

Asia Pacific Network Information Centre  
APNIC

# Welcome!

## APNIC Security Tutorial

*Securing edge network devices*

6 September 2005, Hanoi, Vietnam

*In conjunction with APNIC20*

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### Overview

- Edge security principles
- Threats categories
- Securing edge devices
- Routing protocol security
- Vulnerability update

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### Edge security

Edge security is all about securing the edge devices from any attacks.

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

### Basic principles of network security

- Ability to Identify
- Verification of trust
- Implementation of the policy
- Risk analysis
- Security assessment

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

### Network infrastructure

- Different types of Network infrastructure which can be vulnerable to any attacks
  - Enterprise Networks
  - SME networks
  - Home Users
  - ISP Networks

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

### Edge security

Key points:

- Protect your network
- Provide inside protection from internet users
- Protect the internet from internal users
- Always be ready for any attacks because at any given time there is a possibility...

---

---

---

---

---

---

---

---

### Edge security actions

First priority: protect the router from any attack.

- Protect the router from any types of attack either *Direct attack* or *Break-in*
  - Protect the Routing Protocol from any *Direct attack* or *Route insertion*
  - Protect the Network from *Direct attack* or *Redirection*
- Deploy measures and Stop/Rate-Limit them on the edge of the Network
- Collect data of the attack for further analysis and possible Law enforcement actions.

---

---

---

---

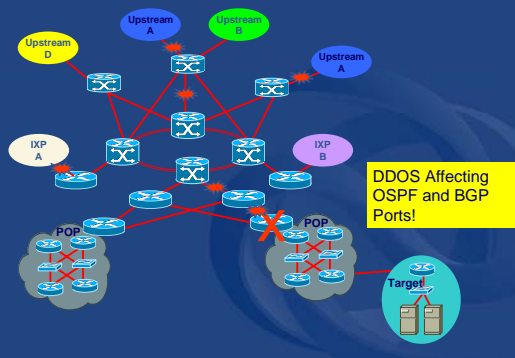
---

---

---

---

### DOS/DDOS attacks today



---

---

---

---

---

---

---

---

### Important things to note

- There are no magic knobs, grand security solutions, or super vendor features that will solve the security problem.
- Likewise, there is no rocket science involved. Just hard work that is within all grasp.

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

# Questions?

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

# Three Key Threat Categories

---

---

---

---

---




---

---

---

APNIC Asia Pacific Network Information Centre

## Classes of threats

- **Reconnaissance**
  - Unauthorized discovery and mapping of systems, services, or vulnerabilities
- **Access**
  - Unauthorized data manipulation, system access, or privilege escalation
- **Denial of Service**
  - Disable or corrupt networks, systems, or services

---

---

---

---

---

---

---

---

### What is the impact?

- **Reconnaissance**
  - Happens all the time
  - It is part of the “attack noise” of the Internet
  - along with low level attacks and backscatter
- **Access**
  - Break-ins on the edge of the network (I.e. customer CPE equipment)
- **DoS**
  - The core threat – knocking out infrastructure, and services

---

---

---

---

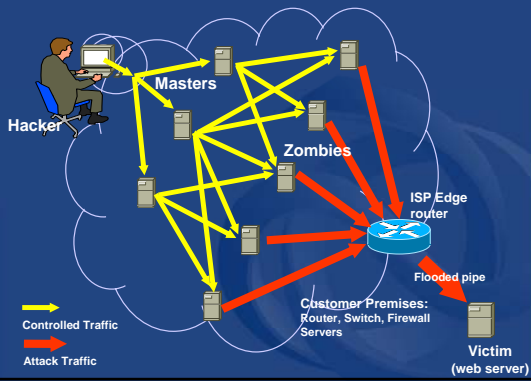
---

---

---

---

### DoS inside ISPs



---

---

---

---

---

---

---

---

### Other attacks

#### Attacks & exploits happening via other protocols

- MAC Addresses
- HTTP
- CDP
- DHCP
- RPC
- DNS
- ..... and many more

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

## Questions?

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

## Securing the edge device

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

## Network device patching / hardening

- Configuring the devices to a step that is taken to ensure the proper operations of the device in a network to increased the security.
- Network devices
  - Switch
  - Router

---

---

---

---

---

---

---

---

APNIC  
 Asia Pacific Network Information Centre

### Switch security

- Silent workhorse of the network
  - Handles the traffic they send and receive
- ARP poisoning
  - Primary attack against a switch
- Port security
  - MAC address security
- VLAN
  - Controls the ARP broadcast

---

---

---

---

---

---

---

---

APNIC  
 Asia Pacific Network Information Centre

### Router security

- Software version
- Control access
- Access control list (ACL)
- Authentication and Authorization
- Access privilege levels
- Unnecessary services and protocols
- Administrative practices
- Simple Network Management Protocol
- Logging

---

---

---

---

---

---

---

---

APNIC  
 Asia Pacific Network Information Centre

### Router security (cont.)

- Edge network devices . It provides an entry to the network
- Routers can initiate attacks into other networks
- Break-in into routers that act as firewalls create more problems.

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre

**APNIC**

## Software version

- Patches with the latest updates released by vendors
- Version security vulnerability

Command

```
sh version
```

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre

**APNIC**

## Control access

- Physical access to router

Console port access

- Through a cable connected to the serial port
- Console access is the default mode of access
- Console port is also used for router password recovery

Auxiliary port access

- Generally used for out of band access
- Also used for connecting to other routers' console port

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre

**APNIC**

## Control access (cont.)

- Virtual access to router

Virtual terminal (line VTY)

- Virtual terminal are provided to get access over the network
- Default protocol is telnet but ssh mode is also possible

HTTP

- Web configuration utility

TFTP

- TFTP to get upload and download software images
- Configuration at boot time

SNMP

- For router performance monitoring using read-only or readwrite

---

---

---

---

---

---

---

---



### Access control list (ACL)

- Routers ability to perform IP packet filtering
  - Filtering based on destination or sources address
  - Filtering TCP or UDP traffic with either permit or deny parameters

---

---

---

---

---

---

---

---

### Access control list (cont.)

- Limiting access to line VTY with specific IP address

```
router (config)# access-list 1 permit 192.168.0.1
router (config)# access-list 1 permit 192.168.0.2
router (config)# access-list 1 deny any
router (config)# line vty 0 4
router (config-line)# access-class 1 in
```

---

---

---

---

---

---

---

---

### Access control list (cont.)

- Limiting access to a single host with only Telnet and SSH access, and denies any IP address to access

```
router (config)# access-list 100 permit 192.168.0.1 host
192.168.1.1 eq telnet
router (config)# access-list 100 permit 192.168.0.1 host
192.168.1.1 eq ssh
router (config)# access-list 100 deny all host 192.168.1.1 eq
telnet
router (config)# access-list 100 deny all host 192.168.1.1 eq ssh
router (config)# access-list 100 permit all all

router (config)# interface ethernet 0
router (config-if)# ip access-group 100 in
```

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### Access control list (cont.)

- Disallowing HTTP access to host 192.168.0.1

```
router (config)# access-list 101 deny tcp 192.168.0.1 any
eq www
router (config)# access-list 101 permit ip any any
router (config)# interface ethernet 1
router (config-if)# ip access-group 101 in
```

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### Access control list (cont.)

#### Limiting HTTP server IP

```
router (config)# access-list 10 permit 192.168.0.1
router (config)# access-list 10 deny any
router (config)# ip http access-class 10
```

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### Authentication / Authorisation

#### Setup console password

```
router (config)# line console 0
router (config-line)# login
router (config-line)# password console-password
```

#### Setup AUX password

```
router (config)# line aux 0
router (config-line)# login
router (config-line)# password aux-password
```

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

### Authentication / Authorisation (cont.)

Setup Line Virtual Terminal (VTY) Password

```
router (config)# line vty 0 4
router (config-line)# login
router (config-line)# password vtty-password
```

Enabling Encryption

```
router (config)# service password-encryption
```

Enabling privilege level password

```
router (config)# enable secret enable-secret
```

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

### Authentication / Authorisation (cont.)

Setup local users

```
router (config)# username mants password password
```

Enable local authentication on VTY terminal

```
router (config)# line vty 0 4
router (config-line)# login local
```

Enable router authentication

```
router (config)# aaa new model
router (config)# aaa authentication default local
```

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

### Access privilege levels

Cisco routers privilege levels

- User mode level 1
  - Check the router status and operation
  - Configuration is not visible
  - Prompt = **router>**
- Privileged mode level 15
  - Allows complete control to the router
  - Does not allow alteration of configuration
  - Prompt = **router#**
- Configuration mode level 15
  - Mode to change configuration settings
  - Full control of the router configuration
  - Prompt = **router(config)#**

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

## Security requirements

By default with Cisco routers there are three privilege levels.

- **Privilege level 1** = non-privileged (prompt is router>), the default level for logging in
- **Privilege level 15** = privileged (prompt is router#), the level after going into enable mode
- **Privilege level 0** = seldom used, but includes 5 commands: *disable*, *enable*, *exit*, *help*, and *logout*
- **Levels 2-14** are not used in a default configuration, but commands that are normally at level 15 can be moved down to one of those levels and commands that are normally at level 1 can be moved up to one of those levels. Obviously, this security model involves some administration on the router.

Cisco Systems Tech Notes

---

---

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

## Access privilege levels (cont.)

### Viewing Privilege Levels

```
router>show privilege
Current privilege level is 1

router>enable
password: enable secret

router#show privilege
Current privilege level is 15
```

---

---

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

## Access privilege levels (cont.)

### Moving between Privilege Levels

```
router#show privilege
Current privilege level is 15

router #disable 5
router#show privilege
Current privilege level is 5

router #enable 10
router#show privilege
Current privilege level is 10
```

---

---

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre

**APNIC**

### Access privilege levels (cont.)

Centralizing access management

- To simplify accounts configuration synchronization
  - To avoid using local username and password
- Use of Authentication / authorization application
  - Terminal Access Controller Access Control System (TACACS)
  - Remote Authentication Dial-In User Service (RADIUS)

---

---

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre

**APNIC**

### Access privilege levels (cont.)

How enable TACACS+ or RADIUS and configure central account repository

```

aaa new-model
aaa authentication login default tacacs+ local
tacacs-server host 192.168.0.2
tacacs-server key security
tacacs-server last-resort password
  
```

---

---

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre

**APNIC**

### Unnecessary service and protocol

- Disable unneeded service and protocol to increase overall security
- Proxy ARP
  - Allows one host to respond to ARP request on behalf of the real host
  - Allows an attacker to mount ARP poisoning against host

---

---

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### Unnecessary service and protocol (cont.)

Disable proxy ARP

```
router(config)#interface ethernet 0
router(config-if)#no ip proxy-arp
```

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### Unnecessary service and protocol (cont.)

- Cisco Discovery Protocol
  - Enable Cisco devices to contain information such as IP address and software version
  - Allows the attacker to gain valuable information about the devices

```
router(config)#no cdp run
```

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### Unnecessary service and protocol (cont.)

- Diagnostics servers
  - Enabled for certain UDP and TCP services, including echo, chargen, discard, daytime.
  - Allows the attacker to send large amount of request to echo, chargen and discharge port from random addresses

```
router(config)#no service udp-small-servers
router(config)#no service tcp-small-servers
```

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### Unnecessary service and protocol (cont.)

- BOOTP server
  - Used to provide DHCP addresses to clients through BOOTP service.

```
router(config)#no ip bootp server
```

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### Unnecessary service and protocol (cont.)

- TFTP server
  - Used to transfer files and software upgrades to and from the router
  - TFTP does not provide authentication and authorisation service

```
router(config)#no tftp-server
```

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### Unnecessary service and protocol (cont.)

- Finger server
  - Used to query who is logged in to the router from and where.
  - Can be source of information leakage

```
router(config)#no service finger
```

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### Unnecessary service and protocol (cont.)

- Web server
  - Used to provide web server access for making configuration changes.
  - Disable service is the router will not be manage in this manner

```
router(config)#no ip http server
```

---

---

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### Administrative practices

- Methods to manage the device
- Command line
  - Telnet
  - Secure Shell Protocol (SSH)
- Web interface
- SNMP (monitoring and management)
- Warning messages is require during login

---

---

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### Administrative practices (cont.)

- Banner to display the warning message
- Remove important information which identify the type and operating system of the device

```
router (config)# banner login ^
Enter TEXT message. End with the Character '^'.
Warning !!!
This system belongs to Amante. Unauthorized
access is prohibited which is a violation of the
cyberlaw of the country and will result in
procecuton. ^
```

---

---

---

---

---

---

---

---

---

---



APNIC Asia Pacific Network Information Centre

### Administrative practices (cont.)

- Banner message types

```
router (config)# banner login ^ banner login ^
router (config)# banner exec ^ banner exec ^
router (config)# banner motd ^ banner motd ^
```

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

### Administrative practices (cont.)

- Remote Command line
- Telnet weakness is cannot protect communication over a transit network
- More secure way is thru Secure Shell (SSH) Protocol
- Failure to encrypt the administrative connection to routers will allow an attacker to capture sensitive information

```
router (config)# hostname amante
router (config)# ip domain-name amante
router (config)# crypto key generate rsa
router (config)# aaa new model
router (config)# username amante password amante
router (config)# hostname amante
router (config)# ip ssh timeout seconds
router (config)# ip ssh authentication-retries integer
```

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

### Simple network management protocol (SNMP)

- Provides centralized mechanism to monitor and configure routers
- Monitoring to CPU load, and personal alerts by sending *traps*

```
snmp-server community readonly RW
snmp-server community readwrite RO
snmp-server host 10.1.1.11 traps private

access-list 100 permit udp host 192.168.0.1 host 192.168.1.1 eq snmp
```

---

---

---

---

---

---

---

---

## Simple network management protocol (SNMP) (cont.)

Configuring Read-only SNMP Access

```
router (config)# snmp-server community infracom RO
```

Using ACLs to limit SNMP access. Completely disabling SNMP

```
router (config)# access-list 1 permit 192.168.0.1  
router (config)# access-list 1 permit 192.168.0.200  
router (config)# access-list 1 deny any  
router (config)# snmp-server community community RO 1
```

---

---

---

---

---

---

---

---

## Simple network management protocol (SNMP) (cont.)

Configuring SNMP v3

```
router (config)# snmp-server view TESTV3 mib-2 include  
router (config)# snmp-server group ORAROV3 v3 auth read  
TESTv3
```

Using MD5 authentication without encryption

```
router (config)# snmp-server user cking ORAROV3 v3 auth md5  
daytoday
```

Using MD5 authentication with DES encryption

```
router (config)# snmp-server user cking ORAROV3 v3 auth md5  
hotkeyrules priv des56 shortguy
```

---

---

---

---

---

---

---

---

## ICMP unreachable messages

- ICMP type 3 destination unreachable message
- Router returns a message if the address or service is specified unreachable
- There are over 15 different type of codes that can be specified
- Malicious attackers can use this message type to determine available host or service.

```
no ip unreachable
```

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### ICMP directed broadcast

- First and last IP address (network and broadcast)
- Sending a packet to either of those is like sending packets to each host of the subnet
- Method like "*bandwidth amplification*" are used by attackers
- Attack tools are known as "smurf attack" and fraggle.

no ip directed-broadcast

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### ICMP redirects

- Used for information of more efficient route path to a network
- Use by routers that belongs to same subnet
- Attackers can manipulate the routing paths, and redirects to untrusted external networks

no ip redirects

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### Anti-spoofing and Source routing

- Attacker insert a fake or spoofed information in TCP/IP packet header
- Dropping such packets protect the network with such kind of attack
- Drop the packet that contain source routing information

no ip source route

---

---

---

---

---

---

---

---

APNIC  
 Asia Pacific Network Information Centre

## Logging

- Maintain logs to gain knowledge of the network traffic behavior
- Can be configured locally
- Can be provide facilities for remote logging to a syslog server

```

logging server enable
logging server 192.168.0.1
  
```

---

---

---

---

---

---

---

---

APNIC  
 Asia Pacific Network Information Centre

## Monitoring

- **SNMP**
  - Watching the baseline and tracking variations/surges
  - Also looking for specific triggers (CPU and input buffer drops are the top two)
- **SYSLOG**
  - Watching the baseline
  - Looking for specific triggers (SNMP Authentication Failure)
  - Watching the ACL Logs
- **Netflow**
  - Anomaly Detection Tools
  - Triggers on flow table overloads

---

---

---

---

---

---

---

---

APNIC  
 Asia Pacific Network Information Centre

## Monitoring (cont.)

- **Netflow**
  - Identify the attack
  - Count the flows
  - Inactive flows signal a worm attack
- **Classify the attack**
  - Small size flows to same destination
  - What is being attacked and origination of attack

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

## Routing protocol security

- Interior routing protocol
  - OSPF
  - ISIS
- Exterior routing protocol
  - BGPv4

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

## OSPF protocol

- Provide security to OSPF protocol by enabling the authentication
- MD5 authentication for OSPF.

Enable authentication to each interface participating the OSPF.

```
router (config)#int fa0/0
router (config-if)#ip ospf message-digest-key 1 md5 pwdkey

router (config)#int eth0/0
router (config-if)#ip ospf message-digest-key 1 md5 pwdkey
```

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

## OSPF protocol (cont.)

Then enable authentication the OSPF configuration.

Enter Configuration Commands,

```
router (config)#router ospf 100
router (config-router)#area 0 authentication message-digest
```

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### OSPF protocol (cont.)

Filtering routes with OSPF

- Prevent the IP to be put in the routing table for inbound routes

```
router (config)#access-list 1 deny 192.168.0.1
router (config)#access-list 1 permit any
router (config)#router ospf 100
router (config-router)#distribute-list 1 in ethernet0
```

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### ISIS protocol

- ISIS authentication configuration for ISIS neighbors

```
router (config)#interface ethernet 0
router (config-if)#ip router isis
router (config-if)#isis password cisco level-2
```

---

---

---

---

---

---

---

---

Asia Pacific Network Information Centre  
APNIC

### BGP protocol

- BGP authentication is enable to peers configuration
- Allowing definitions of password differently for every peers.

```
router (config)#router bgp 100
router (config-router)#neighbor 192.168.0.1
remote-as 101
router (config-router)#neighbor 192.168.0.1
password mypassword
```

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

### BGP protocol (cont.)

- Route filtering with BGP prefix lists
- Filter ingress and egress routes.
- Similar to access-lists function but base on IP address only
- Applied to peers only

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

### BGP protocol (cont.)

```
ip prefix-list out-peer permit 100.4.0.0/18 le 32
ip prefix-list out-peer deny 0.0.0.0/0 le 32

ip prefix-list in-peer permit 100.1.0.0/18 le 32
ip prefix-list in-peer deny 0.0.0.0/0 le 32

router bgp 4
no synchronization
network 100.4.32.0 mask 255.255.240.0
neighbor 100.1.2.1 remote-as 1
neighbor 100.1.2.1 description eBGP peering with Router1
neighbor 100.1.2.1 prefix-list out-peer out
neighbor 100.1.2.1 prefix-list in-peer in
no auto-summary
```

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

### Vulnerability updates

#### Cisco IOS AAA RADIUS Long Username Authentication Bypass

```
aaa authentication login xxxxxx group radius
none
aaa authentication ppp xxxxxx group radius
none
aaa authentication login xxxxxx group radius
local none
aaa authentication ppp xxxxxx group radius
local none
```

<http://www.cisco.com/warp/public/707/cisco-sa-20050629-aaa.shtml>

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

## Vulnerability updates (cont.)

### Cisco Advisory: IPv6 Crafted Packet Vulnerability

```
Router#show ipv6 interface
Serial1/0 is up, line protocol is up
IPv6 is enabled, link-local address is FE80::A8BB:CCFF:FE00:D200
Global unicast address(es):
2001:1:33::3, subnet is 2001:1:33::/64
Joined group address(es):
FF02::1
FF02::1:FF00:3
FF02::1:FF00:D200
MTU is 1500 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds Router#
```

[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a00804d82c9.shtml#de tails](http://www.cisco.com/en/US/products/products_security_advisory09186a00804d82c9.shtml#de tails)

---

---

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

## Preparation is everything!

- Be prepared now or be sorry the #1 difference between networks that survive the crisis

---

---

---

---

---

---

---

---

---

---

APNIC Asia Pacific Network Information Centre

## Think inside and outside the box

---

---

---

---

---

---

---

---

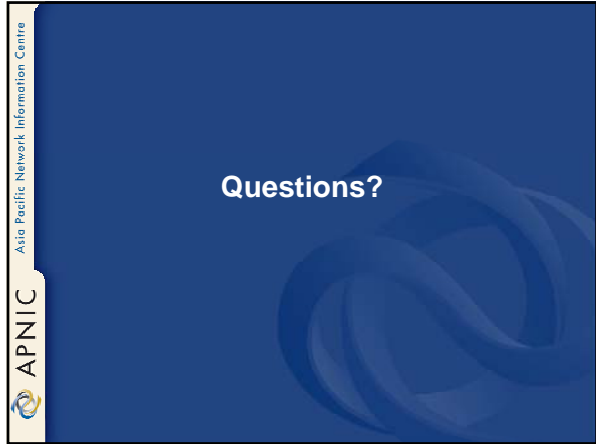
---

---



APNIC Asia Pacific Network Information Centre

Questions?

The slide features a dark blue background with a subtle, abstract graphic of overlapping, curved lines in a lighter shade of blue. The APNIC logo, consisting of a stylized globe icon and the acronym 'APNIC', is positioned in the top left corner. Below the logo, the full name 'Asia Pacific Network Information Centre' is written in a smaller font.

---

---

---

---

---

---

---

---