

10/27

DoS:

prevent access

- break it - make program end w/ error

- overload

DDoS: distributed

- bot net

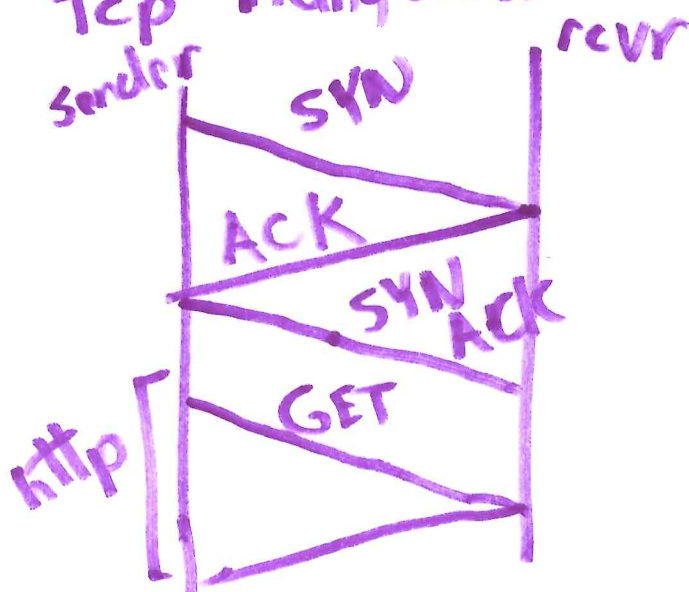
DoS prevention

attack from 1 device

- block the IP address (firewall)
device/network

Syn Flood Attack

tcp handshake



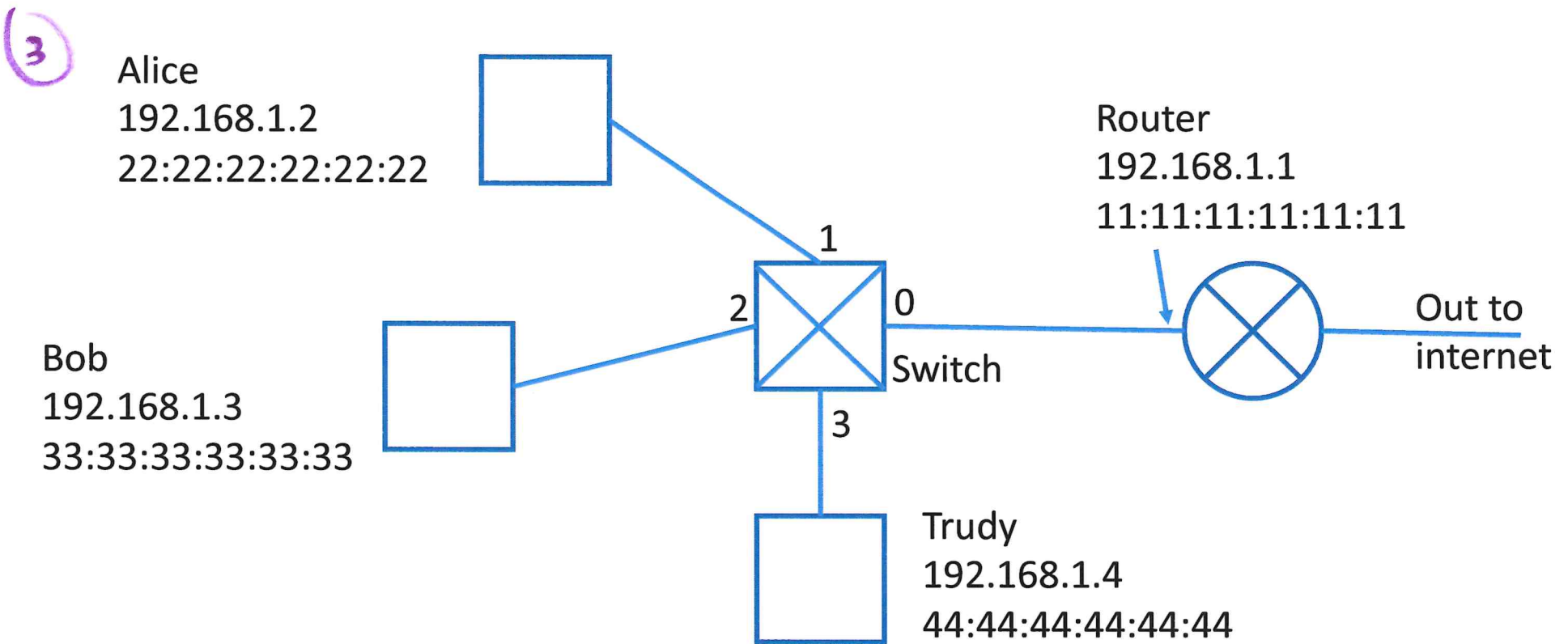
Syn Flood:
→ send a SYN msg
repeat
(fake src IP)

② Smurf Attack

ICMP

- echo request to broadcast addr : 255.255.255.255
- fake src IP (victim)

attacks w/ ARP
translate IP to MAC



Packet from Alice to Bob	
Src IP	192.168.1.2
Dest IP	192.168.1.3
Src Mac	22:22:22:22:22:22
Dest MAC	33:33:33:33:33:33

Packet from Alice to cs1	
Src IP	192.168.1.2
Dest IP	138.134.44.11
Src Mac	22:22:22:22:22:22
Dest MAC	11:11:11:11:11:11

ARP
Alice who has 1.3
I have it Bob
..:33

~~All Bob~~

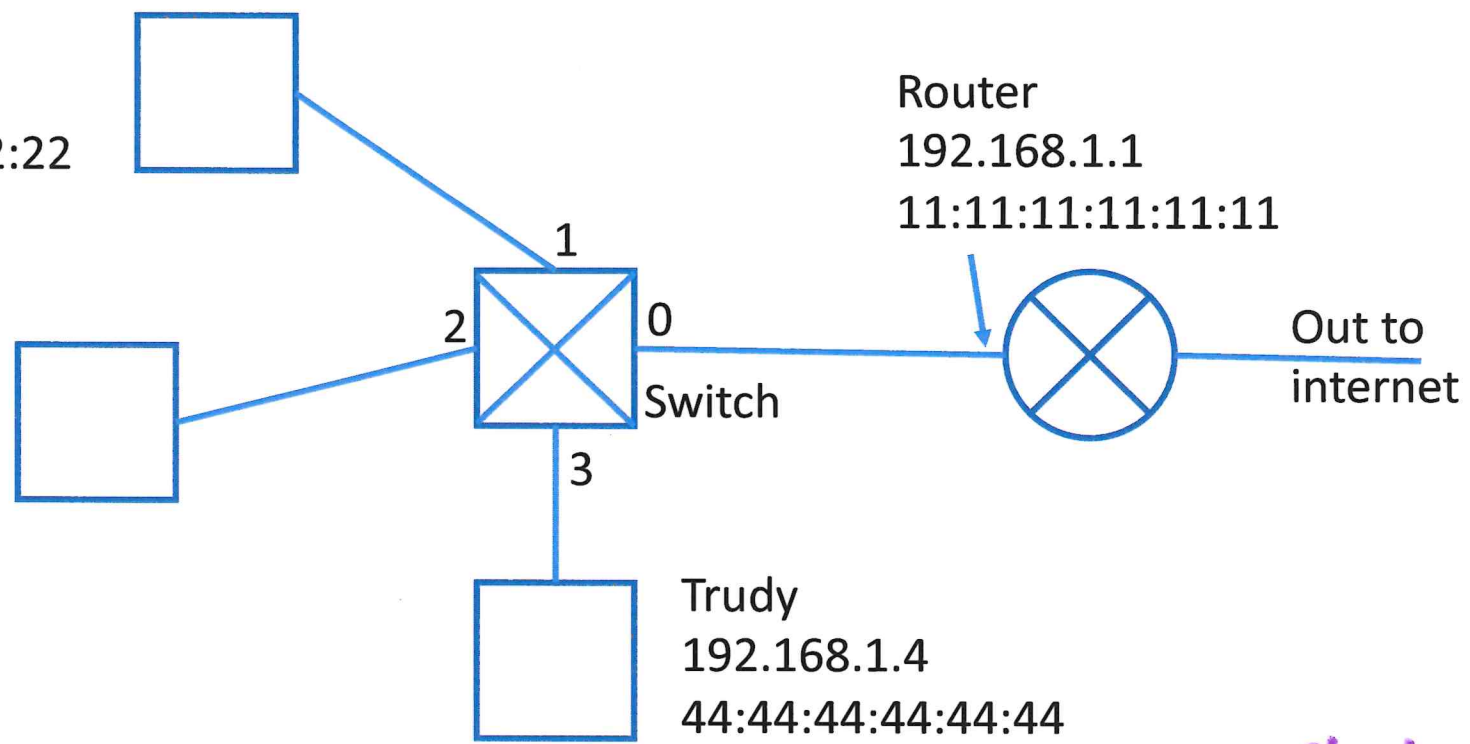
4/6

Alice
192.168.1.2
22:22:22:22:22:22

Bob
192.168.1.3
33:33:33:33:33:33

Trudy
192.168.1.4
44:44:44:44:44:44

Router
192.168.1.1
11:11:11:11:11:11



ARP flooding

Alice ARP Table	
MAC	IP
...:33	.1.3
...:44	.1.4
...:11	.1.1

Bob ARP Table	
MAC	IP
...:22	.1.2
...:44	.1.4
...:11	.1.1

Trudy ARP Table	
MAC	IP
...:22	.1.2
...:33	.1.3
...:11	.1.1

Switch Table	
Interface	MAC
0	...:11
1	...:22
2	...:33
3	...:44

full table works like HUB

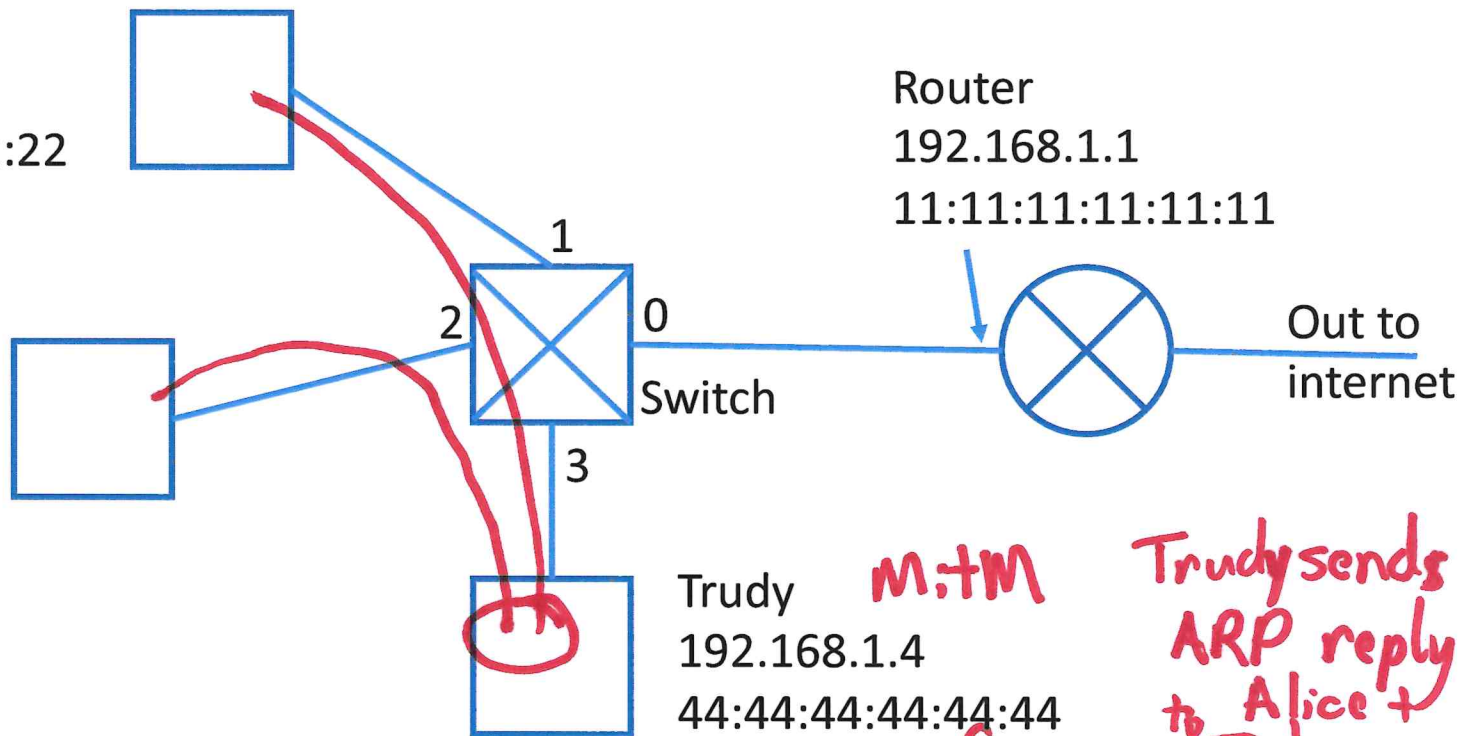
Trudy sends msgs to fake src

5

Alice
192.168.1.2
22:22:22:22:22:22

Bob
192.168.1.3
33:33:33:33:33:33

Router
192.168.1.1
11:11:11:11:11:11



Trudy
192.168.1.4
44:44:44:44:44:44

m:tm
Trudy sends ARP reply to Alice + Bob
ARP spoofing cache poisoning

Alice ARP Table	
MAC	IP
...33 ...44	.1.3
...44	.1.4
...11	.1.1

Bob ARP Table	
MAC	IP
...22 ...44	.1.2
...44	.1.4
...11	.1.1

Trudy ARP Table	
MAC	IP
...22	.1.2
...33	.1.3
...11	.1.1

Switch Table	
Interface	MAC
0	...11
1	...22
2	...33
3	...44

Trudy's MAC

fix: ignore replies w/ no requests

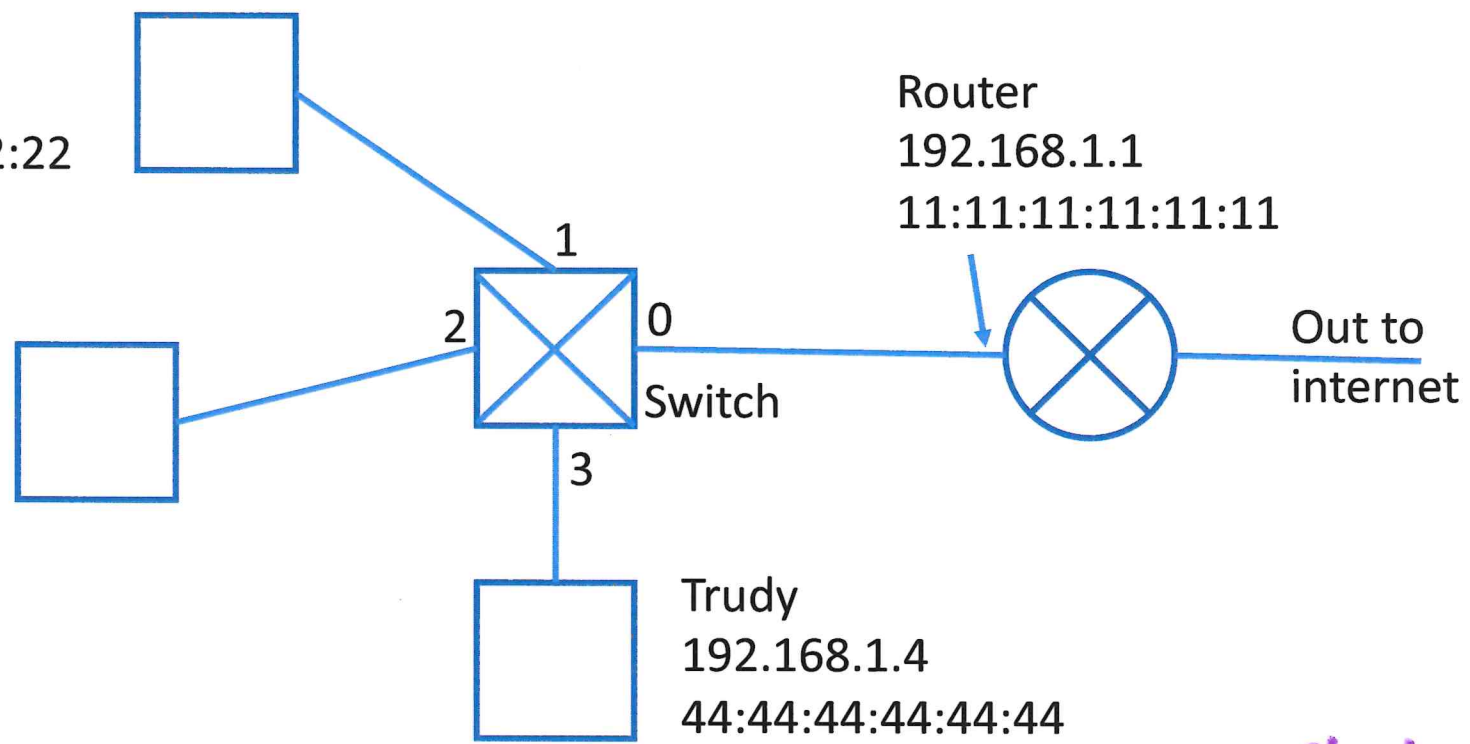
4/6

Alice
192.168.1.2
22:22:22:22:22:22

Bob
192.168.1.3
33:33:33:33:33:33

Trudy
192.168.1.4
44:44:44:44:44:44

Router
192.168.1.1
11:11:11:11:11:11



ARP flooding

Alice ARP Table	
MAC	IP
...:33	.1.3
...:44	.1.4
...:11	.1.1

Bob ARP Table	
MAC	IP
...:22	.1.2
...:44	.1.4
...:11	.1.1

Trudy ARP Table	
MAC	IP
...:22	.1.2
...:33	.1.3
...:11	.1.1

Switch Table	
Interface	MAC
0	...:11
1	...:22
2	...:33
3	...:44

full table works like HUB

Trudy sends msgs to fake src