Denial of Service

Tom Chen
SMU
tchen@engr.smu.edu

Outline

- Introduction
- Basics of DoS
- Distributed DoS (DDoS)
- Defenses
- Tracing Attacks

Introduction

What is DoS?

- 4 types of DoS attack
  - Resource starvation -- disrupt a resource on a particular machine
    - Example: consume CPU cycles, memory
  - Bandwidth consumption -- block all network access by flooding traffic
    - Usually distributed DoS (DDoS) used for flooding

What is DoS (cont)

- Programming flaws -- failure of application or operating system to handle exceptional conditions
  - Example: very long data input
- Routing and DNS attacks
  - Change routing tables or DNS caches

Recent Cases

- August 17, 1999 U. Minnesota campus network shut down by DoS attack
- February 7, 2000 DoS shut down Yahoo, eBay, Amazon, Buy.com, CNN, other Web sites
- October 21, 2002 DoS against Internet root name servers (up to 150,000 pings/ second)

Recent Cases (cont)

- January 2004 DDoS against SCO Web site
  - SCO unpopular for lawsuits against Linux
- June 2004 DDoS against Akamai's servers

Recent Cases (cont)

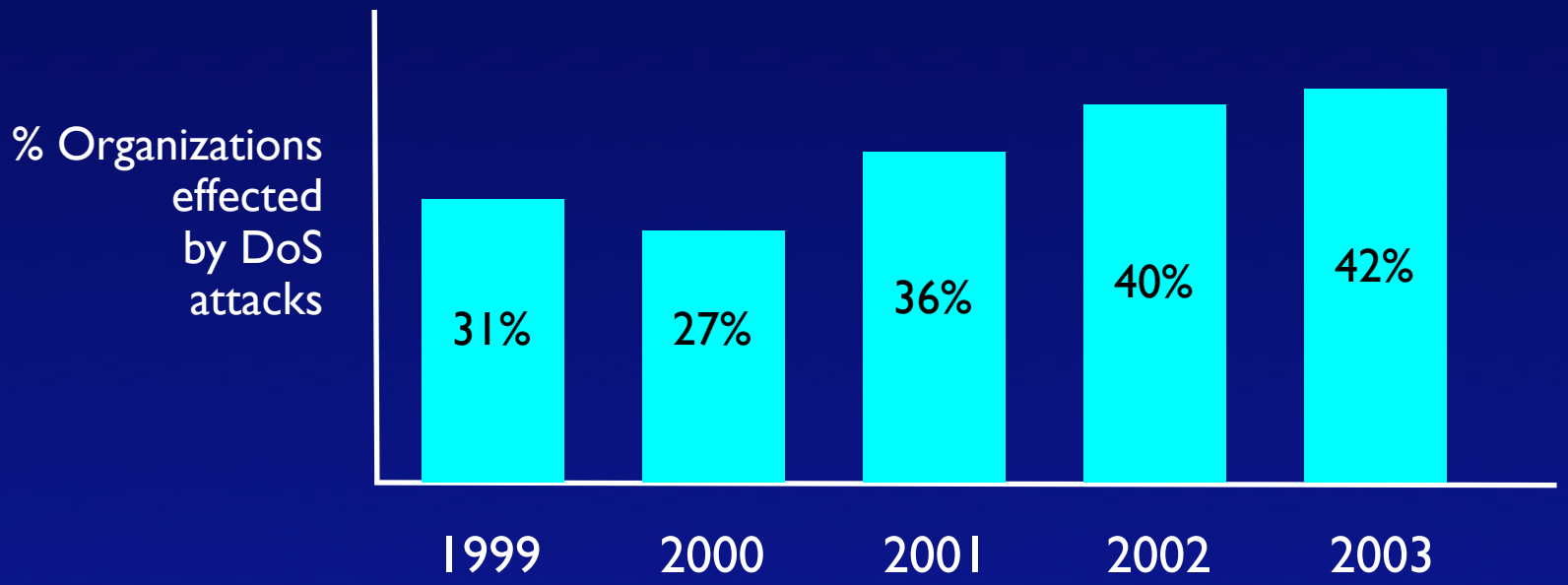
- Jan. 2004 - today: DDoS attacks against online gambling Web sites, to extort money
  - Nov. 2003 British police arrested suspects in Latvia
  - 20 July 2004 Russian and British police arrested extortion group in St Petersburg
  - Believe many other groups worldwide

Goals and Motivations

- Unlike most security attacks, goal is not control of computers
- Goal is usually revenge or extortion, but any motives are possible
- DoS attacks get little respect from hackers (because too easy), but can be highly effective

Prevalence

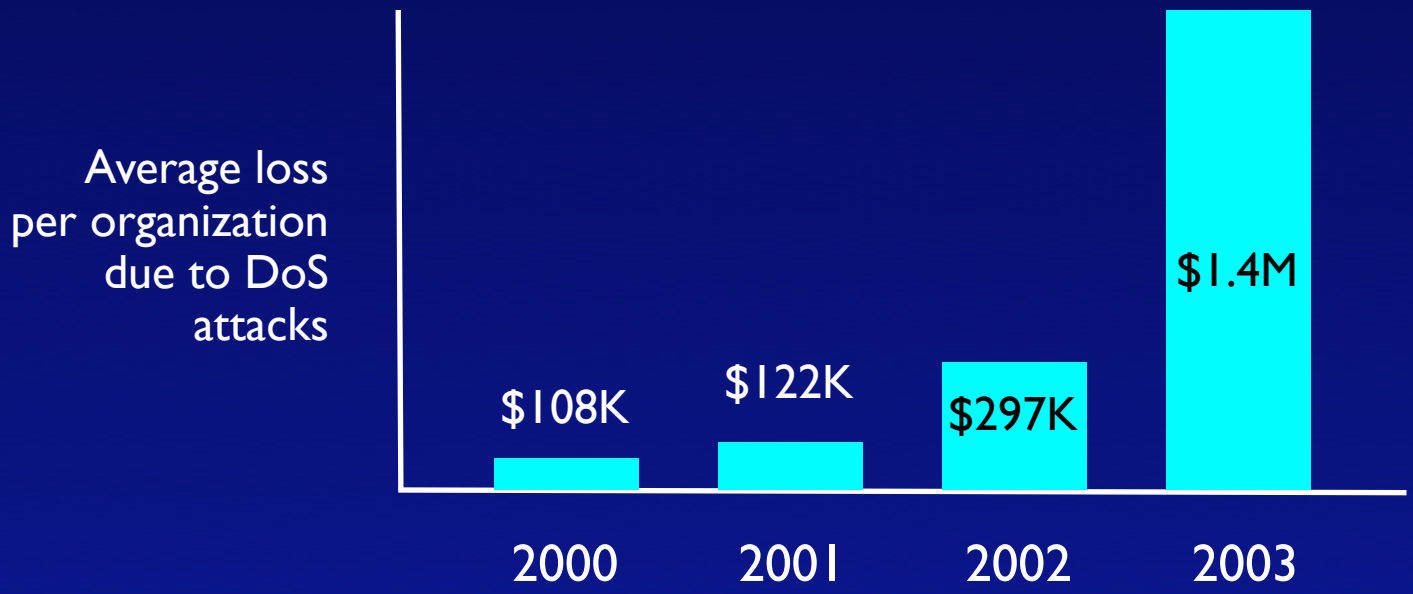
- DoS attacks are common



*2003 CSI/FBI Computer Crime and Security Survey

Damage Costs

- DoS is costly to organizations (second behind theft of proprietary info.)



*2003 CSI/FBI Computer Crime and Security Survey

Basics of DoS

Direct Attacks - Land

- Land attack: IP packet with source address same as destination address
  - Target Windows NT before Service Pack 4
- Causes machine to loop, consuming CPU cycles

Direct Attacks - Teardrop

- Teardrop attack: overlapping IP fragments
  - Target old Linux systems, Windows NT/95
- Some systems cannot reassemble overlapping IP fragments properly -- could cause system to reboot or crash

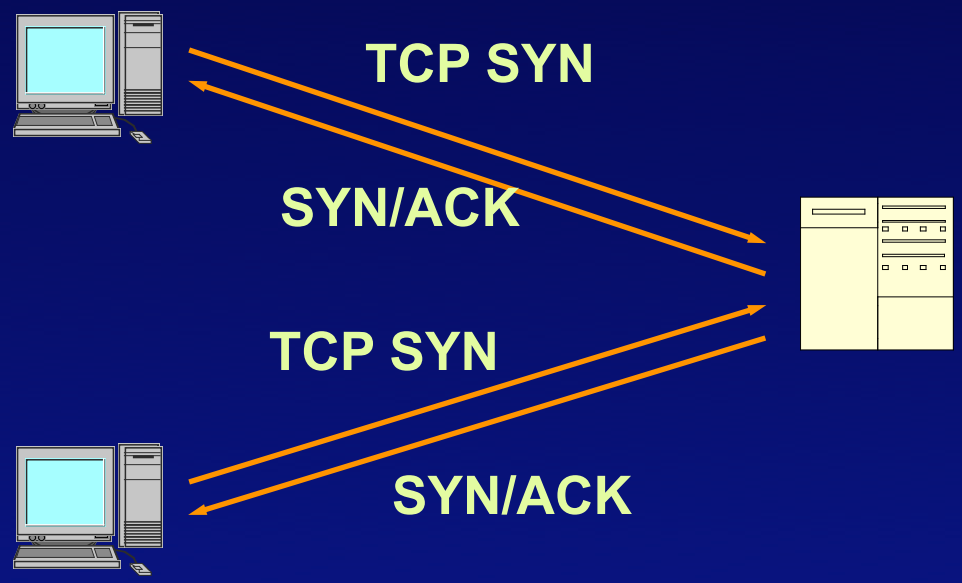
Direct Attacks- Ping of Death

- Ping of death attack: ICMP ping message longer than 65,536 bytes
  - Target early versions of various operating systems
- Some systems could crash or freeze

Direct Attacks - SYN Flood

- SYN flood attack: many TCP SYN requests but no SYN/ACKs
  - Target any system
- Target starts to open many TCP (half-open) connections
- Number of half-open connections is limited -- then machine cannot open any real connections

SYN Flood (cont)

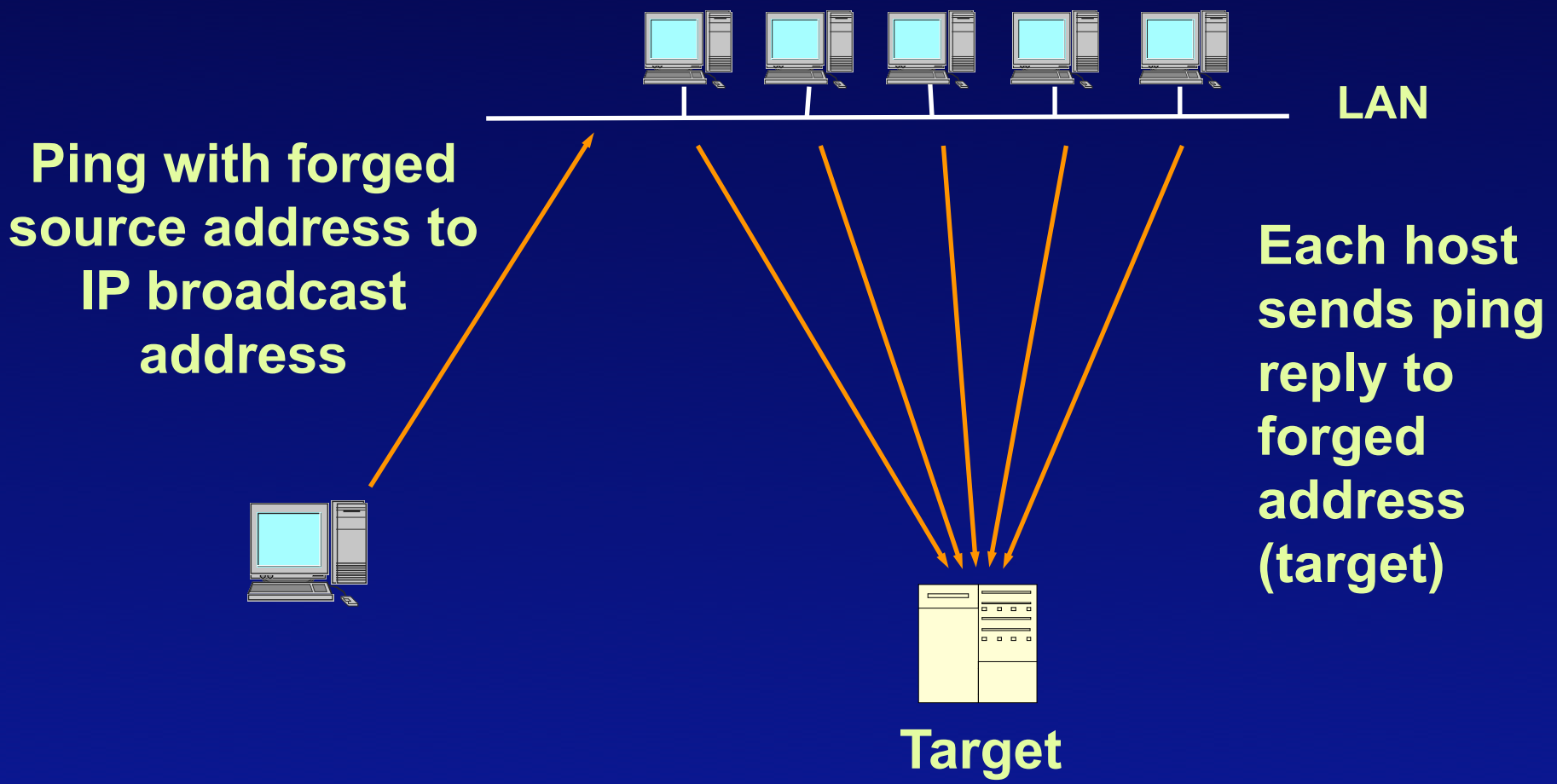


Target keeps half-open connections, waiting for SYN/ACK to complete connections

Indirect Attacks - Smurf

- Smurf attack: ICMP echo request (ping) with fake source IP address to IP broadcast address
  - Fake source address is target
  - Computers must return ICMP echo replies
  - Works with any systems

Smurf (Reflector) Attack



Smurf (cont)

- One packet is “amplified” (multiplied) into many
- Attacker’s address is not seen
- Many innocent machines are used for attack
- Some LANs restrict or disable broadcast address

Distributed DoS (DDoS)

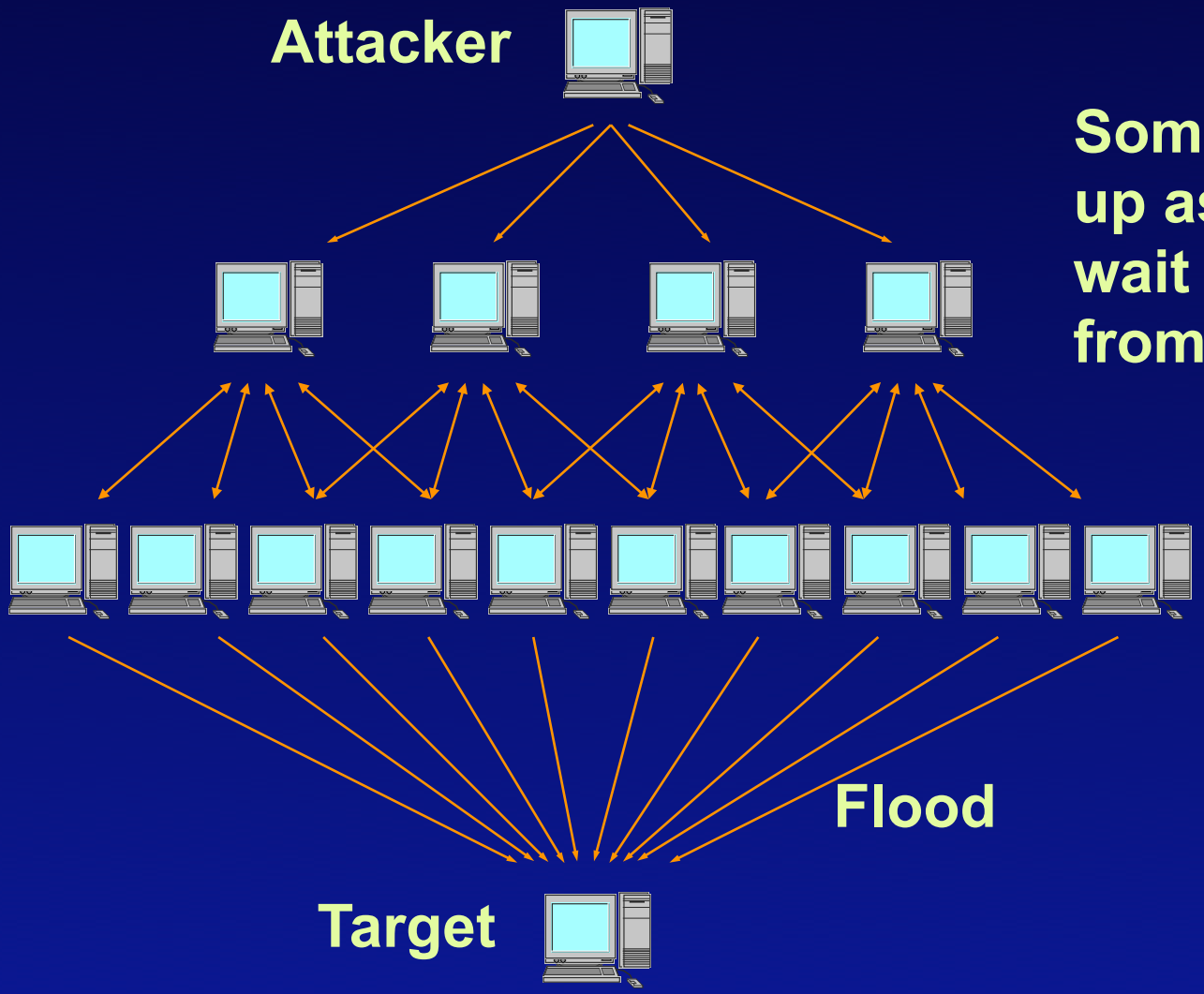
Trend to DDoS

- Nov. 1999 CERT workshop report warned that new distributed DoS tools will make DDoS attacks easier and more common
- 7 Feb. 2000 DDoS attacks took down Yahoo, e*Trade, eBay, Buy.com, CNN.com for several hours
- DDoS attacks are now common

What is DDoS?

- 2-phase attack
- Stealthy preparation: many computers (often home PCs with broadband) are infected with DoS agent (Trojan horse)
- Attack: computers are instructed to flood traffic to target

DDoS network



Some hosts are set up as “masters”, wait for commands from attacker

Many “daemons” wait for commands from masters

DDoS Concerns

- Automated DDoS tools easy to find
- DDoS attack can be launched with single instruction
- Attacker is not directly involved during attack -- hard to trace
- Many innocent computers are compromised (maybe 10,000-100,000)

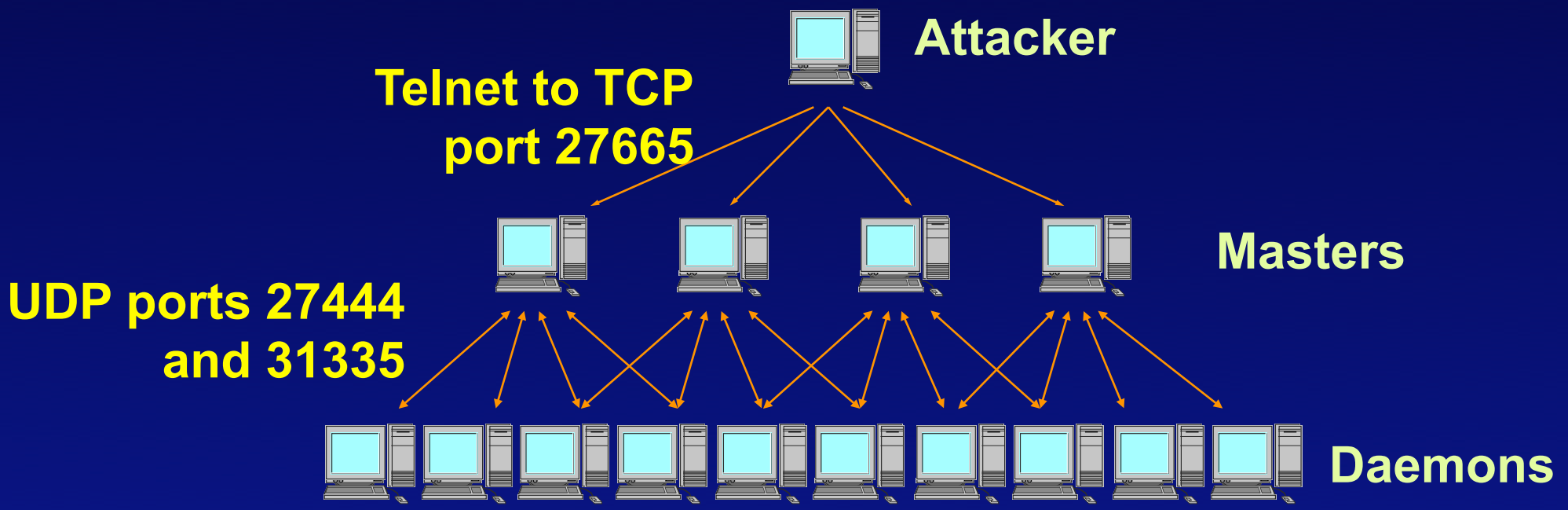
DDoS Tools

- Trin00
- TFN
- TFN2K
- Stacheldraht
- Worms: Code Red, Nimda, Lion,…

Trin00

- Trin00 was used in August 1999 DDoS attack on U. of Minnessota
- Attacker steals an account to use
- Takes over Solaris and Linux systems with buffer overflow attack
  - A few are chosen as “masters”
  - The others are chosen as daemons

Trin00 network



Trin00 (cont)

- Masters understand various commands:
  - Start/stop DoS an IP address
  - Set attack time/duration
  - Ping daemons
  - Disable daemons
  - List daemons

Trin00 (cont)

- Daemons understand commands:
  - DoS an IP address
  - Set attack time/duration
  - Ping request
  - Shut down
- DoS attack is UDP flood to random ports

TFN (Tribe Flood Network)

- Similar to Trin00 with more capabilities:
- More ways for attacker to communicate with masters
- ICMP is used between masters and daemons, instead of TCP, because network monitoring tools sometimes do not look into ICMP data field

TFN (cont)

- More types of attacks:
  - UDP flood
  - ICMP echo request flood
  - SYN flood
  - Smurf attack

TFN2K (TFN 2000)

- More capabilities added to TFN:
- Randomly chooses TCP, UDP, or ICMP for messages
  - More difficult to track TFN2K traffic
- All traffic is one way (attacker to masters, masters to daemons)
  - Daemons never transmit, not even acknowledgements -- harder to detect

TFN2K (cont)

- Masters transmit commands 20 times, hoping daemons will receive at least once
- Random decoy messages are sent to confuse any network monitoring
- Messages are encrypted for privacy
- Teardrop and Land attacks are added

Stacheldraht

- Stacheldraht (German for “barbed wire”) based on TFN with added features
- Attacker uses encrypted telnet-like connection to send commands to masters
- Daemons can upgrade on demand by download new program code

Defenses

Defenses in General

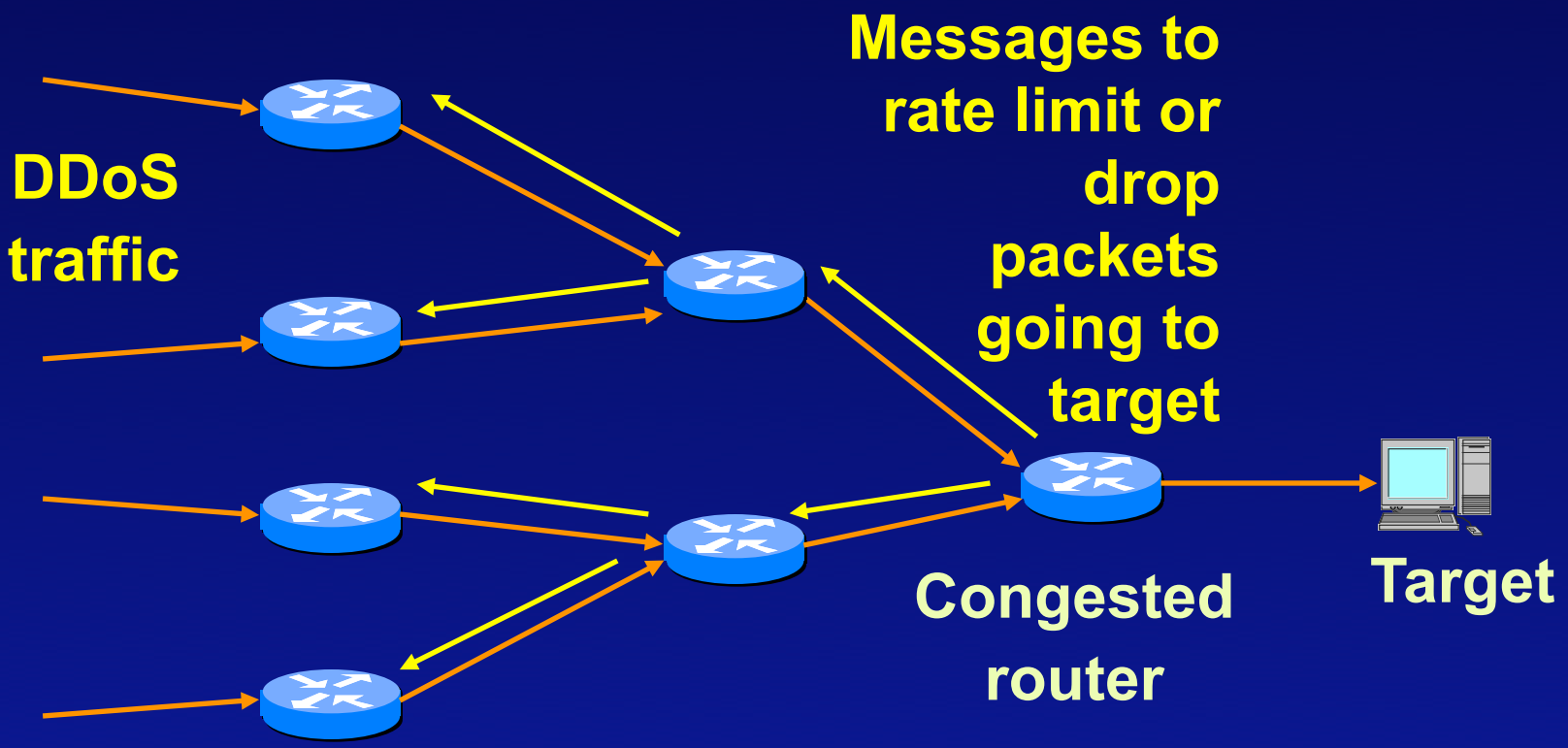
- DoS attacks use various methods, so different defenses are needed
- Land, Teardrop, and ping of death have been fixed in current operating systems
- Current operating systems can detect SYN floods and implement protection
- Directed broadcasts are now usually disabled to protect against Smurf attacks

Defenses in General (cont)

- Defenses against DDoS attacks is most difficult
  - Prevention: specialized tools are available to detect known DDoS tools, but new DDoS tools may be undetectable
  - During attack: firewalls and routers can filter, block, and slow down attack traffic
  - During and after attack: various ideas proposed for IP traceback

Proposed Pushback Scheme

- Backpressure:



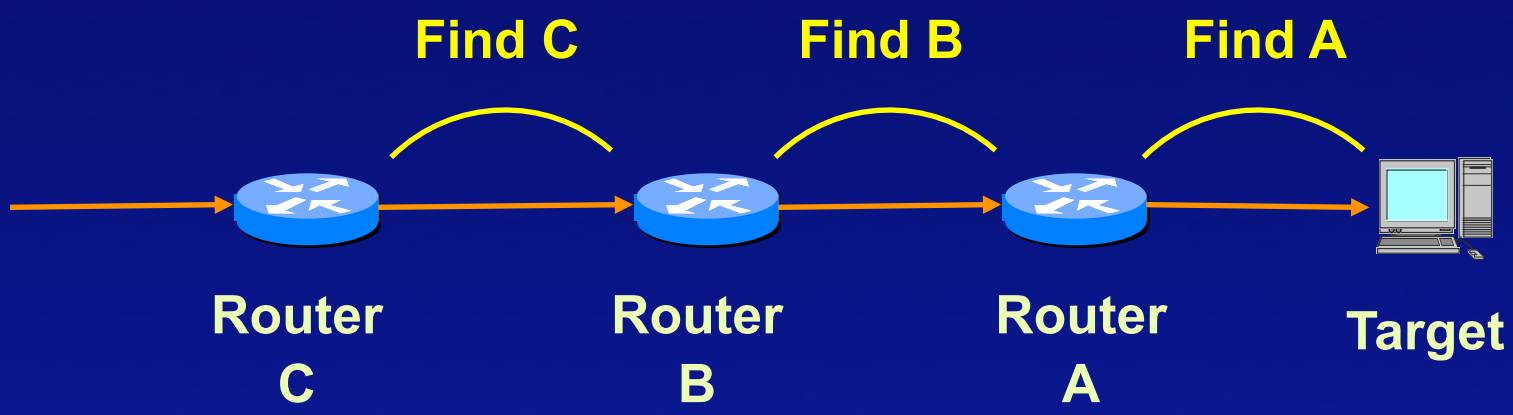
Tracing Attacks

Problem and Difficulties

- IP traceback: to find the real source of DDoS attack when packets are spoofed
- Difficulties
  - Internet not designed for traceback (routers are stateless)
  - DDoS networks have multiple layers -- attacking daemons are innocent victims, not real attacker

Current Traceback

- Today traceback is completely manual -- too slow and complicated
- Log into router A, find traffic coming from router B, log into router B, and so on

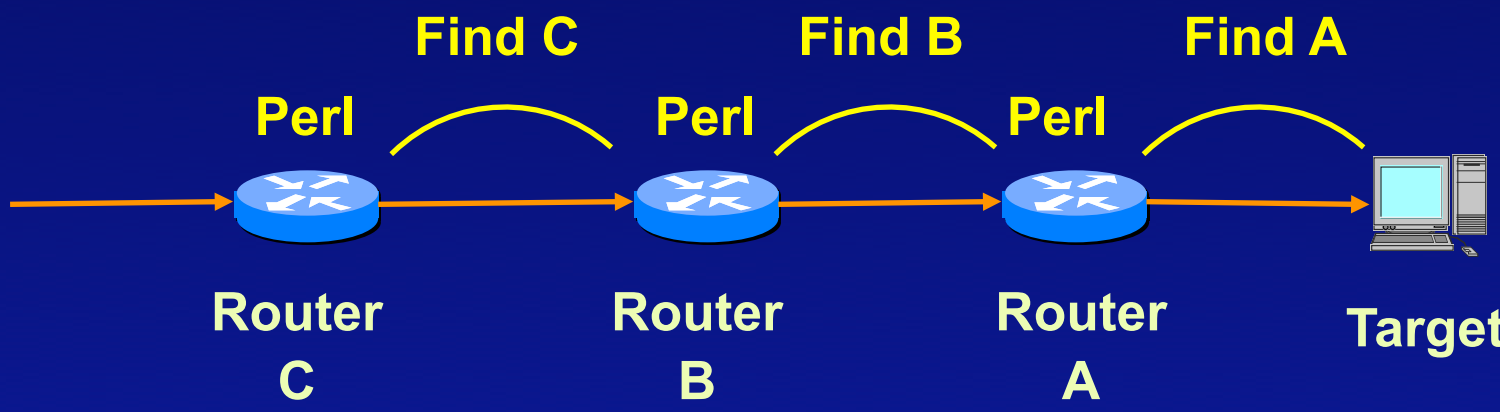


Traceback - Proposals

- Routers record information about forwarded packets for later inquiry
- Routers add information to forwarded packets (packet marking)
- Routers send information about forwarded packets via another channel (e.g., ICMP)

MCI DosTrack

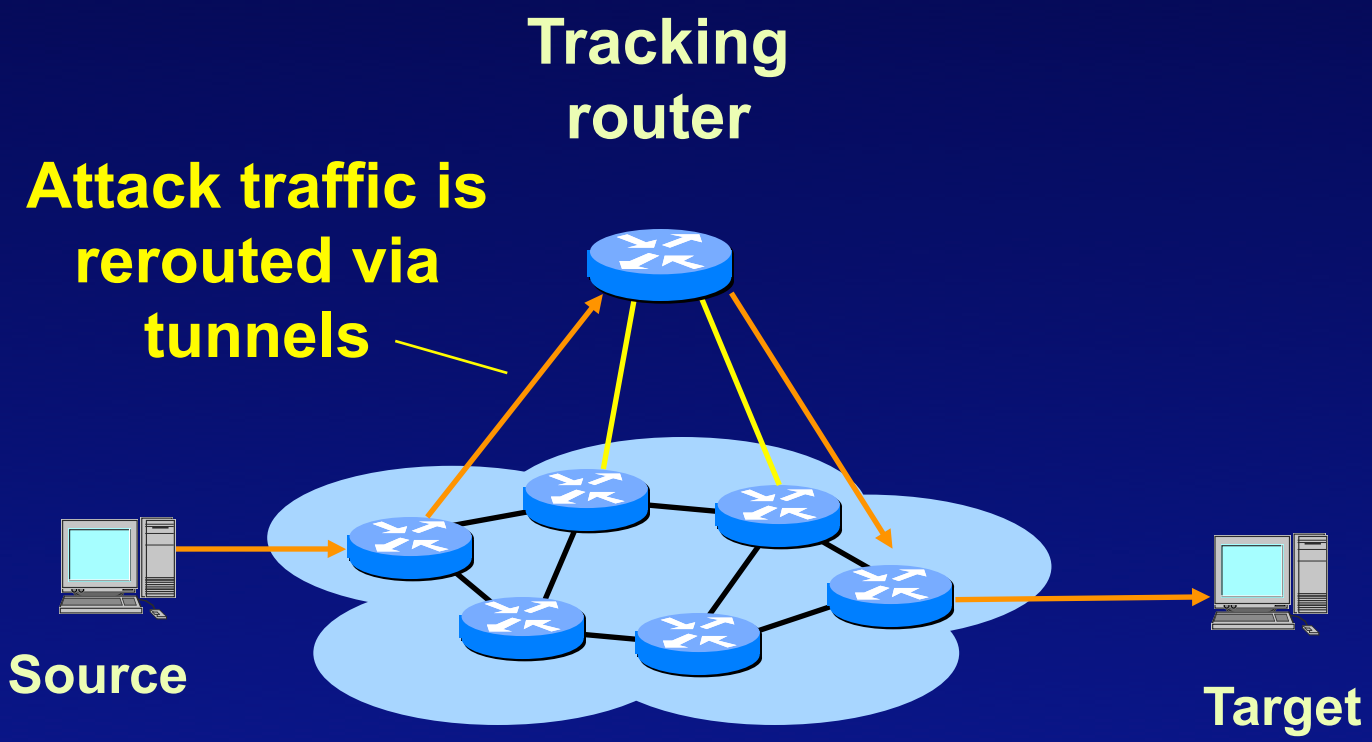
- Automates the manual backtrack process with Perl scripts at routers
- Perl scripts find upstream interface at each router for packets going to target



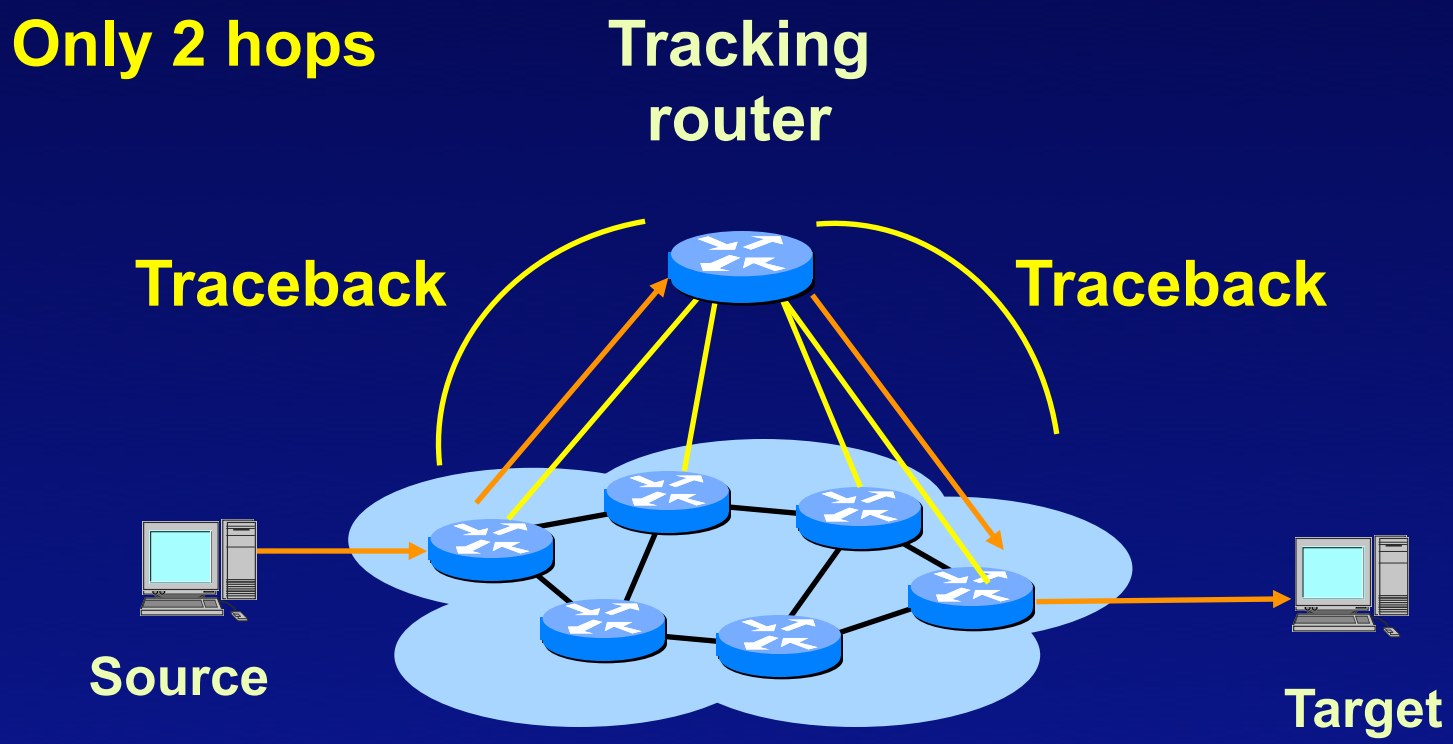
CenterTrack

- DosTrack retraces route hop by hop -- could take long time
- CenterTrack proposes overlay network of IP tunnels to reroute traffic through special tracking routers
  - Tracking routers can retrace more quickly to find edge router near source

CenterTrack



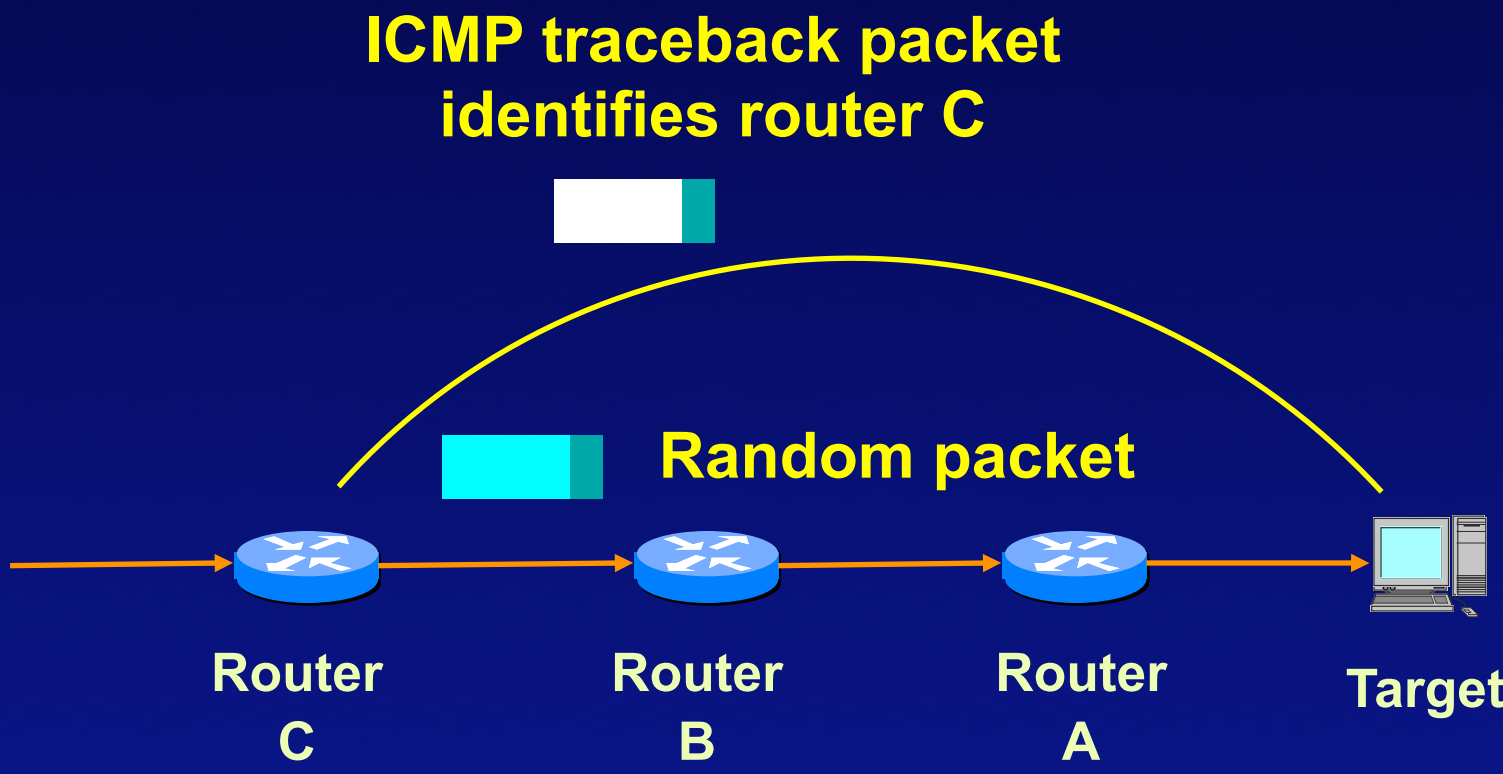
CenterTrack



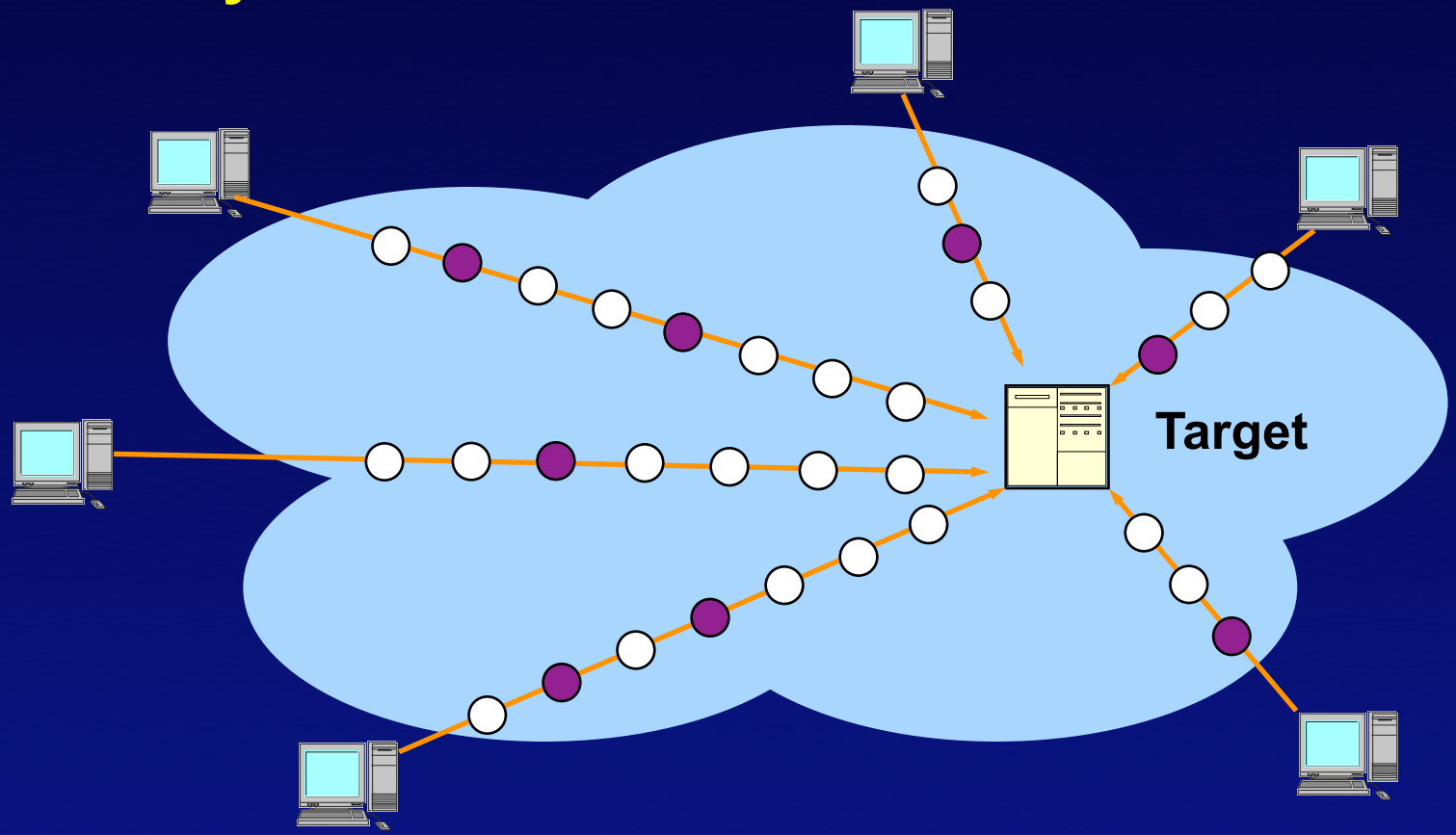
ICMP Traceback

- Proposal for IETF
- Each router chooses a packet randomly, e.g., 1 in 20,000
  - Generates special ICMP traceback packet to follow chosen packet to same destination
  - ICMP traceback packet carries IP address of router

ICMP Traceback (cont)

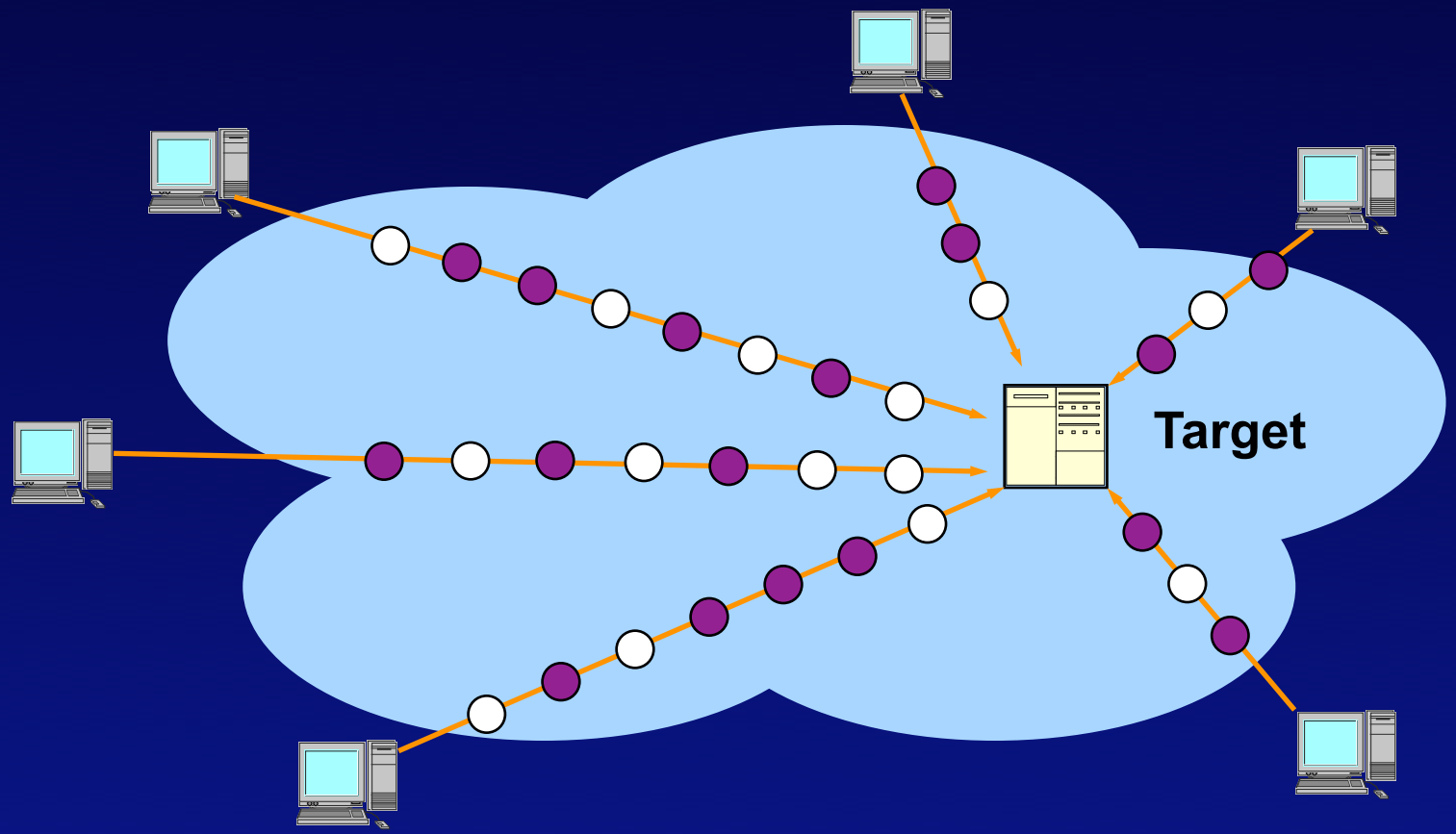


Target discovers a few routers initially



Routers discovered on attack paths

More routers discovered



Routers discovered on attack paths

ICMP Traceback (cont)

- With enough ICMP traceback packets, DDoS target can accumulate info. about routes taken by attack
- Drawbacks:
  - Extra traffic created
  - May be hard to infer routes -- works best for small number of sources
  - ICMP packets may be blocked by firewalls

Hash-based Traceback

- Routers keep a small record of recent packets using a hash function
  - Hash: mathematical thumbprint of packet, virtually unique for every packet
- To trace back, routers ask their neighbors about a packet's hash
  - Packet can be traced hop by hop

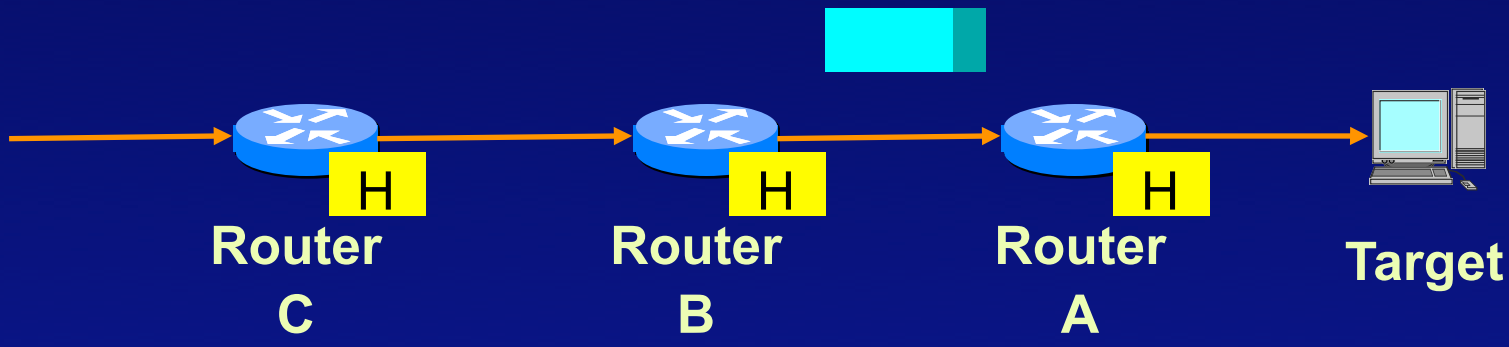
Hash-based Traceback

Packet

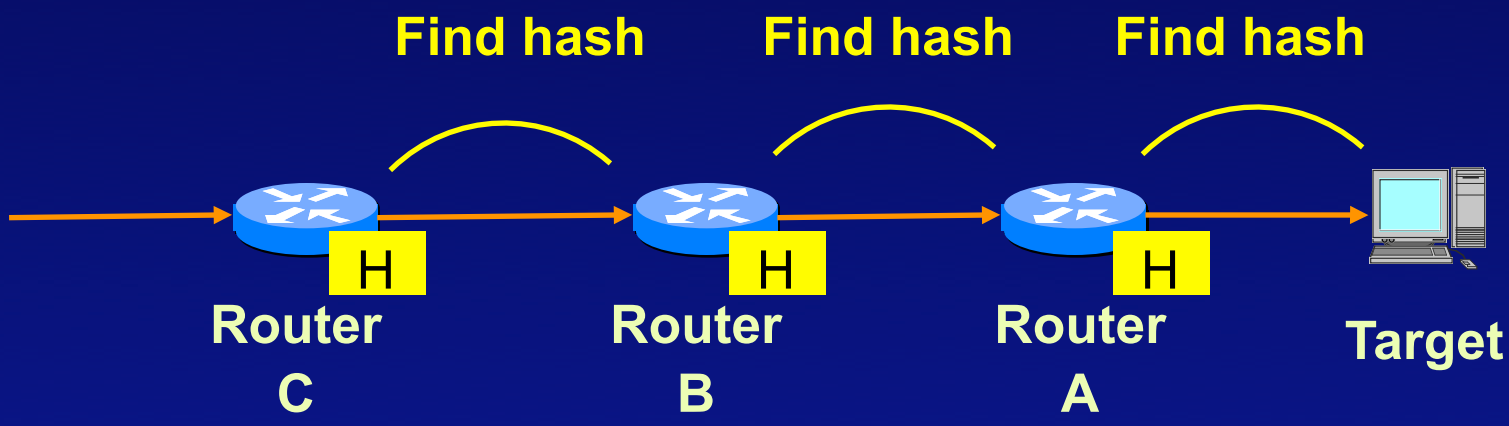
Hash function

H Hash

Packet leaves hash H at each router



Hash-based Traceback



Hash-based Traceback

- No extra traffic
- Disadvantages:
  - Only most recent packets are remembered
    - Traceback must be soon after an attack
  - Tracing is hop by hop -- can take long time for long routes
  - Computation burden (hash) for every packet

Packet Marking

- Advantages:
  - No extra traffic
  - No state info. for routers
  - No need to interrogate routers
- Challenge:
  - Mark packets with enough info. to identify route without changing IP header format

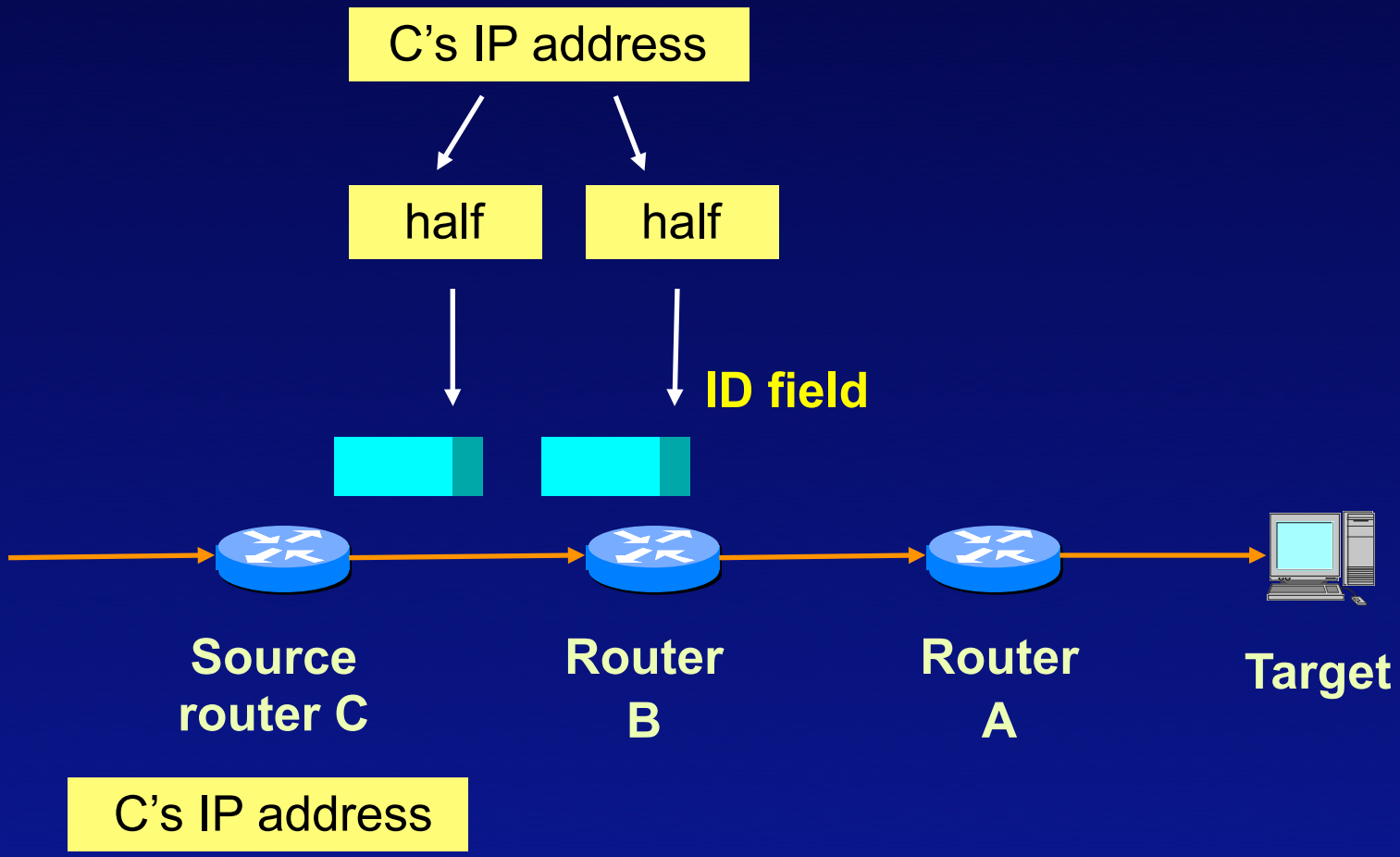
Packet Marking (cont)

- Packet marking can be
  - Deterministic (all packets)
  - Random (subset of packets)

Deterministic Packet Marking

- Each packet is marked upon entry into network to identify source router
- Proposed to use 16-bit identification field for mark, but router IP address is 32 bits
  - Identification field is used for fragmentation, but fragmentation occurs less than 1 percent traffic
  - Need 2 packets to carry router's address

Deterministic Packet Marking



Deterministic Packet Marking

- Computation cost for every packet
- Lost packets can cause errors in traceback (need 2 packets to reconstruct source router's IP address)

Probabilistic Packet Marking

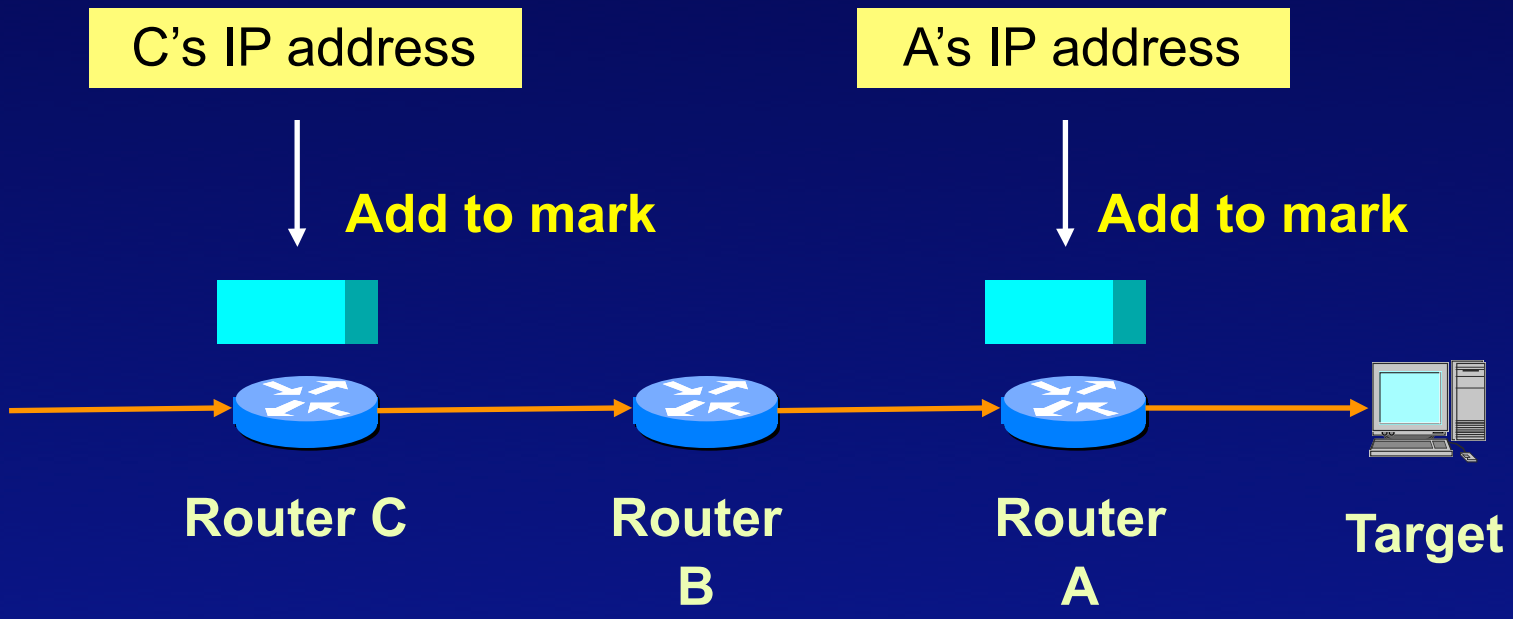
- PPM proposed by U. Washington
- Routers choose packets randomly for marking with some low probability, e.g., 1/25
  - Marked packets are random subset of total traffic

PPM (cont)

- Instead of router address, proposed mark is an “edge” (route segment)
- Edge = <address of first marking router, address of second marking router, distance between the two routers>
  - Edge makes easier to infer entire route than single router address

PPM

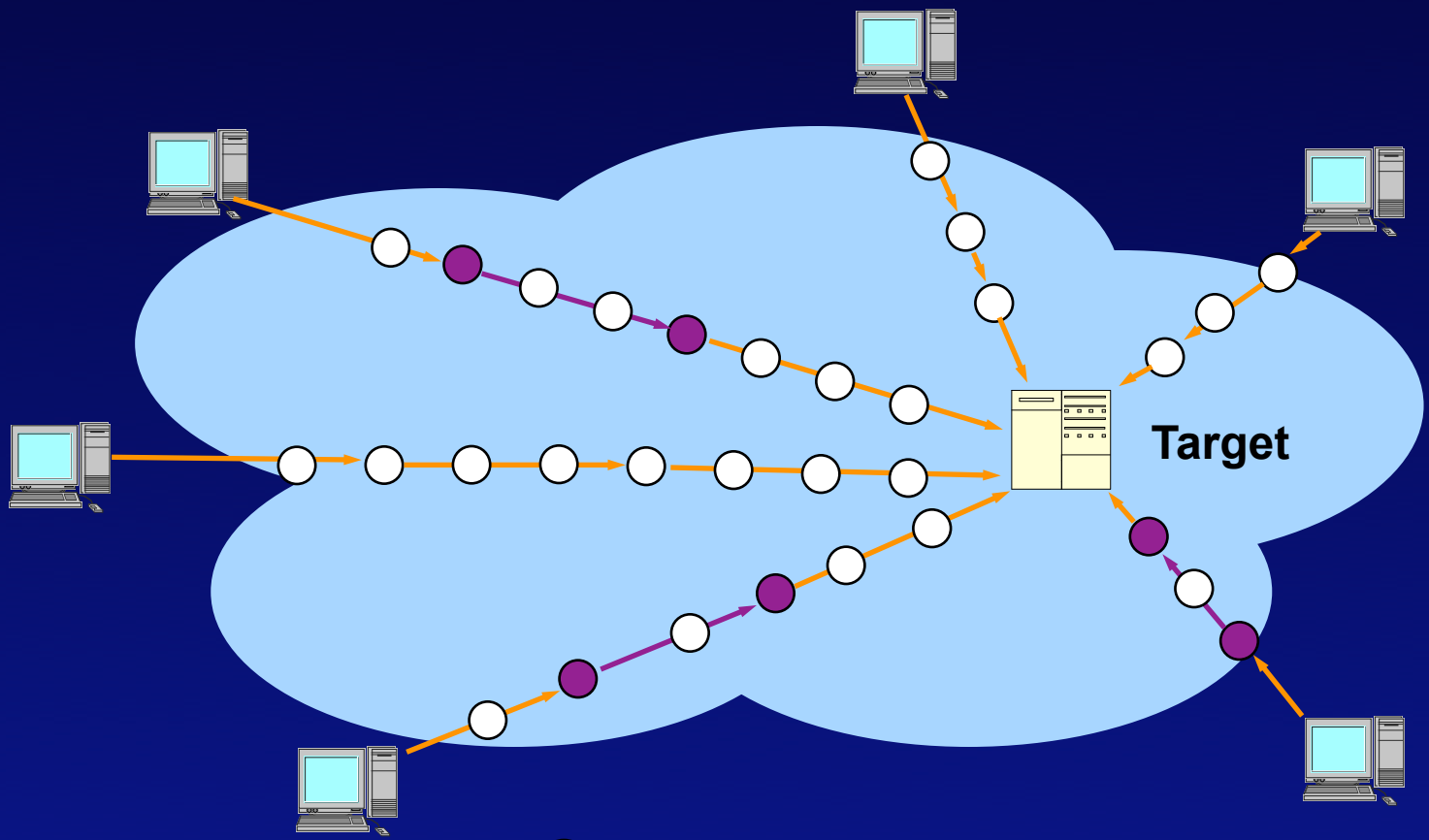
Mark = <C's address, A's address, distance 2>



PPM (cont)

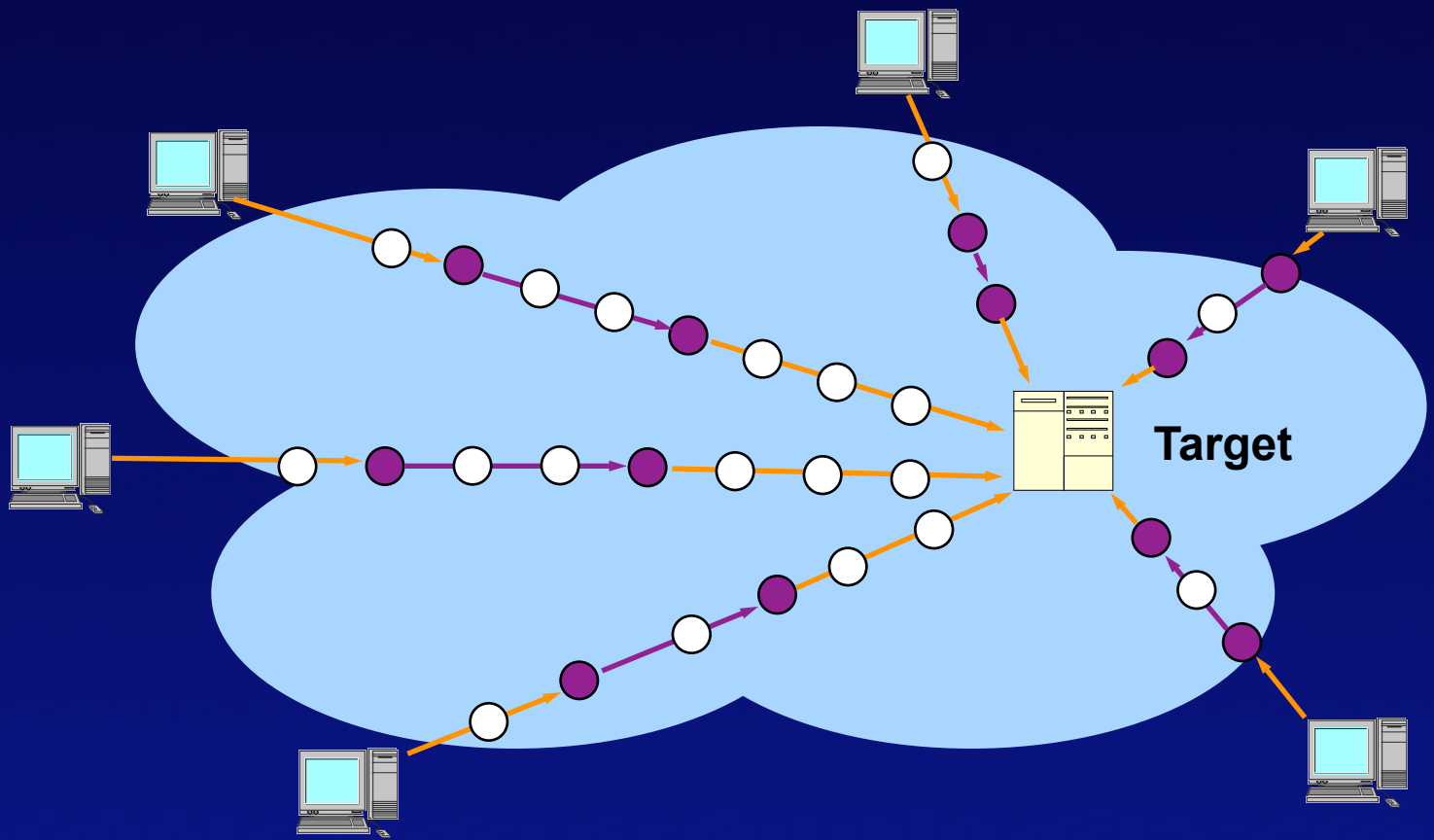
- Mark is put into Identification field in IP header
- 16-bit ID field is too short to carry entire mark
  - Mark is divided into parts, spread over 8 packets
- With enough packets, entire mark can be recovered at destination

Target discovers a few edges initially

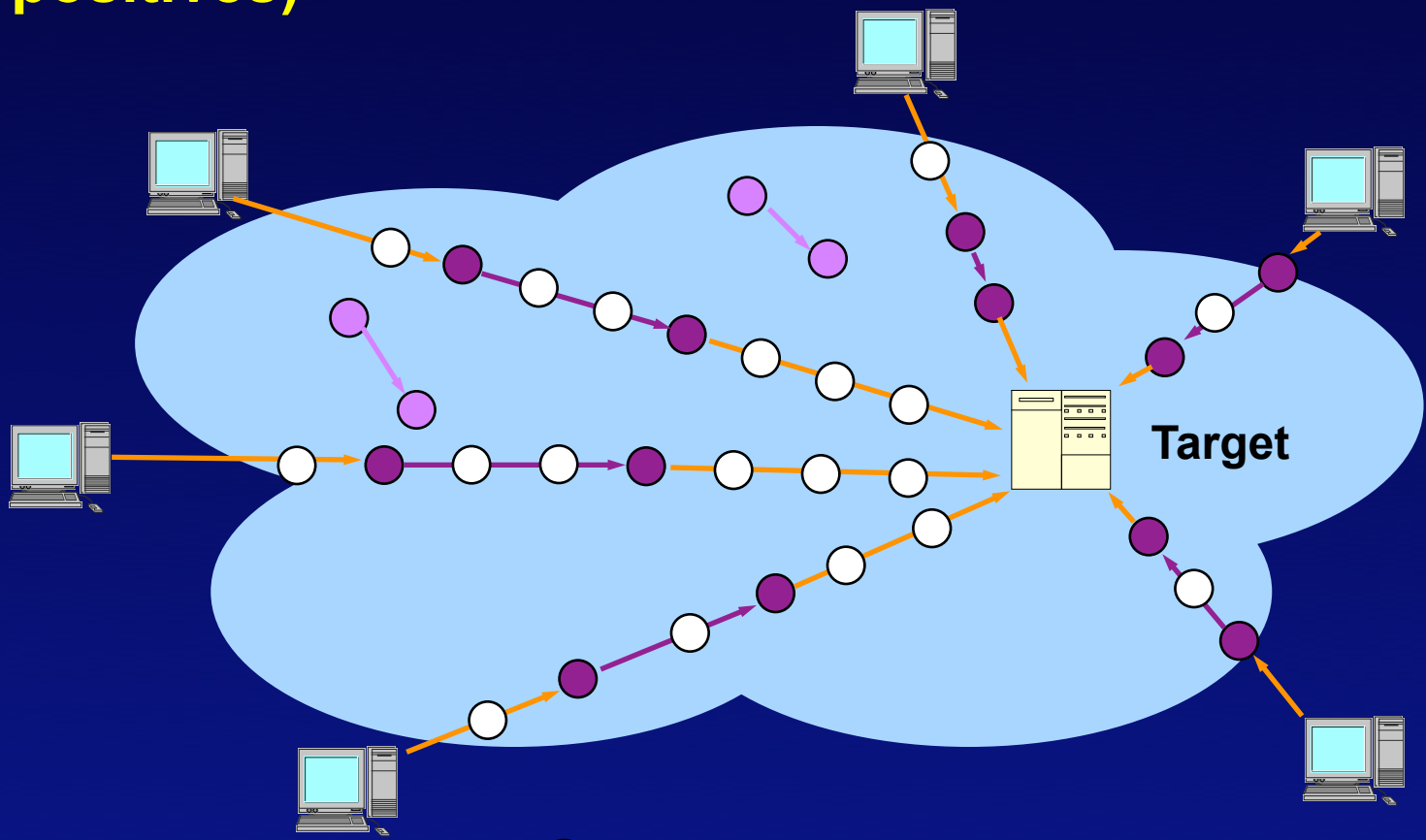


Edges discovered on attack paths

Target discovers more edges



Small chance that marks will be reconstructed incorrectly (false positives)



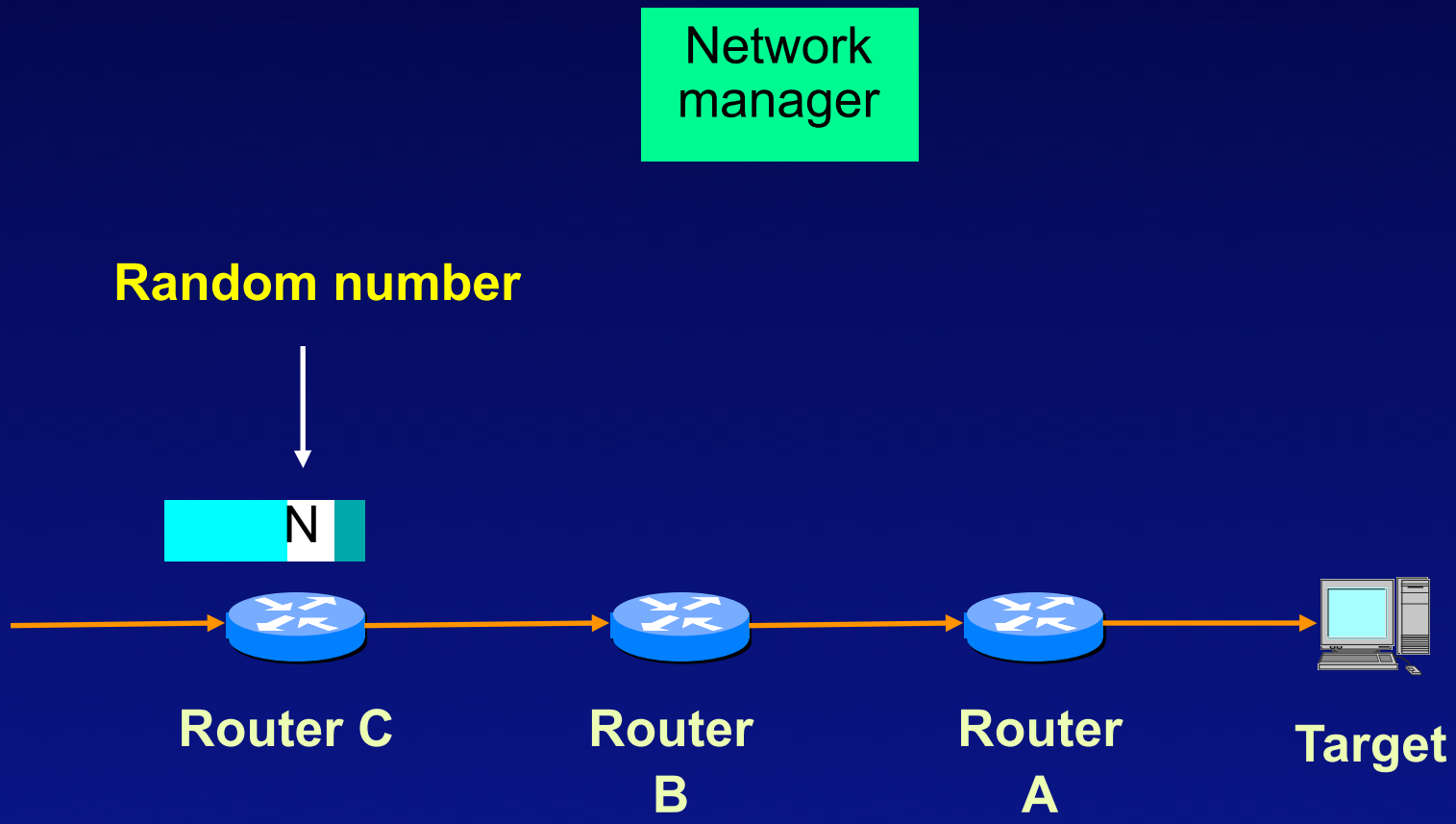
Edges discovered on attack paths

False positives

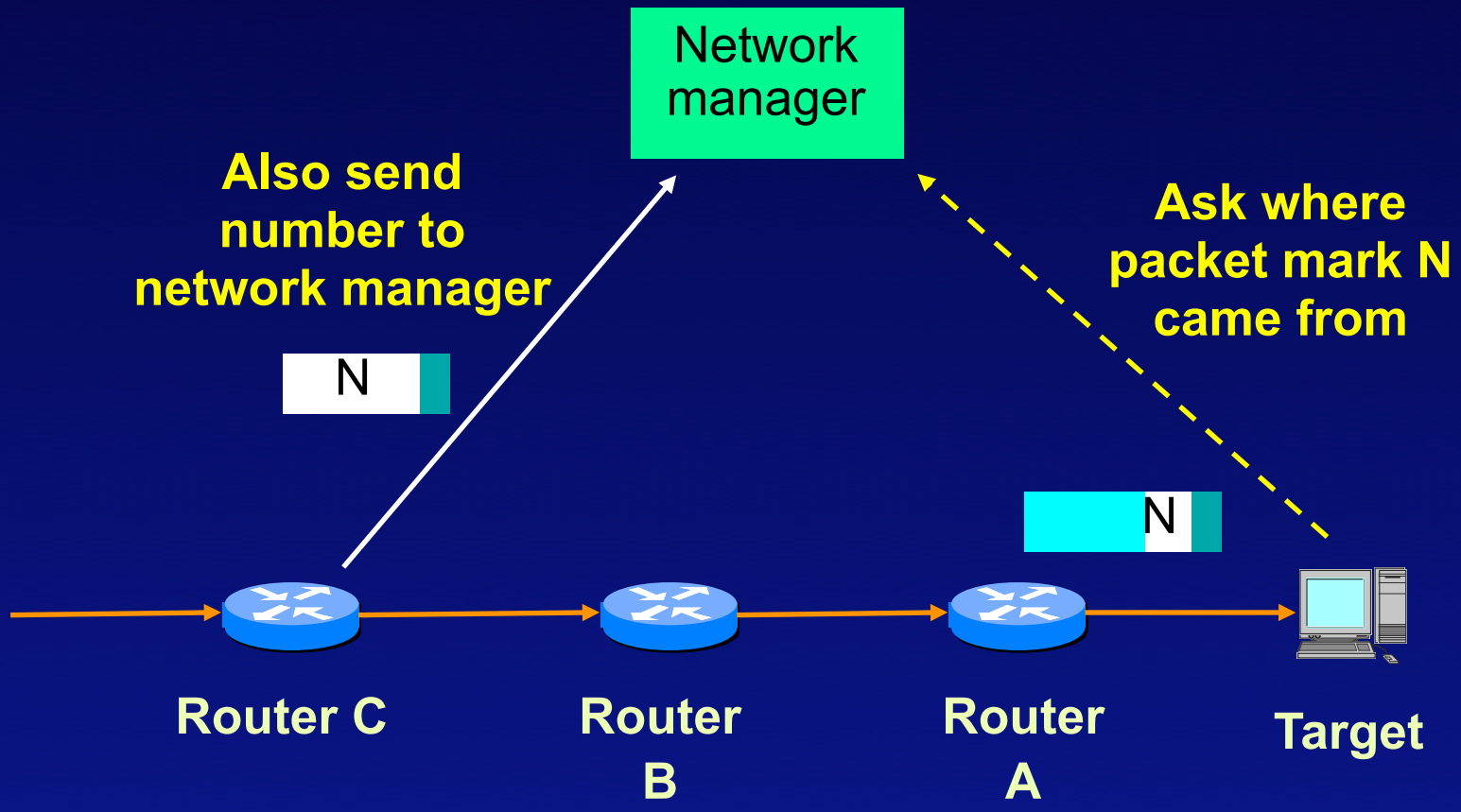
PPM (cont)

- We have proposed a random packet marking scheme
- Router chooses packets at random
  - Mark is a random number, added between packet header and payload
  - Limited to single ISP -- mark must be removed before packet leaves ISP
  - Router sends number to network manager

PPM (cont)


Network manager
Random number
N
Router C
Router B
Router A
Target

PPM (cont)


Network manager
Also send number to network manager
N
Ask where packet mark N came from
N
Router C
Router B
Router A
Target

Conclusions

- IP traceback for DDoS is an active research area
  - Traceback is also useful to find real sources of other types of attacks
- Researchers are studying various approaches, e.g., packet marking