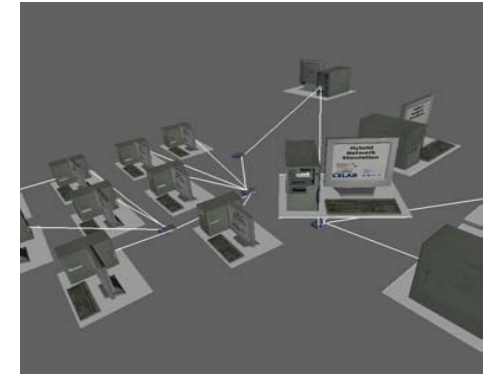
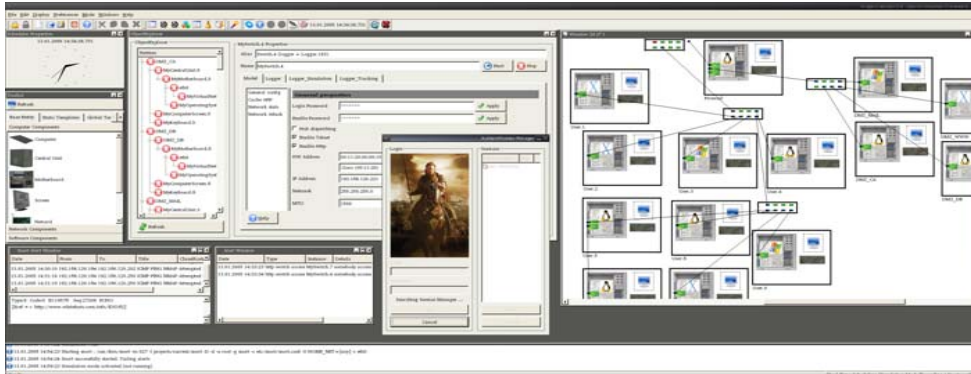


Simulation Hybride de la sécurité des systèmes d'information **« Vers un environnement virtuel de formation »** **La plate-forme EREBOR**

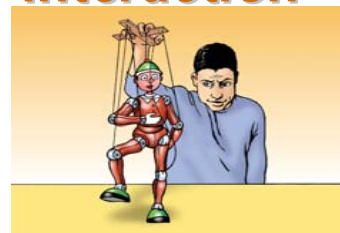
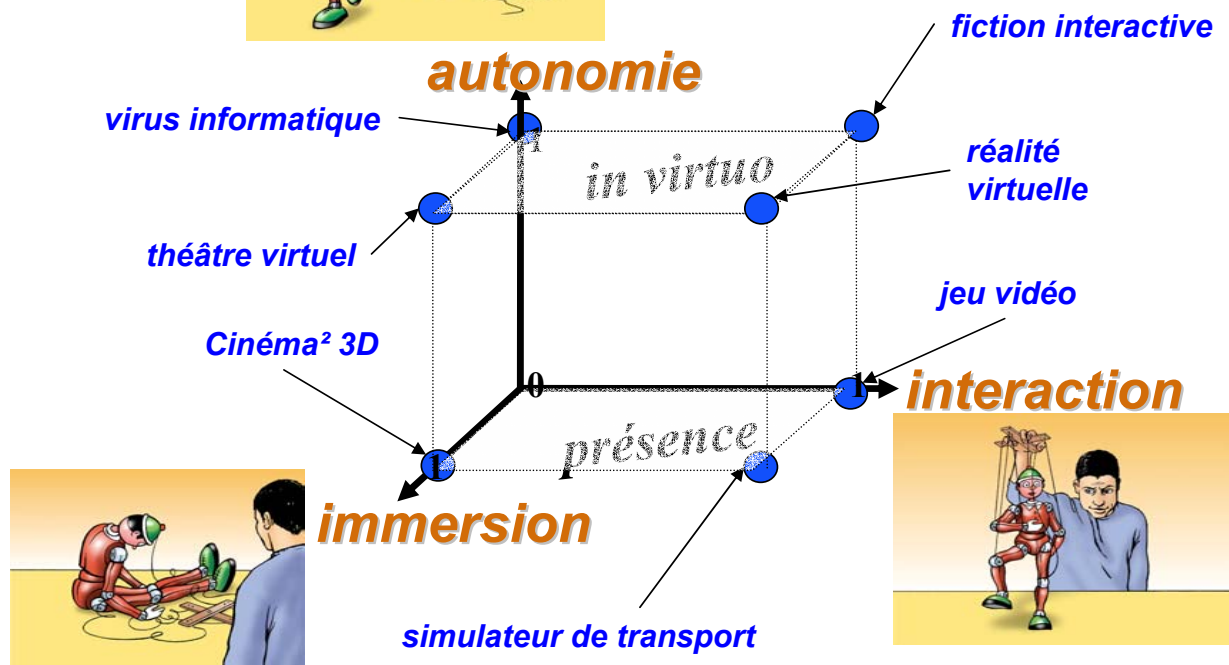


Guillaume PRIGENT / Fabrice HARROUET
Jacques TISSEAU / Frédéric PAUL

Centre Européen de Réalité Virtuelle
Ecole Nationale d'Ingénieurs de Brest

SSTIC 2005 - Rennes







Symposium sur la Sécurité des Technologies
de l'Information et des Communications 2005

**Simulation Hybride de la Sécurité des Systèmes d'Information
Vers un Environnement Virtuel de Formation
La plate-forme EREBOR**



Plate-forme EREBOR : Le projet

- **Projet de recherche**
 - Simulation hybride (au sens couplage)
 - Sécurité des systèmes d'information
- **Objectifs**
 - Formation
 - Tests
 - ...
- **Initiateurs du projet**
 - CERV/Li2/ENIB
 - DGA/CELAR

Plate-forme EREBOR : Principe de fonctionnement

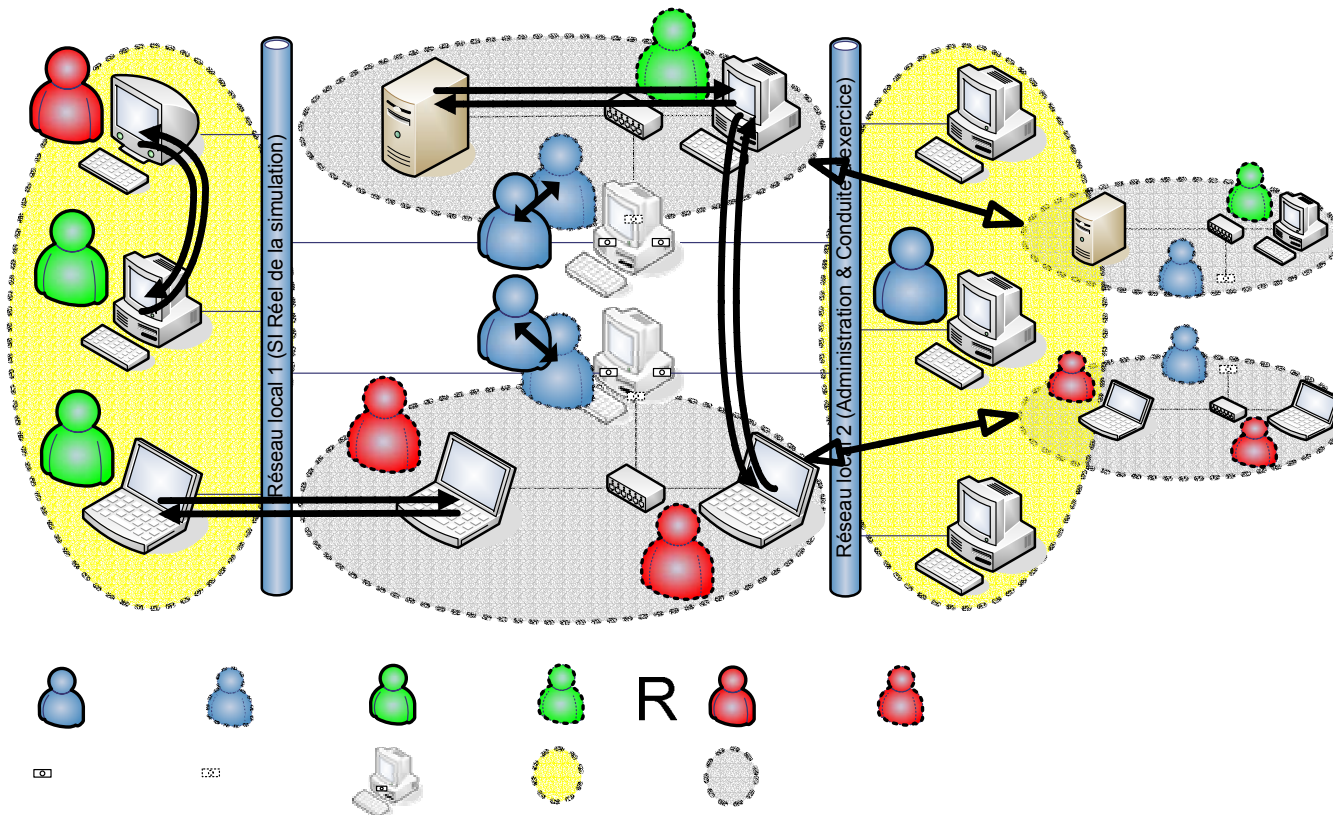
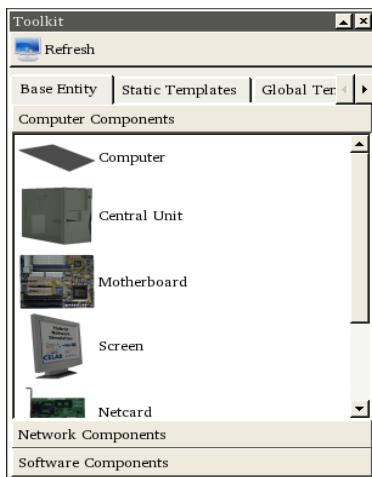
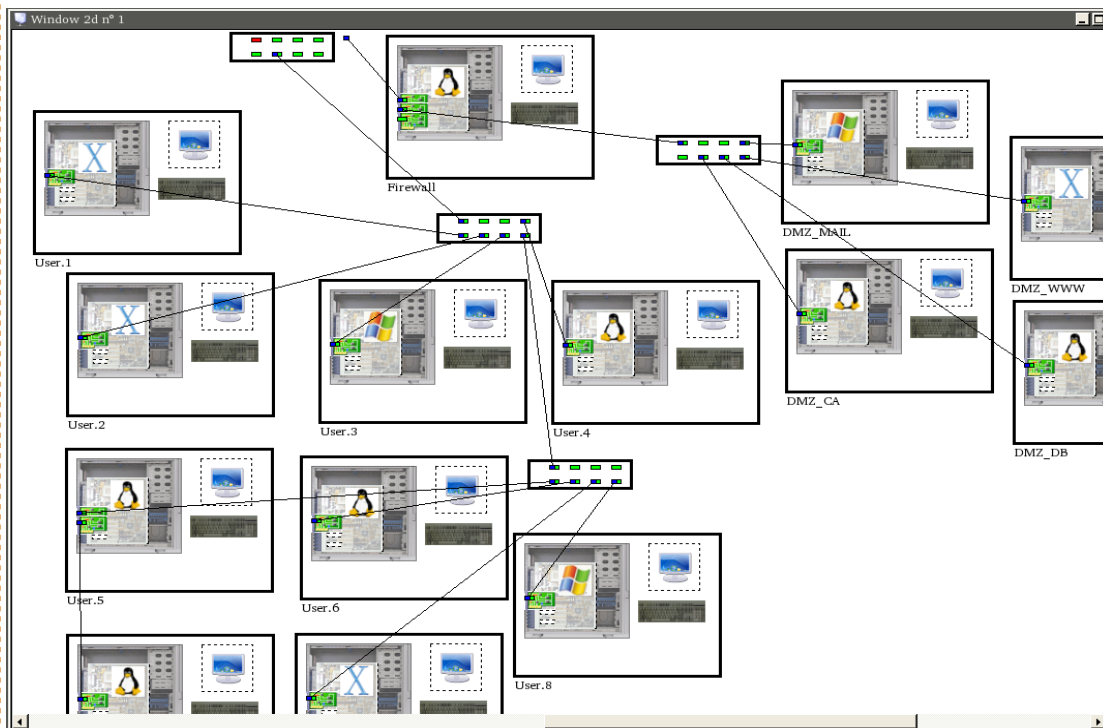


Plate-forme EREBOR : Interaction – Création / Modification du SI virtuel



Toolkit
création des entités
du monde virtuel



Vue d'architecture 2D du SI virtuel

Vue 2D permettant l'interaction avec le SI
(entités créées, branchement câbles...)

Plate-forme EREBOR : Interaction –

Création / Modification d'une entité du SI virtuel : un Système d'exploitation

MyOperatingSystem.8 Properties

Alias: OperatingSystem.8 (logger = Logger.65)

Name: MyOperatingSystem.8 [Start] [Stop]

Model: [Logger] [Logger_Simulation] [Logger_Tracking]

Netcard config

Route config

Stack TCP/IP

Cache ARP

TCP Server

Terminal

Network stats

IP Route's properties

Target: 0.0.0.0 Gateway: 192.168.120.1

Genmask: 0.0.0.0 Interface: eth0

[Help] [Add] [Del] [Apply] [Cancel]

Target	Gateway	Genmask	Interface
192.168.120.0 *		255.255.255.0	eth0
default	192.168.120.1	0.0.0.0	eth0

[Help]

**Propriétés d'un système d'exploitation :
Modification de la table de routage**

MyOperatingSystem.8 Properties

Alias: OperatingSystem.8 (logger = Logger.65)

Name: MyOperatingSystem.8 [Start] [Stop]

Model: [Logger] [Logger_Simulation] [Logger_Tracking]

Netcard config

Stack TCP/IP

Cache ARP

TCP Server

Terminal

Network stats

TCP/IP properties

ICMP: ☒ Reply to Echo Request (ping)

IP: ☐ Ip forwarding (such as router)

Stack Parameters (Experimental)

TTL: 64

TCP window size: 4128

Arp cache timeout: 30000

IP fragmentation timeout: 10000

Arp reply timeout: 1000

Tcp ack timeout: 3000

[Help]

**Propriétés d'un système d'exploitation :
Modification des attributs
de la pile TCP/IP
(ip forwarding, ttl, tcp window size, timeout...)**

Plate-forme EREBOR : Interaction – Création / Modification d'une entité du SI virtuel : un Switch

MySwitch.7 Properties

Alias Switch.7 (logger = Logger.189)

Name MySwitch.7 [Start] [Stop]

Model [Logger] [Logger_Simulation] [Logger_Tracking]

General config

Cache ARP
Network stats
Network Attack

General properties

Login Password [*****] [Apply]

Enable Password [*****] [Apply]

☐ Hub dispatching

☒ Enable Telnet

☒ Enable Http

HW Address [00:11:20:00:00:18] [Apply] [Find]

[Cisco (00:11:20)]

IP Address [192.168.120.224] [Apply] [Find]

Netmask [255.255.255.0] [Apply]

MTU [1500] [Apply]

[Help]

Propriétés d'un switch administrable :

Configuration générale

(login/pass, mode hub, acces telnet/http, adresses
mac/ip, mtu...)

MySwitch.7 Properties

Alias Switch.7 (logger = Logger.189)

Name MySwitch.7 [Start] [Stop]

Model [Logger] [Logger_Simulation] [Logger_Tracking]

General config

Cache ARP
Network stats
Network Attack

ARP Cache's properties

☒ Auto Refresh ARP Entries [Refresh] [Clear]

	Protocol	Address	Age (min)	Hardware Addr	T
1	Unknown	-	2	00:04:00:CB:B7:7	A
2	Internet	192.168.120.167	2	00:04:75:AE:45:6	A
3	Unknown	-	2	00:0E:83:AE:9C:6	A
4	Address Resolutio	192.168.120.207	2	00:11:20:00:00:C	A
5	Address Resolutio	192.168.120.208	2	00:11:20:00:00:C	A
6	Address Resolutio	192.168.120.209	2	00:11:20:00:00:C	A
7	Address Resolutio	192.168.120.210	2	00:11:20:00:00:C	A
8	Address Resolutio	192.168.120.211	2	00:11:20:00:00:C	A
9	Address Resolutio	192.168.120.212	2	00:11:20:00:00:C	A
10	Address Resolutio	192.168.120.214	2	00:11:20:00:00:C	A
11	Address Resolutio	192.168.120.215	2	00:11:20:00:00:C	A

[Help]

Propriétés d'un switch administrable :

Vue / Modification du cache arp

Plate-forme EREBOR : Contrôle / Interaction

Fenêtres d'alertes / logs

- Visualisation des traces d'activité de chaque entité / enregistrement du trafic réseau au format pcap
- Visualisation des connexions aux entités du réseau virtuel
- attaques détectées par IDS

Model Logger Logger_Simulation Logger_Tracking						
Debug Info Warning Error						
Date	Filename/line	Category	Class	Instance	Log type	Details
14.01.2005 14:39:39	../model/switch.cpp:440	Debug	Switch	MySwitch.2	MethodCall	Switch::pullFrame()
14.01.2005 14:39:39	../model/switch.cpp:449	Debug	Switch	MySwitch.2	Misc	memcpy() effected
14.01.2005 14:39:39	../model/switch.cpp:582	Debug	Switch	MySwitch.2	MethodCall	Switch::pullFrame()
14.01.2005 14:39:39	../model/switch.cpp:582	Debug	Switch	MySwitch.2	MethodCall	Switch::pullFrame()
14.01.2005 14:39:39	../model/switch.cpp:582	Debug	Switch	MySwitch.2	MethodCall	Switch::pullFrame()
14.01.2005 14:39:39	../model/switch.cpp:638	Debug	Switch	MySwitch.2	Misc	Switch::processQueue
14.01.2005 14:39:39	../model/switch.cpp:641	Debug	Switch	MySwitch.2	MethodCall	pulling frame to MyS
14.01.2005 14:39:39	../model/switch.cpp:855	Debug	Switch	MySwitch.2	MethodCall	Switch::processQueue
14.01.2005 14:39:40	../model/switch.cpp:438	Debug	Switch	MySwitch.2	MethodCall	Switch::pullFrame()
14.01.2005 14:39:40	../model/switch.cpp:440	Debug	Switch	MySwitch.2	MethodCall	Switch::pullFrame()
14.01.2005 14:39:40	../model/switch.cpp:449	Debug	Switch	MySwitch.2	Misc	memcpy() effected
14.01.2005 14:39:40	../model/switch.cpp:582	Debug	Switch	MySwitch.2	MethodCall	Switch::pullFrame()
14.01.2005 14:39:40	../model/switch.cpp:638	Debug	Switch	MySwitch.2	Misc	Switch::processQueue
14.01.2005 14:39:40	../model/switch.cpp:641	Debug	Switch	MySwitch.2	MethodCall	pulling frame to MyS
14.01.2005 14:39:40	../model/switch.cpp:855	Debug	Switch	MySwitch.2	MethodCall	Switch::processQueue

Alert Window			
Date	Type	Instance	Details
13.01.2005 14:33:23	http switch access	MySwitch.7	somebody access
13.01.2005 14:33:34	http switch access	MySwitch.4	somebody access

Snort Alert Window				
Date	From	To	Title	Classification
13.01.2005 14:30:10	192.168.120.164	192.168.120.202	ICMP PING NMAP Attempted	
13.01.2005 14:31:18	192.168.120.164	192.168.120.250	ICMP PING NMAP Attempted	
13.01.2005 14:31:19	192.168.120.164	192.168.120.250	ICMP PING NMAP Attempted	
Type:8 Code:0 ID:19576 Seq:27208 ECHO				
[Xref => http://www.whitehats.com/info/IDS162]				

Plate-forme EREBOR : Immersion dans un environnement virtuel 3D



Vue 3D physique du SI virtuel

Plate-forme EREBOR : Immersion dans un environnement virtuel 3D (Granularité des entités du monde virtuel)



Visualisation du contenu d'une entité « Computer », composé
d'une carte mère, de cartes réseaux ...

Plate-forme EREBOR : Simulation / Simulation hybride – Virtuel → Réel

Terminals

New Exit Edit

Terminal n°1

Start Stop

```

receive 40 bytes from 192.168.120.1 icmp_seq=5
send 40 bytes to 192.168.120.1 icmp_seq=6 ttl=64
receive 40 bytes from 192.168.120.1 icmp_seq=6
send 40 bytes to 192.168.120.1 icmp_seq=7 ttl=64
receive 40 bytes from 192.168.120.1 icmp_seq=7
send 40 bytes to 192.168.120.1 icmp_seq=8 ttl=64
receive 40 bytes from 192.168.120.1 icmp_seq=8
send 40 bytes to 216.239.59.104 icmp_seq=1 ttl=64
receive 40 bytes from 216.239.59.104 icmp_seq=1
send 40 bytes to 216.239.59.104 icmp_seq=2 ttl=64
receive 40 bytes from 216.239.59.104 icmp_seq=2
send 40 bytes to 216.239.59.104 icmp_seq=3 ttl=64
receive 40 bytes from 216.239.59.104 icmp_seq=3
send 40 bytes to 216.239.59.104 icmp_seq=4 ttl=64
receive 40 bytes from 216.239.59.104 icmp_seq=4

```

Ping virtuel → réel → internet

Terminal n°1

Start Stop

```

Starting mnap 0.5 ( http://www.enib.fr/li2/ )
Interesting ports on 192.168.120.111:
(The 6 ports scanned but not shown below are in state: closed)
PORT      STATE  SERVICE
22/tcp    open   unknow
80/tcp    open   unknow
139/tcp   open   unknow
445/tcp   open   unknow

Mnap run completed -- Thank's to use it !
send 64 bytes to 192.168.130.203 icmp_seq=1 ttl=128
receive 64 bytes from 192.168.130.203 icmp_seq=1
send 64 bytes to 192.168.130.203 icmp_seq=2 ttl=128
receive 64 bytes from 192.168.130.203 icmp_seq=2
send 64 bytes to 192.168.120.1 icmp_seq=1 ttl=128
receive 64 bytes from 192.168.120.1 icmp_seq=1
send 64 bytes to 192.168.120.1 icmp_seq=2 ttl=128
receive 64 bytes from 192.168.120.1 icmp_seq=2

```

**Nmap virtuel → réel /
Ping virtuel → virtuel / réel**

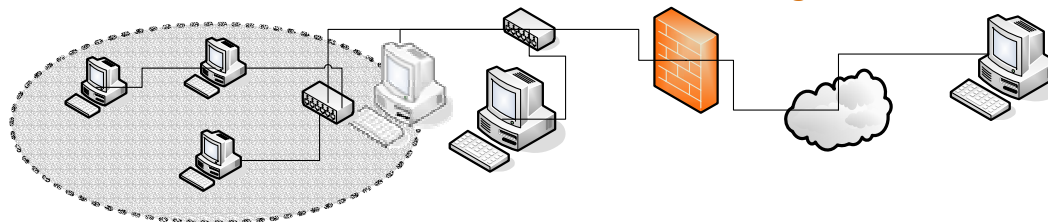


Plate-forme EREBOR : Simulation / Simulation hybride – Réel → Virtuel

```

ereb3:/etc/apt# telnet 192.168.120.202
Trying 192.168.120.202...
Connected to 192.168.120.202.
Escape character is '^['.

User Access Verification

Password:erebor

Password:erebor
MySwitch.1>show arp

```

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	0.0.0.0 30	00:04:00:CB:B7:CC	ARPA	MyHybridNetport.1	
Internet	192.168.120.167 30	00:04:75:AE:45:6A	ARPA	MyHybridNetport.1	
Address Resolution	192.168.120.113 29	00:0C:76:3A:A2:15	ARPA	MyHybridNetport.1	
Unknown	- 30	00:0E:83:AE:9C:C1	ARPA	MyHybridNetport.1	
Address Resolution	192.168.120.201 30	00:11:20:00:00:01	ARPA	MyVirtualNetport.6	
Address Resolution	192.168.120.110 22	00:11:2F:71:C6:A0	ARPA	MyHybridNetport.1	
Internet	207.46.106.102 30	00:40:05:5A:ED:03	ARPA	MyHybridNetport.1	
Internet	192.168.120.164 21	00:C0:4F:63:D6:14	ARPA	MyHybridNetport.1	
Address Resolution	192.168.120.111 29	08:00:46:B2:CF:A1	ARPA	MyHybridNetport.1	

```

MySwitch.1>exit
Connection closed by foreign host.
ereb3:/etc/apt# ping 192.168.120.201
PING 192.168.120.201 (192.168.120.201): 56 data bytes
64 bytes from 192.168.120.201: icmp_seq=0 ttl=64 time=2.1 ms
64 bytes from 192.168.120.201: icmp_seq=1 ttl=64 time=0.4 ms
64 bytes from 192.168.120.201: icmp_seq=2 ttl=128 time=0.5 ms
64 bytes from 192.168.120.201: icmp_seq=3 ttl=128 time=0.5 ms
64 bytes from 192.168.120.201: icmp_seq=4 ttl=128 time=1.4 ms
64 bytes from 192.168.120.201: icmp_seq=9 ttl=128 time=1.1 ms
64 bytes from 192.168.120.201: icmp_seq=10 ttl=128 time=0.6 ms
64 bytes from 192.168.120.201: icmp_seq=11 ttl=128 time=0.4 ms

--- 192.168.120.201 ping statistics ---
12 packets transmitted, 8 packets received, 33% packet loss
round-trip min/avg/max = 0.4/0.8/2.1 ms
ereb3:/etc/apt#

```

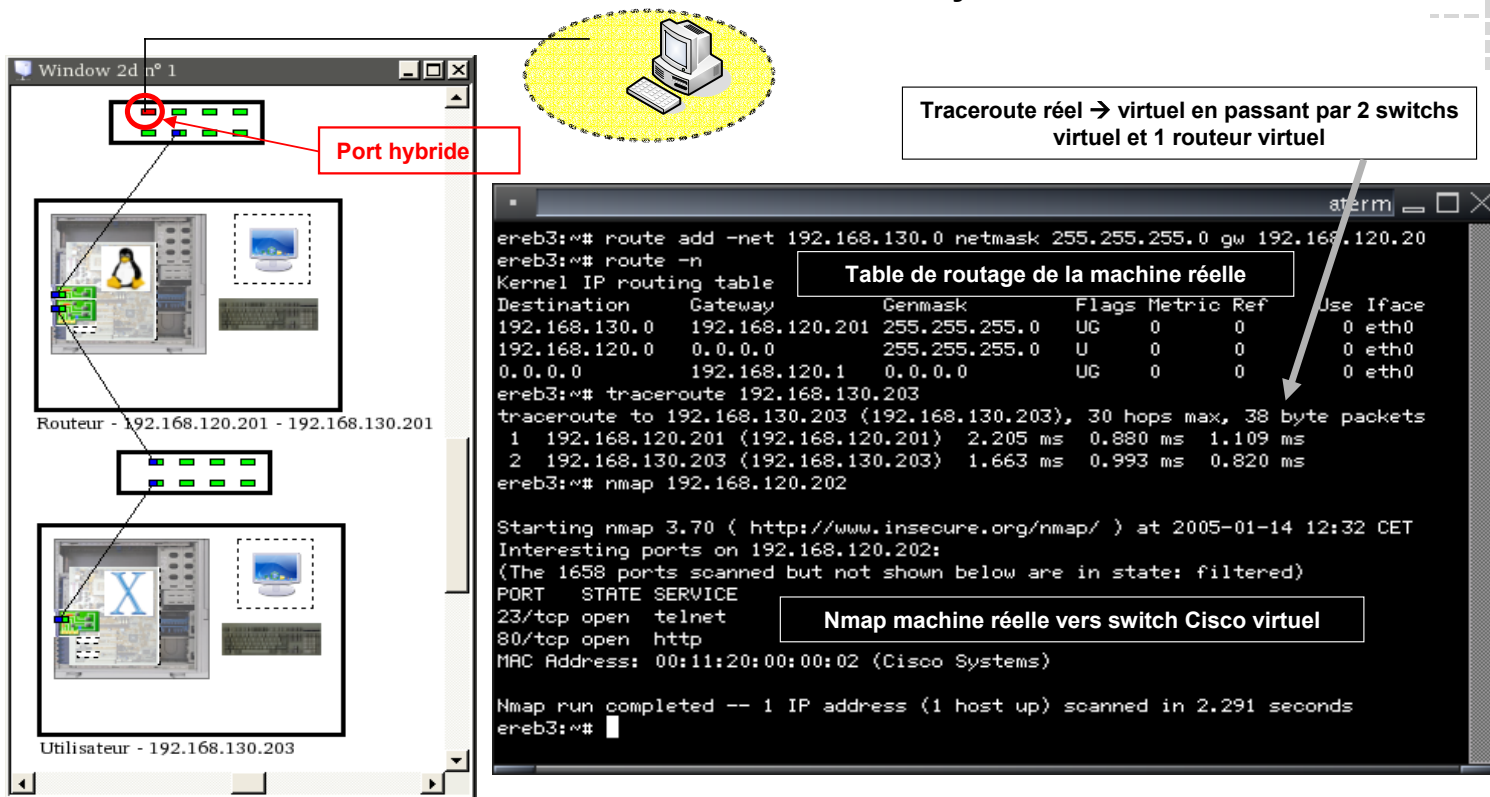
Connexion telnet sur un switch
virtuel administrable

Visualisation du cache arp

Modification du
TTL à la volée

Débranchement du
câble dans le virtuel

Plate-forme EREBOR : Simulation / Simulation hybride – Réel → Virtuel



**Plate-forme EREBOR : Simulation / Simulation hybride – Réel → Virtuel
Connexion http sur un switch virtuel administrable**

Close Window

Toolkit: Roll over tools below

Cisco WS-C2950T-24

HOME
EXPRESS SETUP
CLUSTER
MANAGEMENT SUITE
TOOLS
HELP RESOURCES

Home: Summary Status

Network Identity	
IP Address	192.168.120.202
MAC Address	00:11:20:00:00:02

System Details	
Host Name	MySwitch.1
System Uptime	not yet implemented !
Serial Number	FOC0747YR22
Software Version	12.1(19)EA1c
System Contact	
System Location	

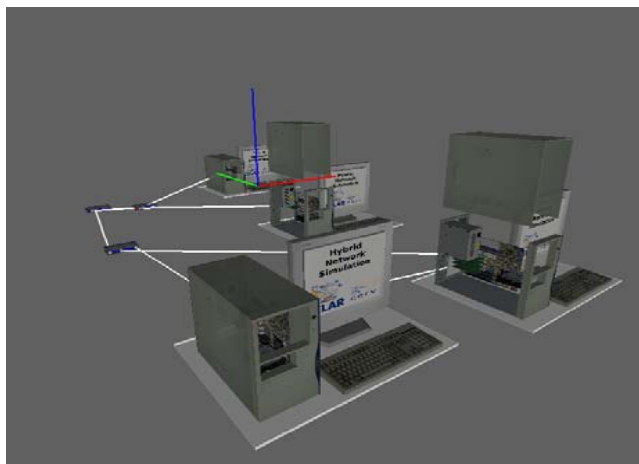
Refresh

Close Window Copyright (c) 2003 by Cisco Systems, Inc.

Plate-forme EREBOR : Fonctionnalités logicielles

- **Ordonnanceur hybride : temps réel + virtuel**
- **Enregistrement du trafic réseau (format pcap)**
- **Interaction avec le réseau virtuel à la volée**
- **Création / sauvegarde / chargement de modèles de systèmes**

**Merci de votre attention.
Avez-vous des questions ?**



**Symposium sur la Sécurité des Technologies de l'Information
et des Communications 2005**

- Rennes, Juin 2005 -

CERV/Li2/ENIB 2005 – guillaume.prigent@enib.fr - harrouet@enib.fr - tisseau@enib.fr - fpaul@enib.fr

