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

<table>
<thead>
<tr>
<th>Host</th>
<th>Loss%</th>
<th>Snt</th>
<th>Last</th>
<th>Avg</th>
<th>Best</th>
<th>Wrst</th>
<th>StDev</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 10.254.254.254</td>
<td>0.0%</td>
<td>7</td>
<td>3.8</td>
<td>3.9</td>
<td>3.7</td>
<td>4.2</td>
<td>0.2</td>
</tr>
<tr>
<td>2. 140.112.149.121</td>
<td>0.0%</td>
<td>7</td>
<td>0.6</td>
<td>0.5</td>
<td>0.5</td>
<td>0.6</td>
<td>0.1</td>
</tr>
<tr>
<td>3. 140.112.0.214</td>
<td>0.0%</td>
<td>7</td>
<td>0.6</td>
<td>0.7</td>
<td>0.5</td>
<td>0.9</td>
<td>0.1</td>
</tr>
<tr>
<td>4. 140.112.0.186</td>
<td>0.0%</td>
<td>7</td>
<td>0.8</td>
<td>1.1</td>
<td>0.7</td>
<td>2.7</td>
<td>0.7</td>
</tr>
<tr>
<td>5. 140.112.0.198</td>
<td>0.0%</td>
<td>7</td>
<td>1.2</td>
<td>1.3</td>
<td>1.1</td>
<td>1.9</td>
<td>0.3</td>
</tr>
<tr>
<td>6. 140.112.0.34</td>
<td>0.0%</td>
<td>7</td>
<td>1.2</td>
<td>1.3</td>
<td>1.2</td>
<td>1.5</td>
<td>0.1</td>
</tr>
<tr>
<td>7. 72.14.196.229</td>
<td>0.0%</td>
<td>6</td>
<td>3.2</td>
<td>2.5</td>
<td>1.9</td>
<td>3.2</td>
<td>0.6</td>
</tr>
<tr>
<td>8. 209.85.243.30</td>
<td>0.0%</td>
<td>6</td>
<td>4.4</td>
<td>9.7</td>
<td>3.4</td>
<td>38.3</td>
<td>14.0</td>
</tr>
<tr>
<td>9. 209.85.243.21</td>
<td>0.0%</td>
<td>6</td>
<td>55.7</td>
<td>13.8</td>
<td>3.4</td>
<td>55.7</td>
<td>20.8</td>
</tr>
<tr>
<td>10. 209.85.243.23</td>
<td>0.0%</td>
<td>6</td>
<td>3.6</td>
<td>3.7</td>
<td>3.4</td>
<td>4.0</td>
<td>0.3</td>
</tr>
<tr>
<td>11. google-public-dns-a.google.com</td>
<td>0.0%</td>
<td>6</td>
<td>3.6</td>
<td>3.7</td>
<td>3.4</td>
<td>4.0</td>
<td>0.3</td>
</tr>
</tbody>
</table>

- 'Cached': Indicates that the destination is reachable and the connection is maintained.
- 'Connection': Indicates a TCP connection is maintained.
- 'Ping': Function that sends a ping to the destination.
- 'Download': Function that downloads data from the destination.
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
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)

<table>
<thead>
<tr>
<th>Short form</th>
<th>Long form</th>
</tr>
</thead>
<tbody>
<tr>
<td>-s</td>
<td>--source</td>
</tr>
<tr>
<td>-d</td>
<td>--destination</td>
</tr>
<tr>
<td>--sport</td>
<td>--source-port</td>
</tr>
<tr>
<td>--dport</td>
<td>--destination-port</td>
</tr>
</tbody>
</table>
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)