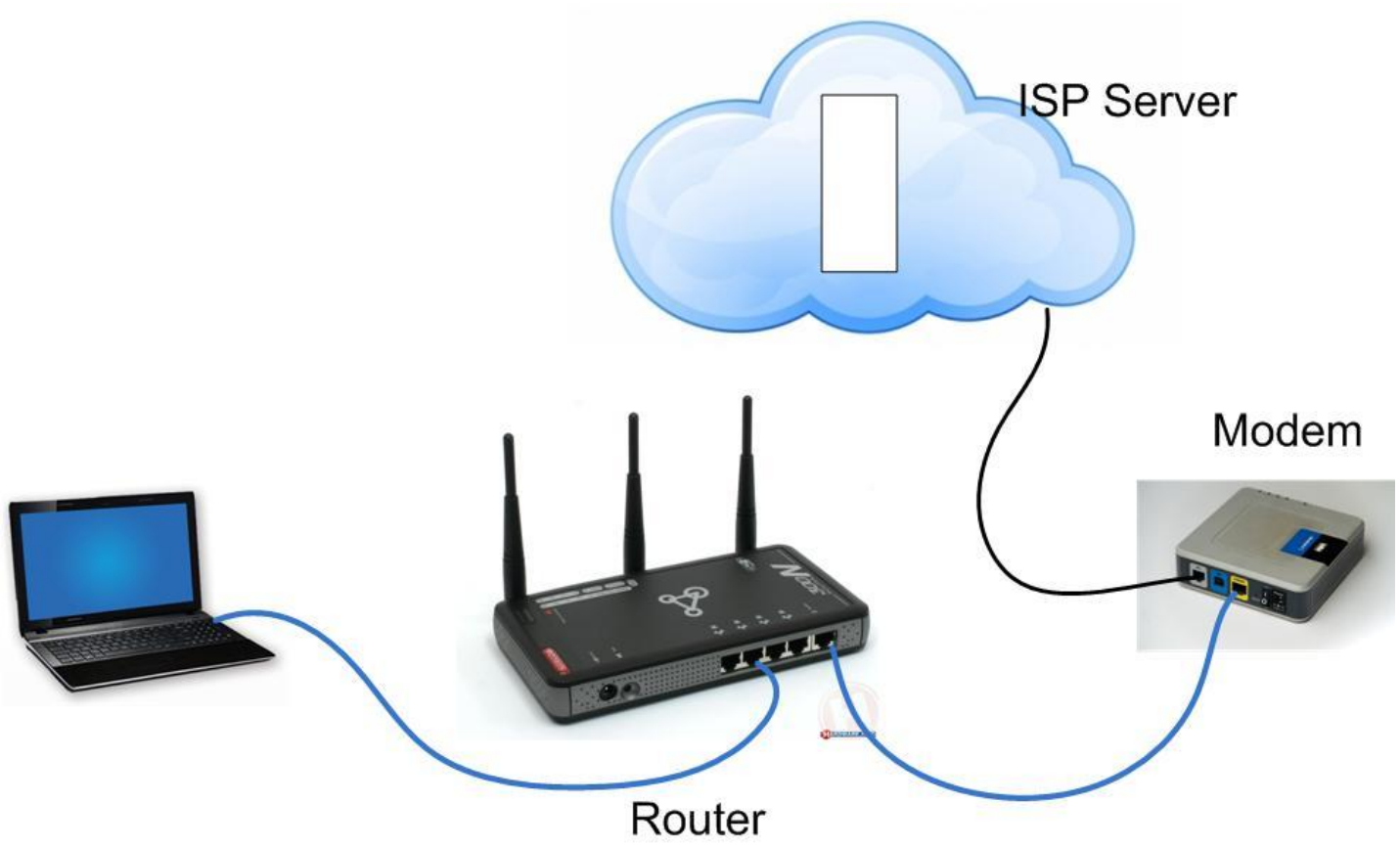
IP ADDRESSES

HARDWARE OCTOBER2014

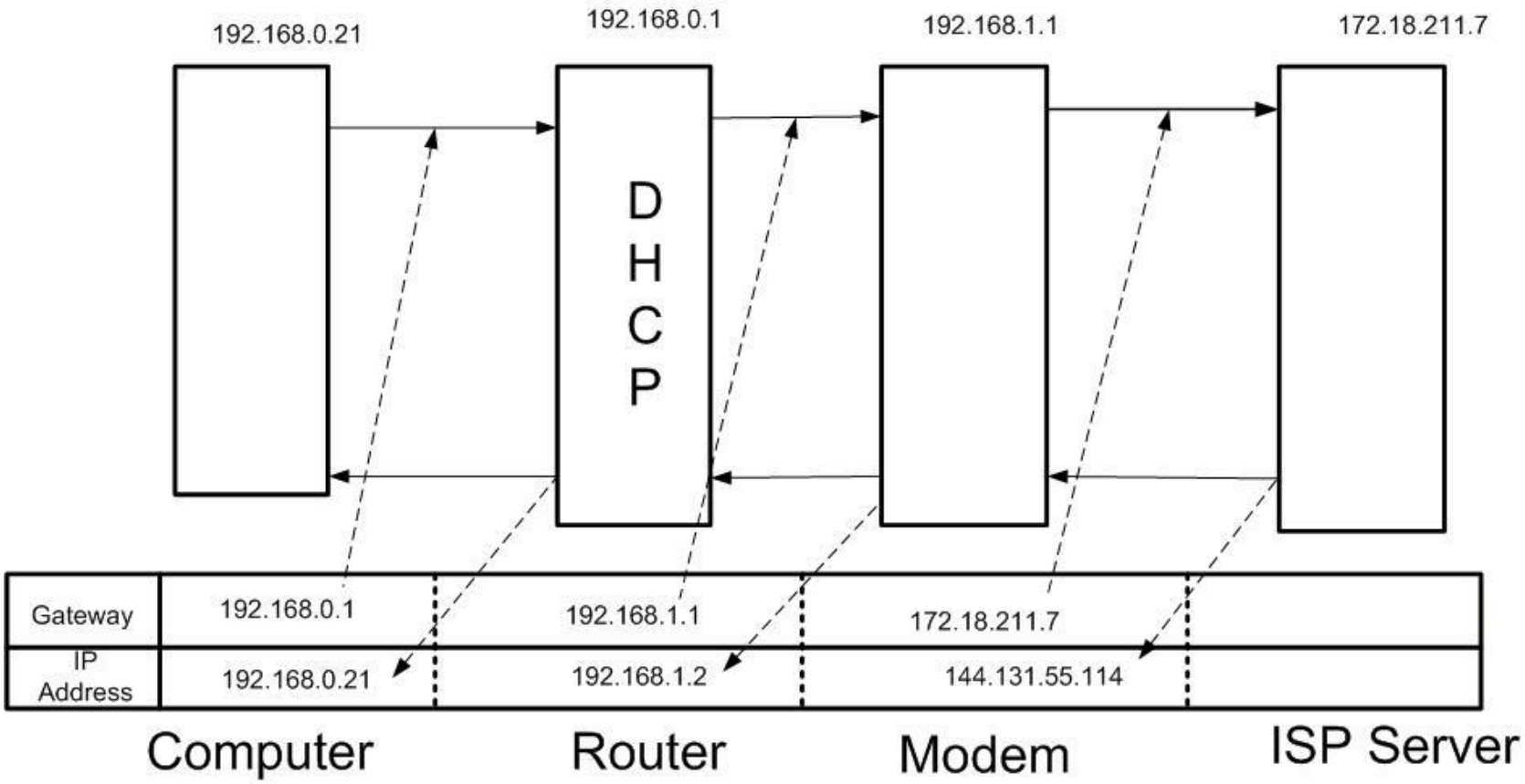
General Structure

- IPv4 4 Octets (32 bits) 8 bits is 256 decimal numbers
  - Eg 192.168.0.1
- IPv6 is future standard 16 Octets (128 bits)

Home Network



IP ADDRESSES



What is NAT?

NAT = “Net Address Translation”

Most frequently encountered method is the one used in home broadband routers which “hide” an entire non-routable network range behind a single routable “public” IP address.

Network Address Translation (NAT)

Local (LAN) addresses are not used in the wider internet (WAN)

The Router/Modem provides the network translation

- Only need a single IP address from your ISP and share that address among a large number of devices.
- All devices on the local network can access the Internet at the same time, though the bandwidth is shared

NAT router setup

NAT routers/Modems are given two IP's addresses:

- 1 non-routable (LAN -- you)
- 1 routable (WAN – ISP)

Machines on LAN side get special non-routable addresses (usually 10.*.*.* or 192.168.*.*).

- No IP addresses in these ranges are routed on the Internet.
- The Router/Modem translates the LAN address to the WAN IP address eg 144.131.55.114
- From the internet every computer behind the router/modem appears to come from the same address.

How NAT works

Normal routers maintain source and destination IP addresses from end-to-end.

NAT routers change IP addresses

Outgoing packets appear to come from the NAT router's public address.

- NAT routers keep track of each "flow" so that replies can be returned.

How NAT firewalling works

Suppose a host (either friendly or malicious) sends a packet to the NAT router without the connection being initiated from the inside.

- Outside hosts can't send directly to the hosts on the local network side -- they have non-routable addresses!

Since there is no entry in the flow table, the NAT router has no idea where to forward it and drops the packet. Instant firewall!