

# IP Masquerade

- IP address is becoming increasingly full
- assigning each machine with a static IP address is not practical anymore
  - address space might not support it
  - security problems - intruder can pretend to be the victim
  - moving machines across different network boundaries causes reconfiguration problems

# IP Masquerade

- Internet is rapidly running out of IP addresses
  - potentially more than 2 billion addresses
  - class B's are only partly used - the culprit
  
- for most medium to large organisations a class A address is too large (16 million hosts)
  - a class C is too small (254 hosts)
  - but a class B is just right (65534 hosts)
  - the **three bears problem**

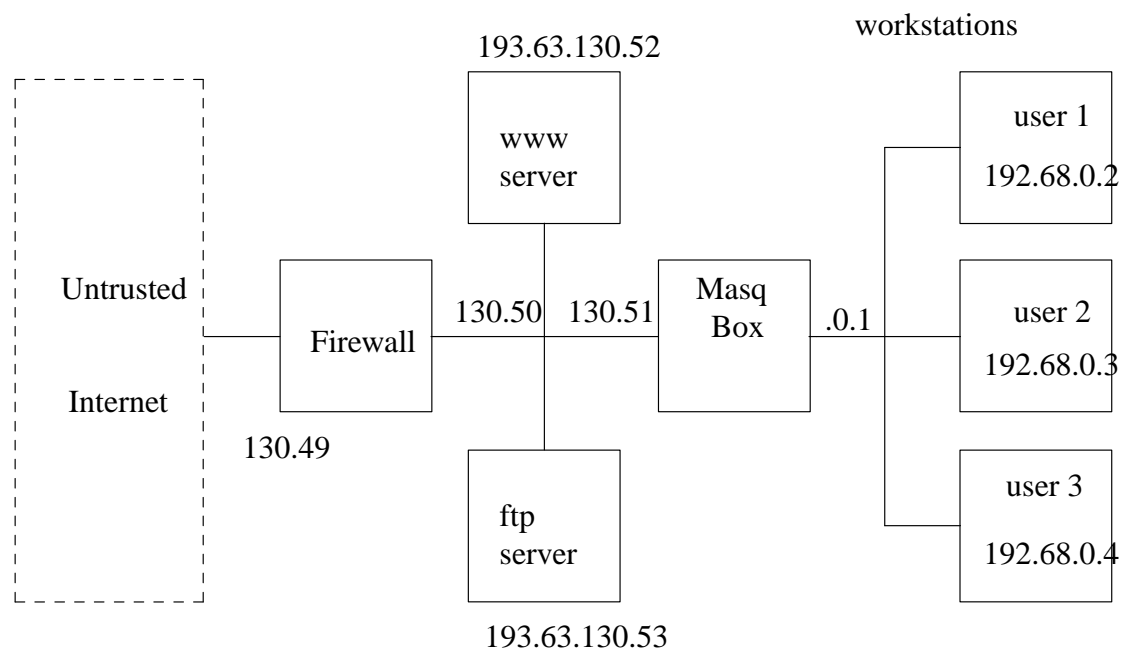
## IP Masquerade

- studies have shown that more than half class B networks have  $\leq 50$  hosts
  
- maybe it would have been better for the Internet designers to create class C networks with 10 host bits, rather than the 8
  - this would allow companies to add 1022 hosts
  - nevertheless the Internet designer could not foresee the growth of the Internet
  - in 1987 some visionaries predicted the Internet would grow to 100,000
  - laughed at by most people - and became reality in 1996

## IP Masquerade

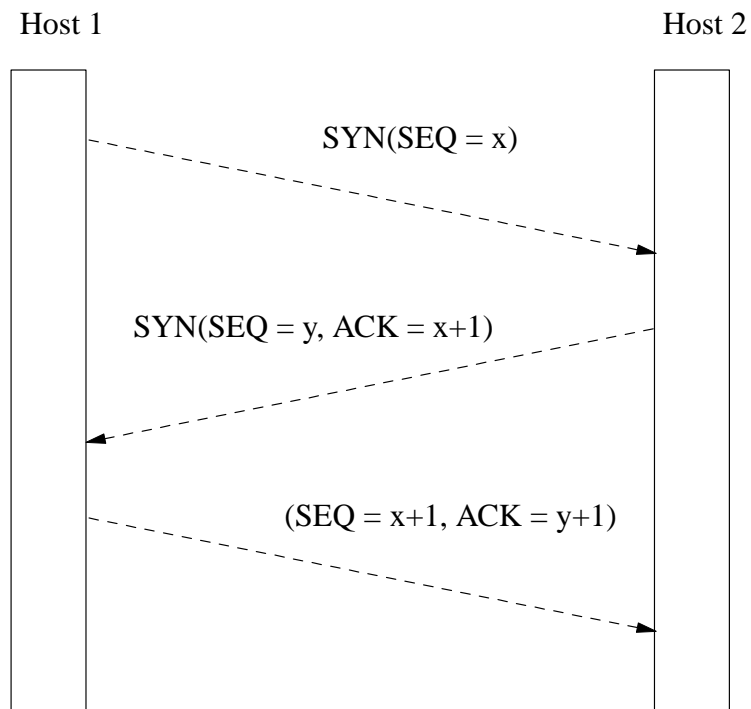
- class B was typically thought of as a University sized network
  - only 2000 Universities in USA and probably < 10000 in the world
  - there are approximately 16000 class B addresses
- Classless InterDomain Routing (CIDR) as attempted to break into the component classes and allocate blocks of addresses
- another solution to the problem of lack of address space is IP masquerading (sometimes referred to as NAT network address translation)
- IP masquerading allows us to configure a local area network which is invisible to the outside world

# New IP configuration



## How does this work?

- recall that normally IP contains either: TCP or UDP
- TCP starts with a 3 way handshake
- 



## How does this work?

- IP masquerade is a quick fix and it allows many machines to share a common static IP address
- idea is to allocate each company with a few static IP addresses (typically 1..5) at most
- within the company each computer gets allocated an internally unique IP address
- however no packet containing these internal IP addresses may appear on the Internet itself

## Reserved IP addresses for private networks

- the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private networks

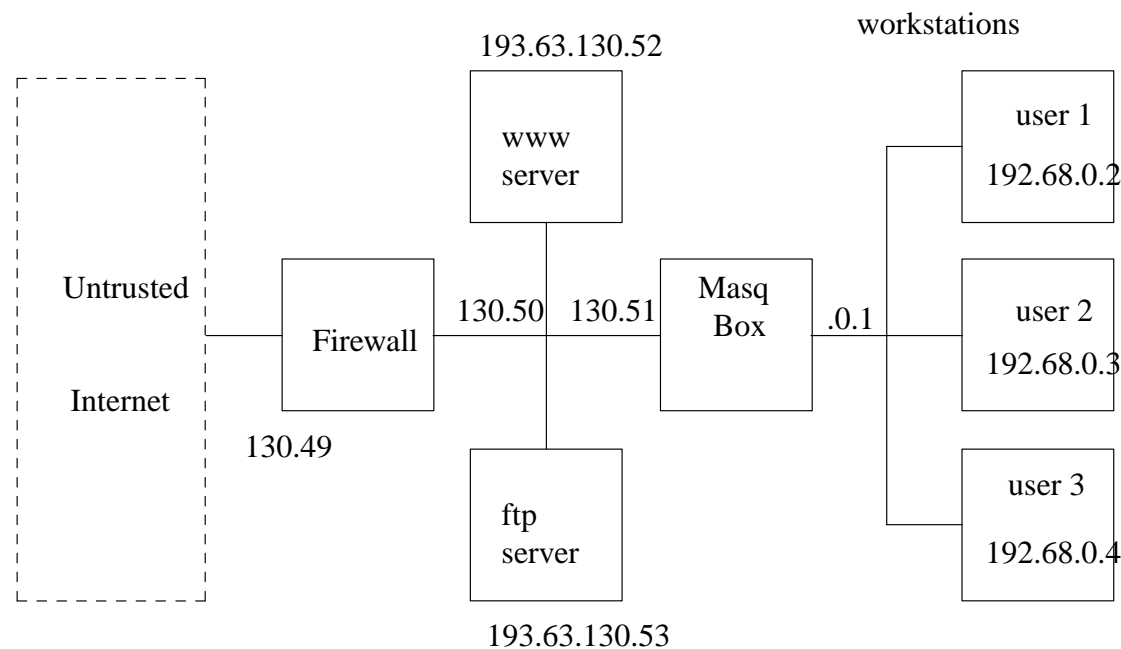


no of classes	netid	subnet mask
1 A	10.0.0.0	10.255.255.255
16 B	172.16.0.0	172.31.255.255
255 C	192.168.0.0	192.168.255.255

- companies are free to choose to use any one, two or three of these classes (internally)
  - typically they normally choose one

## Reserved IP addresses for private networks

- the operation of the IP masquerade is show below:



- here each desktop/laptop is assigned a local IP address of 192.168.0.x and when it communicates with the outside world it passes through the IP masquerade (NAT) box

## Reserved IP addresses for private networks

- the NAT converts the internal IP address into a global unique address, in this case: 193.63.130.51
- the NAT uses the internal IP address and the TCP or UDP port number to keep track of each packet

## Process establishing a TCP connection without NAT

- when a process on a desktop wishes to set up a TCP connection with an external web server it attaches itself to an unused port number on the local machine
  - known as the source port number
  
- the process fills in the destination port number (in this case 80 for the web server)
  - the packet is then transmitted
  - web server receives the message and send a reply
    - goes back to the original source port number

## Process establishing a TCP connection with NAT

- the process on the desktop does not need to know its packets will be masqueraded, so it behaves in exactly the same way
  
- so it attaches itself to an unused port number on the local machine
  - known as the source port number
  
- the process fills in the destination port number (in this case 80 for the web server)
  - the packet is then transmitted

## Process establishing a TCP connection with NAT

- the packet reaches the NAT (192.168.0.1)
  - this packets IP address is replaced by 193.63.130.51
  
- it replaces the source port by an index into the 65536 NAT table
  - each table entry contains
    - original IP address
    - original source port number
  
- the packet is sent from the external NAT interface

## Receiving NAT packets

- the NAT on receiving the reply datagram
  - extracts the source port from the UDP or TCP header (inside the IP packet)
  
- looks up the NAT table entry created earlier
  - replaces the packets IP address and dest address with the
    - tables source port number and
    - IP address
  
- it passes the packet to the 192.168.0.1 interface

## Criticisms of NAT

- NAT works, but not for all application protocols
- (i) NAT violates the architectural model of IP
  - an IP address should determine a unique host, worldwide
- (ii) NAT changes the Internet from being a connection less network into a connection oriented network
  - consider UDP packets are still entered into NAT tables
- if the NAT box is reset - all machines connected to the Internet loose their outstanding connections
  - network becomes vulnerable

## Criticisms of NAT

- (iii) NAT violates a key rule of network protocols
  - layer  $k$  should not make any assumptions about layer,  $k+1$  and should not examine its payload field
  
- (vi) processes do not have to use UDP or TCP transport layers
  - but with NAT they must
  
- (vi) some applications insert IP addresses into application layer
  - if NAT manipulates the IP address then the application layer will fail

## Criticisms of NAT

- ftp, xdmcp both do this and will fail with NAT
- in Linux you can insert ftp masquerade modules into the kernel
- effectively means IP layer peeks inside TCP and ftp layers and modifies the headers in both upper layers
  - definitely against the architecture of network protocols