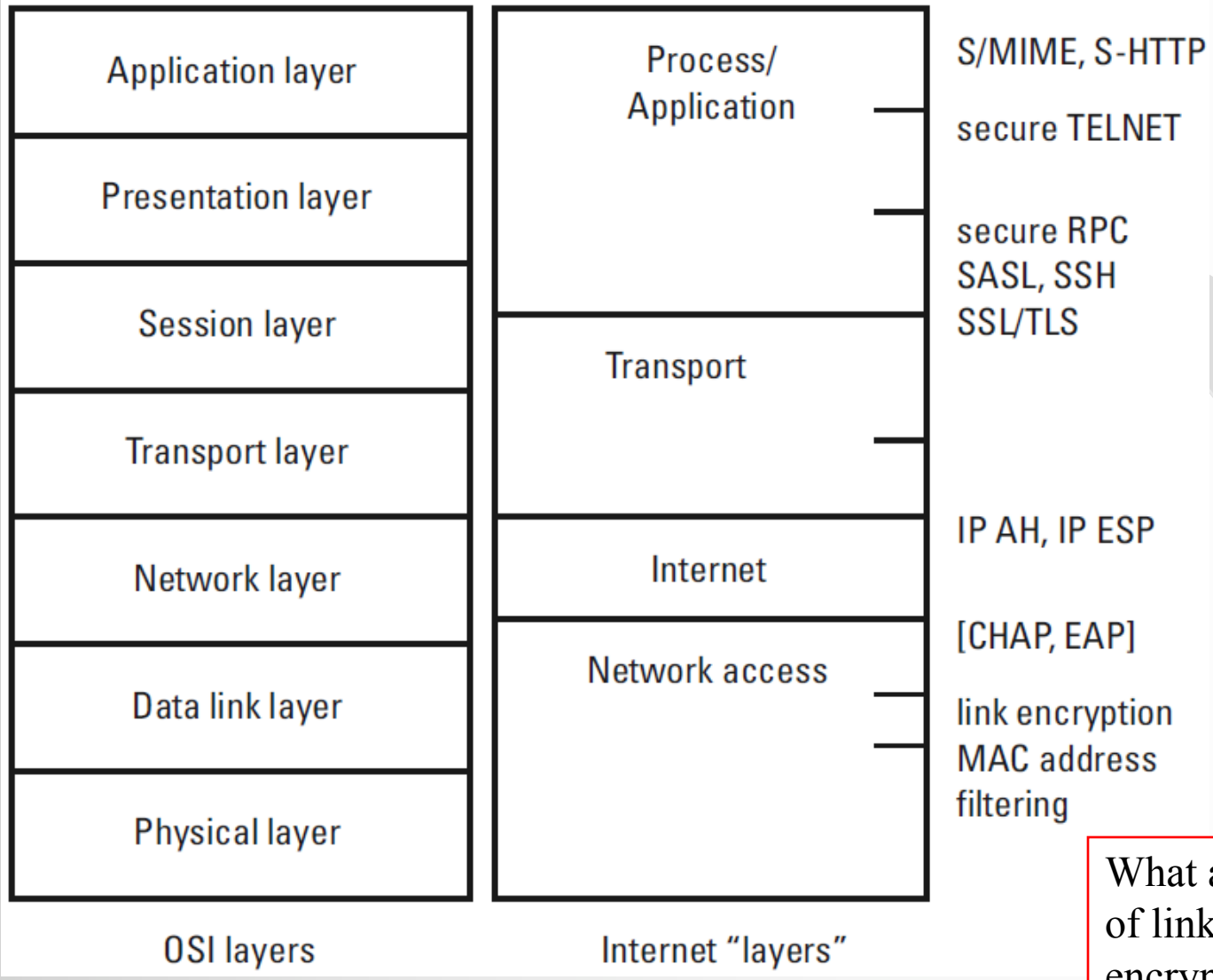
COMP 3355
Internet Layer Security

K.P. Chow

University of Hong Kong

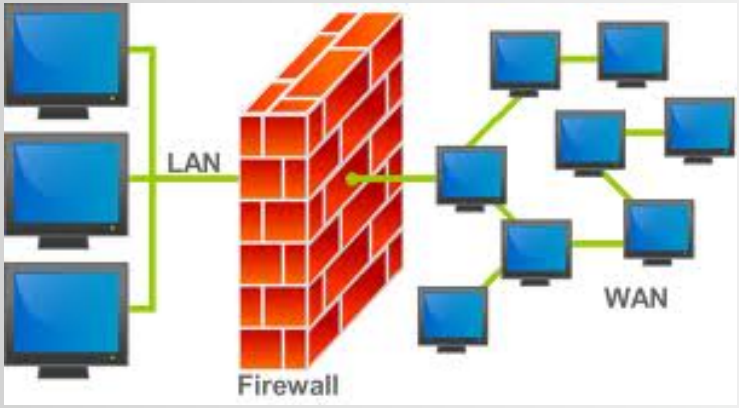
Security mechanisms at different layers

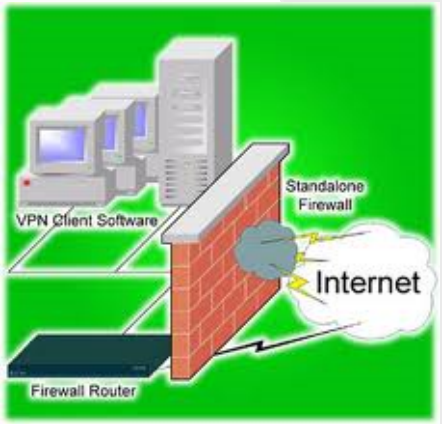


What are disadvantages of link-level encryption?

Firewall

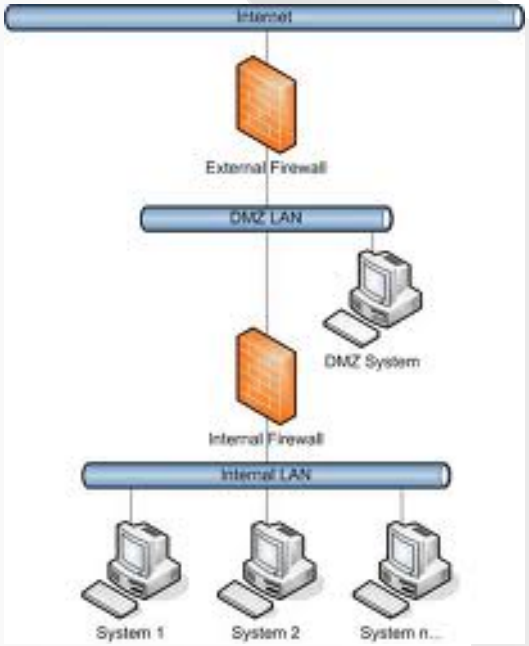
- A firewall is a combination of hardware and software that isolates an **organization's internal network** from the **Internet**, allowing some packets to pass and blocking others
- Firewall can also provide segmentation between internal resources
- In the simplest form, firewall control access to, from and between networks within the organization and the Internet





Demilitarized Zone (DMZ)

- A physical or logical subnetwork that contains and exposes an organization's external services to the Internet
- The purpose of a DMZ is to **add an additional layer of security** to an organization's local area network (LAN); an external attacker only has access to equipment in the DMZ, rather than any other part of the network
- Typical services in DMZ
  - Web server
  - Proxy server
  - Email server
  - Reverse proxy server



3-Legged Firewall with DMZ

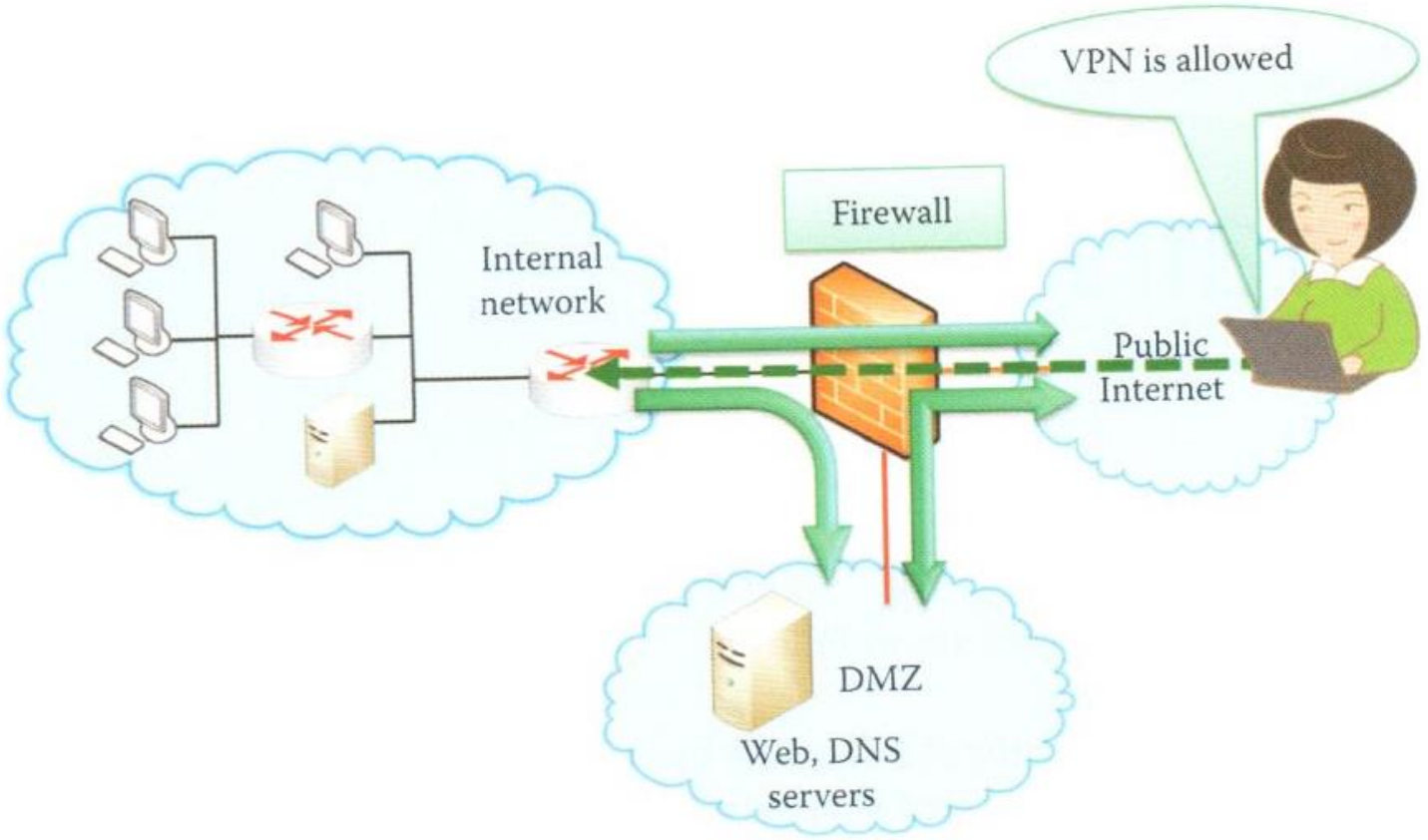


FIGURE 18.1 A 3-legged firewall with DMZ.

Unified Threat Management (UTM)

- An integrated security gateway that contains up to 8 components:
  - Firewall
  - Content filtering by proxy server
  - Network address translation (NAT)
  - Virtual private network (VPN)
  - Anti-virus
  - Anti-spam
  - URL filtering
  - Intrusion detection/prevention system (IDS/IPS)
- Low cost all-in-one tools that are deployed to small to medium businesses: usually deployed at the edge of the enterprise network

Types of Firewalls

- Packet filtering – network layer
  - A multi-ported IP router that applies a set of rules to each incoming/outgoing IP packet and decides whether it is to be forwarded or not
- Proxy gateway – also known as application layer gateway, proxy server
  - A gateway from one network to another for a specific network application, acts as a proxy on behalf of the network users
- Circuit level inspection SOCKS (i.e. SOCKetS)
  - A protocol that is application independent and transparent to user, performs filtering at the Session Layer (no content filtering)

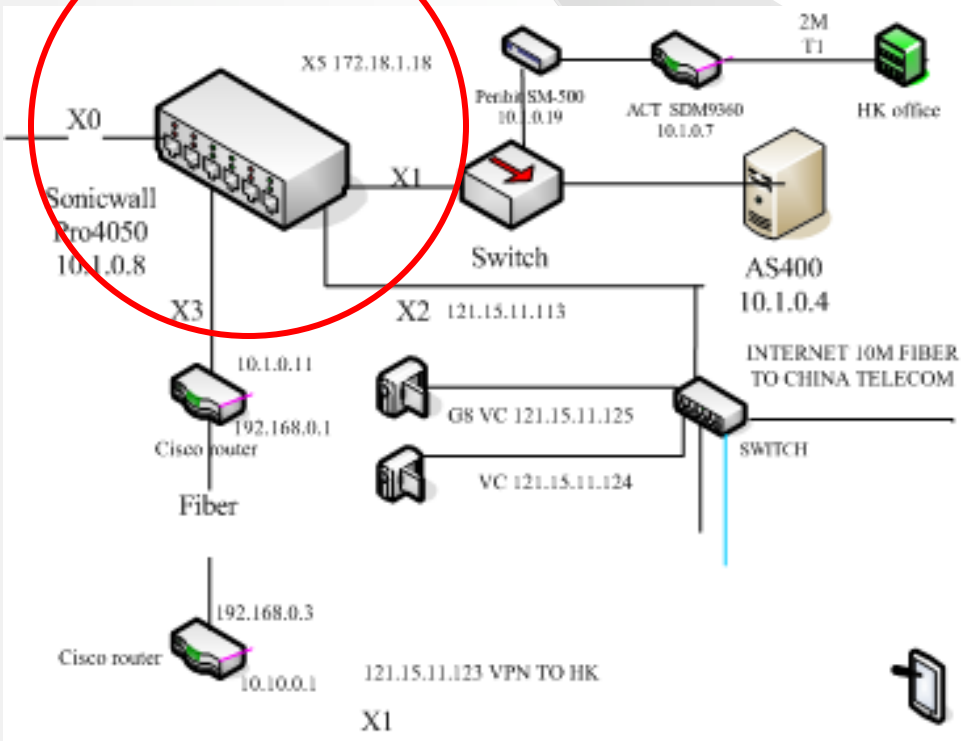
FIREWALLS – PACKET FILTERING

Stateless Packet Filtering

- An organization usually has a router that connects its internal network to its ISP, then to the Internet: all traffic leaving and entering the internal network passes through this router
- Most router provides option for filtering, i.e. some data packets pass through the router and filter out other data packets

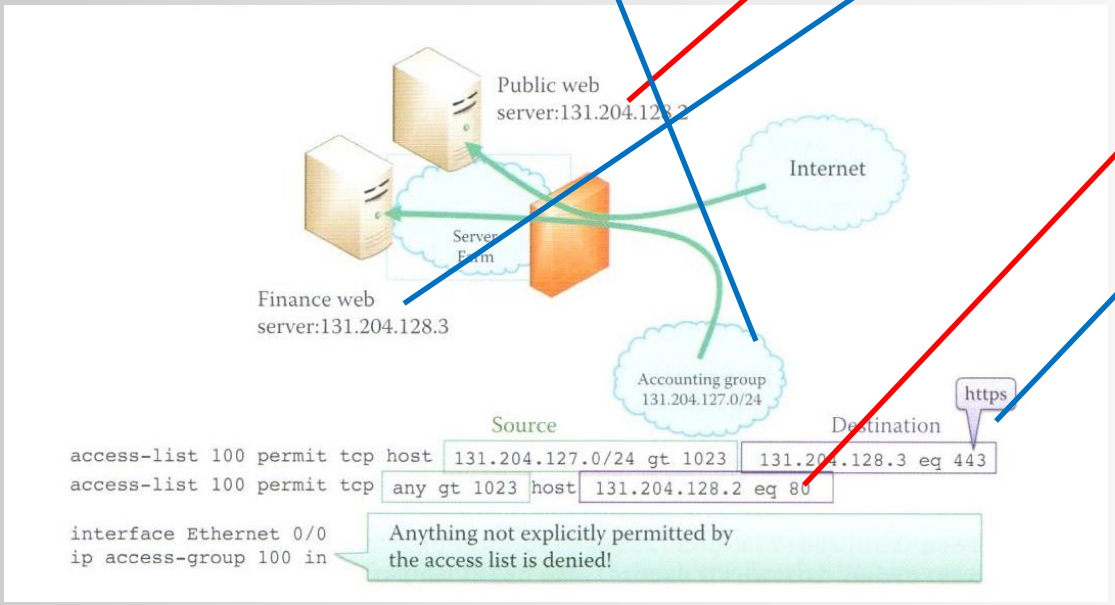
Typical filtering decision are based on:

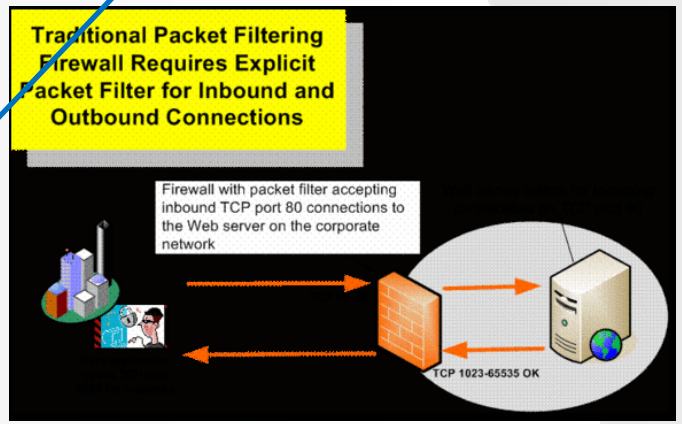
- Source IP address
- Destination IP address
- Source port
- Destination port
- Other data fields that commonly used by hackers, e.g. TCP SYN or ACK bits



Packet Filtering Rule

Action	Source	Port	Destination	Port
Allow	Any	Any	www.cs.hku.hk	TCP 80
Allow	IP address at accounting group	Any	finan.cs.hku.hk	TCP 443
Block	Any	Any	baidu.com	*

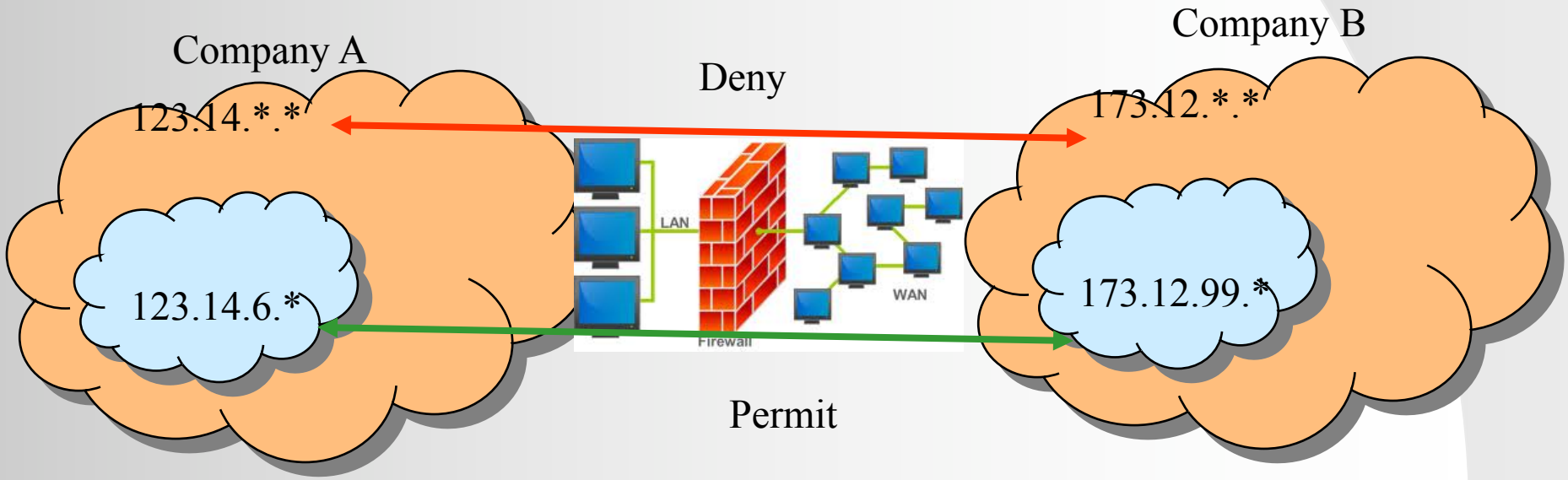




Filtering based on IP Addresses

Rule	Source IP address	Destination IP address	Action
1	173.12.99.*	123.14.6.*	Permit
2	173.12.*.*	123.14.*.*	Deny
3	123.14.6.*	173.12.99.*	Permit
4	123.14.*.*	173.12.*.*	Deny
5	*.*.*.*	*.*.*.*	Deny

Redundant



Filtering based on IP Addresses and Port Numbers

Rule	Connection	Type	Source IP addr	Dest. IP addr	Source Port	Dest. Port	Action
1	Inbound	TCP	External	Internal	≥1024	25	Permit
2	Inbound	TCP	Internal	External	25	≥1024	Permit
3	Outbound	TCP	Internal	External	≥1024	25	Permit
4	Outbound	TCP	External	Internal	25	≥1024	Permit
5	Any	Any	*.*.*.*	*.*.*.*	Any	Any	Deny

Rules for Simple Mail Transfer Protocol (SMTP)

- SMTP server listens to port 25
- Send email:
  - Permitting *outbound TCP connections* ***request*** with source port from internal client to external SMTP server (25) (Rule 3)
  - Permitting *outbound TCP connection* ***reply*** from SMTP server (25) to an internal client (Rule 4)
- What are the purposes of Rules 1 & 2?

SMTP Filtering Rules

- Need to include source port in the rules, otherwise lead to security holes, e.g. rules 2 & 4 would allow all connections between internal and external hosts with port numbers >= 1024
- Rule 4 should apply only to established connections that are initiated by an internal client
  - Should add an attribute to the rule parameters: the value of the ACK flag in the TCP header, which indicates the packet belongs to an established connection

Filtering with ACK Flag

Rule	Connection	Type	Source IP addr	Dest. IP addr	Source Port	Dest. Port	Flag	Action
1	Inbound	TCP	External	Internal	≥1024	25		Permit
2	Inbound	TCP	Internal	External	25	≥1024		Permit
3	Outbound	TCP	Internal	External	≥1024	25		Permit
4	Outbound	TCP	External	Internal	25	≥1024	ACK	Permit
5	Any	Any	*.*.*.*	*.*.*.*	Any	Any		Deny

Rules for Simple Mail Transfer Protocol (SMTP)

- SMTP server listens to port 25
- Rule 4 should apply only to established connections that are initiated by an internal client
- Do we need the ACK flag for Rule 2?

Stateless Packet Filtering Problem – IP Fragmentation

- A TCP segment or a UDP datagram is too big to fit into 1 packet
  - Port numbers and TCP ACK flag can be obtained from the first fragment only
  - Impossible to filter except the first packet
  - Need to introduce states into packet filters
- Commercial firewalls
  - Support packet filter per connection and service
  - Support actions other than “permit” and “deny”, such as user authentication and encryption, e.g. “perform FTP connection between any IP address and 123.14.6.23 if user authentication is successful”

Packet Filtering Problem – FTP Problem

- FTP server daemon listens on port 21
  - Client (random port) initiates ftp connect to port 21 of the FTP server
  - FTP data transfer on port 20, initiated by the FTP server to the client (another random port)
  - What are the rules?

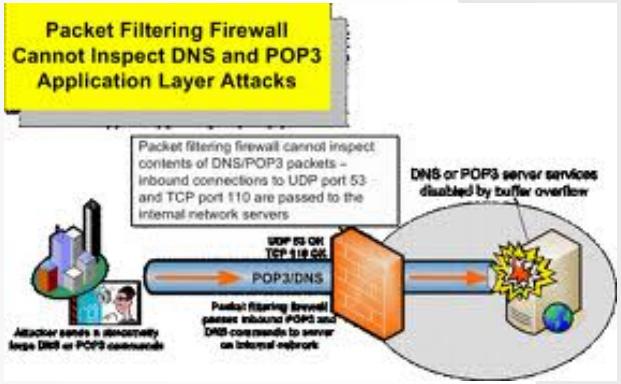
Rule	Connection	Type	Source IP addr	Dest. IP addr	Source Port	Dest. Port	Flag	Action
1	Outbound	TCP	Internal	External	≥1024	21		Permit
2	Outbound	TCP	External	Internal	21	≥1024	ACK	Permit
3	Inbound	TCP	External	Internal	20	≥1024		Permit
4	Inbound	TCP	Internal	External	≥1024	20	ACK	Permit
5	Any	Any	*.*.*.*	*.*.*.*	Any	Any		Deny

Security hole: Rule 3

Need to have states!!!

Limitations of Stateless Packet Filtering

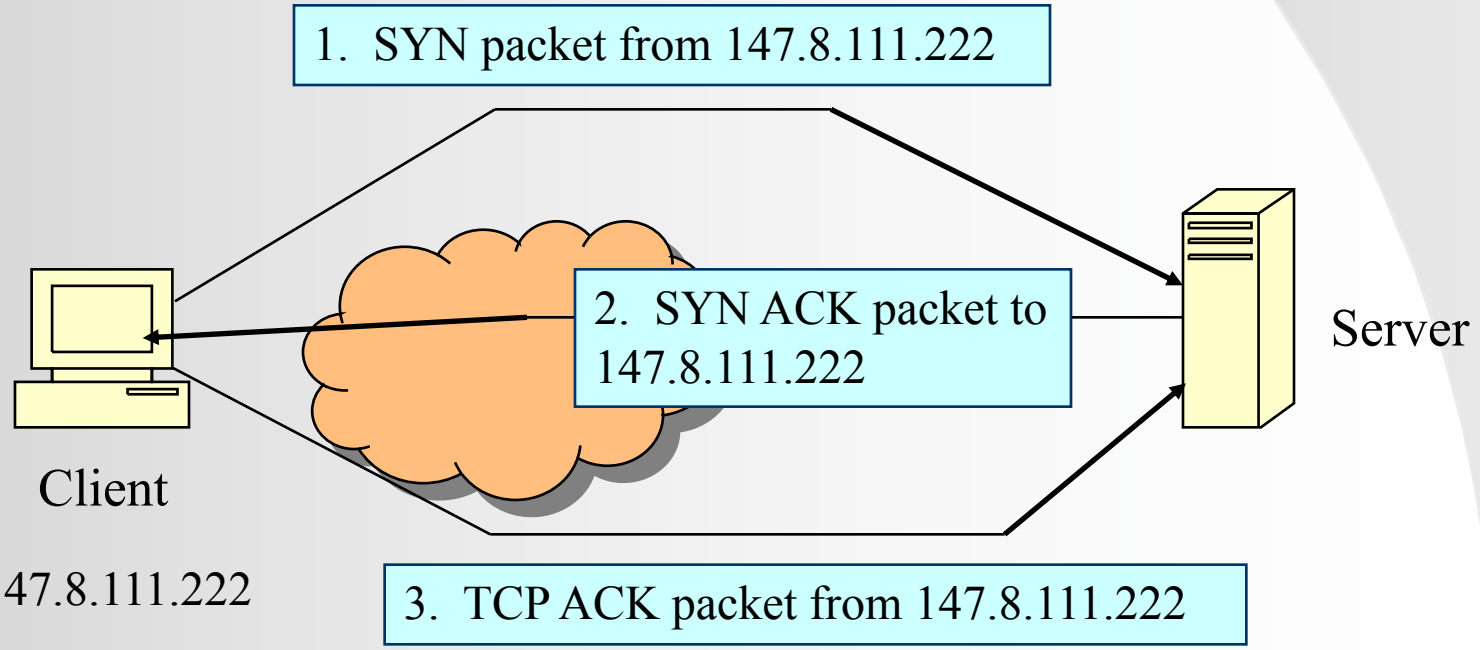
- Only control access based on source and destination information, do not monitor state of communication and application information, e.g. unable to limit certain users to use some services such as *telnet*
- Managing filtering rules is cumbersome, leading to simple mistakes, such as giving access right to threatening packets
- Well known problem:
  - Having a poorly configured firewall is worse than having no firewall at all because it gives you a false sense of security



TCP 3-Way Handshake

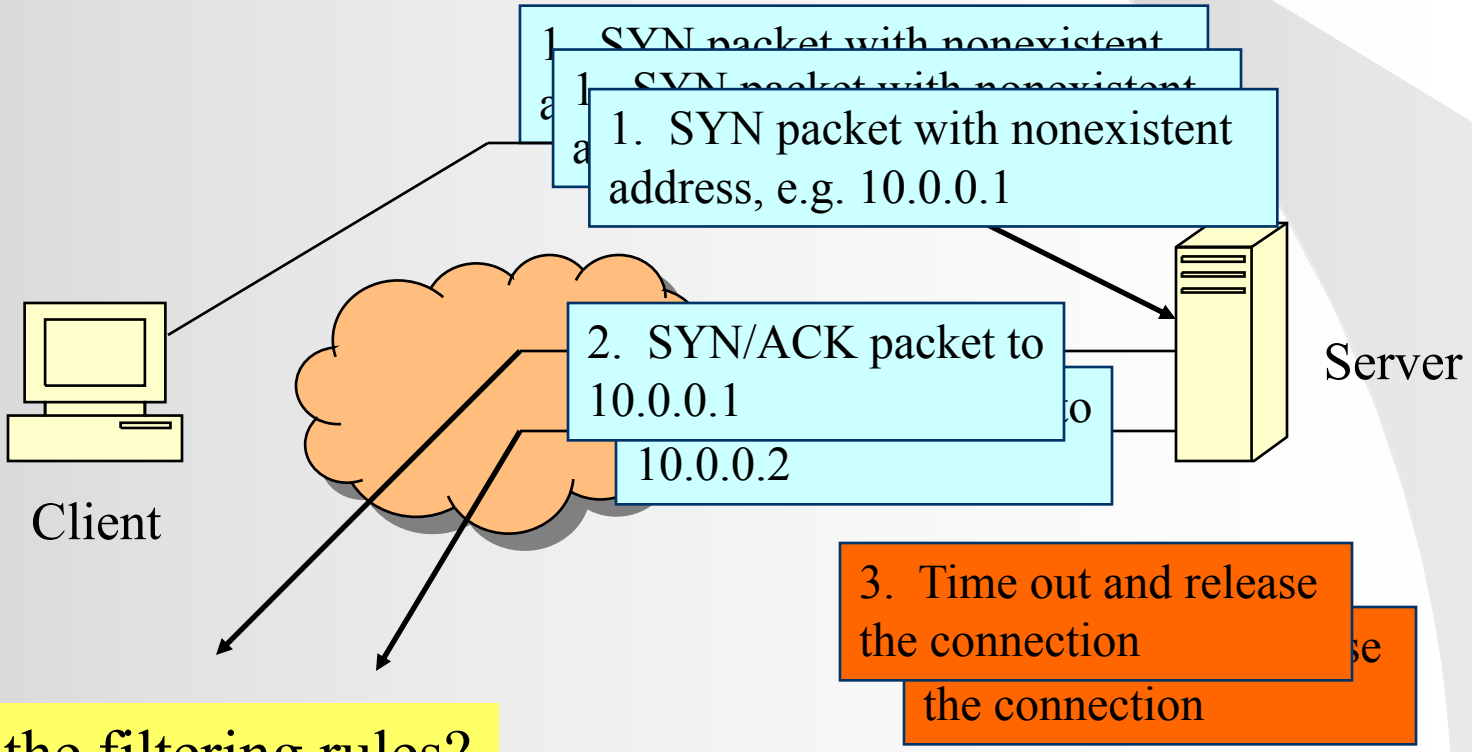
- Before a connection is established, the data transfer must be synchronized using the 3-way handshake
  - Client to server: (SYN flag, SeqNumC)
  - Server to client: (SYN/ACK flag, AckNumS=SeqNumC+1, SeqNumS)
  - Client to server: (ACK flag, AckNumC=SeqNumS+1)

TCP/IP 3-way handshake



SYN Flooding

- The attacks take the form of a large number of packets directed at the victim, e.g. SYN flooding
- SYN flooding
  - Send TCP connection requests faster than a system can process them
  - Exhaust states in the TCP/IP stack



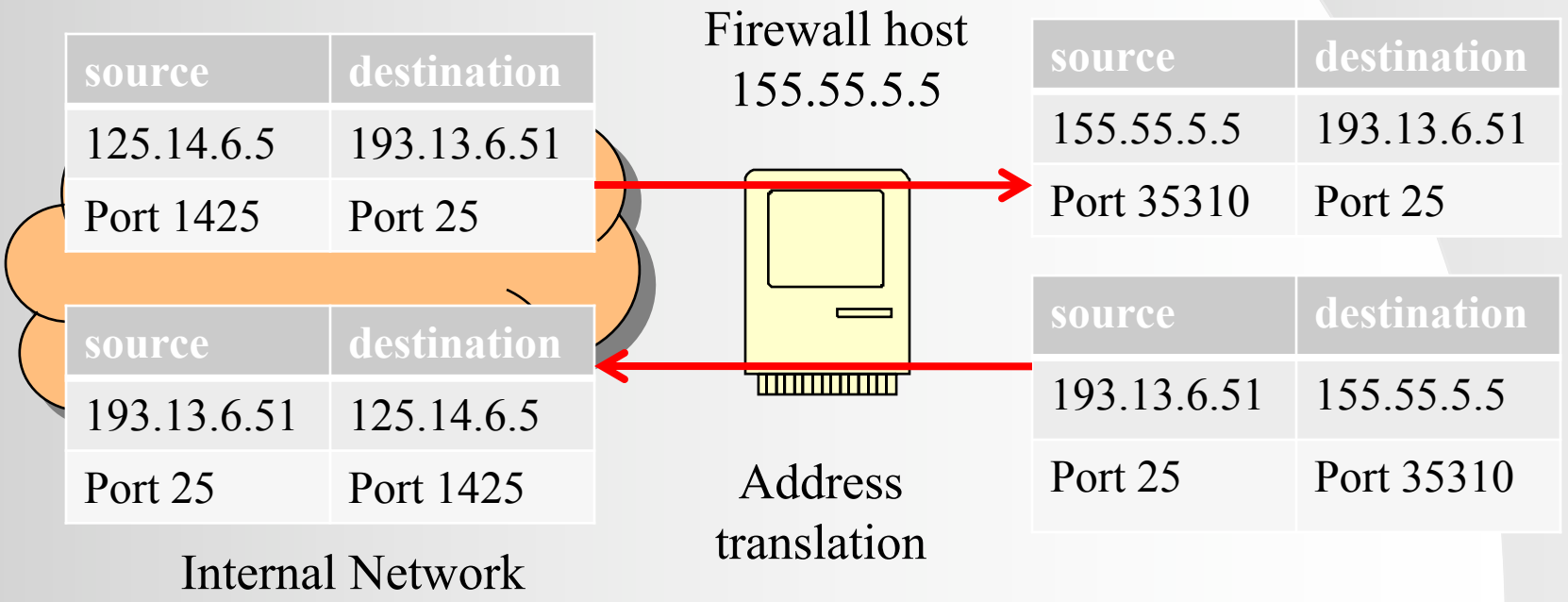
What are the filtering rules?

SYN Flooding Protection by Firewall

- Unable to handle with filtering rules
- Relay mechanism:
  - The firewall completes the 3-way handshake with an external client for an internal server
  - When the firewall receives the ACK from the client, it start a handshake with the server
- Gateway mechanism:
  - The firewall intercepts the SYN and ACK messages between the client and the server
  - The firewall does not wait from the ACK message from client, but sends the ACK immediately to the server
  - If no ACK is received from the client, the firewall sends a RST to the server
- Passive gateway
  - Similar to gateway mechanism except it does not send the ACK immediately, but with a shorter timeout period

Stateful Packet Filter
Network Address Translation (NAT)

- NAT (aka masquerading with port forwarding) is a mechanism for replacing one IP address in a packet with another IP address
  - Used to conceal the intranet's IP addresses for security reasons
  - To translate IP address from the intranet that are not valid with regard to the Internet



Problems with NAT when handling incoming requests

- When port number cannot be changed, e.g. service supported by a server
- When an external server must distinguish between clients based on their IP addresses, e.g. peer-to-peer application

Methods in handling incoming requests in NAT:

- Application level gateways
- Static port forwarding
- Universal Plug and Play (UPnP) Internet Gateway Device (IGD) protocol
- Traversal Using Relays around NAT (TURN)

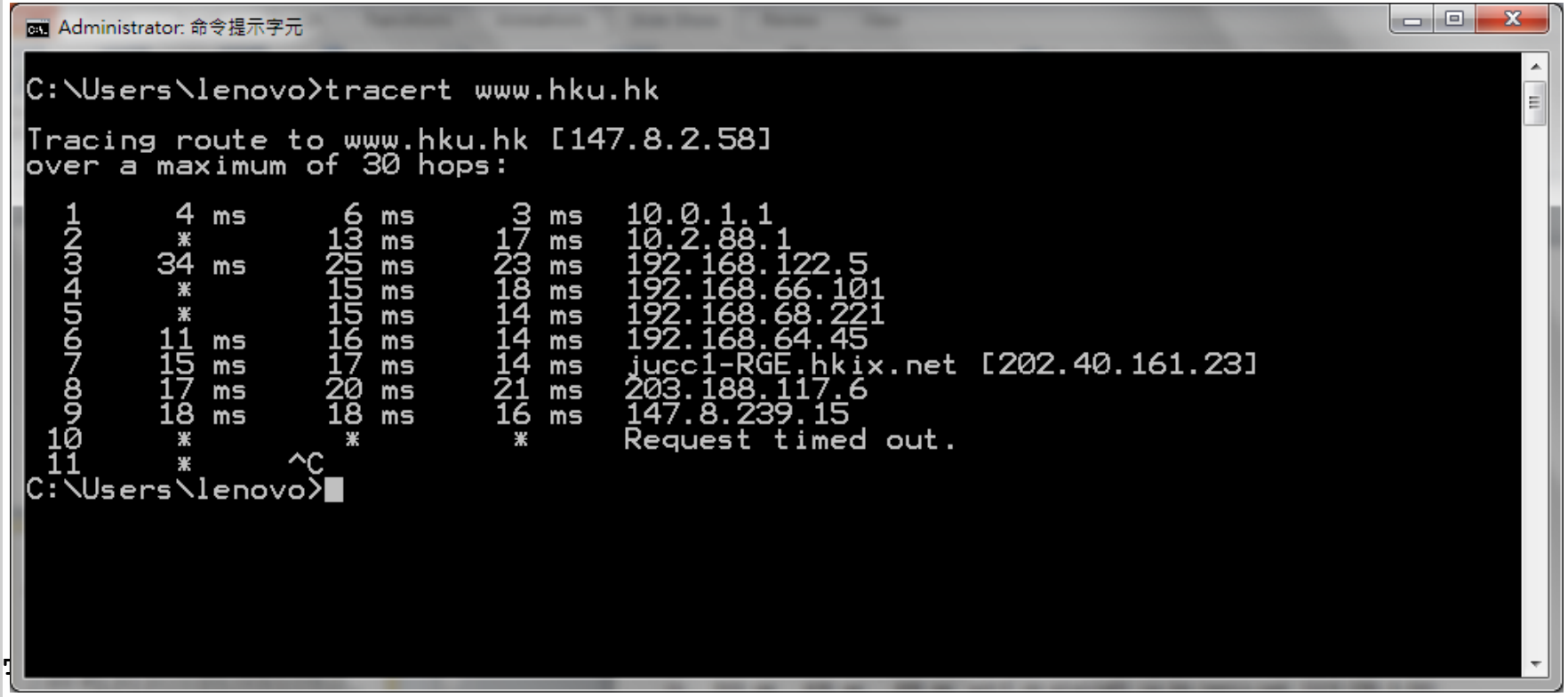
Common TCP/IP Network Tools

Common TCP/IP network tools

- Ping
  - tests whether another host is reachable
- traceroute
  - Determines the path taken to a destination
- nslookup
  - map hostname to an IP address, or map an IP address to hostname
- Netstat
  - Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics
- nbtstat
  - Displays NetBIOS over TCP/IP (NetBT) protocol statistics, NetBIOS name tables for both the local computer and remote computers, and the NetBIOS name cache

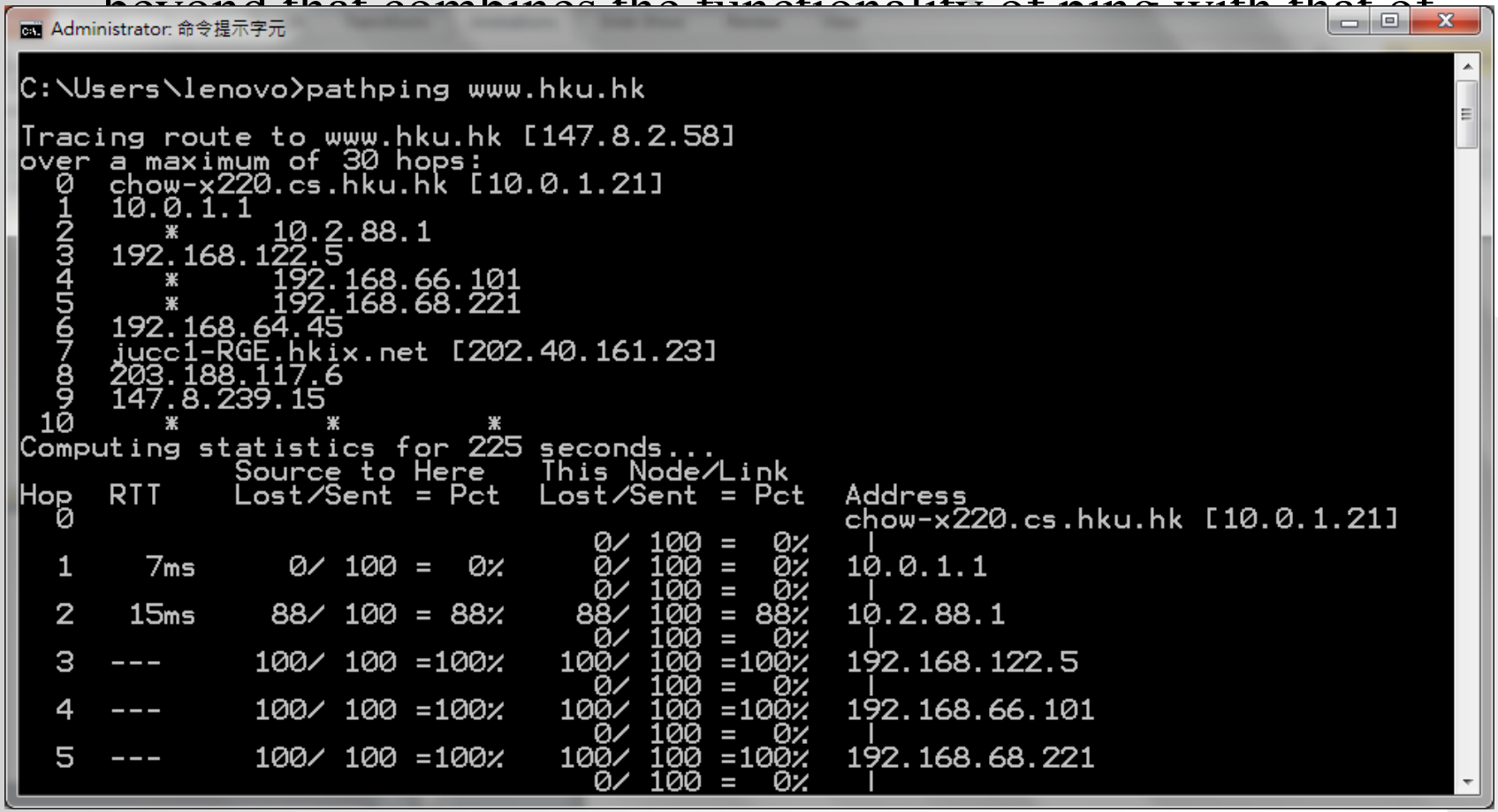
Tracert command

```
Tracing route to www.yahoo.akadns.net [64.58.76.227] over a maximum of 30 hops:

  1    25 ms    23 ms    24 ms  cm203-168-208-1.hkcable.com.hk [203.168.208.1]
  2    32 ms    27 ms    36 ms  10.255.36.254
  3    28 ms    24 ms    30 ms  192.168.16.50
```

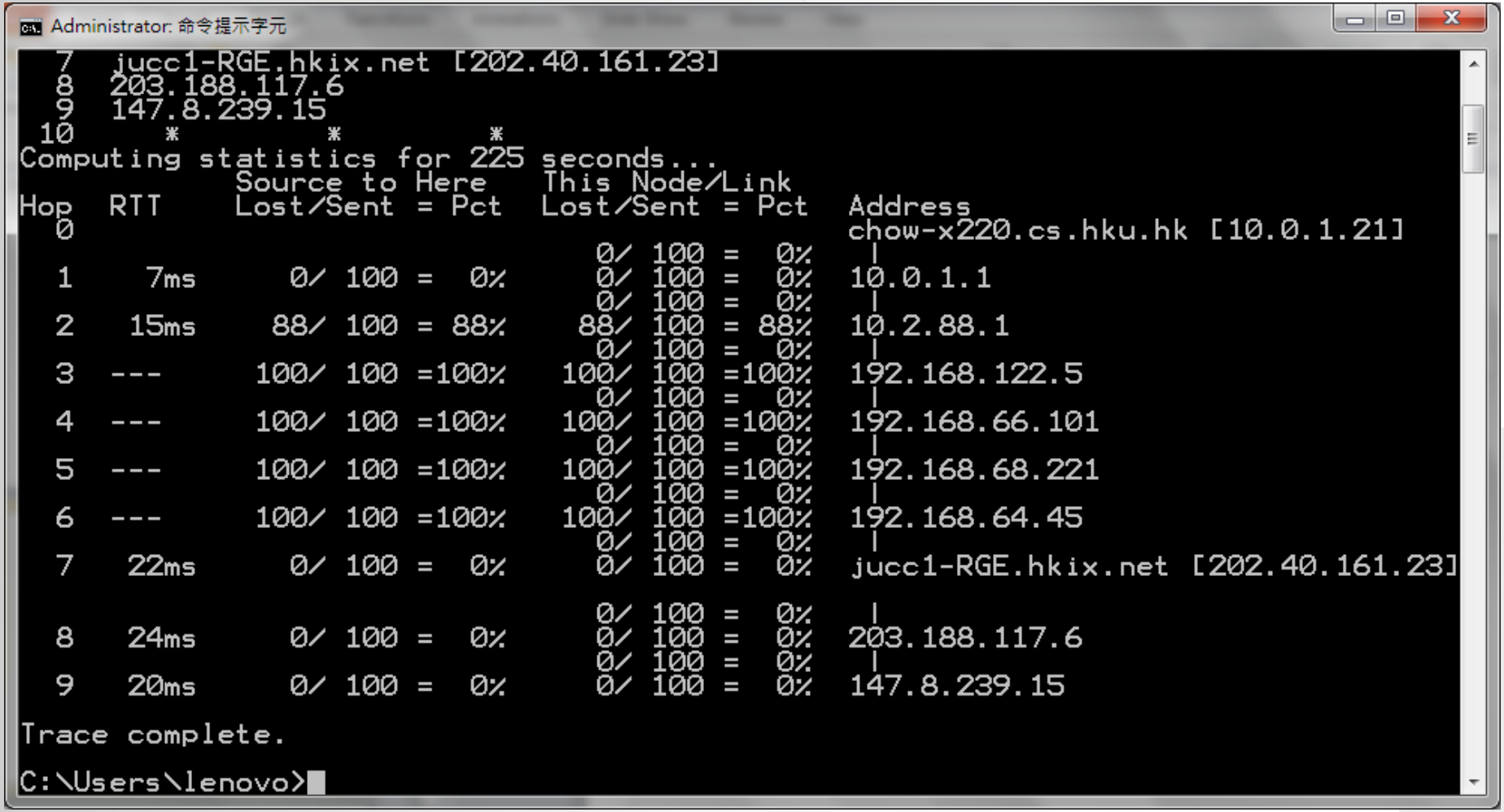


PathPing

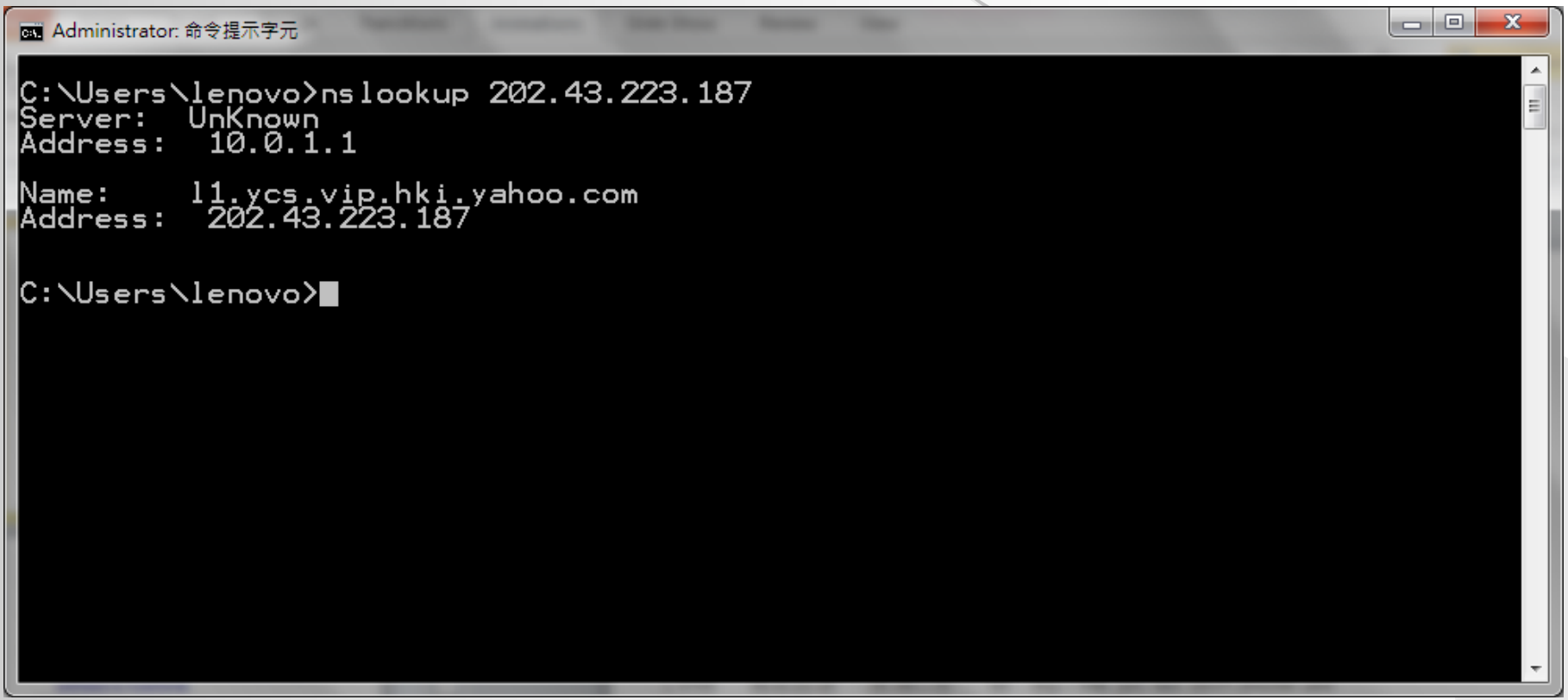
- PathPing is a network utility supplied in Windows NT and beyond that combines the functionality of ping with that of



Pathping


Administrator: 命令提示字元
7 jucc1-RGE.hkix.net [202.40.161.23]
8 203.188.117.6
9 147.8.239.15
10 * * *
Computing statistics for 225 seconds...
Source to Here This Node/Link
Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address
0 chow-x220.cs.hku.hk [10.0.1.21]
0/ 100 = 0% |
1 7ms 0/ 100 = 0% 0/ 100 = 0% 10.0.1.1
0/ 100 = 0% |
2 15ms 88/ 100 = 88% 88/ 100 = 88% 10.2.88.1
0/ 100 = 0% |
3 --- 100/ 100 =100% 100/ 100 =100% 192.168.122.5
0/ 100 = 0% |
4 --- 100/ 100 =100% 100/ 100 =100% 192.168.66.101
0/ 100 = 0% |
5 --- 100/ 100 =100% 100/ 100 =100% 192.168.68.221
0/ 100 = 0% |
6 --- 100/ 100 =100% 100/ 100 =100% 192.168.64.45
0/ 100 = 0% |
7 22ms 0/ 100 = 0% 0/ 100 = 0% jucc1-RGE.hkix.net [202.40.161.23]
0/ 100 = 0% |
8 24ms 0/ 100 = 0% 0/ 100 = 0% 203.188.117.6
0/ 100 = 0% |
9 20ms 0/ 100 = 0% 0/ 100 = 0% 147.8.239.15
Trace complete.
C:\Users\lenovo>

The nslookup command

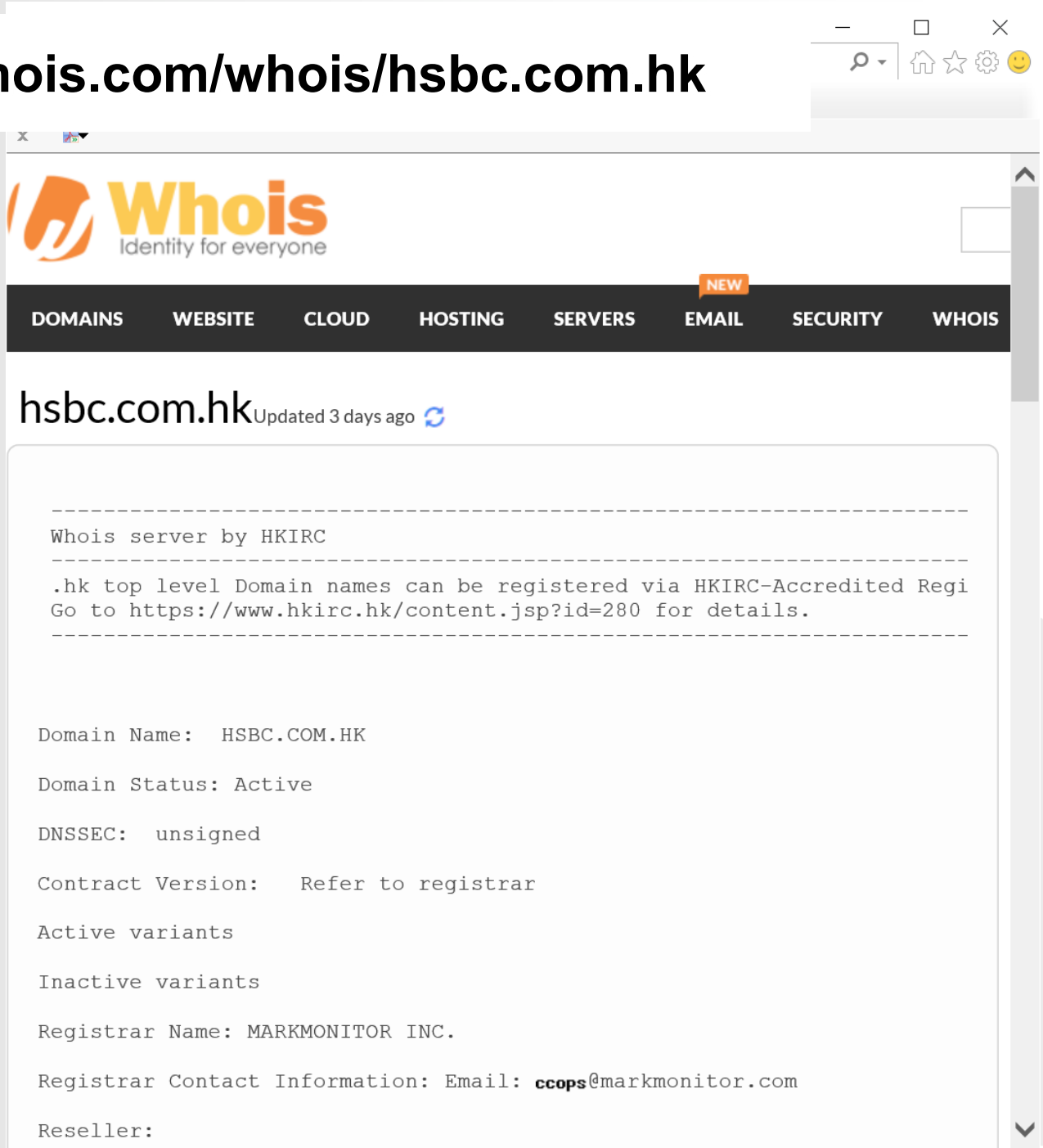


Network Applications: WHOIS

Who is Who

- **WHOIS** is a query and response protocol that is widely used for querying databases that store the registered users or assignees of an Internet resource, such as a domain name, an IP address block, or an autonomous system, but is also used for a wider range of other information.
- The protocol stores and delivers database content in a human-readable format. The WHOIS protocol is documented in RFC 3912.

https://www.whois.com/whois/hsbc.com.hk

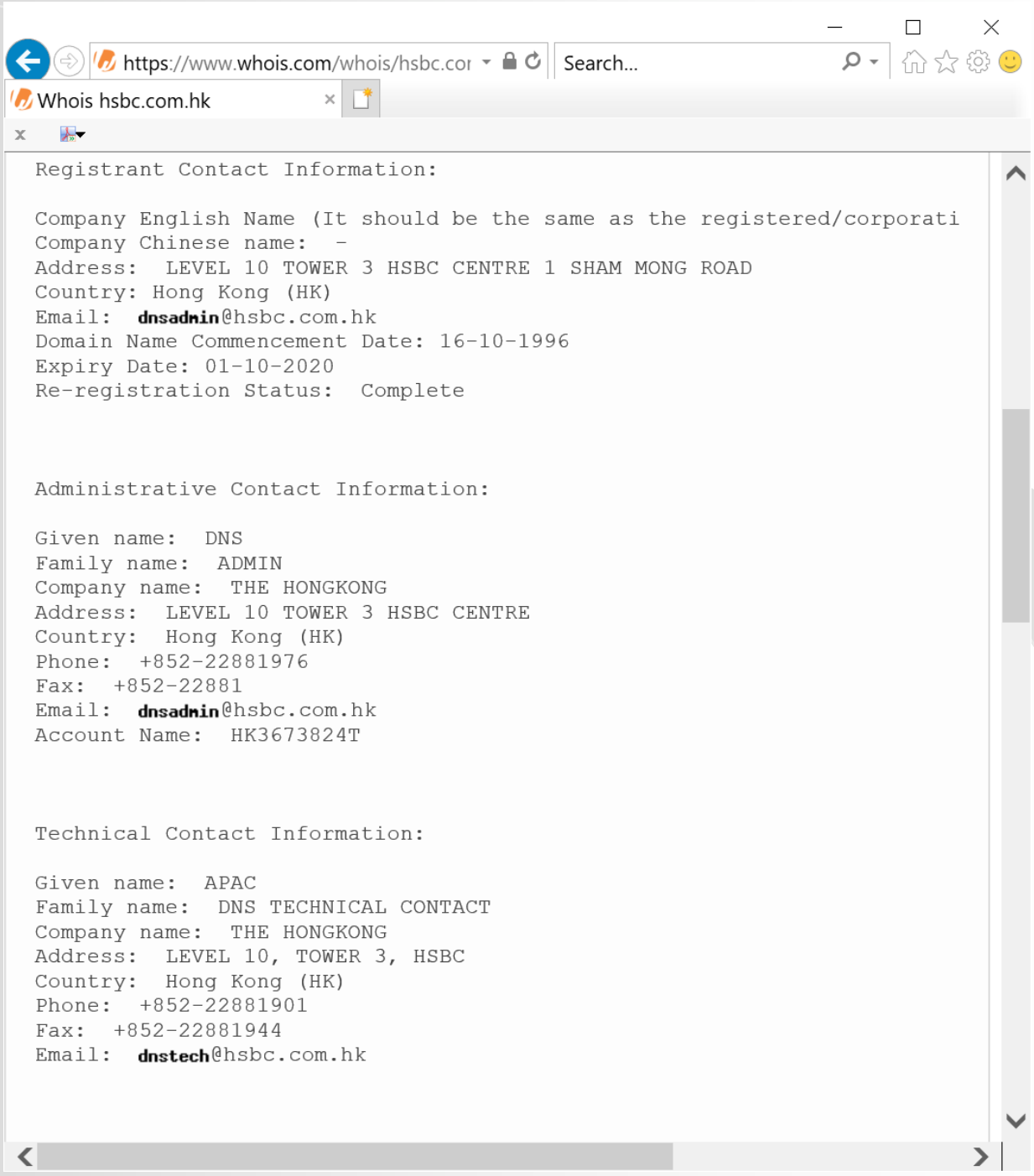


Whois
Identity for everyone

DOMAINS | WEBSITE | CLOUD | HOSTING | SERVERS | NEW EMAIL | SECURITY | WHOIS

hsbc.com.hk Updated 3 days ago

```
---------------------------------------------------------------------
Whois server by HKIRC
---------------------------------------------------------------------
.hk top level Domain names can be registered via HKIRC-Accredited Regi
Go to https://www.hkirc.hk/content.jsp?id=280 for details.
---------------------------------------------------------------------


Domain Name:  HSBC.COM.HK

Domain Status: Active

DNSSEC:  unsigned

Contract Version:   Refer to registrar

Active variants

Inactive variants

Registrar Name: MARKMONITOR INC.

Registrar Contact Information: Email: ccops@markmonitor.com

Reseller:
```



Registrant Contact Information:

Company English Name (It should be the same as the registered/corporati
Company Chinese name: -
Address: LEVEL 10 TOWER 3 HSBC CENTRE 1 SHAM MONG ROAD
Country: Hong Kong (HK)
Email: dnsadmin@hsbc.com.hk
Domain Name Commencement Date: 16-10-1996
Expiry Date: 01-10-2020
Re-registration Status: Complete

Administrative Contact Information:

Given name: DNS
Family name: ADMIN
Company name: THE HONGKONG
Address: LEVEL 10 TOWER 3 HSBC CENTRE
Country: Hong Kong (HK)
Phone: +852-22881976
Fax: +852-22881
Email: dnsadmin@hsbc.com.hk
Account Name: HK3673824T

Technical Contact Information:

Given name: APAC
Family name: DNS TECHNICAL CONTACT
Company name: THE HONGKONG
Address: LEVEL 10, TOWER 3, HSBC
Country: Hong Kong (HK)
Phone: +852-22881901
Fax: +852-22881944
Email: dnstech@hsbc.com.hk

Whois Database

- http://www.apnic.net/
- http://www.arin.net