System Administration

Network Tools

ping

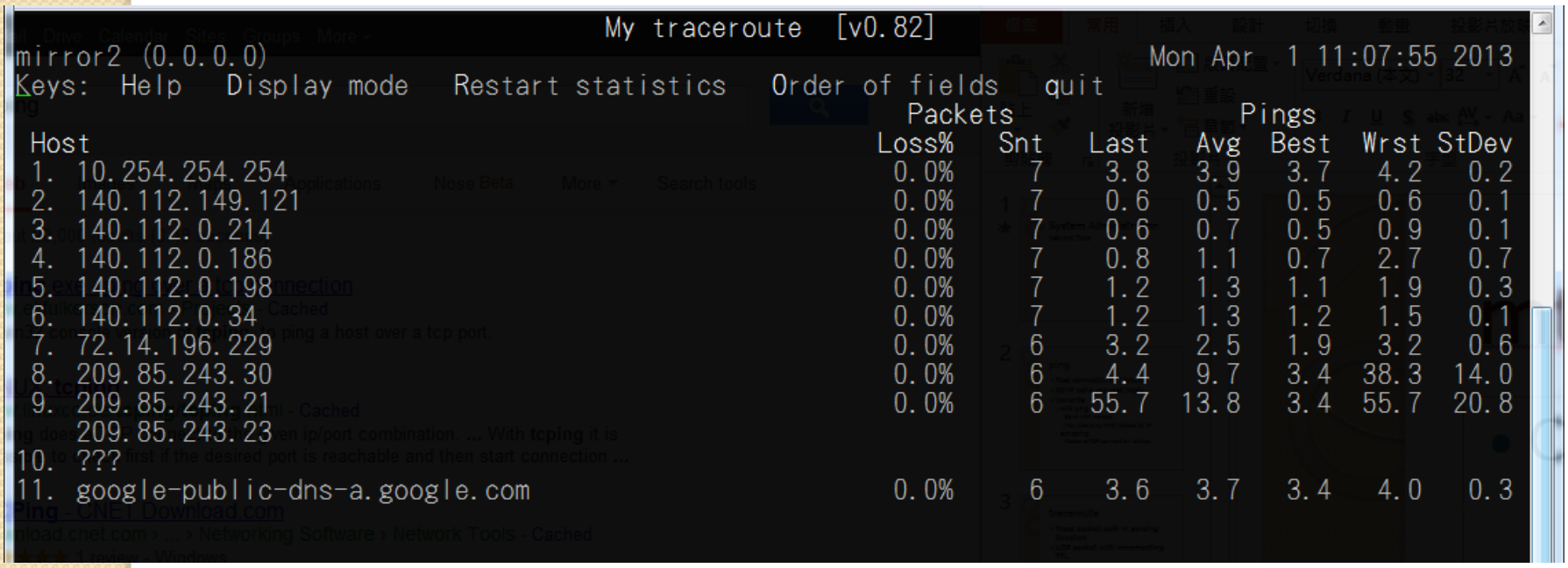
- Test connectivity / latency (RTT)
- ICMP echo request/reply
- Variants
  - ARP ping
    - Send ARP instead
    - May also ping MAC instead of IP
  - echoping
    - Measure TCP connection latency

traceroute

- Trace packet path in *sending* direction
- UDP packet with incrementing TTL
- Can also use ICMP ping or TCP

mtr

- Combines ping and traceroute with friendly output



Looking Glass

- Ping / Traceroute from ISP routers
- Provided by most large ISPs
  - http://lg.he.net/

host

- Query DNS records
- host [-t type | -a] name [server]

dig

- Query DNS records
- More versatile than host
  - Supports DNSSEC
  - Multiple queries
  - Tweakable output format
  - Batch mode
- Better for scripting

nslookup

- Old way to query DNS
  - Interactive command line
  - Best not to use

whois

- Query domain and IP registration
- Online tool: http://www.whois365.com/tw

netstat

- Show network information
  - Connections
  - Routing table
  - Statistics
  - Etc.

arp

- Show/manipulate ARP table
  - IP => MAC mapping

ifconfig

- Show interface configuration
- Configure network interfaces
  - Bring up/down interface
  - Set IP/netmask
  - Add/delete address (alias)
- 2 ways to alias
  1. add/del – IP listed under same interface
  2. ethX:X – Add symbolic name

ethtool

- Control network driver
  - IRQ Coalesce
  - Line speed
  - Auto negotiate

route

- Show routing table
- Manipulate routing table
  - Local network route is added when IP is configured
  - Default gateway:
    - Destination is “default” or 0.0.0.0
    - No netmask required

ip

- *The* way to do network configuration
  - Network interfaces
  - IPs
  - ARP table
  - Routing tables
  - Etc.

ip

- ip link
  - Interface up/down, settings
  - Manpage: ip-link (8)
- ip addr
  - IP addresses
  - Manpage: ip-address (8)
- ip neigh
  - ARP table
  - Manpage: ip-neighbour (8)

ip

- ip route
  - Routing tables
  - Manpage: ip-route (8)
- ip rule
  - Routing policies
  - Match rule => different routing table
  - Manpage: ip-rule (8)

iptables

- Linux 2.4+
- Also known as Netfilter
- Filter
  - ACCEPT/REJECT packets
  - Rate limiting
  - QoS
  - Log traffic
- NAT
  - Redirect
  - NAT

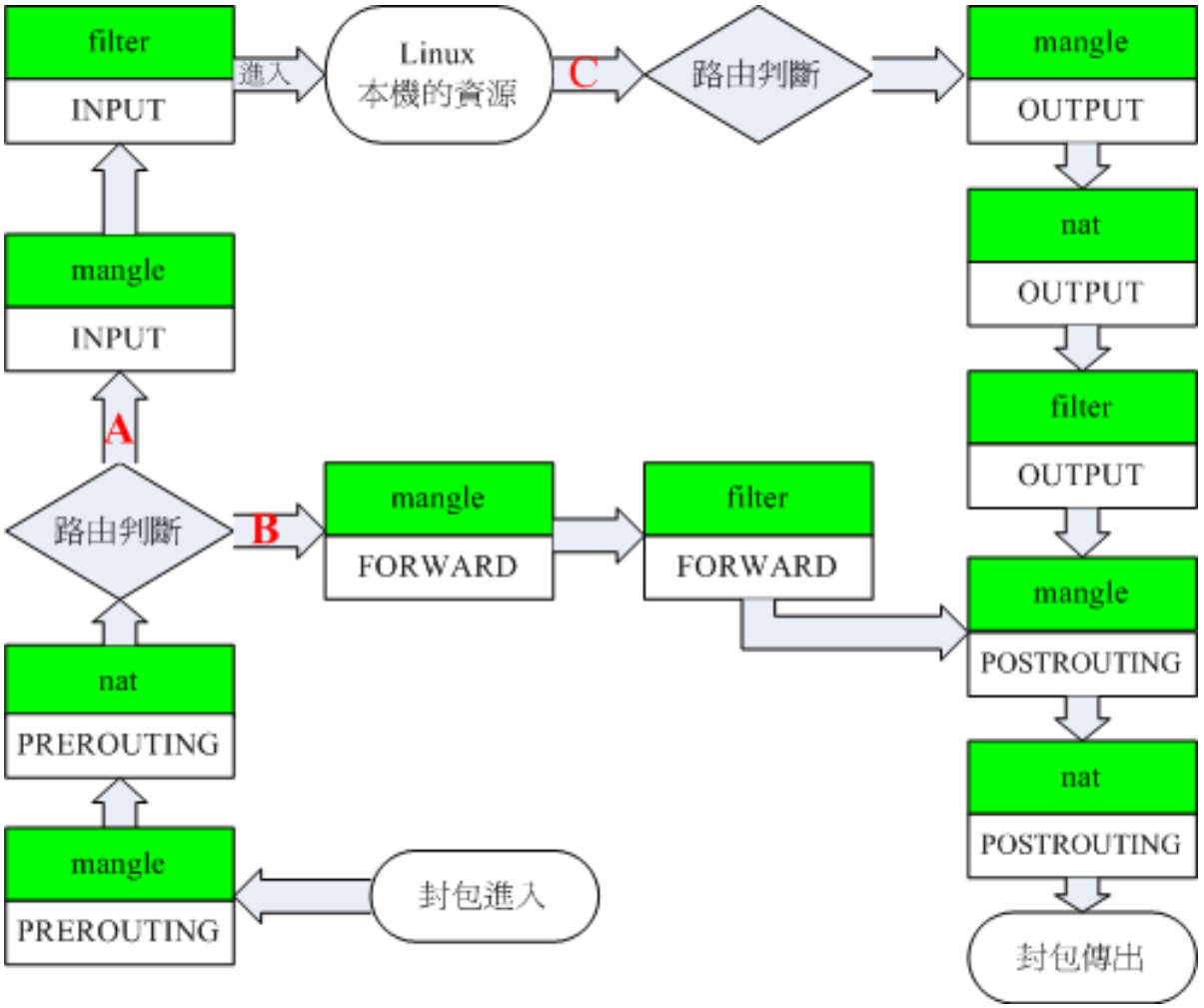
iptables – Commands

- iptables -A <chain> <rule> -j <TARGET>
  - Chain: see next page
  - Rule: see second next page
  - TARGET: action
    - ACCEPT
    - DROP (silently ignore)
    - REJECT
    - Etc.

Iptables – Commands

- iptables -L
  - List current rules
- iptables –D <chain> <number>
  - Delete a rule
- iptables –F <chain>
  - Flush (clear) a chain

iptables – Chain Map



iptables – Rules

- Match
  - IPs (-s -d)
  - Protocol (-p TCP/UDP/ICMP/…)
  - Port (--sport --dport)
  - Protocol options
    - ICMP type
    - TCP SYN/ACK
    - Etc.
  - Owner (UID, for OUTPUT chain)
  - Etc.

iptables (short hand)

Short form	Long form
-s	--source
-d	--destination
--sport	--source-port
--dport	--destination-port

iptables – Simple Rules

- Block a source IP
  - iptables -A INPUT -s <IP> -j DROP
- Block a destination IP
  - iptables -A OUTPUT -d <ip> -j DROP
- Block a TCP source port
  - iptables -A INPUT -p tcp --sport <port> -j DROP
- Block a TCP destination port
  - iptables -A OUTPUT -p tcp --dport <port> -j DROP

Combination

- Drop packets from 140.112.30.0/22 to local TCP port 80
- iptables -A INPUT --source 140.112.30.0/22 -p tcp --dport 80 -j DROP

iptables – Evaluation

- Packets are evaluated rule by rule
- First match counts
- Ordering is important
- Be careful not to block yourself out

Homework

- 從家裡 Ping / Traceroute 系上網站
- 查詢系上網域的DNS MX紀錄
- 寫出設定網路的指令 (ifconfig+route)
  - eth1 (未啟動)
    - IP: 192.168.30.XXX (XXX是座號)
    - Netmask: 255.255.255.0 (/24)
  - Default gateway: 192.168.30.254
- 同上，但改用ip系列指令
- 防火牆
  - 擋掉所有進來的封包，但要允許系上連到本機的 SSH (TCP port 22)