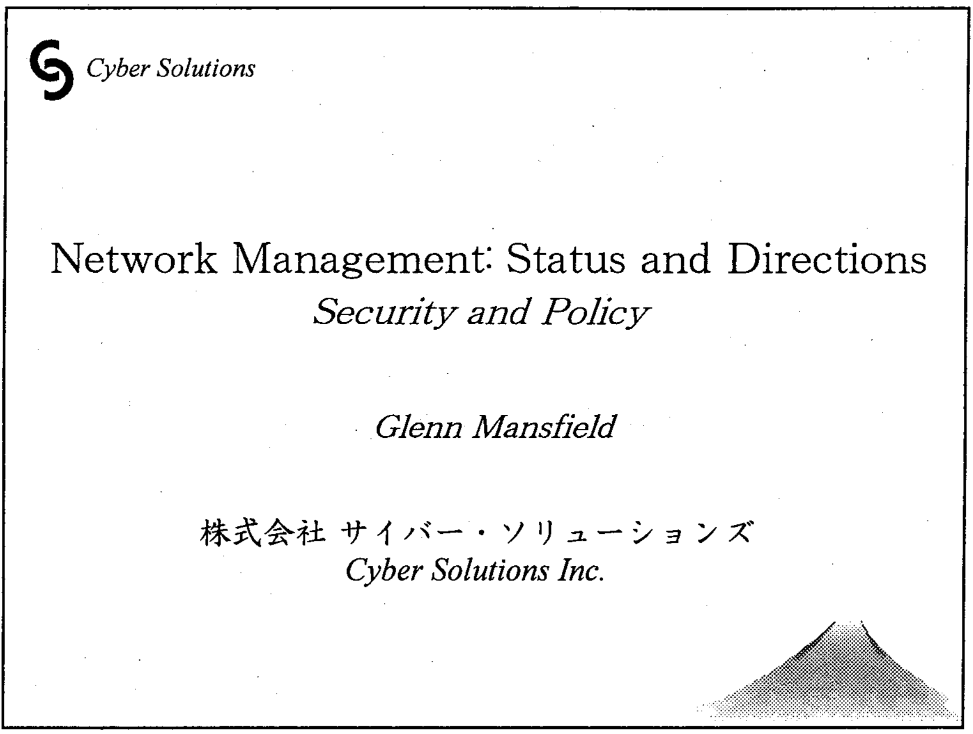


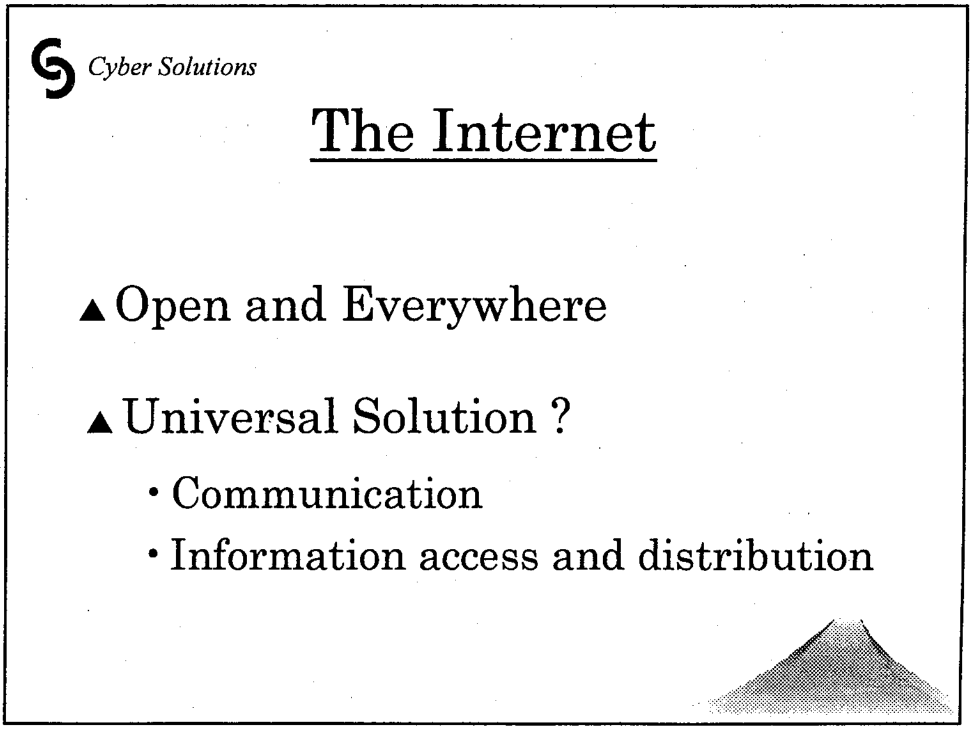
Cyber Solutions

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.



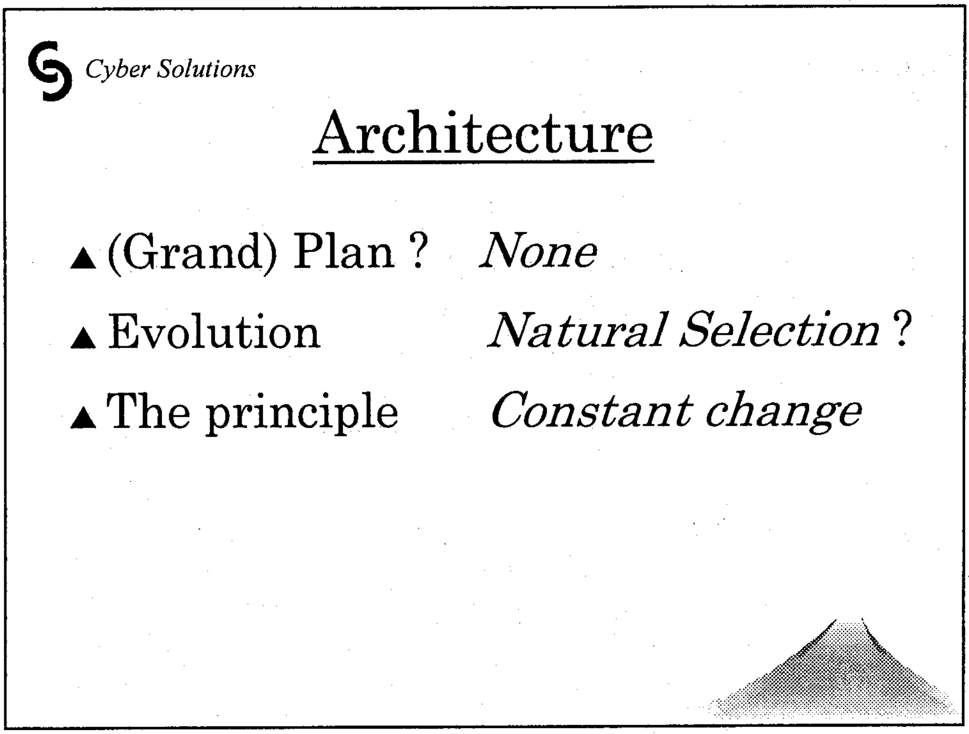
Cyber Solutions

The Internet

▲ Open and Everywhere

▲ Universal Solution ?

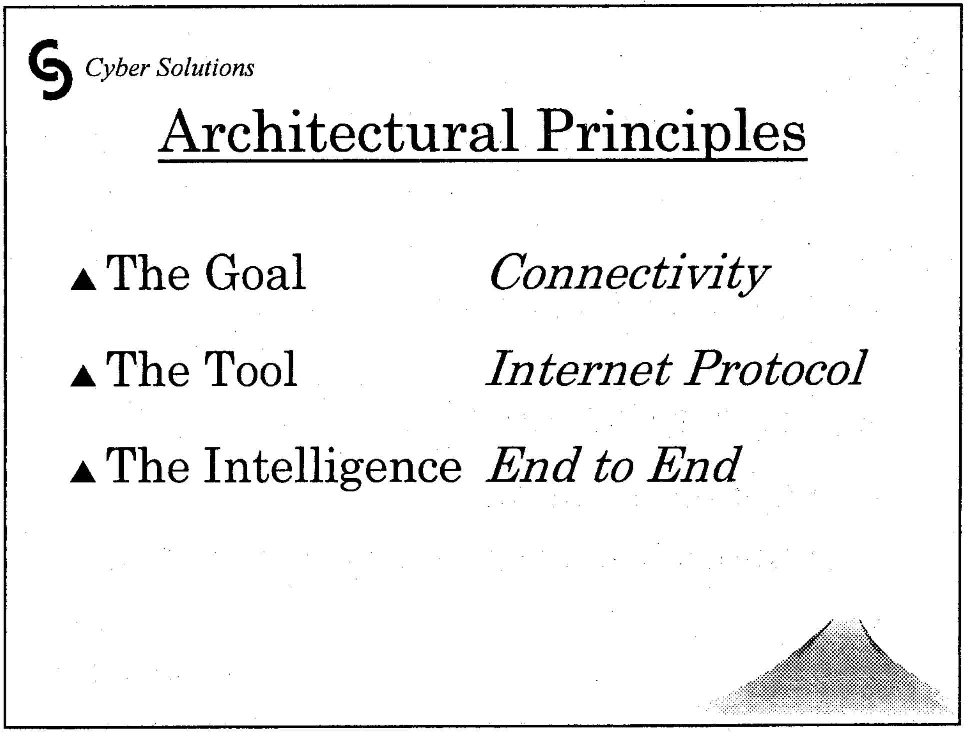
- Communication
- Information access and distribution



Cyber Solutions

Architecture

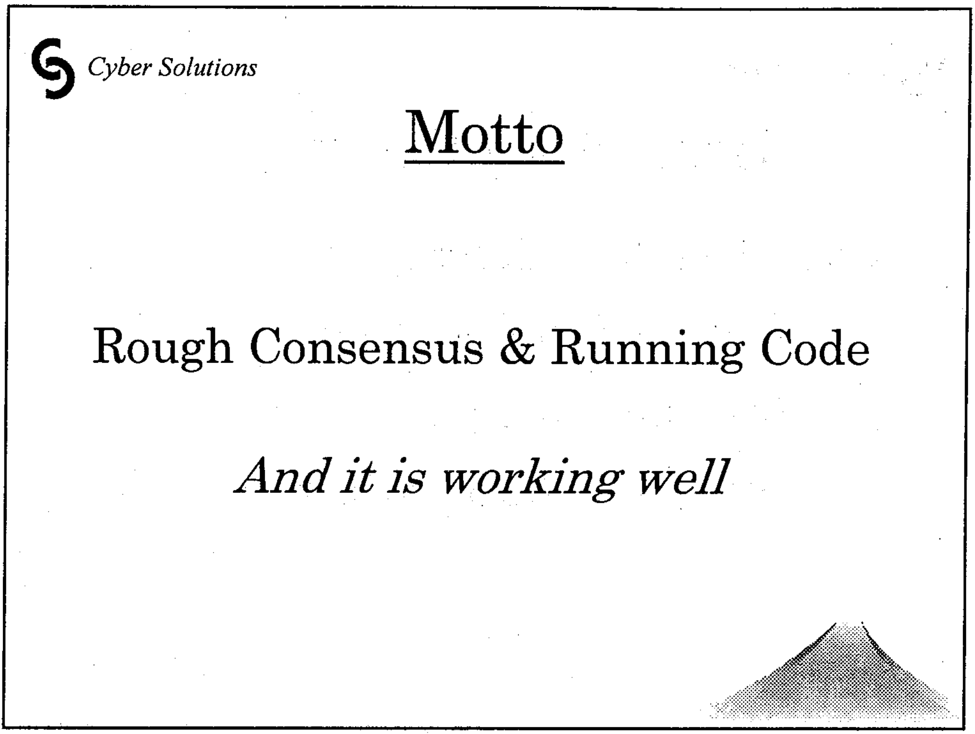
- ▲ (Grand) Plan ? *None*
- ▲ Evolution *Natural Selection* ?
- ▲ The principle *Constant change*



Cyber Solutions

Architectural Principles

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

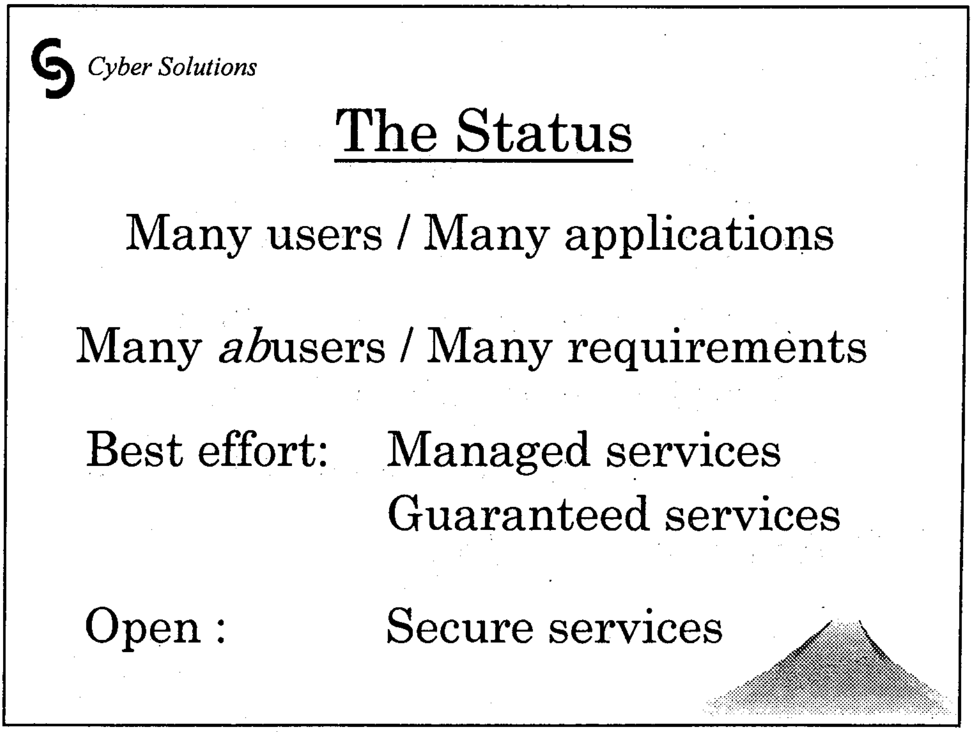


Cyber Solutions

Motto

Rough Consensus & Running Code

And it is working well



Cyber Solutions

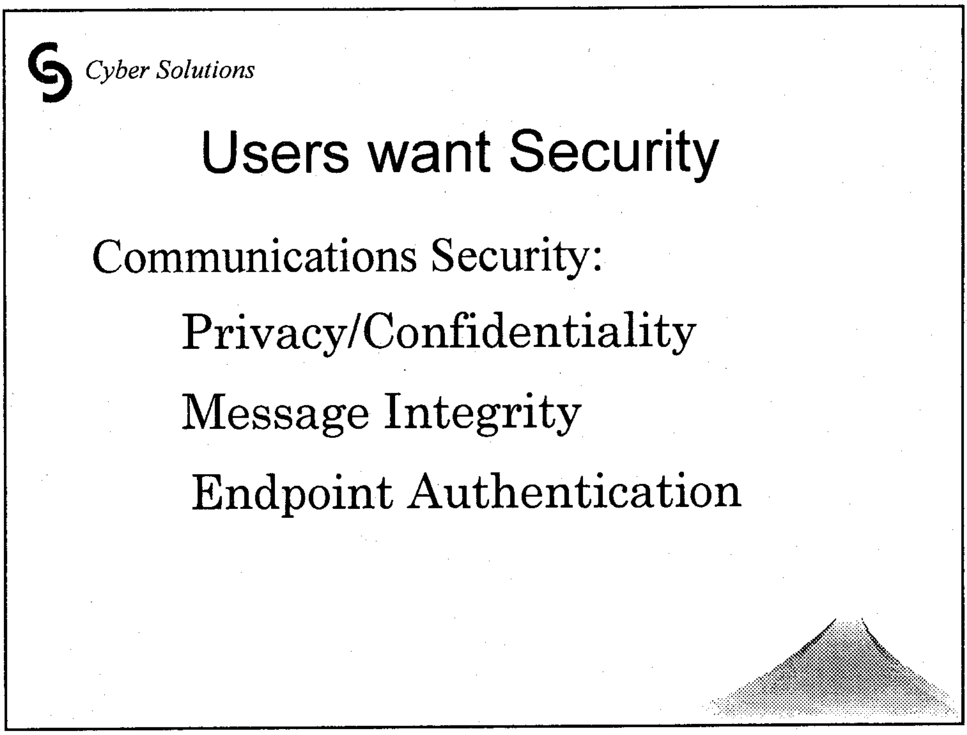
The Status

Many users / Many applications

Many *ab*users / Many requirements

Best effort: Managed services
Guaranteed services

Open : Secure services

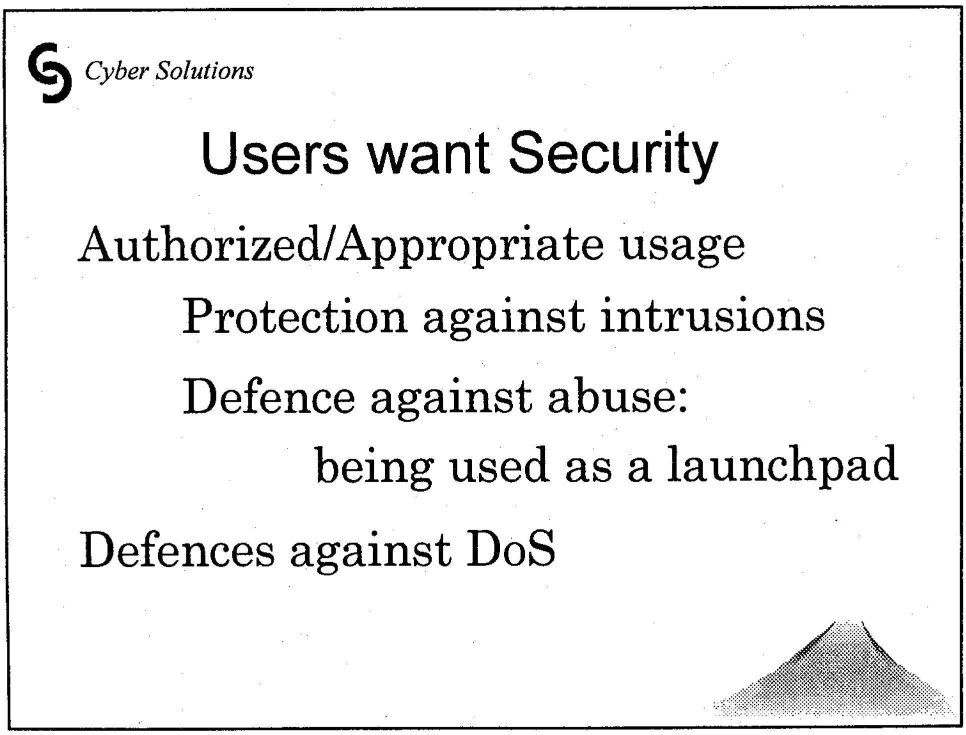


Cyber Solutions

Users want Security

Communications Security:

- Privacy/Confidentiality
- Message Integrity
- Endpoint Authentication



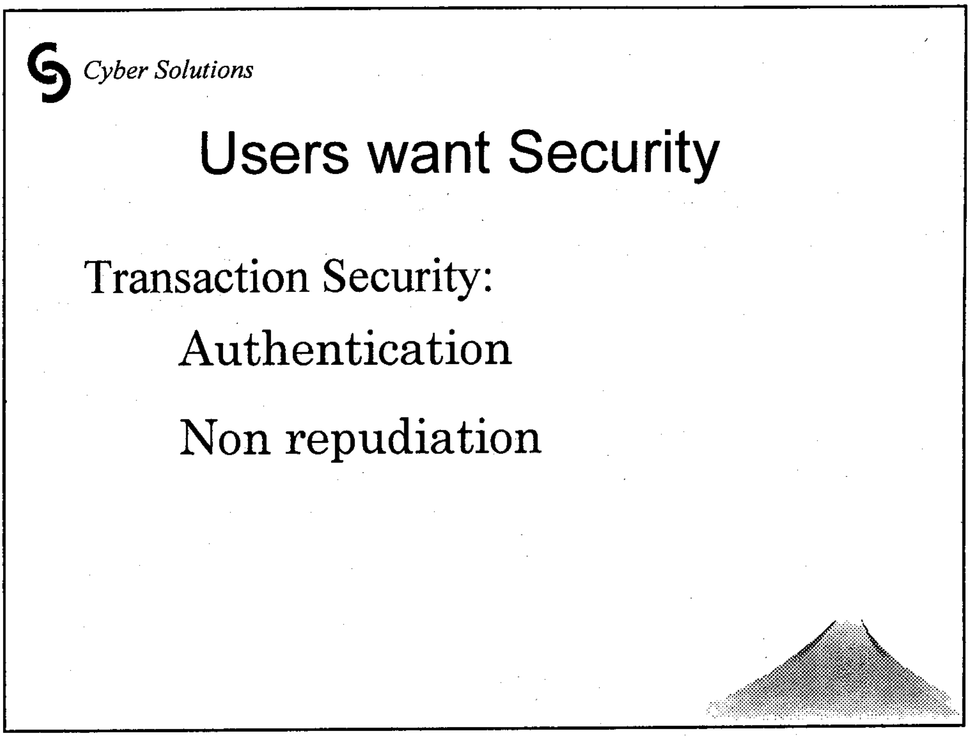
Cyber Solutions

Users want Security

Authorized/Appropriate usage

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

Defences against DoS

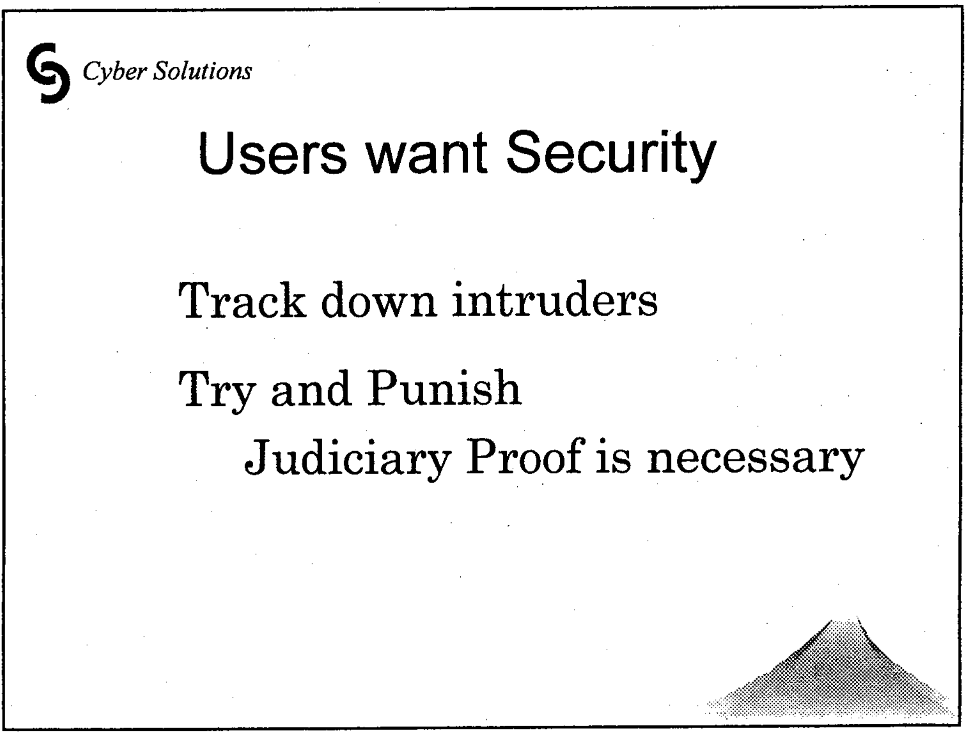


Cyber Solutions

Users want Security

Transaction Security:

- Authentication
- Non repudiation



Cyber Solutions

Users want Security

- Track down intruders
- Try and Punish
  - Judiciary Proof is necessary

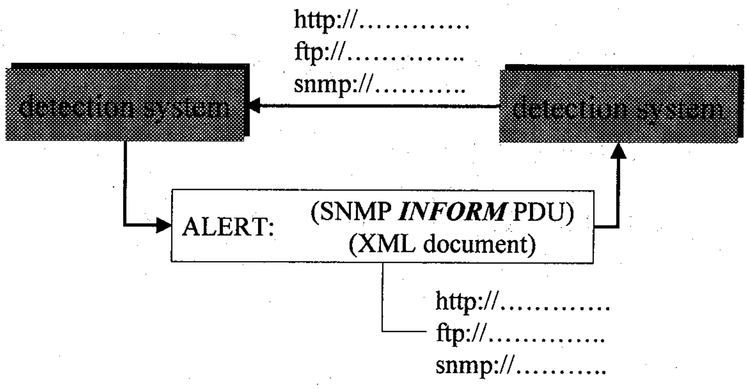
Cyber Solutions

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



http://............
ftp://.............
snmp://..........

detection system

detection system

ALERT: (SNMP ***INFORM*** PDU)
(XML document)

http://............
ftp://.............
snmp://..........

Cyber Solutions

IDS *vs* SNMP

Nikkei Internet Technology August 2000

Product name	NetProwler	CISCO Secure IDS	RealSecure Network Senso	NFR	SessionWall-3
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 E-mail Pager FAX *SNMP trap*	Popup Window E-mail *SNMP trap* Arbitrary program	Popup Window E-mail Pager *SNMP trap* Arbitrary program	Popup Window E-mail Pager FAX	Popup Window E-mail Pager *SNMP trap* Arbitrary program
Carrabolate firewall	Firewall-1 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

Intruder Alert	RealSecure OS Sensor	Kane Secure Enterprise	CyberCop Monitor	ICEpac
AXENT technologies	Internet Security Systems	Intrusion.com Inc.	Network Associates	Network ICE
http://www.axent.com/	http://www.iss.net/	http://www.inrusion.com/	http://www.nai.com/	http://www.networkice.com/
HIDS	HIDS	HIDS	NIDS/HIDS	NIDS/HIDS
50	50	5300	169	400
Popup Window E-mail Pager *SNMP trap* Arbitrary program	Popup Window E-mail Pager *SNMP trap* Arbitrary program	Popup Window E-mail Pager FAX	Popup Window E-mail *SNMP trap*	Popup Window E-mail *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 ?

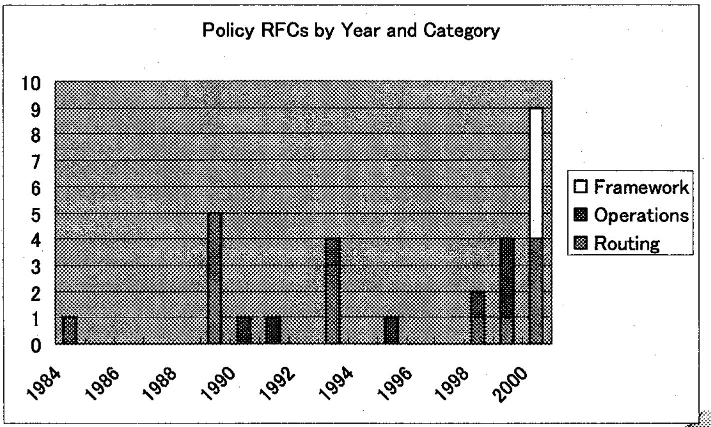
Cyber Solutions

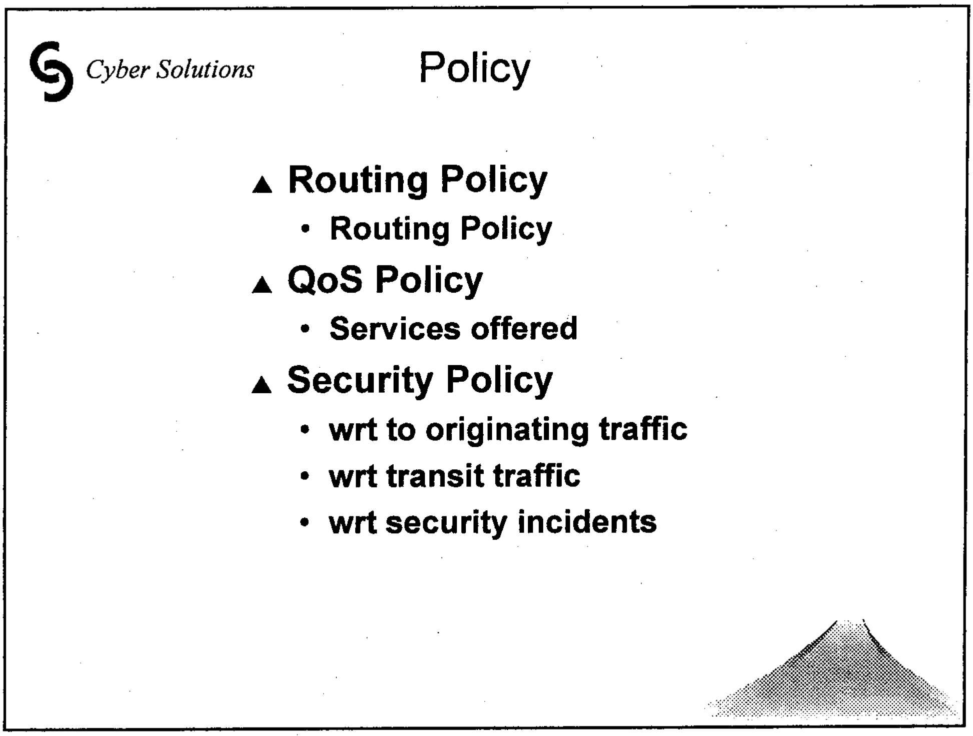
What Policy ?

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

Cyber Solutions

Policy Activity in the Internet

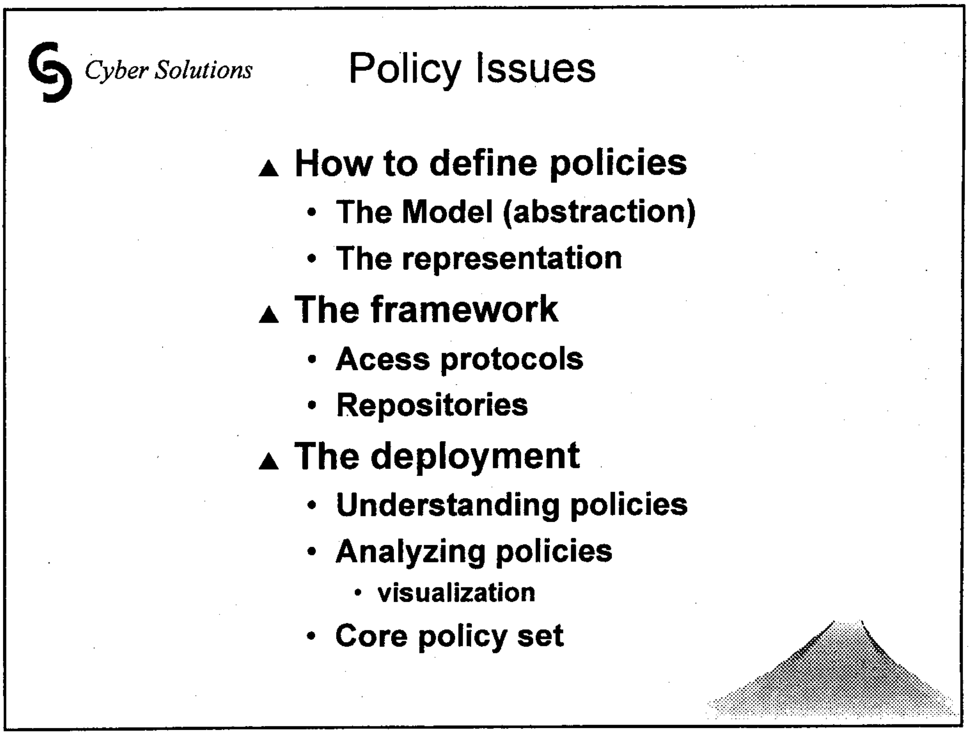




Cyber Solutions

Policy

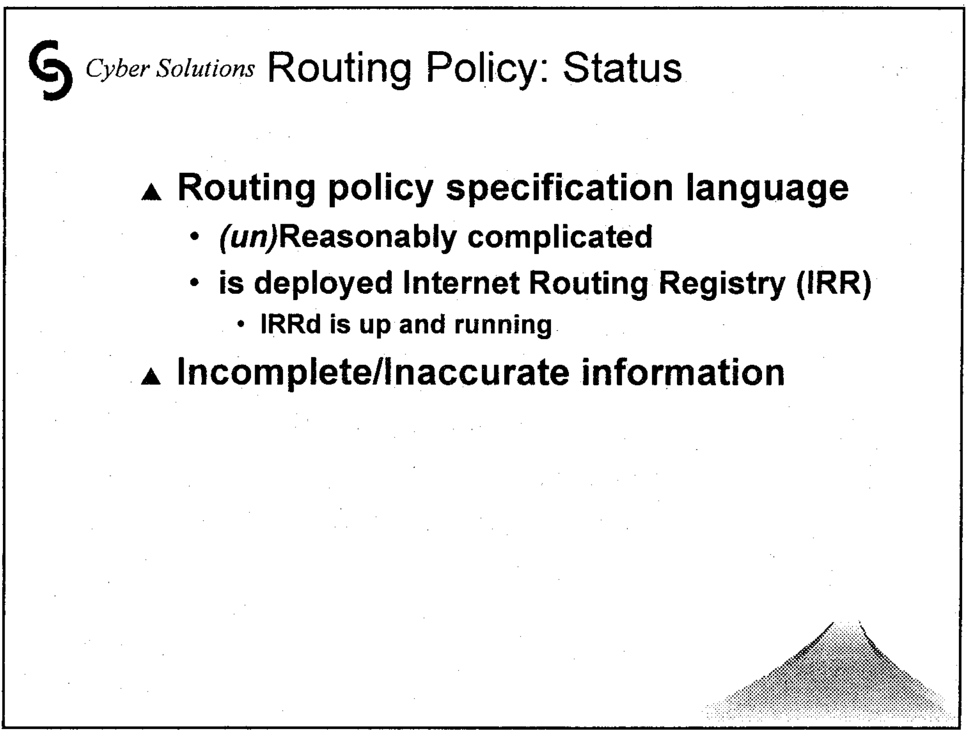
- ▲ **Routing Policy**
  - **Routing Policy**
- ▲ **QoS Policy**
  - **Services offered**
- ▲ **Security Policy**
  - **wrt to originating traffic**
  - **wrt transit traffic**
  - **wrt security incidents**



Cyber Solutions

Policy Issues

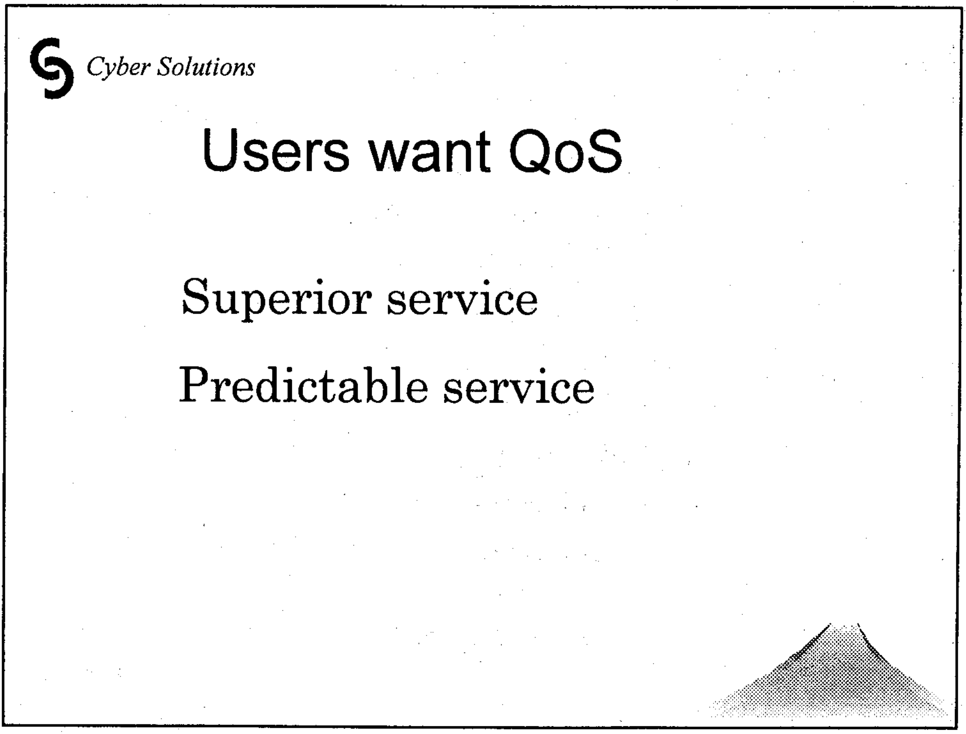
- ▲ **How to define policies**
  - **The Model (abstraction)**
  - **The representation**
- ▲ **The framework**
  - **Acess protocols**
  - **Repositories**
- ▲ **The deployment**
  - **Understanding policies**
  - **Analyzing policies**
    - **visualization**
  - **Core policy set**



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

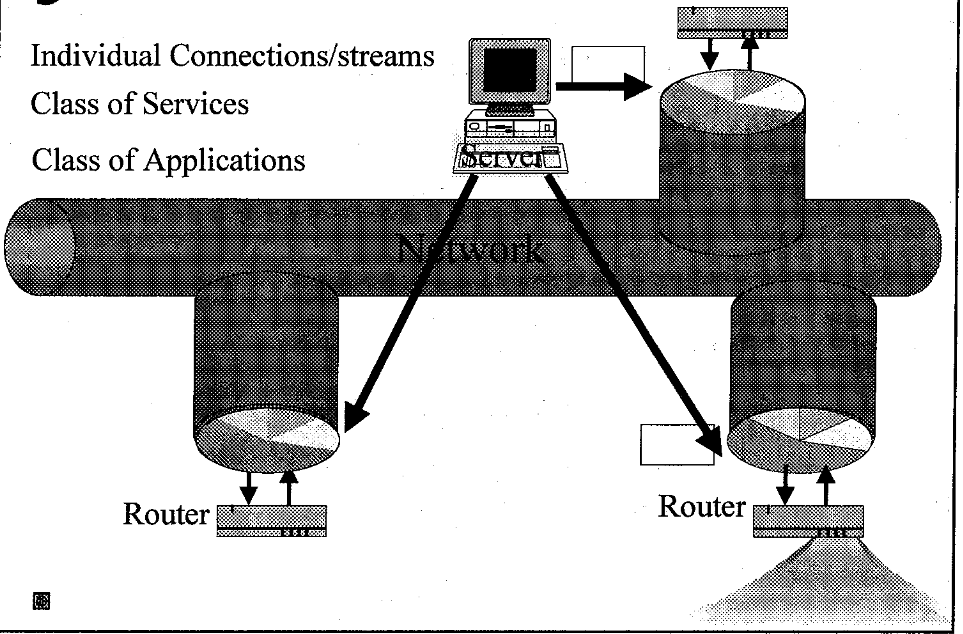
Cyber Solutions

QoS Management

Individual Connections/streams

Class of Services

Class of Applications



Cyber Solutions

QoS: The issues

Service Environment :

inaccurate and/or non-scaling

DiffServ is inaccurate

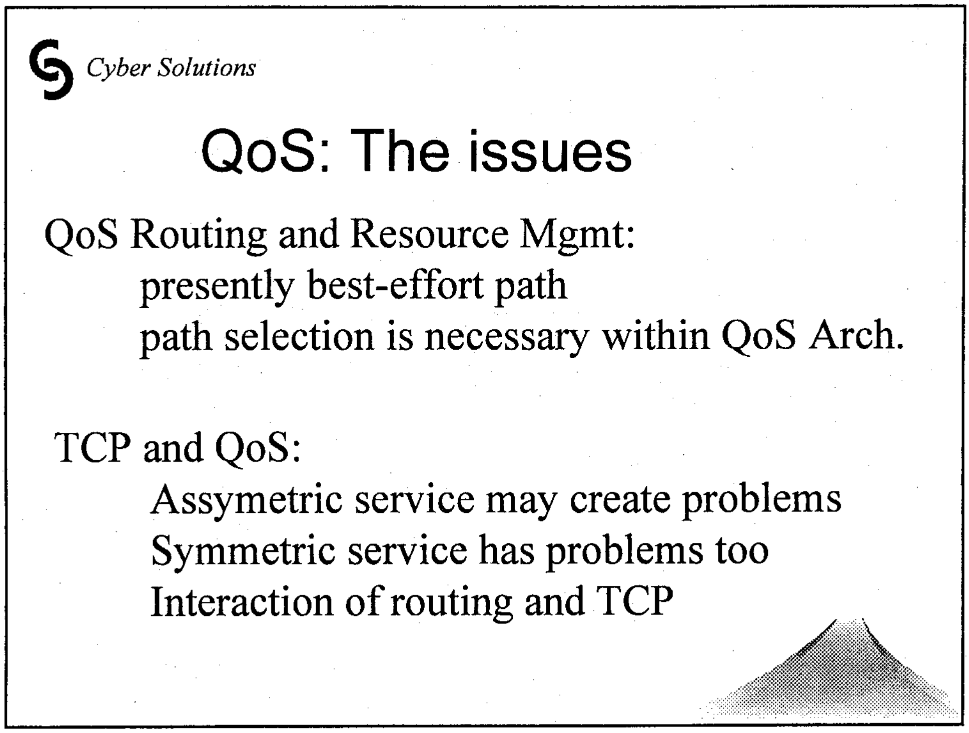
IntServ does not scale

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

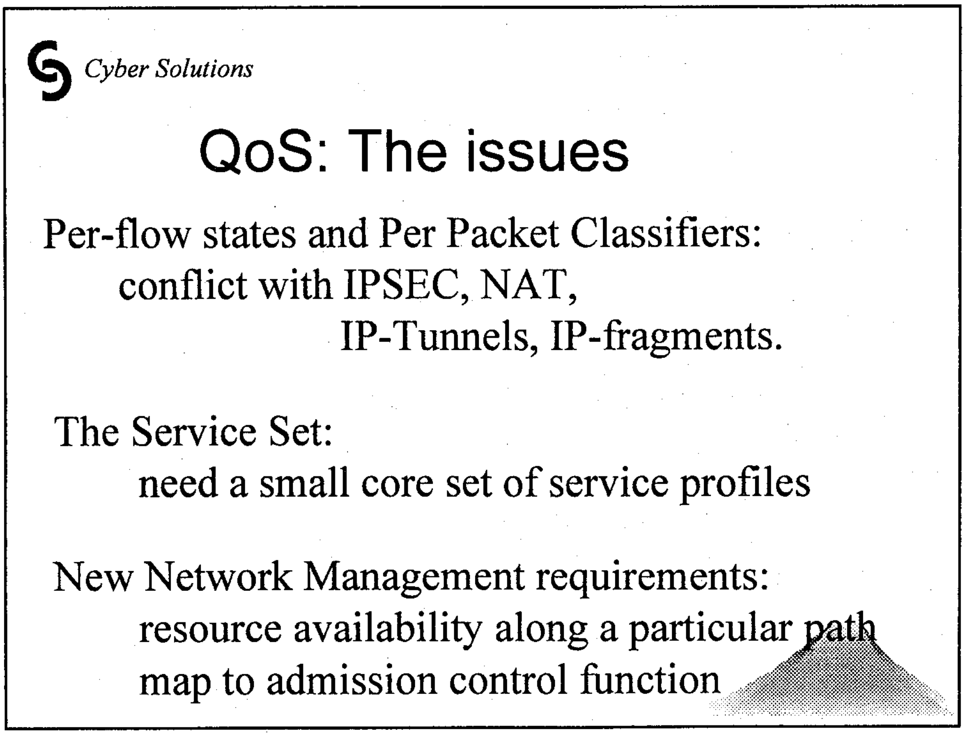
path selection is necessary within QoS Arch.

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.

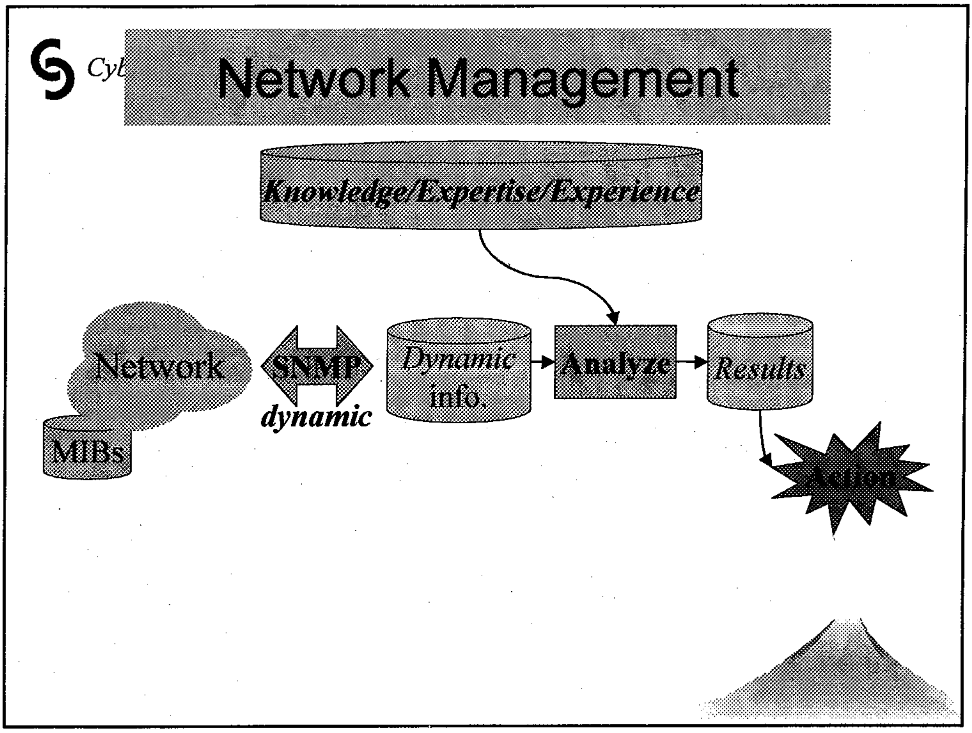
The Service Set:

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

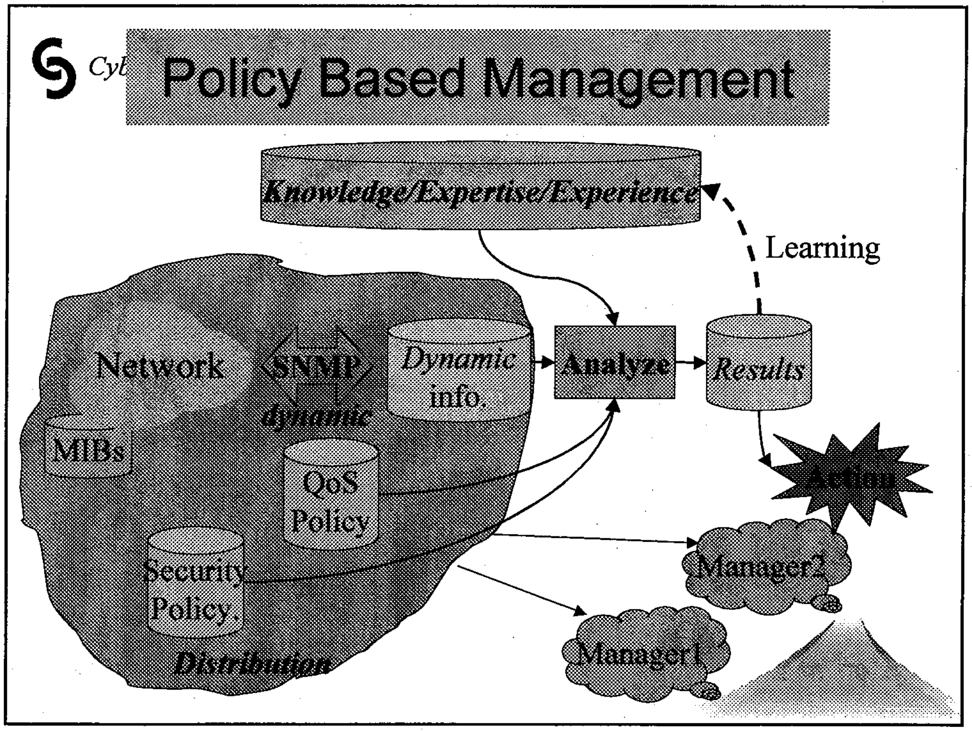
dynamic

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

Cyber Solutions

NetSkate

New-Generation network visualization and management tool

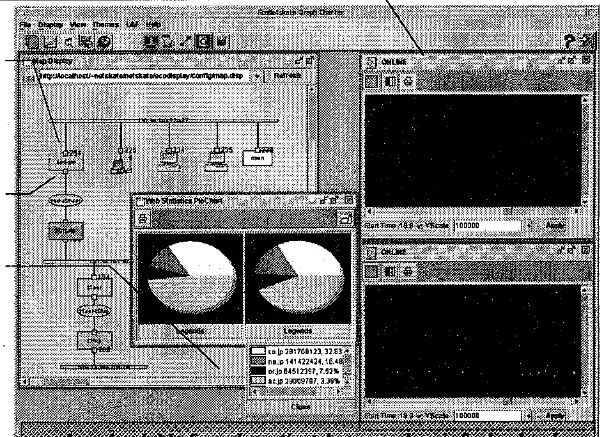
Online Network Taffic Graph

Map Auto Generation

Map Editor

On Map Status

Service Status



downloadable from http://netskate.cysol.co.jp/index.html

Cyber Solutions

ChaIn: Charting the Internet

http://www.cysols.com/IPAMaps/

File Edit View Places Help
Place: http://pooo.nemoto.ecei.tohoku.ac.jp/IPAMaps/
ChaIn
IPA

[illegible]

Moving ahead...
Keeping in pace with the times, we are now involved in the development of a web based system, developed using **Java**. The new system enables a user with a Java enabled browser, to access the maps and obtain information from the same.

The Projects ...

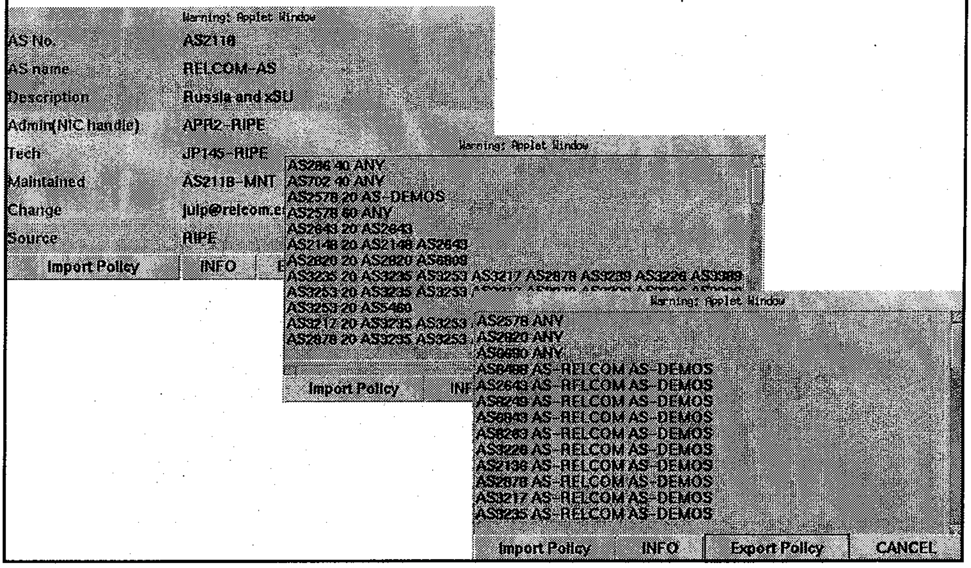
- The Intelligent and Interactive Map Display: This package is a convenient tool for getting a graphical representation of the inter-networked computers. It has many features like a good graphical interface, and search options.
- The Map Editor: This package is a map editor for modifying network maps which were auto-generated. *Please note: The Map Editor is not public, and requires a password to be entered for access.*
- Documentation: Documentation of the work done.

To view the Java applications you will need to have a Java Version 1.1 enabled browser. HotJava Browser 1.1.x supports Java 1.1. Click HERE to go to the HotJava page at JavaSoft.

IPA:Information technology Promotion Agency, Japan (www.ipa.go.jp)

Cyber Solutions

Policy Browser



Warning: Applet Window

AS No. AS2118
AS name RELCOM-AS
Description Russia and xSU
Admin(NIC handle) APR2-RIPE
Tech JP145-RIPE
Maintained AS2118-MNT
Change julp@relcom.e
Source RIPE

Warning: Applet Window

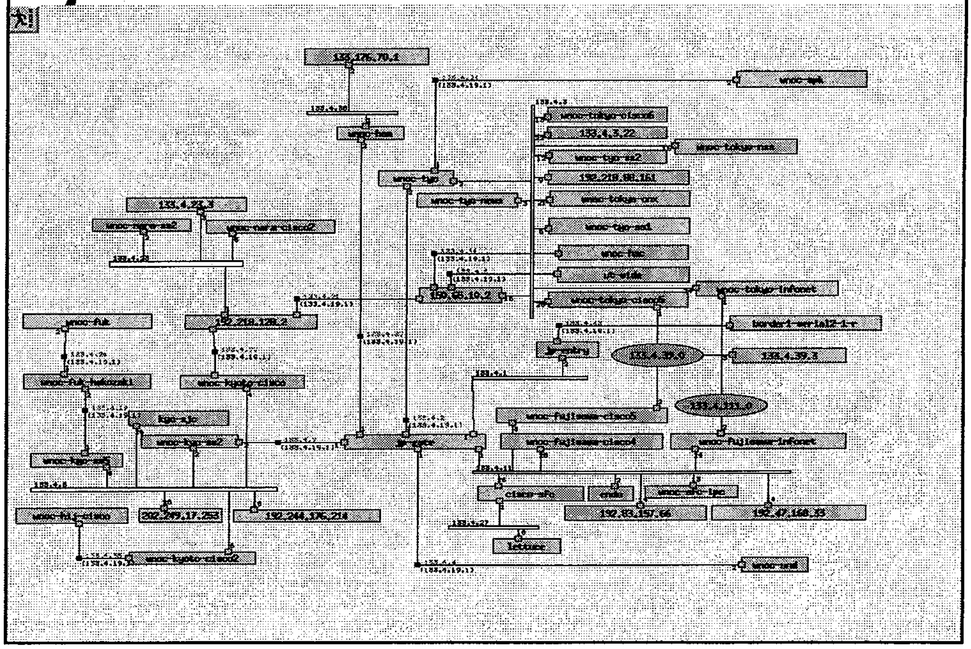
```
AS286 40 ANY
AS702 40 ANY
AS2578 20 AS-DEMOS
AS2578 60 ANY
AS2843 20 AS2843
AS2148 20 AS2148 AS2649
AS2820 20 AS2820 AS8809
AS3235 20 AS3235 AS3253 AS3217 AS2878 AS3239 AS3226 AS3989
AS3253 20 AS3235 AS3253
AS3253 20 AS5460
AS3217 20 AS3235 AS3253
AS2878 20 AS3235 AS3253
```

Warning: Applet Window

```
AS2578 ANY
AS2820 ANY
AS8690 ANY
AS8498 AS-RELCOM AS-DEMOS
AS2649 AS-RELCOM AS-DEMOS
AS8249 AS-RELCOM AS-DEMOS
AS6843 AS-RELCOM AS-DEMOS
AS8263 AS-RELCOM AS-DEMOS
AS3226 AS-RELCOM AS-DEMOS
AS2136 AS-RELCOM AS-DEMOS
AS2878 AS-RELCOM AS-DEMOS
AS3217 AS-RELCOM AS-DEMOS
AS3235 AS-RELCOM AS-DEMOS
```

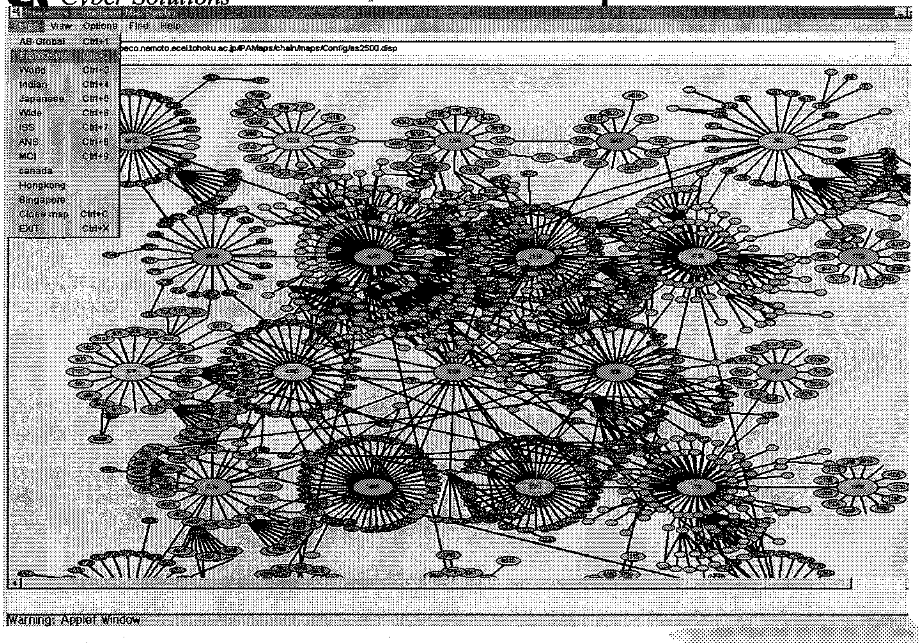
Cyber Solutions

AS Internals *from OSPF-MIB*



Cyber Solutions

AS-level Map

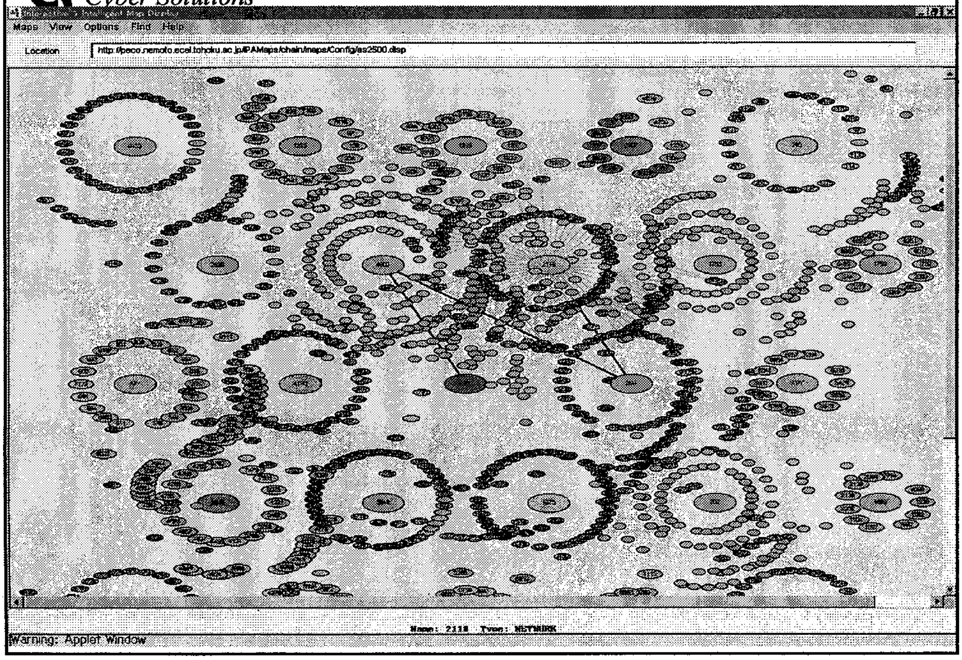


peco.nemoto.ecei.tohoku.ac.jp/PAMaps/chain/maps/Config/as2500.disp

Warning: Applet Window

Cyber Solutions

AS-Paths



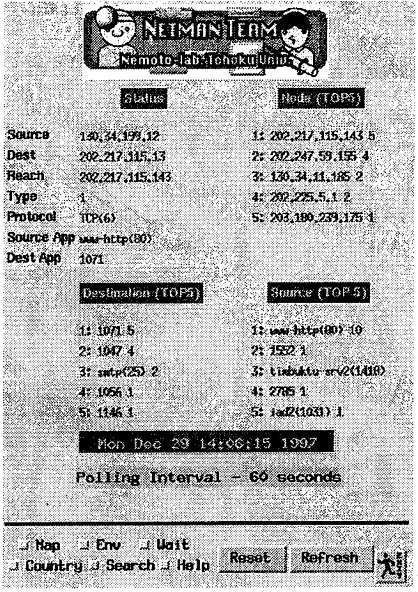
Location http://peco.nemoto.ecei.tohoku.ac.jp/PAMaps/chain/maps/Config/as2500.disp

Name: 7118 Type: NETWORK

Warning: Applet Window

Cyber Solutions

Wide-Area Management



NETMAN TEAM
Nemoto-lab Tohoku Univ.

Status

Source 130.34.199.12
Dest 202.217.115.13
Reach 202.217.115.143
Type 1
Protocol TCP(6)
Source App www-http(80)
Dest App 1071

Node (TOP5)

1: 202.217.115.143 5
2: 202.247.59.155 4
3: 130.34.11.185 2
4: 202.225.5.1 2
5: 203.180.239.175 1

Destination (TOP5)

1: 1071 5
2: 1047 4
3: smtp(25) 2
4: 1056 1
5: 1146 1

Source (TOP 5)

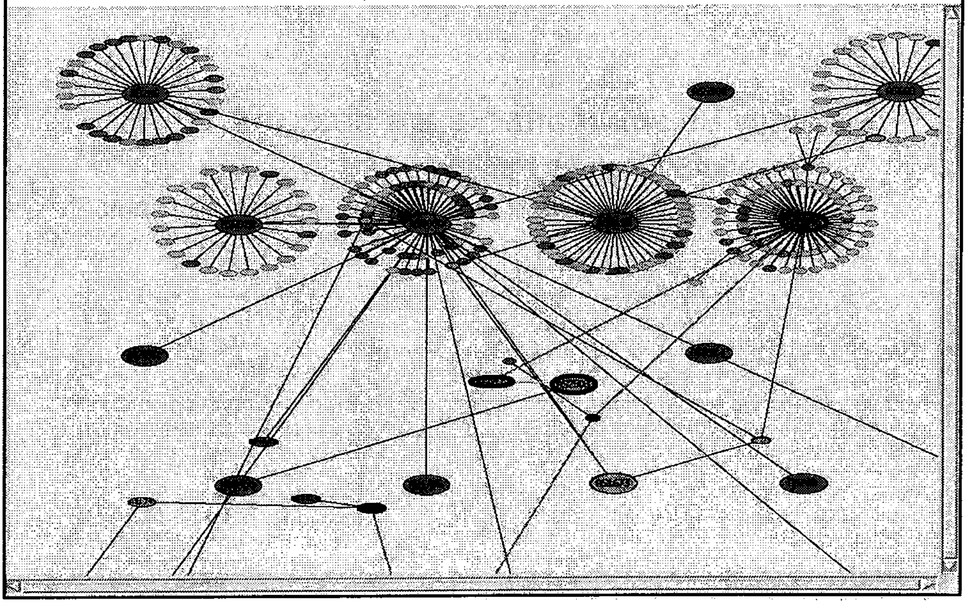
1: www-http(80) 10
2: 1552 1
3: timbuktu-srv2(1418)
4: 2785 1
5: iad2(1031) 1

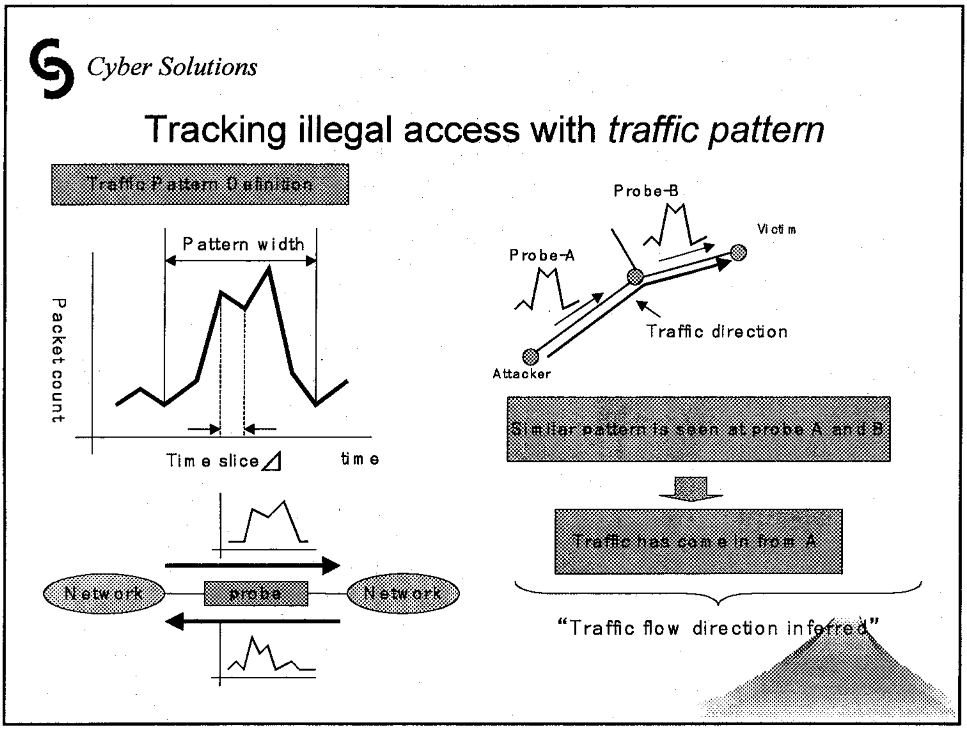
Mon Dec 29 14:06:15 1997

Polling Interval - 60 seconds

Cyber Solutions

Wide-Area Management





Cyber Solutions

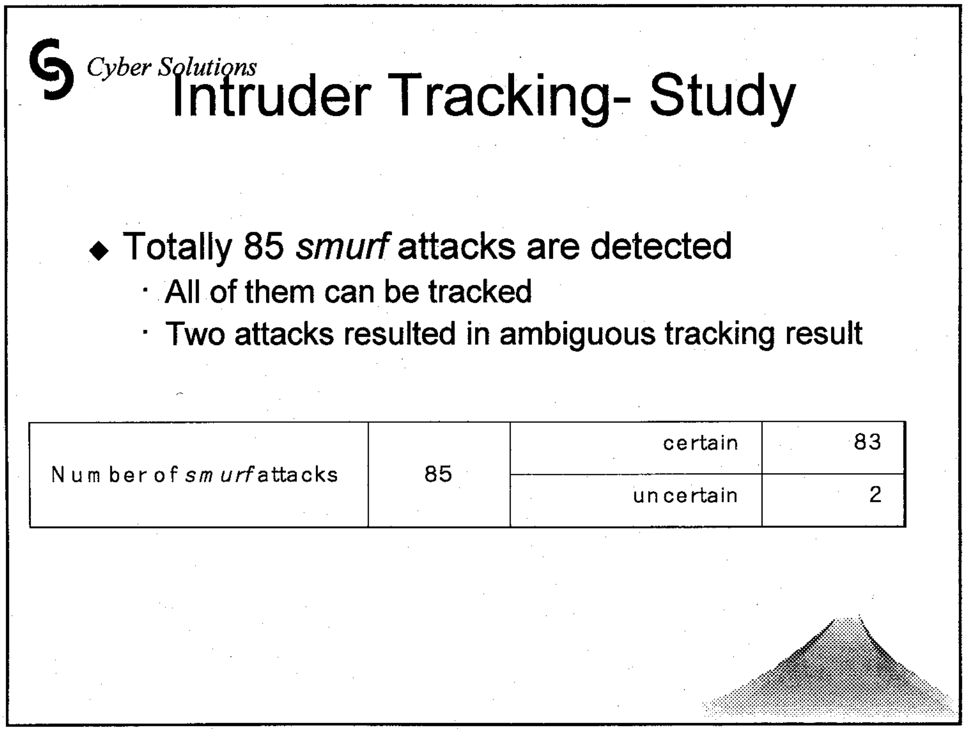
Tracking illegal access with *traffic pattern*

Traffic Pattern Definition

Similar pattern is seen at probe A and B

Traffic has come in from A

"Traffic flow direction inferred"



Cyber Solutions

Intruder Tracking- Study

- Totally 85 *smurf* attacks are detected
  - All of them can be tracked
  - Two attacks resulted in ambiguous tracking result

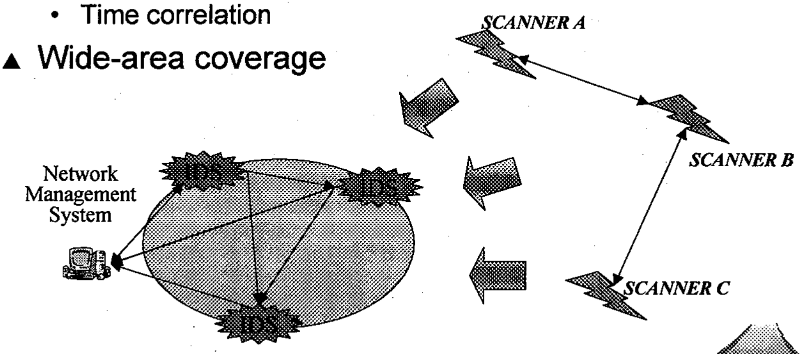
Number of *smurf* attacks	85	certain	83
		uncertain	2

Cyber Solutions

Distributed attack detection

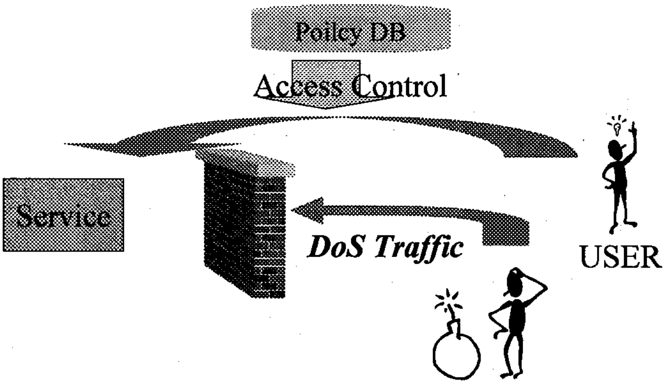
- for random, slow, distributed scan -

- ▲ Information correlation
  - Spatial correlation
  - Time correlation
- ▲ Wide-area coverage



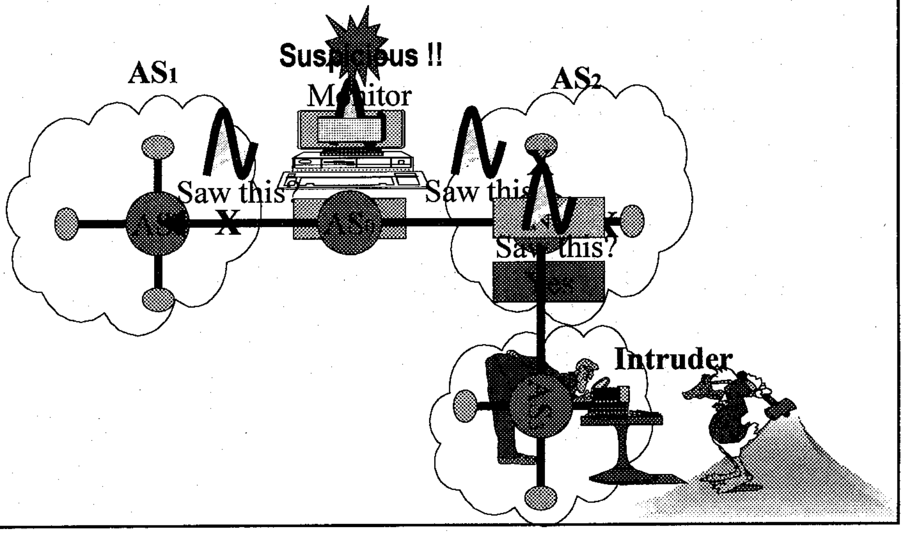
Cyber Solutions

DoS and Policy



Cyber Solutions

Distributed ID



Cyber Solutions

Conclusion

- ▲ Technology convergence
- ▲ Deploy enabling technologies -
  - Directory Services
  - IPv6
- ▲ New Ideas: Dynamic Directories