Network Address Translation (NAT)

Reading: Chapter 21

Concepts

- NAT
  - Translation between IP addresses (and port numbers)
- Basic NAT
  - Only involving IP address translation
- Network address and port translation
  - Involving both IP address and port number

Some application specific problems

- FTP
  - PORT command contains IP/port
  - May need to change content
- Fragmentation
  - Only the first fragment has TCP/UDP header
  - May need to do assembly first
NAT implementation in Linux

How packet flows in NAT
- Incoming packets
  - NF_IP_PRE_ROUTING
    - ip_nat_fn()
- Locally generated packets
  - NF_IP_LOCAL_OUT
    - ip_nat_local_fn() for unfragmented packets
    - Passing on other packets
- Outgoing packets
  - NF_IP_POST_ROUTING
    - ip_nat_out() – Reassemble packets, passing on to ip_nat_fn()

Initialization and uninitialization
- Done by init() and fini()
  - They call init_or_cleanup()
- init_or_cleanup()
  - Initialization
    - Initializing some netfilter tables
    - Initializing some protocol specific stuffs
    - Link (register) netfilter hooks
      - ip_nat_fn(), ip_nat_local_fn(), ip_nat_out()
  - Uninitializing
    - Reversing the process

ip_nat_fn()
- Determining what NAT needs to be used (src or dst)
- Determining associated flow of the packet
- Handling the packet depending on state
  - Expected connection (IP_CTRELATED)
  - New connection (IP_CTNEW)
  - Others
- Doing real binding (translation)
  - Do Bindings()
Initializing address-binding process

- Netfilter registered branch destinations
  - ipt_snat_target(), ipt_dnat_target()
  - Finding associated flow/connection entry
  - Calling ip_nat_setup_info() to do new binding

Actual address translation

- do_bindings()
  - Searching associated bindings
  - Calling manip_pkt() to do address translation

- manip_pkt()
  - Translating ip address
  - Updating checksum
  - Calling prot->manip_pkt() to handle protocol specific translation