Cyber Solutions

# Network Management: Status and Directions

*Security and Policy*

*Glenn Mansfield*

株式会社 サイバー・ソリューションズ
*Cyber Solutions Inc.*

Cyber Solutions

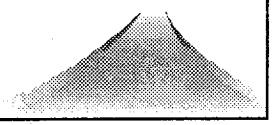
## The Internet

- ▲Open and Everywhere
- ▲Universal Solution ?
  - • Communication
  - • Information access and distribution

Cyber Solutions

## Architecture

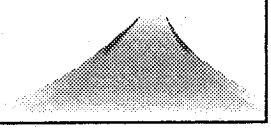
- ▲ (Grand) Plan ? *None*
- ▲ Evolution *Natural Selection* ?
- ▲ The principle *Constant change*



Cyber Solutions

## Architectural Principles

- ▲ The Goal *Connectivity*
- ▲ The Tool *Internet Protocol*
- ▲ The Intelligence *End to End*

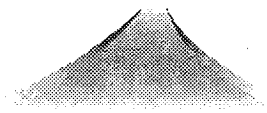


Cyber Solutions

# Motto

Rough Consensus & Running Code

*And it is working well*



Cyber Solutions

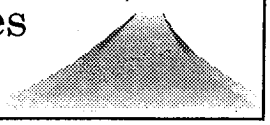
# The Status

Many users / Many applications

Many *ab*users / Many requirements

Best effort: Managed services
Guaranteed services

Open : Secure services

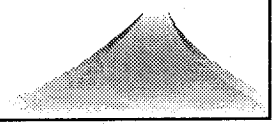


*Cyber Solutions*

## Users want Security

Communications Security:

- Privacy/Confidentiality
- Message Integrity
- Endpoint Authentication



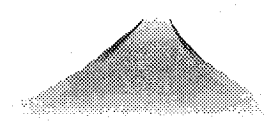
*Cyber Solutions*

## Users want Security

Authorized/Appropriate usage

- Protection against intrusions
- Defence against abuse:
  - being used as a launchpad

Defences against DoS



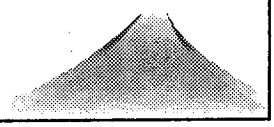
Cyber Solutions

## Users want Security

Transaction Security:

Authentication

Non repudiation



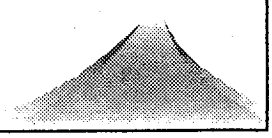
Cyber Solutions

## Users want Security

Track down intruders

Try and Punish

Judiciary Proof is necessary



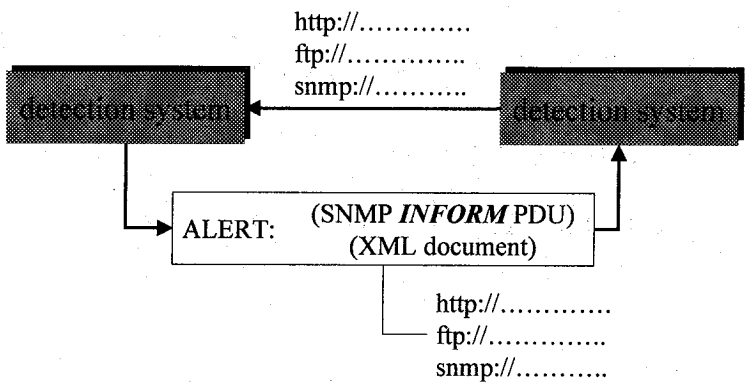
Cyber Solutions

## Security Issues

- ▲ **User Authentication**
  - username/passwd
  - Challenge Response/ OneTimePassword
  - Certificates
  - Host authentication
    ID should be hostname or address
- ▲ **Authorization**
  - Access control mechanism
- ▲ **Authenticating Certificates**
- ▲ **Traffic Security**
  - IPSEC - interhost comm
  - SSL/TLS
- ▲ **Object Security**

Cyber Solutions

## Distributed-ID Model



Cyber Solutions

# IDS *vs* SNMP

## *Nikkei Internet Technology August 2000*

| Product name | NetRecon | CISCO Secure IDS | RealSecure Network Sensor | Flight | Session Watch |
|---|---|---|---|---|---|
| Vendor | AXENT Technologies | CISCO Systems | Internet Security Systems | Network Flight Recorder | Computer Associates |
| URL | http://www.axent.com/ | http://www.cisco.com | http://www.iss.net/ | http://www.nfr.com/ | http://www.cai.com/ |
| Type | NIDS | NIDS | NIDS | NIDS | NIDS |
| Number of signature | 200 | 200 | 217 | 800 | 193 |
| Alert action | Popup Window<br>E-mail<br>Pager<br>FAX<br>*SNMP trap* | Popup Window<br>E-mail<br>*SNMP trap*<br>Arbitrary program | Popup Window<br>E-mail<br>Pager<br>*SNMP trap*<br>Arbitrary program | Popup Window<br>E-mail<br>Pager<br>FAX | Popup Window<br>E-mail<br>Pager<br>*SNMP trap*<br>Arbitrary program |
| Correlate to firewall | Firewall-1<br>Raptor Firewall | CISCO router | Firewall-1 | Firewall-1 | Firewall-1 |
| Platform | Windows NT4.0 | Solaris, HP-UX | Windows NT,Solaris | OpenBSD, Solaris(manager) | Windows NT4.0 |

| Intrusion Alert | RealSecure OS Sensor | Kane Security Enterprise | CyberCop Monitor | IS Eye |
|---|---|---|---|---|
| AXENT technologies | Internet Security Systems | Intrusion.com Inc. | Network Associates | Network ICE |
| http://www.axent.com/ | http://www.iss.net/ | http://www.intrusion.com/ | http://www.nai.com/ | http://www.networkice.com/ |
| HIDS | HIDS | HIDS | NIDS/HIDS | NIDS/HIDS |
| 50 | 50 | 5300 | 169 | 400 |
| Popup Window<br>E-mail<br>Pager<br>*SNMP trap*<br>Arbitrary program | Popup Window<br>E-mail<br>Pager<br>*SNMP trap*<br>Arbitrary program | Popup Window<br>E-mail<br>Pager<br>FAX | Popup Window<br>E-mail<br>*SNMP trap* | Popup Window<br>E-mail<br>*SNMP trap* |
| by user program | Firewall-1 | Firewall-1 | Gauntlet Firewall | |
| Windows NT, Netware, AIX, HP-UX, Sun S, Solaris, OSF/1, Digital UNIX, IRIX | Windows NT, NetWare, UNIX | Windows NT4.0 | Windows NT4.0 | Windows95/98/NT4.0/2000 |

Cyber Solutions

# Is There a Policy ?

Policy ?

What policy ?

What is policy ?

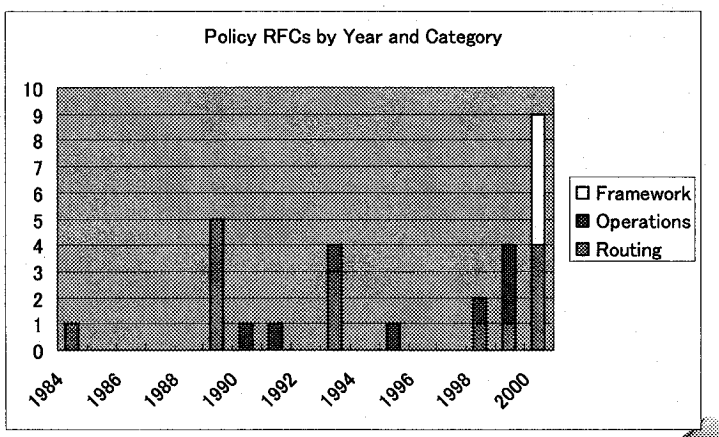
Cyber Solutions

# What Policy ?

Operations Policy
Management Policy
Security Policy
Privacy Policy
Language Policy
Business Policy

Cyber Solutions

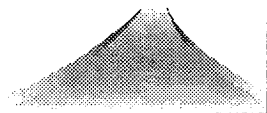
# Policy Activity in the Internet



Cyber Solutions

## Policy

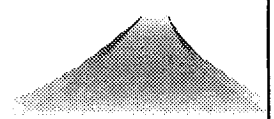
- ▲ Routing Policy
  - Routing Policy
- ▲ QoS Policy
  - Services offered
- ▲ Security Policy
  - wrt to originating traffic
  - wrt transit traffic
  - wrt security incidents



Cyber Solutions

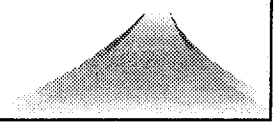
## Policy Issues

- ▲ How to define policies
  - The Model (abstraction)
  - The representation
- ▲ The framework
  - Acess protocols
  - Repositories
- ▲ The deployment
  - Understanding policies
  - Analyzing policies
    - visualization
  - Core policy set



## Cyber Solutions Routing Policy: Status

- ▲ **Routing policy specification language**
  - ***(un)*Reasonably complicated**
  - **is deployed Internet Routing Registry (IRR)**
    - **IRRd is up and running**
- ▲ **Incomplete/Inaccurate information**

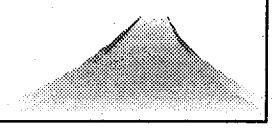


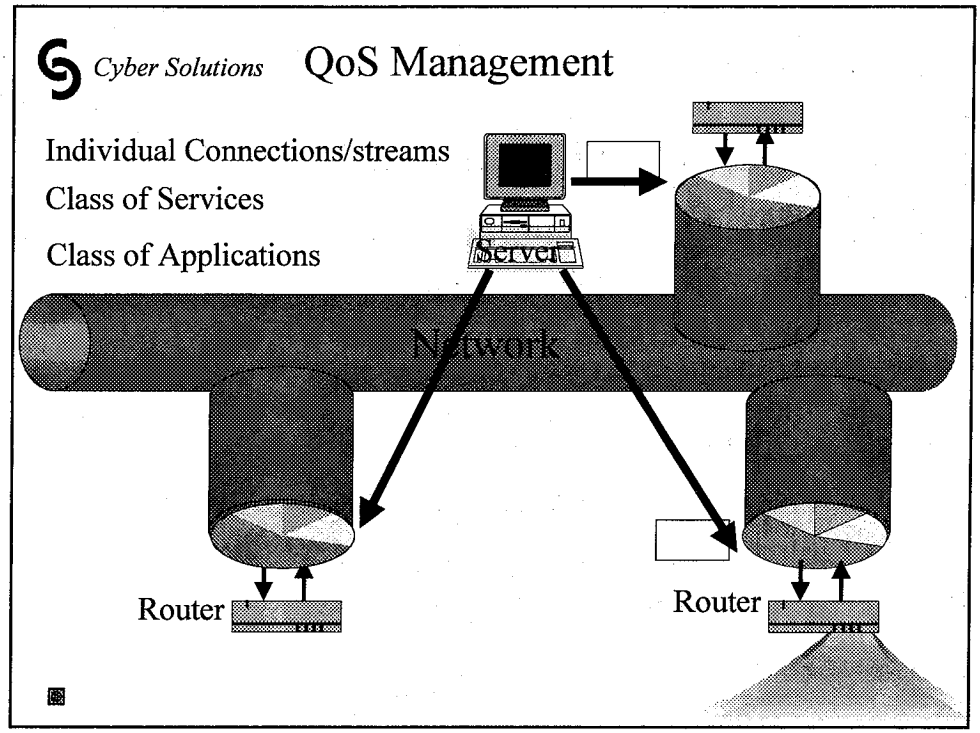
## Cyber Solutions

# Users want QoS

Superior service

Predictable service






Cyber Solutions

# QoS: The issues

Service Environment :

- inaccurate and/or non-scaling
  - DiffServ is inaccurate
  - IntServ does not scale

QoS Discovery:

- Not possible
- Cannot find QoS path(s)
- Cannot choose from path(s)

Cyber Solutions

# QoS: The issues

QoS Routing and Resource Mgmt:

presently best-effort path

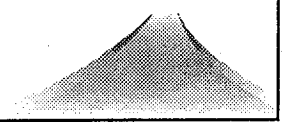
path selection is necessary within QoS Arch.

TCP and QoS:

Assymetric service may create problems

Symmetric service has problems too

Interaction of routing and TCP



Cyber Solutions

# QoS: The issues

Per-flow states and Per Packet Classifiers:

conflict with IPSEC, NAT,

IP-Tunnels, IP-fragments.

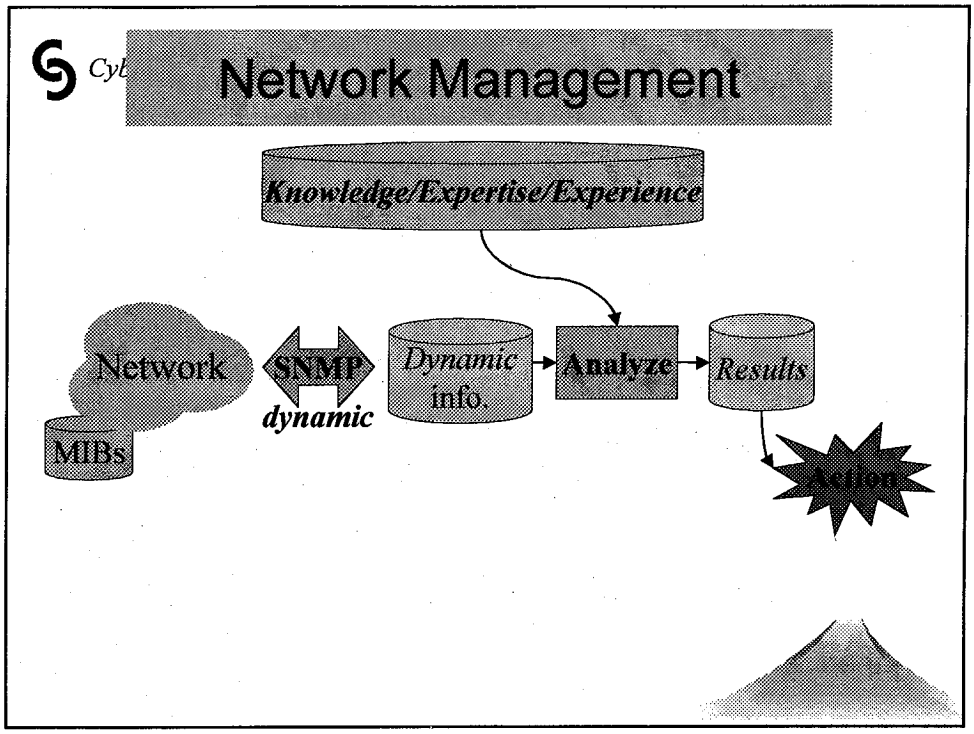
The Service Set:

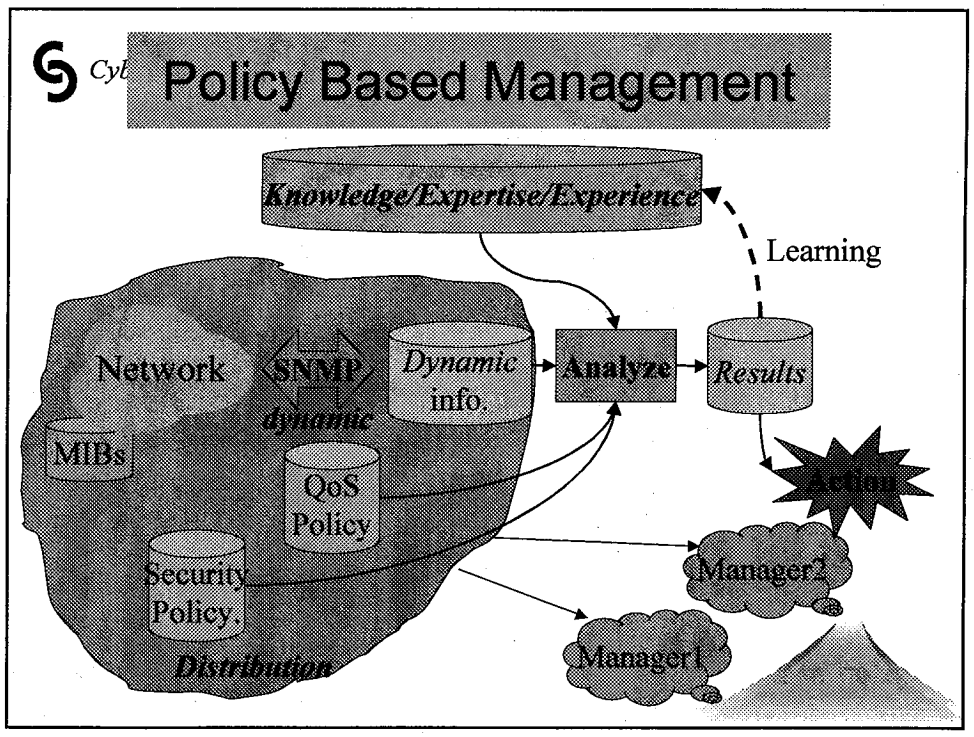
need a small core set of service profiles

New Network Management requirements:

resource availability along a particular path

map to admission control function


Cyb
Network Management
Knowledge/Expertise/Experience
Network
MIBs
SNMP
dynamic
Dynamic
info.
Analyze
Results
Action


Cyb
Policy Based Management
Knowledge/Expertise/Experience
Learning
Network
MIBs
SNMP
dynamic
Dynamic
info.
Analyze
Results
Action
QoS
Policy
Security
Policy
Distribution
Manager2
Manager1