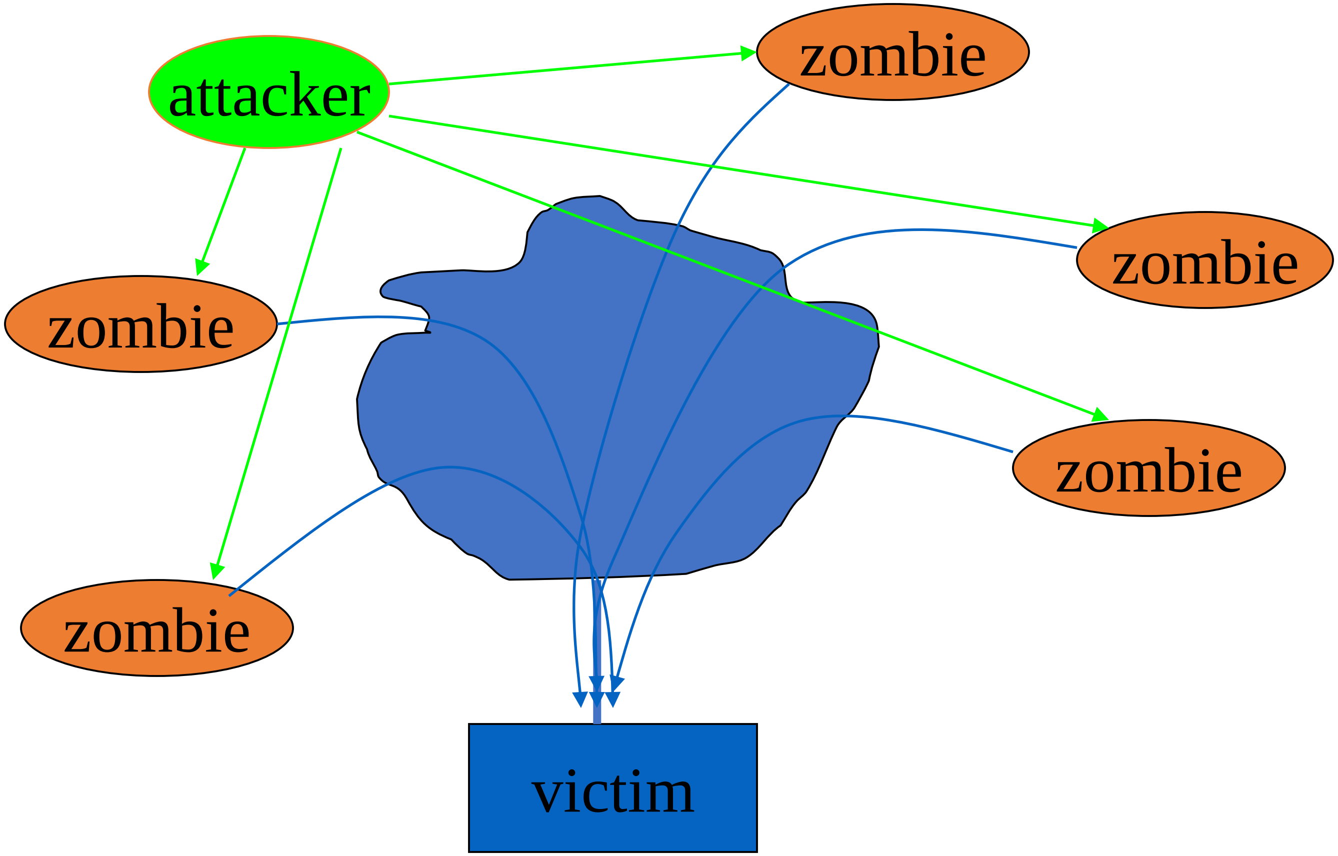
Want utility? Get storage

IBM insiders say storage is a proving

Distributed Denial-of-Service (DDoS) attacks



Distributed Denial-of-Service (DDoS) attacks



Some other famous DoS/DDoS events

- <1999: mostly “old fashion” DoS attacks, such as SYN flood, Ping of death, ..., first distributed attack tools (‘fapi’)

- 1999 - 2000: more robust DDoS tools (trinoo, TFN, Stacheldraht), auto-update, added encryption, bundled with rootkits, controlled with talk or ÍRC

- 2000: Brazilian government attacks, CNN, Yahoo, E-Bay, Datek taken down for several hours at a time due to traffic flooding

Famous events (cont'd)

- 2001: worms include DDos-features (i.e. Code Red), include time synchro., Register.com reflected DNS attack (Jan. 2001)

- 2002: DrDos (reflected) attack tools, (179/TCP; BGP=Border Gateway Protocol), India/Pakistani conflict - Yaha worm (2002) http://www.vnunet.com/News/1133119, Root DNS servers

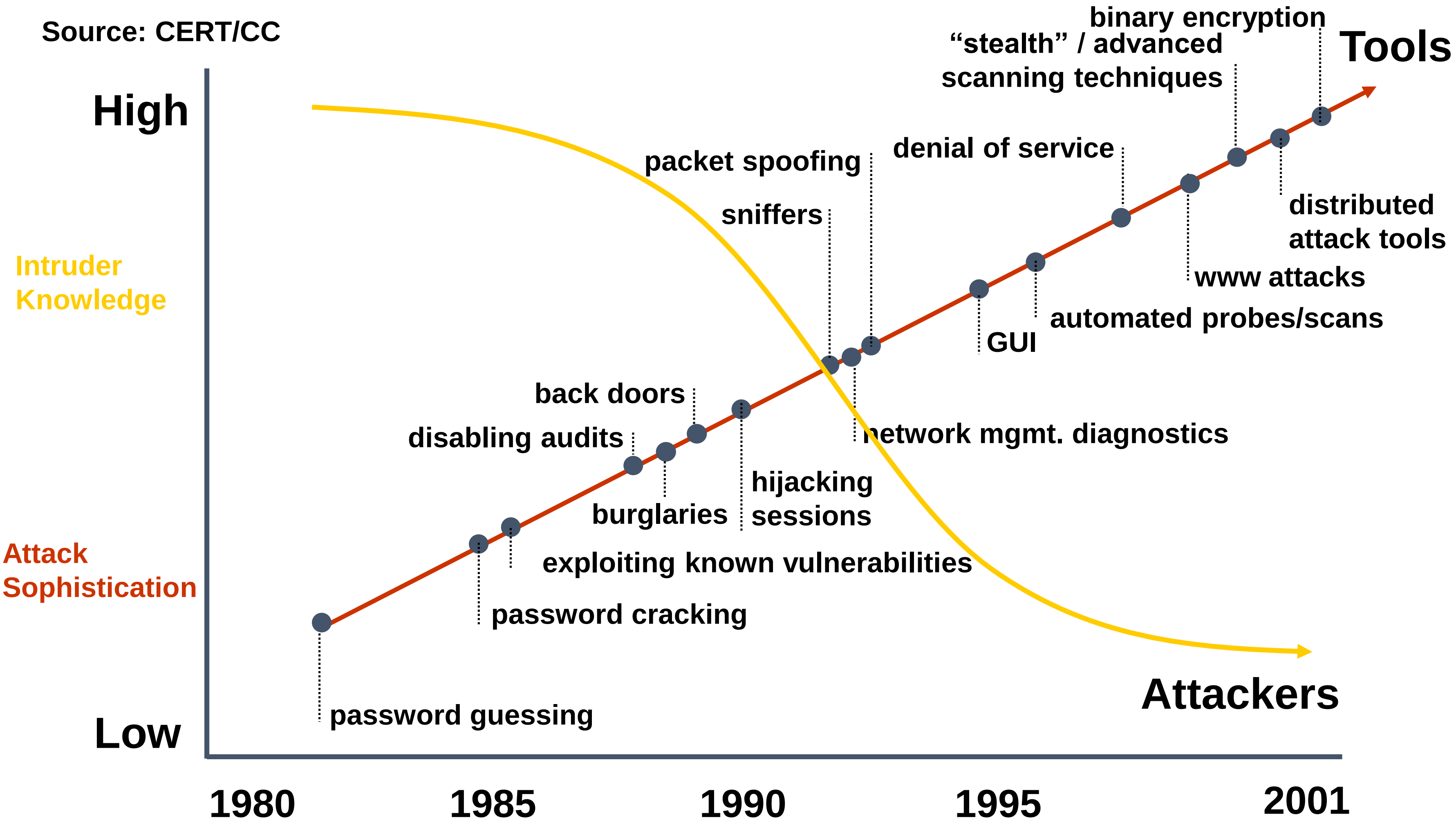
- 2003/2004: Mydoom infects thousands of victims to attack SCO and Microsoft. Al Jazeera web site was attacked http://www.infoworld.com/article/03/03/26/HNjazeera_1.html

Why DoS?

- “An Introduction to Denial of Service,” Hans Husman, 1996 http://packetstormsecurity.nl/docs/hack/denial.txt
  - Sub-cultural status
  - To gain access
  - Revenge
  - Political reasons
  - Economic reasons
  - Nastiness

Trend of attacks

Source: CERT/CC



Attackers

From

Dave Dittrich's

slides

The Joy of Tech
by Nitrozac & Snaggy
I'm so proud of Jimmy. Apparently he's one of the world's best at a new computer game.
Oh really! Which game?
Something called "DDOS Attack"
HACKER MOM
© 2000 Geek Culture™
joyoftech.com

Who downed CNN, E-Bay and Yahoo

From
Dave Dittrich's
slides

SHENEMAN The Star-Ledger
SAID HE DID IT TO IMPRESS BRITNEY SPEARS.
OFFICIALS APPREHEND 15 YEAR OLD HACKER, MAFIABOY

Denial of Service

- Some important DoS attacks

DoS and network protocol layers

- TCP/IP protocol suite contains four layers
  - Link, IP, TCP and application

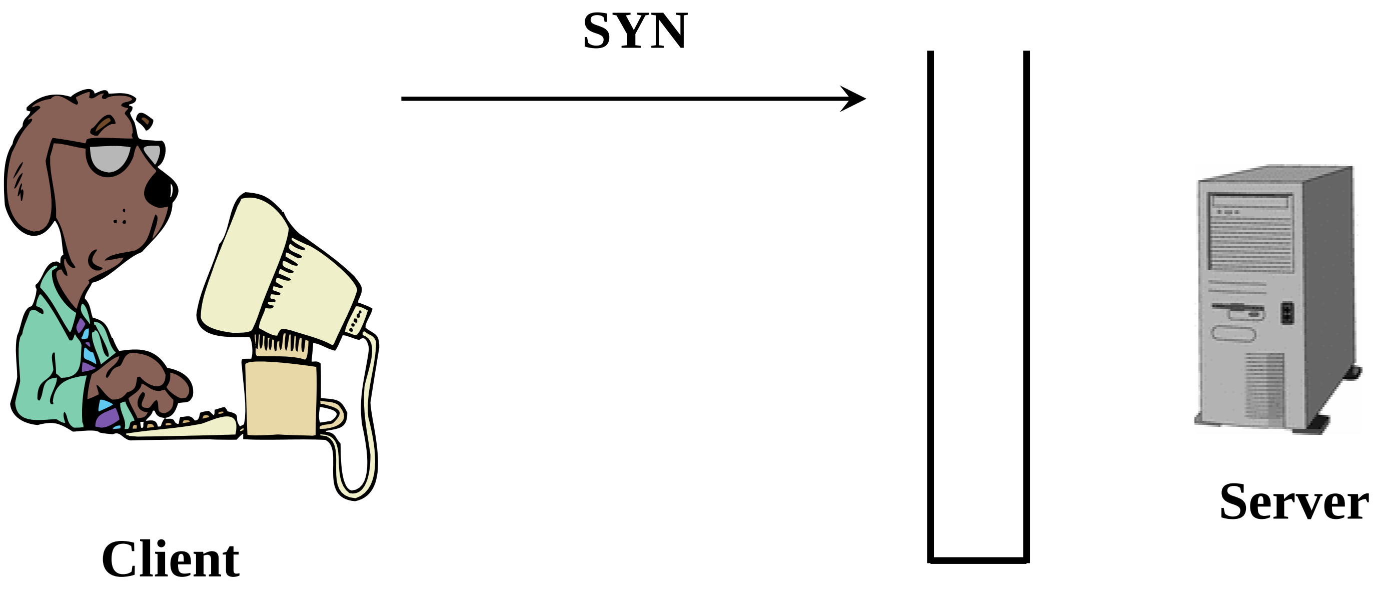
- DoS attacks could aim at all these layers
  - Link: damage of hardware, signal jamming, etc
  - IP: bandwidth exhaustion attacks, etc
  - TCP: Syn-flooding, etc
  - Application: authentication attacks, SPAM, etc

DoS on TCP: Syn-flooding attacks

- One of the most famous “old-fashion” DoS attacks
  - Attacker: an individual, with limited resources
  - Target: high performance computers on a high-speed network
  - Method: exploiting a vulnerability in the software system

- Syn-flooding
  - Exploiting the vulnerability in TCP connection protocol which is also known as three-way handshaking protocol

TCP three-way handshaking

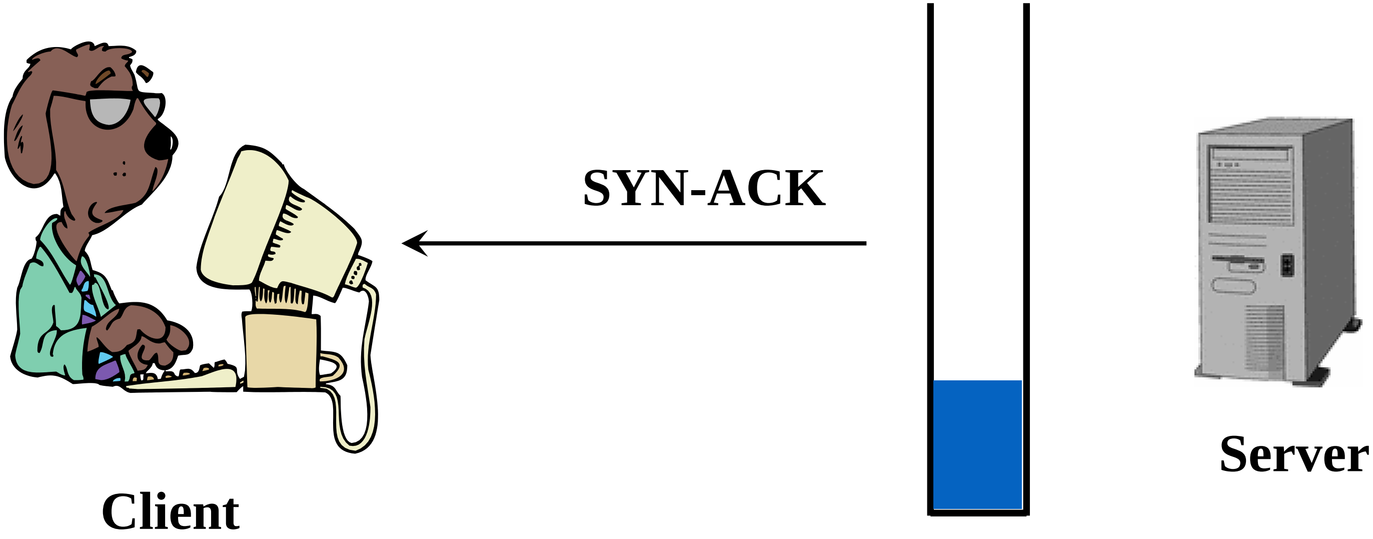


SYN

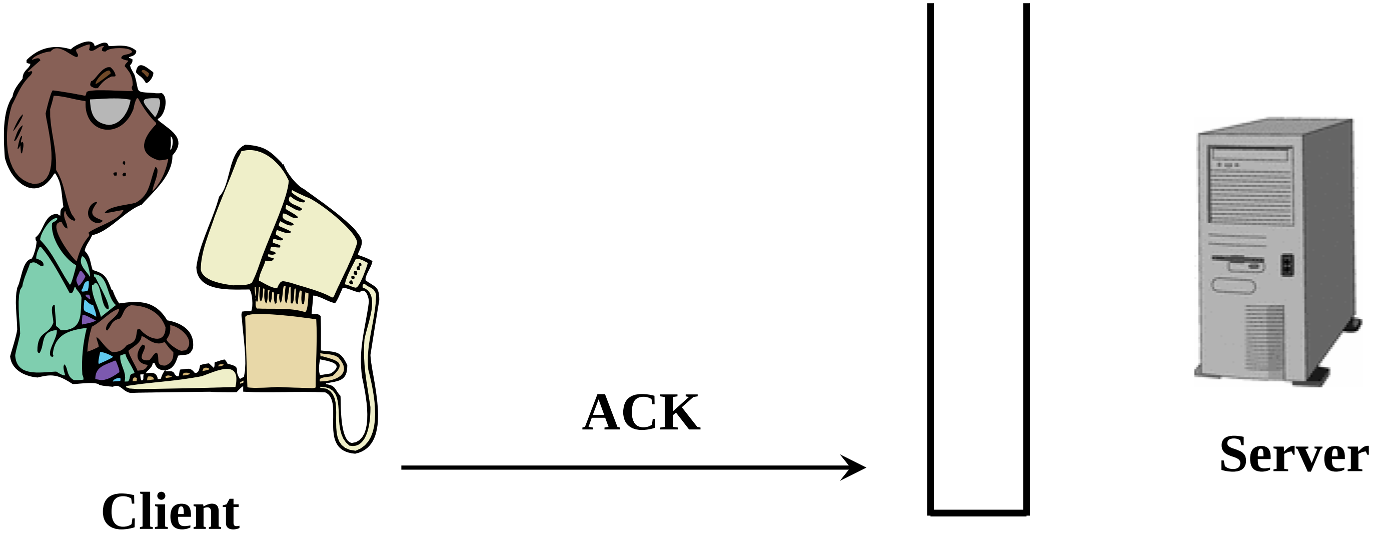
Client

Server

TCP three-way handshaking



TCP three-way handshaking

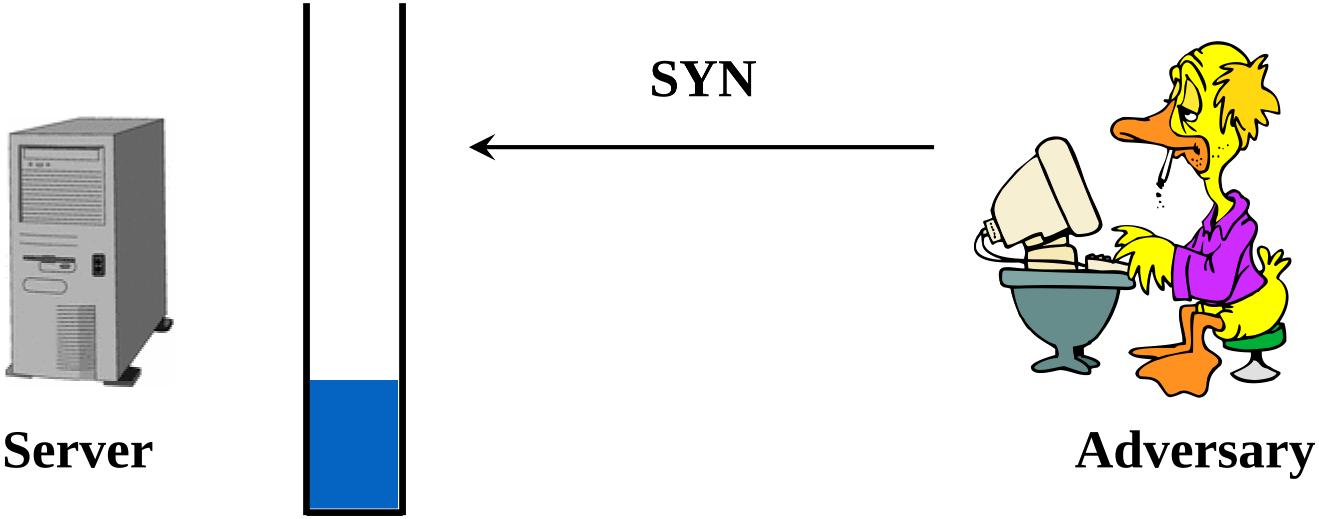


ACK

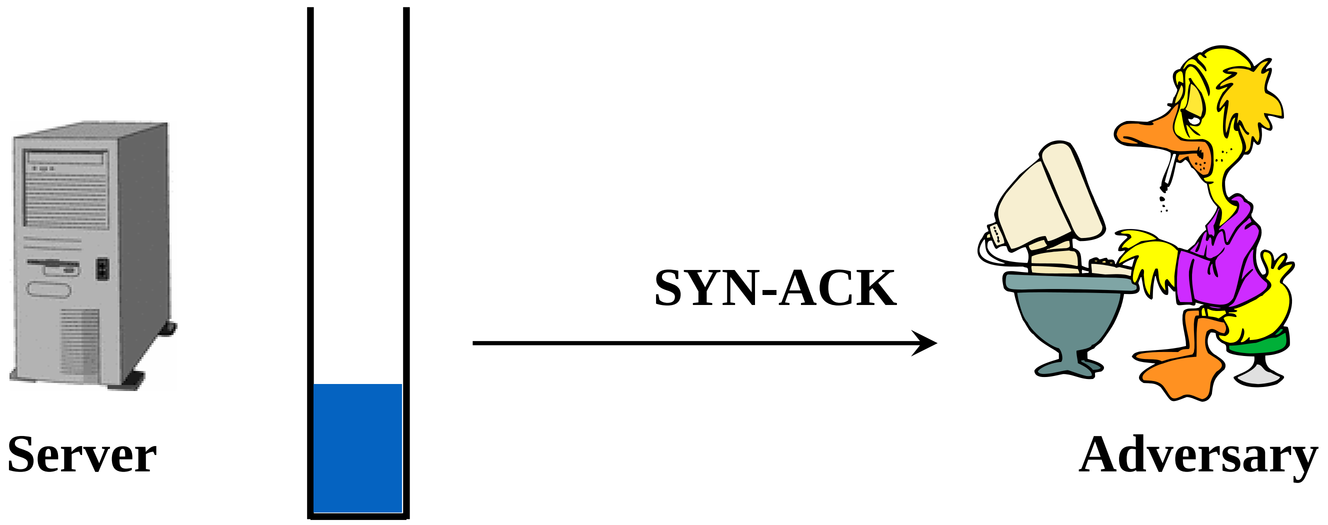
Client

Server

Syn-flooding !



Syn-flooding !

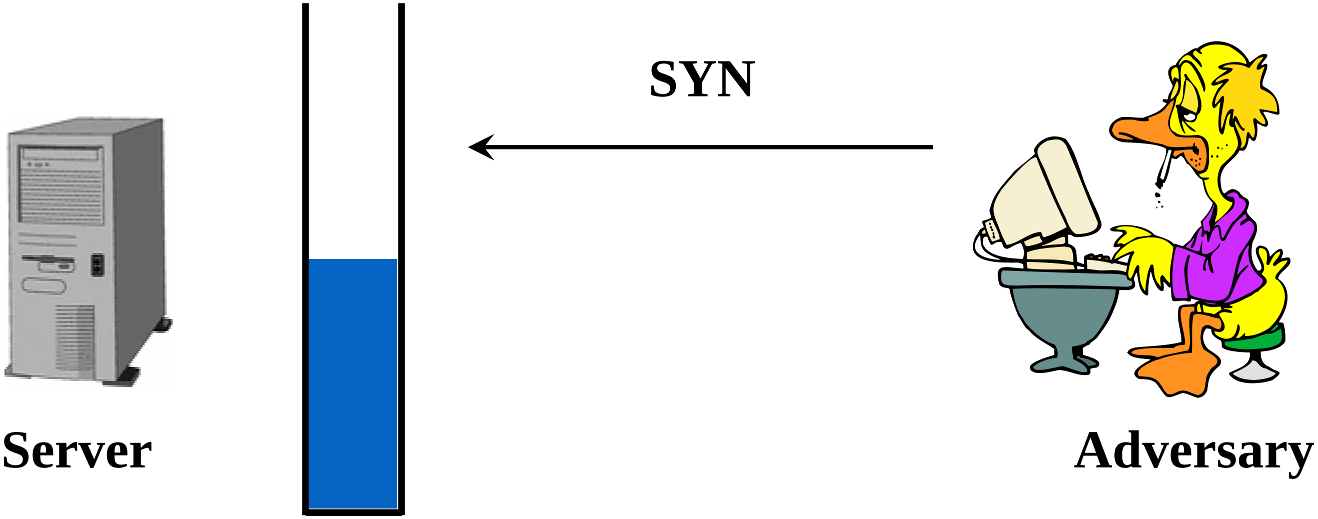


SYN-ACK

Server

Adversary

Syn-flooding !

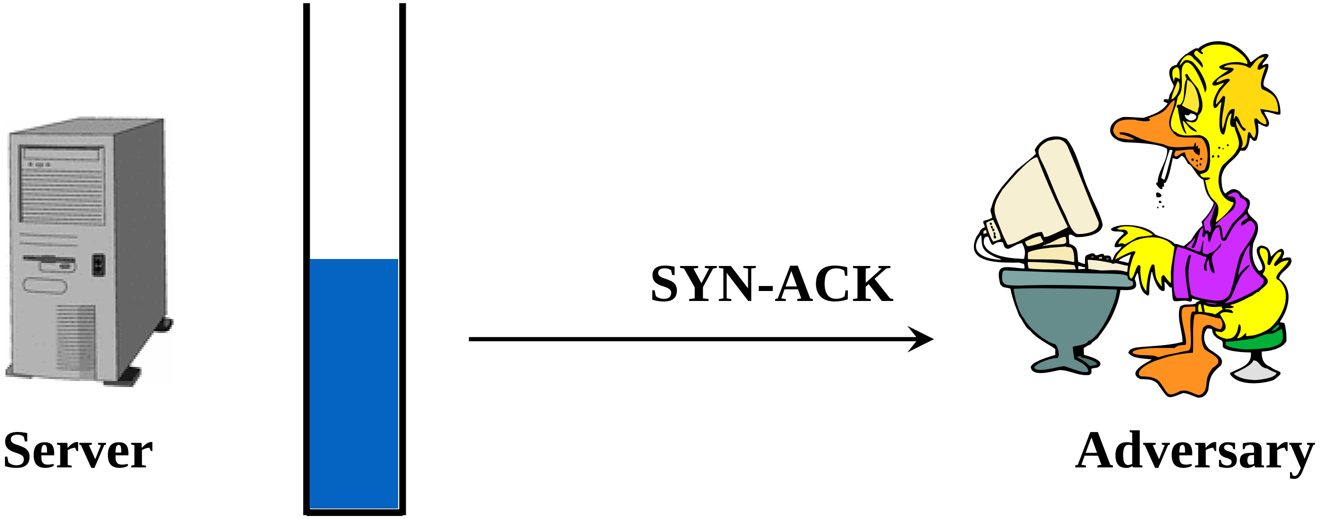


SYN

Server

Adversary

Syn-flooding !

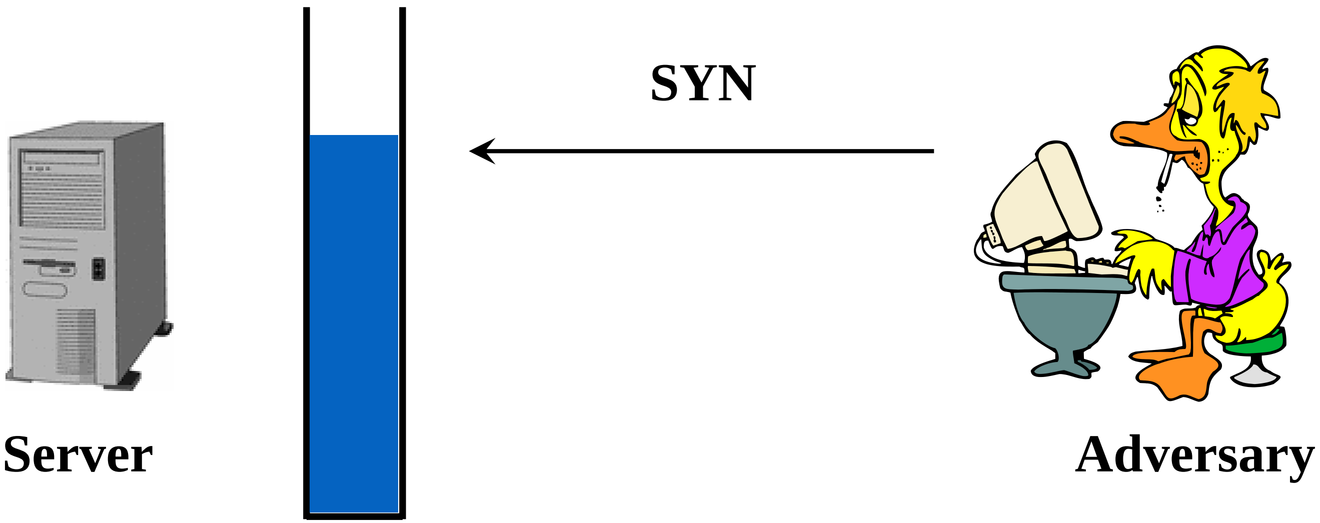


Server

SYN-ACK

Adversary

Syn-flooding !

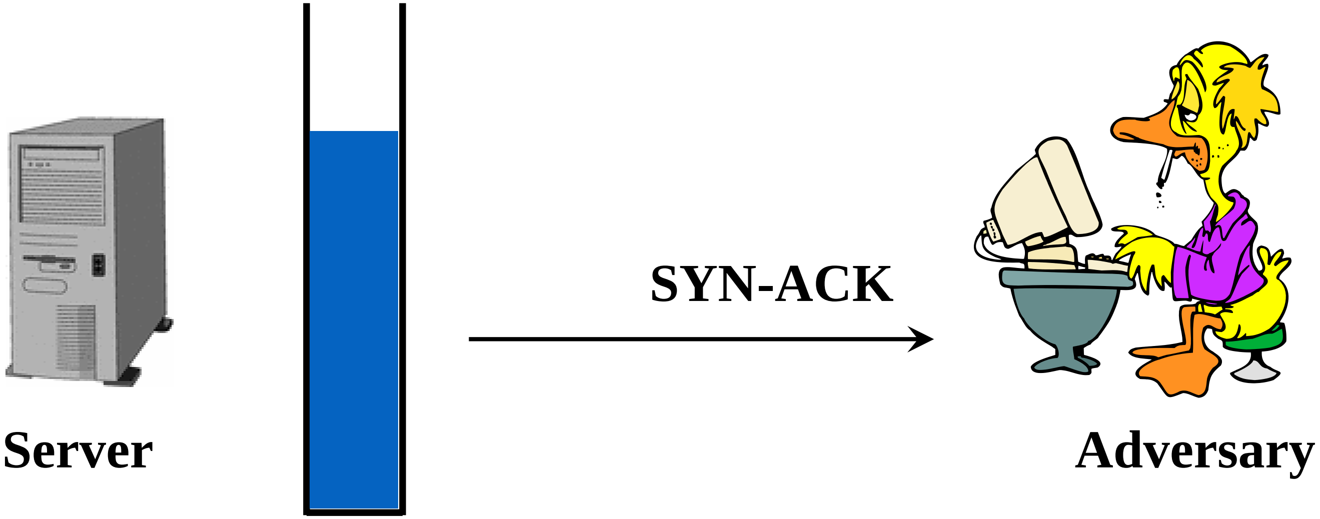


SYN

Server

Adversary

Syn-flooding !

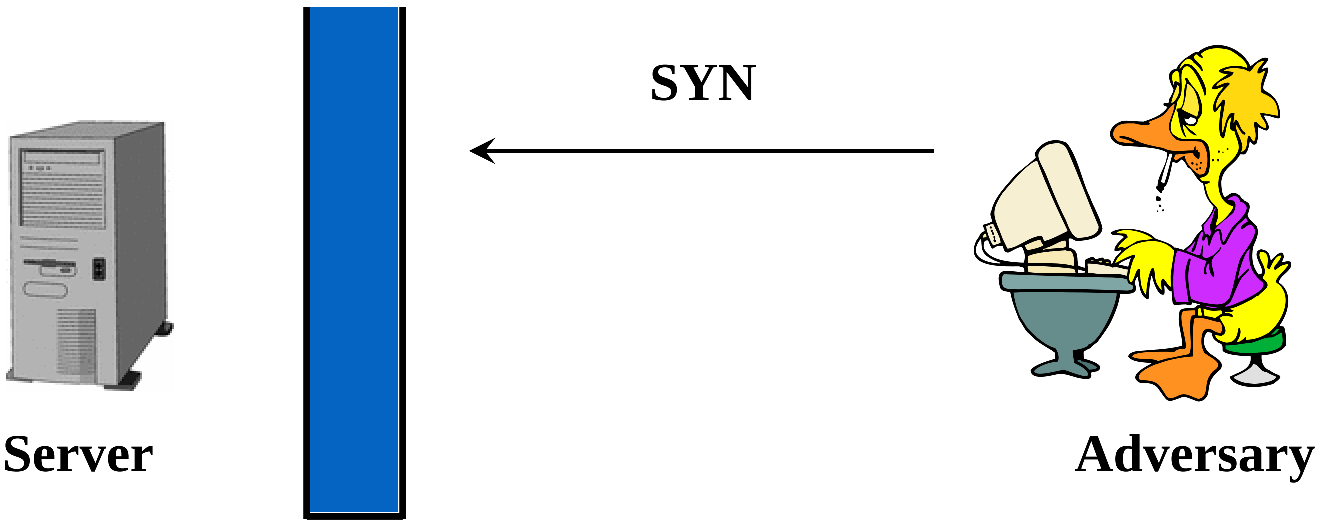


SYN-ACK

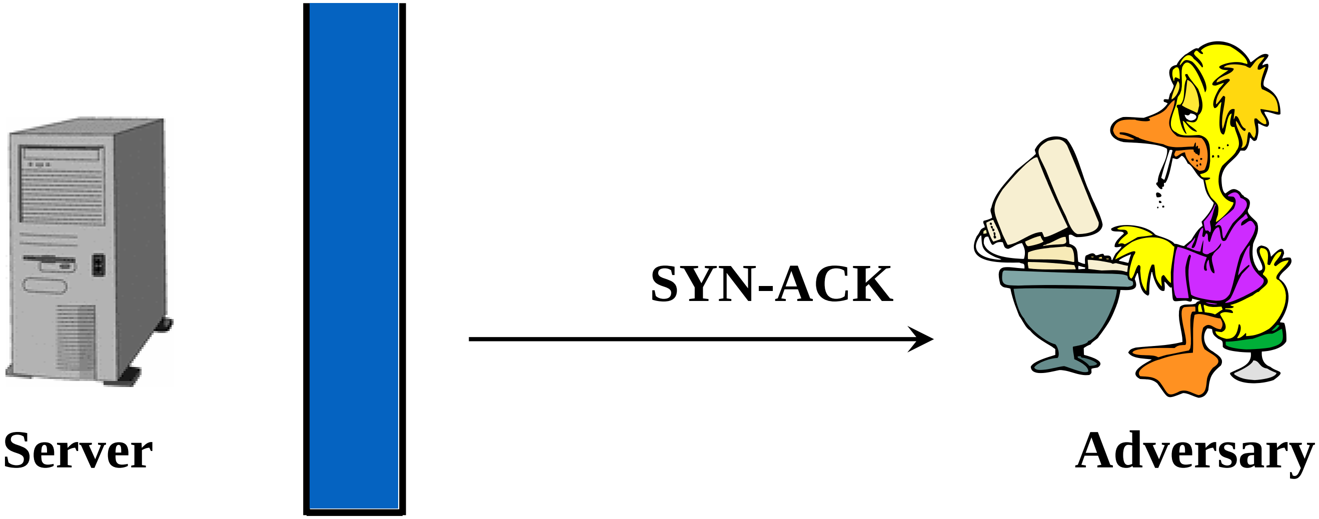
Server

Adversary

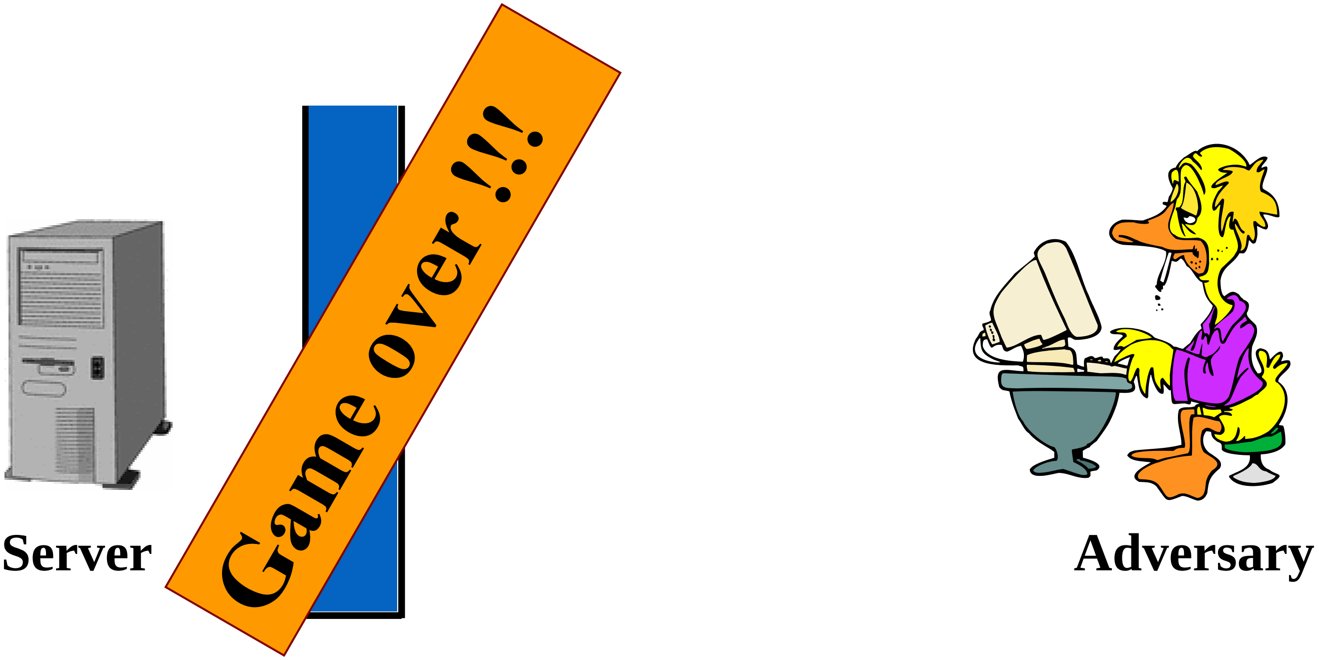
Syn-flooding !



Syn-flooding !



Syn-flooding !



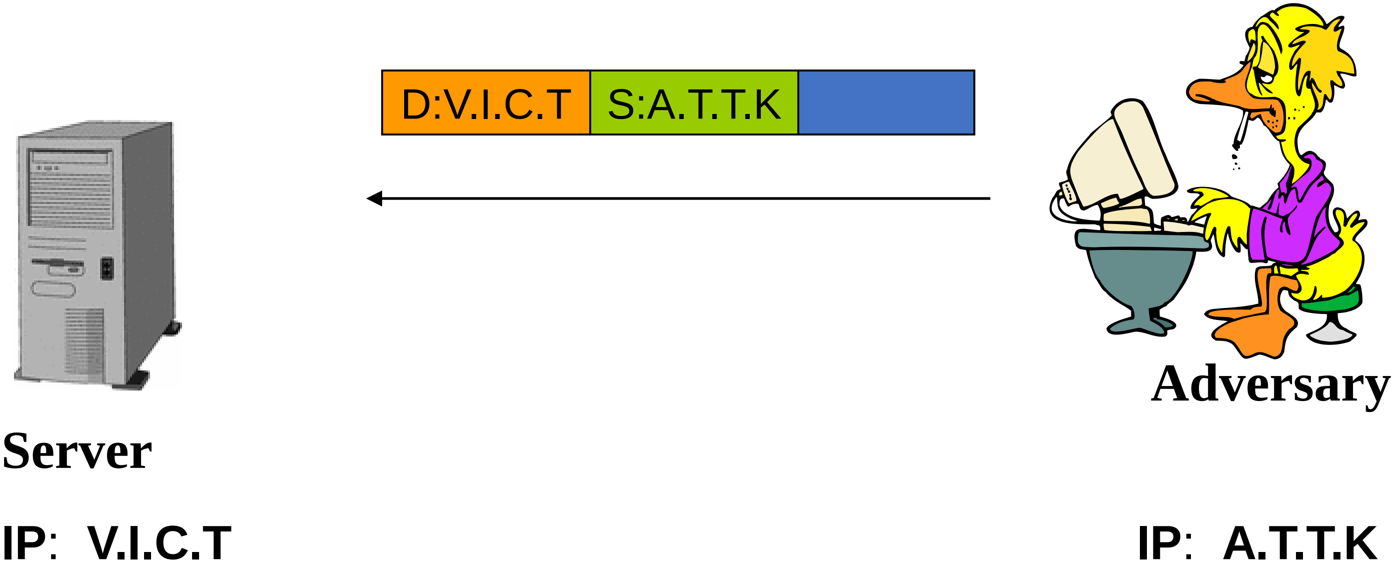
Server

Game over !!!

Adversary

IP spoofing and DoS attacks

- If the attacker uses the real IP to attack the server, he will be captured easily
- How about using someone else's? This is easy on the Internet



D:V.I.C.T | S:A.T.T.K

Adversary

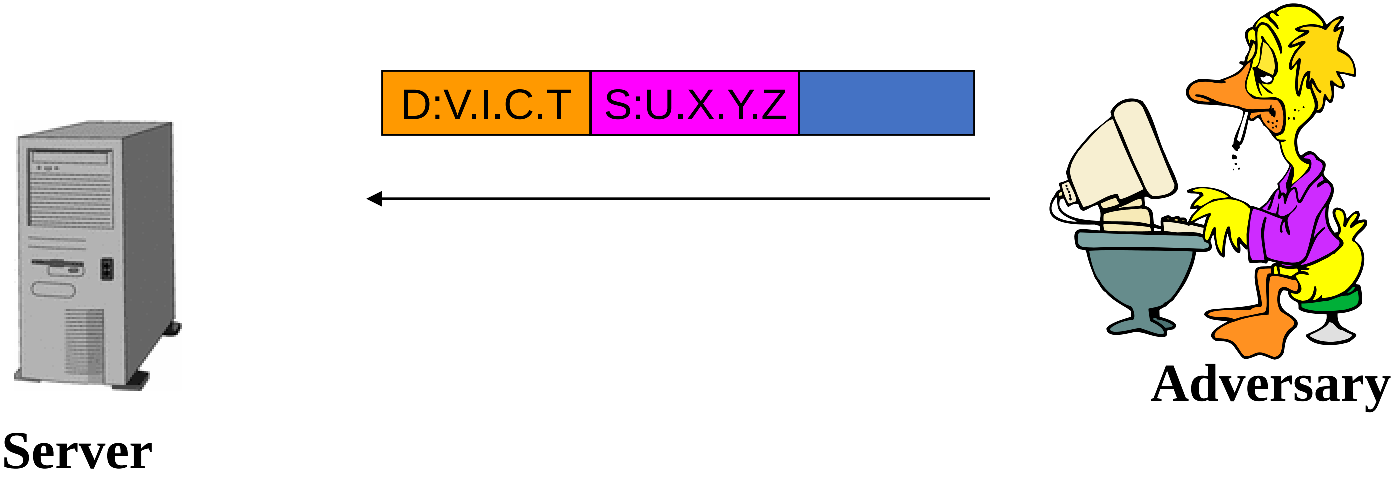
Server

IP: V.I.C.T

IP: A.T.T.K

IP spoofing and DoS attacks

- If the attacker uses the real IP to attack the server, he will be captured easily
- How about using someone else's? This is easy on the Internet



D:V.I.C.T	S:U.X.Y.Z	

Server

Adversary

IP: **V.I.C.T**

IP: **A.T.T.K**

Getting a spoofed IP address

- ➢ Fully random IP addresses
  - Some could be exotic and unroutable
  - Most could be valid
- ➢ Subnet spoofing
  - Spoof the IP of the computer in the same sub-net could evade egress filtering
- ➢ Spoofing the victim’s IP
  - This leads to the reflection attacks

Why is IP spoofing Challenging?

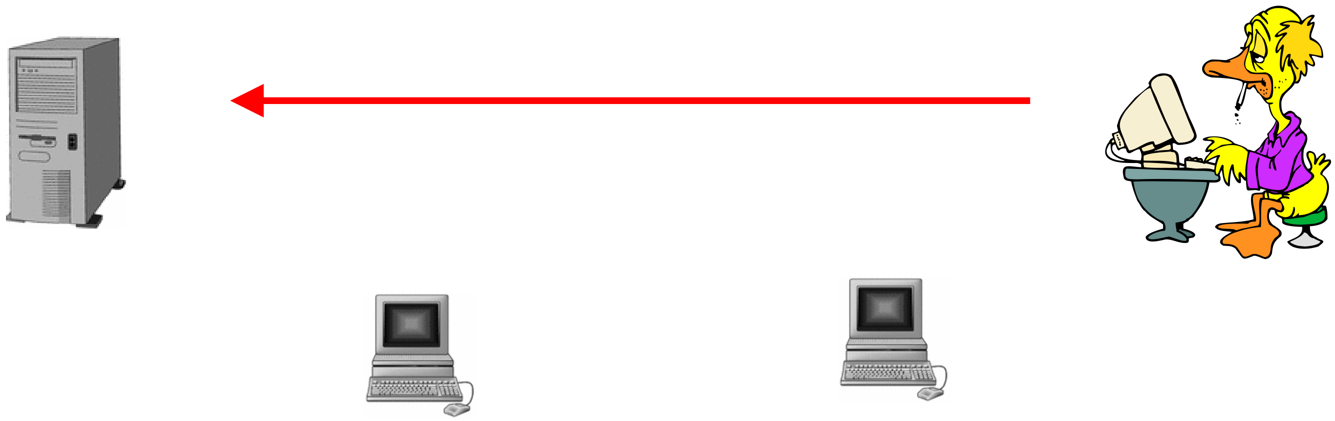
- Whoever accessible to network socket is able to spoof IP

- The most effective defense is egress filtering
  - Edge routers of a network only allow the packets with source IP in that network to leave
  - E.g, in a network 192.168.1.0/24, only IP between 192.168.1.1 and 192.168.1.254 are valid

- However, a network has little incentive to do egress filtering
  - Require extra network administration
  - May break mobile IP support
  - Your security expense is used to only protect OTHERS' security!!!

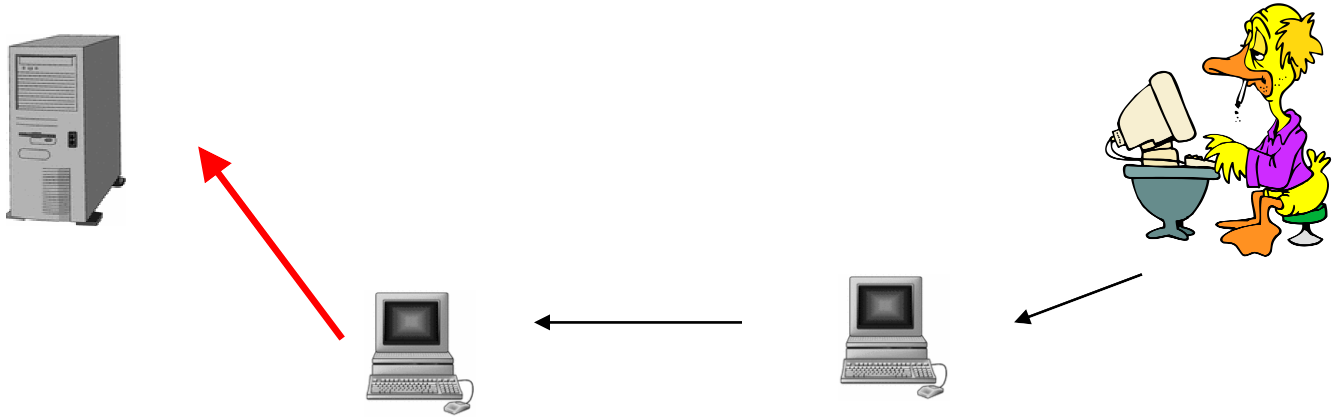
DoS on IP: bandwidth exhaustion attacks

- Objective: saturating the victim’s bandwidth in a brute-force fashion
- Strategies
  - Control of a large number of hosts, called zombies
  - Can be easily launched using DDoS tools
  - A multiple stepping-stone approach

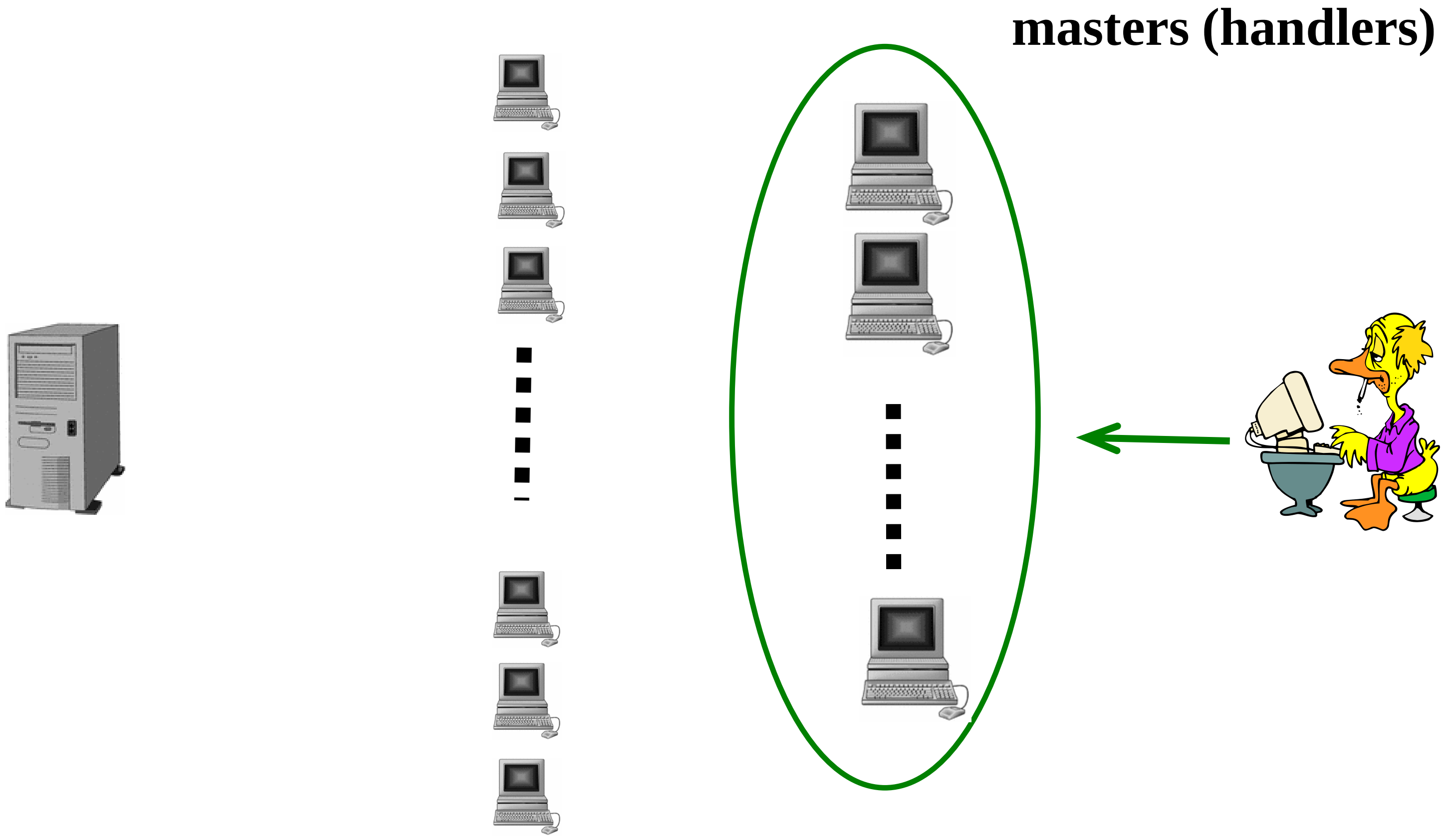


DoS on IP: bandwidth exhaustion attacks

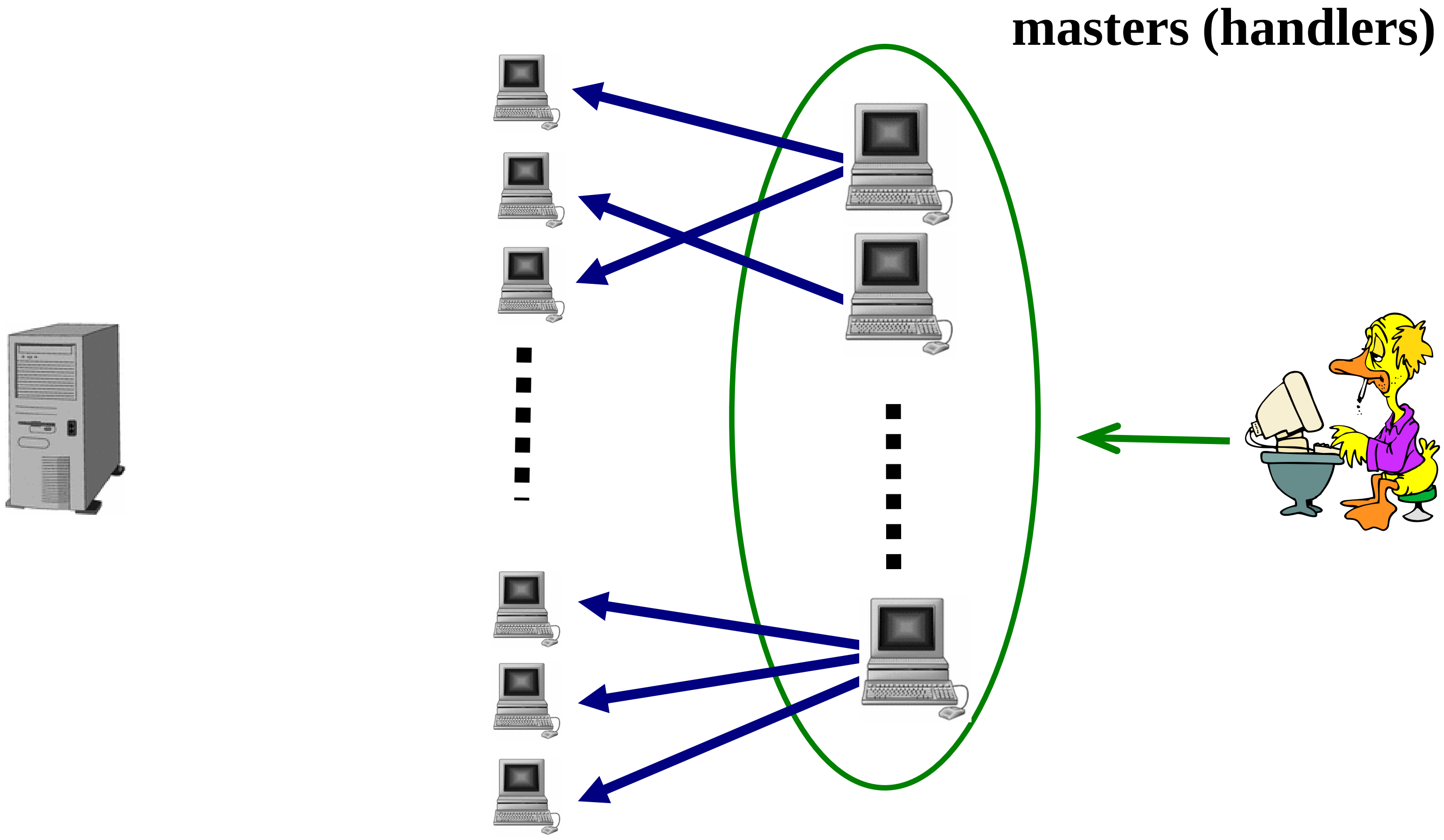
- Objective: saturating the victim’s bandwidth in a brute-force fashion
- Strategies
  - Control of a large number of hosts, called zombies
  - Can be easily launched using DDoS tools
  - A multiple stepping-stone approach



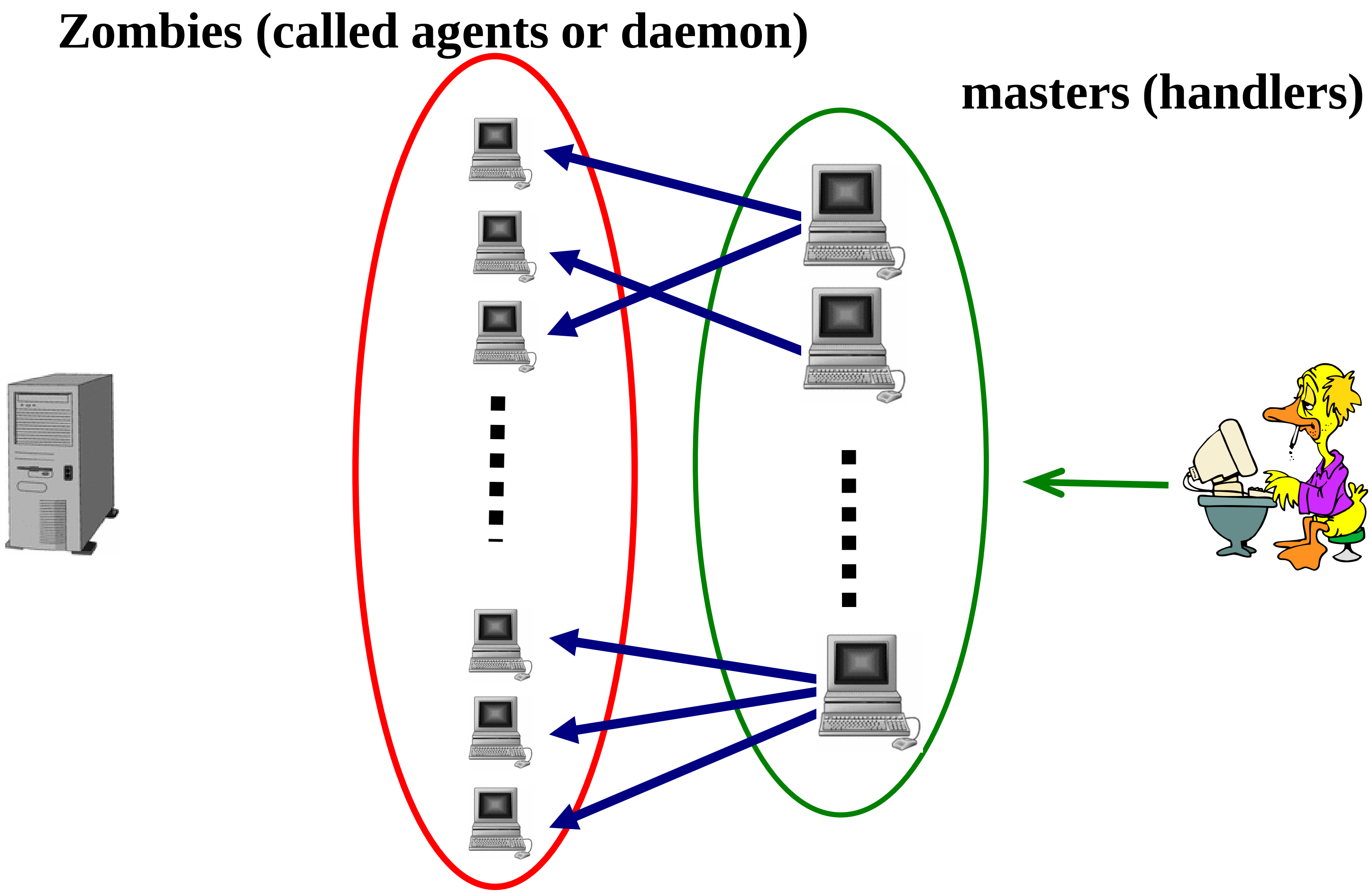
A typical DDoS attack on bandwidth



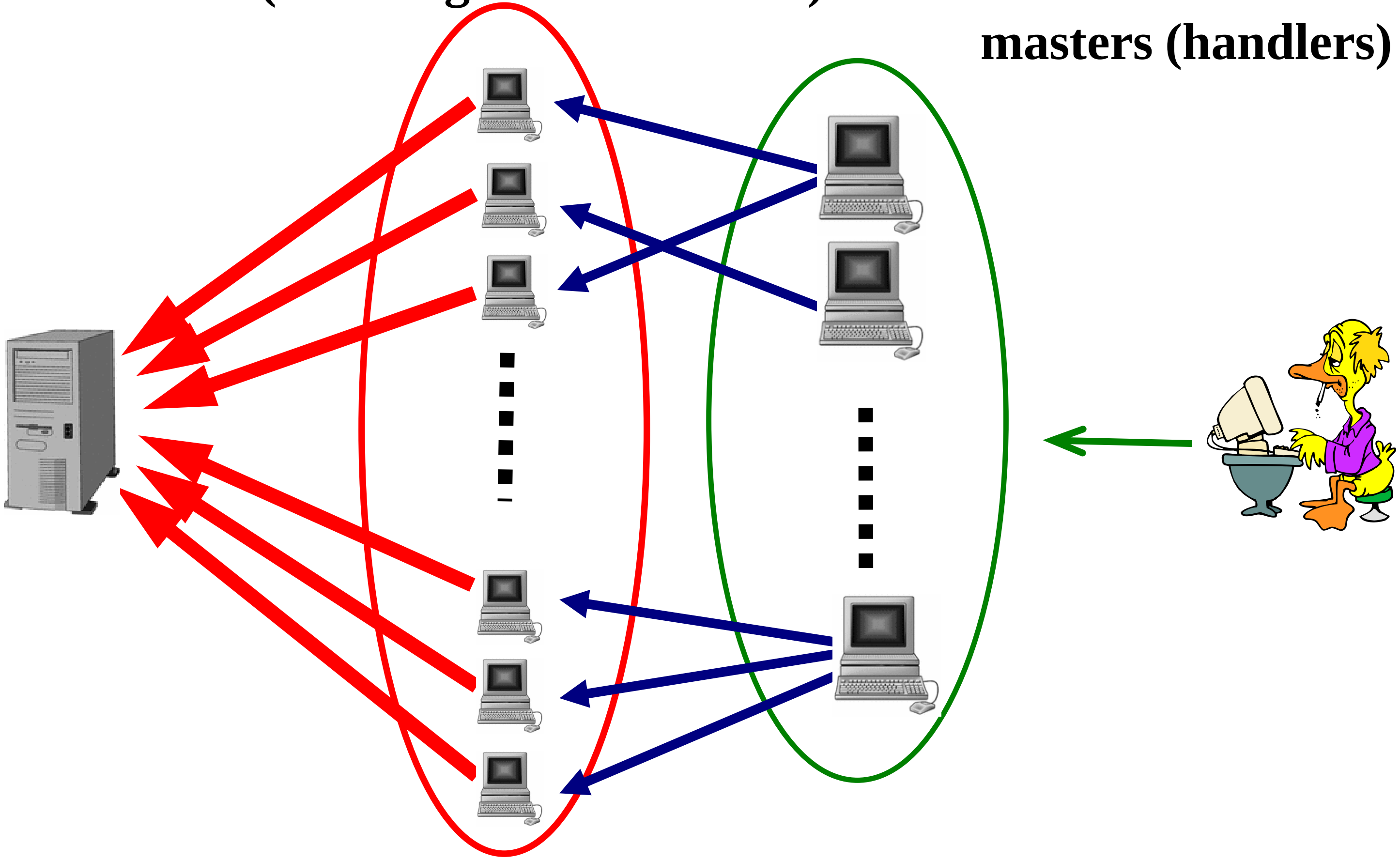
A typical DDoS attack on bandwidth



A typical DDoS attack on bandwidth



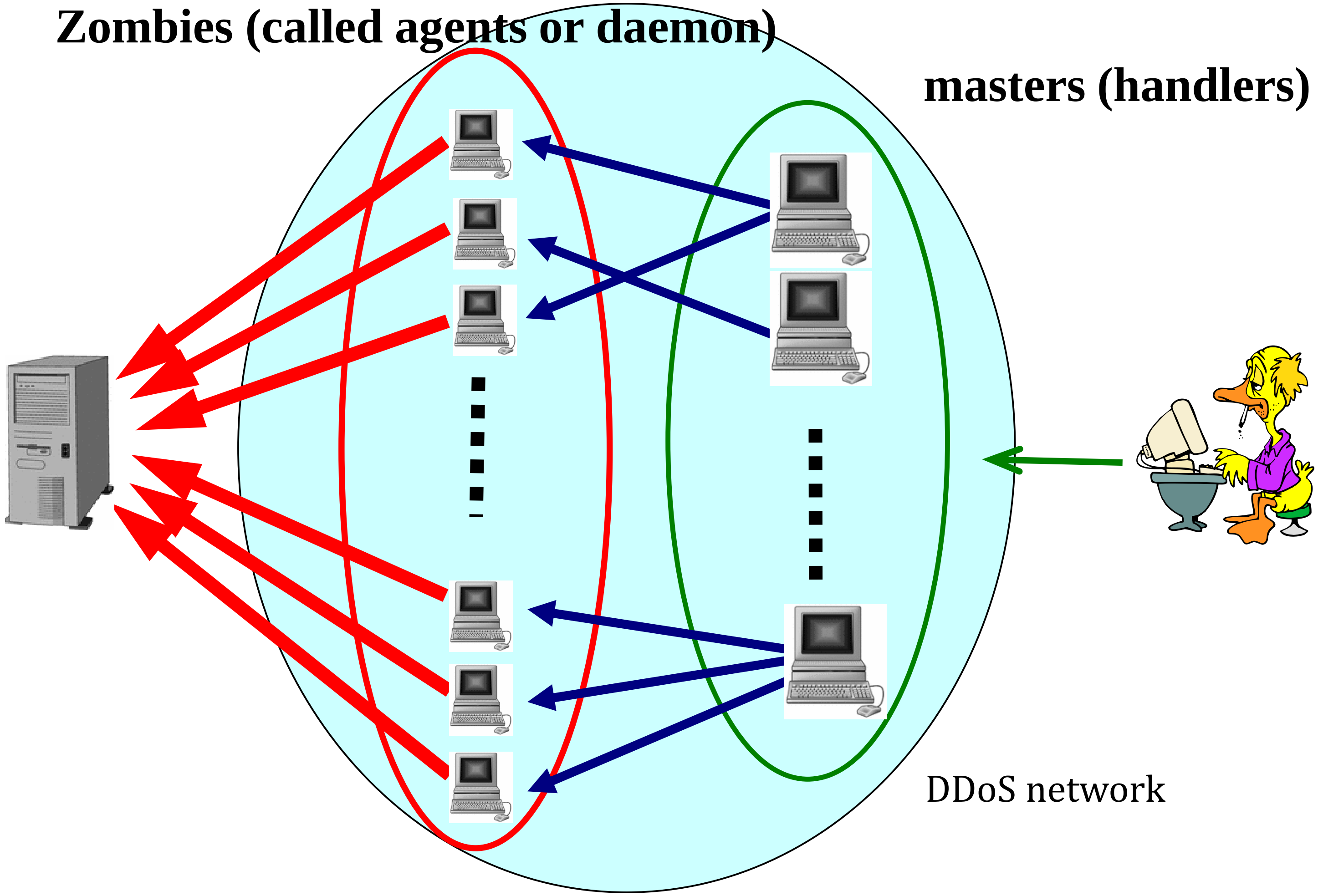
A typical DDoS attack on bandwidth



Zombies (called agents or daemon)

masters (handlers)

A typical DDoS attack on bandwidth



Zombies (called agents or daemon)

masters (handlers)

DDoS network

DDoS attack tools

➢Trinoo

- Attacker : tcp(27665) → master : udp(27444) ↔ agent : udp(31335)
- Handler and agents are protected by passwords
- Udp based flooding

➢Tribe Flood Network (TFN) and TFN2K

- Attacker: tcp (all kinds of application, including ssh)→ master: icmp echo (ping) ↔ agent
- The ICMP packets are encoded
- Udp flooding, TCP syn flooding, icmp echo flooding and smurf attacks
- TFN2K offers more sophisticated mechanisms to hide structure of attack network, including decoy messages, spoofed IP, etc

DDoS attack tools (cont’d)

- Stacheldraht (German for “barbed wire”)
  - Combining features of trinoo and TFN
  - The communication between attackers and handlers is encrypted
  - Attacking code on agents can be automatically updated

- Shaft
  - Shared properties of all above attack tools
  - Can dynamically switch port numbers to evade detection
  - Can link transactions and do packet statistics

DDoS attack tools (cont’d)

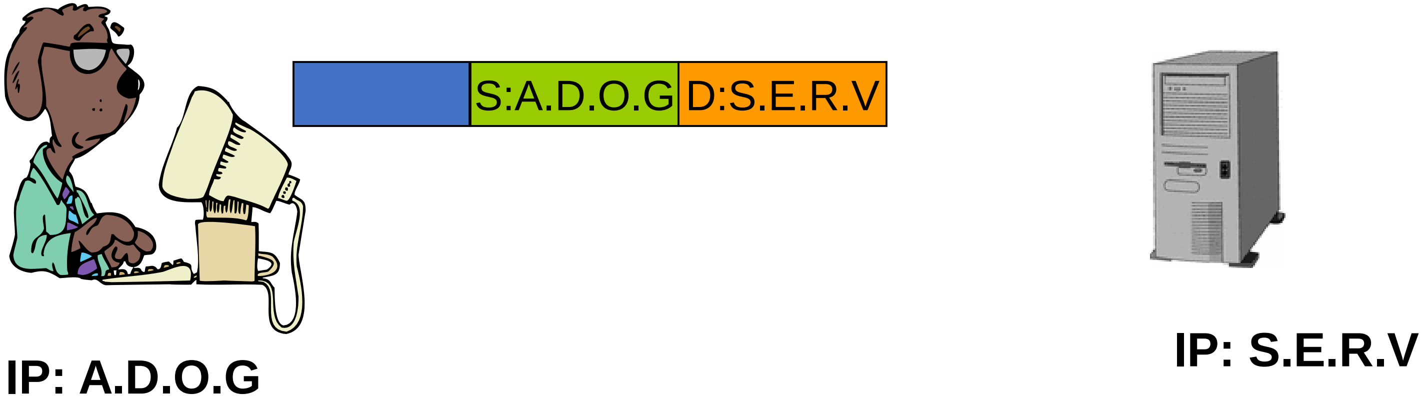
- Mstream
  - Can be controlled by multiple attackers
  - Using TCP ack flooding to saturate links

- Trinity
  - The first IRC based DDoS tool
  - All handlers can be summoned to an Internet Chat room to organize attacks

- DDoS “Swiss army knifes”--- Agobot and Phatbot
  - The fashion of 2003/2004
  - Combination of multiple known DDoS attacks, on IP and TCP
  - Can simulate legitimate traffics

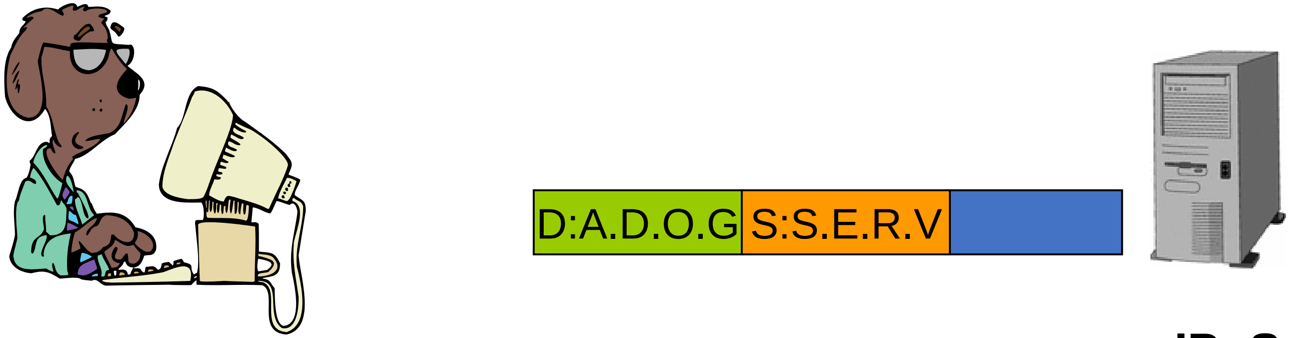
Flooding without a zombie army

- Ping (icmp echo)



Flooding without a zombie army

- Ping (icmp echo)

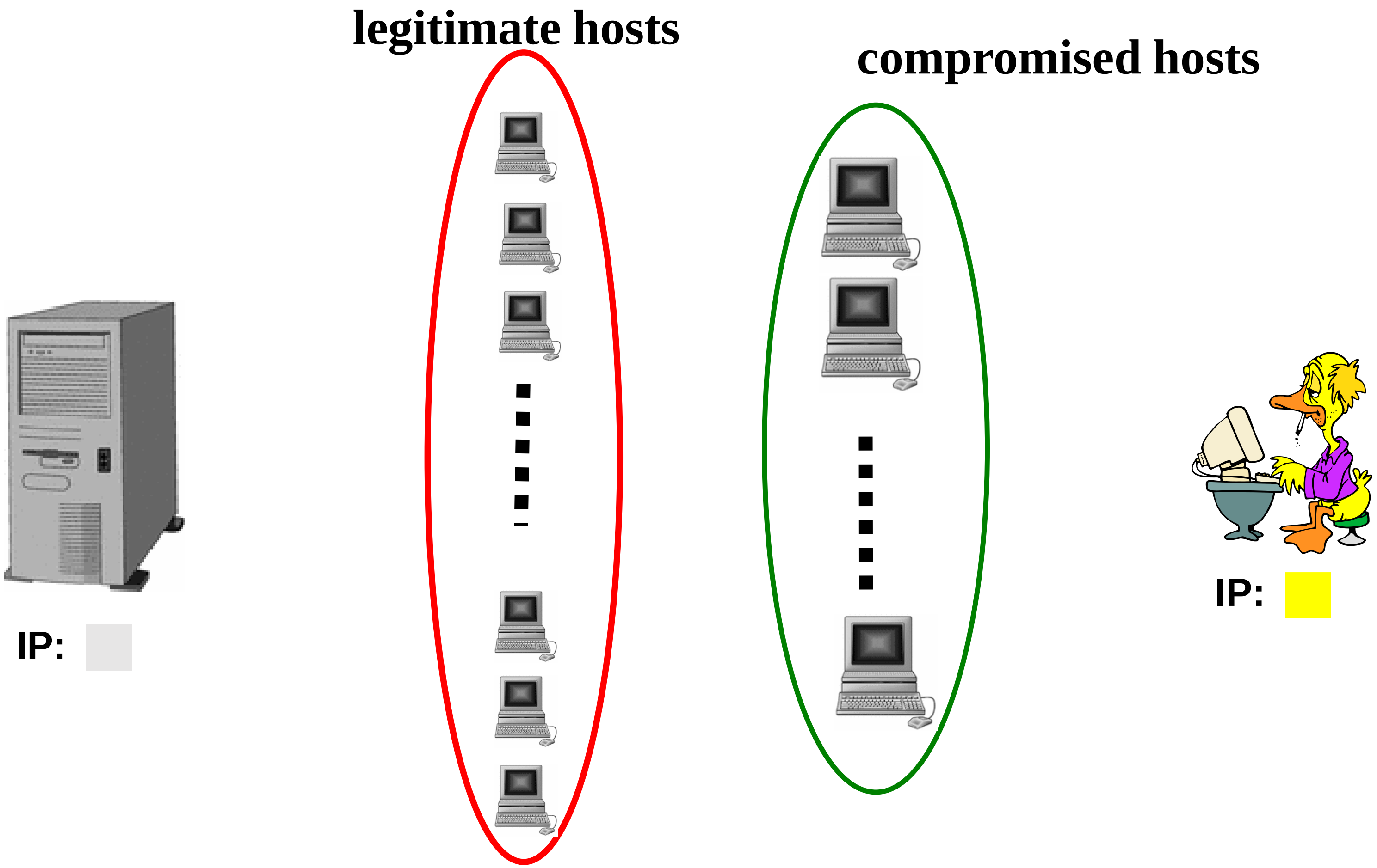


D:A.D.O.G S:S.E.R.V

IP: A.D.O.G

IP: S.E.R.V

Reflection flooding



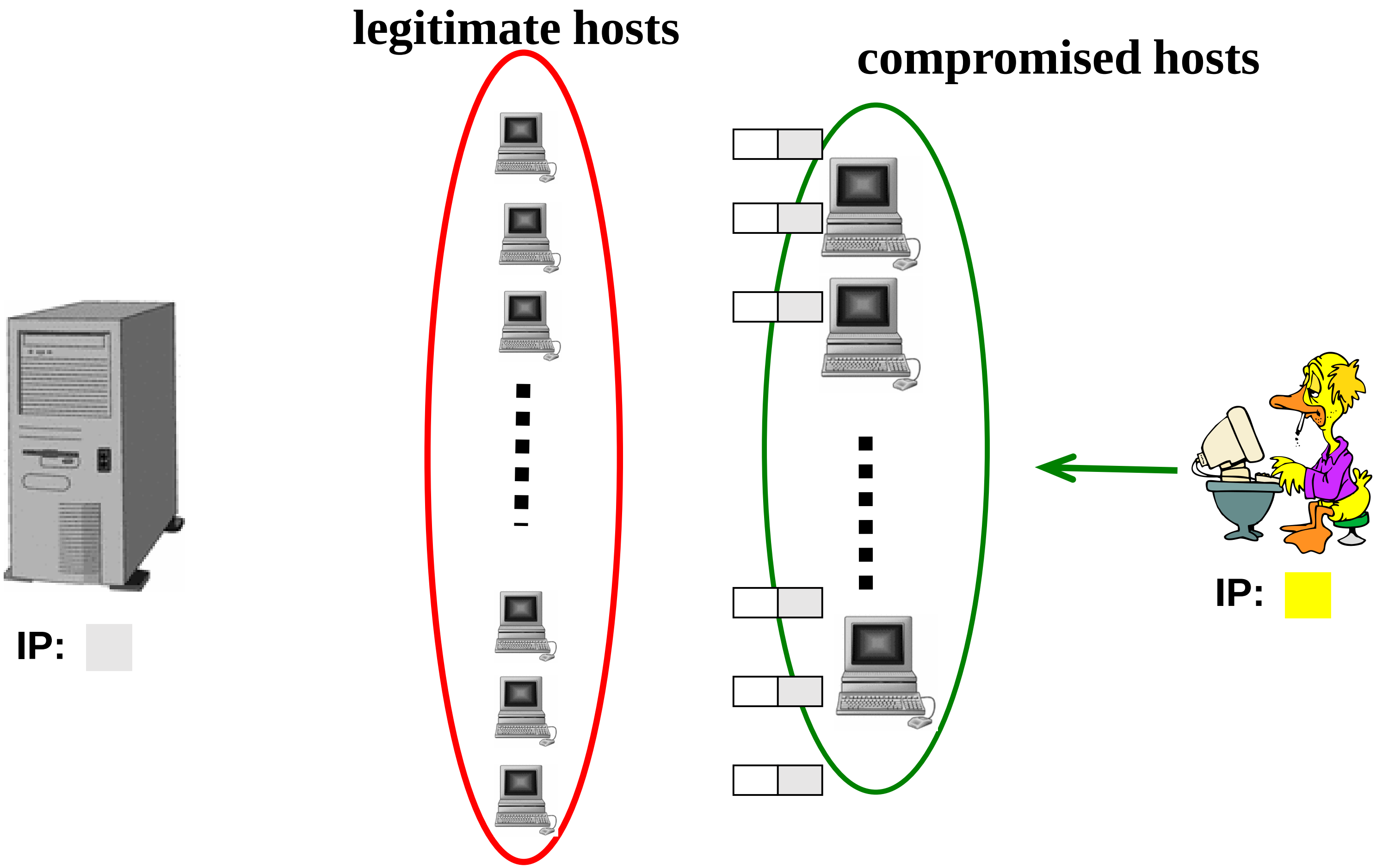
legitimate hosts

compromised hosts

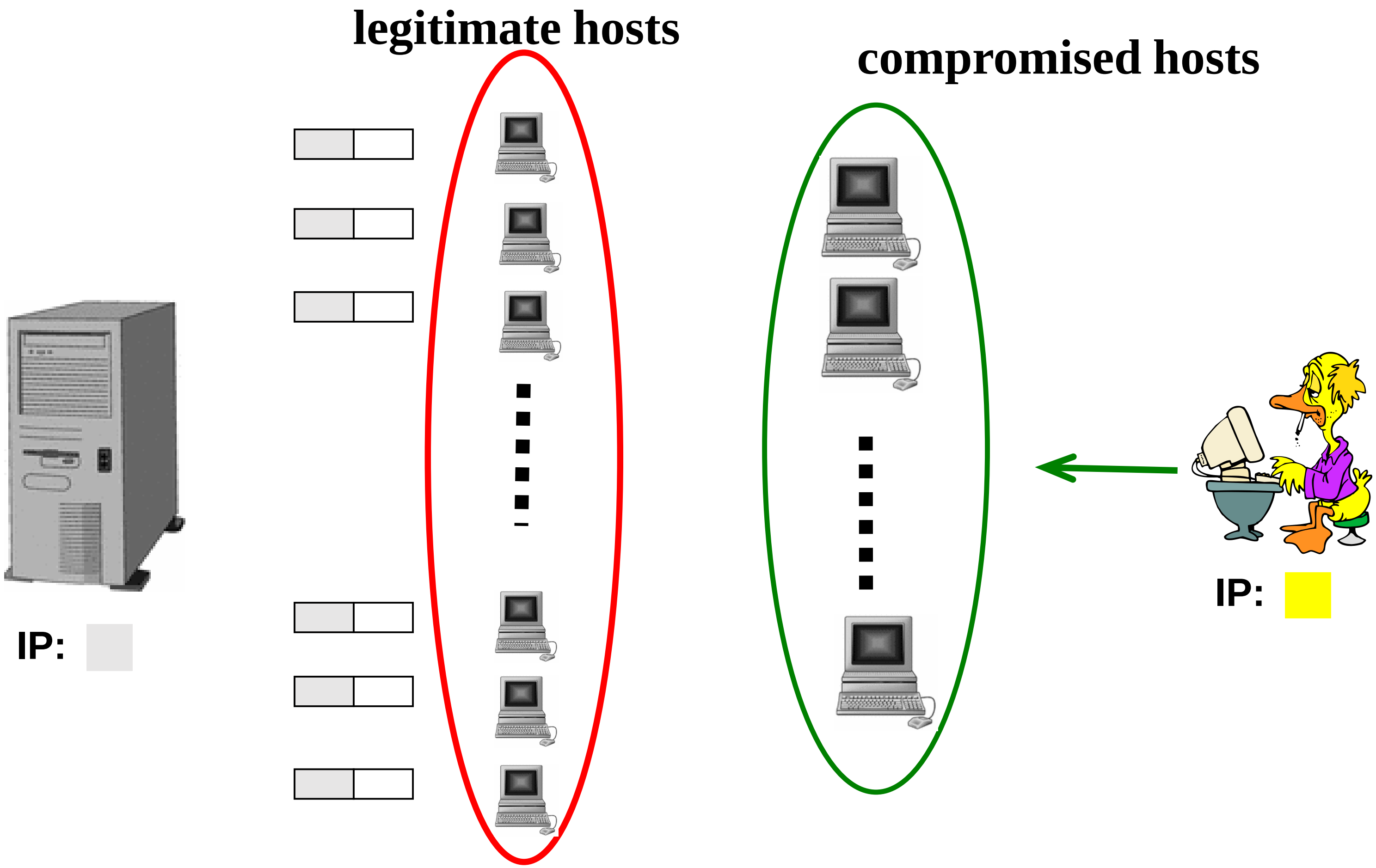
IP: ⬜

IP: 🟨

Reflection flooding

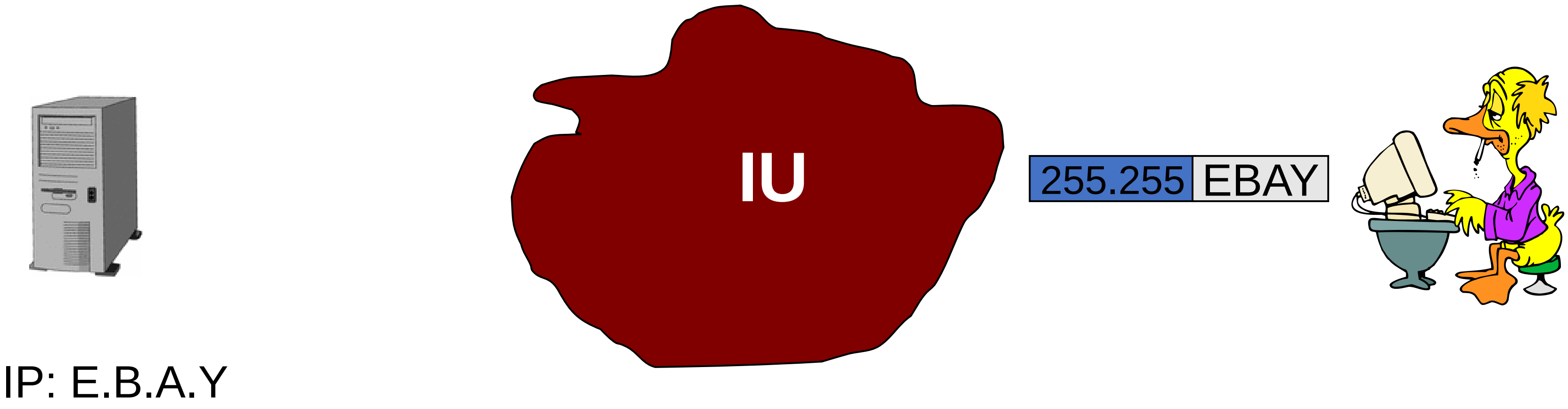


Reflection flooding



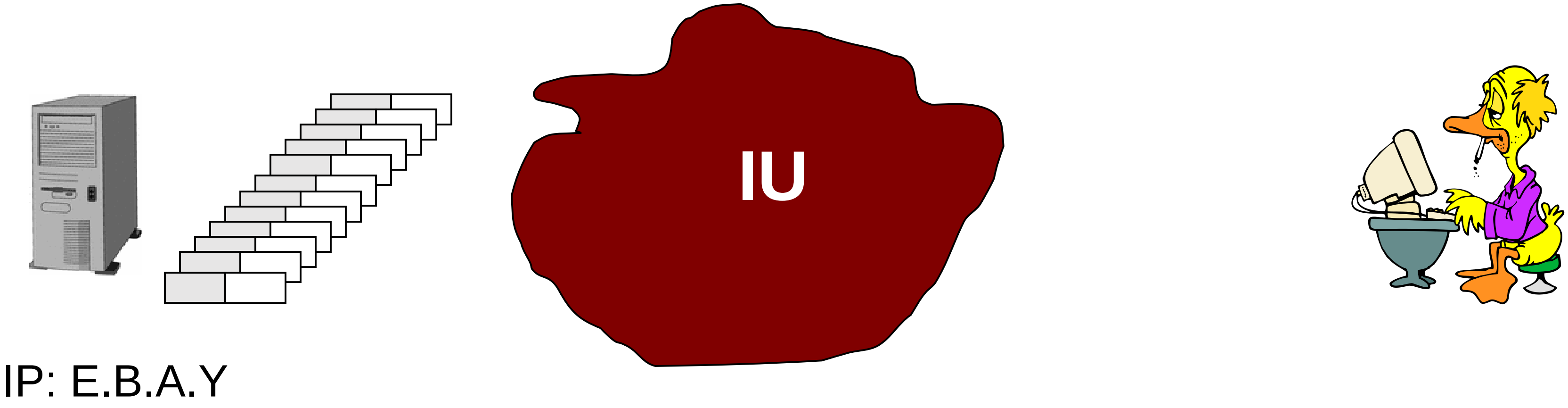
Smurf flooding

- Reflection attacks using broadcast address
  - For a /*n* network, the broadcast address is the one which has *n* 1s on the least important part, e.g, IU's broadcast address: 156.56.255.255
  - A message to the broadcast address of a network is forwarded to ALL computers in that network



Smurf flooding

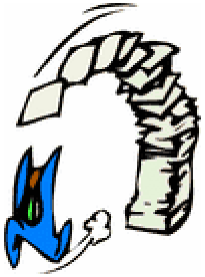
- Reflection attacks using broadcast address
  - For a /*n* network, the broadcast address is the one which has *n* 1s on the least important part, e.g, IU's broadcast address: 156.56.255.255
  - A message to the broadcast address of a network is forwarded to ALL computers in that network



DoS on application

- DoS on authentication server
  - Computation intensive operation: public key authentication
  - Attack: large number of junk messages →exhaustion of cpu cycles

- SPAM
  - Squandering mailbox space, human energy
  - About 2/3 spam from zombies (CNN)
  - SPAM virus: SoBig



Denial of Service

- Defense

DoS defense

- Attacks exploiting software vulnerability
    - Defense: software engineering, patching

- Attacks on system configuration information
    - Defense: authentication

- Resource exhaustion (RE) DoS
    - Defense: difficult in an open system

What make RE DoS possible?

- Limited resources

- Unlimited service requests

- Difficulty to tell good and bad requests apart

plausible when attackers control many zombies

Defending against RE DoS

➢ Acquiring more resources
  - Content distribution networks, such as Akamai

➢ Limiting service requests
  - Rate limiting/push back
  - Puzzles

➢ Identifying good or bad requests
  - Identifying bad traffic: Intrusion detection, IP traceback, D-WARD, etc
  - Identifying good traffic: Capability token, Secure Overlay Systems, etc

DoS defense

⇒Acquiring more resources

➢Limiting service requests

➢Identifying good/bad requests

Vulnerability of an open system

- Resources: limited
- Control: centralized
- Access: global

From Bruce Maggs's slides

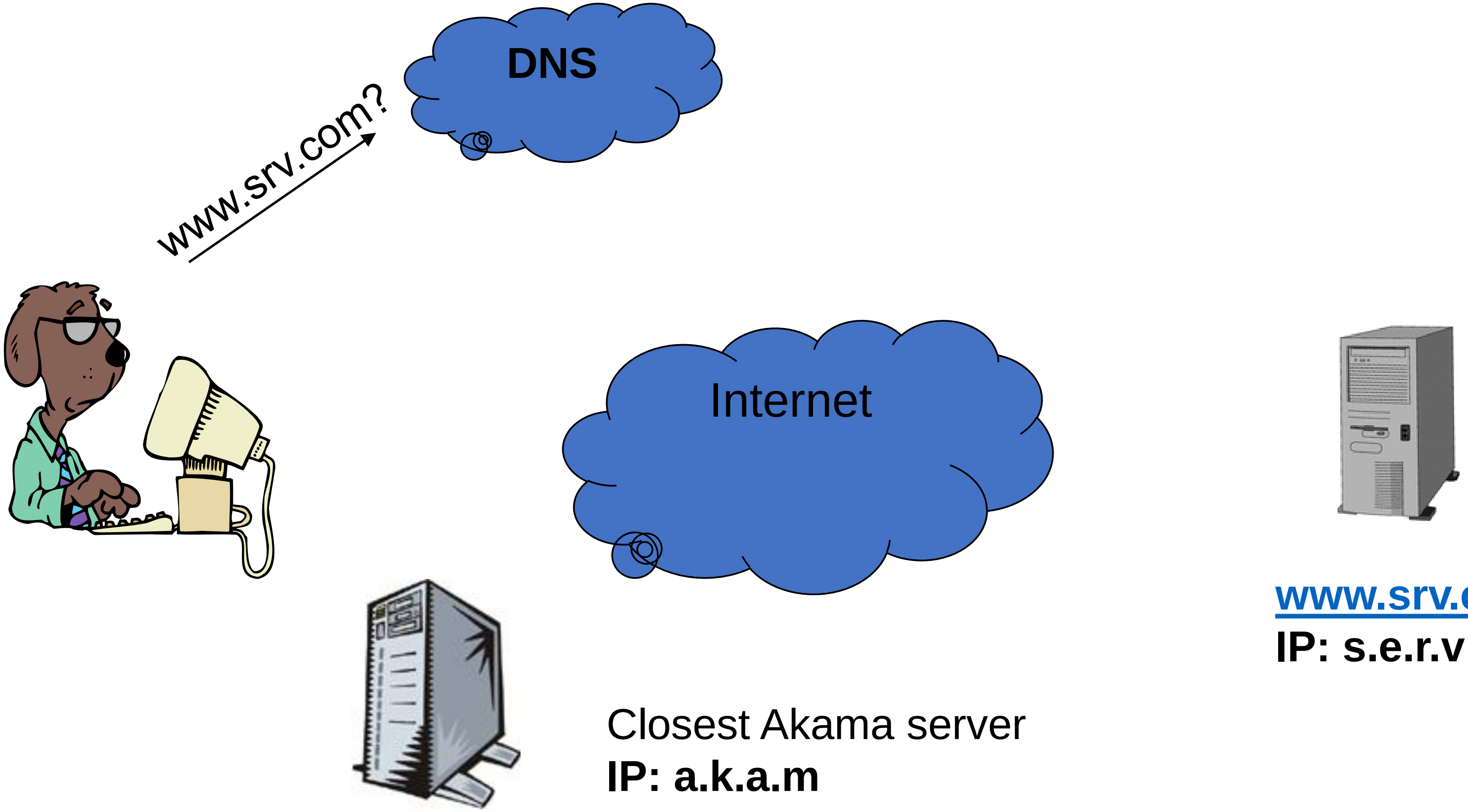
Content distribution network: Akamai

- Content provider delegates its service to Akamai

- What Akamai does
  - deploys servers wherever there are clients
  - Direct clients to “nearby” servers
  - Monitor the Internet and route around trouble spots

From Bruce Maggs’s slides

Downloading objects using Akamai



DNS

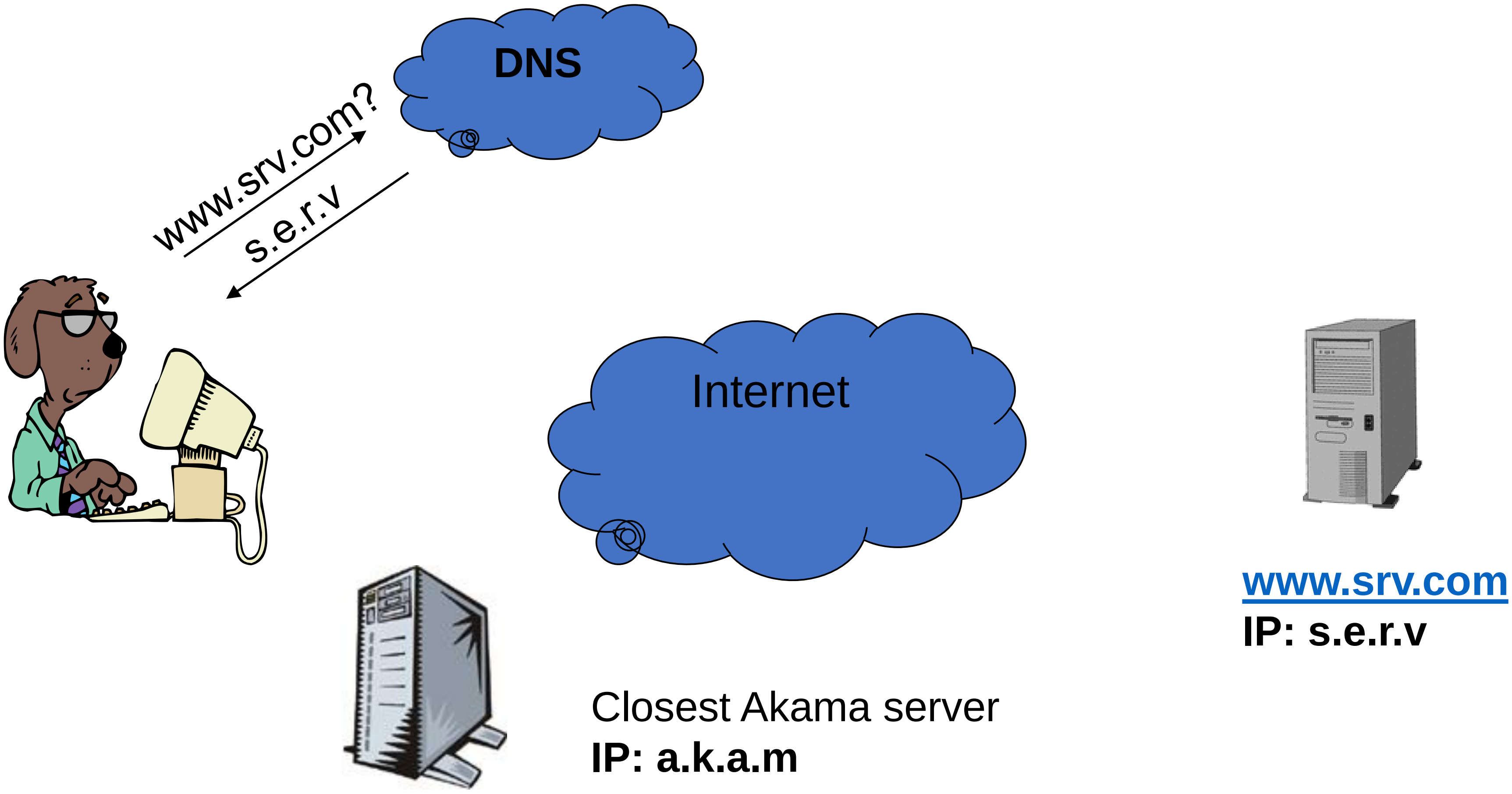
www.srv.com?

Internet

www.srv.com
IP: s.e.r.v

Closest Akama server
IP: a.k.a.m

Downloading objects using Akamai



DNS

www.srv.com?

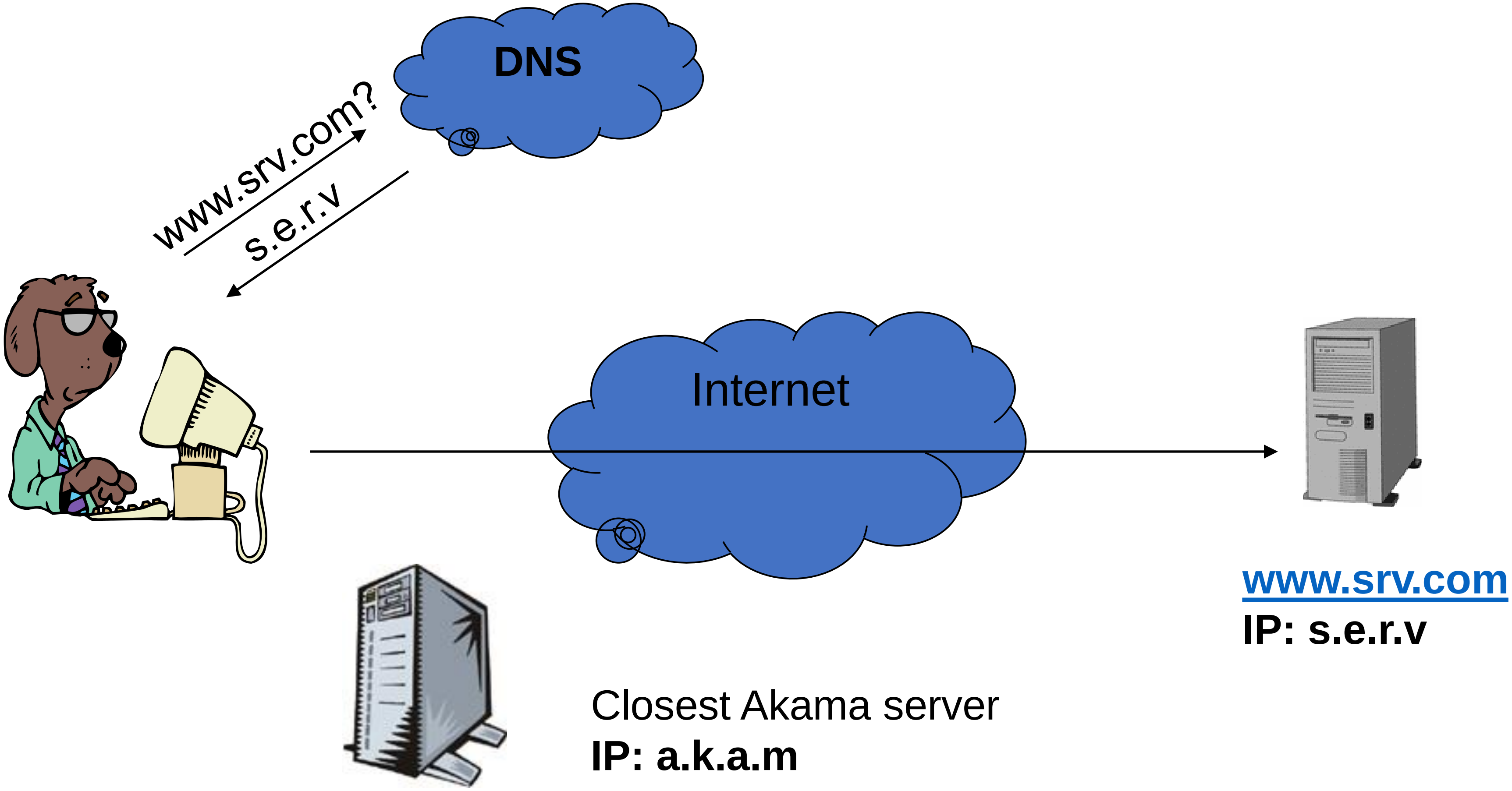
s.e.r.v

Internet

www.srv.com
IP: s.e.r.v

Closest Akama server
IP: a.k.a.m

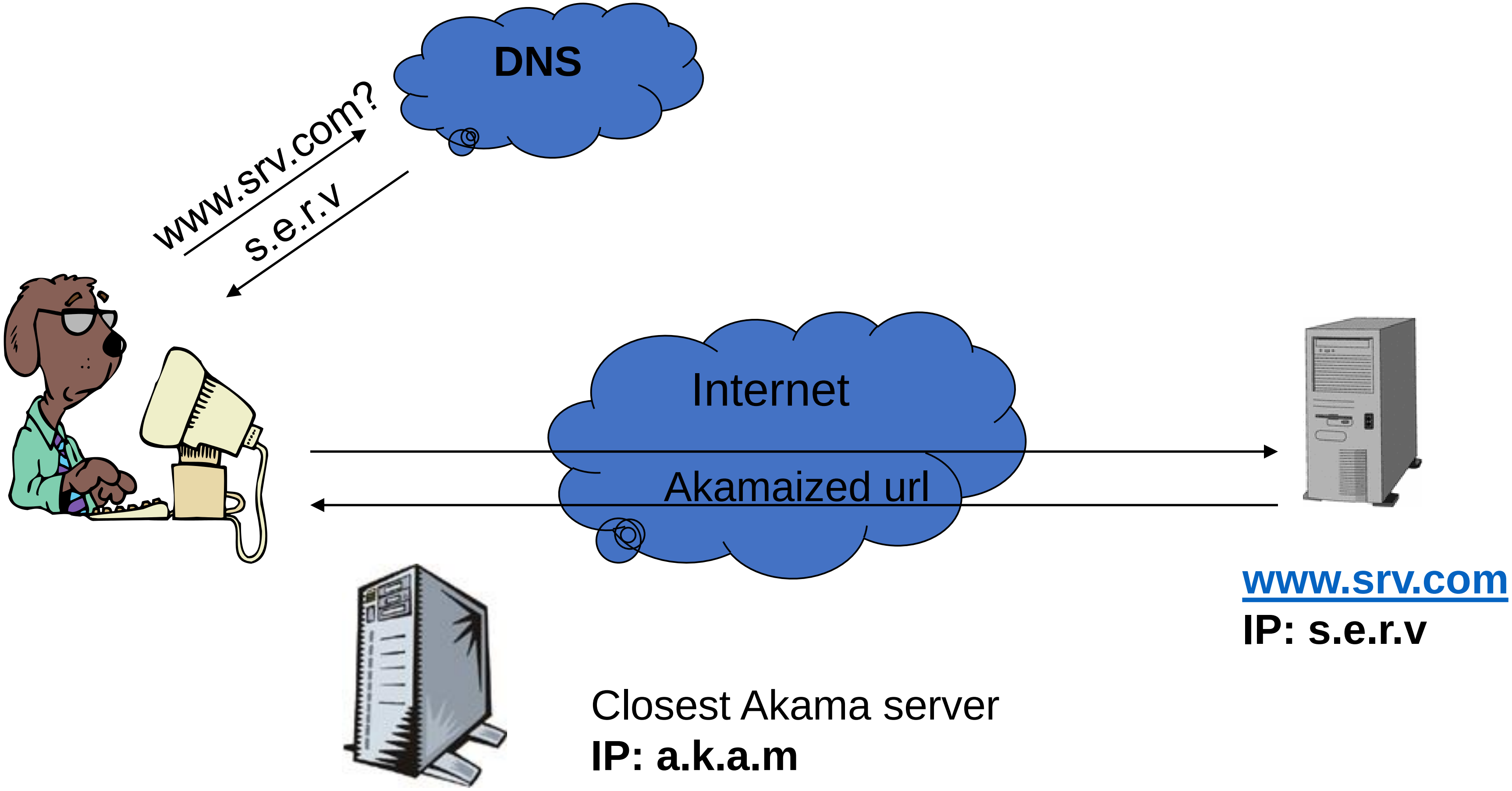
Downloading objects using Akamai



www.srv.com
IP: s.e.r.v

Closest Akama server
IP: a.k.a.m

Downloading objects using Akamai



DNS

www.srv.com?

s.e.r.v

Internet

Akamaized url

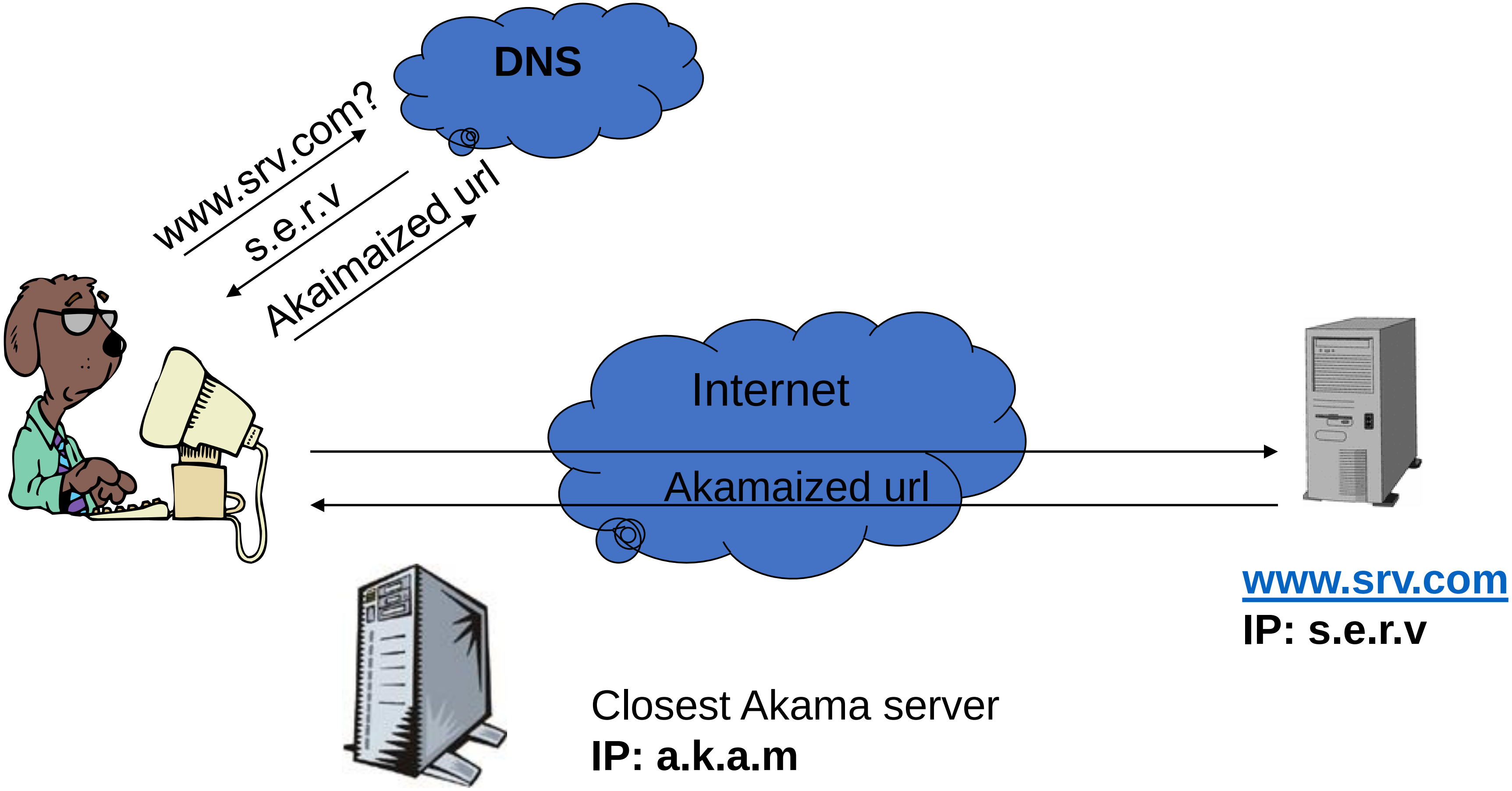
www.srv.com

IP: s.e.r.v

Closest Akama server

IP: a.k.a.m

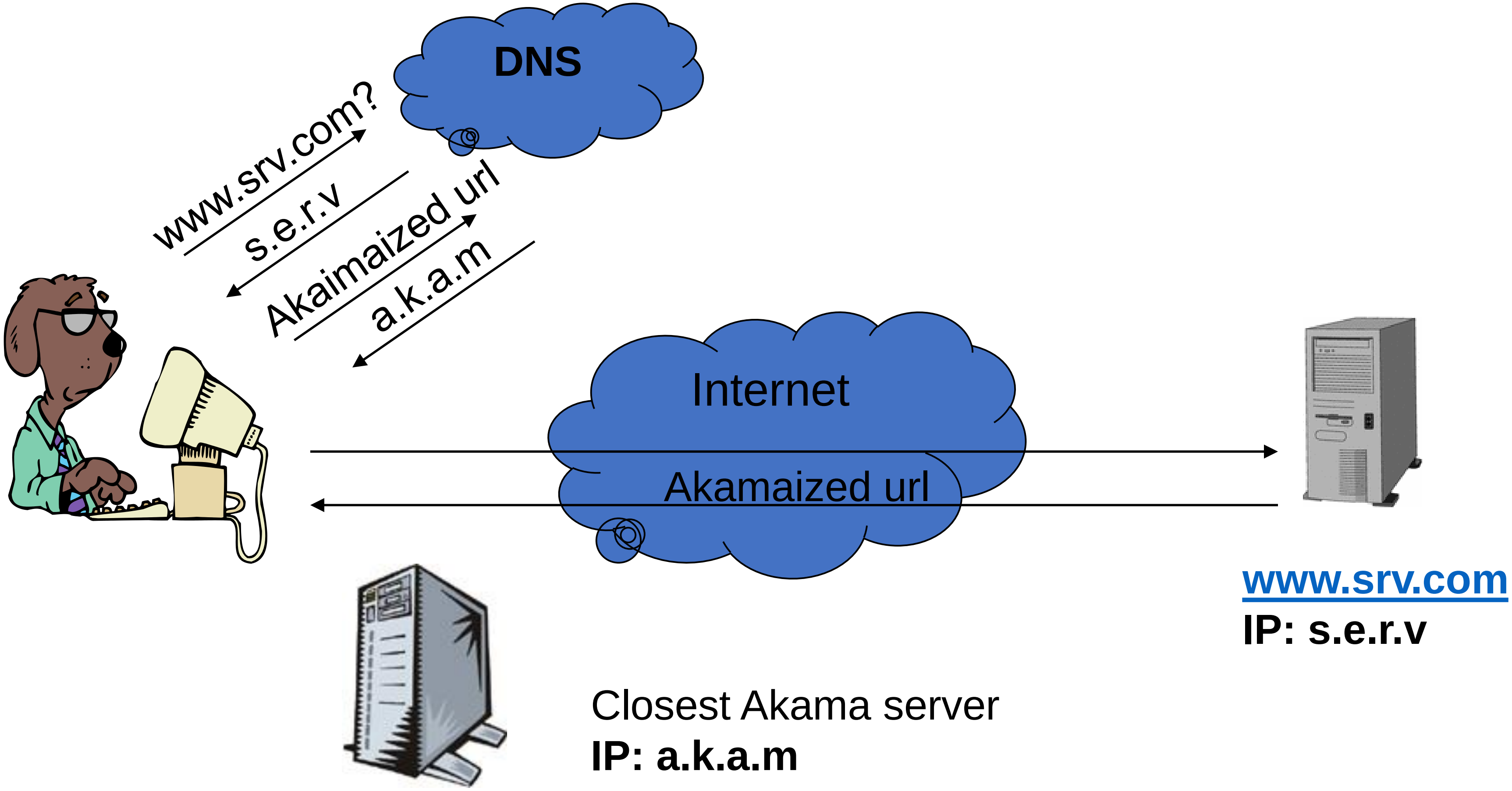
Downloading objects using Akamai



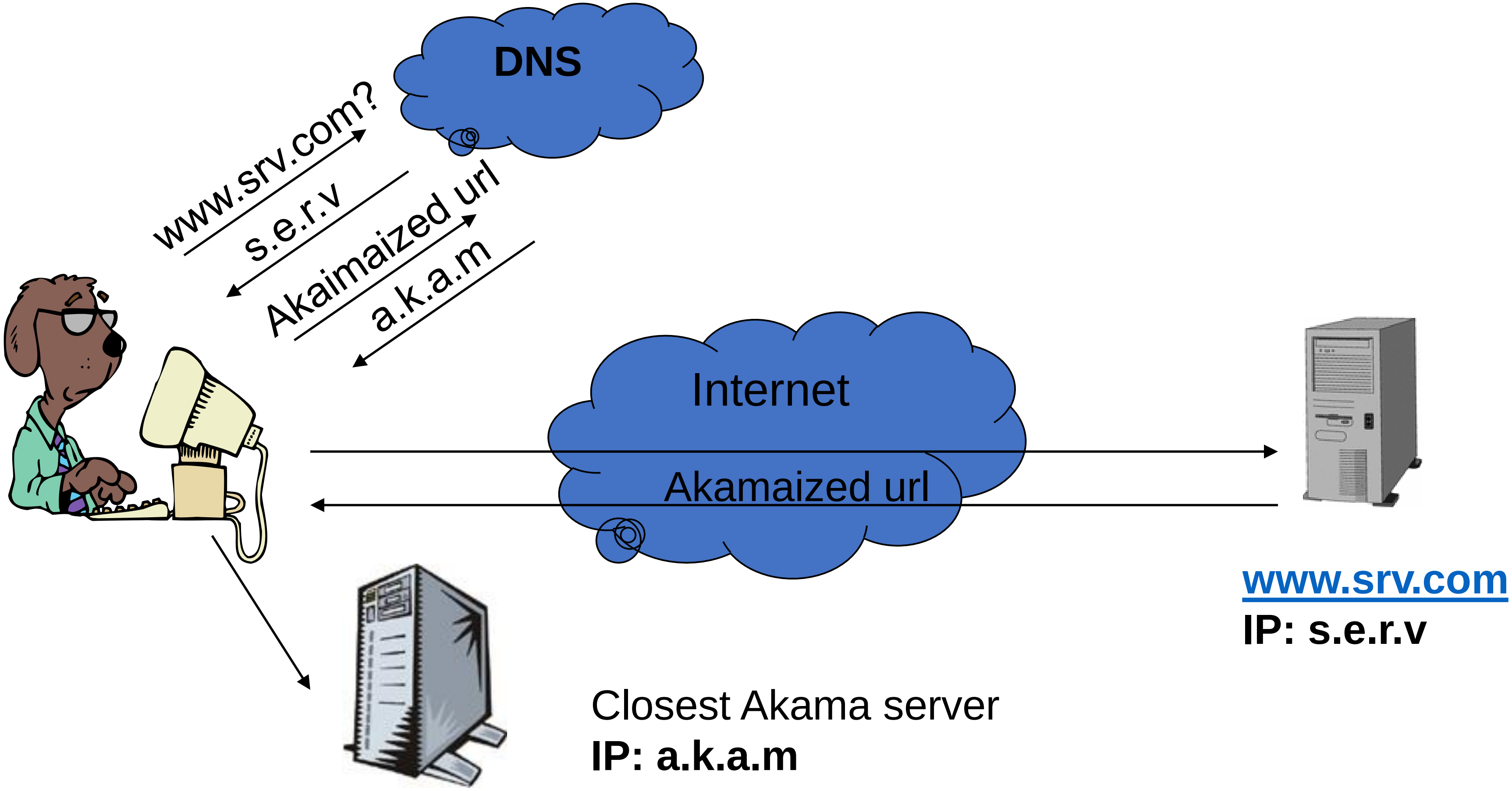
www.srv.com
IP: s.e.r.v

Closest Akama server
IP: a.k.a.m

Downloading objects using Akamai



Downloading objects using Akamai



DNS

www.srv.com?

s.e.r.v

Akaimaized url

a.k.a.m

Internet

Akamaized url

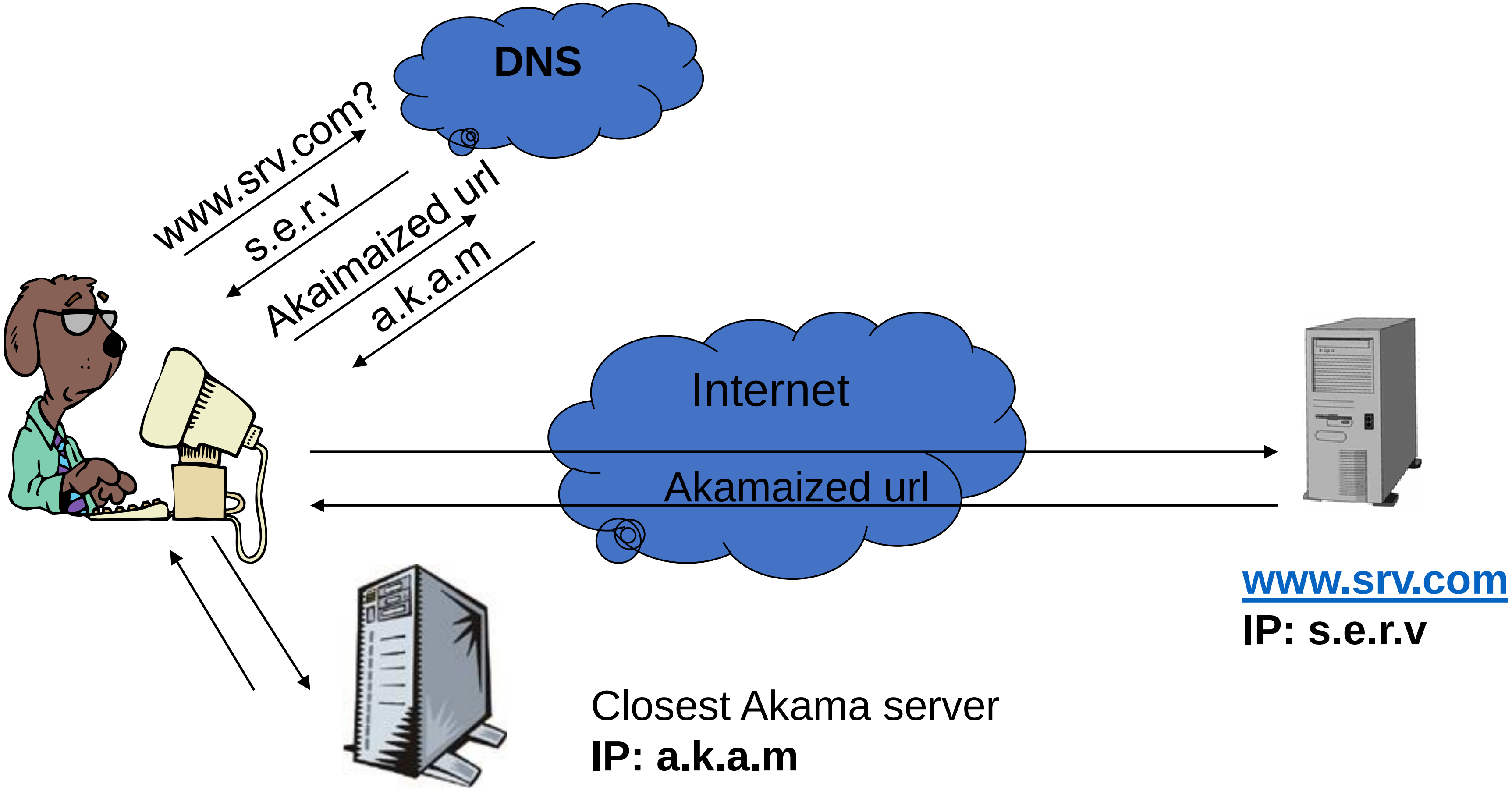
www.srv.com

IP: s.e.r.v

Closest Akama server

IP: a.k.a.m

Downloading objects using Akamai



Scale of Akamai network

- They claim having
  - 15,000 servers
  - distributing over 1,000 networks
  - in 69 countries

- Most of the major websites, including CNN, Yahoo!, Microsoft, are their customers

Weaknesses of Akamai

- Limits in handling contents
  - Good for static contents, such as pictures
  - Insufficient for real-time, dynamic contents

- Scalability
  - Akamai itself is having scalability problem

- Not complete immunization to DDoS
  - Jun, 2004, Akamai was attacked by a DDoS with thousands of zombies
  - Its service to some customers was interrupted for 2 hours

DoS defense

➢Acquiring more resources

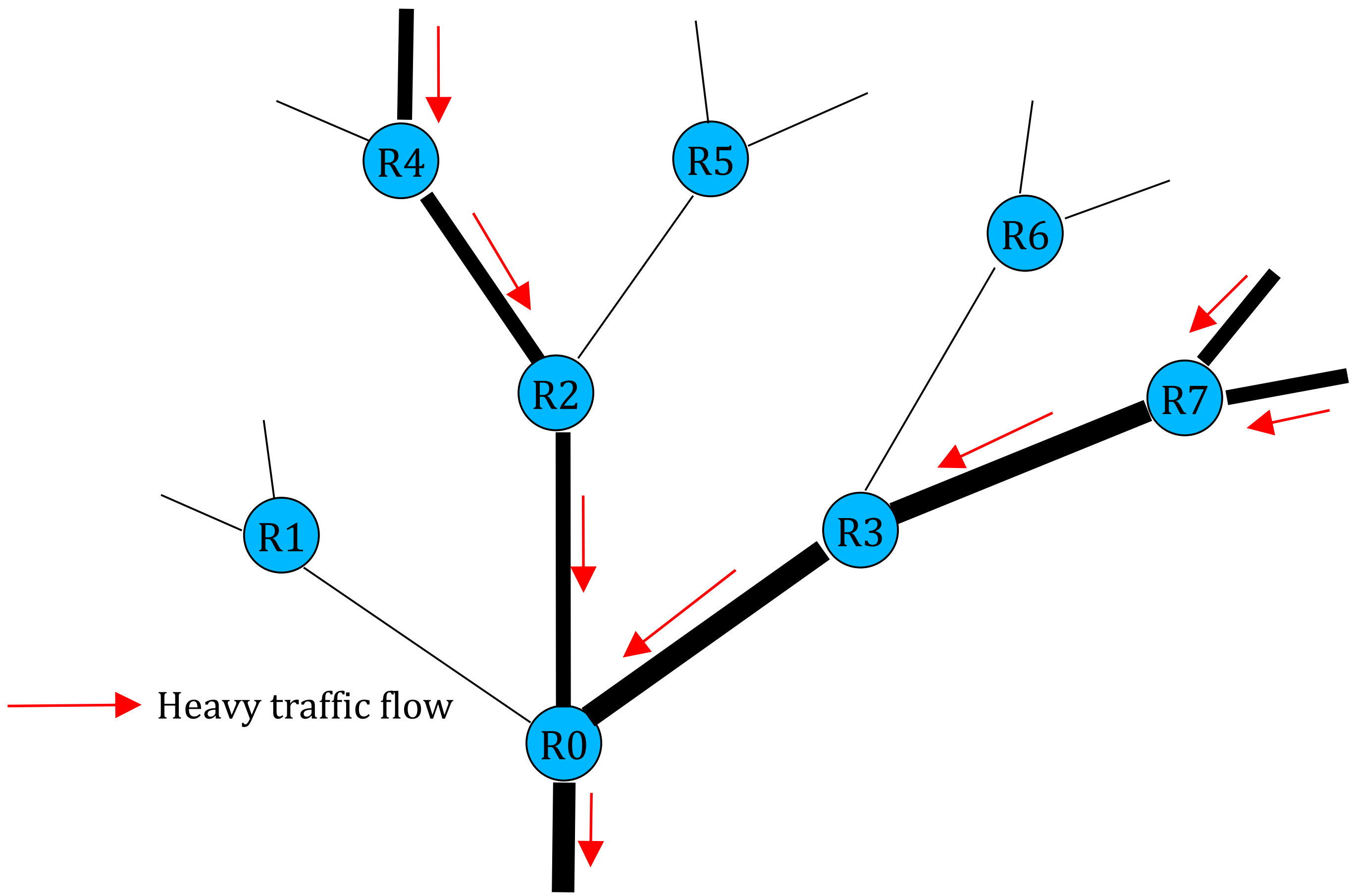
⇒Limiting service requests

➢Identifying good/bad requests

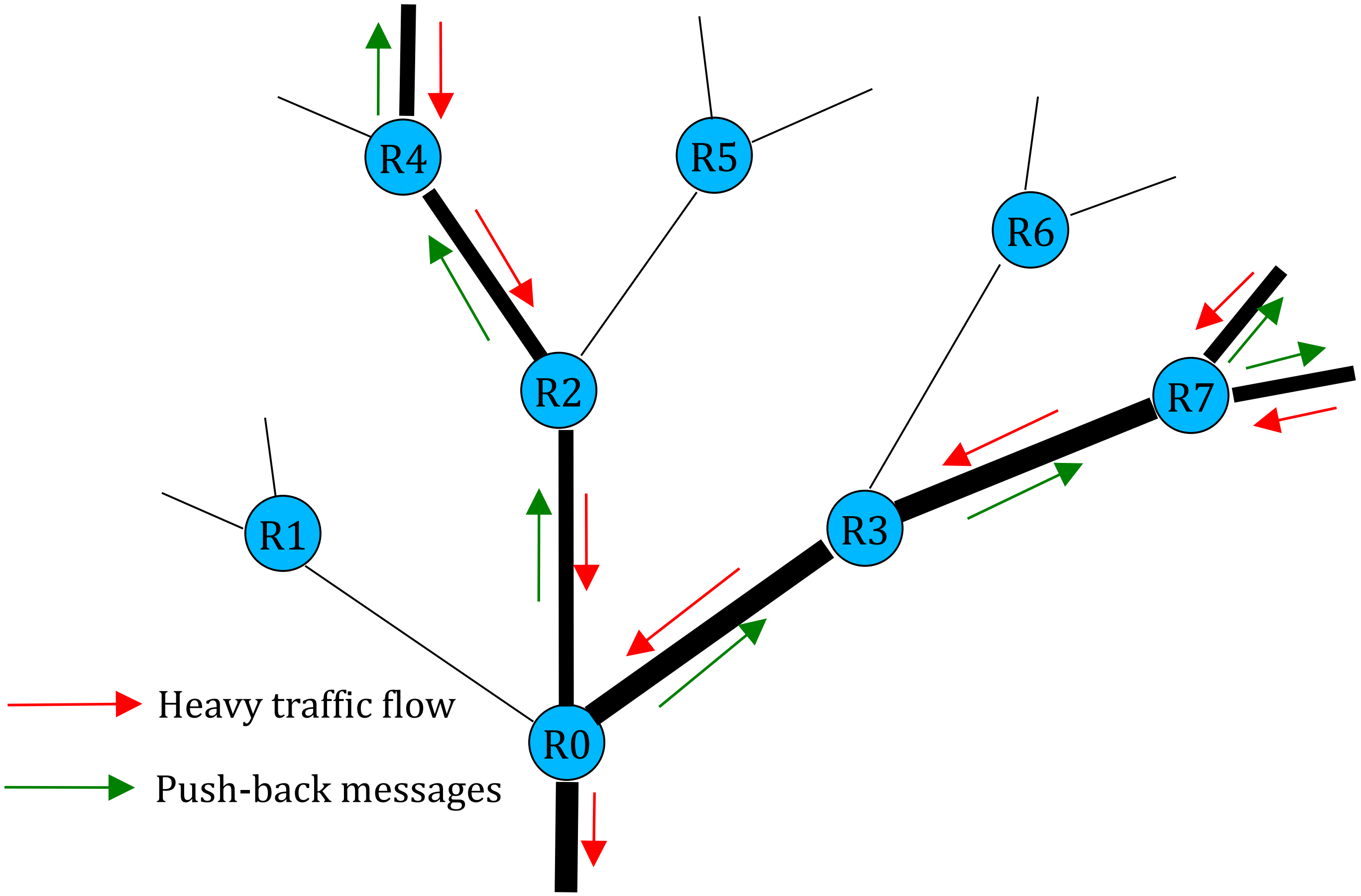
Rate-limiting and Push-back

- Rate-limiting
  - Limiting the traffic from individual incoming links, to achieve fairness
  - Maxmin fairness: small requestor gets what he asks, while big requestor gets average portion
- Push-back
  - Individual router pushes the rate-limiting requests to its upstream routers

Rate-limiting and Push-back



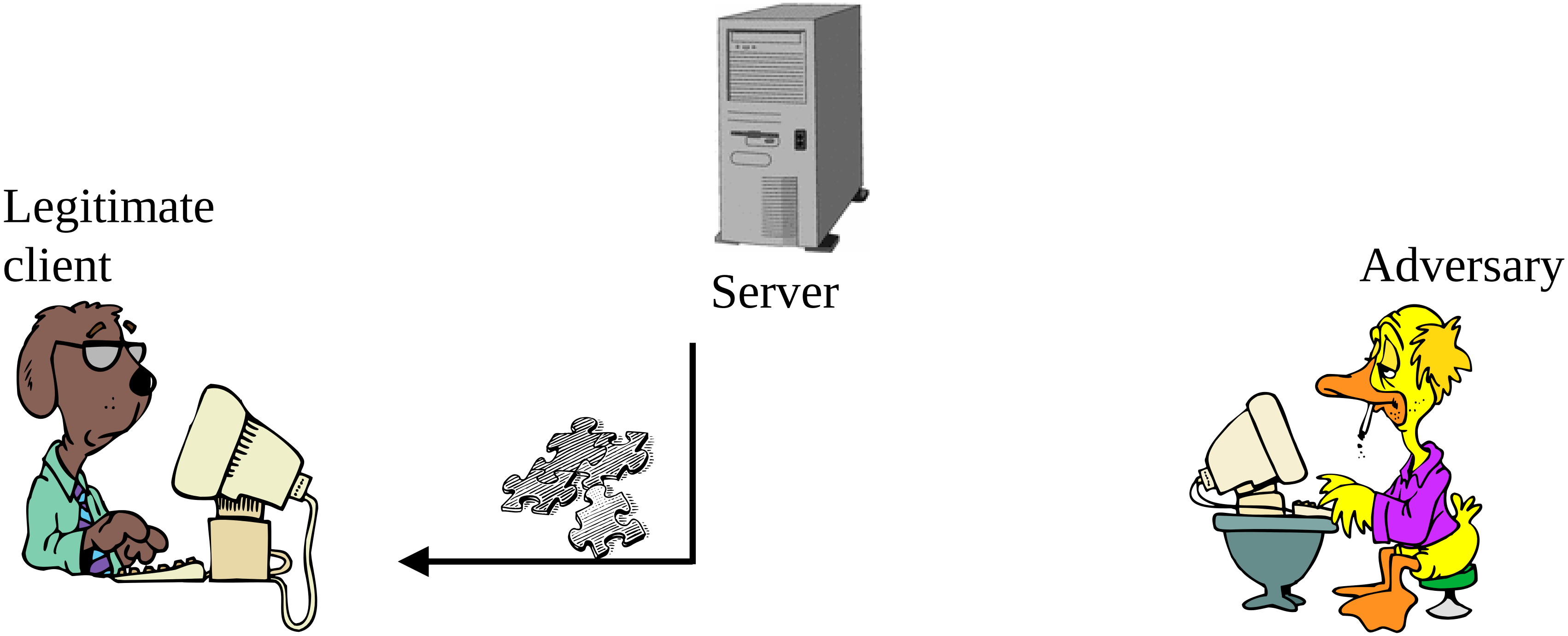
Rate-limiting and Push-back



Weaknesses

- ➢Need large-scale deployment
  - Otherwise, collateral damage could be substantial
  - Proper deployed attacking flows may evade controls
- ➢Router needs to keep per flow state
- ➢However, the mechanism could be more effective if combined with detection mechanisms

Client puzzles

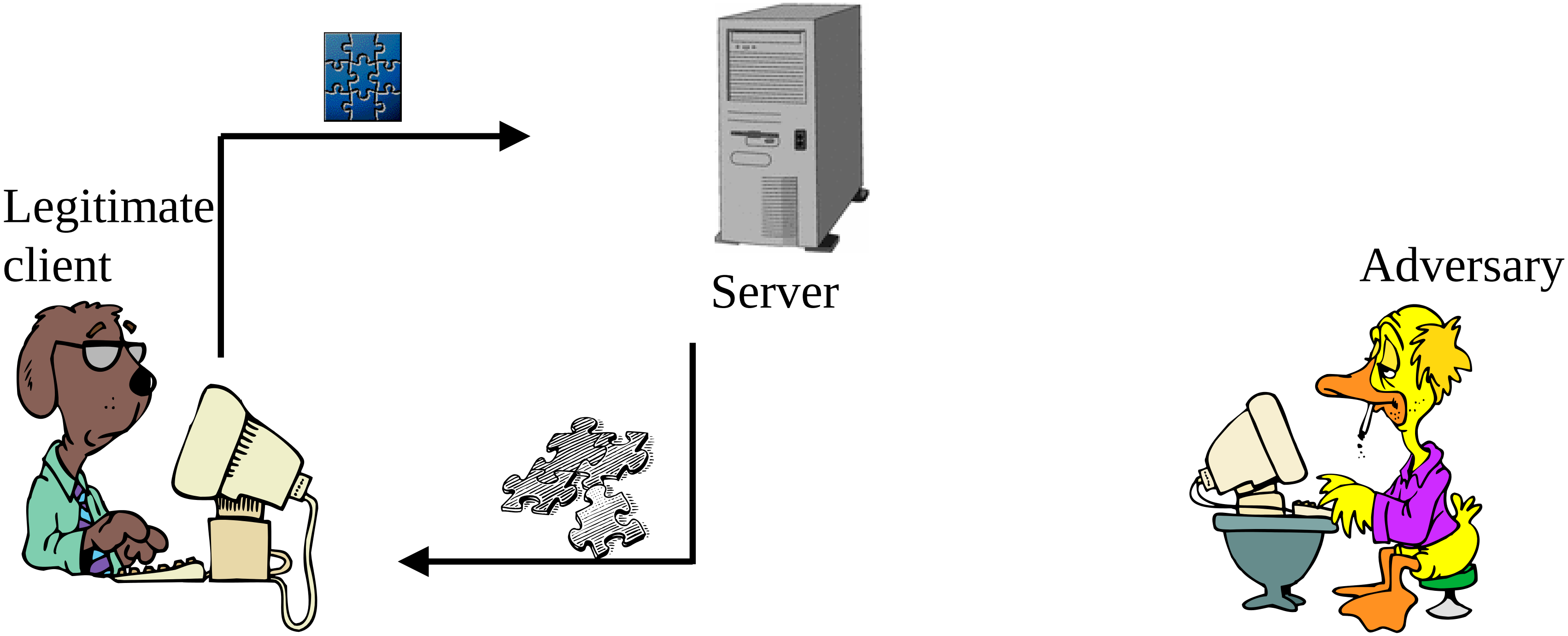


Legitimate client

Server

Adversary

Client puzzles

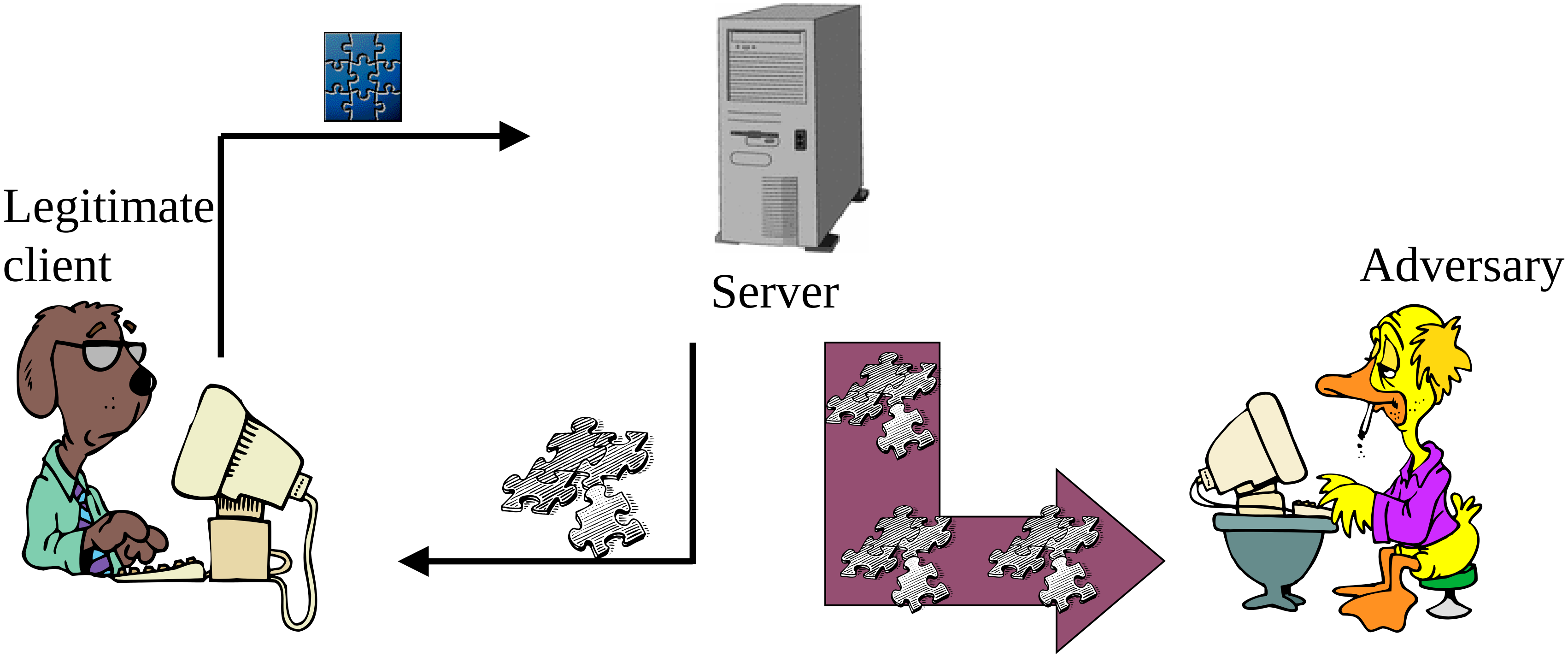


Legitimate client

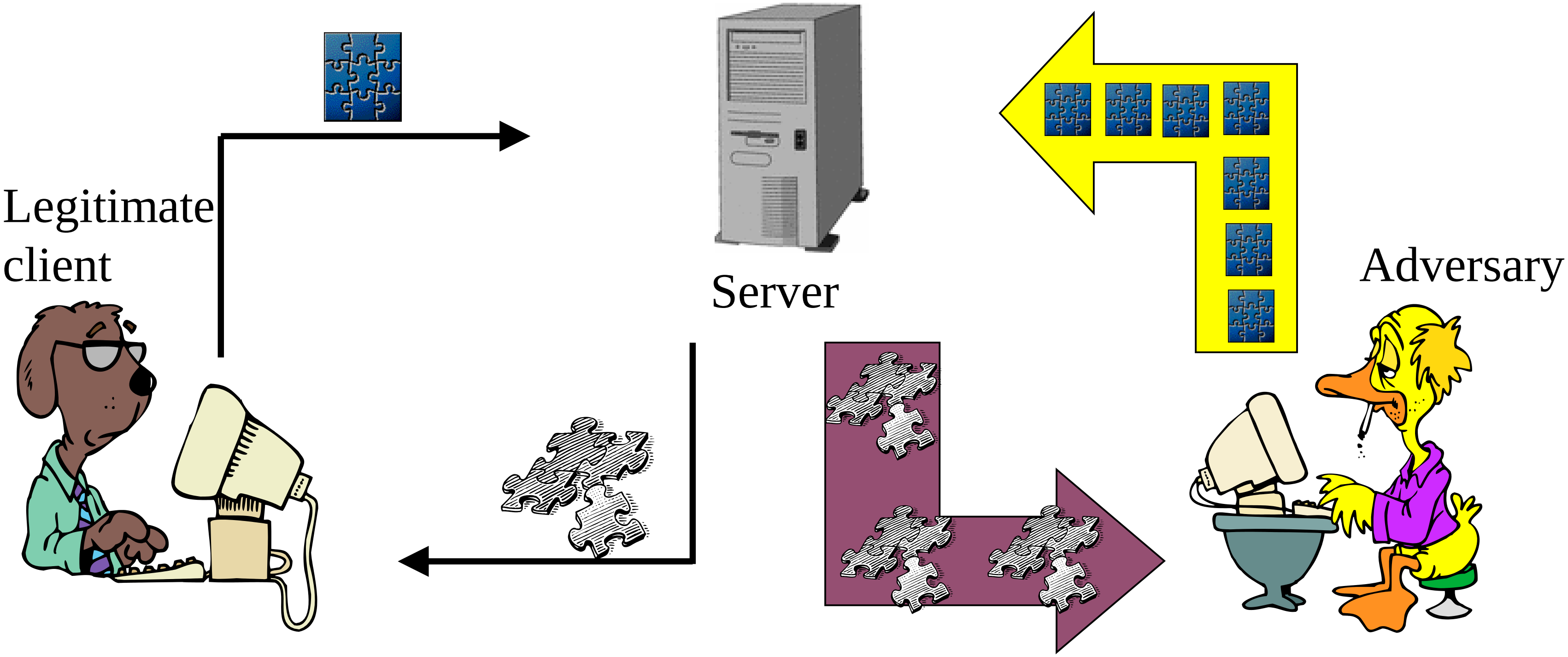
Server

Adversary

Client puzzles



Client puzzles



Application of puzzles

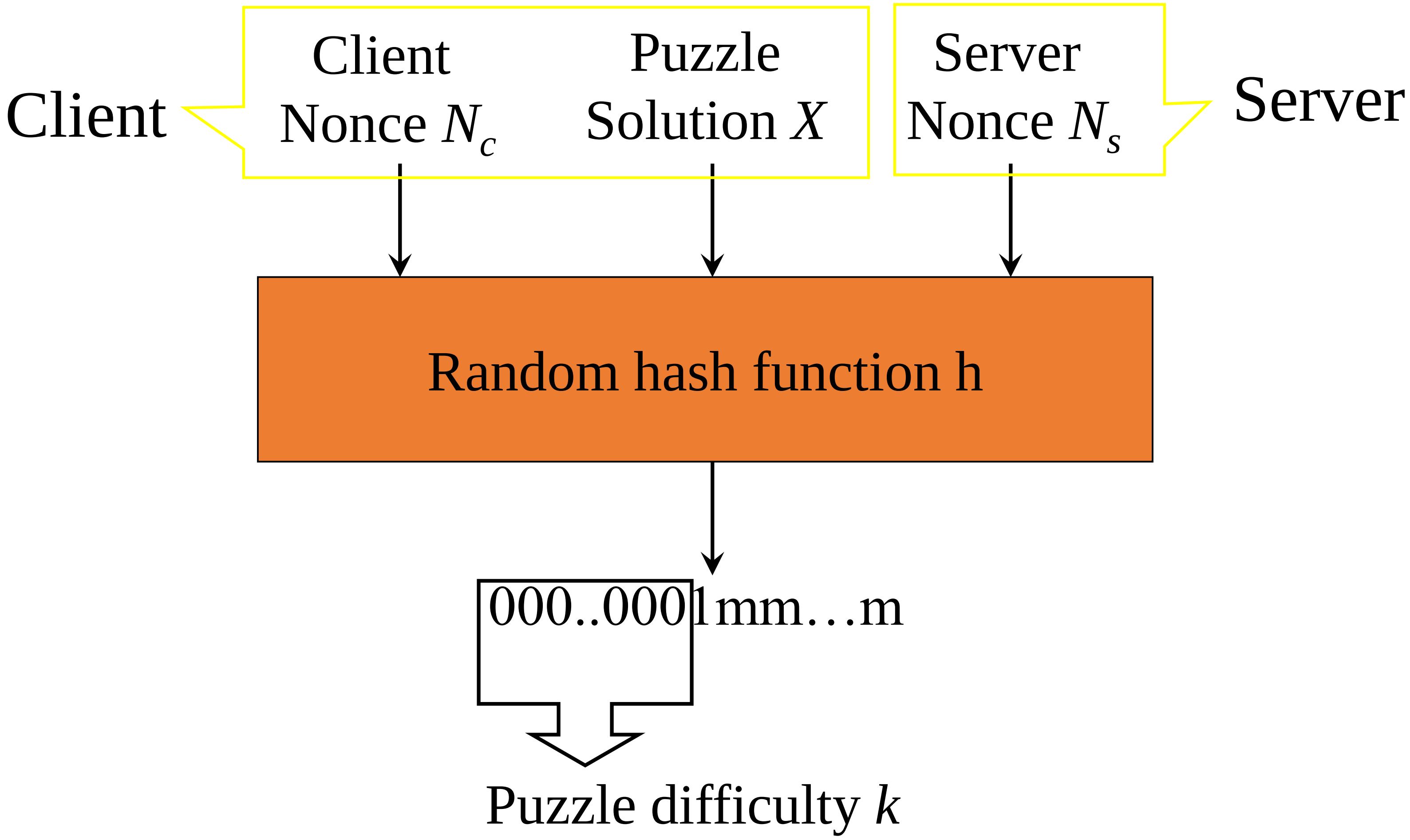
- Mitigate bandwidth exhaustion attacks (Wang&Reiter, 04)
- Prevent Connectivity attacks (Juels&Brainard,99 Wang&Reiter, 03)
- Computing resource attacks (Aura, et al, 00) (Dean&Stubblefield, 01)
- Fighting SPAM (Abadi, et al 03) (Dwork&Naor, 92)
- Others: key agreement protocols, creating time capsules, metering web-usage and fair exchange protocols

Puzzle types

- CPU bounded puzzle functions
  - Hash function (Juels&Brainard,99)
  - Signature scheme (Dwork&Naor,92)

- Memory bounded puzzles (Abadi, et al, 03)

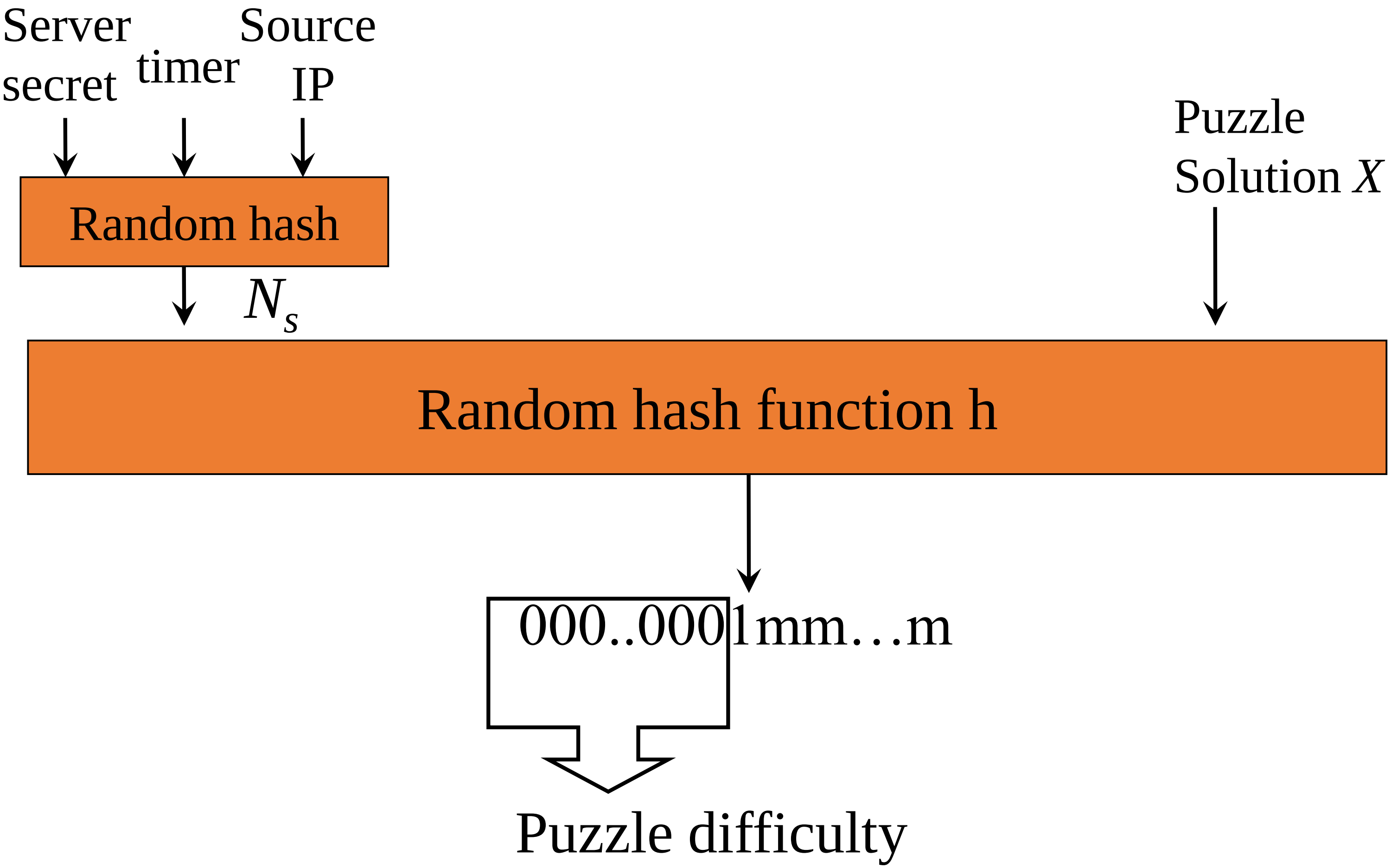
What a puzzle looks like?



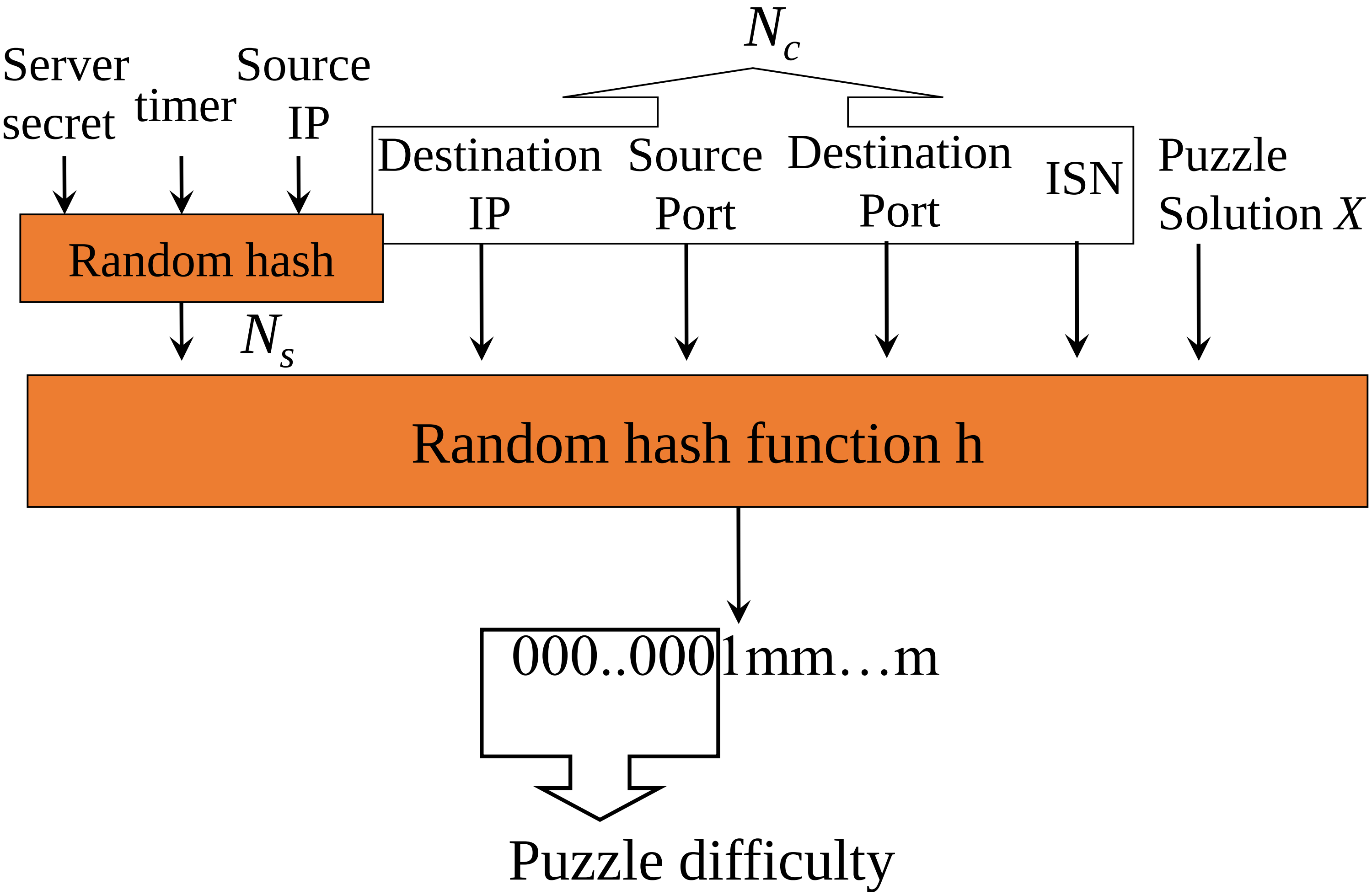
Puzzle auction

- Puzzle Auctions
  - Servers hold an auction
  - Clients bid for the service with the puzzles
  - Those who solve the most difficult puzzles get resources
- Valuation of service
  - Observation (Geng&Whinston,00): Attackers do not want to cost zombies
  - Implication: legitimate clients value service more
- Incremental bidding: gradually raise the bid via retransmission mechanism until get communication through

Example: TCP puzzles

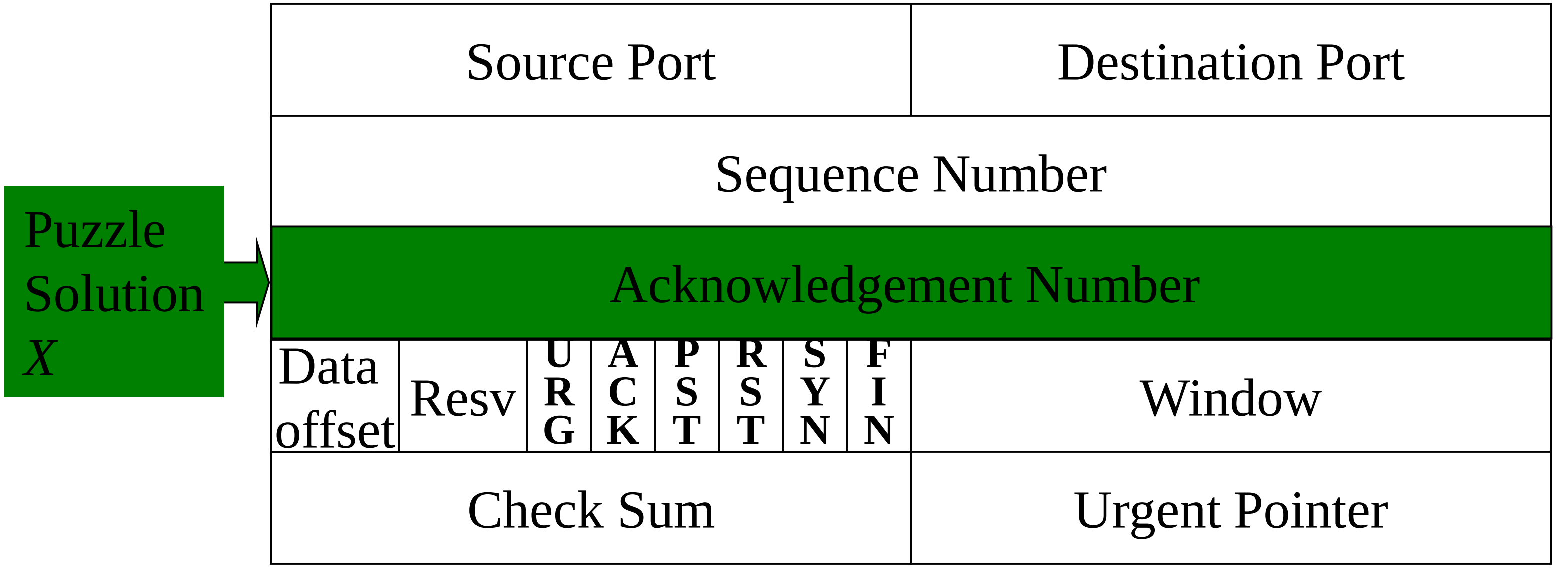


Example: TCP puzzles



Embedding puzzles to covert channel

TCP Frame: SYN



Puzzle Solution *X*

Source Port

Destination Port

Sequence Number

Acknowledgement Number

Data offset

Resv

URG

ACK

PST

RST

SYN

FIN

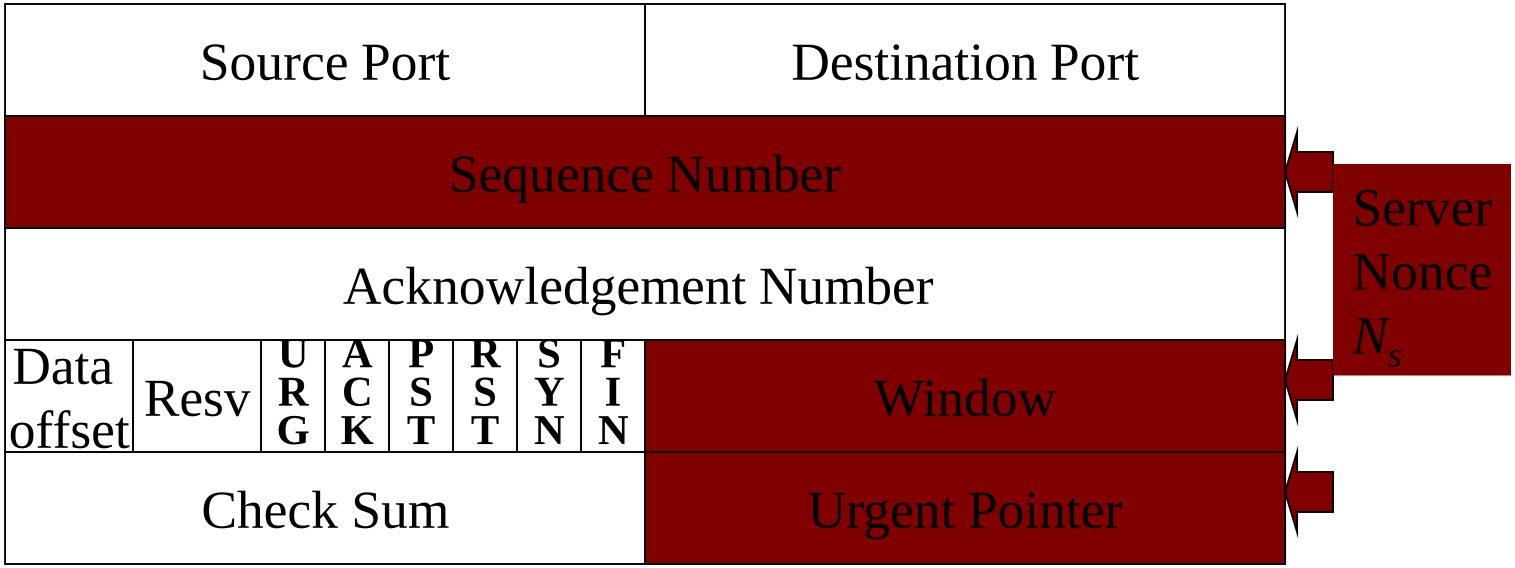
Window

Check Sum

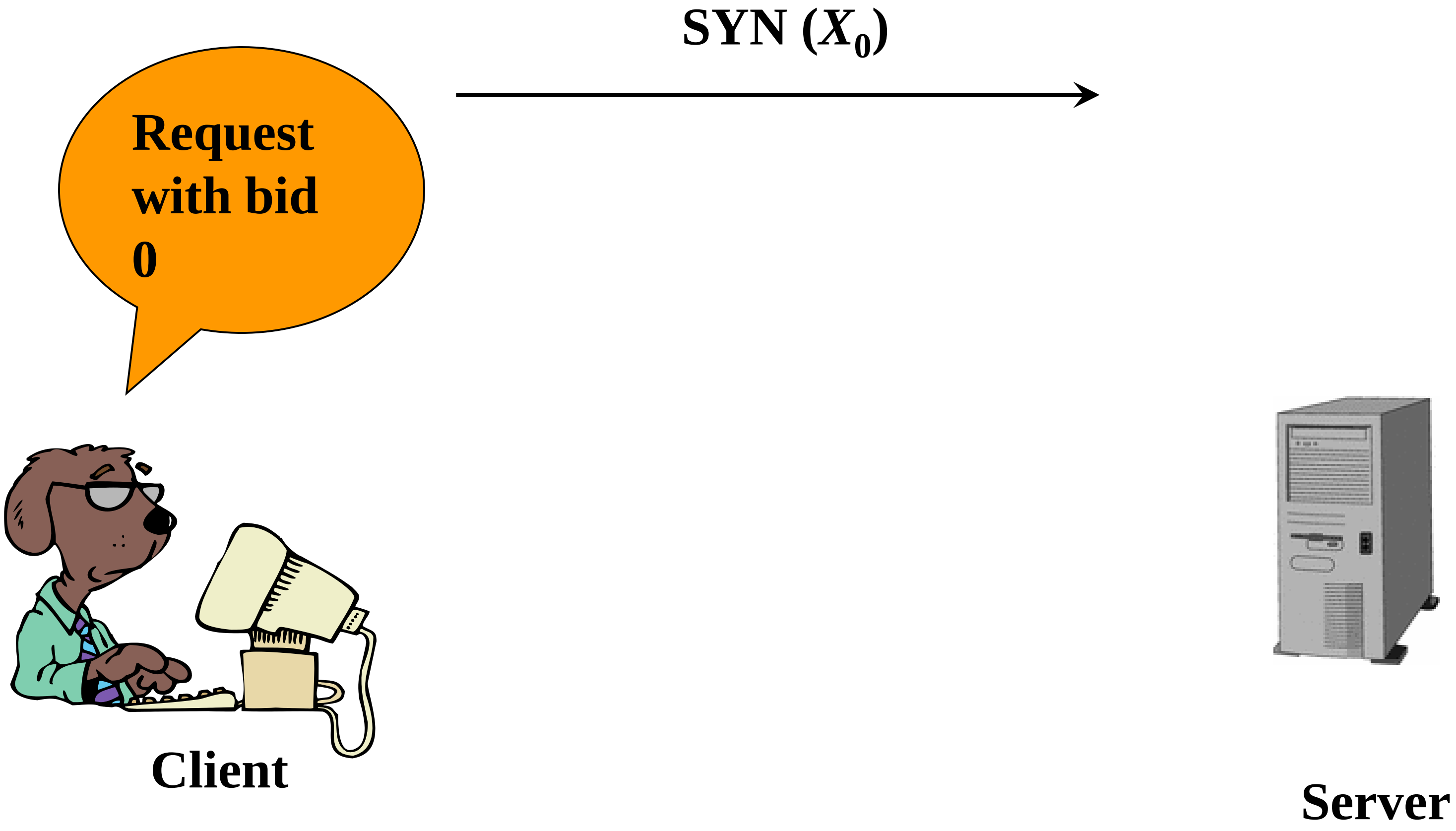
Urgent Pointer

Embedding puzzles to covert channel

TCP Frame: RST



TCP puzzle auction



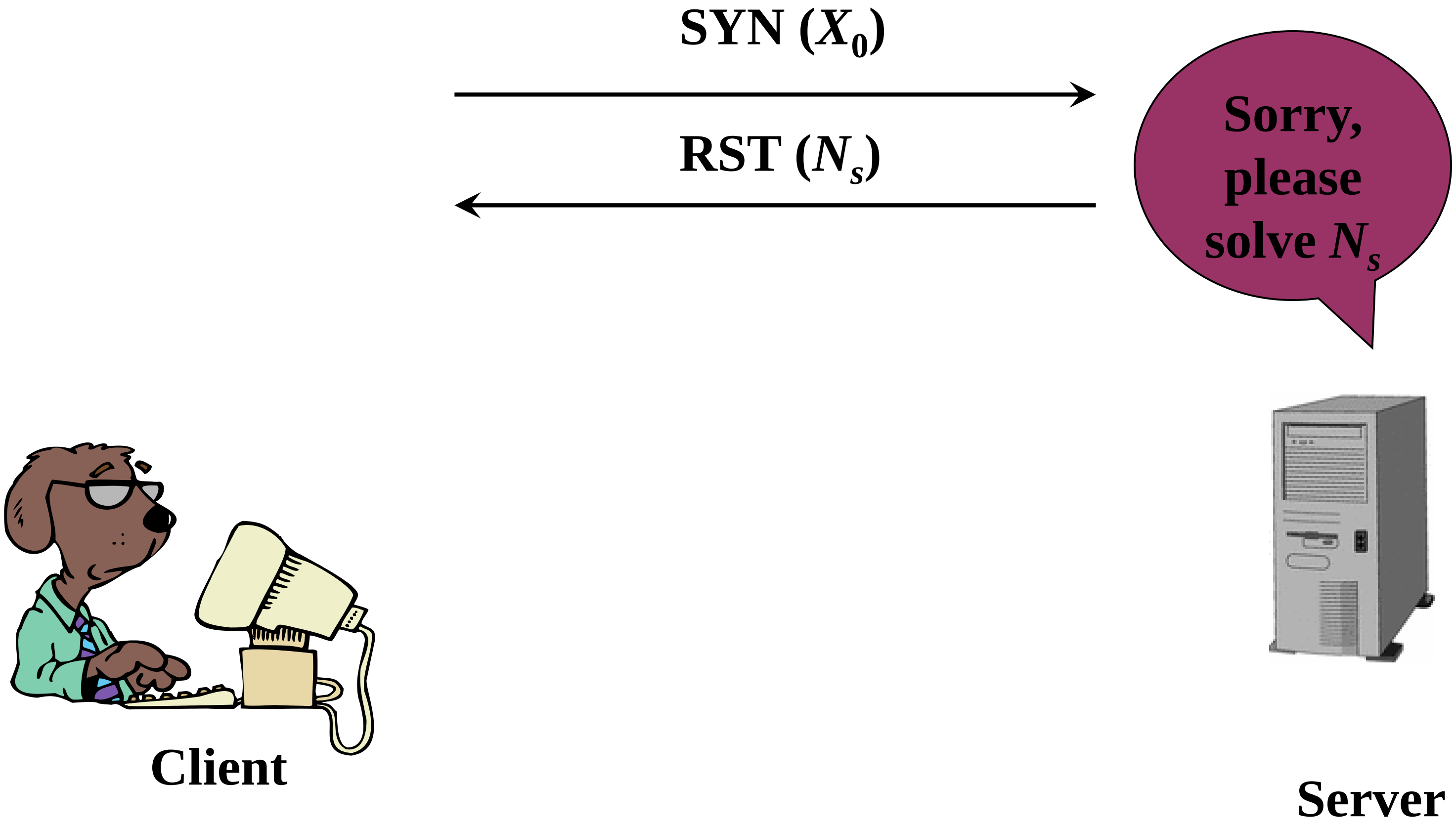
SYN (X_0)

Request with bid 0

Client

Server

TCP puzzle auction



SYN (X_0)

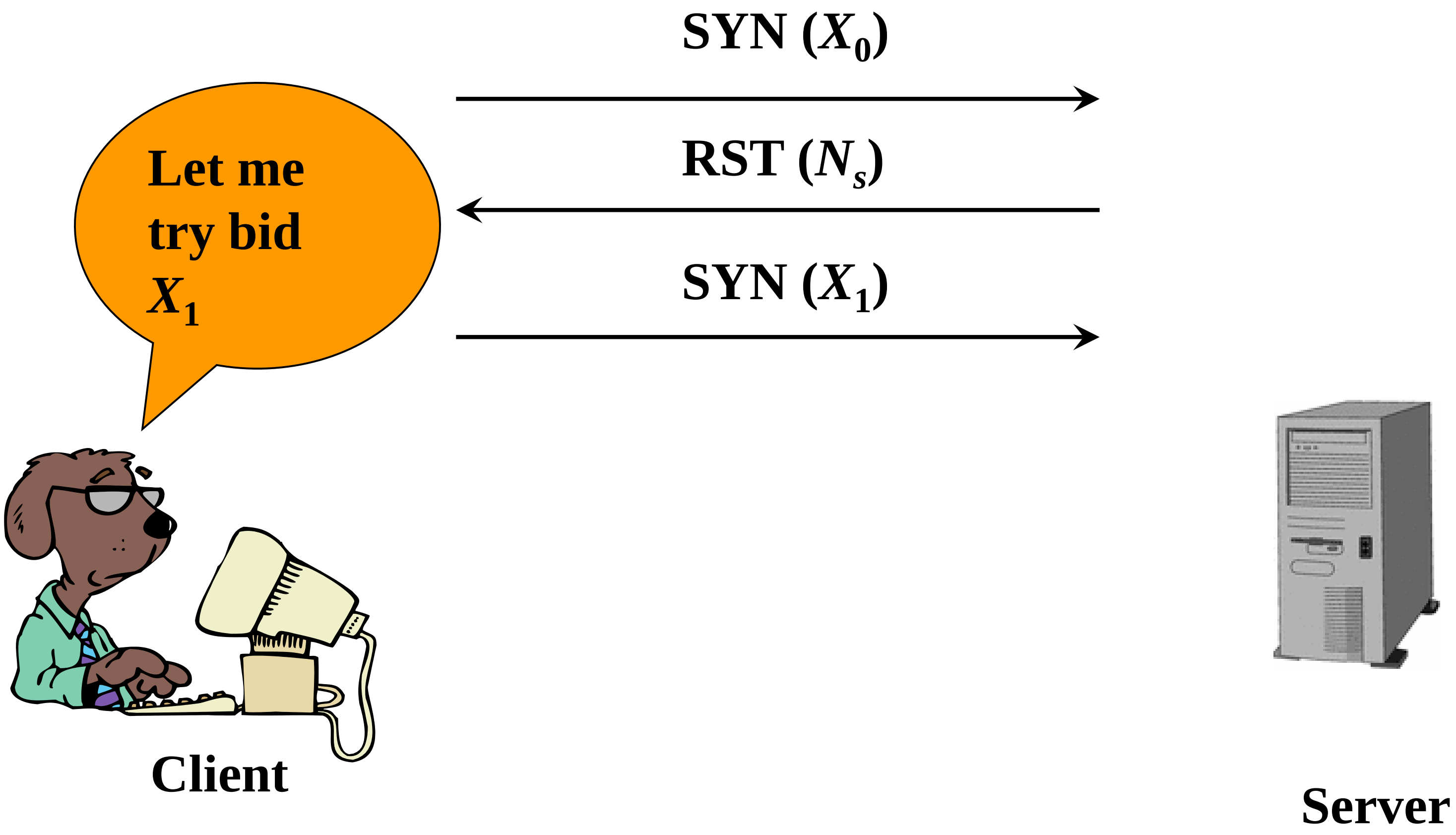
RST (N_s)

Sorry, please solve N_s

Client

Server

TCP puzzle auction



SYN (X_0)

RST (N_s)

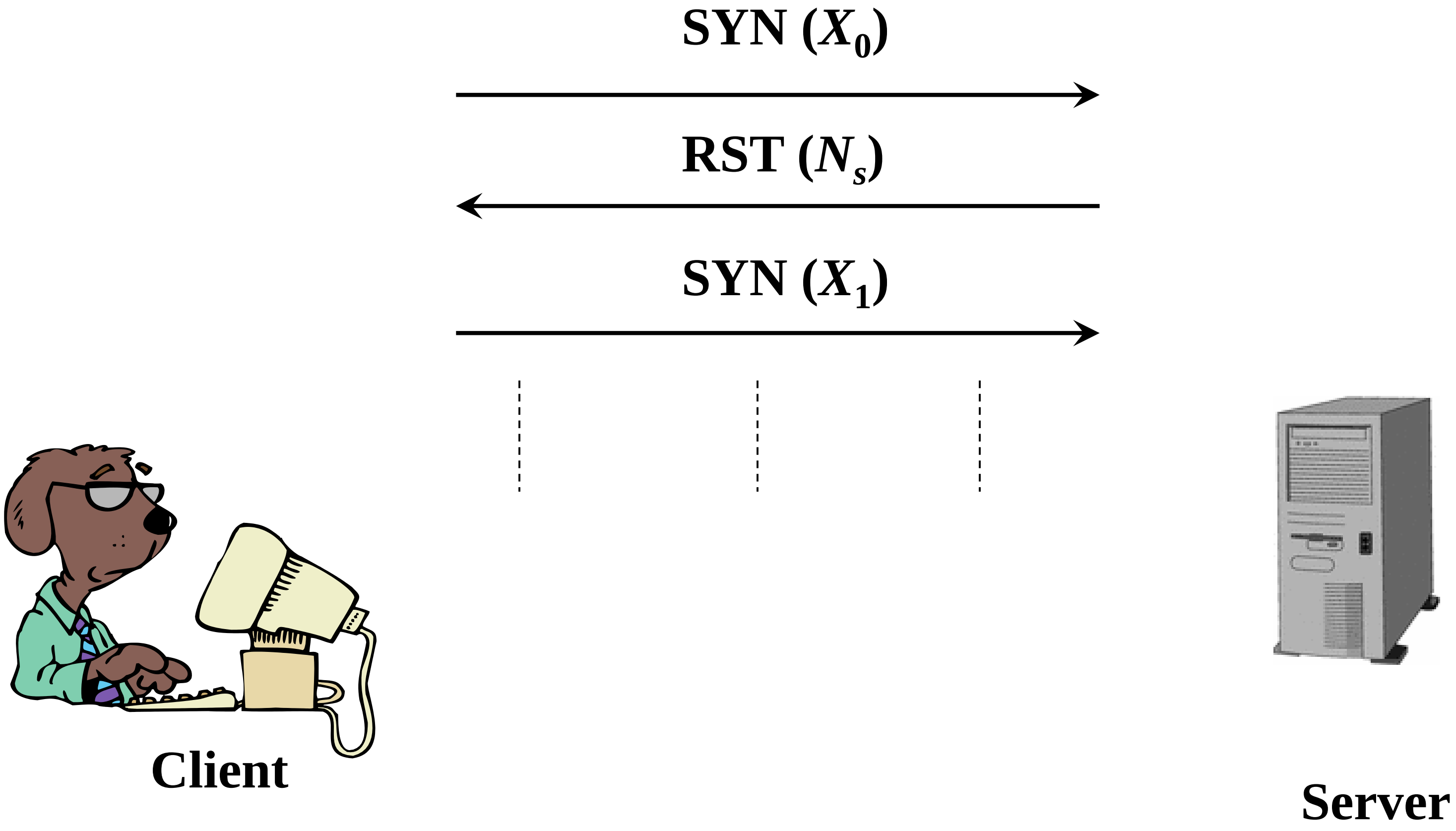
SYN (X_1)

Let me try bid X_1

Client

Server

TCP puzzle auction



SYN (X_0)

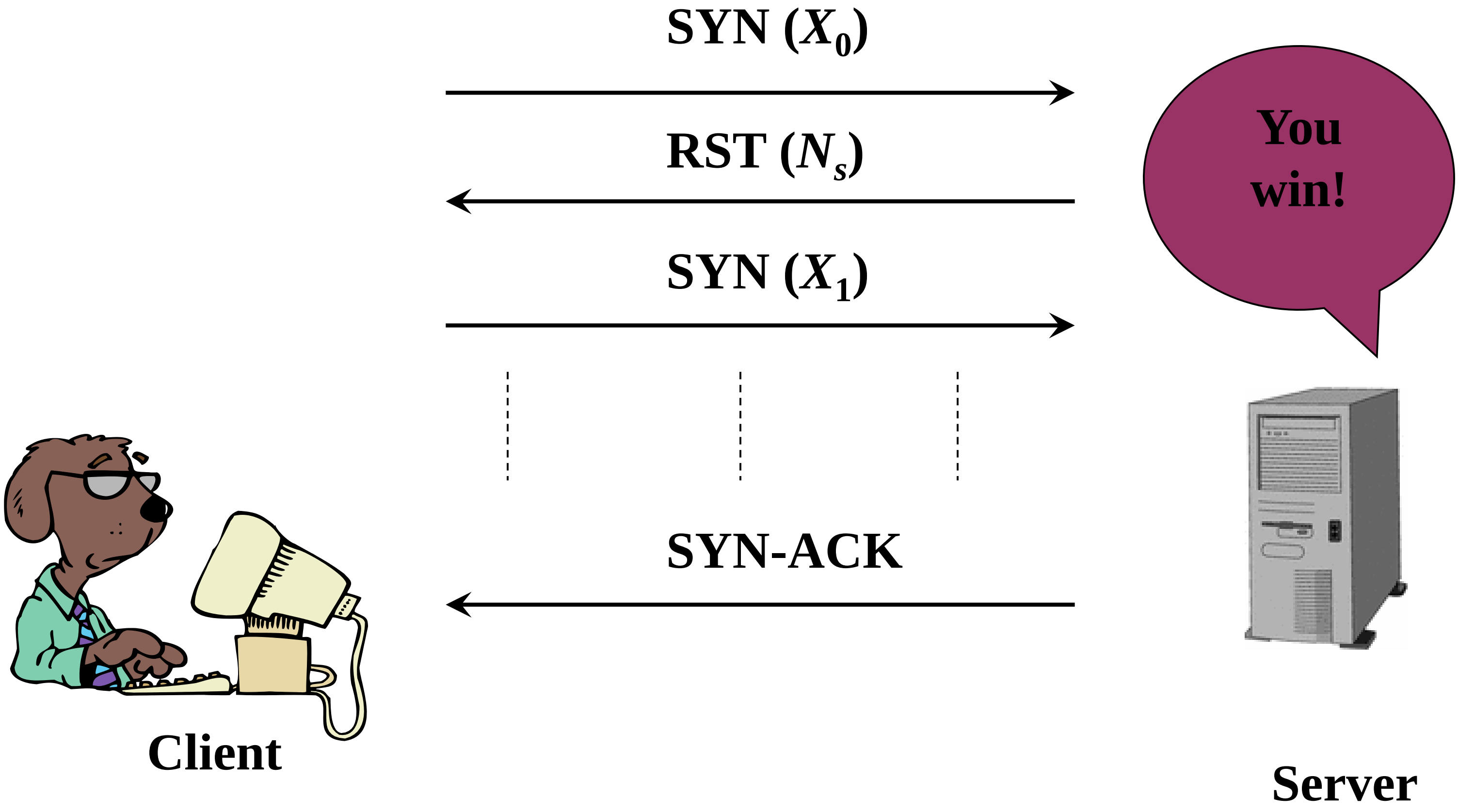
RST (N_s)

SYN (X_1)

Client

Server

TCP puzzle auction



SYN (X_0)

RST (N_s)

SYN (X_1)

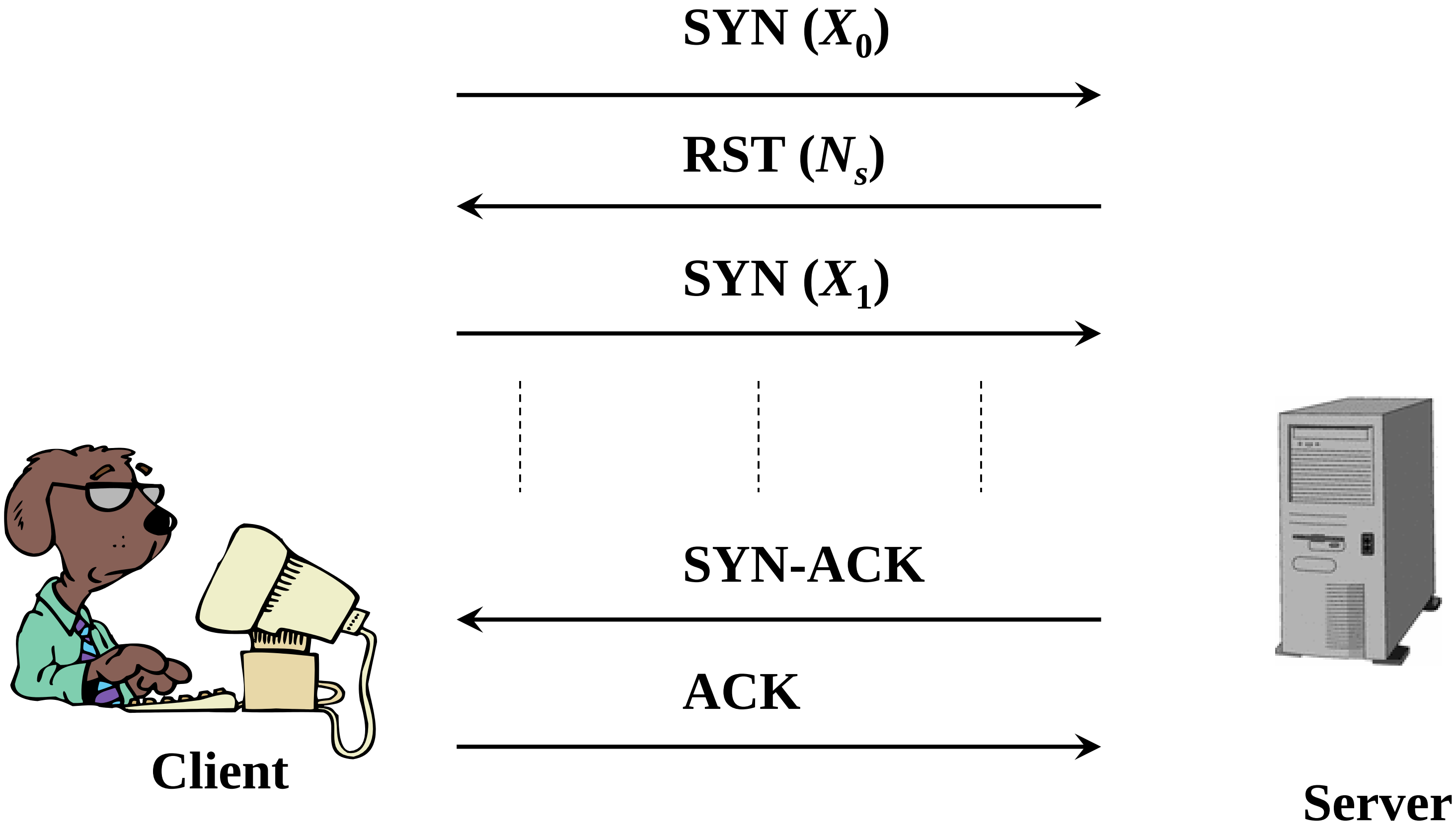
SYN-ACK

You win!

Client

Server

TCP puzzle auction



SYN (X_0)

RST (N_s)

SYN (X_1)

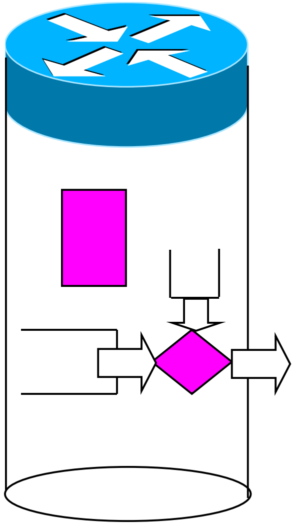
SYN-ACK

ACK

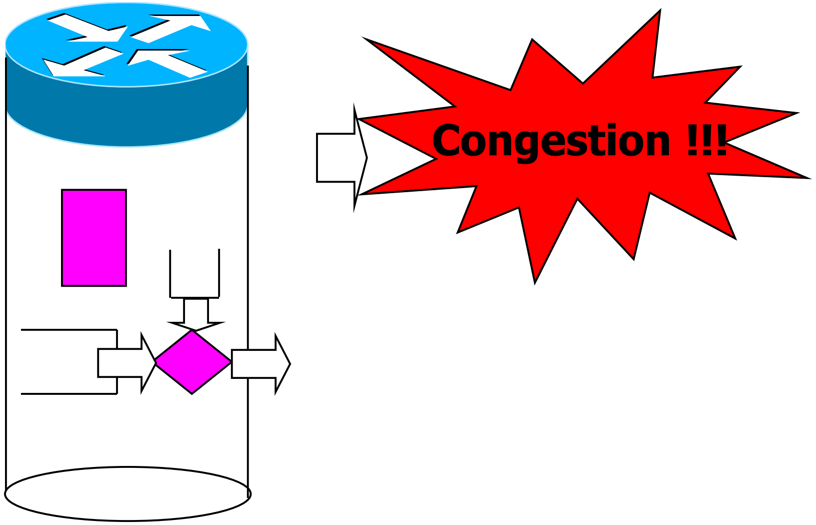
Client

Server

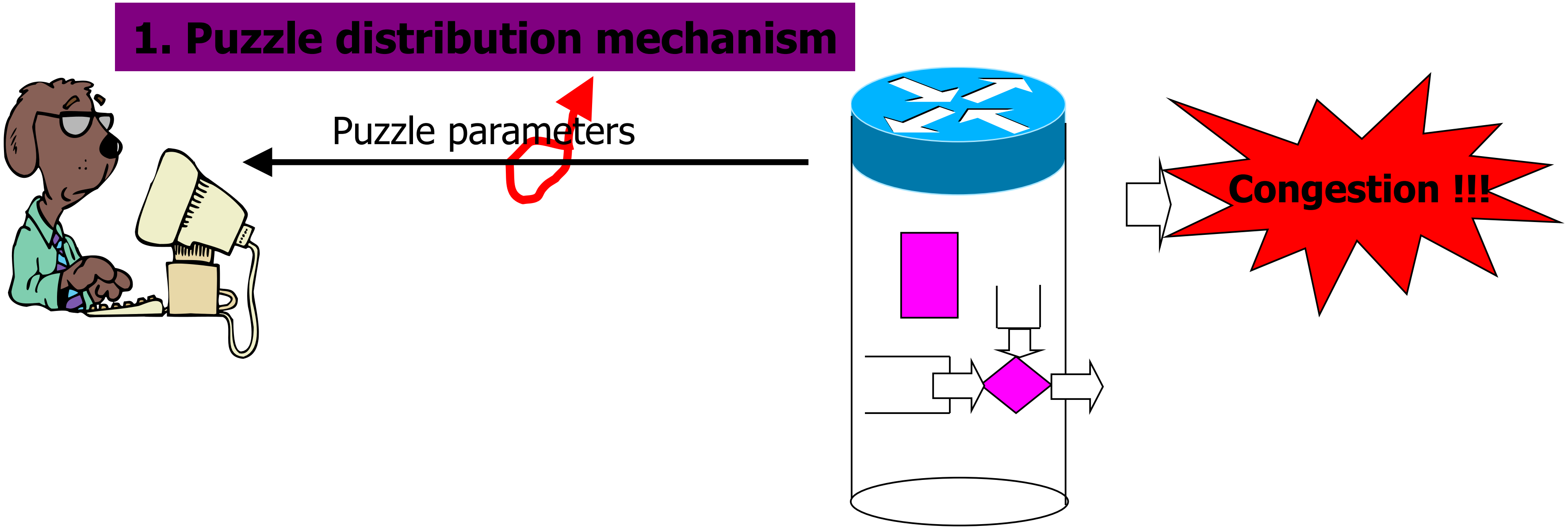
Congestion puzzles



Congestion puzzles



Congestion puzzles

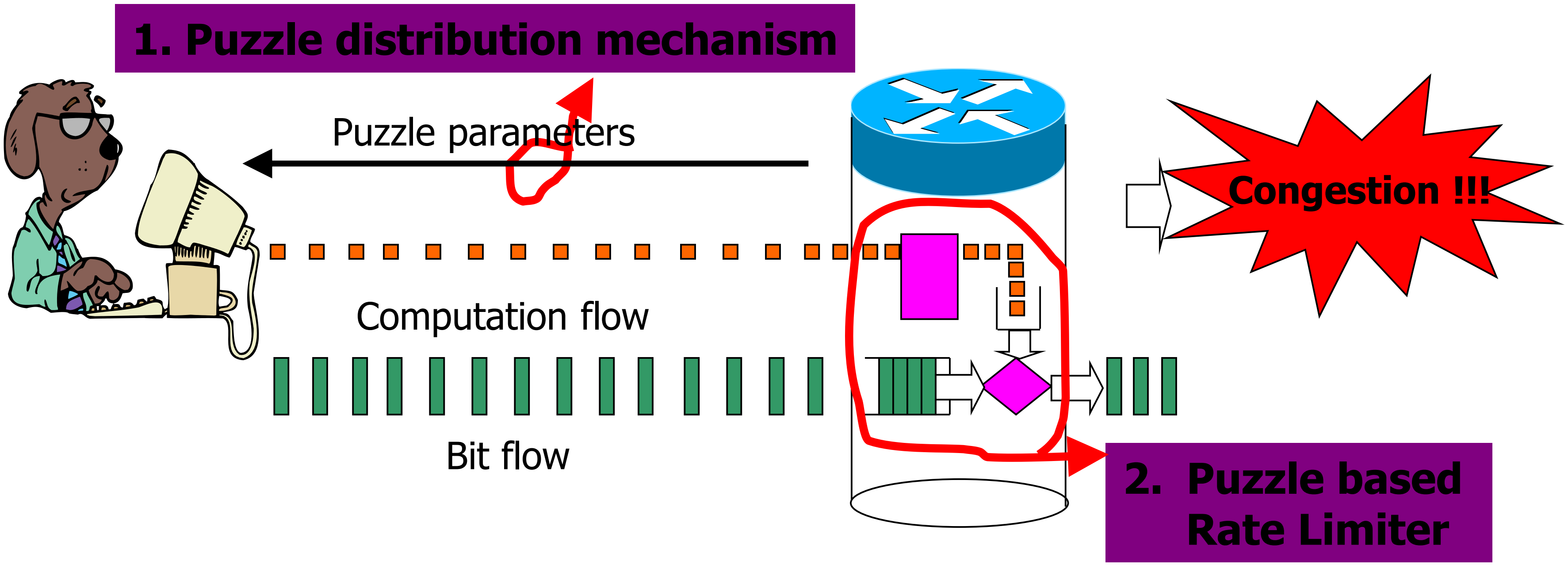


1. Puzzle distribution mechanism

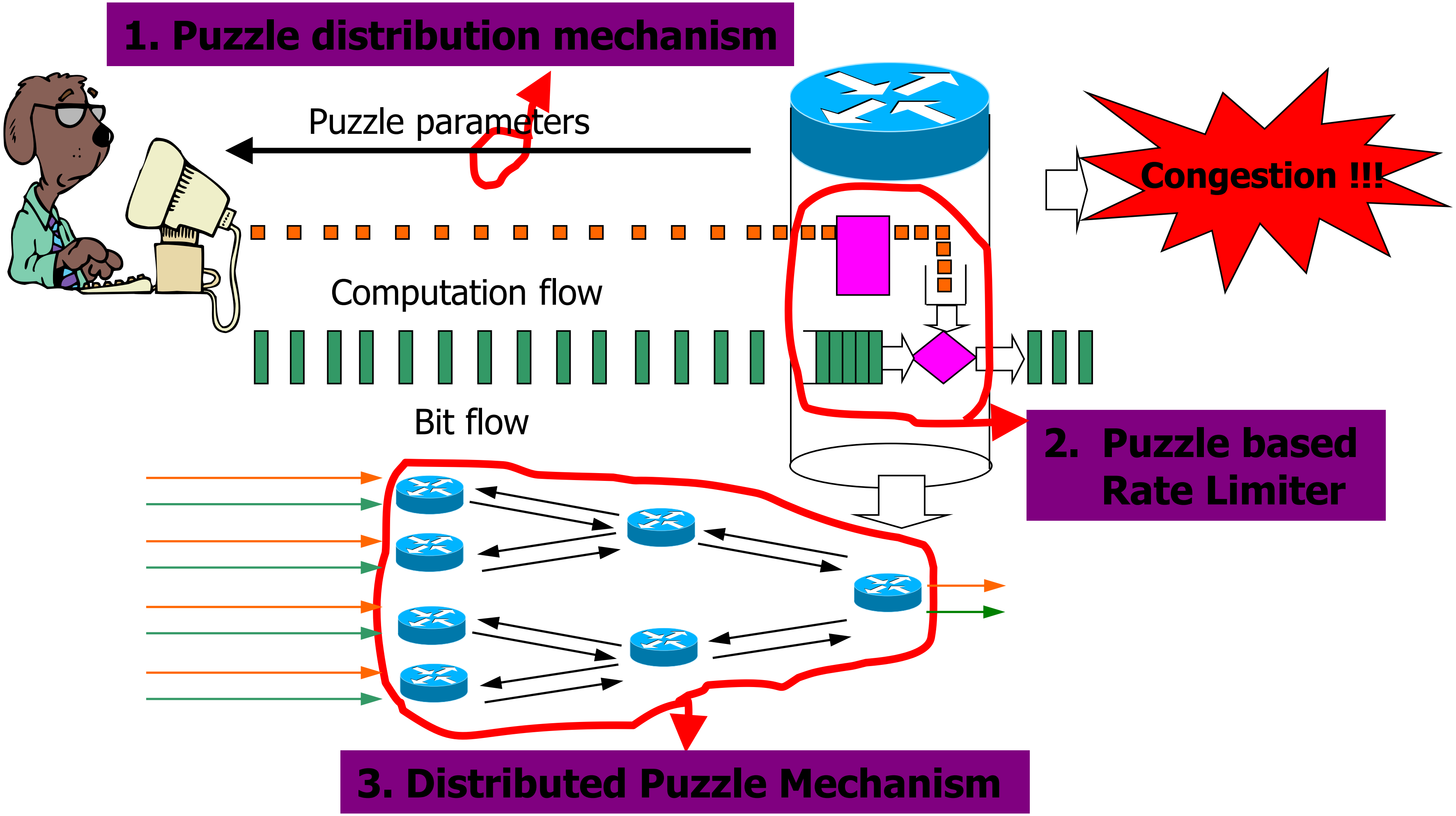
Puzzle parameters

Congestion !!!

Congestion puzzles


1. Puzzle distribution mechanism
Puzzle parameters
Congestion !!!
Computation flow
Bit flow
2. Puzzle based Rate Limiter

Congestion puzzles



1. Puzzle distribution mechanism

Puzzle parameters

Computation flow

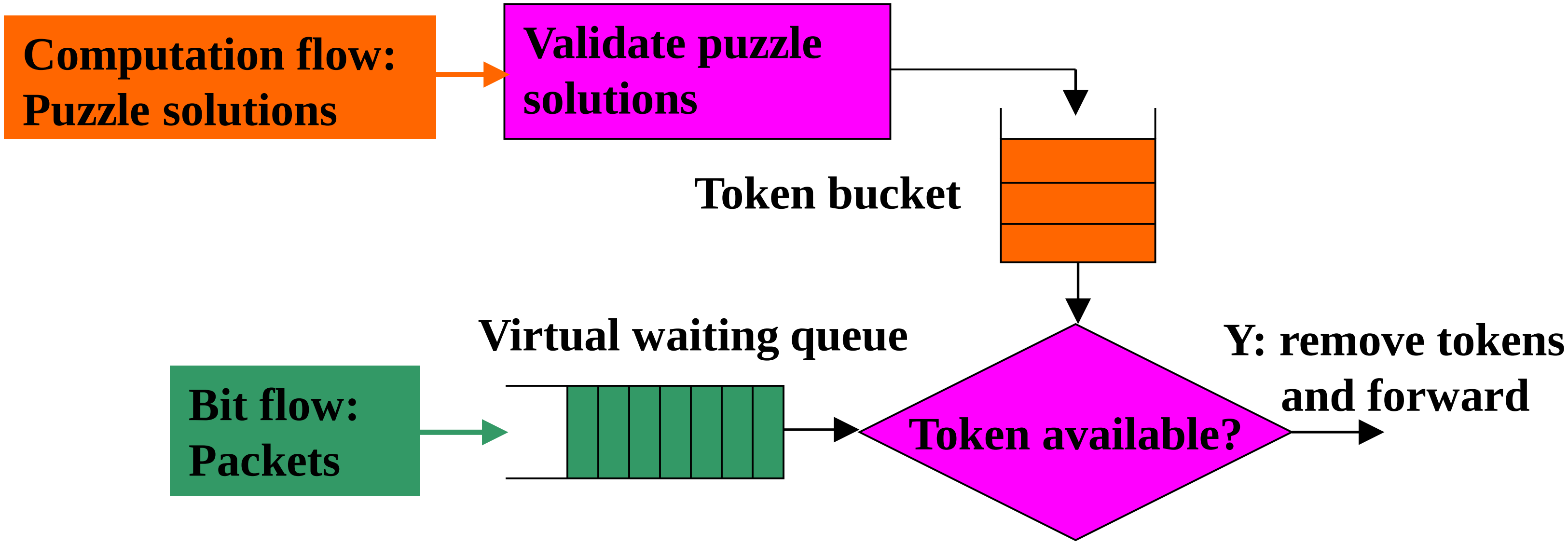
Bit flow

Congestion !!!

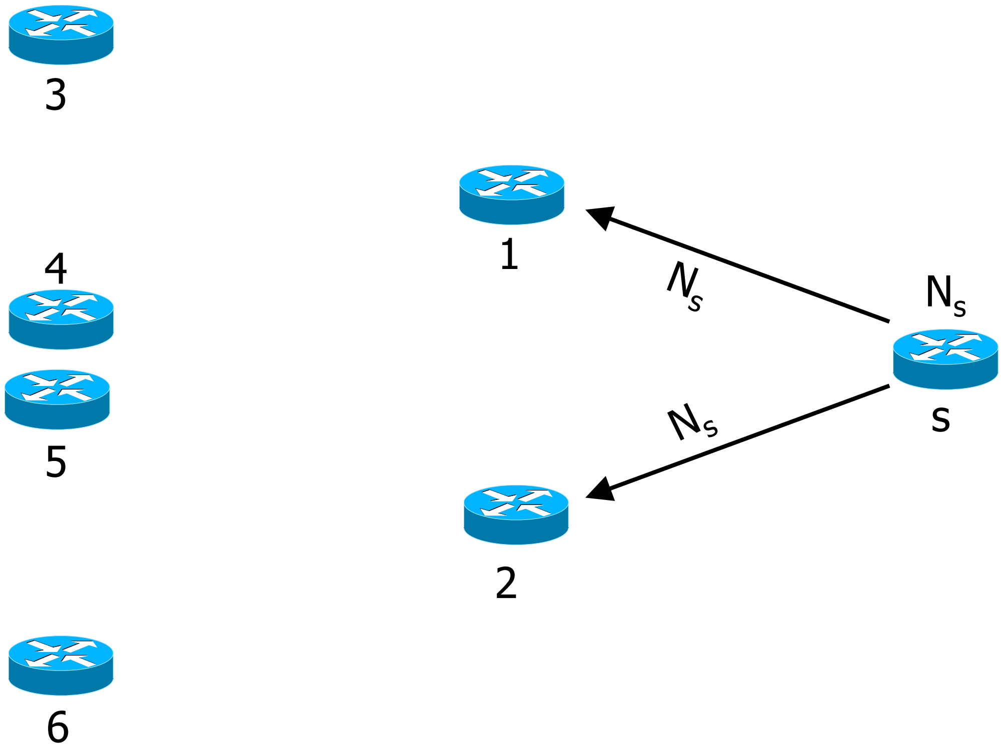
2. Puzzle based Rate Limiter

3. Distributed Puzzle Mechanism

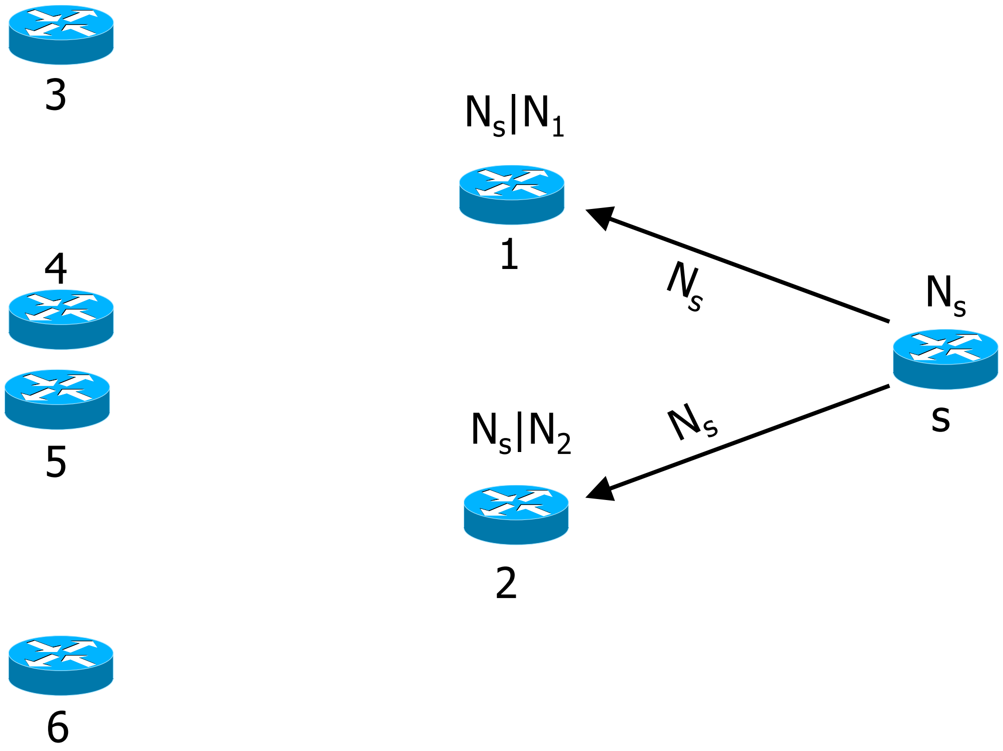
Puzzle-based rate limiter



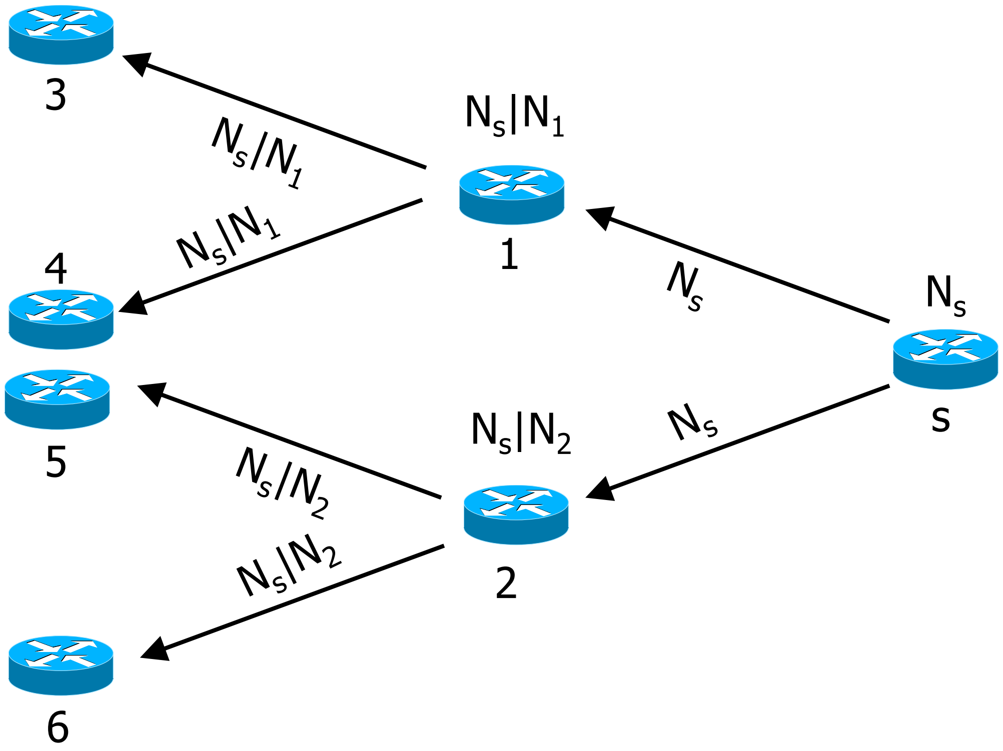
Distributed puzzle mechanism



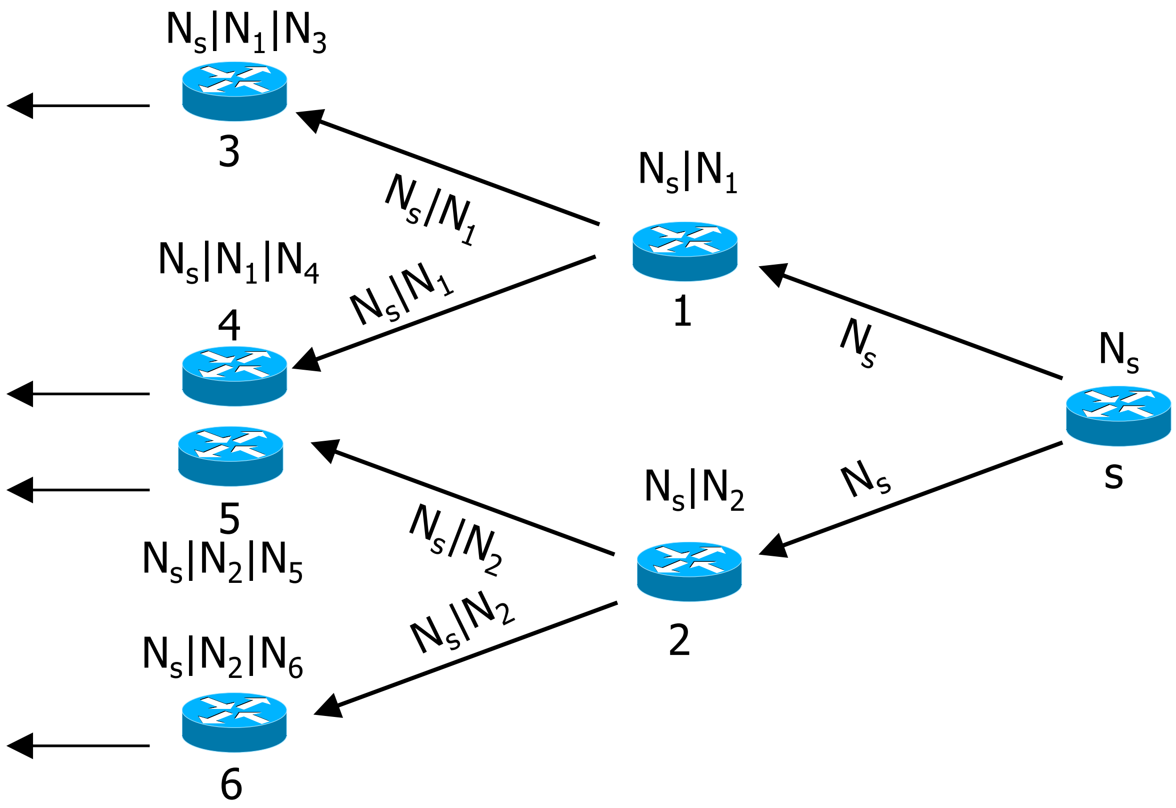
Distributed puzzle mechanism



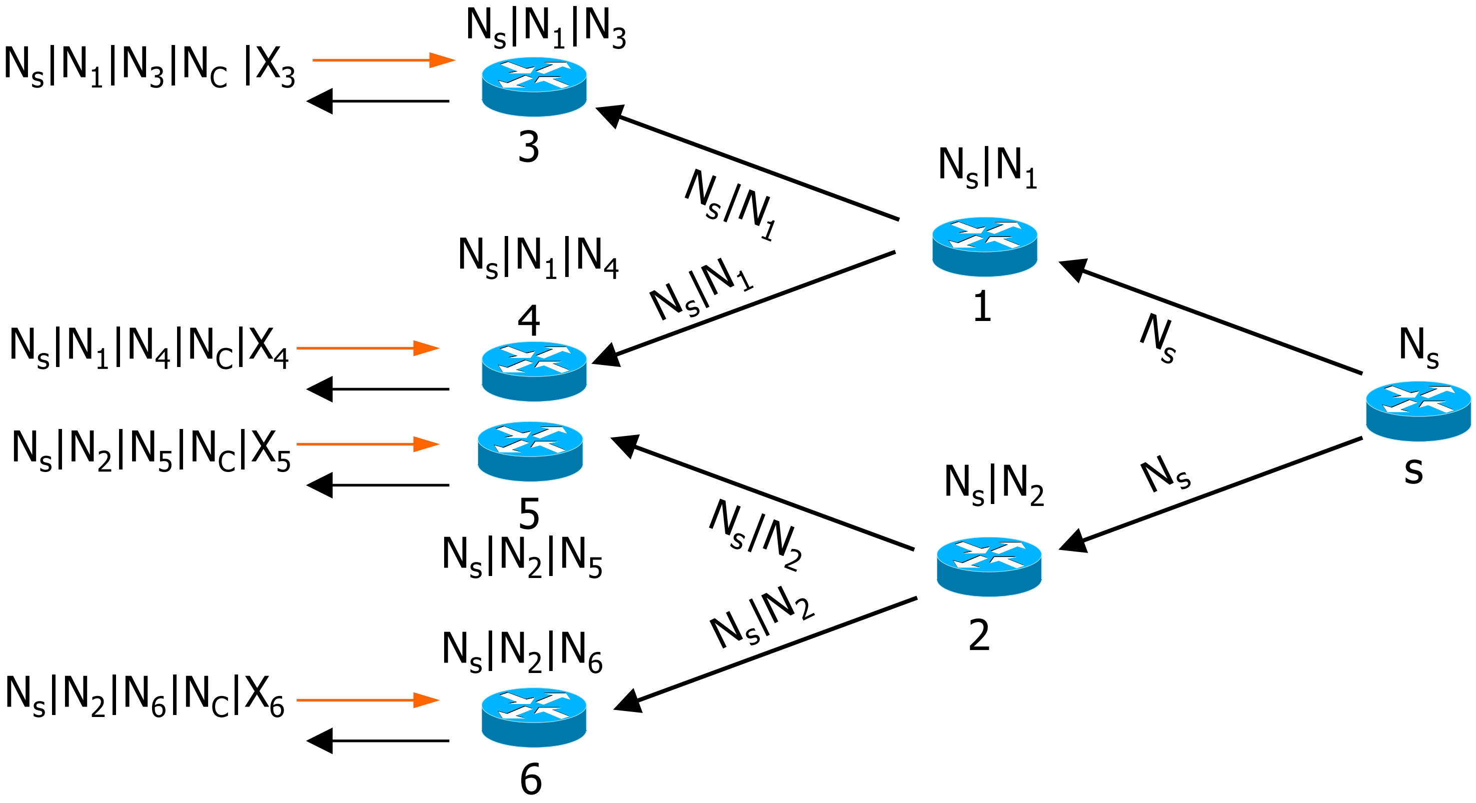
Distributed puzzle mechanism



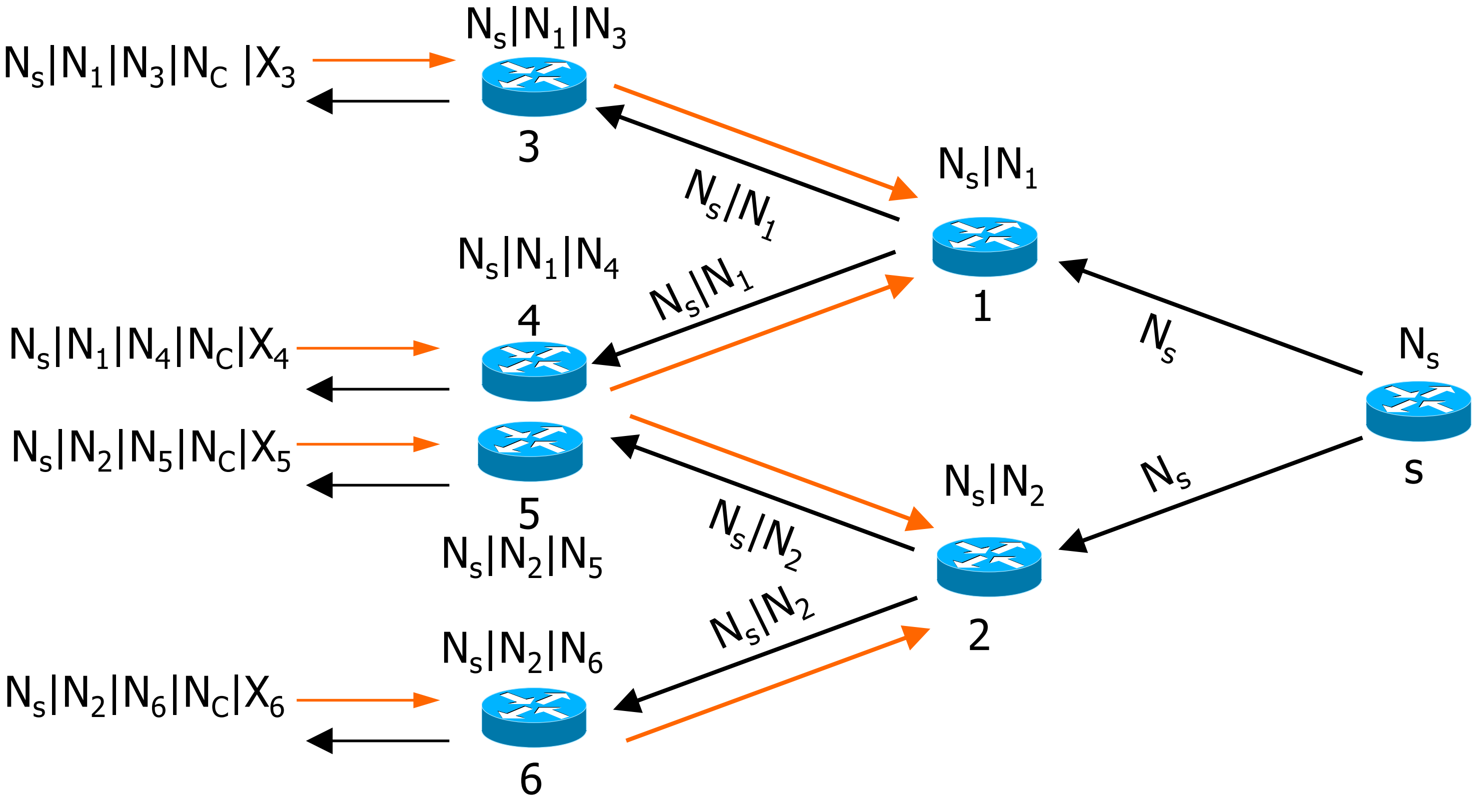
Distributed puzzle mechanism



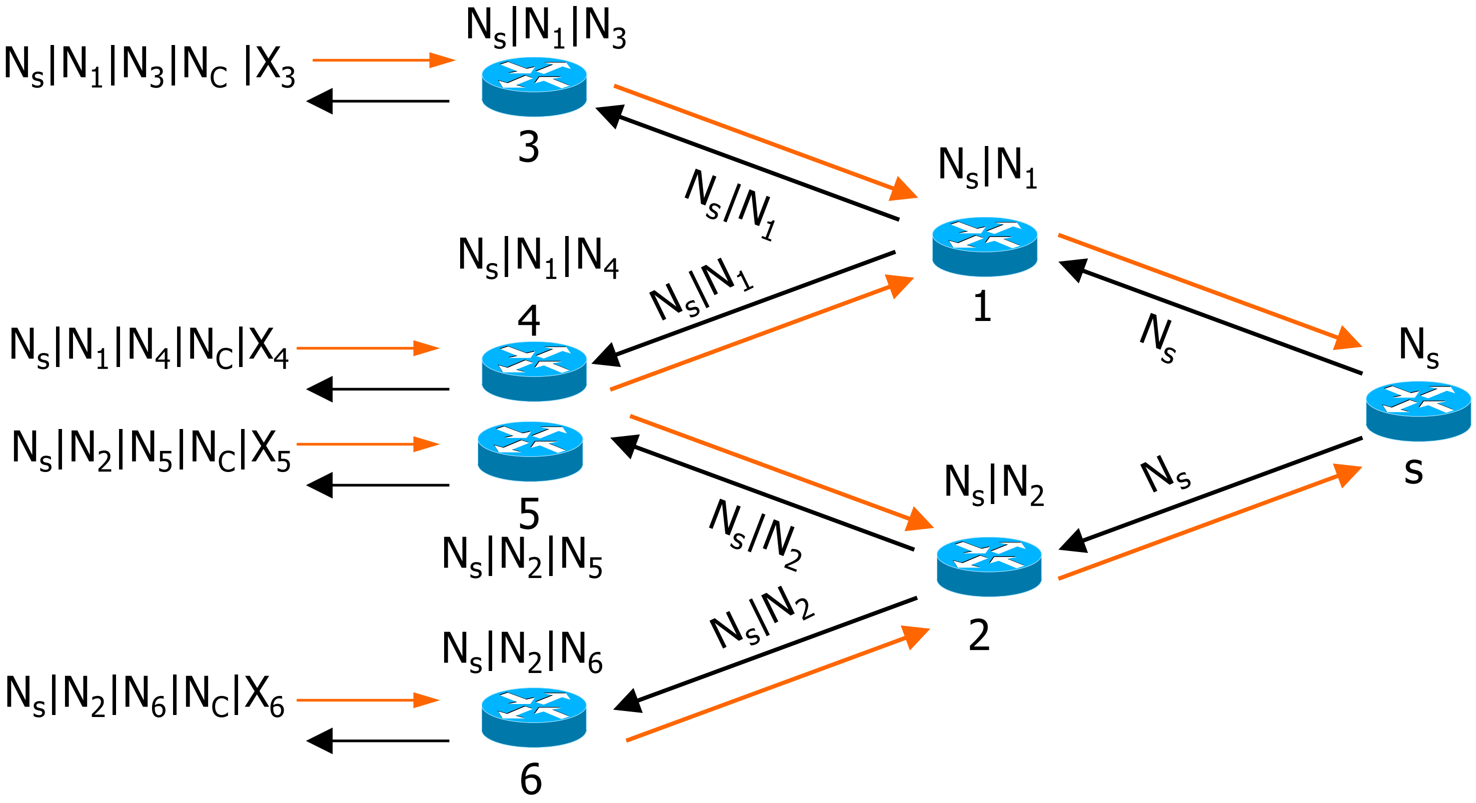
Distributed puzzle mechanism



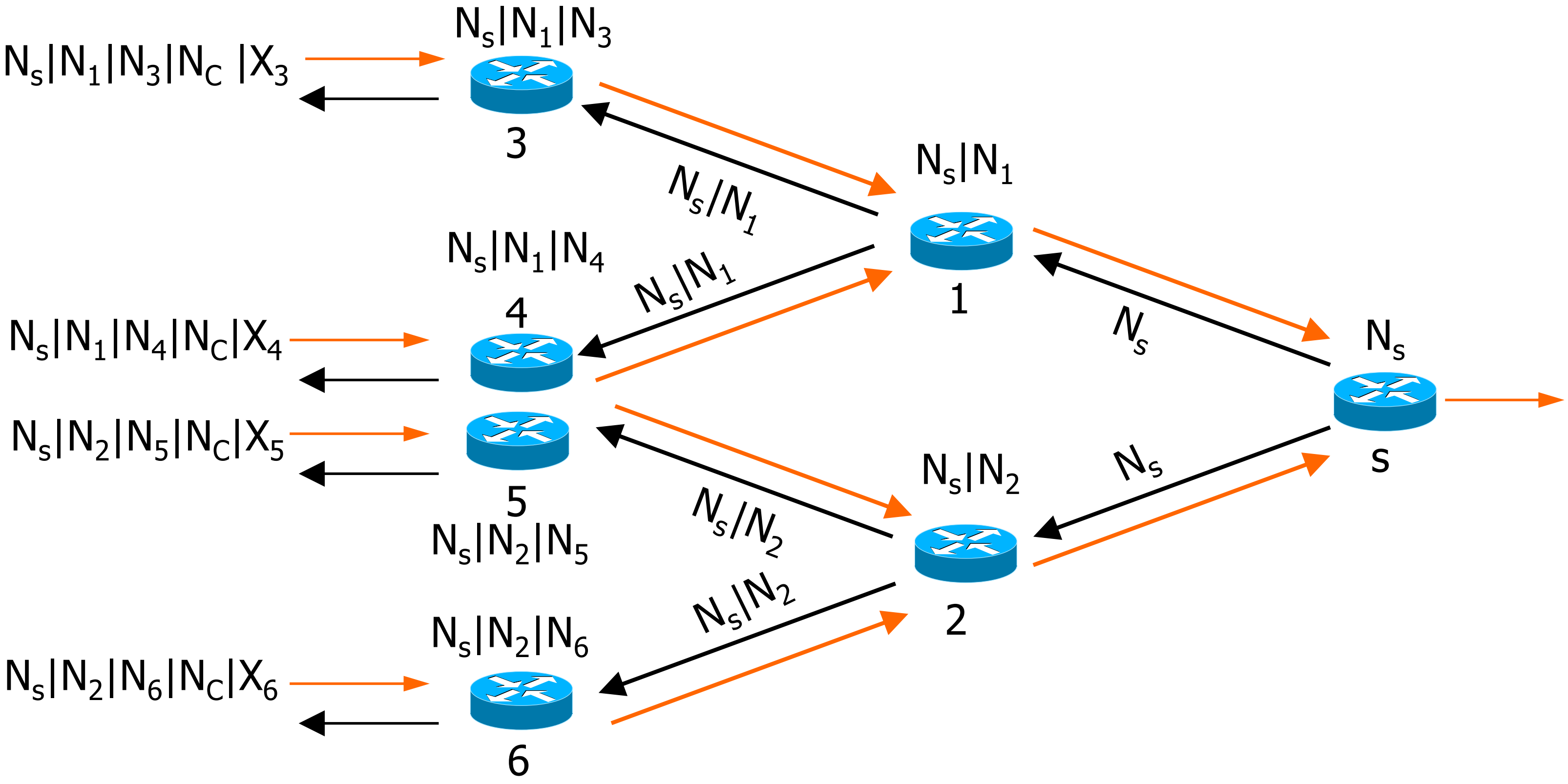
Distributed puzzle mechanism



Distributed puzzle mechanism



Distributed puzzle mechanism



What puzzles can do

- Fairness in resource allocation
  - DoS attacks violate fairness

- Incentives to work with victim to fight against DoS
  - Attacker becomes more difficult to find zombies

What puzzles cannot do

- Very large number of zombies
  - Indistinguishable from flash crowd

- Puzzle-based incentive engineering makes this hard to happen!

DoS defense

➢Acquiring more resources

➢Limiting service requests

⇒Identifying good/bad requests

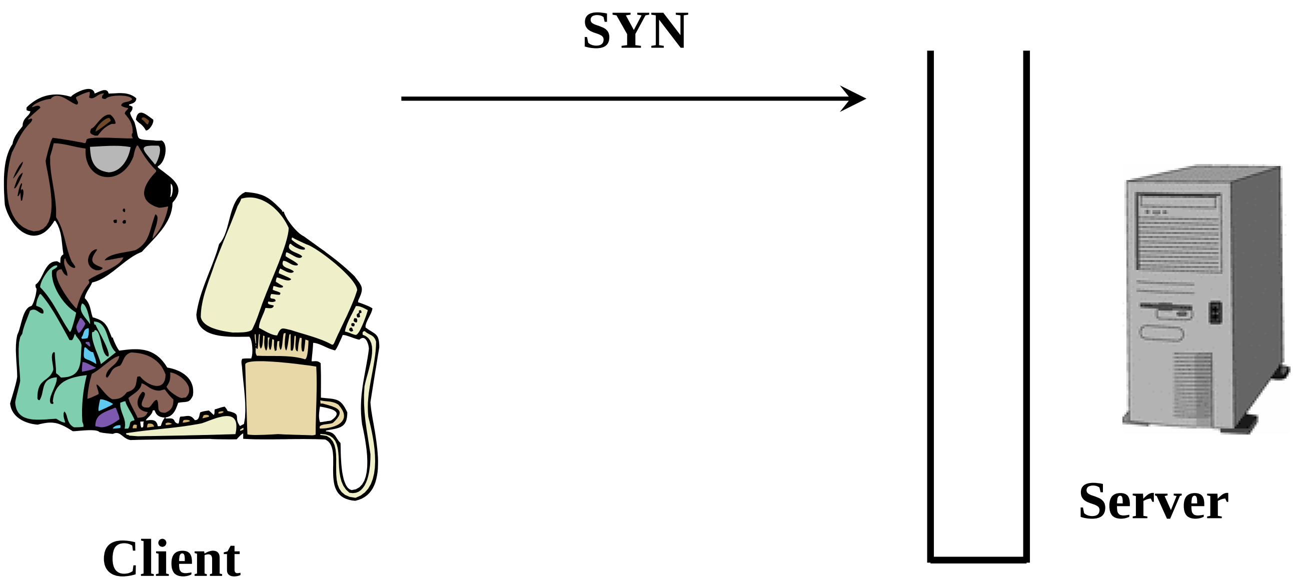
Identifying bad requests

- Syn-cookie
- Traceback
- Filtering
- D-WARD

Syn-cookie

- An implementation in Linux to mitigate the threat of syn-flooding
- Mainly designed for detecting syn packets using spoofed IP addresses

TCP three-way handshaking

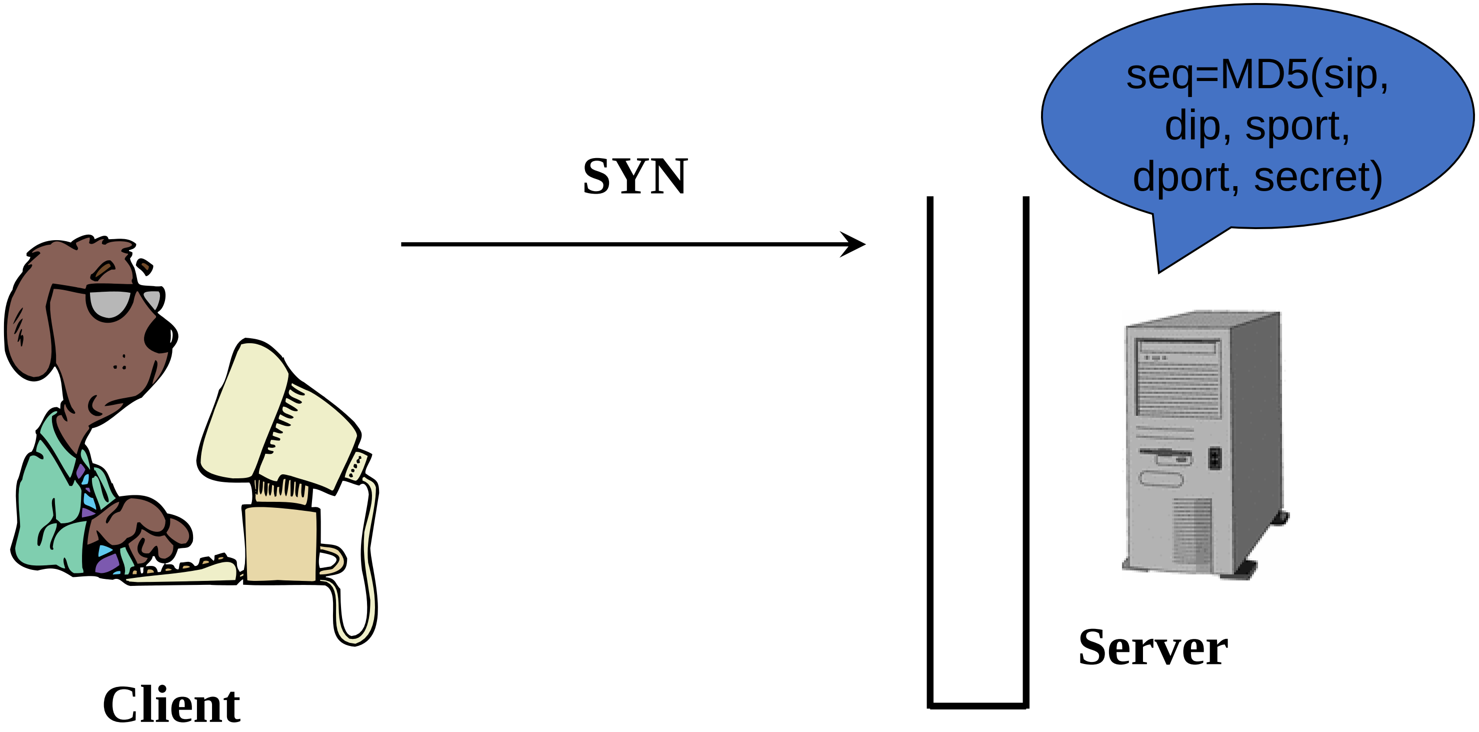


SYN

Client

Server

TCP three-way handshaking



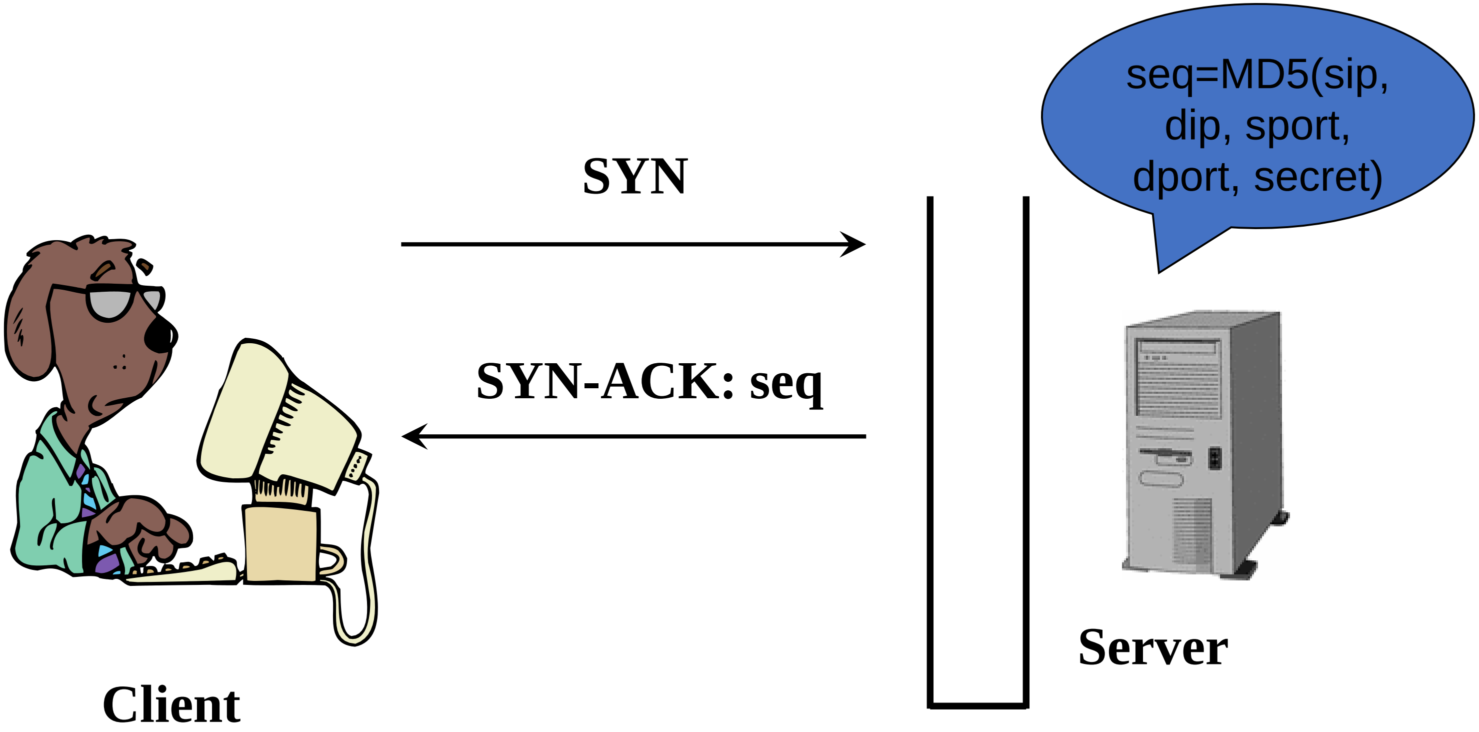
SYN

seq=MD5(sip, dip, sport, dport, secret)

Server

Client

TCP three-way handshaking



SYN

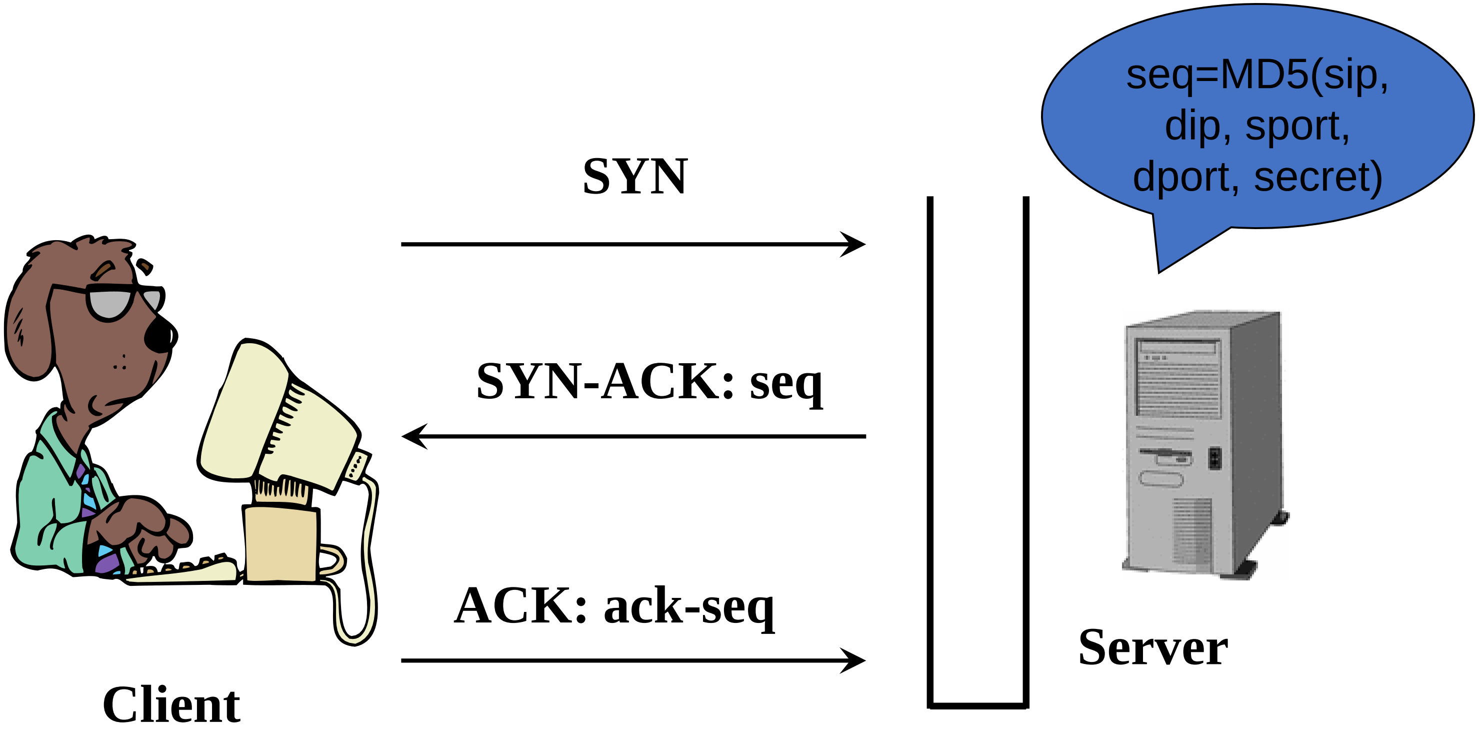
SYN-ACK: seq

seq=MD5(sip, dip, sport, dport, secret)

Client

Server

TCP three-way handshaking



seq=MD5(sip, dip, sport, dport, secret)

SYN

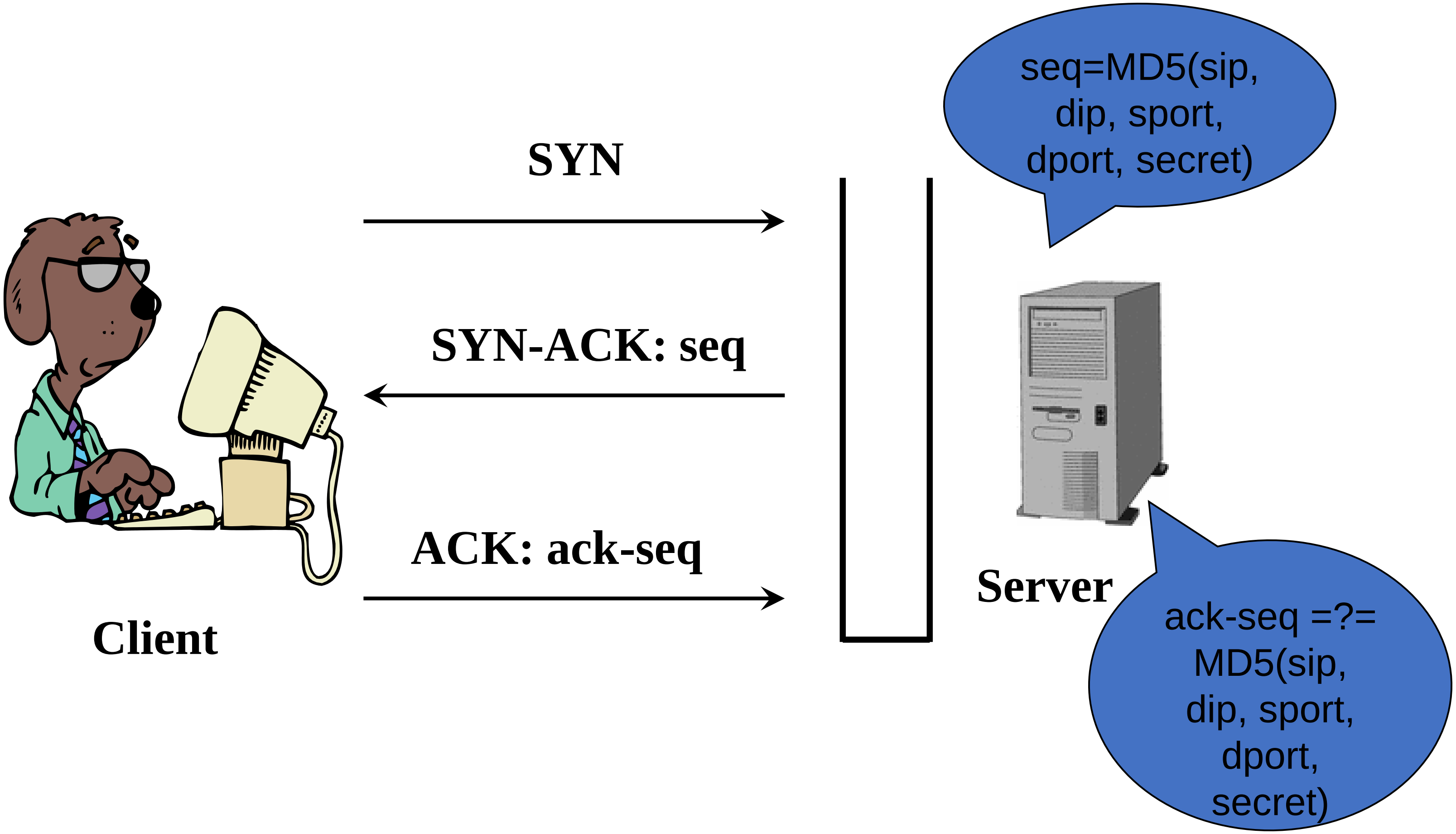
SYN-ACK: seq

ACK: ack-seq

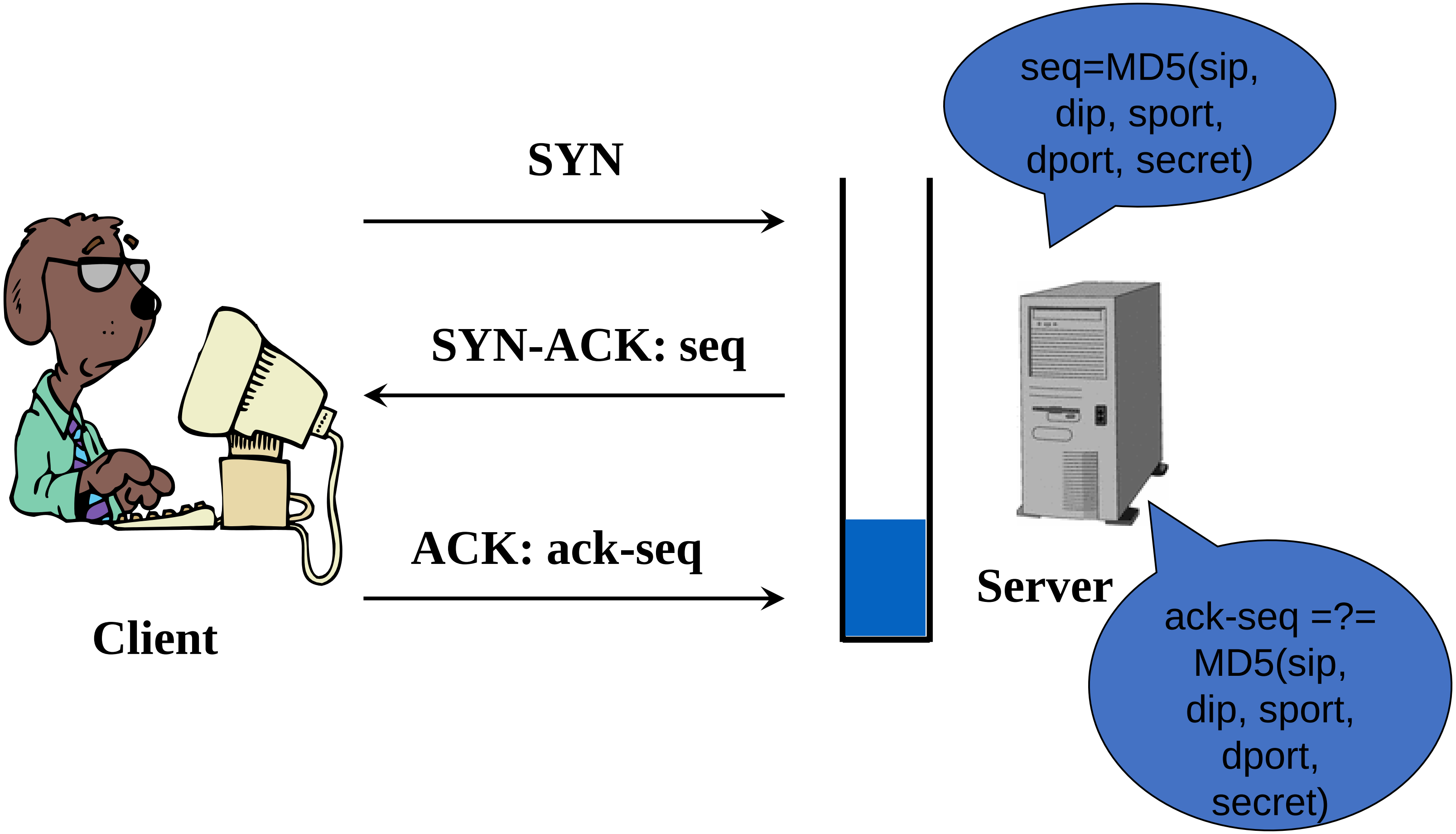
Client

Server

TCP three-way handshaking


SYN
SYN-ACK: seq
ACK: ack-seq
Client
Server
seq=MD5(sip, dip, sport, dport, secret)
ack-seq =?= MD5(sip, dip, sport, dport, secret)

TCP three-way handshaking


SYN
SYN-ACK: seq
ACK: ack-seq
Client
Server
seq=MD5(sip, dip, sport, dport, secret)
ack-seq =?= MD5(sip, dip, sport, dport, secret)

Strength and weaknesses of syn-cookie

- Strength:
  - Practical: It has already been used in the kernel
  - Simple and effective

- Weaknesses
  - Violating TCP semantics
    - Problems occur when packet drops
    - Some applications may not work
  - Not effective in the presence of large number of attackers using authenticate source IP addresses

IP traceback

- Many DDoS attacks spoof IP to hide location of the attacker

- IP traceback attempts to identify the real origin of attack flows
  - Basic idea: each router marks individual packets it forwards, or keeps some trace of these packets

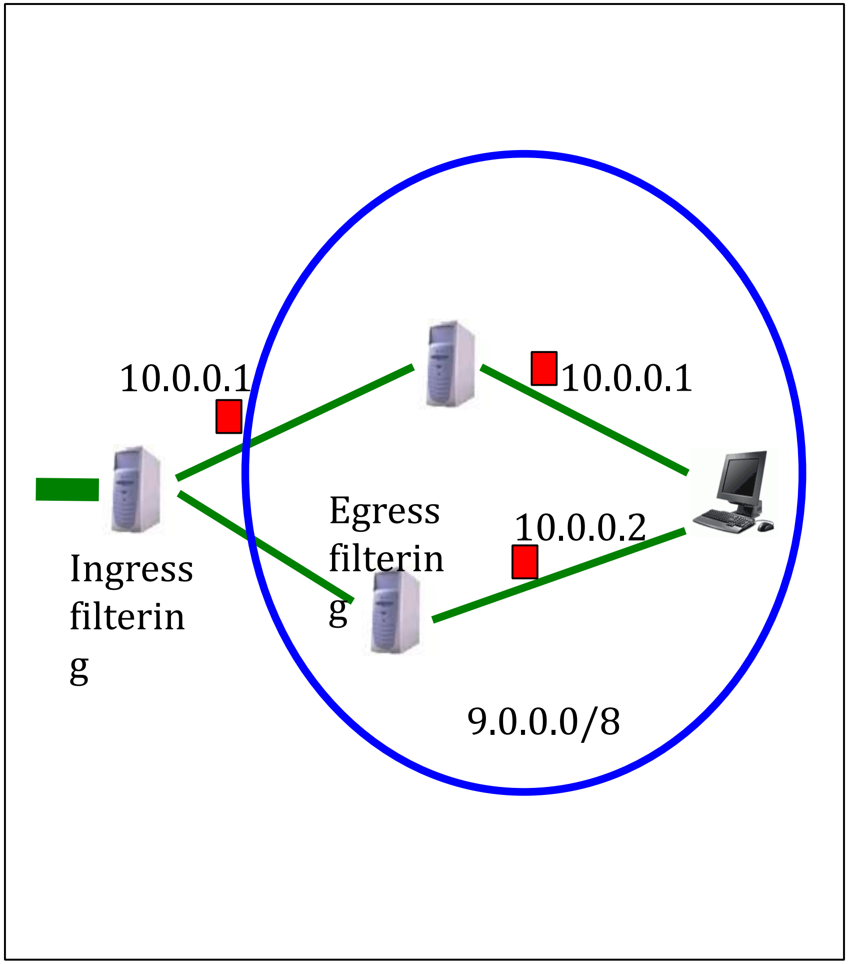
- The same techniques are also used to detect and filter packets using spoofed IP addresses

Weaknesses of IP traceback

- Need large deployment to be effective
- Not effective during the attack
- Only traced back to zombies, not the attacker
- Useless towards attack flows using authentic IP addresses

Ingress/egress Filtering

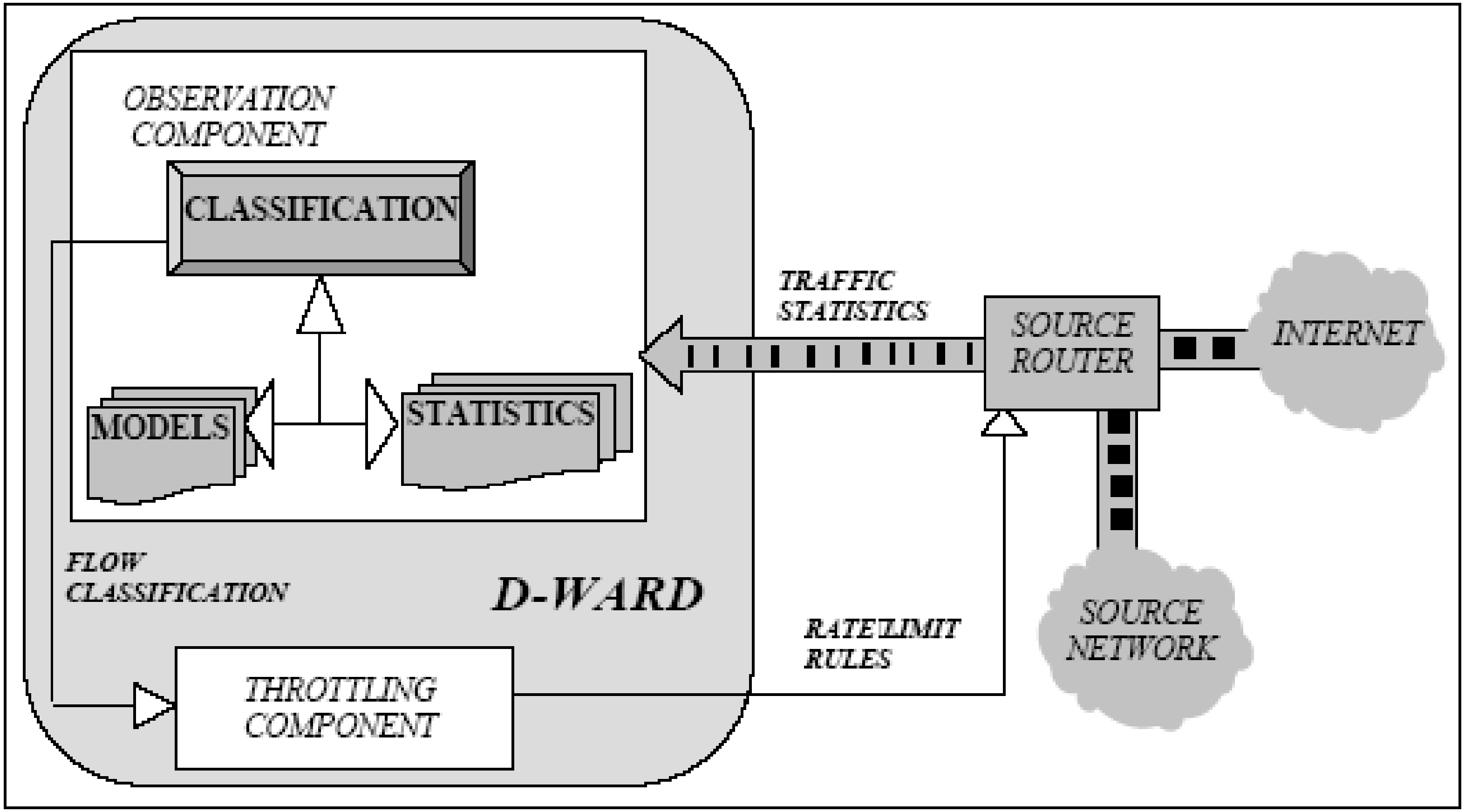
- Ingress filtering
  - To prevent packets with faked source IP addresses from entering the network
- Egress filtering
  - To prevent packets with faked source IP addresses from leaving the network



D-WARD

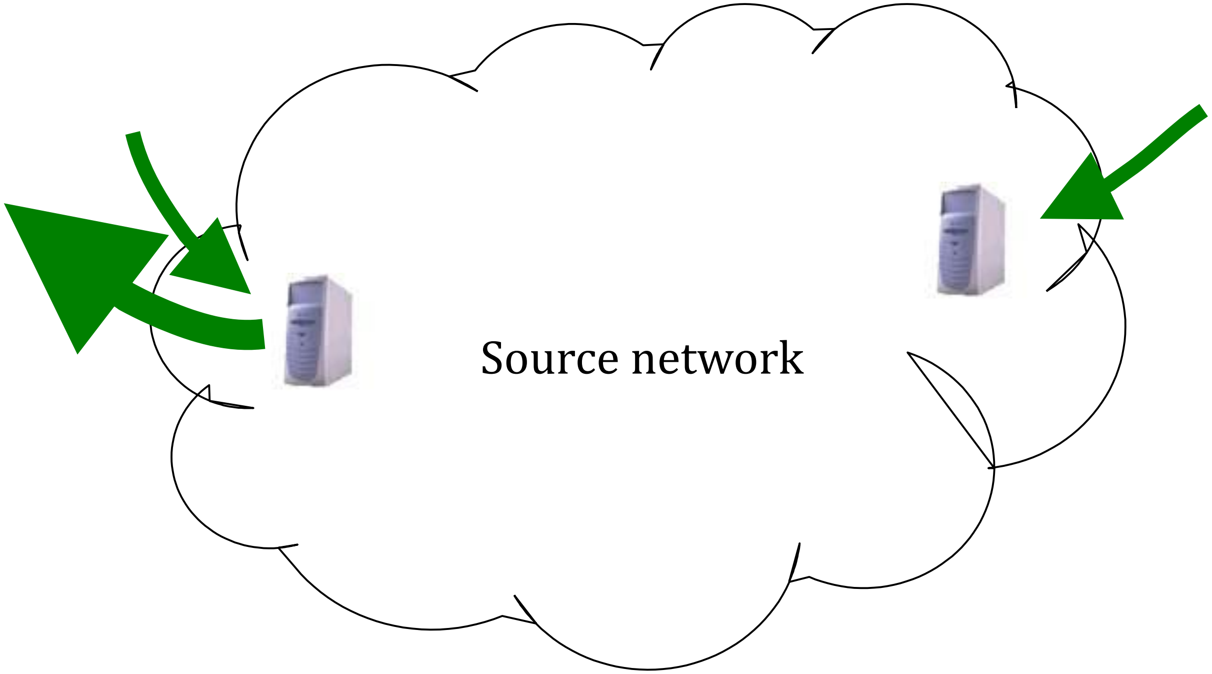
- Deployed at the source router that serves as the gateway between source network and the Internet
- Prevents the machines in the source network from participating in DDoS attacks
- Configured with the police address set
- Monitors two-way traffic between the police address set and the rest of the internet
- Online traffic statistics periodically compared with predefined models of normal traffic
- Non-complying flows are rate-limited
- Guarantees good service to legitimate traffic by monitoring individual connections, regardless of the imposed rate limit

D-WARD Architecture



D-WARD weaknesses

- Motivation of deployment
- Asymmetric problems



Hop-counting filtering

- Using TTL to detect packets with spoofed IP
  - TTL is a field on IP header
  - Every router a packet passes by decrements TTL by 1
  - A router drops the packets with TTL=0
- TTL values are bound to the hops between a client and a server
  - There are only a small number of initial TTL settings in operating systems
- Using TTL and IP mapping to detect spoofed IPs

Strength and weaknesses of Hop-counting

- Simple, easy to implement

- However
  - Just raise the bar to the attacker a little bit
  - Filtering may not work in the presence of link saturation (bandwidth exhaustion) attacks

Identifying good requests

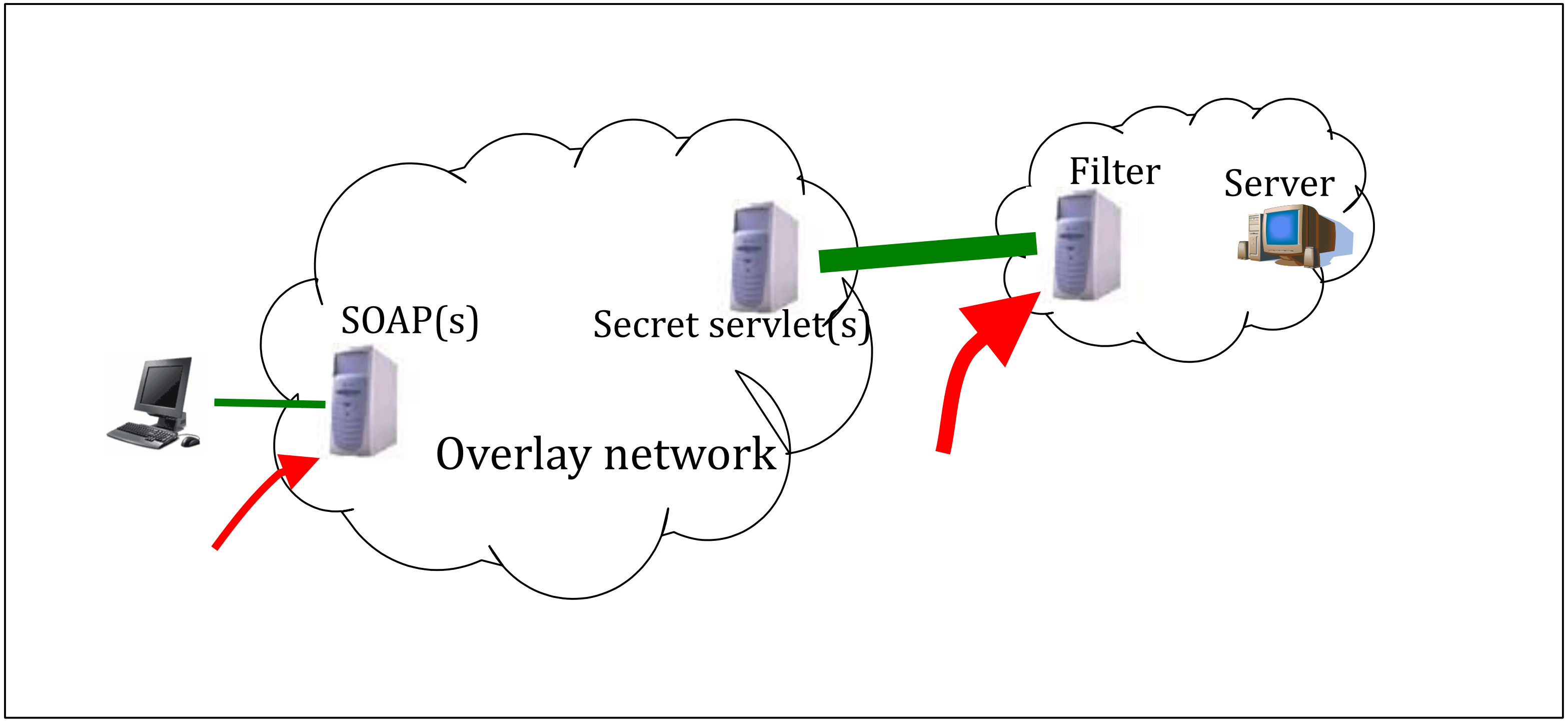
- Secure Overlay Systems

- Access control

SOS – Security Overlay Service

- To protect a dedicated server from DDoS attacks
- Use high-performance filters to drop all the packets not from secret servlets
- Path redundancy in overlay network is used to hide the identities of secret servlets
- Legitimate users enter the overlay network at the point of SOAP (secure overlay access point)

SOS (cont.)



Strength and Weaknesses

- Strength
  - Attacker needs to take down all the entrance nodes to DoS the server

- Weaknesses
  - Deployment difficulty
  - Modification of routing structure

Access control

- Server can grant some privileged clients capability token
- Clients embed the capability tokens to the packets sent to the server
- Routers of the server's ISP checks individual packets, and treats these packets according to their access privileges

Strength and weaknesses

- Strength
  - Allow the end server to determine the routing privileges of the packets it receives

- Weaknesses
  - During flooding, legitimate but yet unprivileged clients cannot access the server
  - Clients need to change software