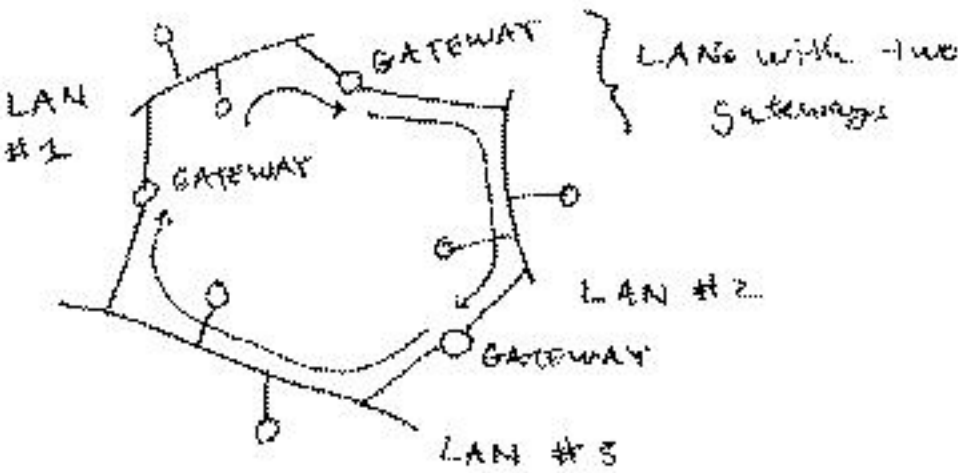
LOOPING PACKETS

Suppose administrators make a mistake in setting up the IP packet forwarding tables



Cycle of default gateways is possible.

What prevents IP packets from endlessly going around the cycle?

▷ EACH IP packet header has a field called TTL (time-to-live). Initially, it is a positive number (say 32), and each time a packet is received, if TTL = 0, discard packet; otherwise TTL ← TTL - 1 as packet is forwarded.

Another application using TTL is traceroute, which uses the "ping" idea with different TTL values, e.g. TTL = 1, 2, 3 ....

ping uses a protocol called ICMP

Source host of the ping packet

Target host

sends "ICMP echo" in response to ping

OR

Source host

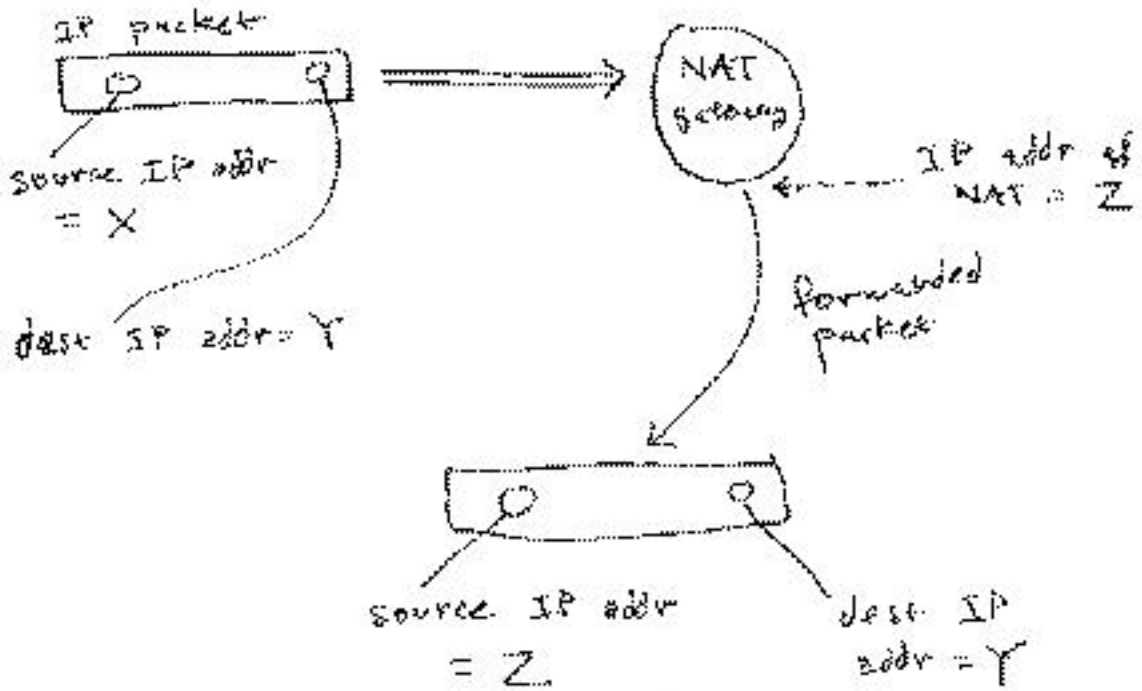
sends ICMP error packet if TTL = 0 in response to ping

FIREWALLS & NAT

A firewall is a gateway that is programmed to drop some packets instead of forwarding them

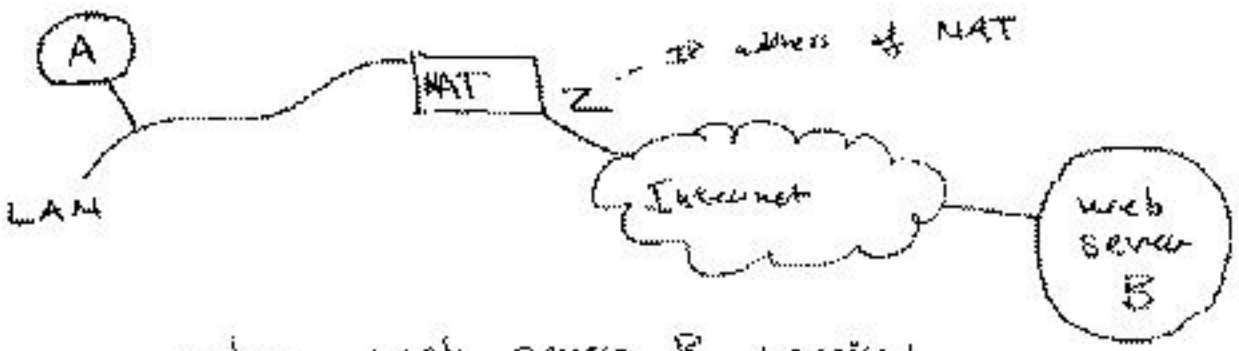
- Another table lookup algorithm!
- Used to protect organizations from attack, viruses, etc

NAT (network address translation) is a technique to "remap" IP addresses in packets:



How can this work??

NAT must have bookkeeping ....



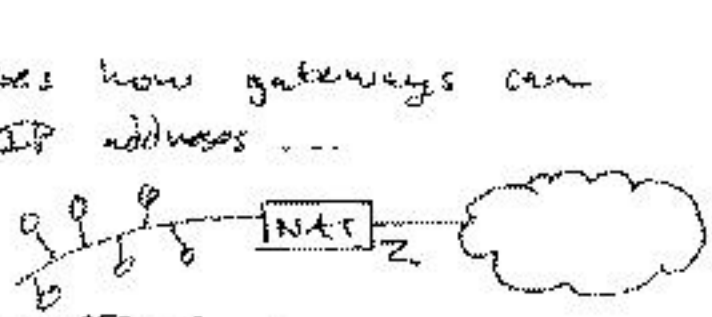
when web server B receives packet from A, the packet looks like it came from Z

⇒ B will send a response packet to Z

⇒ Now Z has to figure out that this packet is intended for A

NAT illustrates how gateways can manipulate IP addresses ...

Why?



all can share one IP address Z, reducing the overall # IP addresses of the Internet.

DANGER: IP "Spoofing"

Programming with TCP/IP

Systems use "file descriptors" for all manner of device - program communication -- including networks

For TCP/IP, the file descriptor is a socket (a object via which programs send or receive data)

FACT In TCP or UDP, the basic setup for communication is "caller - callee", usually known as client - server

client takes the initiative by contacting server
-- but this only works if server is "standing by"

Example: UDP Sockets

(shown interactively)