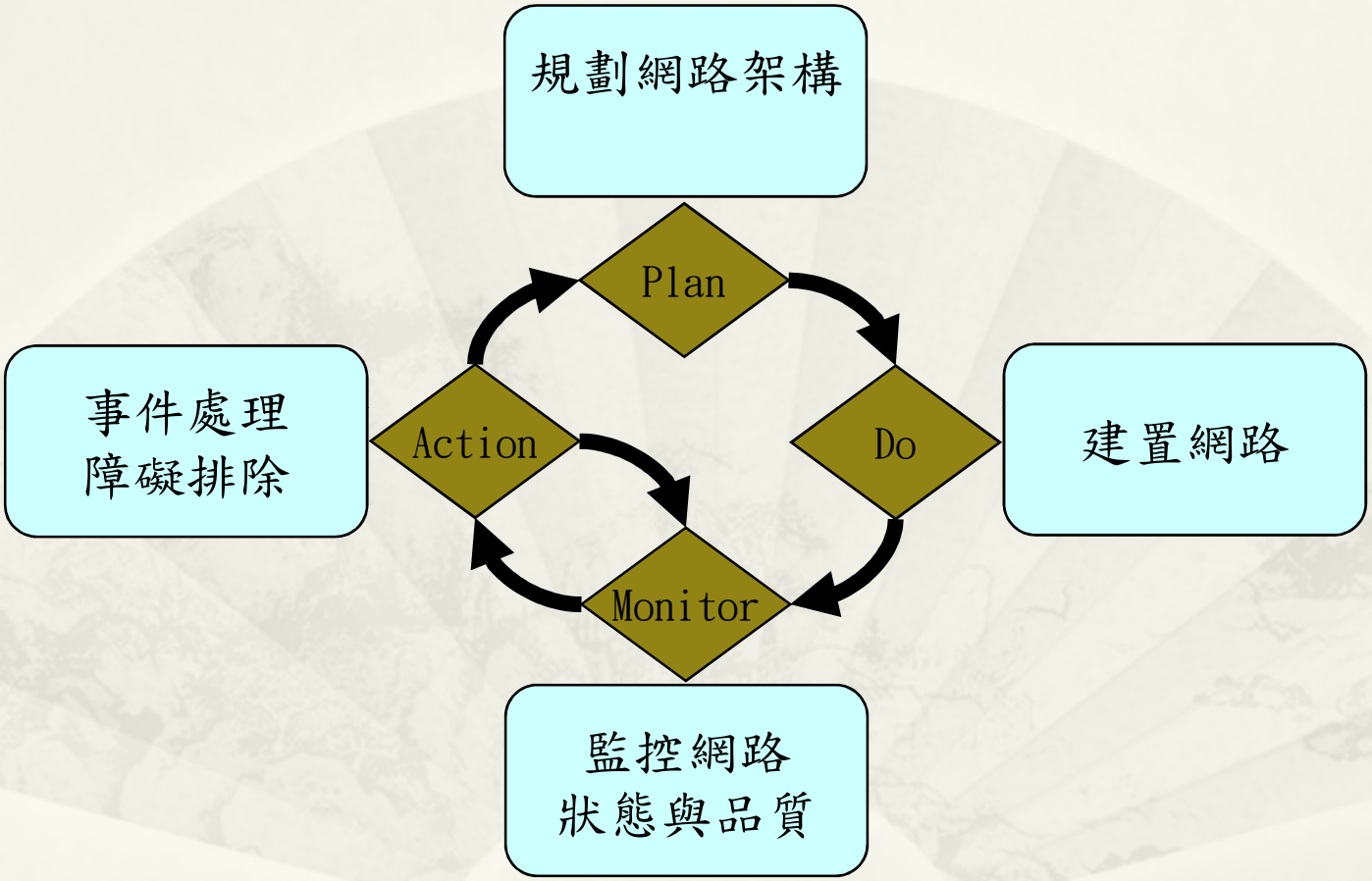
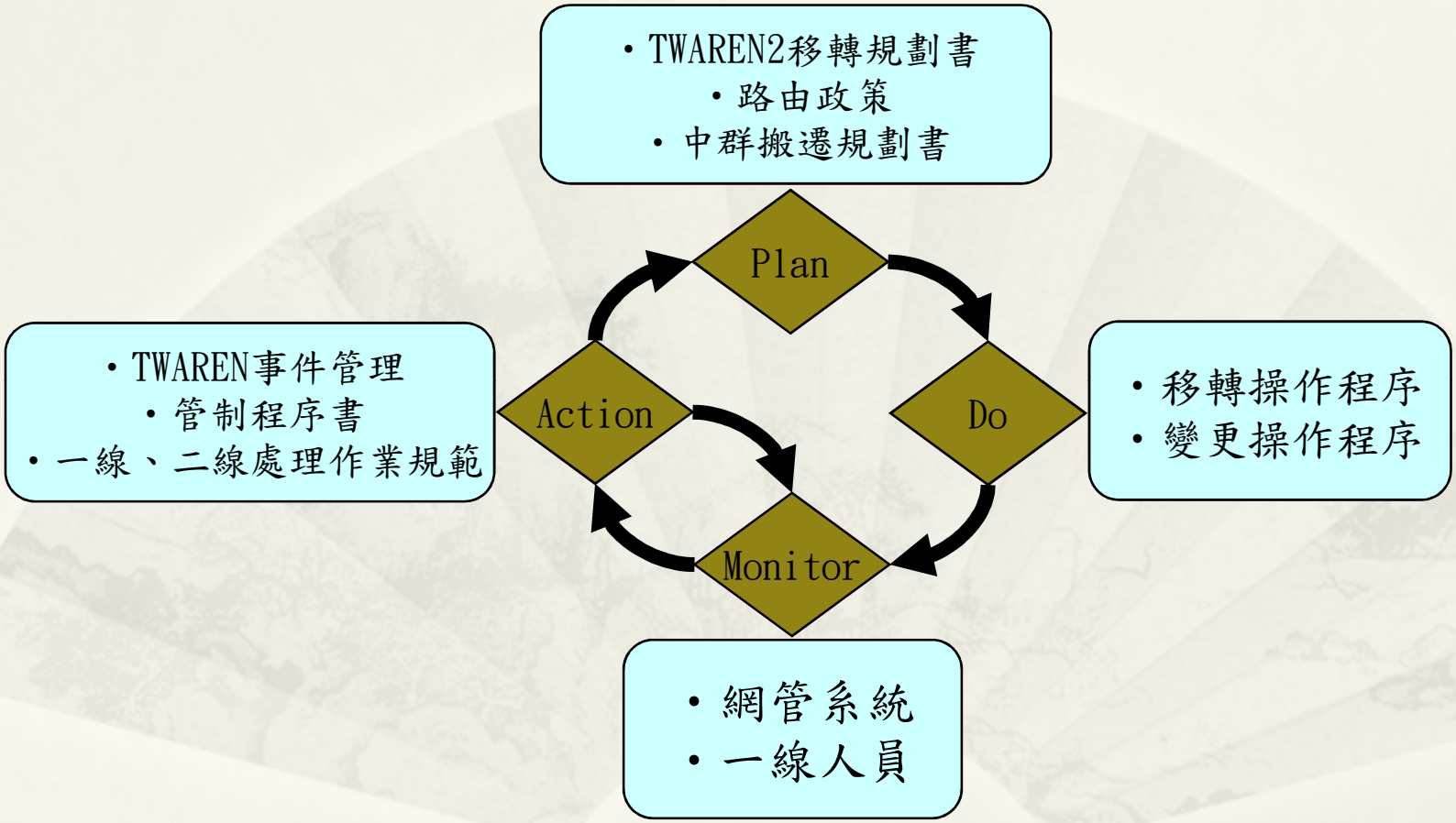
網路管理與監控
技術介紹

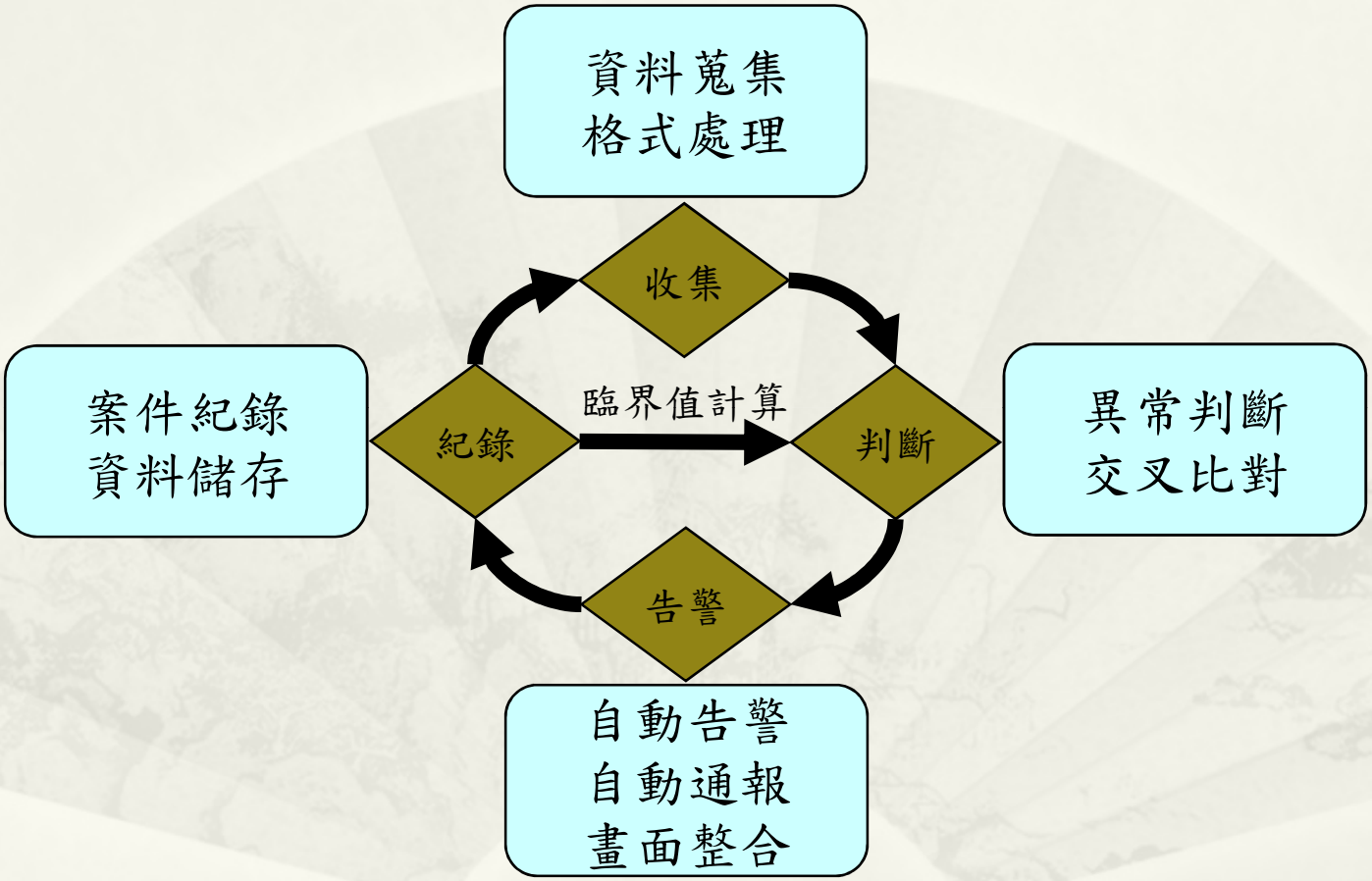
網路管理工作流程



網路管理工作流程


・TWAREN2移轉規劃書
・路由政策
・中群搬遷規劃書
Plan
Do
Monitor
Action
・TWAREN事件管理
・管制程序書
・一線、二線處理作業規範
・移轉操作程序
・變更操作程序
・網管系統
・一線人員

網路監控流程



監控項目舉例

- 設備故障發出的Trap
- 主動查詢的MIB
  - 機房環境
    - 環境溫度、設備電力
  - 國內外互連網
    - Peering 狀態、使用狀態
  - 品質
    - End to End RTT、Packet Lost Rate
  - 流量異常
    - 骨幹、特定介面
  - Top N 排行榜
    - Bytes、Flows、Packets
  - 設備狀態
    - CPU、Memory 、風扇
  - 路由監控
    - 連線單位路由、互連網重點路由

網管資料收集來源

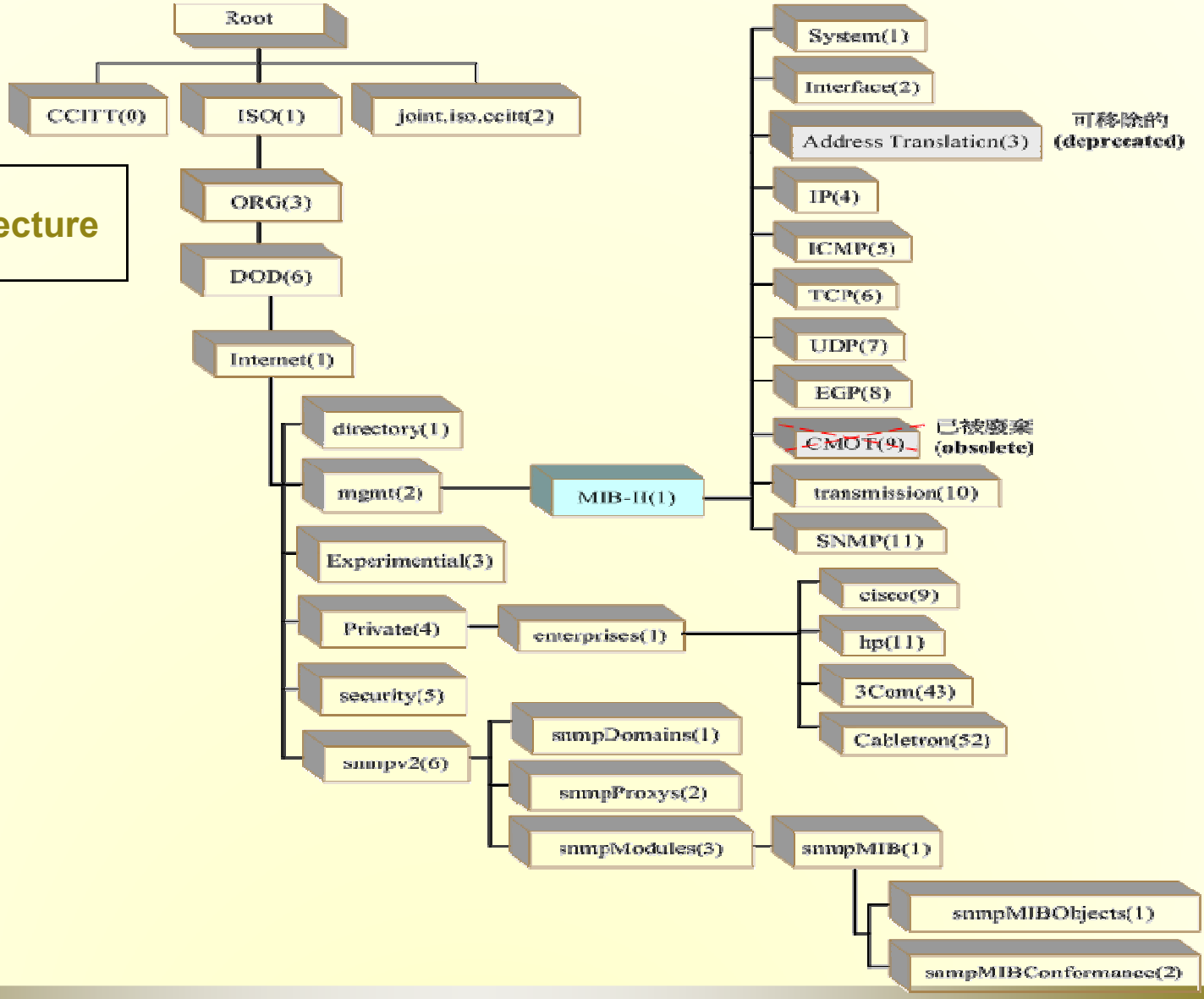
* Trap
* MIB (Management Information Base)
* System Log
* Flow data
* TL1 (Transaction Language 1)
* Packet/Frame mirror
* Simulate Telnet/SSH
* Internet Services Protocols

SNMP

* Simple Network Management Protocol
* 主要運作方式
  * Trap：乃是SNMP Agent在指定狀況發生時主動發送給NMS的SNMP訊息封包，採用UDP封包單向傳輸。
  * MIB：乃是NMS主動向SNMP Agent發出SNMP查詢封包，代理人收到後，回送SNMP回應封包給NMS，是一來一回的UDP封包傳輸過程，若經驗資料充足，可能預見障礙之發生，進行預防。
* OID (Object Identifier)
  * Global identifier for a particular object type.
  * Trap & MIB 封包內都會包含OID以描述訊息意義。
* 參考網頁
  * http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en
  * http://netdisco.cvs.sourceforge.net/viewvc/netdisco/mibs/

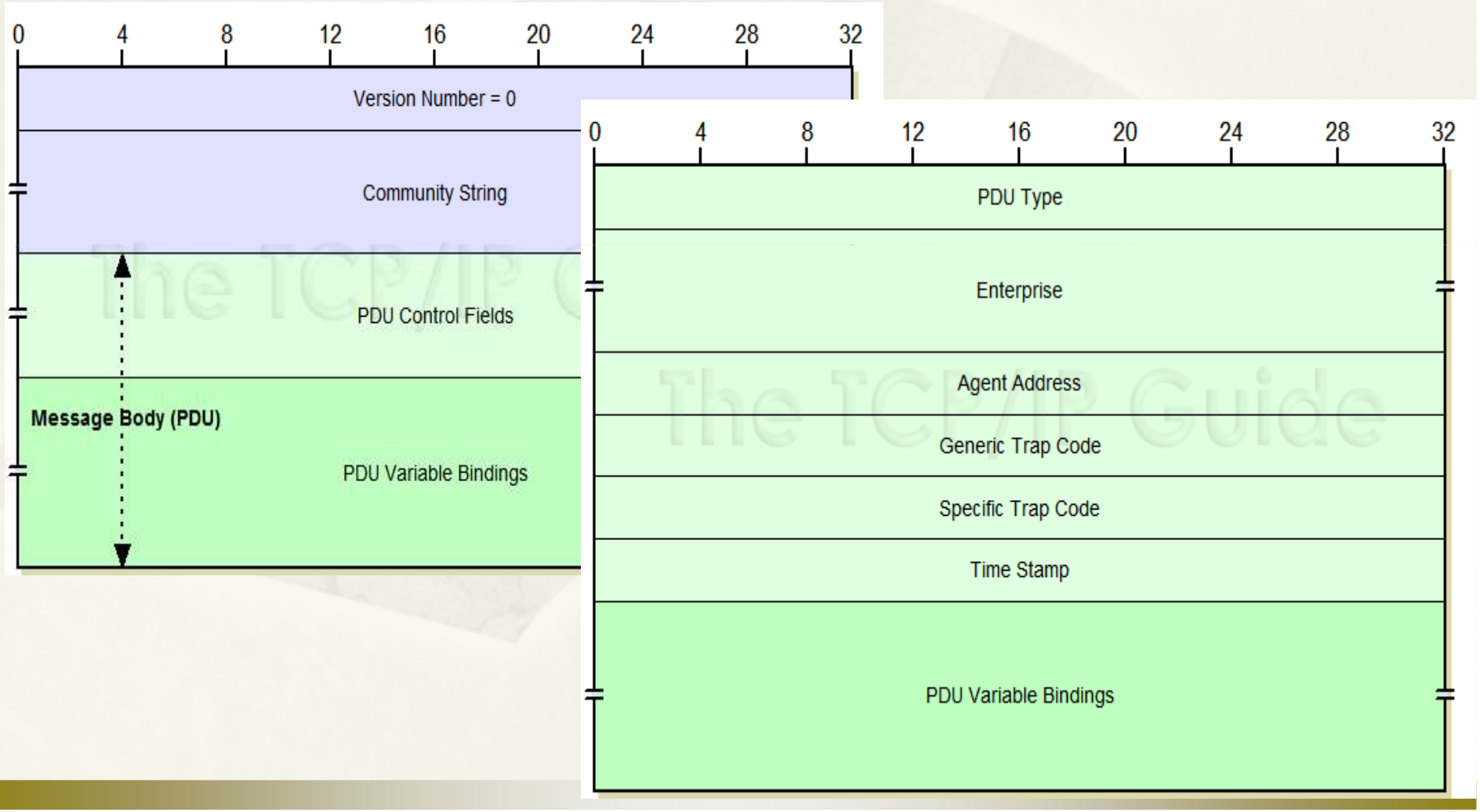
OID Tree

MIB-II Tree Architecture



SNMP Version 1 (SNMPv1) Trap Message Format

http://noc.twaren.net/~liangmc/nuk/nsm972/SNMP_Header.rar



Trap

* 參考網頁
  * http://www.mibdepot.com/engine/cisco_TRAP.html
* 舉例

Object	linkDown
OID	1.3.6.1.6.3.1.1.5.3
Status	current
MIB	IF-MIB ; - View Supporting Images
Trap Components	ifIndex ifAdminStatus ifOperStatus
Description	"A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus."

MIB

Object	ifIndex
OID	1.3.6.1.2.1.2.2.1.1
Type	InterfaceIndex
Permission	read-only
Status	current
MIB	IF-MIB ; - View Supporting Images
Description	"A unique value, greater than zero, for each interface. It is recommended that values are assigned contiguously starting from 1. The value for each interface sub-layer must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization."

MIB

Object	ifOperStatus
OID	1.3.6.1.2.1.2.2.1.8
Type	INTEGER
Permission	read-only
Status	current
Values	1 : up 2 : down 3 : testing 4 : unknown 5 : dormant 6 : notPresent 7 : lowerLayerDown
MIB	IF-MIB ; - View Supporting Images
Description	"The current operational state of the interface. The testing(3) state indicates that no operational packets can be passed. If ifAdminStatus is down(2) then ifOperStatus should be down(2). If ifAdminStatus is changed to up(1) then ifOperStatus should change to up(1) if the interface is ready to transmit and receive network traffic; it should change to dormant(5) if the interface is waiting for external actions (such as a serial line waiting for an incoming connection); it should remain in the down(2) state if and only if there is a fault that prevents it from going to the up(1) state; it should remain in the notPresent(6) state if the interface has missing (typically, hardware) components."

SNMP MIB Example

- snmpwalk -v2c -c 'public' 192.168.3.12 .1.3.6.1.2.1.1.5
  - SNMPv2-MIB::sysName.0 = STRING: TN-7609P.twaren.net
- snmpwalk -v2c -c 'public' 192.168.3.12 .1.3.6.1.2.1.31.1.1.1.1
  - IF-MIB::ifName.1 = STRING: Gi1/1
  - IF-MIB::ifName.2 = STRING: Gi1/2
- snmpwalk -v2c -c 'public' 192.168.3.12 .1.3.6.1.2.1.2.2.1.7
  - IF-MIB::ifAdminStatus.1 = INTEGER: down(2)
  - IF-MIB::ifAdminStatus.2 = INTEGER: down(2)
- snmpwalk -v2c -c 'public' 192.168.3.12 .1.3.6.1.2.1.2.2.1.8
  - IF-MIB::ifOperStatus.1 = INTEGER: down(2)
  - IF-MIB::ifOperStatus.2 = INTEGER: down(2)
- snmpwalk -v2c -c 'public' 192.168.3.12 .1.3.6.1.2.1.31.1.1.1.18
  - IF-MIB::ifAlias.25 = STRING: 7609 <--> TN-12416P 10GbE 3/1
  - IF-MIB::ifAlias.28 = STRING: "to-TN-7609C-Ten2/2-Trunk"

System Log

- 由系統在指定狀況發生時主動發送給內部 Log Daemon 或外部的 Log Collector 機器以資記錄。
- 外部傳送大部分採用UDP傳輸，採用TCP傳輸的Daemon甚少。
- Unix
  - Jun 22 23:00:01 noc cron[16182]: (root) CMD (test -x /usr/sbin/run-crons && /usr/sbin/run-crons)
  - Jun 22 23:02:36 noc sshd[16966]: refused connect from 59-127-207-117.HINET-IP.hinet.net (::ffff:59.127.207.117)
  - Jun 22 23:02:49 noc sshd[17045]: Invalid user lmj from 140.110.96.20
  - Jun 22 23:02:55 noc sshd(pam_unix)[17048]: check pass; user unknown
  - Jun 22 23:02:55 noc sshd(pam_unix)[17048]: authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=140.110.96.20
  - Jun 22 23:02:56 noc sshd[17045]: error: PAM: Authentication failure for illegal user lmj from 140.110.96.20

System Log

* Cisco Router
  * Jun 15 18:42:02: %PFINIT-SP-5-CONFIG_SYNC: Sync'ing the startup configuration to the standby Router
  * Jun 15 18:42:02: %PFINIT-SP-1-CONFIG_SYNC_FAIL: Sync'ing the startup configuration to the standby Router FAILED, the file may be already locked by a command like: show config.
  * Jun 16 21:57:24: %OSPF-5-ADJCHG: Process 7539, Nbr 211.79.60.130 on Vlan20 from 2WAY to DOWN, Neighbor Down: Dead timer expired
  * Jun 16 21:57:24: %OSPFv3-5-ADJCHG: Process 7539, Nbr 211.79.60.130 on Vlan20 from 2WAY to DOWN, Neighbor Down: Dead timer expired
  * Jun 16 21:57:32: %PIM-5-NBRCHG: neighbor 211.79.60.116 DOWN on interface Vlan20 (vrf default) non DR
  * Jun 16 21:58:50: %PIM-5-NBRCHG: neighbor 211.79.60.116 UP on interface Vlan20 (vrf default)
  * Jun 22 15:23:02: %SYS-5-CONFIG_I: Configured from console by tjs onvty0 (192.168.3.98)
  * Jun 22 15:23:46: %SYS-5-CONFIG_I: Configured from console by tjs onvty0 (192.168.3.98)
  * Jun 22 15:23:59: %PFINIT-SP-5-CONFIG_SYNC: Sync'ing the startup configuration to the standby Router

Netflow

- 由設備主動發送符合指定條件的Flow Data給收集器，含有Layer3~4的資訊。
- Version 5 packet header

Bytes	Contents	Description
0-1	version	NetFlow export format version number (1,5,6,7,8,9)
2-3	count	Number of flows exported in this packet (1-30)
4-7	sys_uptime	Current time in milliseconds since the export device booted
8-11	unix_secs	Current count of seconds since 0000 UTC 1970
12-15	unix_nsecs	Residual nanoseconds since 0000 UTC 1970
16-19	flow_sequence	Sequence counter of total flows seen
20	engine_type	Type of flow-switching engine
21	engine_id	Slot number of the flow-switching engine
22-23	sampling_interval	First two bits hold the sampling mode; remaining 14 bits hold value of sampling interval

Netflow

* Version 5 packet record format

Bytes	Contents	Description
0-3	srcaddr	Source IP address
4-7	dstaddr	Destination IP address
8-11	nexthop	IP address of next hop router
12-13	input	SNMP index of input interface
14-15	output	SNMP index of output interface
16-19	dPkts	Packets in the flow
20-23	dOctets	Total number of Layer 3 bytes in the packets of the flow
24-27	first	SysUptime at start of flow
28-31	last	SysUptime at the time the last packet of the flow was received
32-33	srcport	TCP/UDP source port number or equivalent
34-35	dstport	TCP/UDP destination port number or equivalent
36	pad1	Unused (zero) bytes
37	tcp_flags	Cumulative OR of TCP flags
38	prot	IP protocol type (for example, TCP = 6; UDP = 17)
39	tos	IP type of service (ToS)
40-41	src_as	Autonomous system number of the source, either origin or peer
42-43	dst_as	Autonomous system number of the destination, either origin or peer
44	src_mask	Source address prefix mask bits
45	dst_mask	Destination address prefix mask bits
46-47	pad2	Unused (zero) bytes

TL1

- TL1 messages follow a fixed structure, and all commands must conform to it. However, the commands themselves are extensible and new commands can be added by NE vendors.
- Target identifier (TID) & Source identifier (SID)
  - TID/SID is a unique name assigned to each NE. TID is used to route the message to an NE, SID is used to identify the source of an autonomous message.
- Access identifier (AID)
  - AID identifies an entity within an NE.
- Correlation tag (CTAG) & Autonomous correlation tag (ATAG)
  - CTAG/ATAG are numbers used to correlate messages.

TL1

* TL1 input message
* Example:
* ACT-USER-SECU:MyNE:sridev:101::password;
* Structure:

TL1 input message							
Command code			Staging block				Payload block
Verb	modifier1	modifier2	TID	AID	CTAG	General block	Data block
ACT	*USER*	*SECU*	*MyNE*	*sridev*	*101*		*password*

TL1

* TL1 output message
* Example:
* MyNE 04-08-14 09:12:04M 101 COMPLD"UID=sridev:CID=CRAFT,UAP=1:";
* Structure

TL1 output message							
Response Header			Response Id			Response block	Terminators
SID	Date	Time	M	CTAG	Completion code		
MyNE	*04-08-14*	*09:12:04*	*M*	*101*	*COMPLD*	*"UID=sridev:CID=CRAFT,UAP=1:"*	*;*

TL1

- 指令範例
  - ACT-USER::training:123::*****;
  - RTRV-EQPT::SLOT-ALL:123;
  - RTRV-CRS::ALL:123;
  - ENT-CRS-VC4::FAC-4-1,VC4-12-1-1:123::2way;
  - RTRV-CRS::ALL:123;
  - DLT-CRS-VC4::FAC-4-1,VC4-12-1-1:123;
  - CANC-USER::training:123;

TL1

```
*    > RTRV-CRS::ALL:123;

*       TN-15600 2007-10-12 10:27:49 M  123 COMPLD
*       "VC4-11-1-5,VC4-11-3-9:2WAY,VC44C:CKTID=\"NCTUP-NCTU-NCKU-VC4-4c\":unlocked-enabled,"
*       "VC4-11-1-9,VC4-4-3-17:2WAY,VC44C:CKTID=\"NCTUP-NCTU-NSYSU-VC4-4c\":unlocked-enabled,"
*       "VC4-11-1-17,VC4-2-2-1:2WAY,VC416C:CKTID=\"OORC-HCC-TNC-VC4-16c\":unlocked-enabled,"
*       "VC4-4-2-25,VC4-11-1-33:2WAY,VC48C:CKTID=\"TNintra-HCintra-VC4-8c\":unlocked-enabled,"
*       "VC4-4-4-17,VC4-2-1-1:2WAY,VC416C:CKTID=\"OORC-TCC-TNC-VC4-16c\":unlocked-enabled,"
*       "VC4-4-4-64,VC4-11-4-64:2WAY,VC4:CKTID=\"PEER-NDHU-CCU-VC4-4c\":unlocked-enabled,"
*       "VC4-4-4-63,VC4-4-3-64:2WAY,VC4:CKTID=\"PEER-NDHU-NSYSU-VC4-4c\":unlocked-enabled,"
*       "VC4-11-1-64,VC4-11-3-64:2WAY,VC4:CKTID=\"NHRI-NTHU-NCKU-VC4\":unlocked-enabled,"
*       "VC4-11-3-63,VC4-11-4-62:2WAY,VC4:CKTID=\"NCKUH-NCKU-CCU-VC4\":unlocked-enabled,"
*       "VC4-11-1-62,VC4-11-4-63:2WAY,VC4:CKTID=\"NTUH-NTU-CCU-VC4\":unlocked-enabled,"
*       "VC4-4-3-1,VC4-11-1-1:2WAY,VC44C:CKTID=\"PEER-NSYSU-ASCC-VC4-4c\":unlocked-enabled,"
*       "VC4-11-3-62,VC4-4-2-64:2WAY,VC4:CKTID=\"Select-NCKU-TN-VC4\":unlocked-enabled,"
*       "VC4-11-1-63,VC4-4-2-63:2WAY,VC4:CKTID=\"SIPA-HC-TN-VC4\":unlocked-enabled,"
*       "VC4-11-3-61,VC4-4-2-62:2WAY,VC4:CKTID=\"TN-NDL-CIC-NCKU-TN-VC4\":unlocked-enabled,"
*    ;
*    >
```

Packet/Frame Mirror

- Mirror data 有觸犯隱私權的法律問題
- Flow data 主要提供L3~L4表頭資訊，但Packet mirror能提供L2~L7多方面資訊
- Mirror data 資訊處理所需之計算能力遠高於flow data，投注一般成本僅能針對特定對象範圍使用

Simulate Telnet/SSH

- 網管程式以模擬 telnet 或 ssh client 的方式連上設備或主機，下達事先規劃的指令，並分析回應的內容，以獲取所需資訊。
- Perl/PHP/C/Java/C# 在網路上都有免費可用的 Telnet/SSH Lib 可以下載。

Internet Services Protocols

- 以程式模擬 client 連線，進行簡單對談，以確認服務正常。
- 了解Internet Services Protocols
  - /etc/services （Unix）
  - C:\WINDOWS\system32\drivers\etc （MsWindows）
  - Protocols 可參考RFC
  - 何謂RFC？
    - http://zh.wikipedia.org/w/index.php?title=RFC&variant=zh-hant
    - http://www.rfc-editor.org/
    - http://www.ietf.org/rfc.html