Testing indirecto asistido por virtualización:
Aplicación al testing de IPsec en IPv6

Ariel Sabiguero María Eugenia Corti

Instituto de Computación, Facultad de Ingeniería, Universidad de la República
J. Herrera y Reissig 565, Montevideo, Uruguay
{asabigue,mcorti}@fing.edu.uy

25/11/2008

1. Introducción
   - Acerca de IPsec
   - Modalidades de operación
   - Descripción de los casos de prueba

2. Tests de conformidad en protocolos de red
   - Concepto de conformance testing
   - Modelo de referencia de redes TCP/IP
   - Comparación de los requerimientos de implementación

3. Resumen y conclusiones
   - Resumen
   - Conclusiones

jiio 2008

Motivación: ¿Por qué es relevante IPsec sobre IPv6?

- IPv6 reamplazará IPv4 y cuando esto ocurra, deberá ser, al menos, igual de confiable
- IETF, a través del *IPv6 Forum* ha puesto especial énfasis en las características de seguridad de IPv6, recomendando que todas las implementaciones incluyan IPsec
- El IPv6 Ready Logo, del IPv6 Forum publicó un conjunto de pruebas estándar que tienen que cumplir las implementaciones de IPsec
- La metodología aplicada hasta el presente por el v6RL presenta dificultades para la implementación...

jiio 2008

IPsec: suite de protocolos de seguridad

	Authentication Header (AH)	Encapsulating Security Payload (ESP)
Connectionless Integrity	√	√
Data Origin Authentication	√	√
Access Control	√	√
Confidentiality	×	√

jiio 2008

Conjunto de algoritmos criptográficos

Algoritmos de encriptación

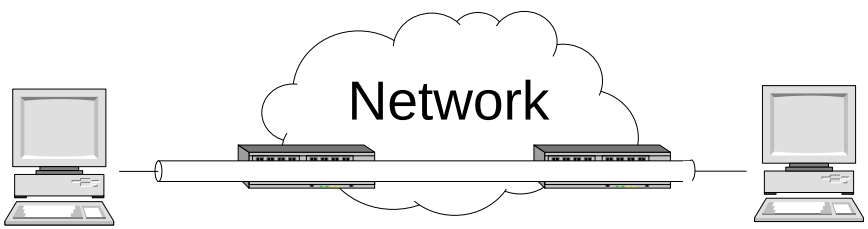
- 3DES-CBC
- NULL
- AES-CBC
- AES-CTR

Algoritmos de autenticación

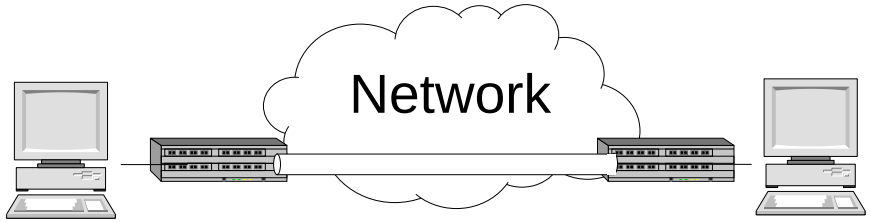
- HMAC-SHA1-96
- NULL
- AES-XCBX-MAC-96

jiio 2008

Modos de IPsec



Modo Transporte



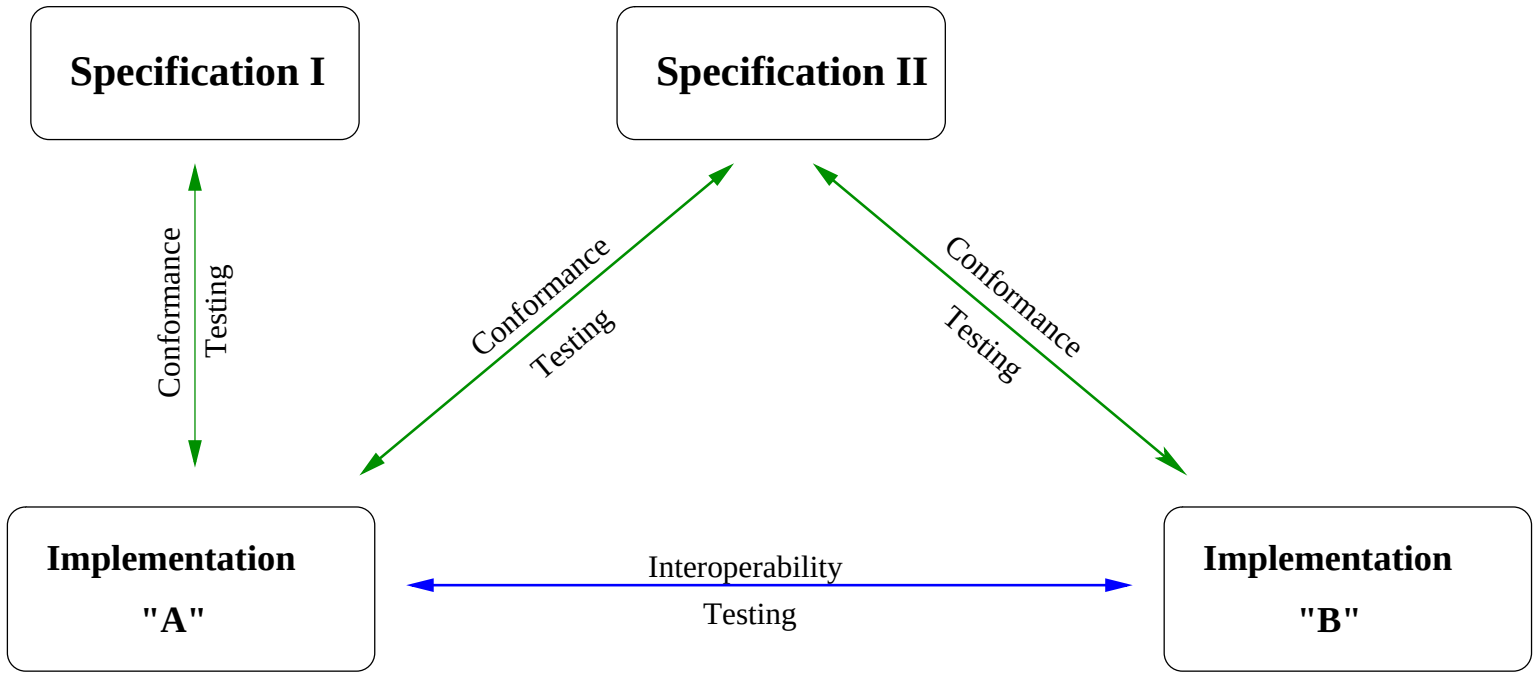
Modo Tunel

Cobertura de la suite de pruebas del v6RL

- Modos Tunel y Transporte
- Combinación de diferentes algoritmos de encriptación y autenticación
- Solamente ESP
- Configuración manual de las claves
- Se prueba conectividad mediante intercambio de mensajes ICMPv6
- ...

jiio 2008

Objeto del test Conformidad o Conformance

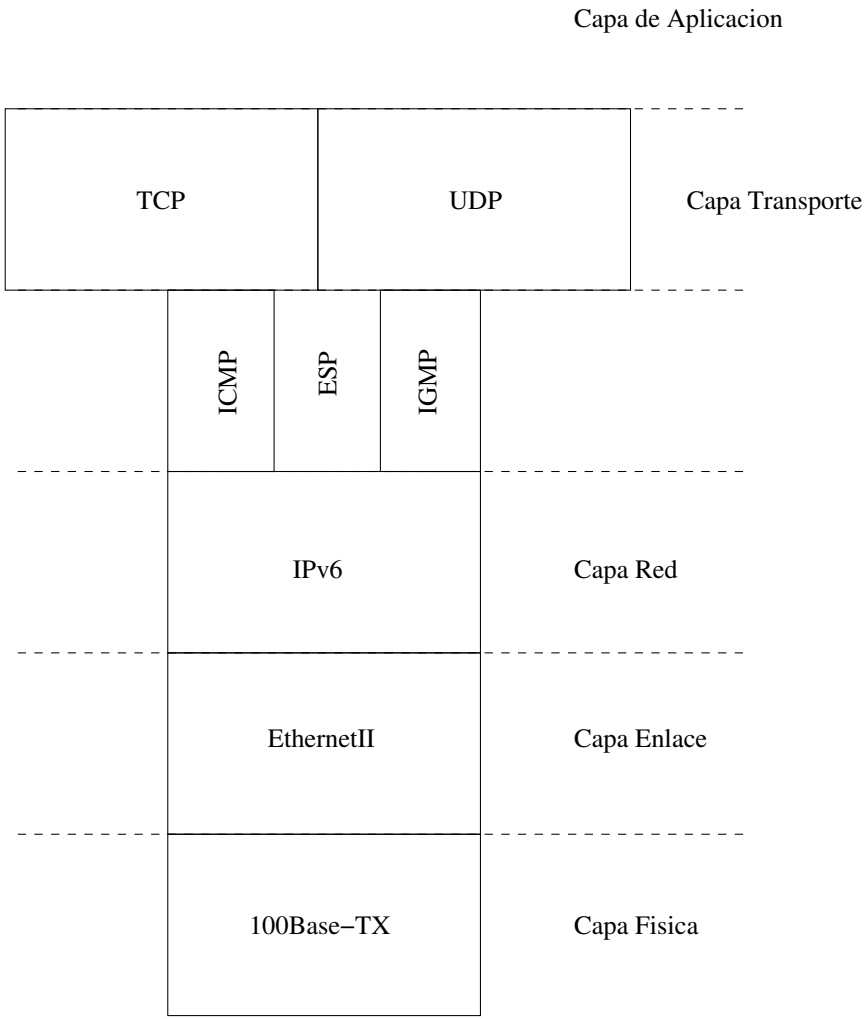


Informalmente

Asegurar que una implementación (IUT-Implementation Under Test) se comporta correctamente de acuerdo a su especificación.

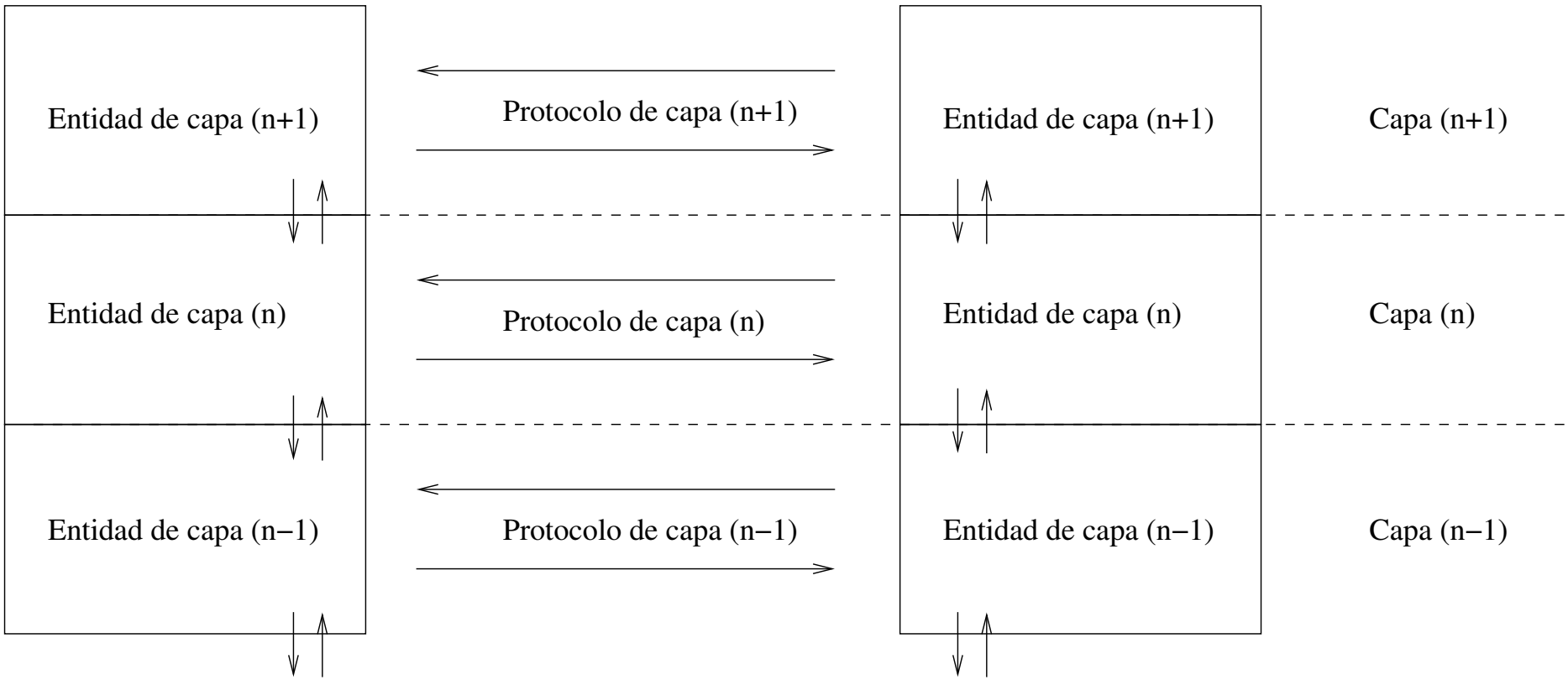
jiio 2008

Modelo de referencia de redes TCP/IP



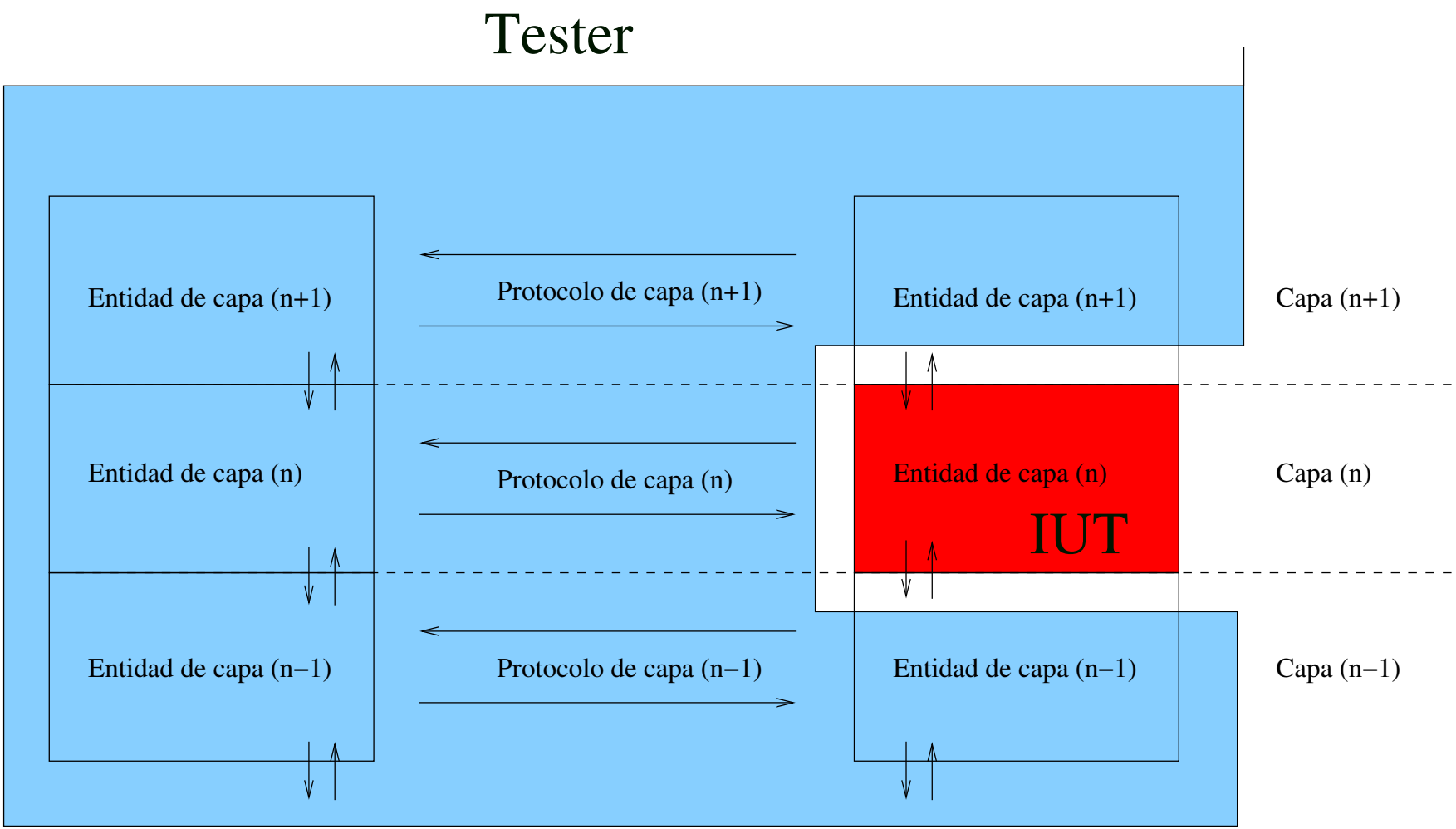
jiio 2008

Vista orientada a protocolos y capas



jiio 2008

Pruebas de una entidad de capa (n)



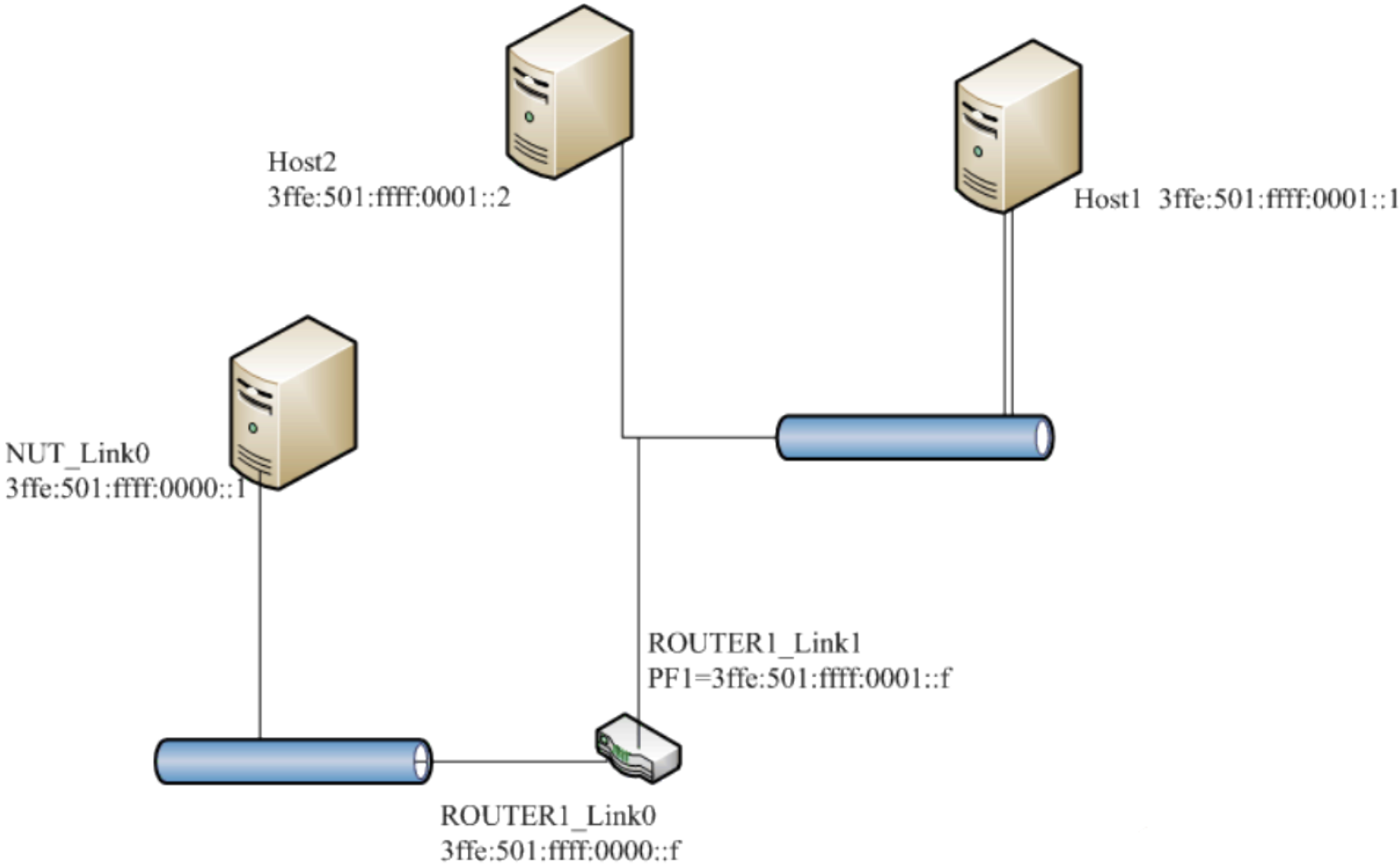
jiio 2008

Metodología y herramientas de prueba del v6RL

- Basado en PERL + FreeBSD
- En desarrollo desde 1998
- Objetos PERL para modelar y procesar todas las capas
- Es consecuencia de la mala separación de capas de TCP/IP
- Es *simple* de extender, pero muy complejo para alcanzar un nivel equivalente
- Coherente dentro de la suite IPv6... ¿Hasta cuándo extenderlo?

jiio 2008

Ejemplo de caso de prueba



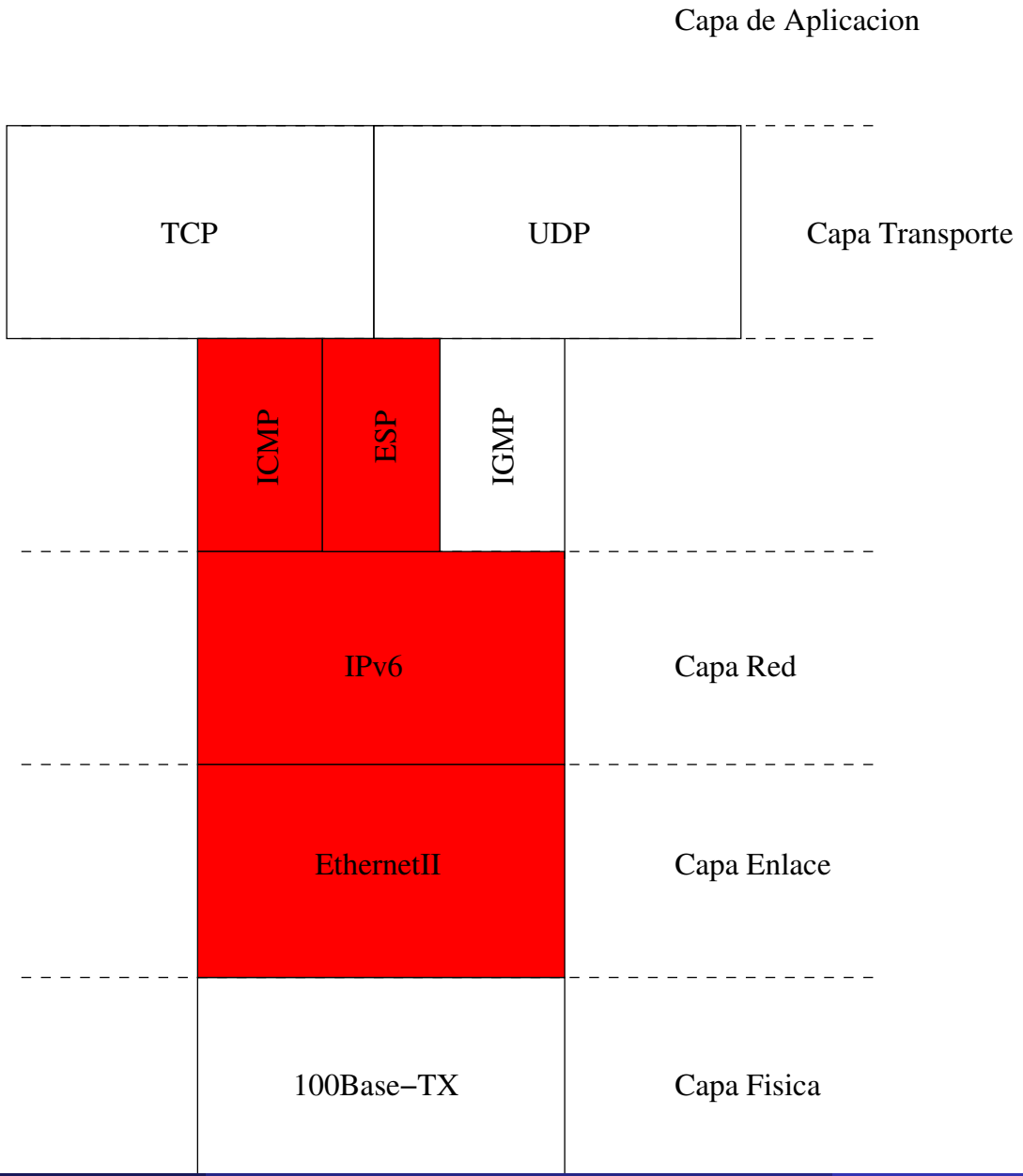
jiio 2008

Ejecución del caso de prueba

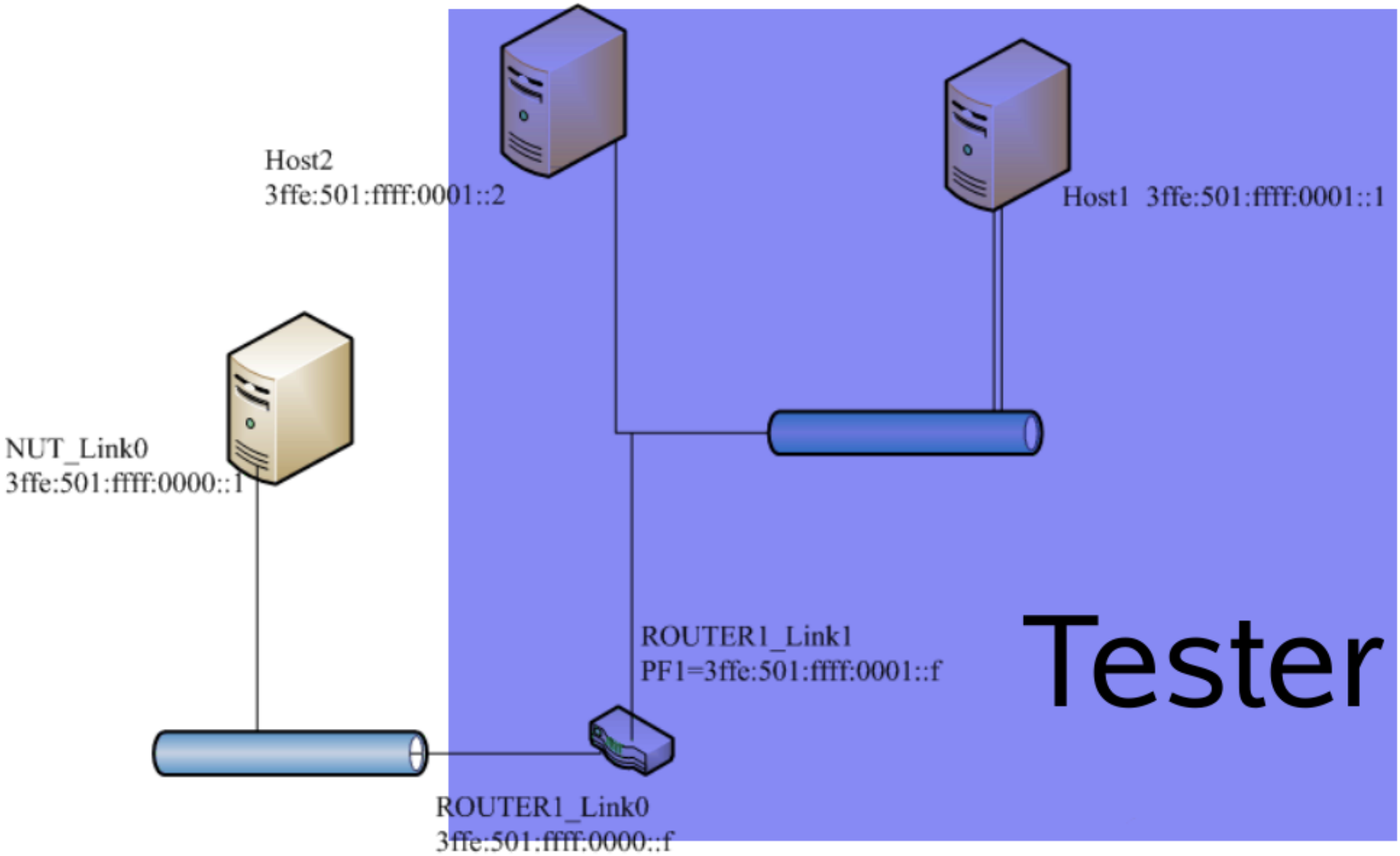
- Se configura un tunel IPsec entre el Router 1 y el NUT
- Se envia un mensaje ICMPv6 Echo Request desde el Host1 hasta el NUT por adentro del tunel
- Se debe recibir el mensaje ICMP Echo Reply a través del tunel
- Si todo funcionó de acuerdo a lo esperado, se emite el veredicto de conformidad

jiio 2008

Requerimiento de implementación de Tahi

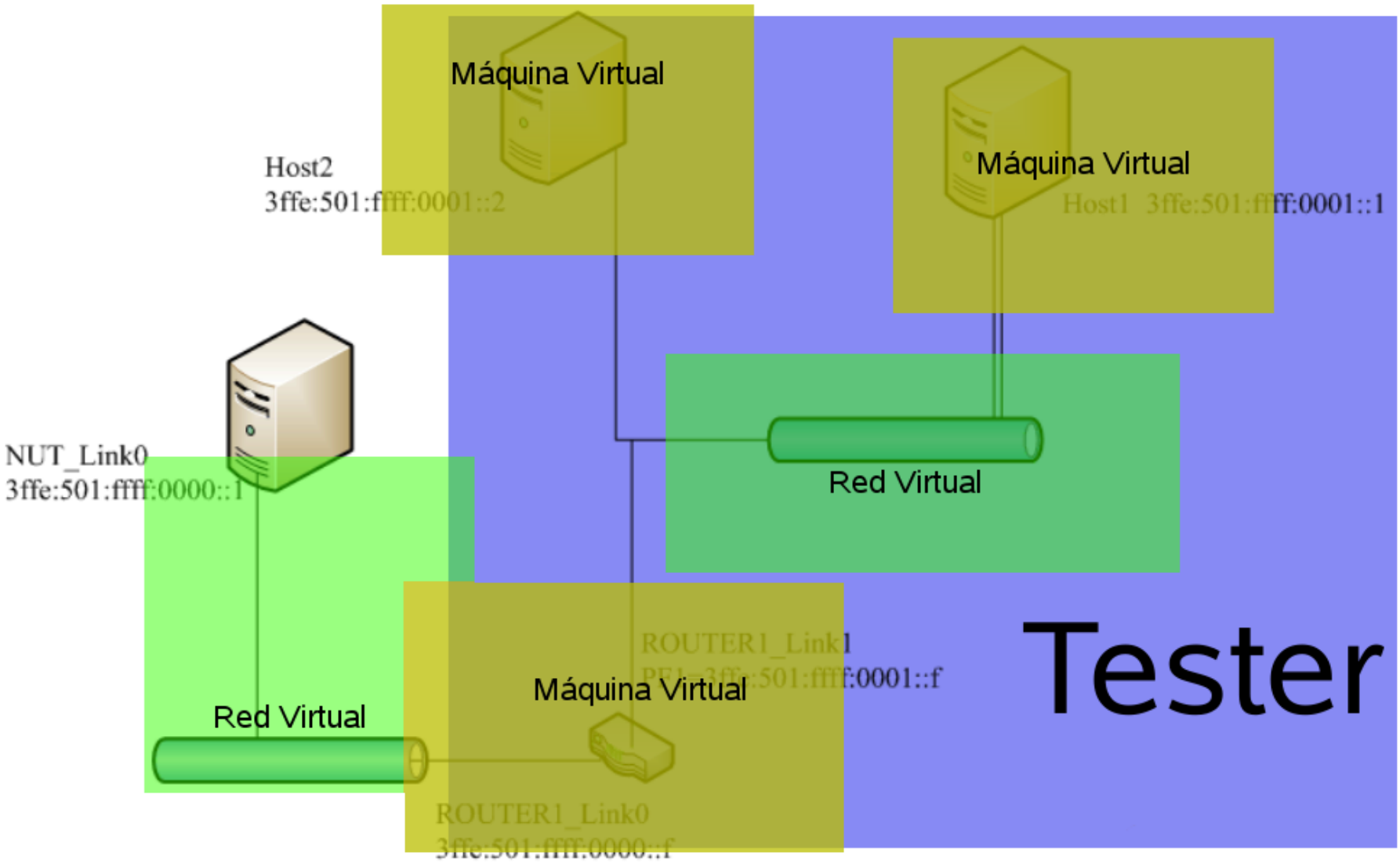


Arquitectura Tester Tahi



jiio 2008

Arquitectura Tester Propuesta



jiio 2008

Descripción de la arquitectura

- El proceso de routing lo hace un router (testeado)
- La transmisión y recepción la hace un stack IPv6 (testeado)
- Los dominios de colisiones se implementan utilizando VLANs
- El deploy del tester completo se realiza en un único host
- Exteriormente ambas soluciones involucran un NUT y un Tester
  - Los mensajes que intercambian coinciden
  - Solamente se modifica la forma en la que se sintetizan los mensajes

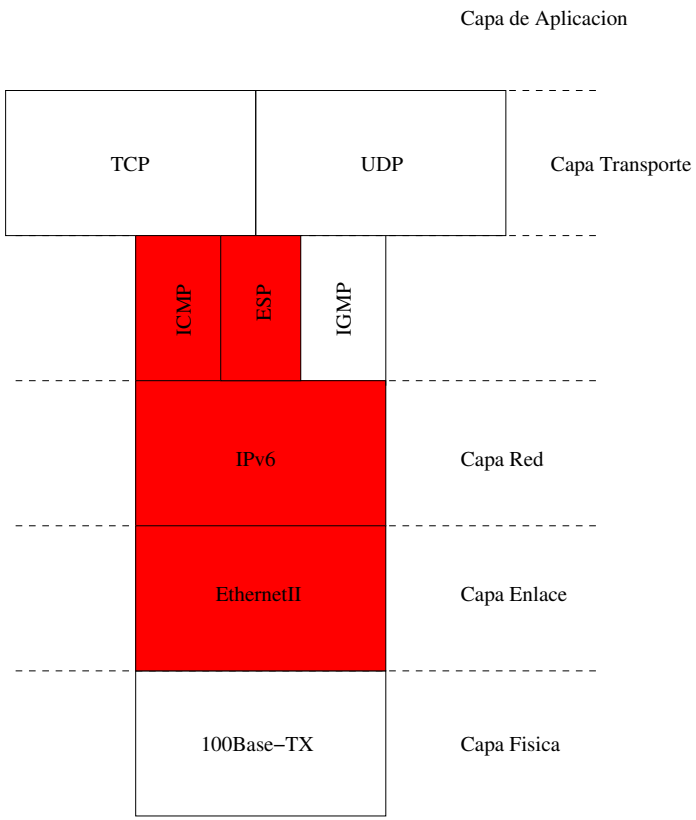
jiio 2008

Consideraciones metodológicas

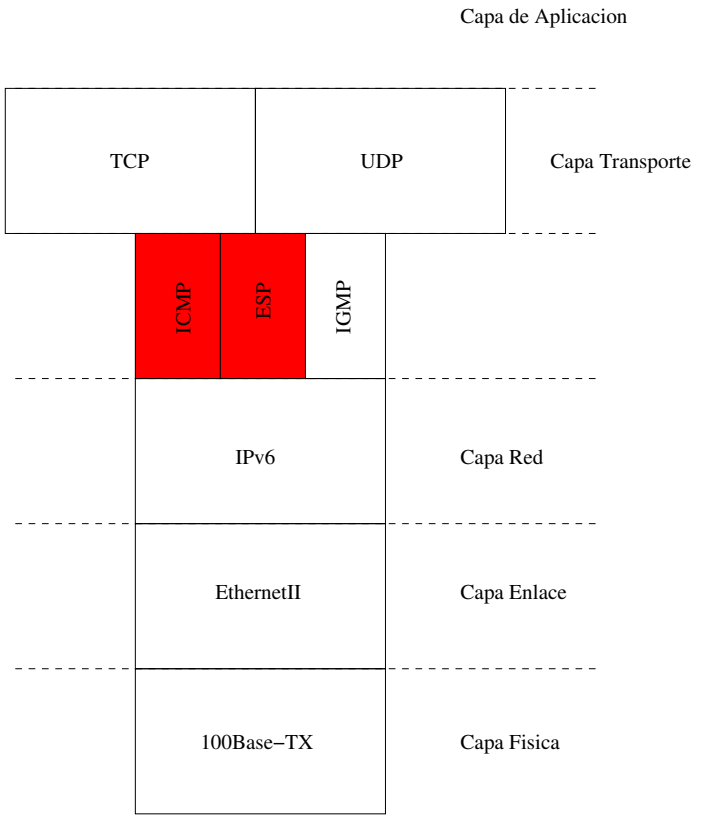
- La disciplina aplicada se denomina *testing indirecto*
- No es nueva, pero si lo es el nivel de automatismo permitido por la virtualización
- Tampoco es trivial su implementación, pues se requiere un manejo complejo de tecnologías de virtualización
- La implementación del caso de prueba es *más clara* pues solamente involucra el manejo de IPsec, mientras que la configuración de la topologa es solamente eso

jiio 2008

Comparación de los requerimientos de implementación



Desarrollo Tahi



Desarrollo metodología propuesta

jiio 2008

Resumen

- Trabajo de investigación conjunto entre INRIA-InCo
  - Un stage en Francia
  - Un proyecto de grado
- Los resultados observados validan empíricamente la metodología
- Por razones políticas el v6RL no acepta técnicas de virtualización para certificación
- Las técnicas utilizadas pueden ser utilizadas en otros ámbitos de forma confiable

jiio 2008

Conclusiones

- La virtualización es aplicable, y con buenos resultados, también para pruebas de conformidad
- Las técnicas de virtualización utilizadas son las mismas que en las pruebas de interoperabilidad, por lo que pueden ser reutilizadas
- La complejidad específica del manejo del protocolo se circunscribe al manejo específico de IPsec
- Los casos de prueba son manipulables por un experto en IPsec, sin la necesidad de un conocimiento profundo de toda la suite IPv6
- Se aportó en la formación de grado y posgrado a nivel nacional

jiio 2008

Gracias por su tiempo....

¿Preguntas?

jiio 2008