MINISTERIO
DE CIENCIA
Y TECNOLOGÍA

Este proyecto ha sido
cofinanciado por PROFIT

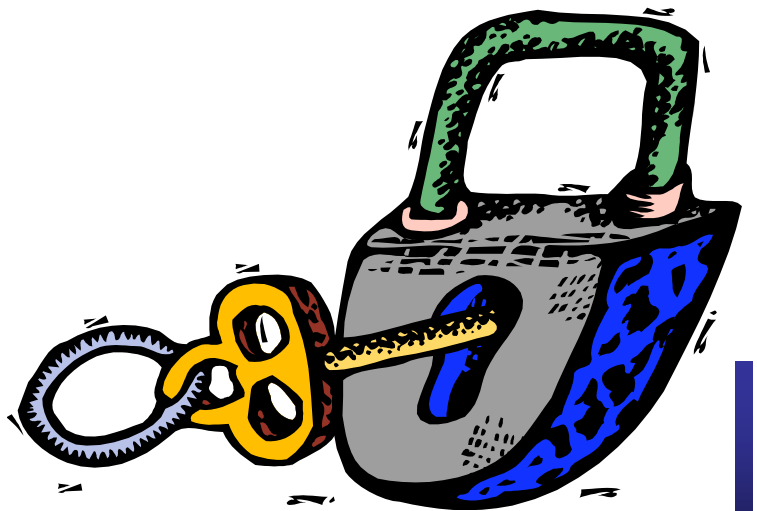
IPv6 y la respuesta a la muerte de Alice

Antonio F. Gómez Skarmeta
Dept. Ingeniería de la Información y las Comunicaciones, Universidad de Murcia

Fecha 18 | 02 | 2004

IPv6 y la respuesta a la muerte de Alice

Antonio F. Gomez Skarmeta
skarmeta@dif.um.es>
Universidad de Murcia (UMU)



www.6sos.org

Agenda

- La Muerte de Alice
- Componentes de la Seguridad
- Astrid y Bernard
- Conclusiones

www.6sos.org

La Muerte de Alice

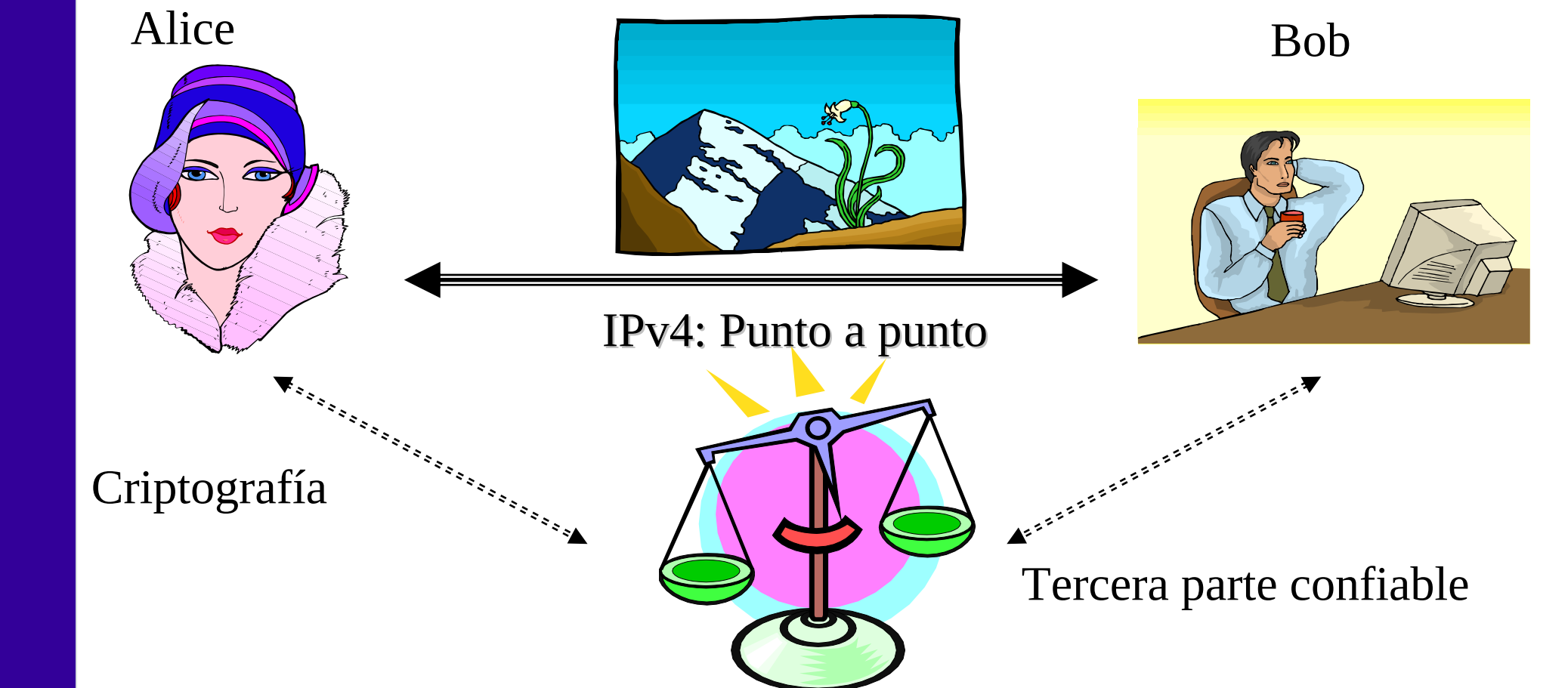
- Un acertijo legal:
- Bob dispara a Alice, buscando matarla, pero sólo la hiere en un brazo. Una ambulancia la lleva al hospital más cercano donde se ve expuesta a una enfermera con escarlatina. Alice contrate la enfermedad y muere.

- Alice muere no por el acto de BoB, pero es Bob culpable de su muerte?

Soluciones Seguridad Clásicas

www.6sos.org

- PKIs, Certificates (X509), SSL, IPSec, Firewalls
- Modelos de Securidad basados en criptografía
  - Alice y Bob comparten un secreto
    - Dicho secreto les permite cifrar y autenticar las comunicaciones



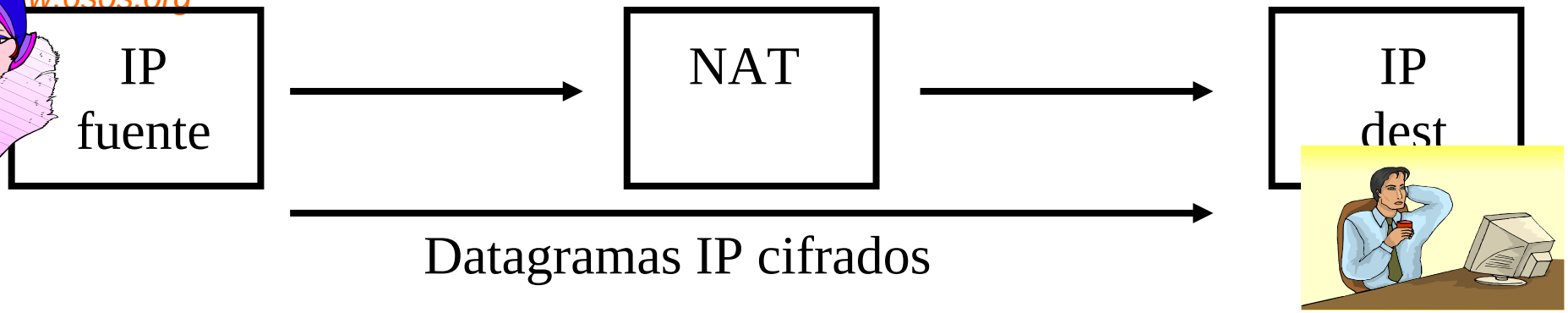
www.6sos.org

Actores en Internet

- Alice: Seguridad E2E
- Bob: Ataques seguridad
- Ambulancia: IPv4
- Enfermera: NATs

- Consecuencia: Internet Actual
  - Con el IPv4 no hay seguridad completa en Internet.
  - La desaparición del NATs facilitará la seguridad E2E
  - Necesidad de varios niveles de seguridad

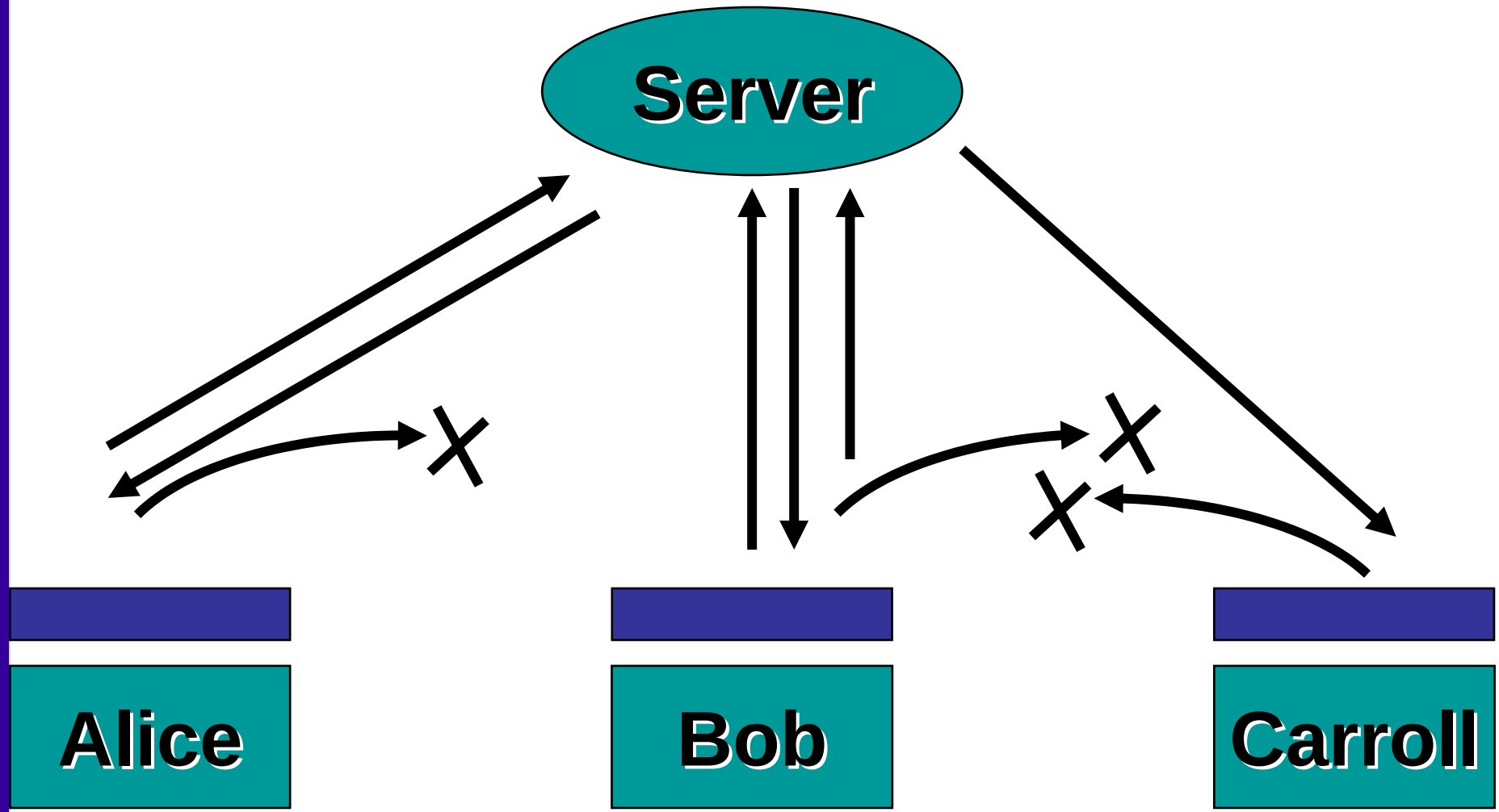
Seguridad y los NATs



- NATs introducen un problema en las comunicaciones seguras E2E
  - NATs requieren tener conocimiento de los puerto TCP y esto puede estar cifrado por IPsec
  - Además NATs requiren cambiar puertos y direcciones origen, alterando por tanto el contenido e invalidando la firma digital

www.6sos.org

En un mundo de NATs, NAPSTER no puede funcionar!



www.6sos.org

IPv6 y la seguridad

- IPv6 restituye el modelo E2E
- IPv6 integra la seguridad como parte del protocolo y no como un añadido
- IPv6 soporte direccionamiento de dispositivos finales

¿Alice puede resucitar?

www.6sos.org

Agenda

- La Muerte de Alice
- **Componentes de la Seguridad**
- Astrid y Bernard
- Conclusiones

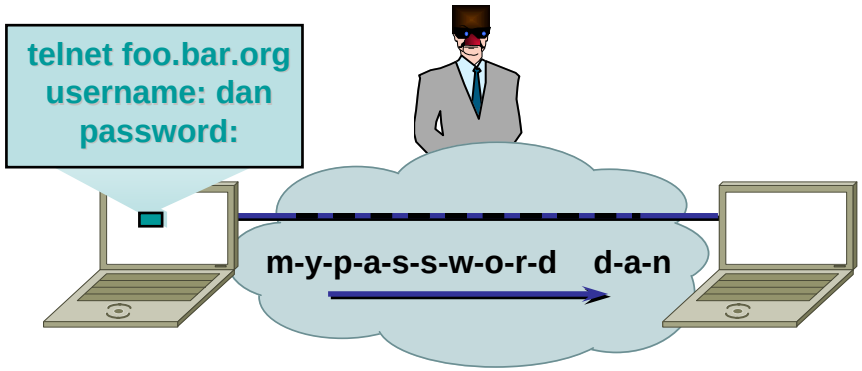
www.6sos.org

Seguridad en Internet

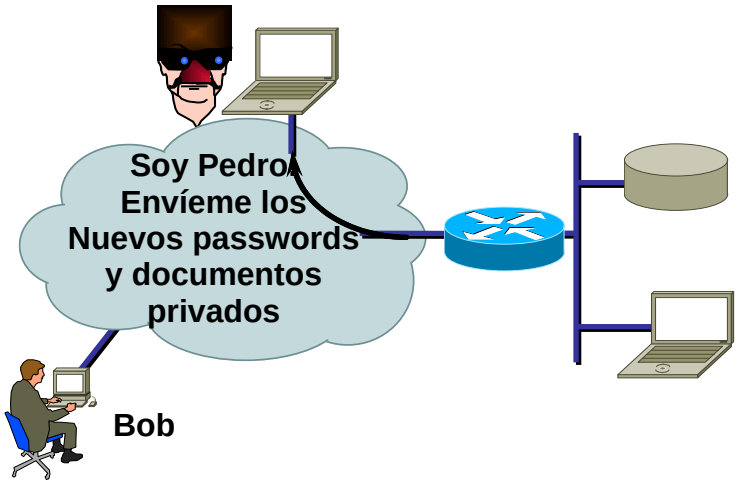
- La **Seguridad** es uno de los **puntos débiles** de Internet
- La **Seguridad** en Internet se ve **amenazada**, entre otras cosas, por:
  - intrusiones físicas o lógicas en uno o más de los elementos de la comunicación.
  - enmascaramiento (“spoofing”) de la identidad que permite accesos no autorizados, ciber-delincuencia, fraudes en la facturación, ataques con virus,...
  - violación de la confidencialidad de las comunicaciones, datos de los usuarios, métodos de pago,...
  - denegación de servicio, repudio, manipulación de información por agentes de intermediación,...
  - violación de los Derechos de Propiedad Intelectual (música, vídeos,..)

www.6sos.org

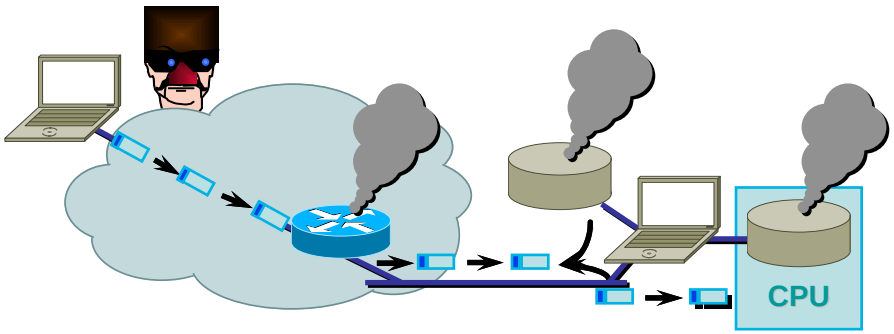
¿A que tipo de seguridad nos estamos refiriendo?



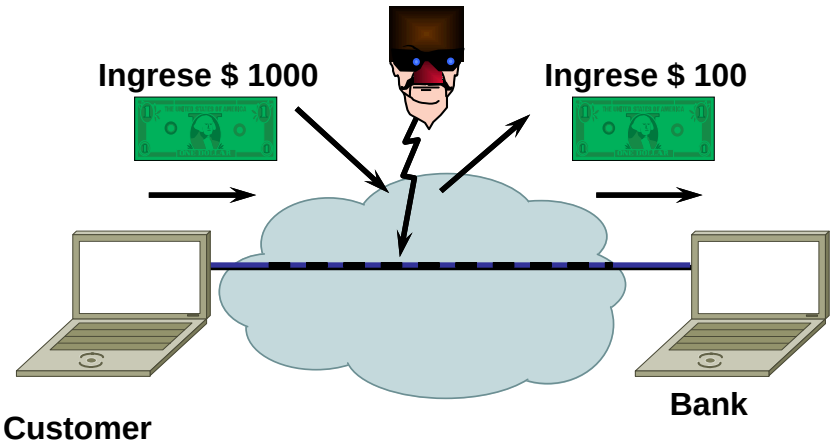
Confidencialidad



autenticación



Denegación de servicio



Integridad

www.6sos.org

Seguridad en Internet (II)

- La **Seguridad** en Internet no es posible sin el concurso de:
  - operadores de redes públicas y privadas
  - proveedores de acceso a Internet
  - proveedores de servicios
  - proveedores de contenidos
  - usuarios finales
  - fabricantes de equipos.
- La Seguridad precisa **infraestructura adicional** y **nuevos agentes** (ej. Trusted Third Party) ⇨ No está claro quién cubre el coste.
- La consecución de la **Seguridad** precisa **medidas** de 4 tipos:
  - legales
  - técnicas
  - económicas
  - de información
- Las direcciones IP deberían tratarse como datos personales
  - Estar sujetas a la legislación de protección vigente

www.6sos.org

Aspectos técnicos de la Seguridad en Internet

- Las normas técnicas asociadas a la Seguridad en Internet son:
  - **IPSec** (autenticación + encriptación) **-** Seguridad Extremo a Extremo
  - **Identidad Digital** (identificación) – Gestión de Identidad

- La **Identidad Digital** puede implementarse en IPv4 y en IPv6,
  - Ya se han empezado a crear autoridades de certificación
    - Certificado del Ministerio de Hacienda es un primer paso

- La norma **IPSec** está incluida (es obligatoria) en el protocolo IPv6
  - Puede añadirse a IPv4 usando direcciones públicas
    - Se añade como parche o software adicional
    - Es incompatible con dispositivos NAT

- La implementación de **IPSec** requiere **elementos adicionales** a la propia Internet cuya implantación involucra múltiples agentes
  - Se precisa una ***revisión de los modelos de negocio***. Esto está retrasando su disponibilidad

www.6sos.org

Identidad digital

- Garantiza digitalmente la identidad del usuario, y le da capacidad para firmar documentos electrónicos.
- Es el documento digital público que acredita la auténtica personalidad de su titular, constituyendo el justificante completo de la identidad de la persona.
- Servirá para acreditar y autenticar los accesos en la red, servicios y en general en todo punto que necesite control.
- Basado en claves públicas permite a las entidades comunicantes establecer conexiones seguras para soportar autenticación y confidencialidad

www.6sos.org

Posible Confianza Electrónica

- **Confidencialidad**
  - cifrado
- **Autenticación**
  - Certificados
- **Integridad**
  - Firma Digital
- **No Repudio**
  - Certificado y Firma Digital

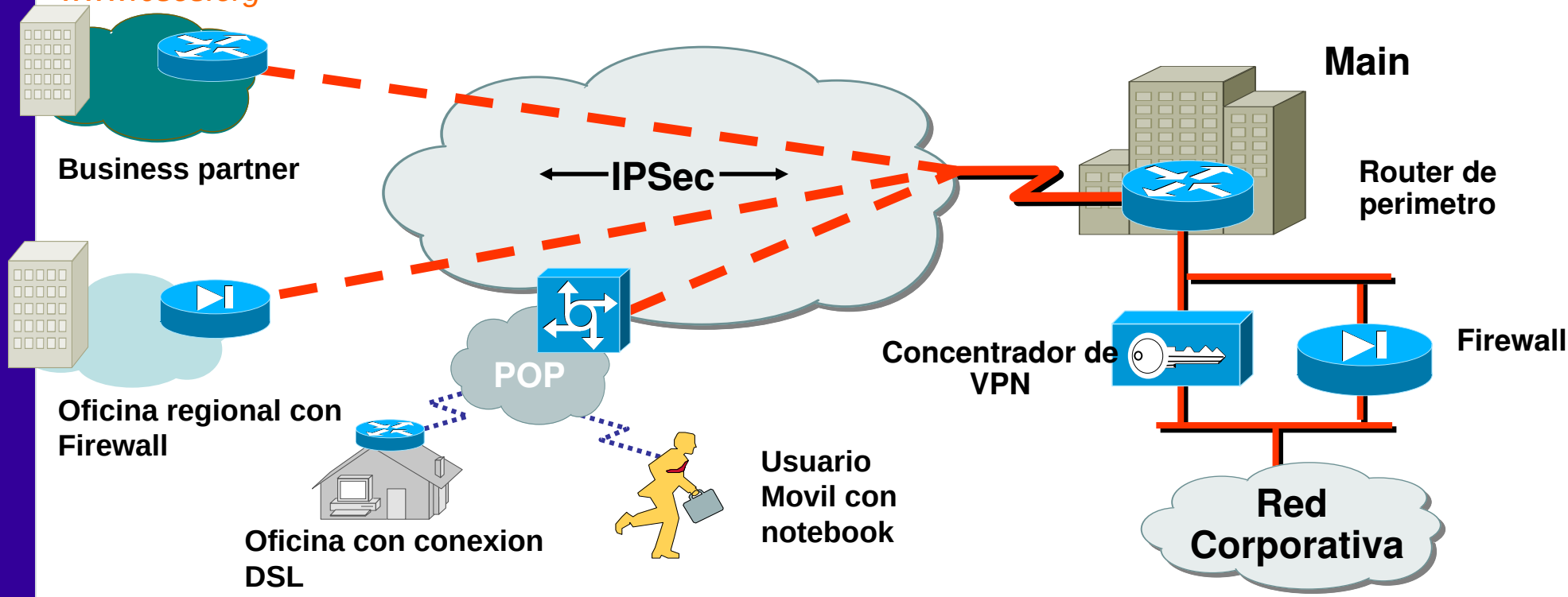
www.6sos.org

¿Qué es IPsec?

- Autenticación y cifrado a nivel de red
- Estandar abierto para proporcionar comunicaciones privadas y seguras
- Obligatorio en implementaciones IPv6
- Ofrece una solución flexible y basada en estándares para implementar una política de seguridad en toda una red
- Ventajas:
  - Estándar para privacidad, integridad y autenticación para comercio en la red
  - Se implementa de forma transparente en la infraestructura de red
  - Ofrece seguridad extremo a extremo incluyendo a routers, firewalls, PCs y servidores

www.6sos.org

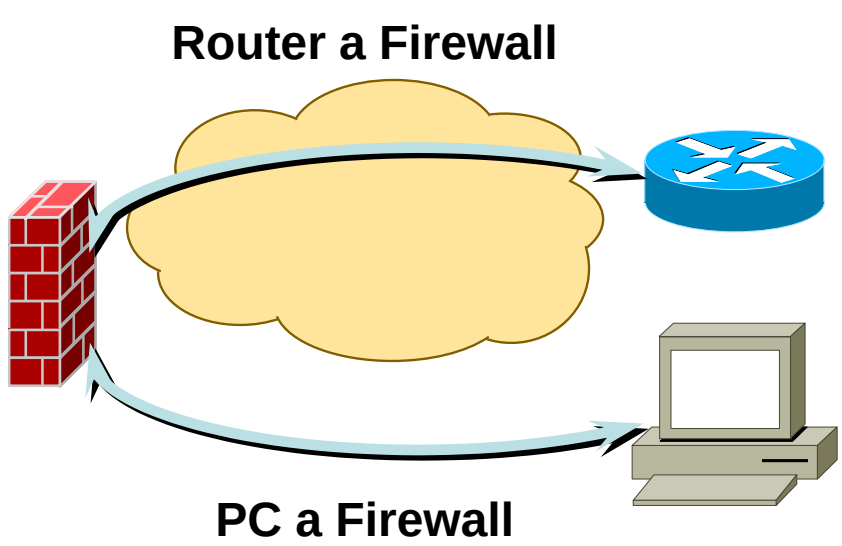
¿Qué es IPSec?

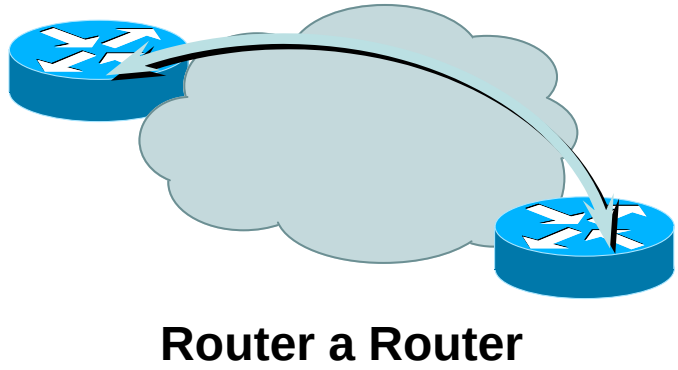


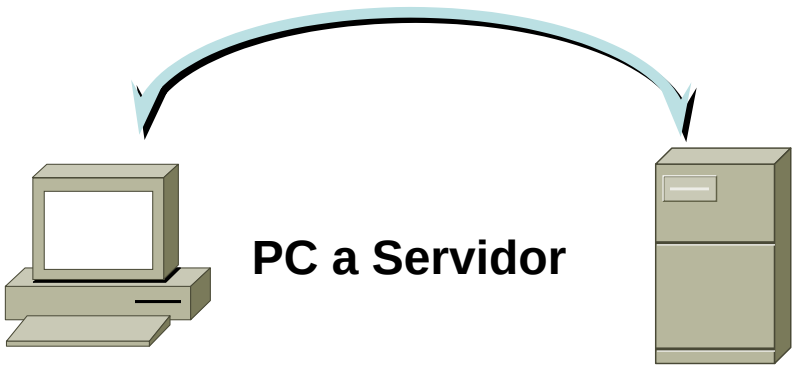
- Standard del IETF que permite comunicaciones encriptadas entre dos entes
  - Estandar abierto que permite asegurar transmisines de datos
  - Conjunto de estandares que permiten asegurar la confidencialidad, integridad y verificación de origen de los datos

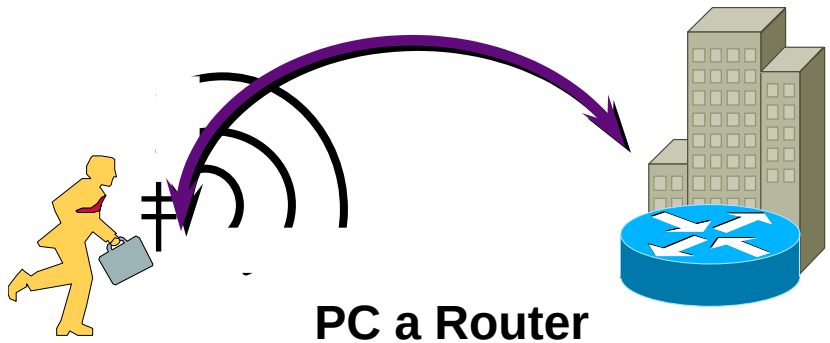
www.6sos.org

Aplicabilidad en IPsec



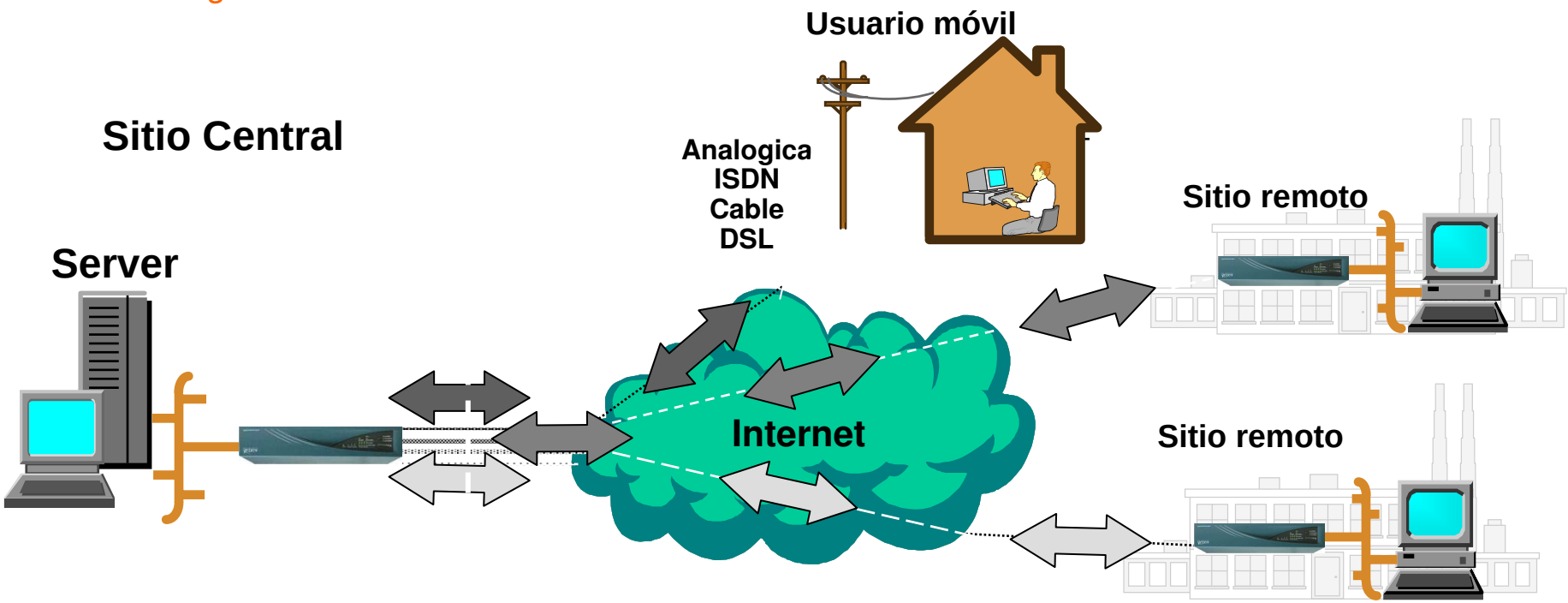






www.6sos.org

Definición de VPN



– Virtual Private Network (VPN). Conexión encriptada entre redes privadas usando una red pública como Internet

www.6sos.org

Agenda

- La Muerte de Alice
- Componentes de la Seguridad
- **Astrid y Bernard**
- Conclusiones

www.6sos.org

Gestión Seguridad

Nuevos paradigmas: Nacen Astrid y Bernard

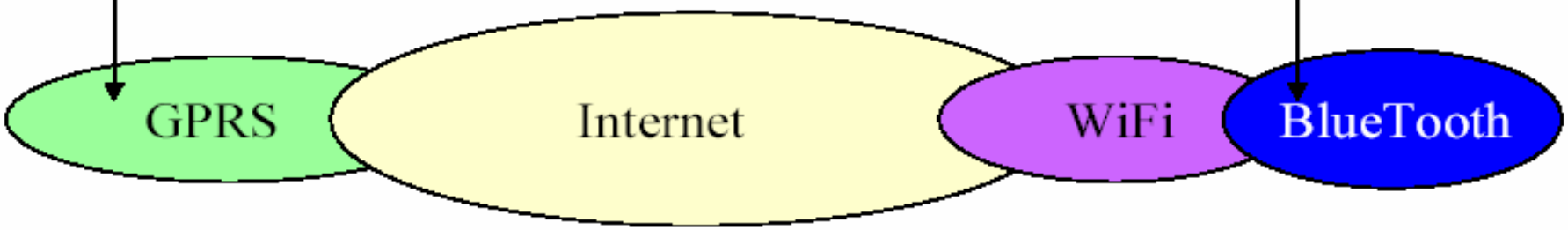
www.6sos.org

Nuevo retos en Seguridad

Astrid

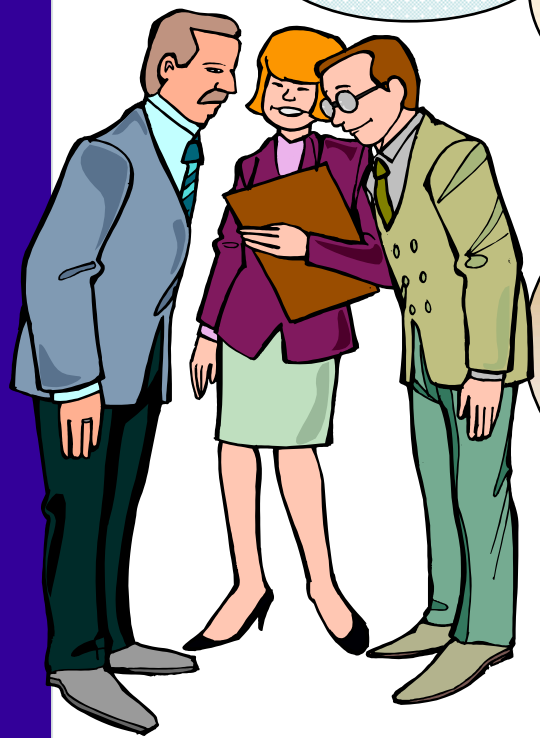
Bernard

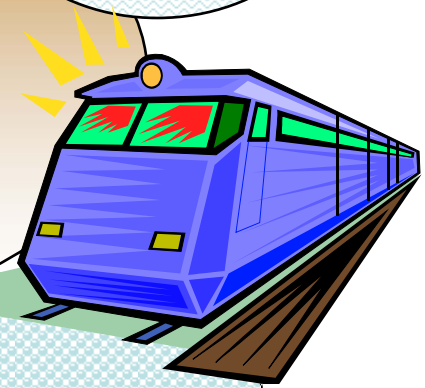
Identity
Authentication
Audit
Access control
Data protection
Trust management



www.6sos.org

Versatilidad Redes de Acceso Heterogeneidad, Global roaming, QoS, Servicios Valor Añadido





Bluetooth

Ad hoc

Access / Intermediation

IEEE802.11

IPv6

Core Network

UMTS

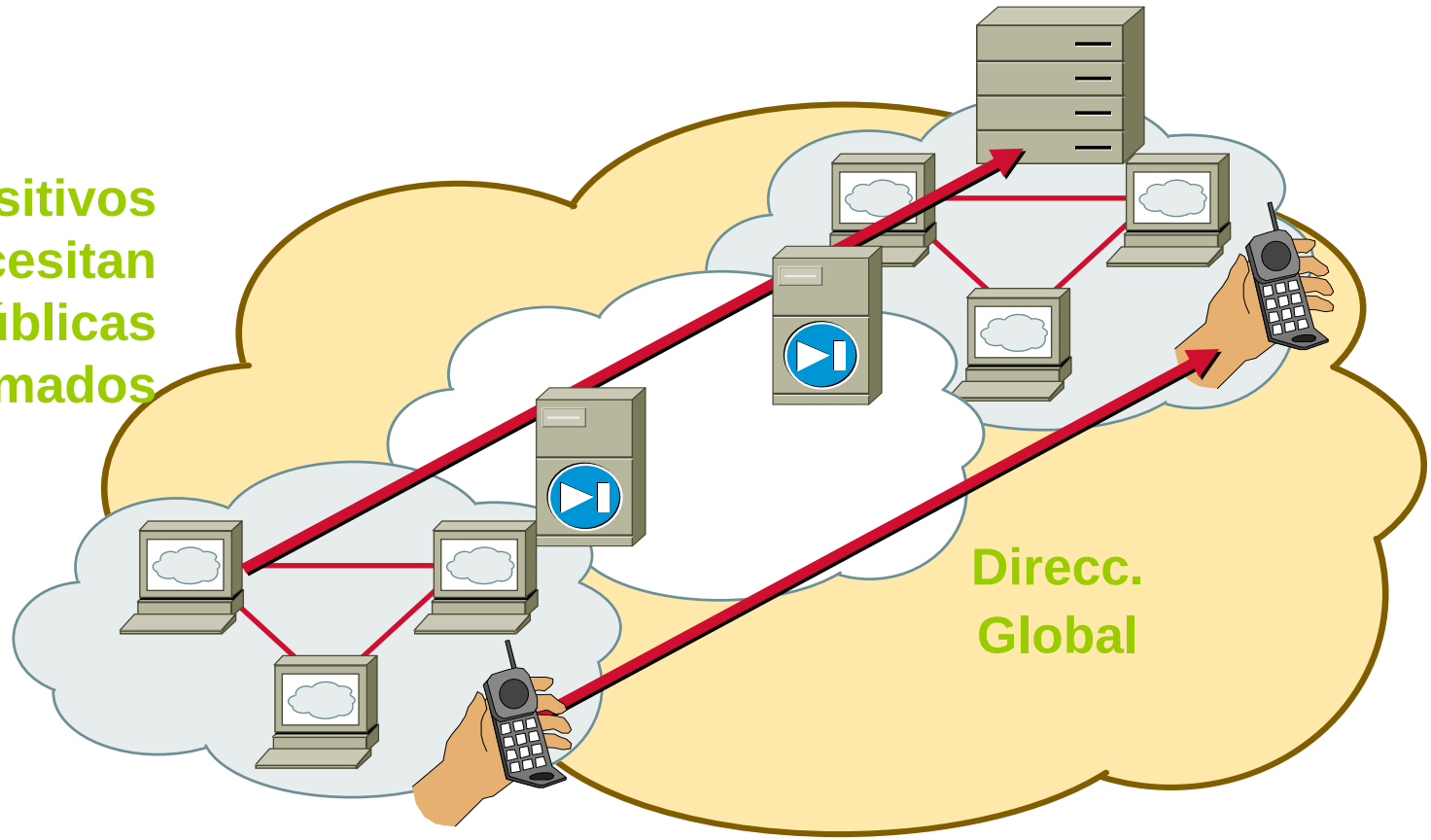
www.6sos.org

Vuelta al modelo End-to-End

Nuevas tecnologías/servicios para los usuarios

'Always-on'—Cable, DSL, Ethernet@home, Wireless,...

Los dispositivos always-on necesitan direcciones públicas cuando son llamados



www.6sos.org

Ventajas de IPv6

SEGURIDAD

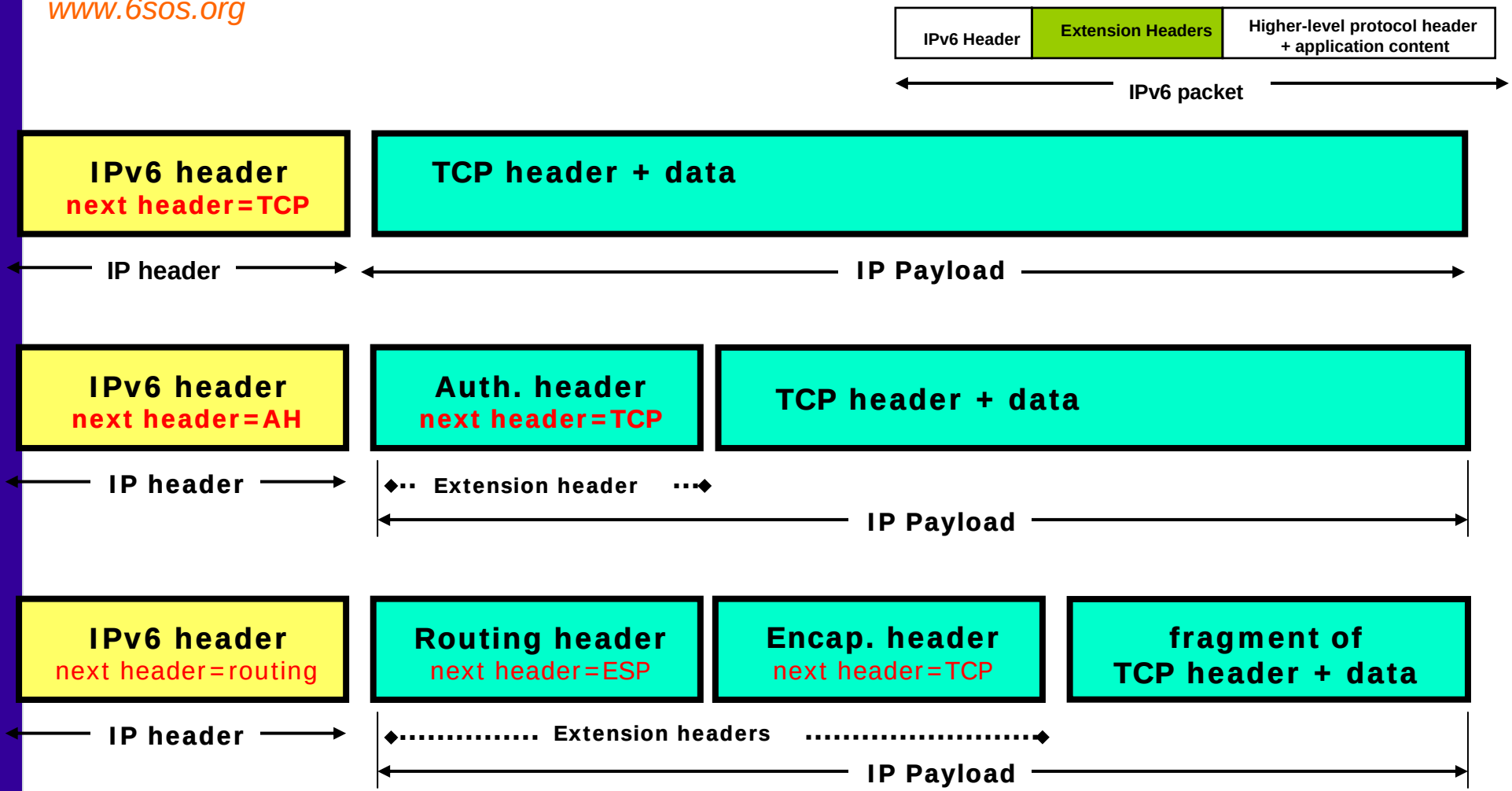
- IPsec es obligatorio en todos los nodos IPv6, por lo tanto al establecer una sesión IPv6 siempre es posible disponer de una conexión segura extremo a extremo.

- La autenticación de los comunicantes y el cifrado de los datos para protegerlos de otros terminales, posibilita la realización de transacciones seguras sobre IPv6.

- La disponibilidad de direcciones IPv6 suficientes, permite evitar el problema de seguridad que supone la traducción de direcciones que hacen los NATs, y permite identificar biunívocamente a un nodo.

www.6sos.org

Cabeceras de extensión



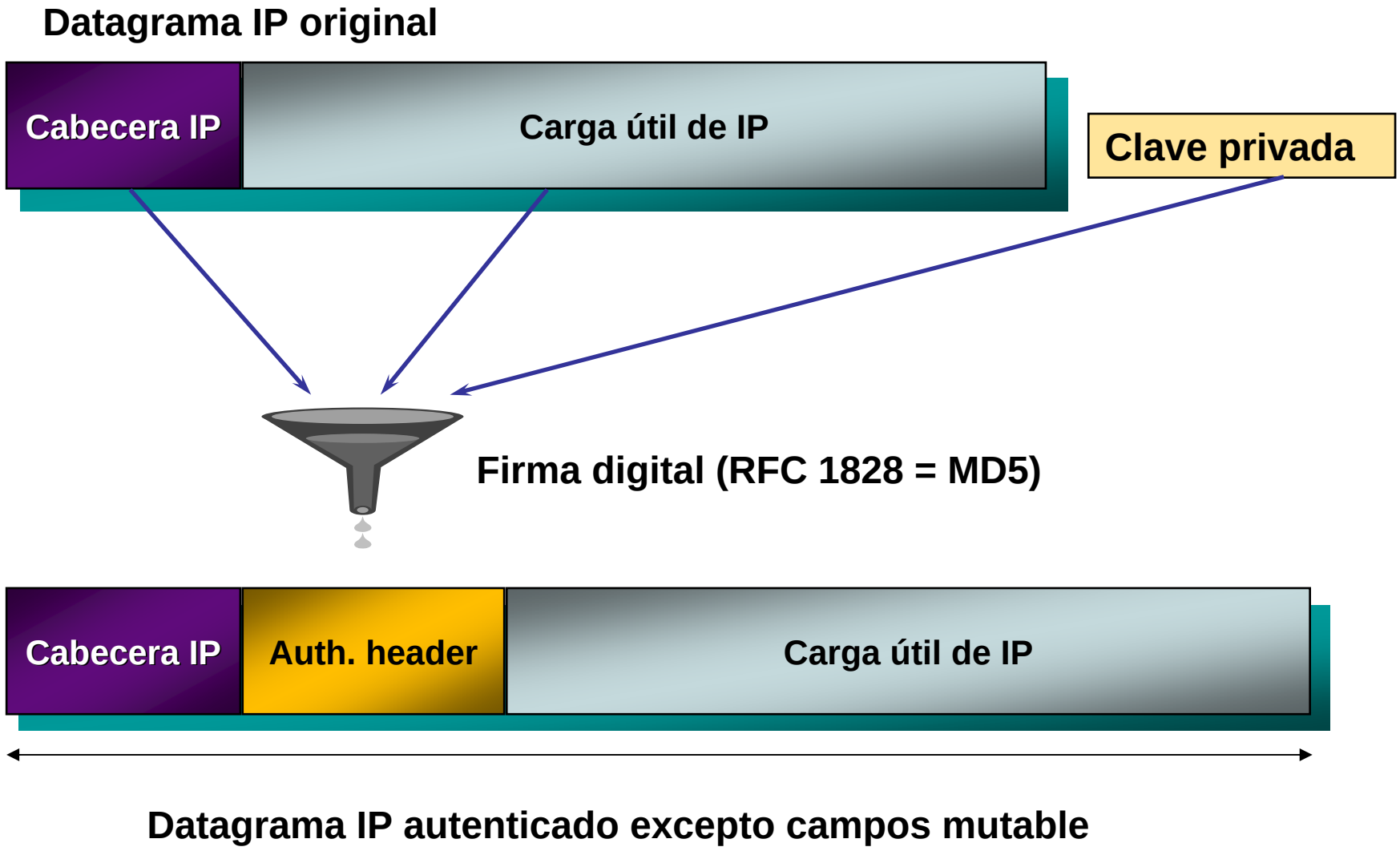
www.6sos.org

IPSec

- Authentication Header (AH)
  - Se utiliza para obtener integridad y autenticación
    - Opcionalmente protege contra reenvío
  - Autentica los campos del datagrama, salvo los mutables de IPv4
    - » Type of Service (TOS)
    - » Flags
    - » Fragment Offset
    - Time to Live (TTL)
    - Header Checksum
    - Sólo autentica los mutables en el modo túnel
- Encapsulating Security Payload (ESP)
  - Se utiliza para integridad, autenticación, y cifrado
    - Opcionalmente protege contra reenvío
    - Servicios no orientados a conexión
    - Selección opcional de servicios
      - » Al menos uno debe de estar activado

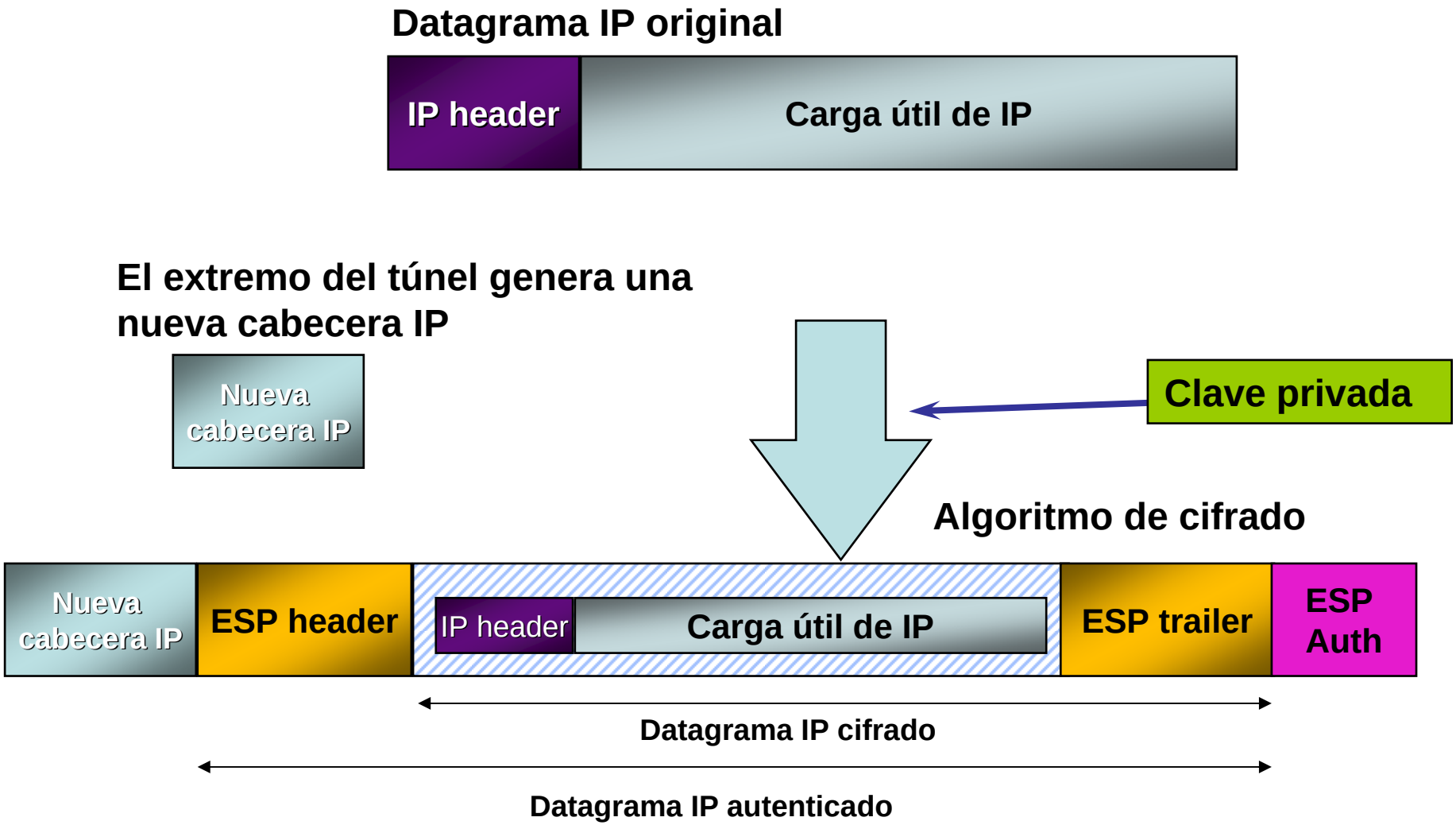
www.6sos.org

IPsec Authentication Header (AH)



www.6sos.org

IPsec ESP Tunnel



www.6sos.org

Ventajas de IPv6

Identificación y Movilidad

- IPv6 permite además plantearse nuevos paradigmas de seguridad.
- La visión de espacios de seguridad dependiendo de contextos y de contenidos.
- Posibilidad de crear diferentes identificaciones (multihoming) del usuario en función del tipo de seguridad, y en función de donde este y con quien quiera comunicar

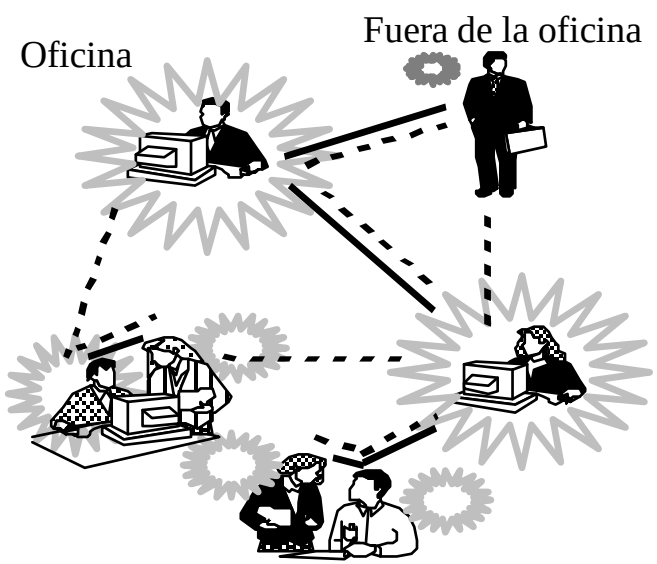
Movilidad e Infoesferas

Evolución de los espacios: regular & inteligentes

www.6sos.org

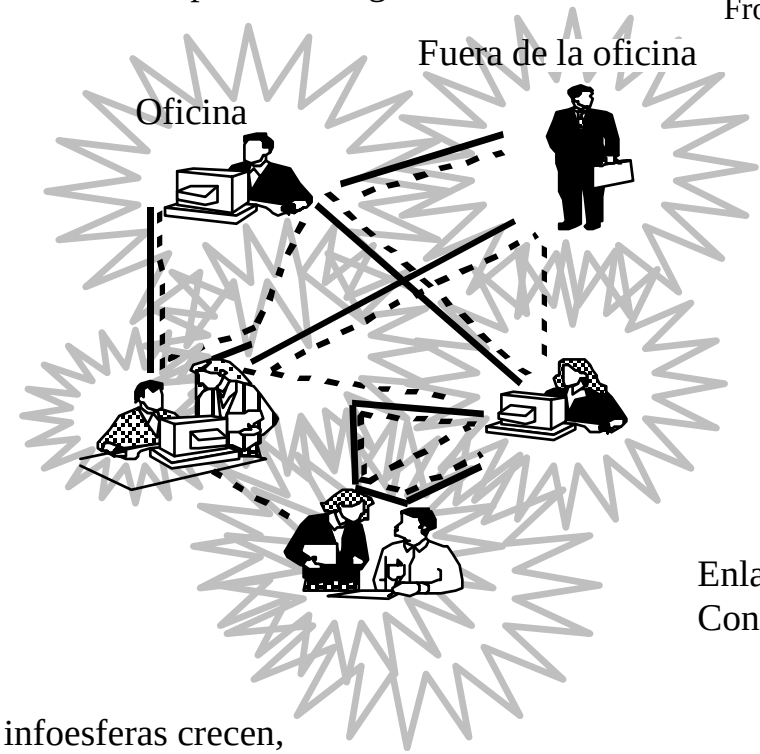
PAN-Bluetooth-WLan-UMTS-Internet

Espacio Regular



Espacio Inteligentes

From K. M. Carley CMU



Enlaces permanentes
Con IPv6

Al tiempo que los espacios se hacen más inteligentes las infoesferas crecen, afectando a las personas

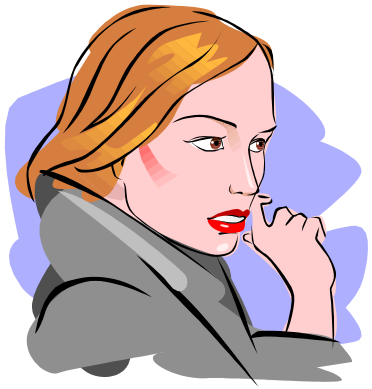
Infoesferas : círculos
interacciones : líneas oscuras
Redes conocimiento : líneas discontinuas

www.6sos.org

Nuevos Objetivos de la Seguridad

En casa

En trabajo



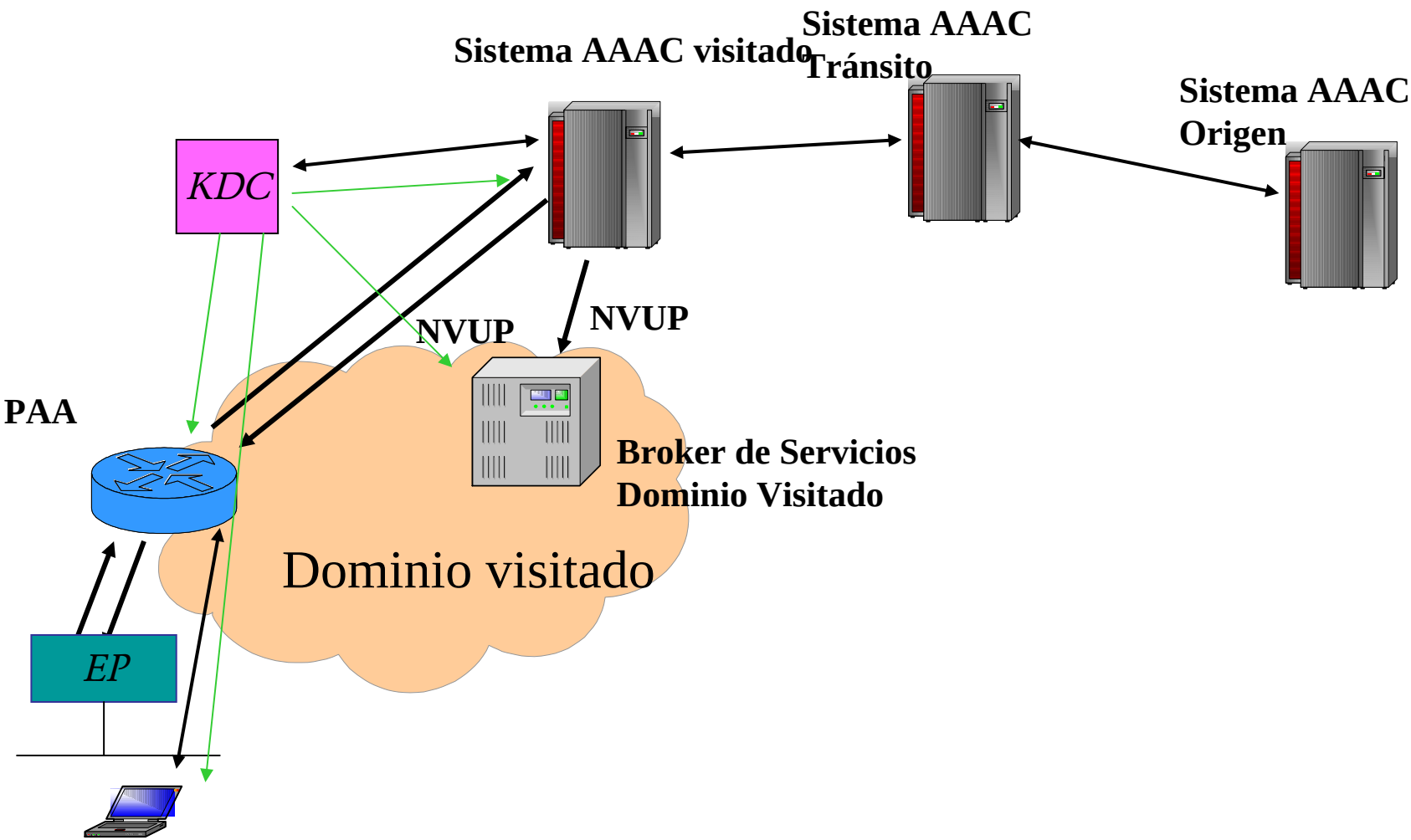
Privacidad

Disponibilidad

No observabilidad e Integridad

www.6sos.org

Componentes de Autenticación



www.6sos.org

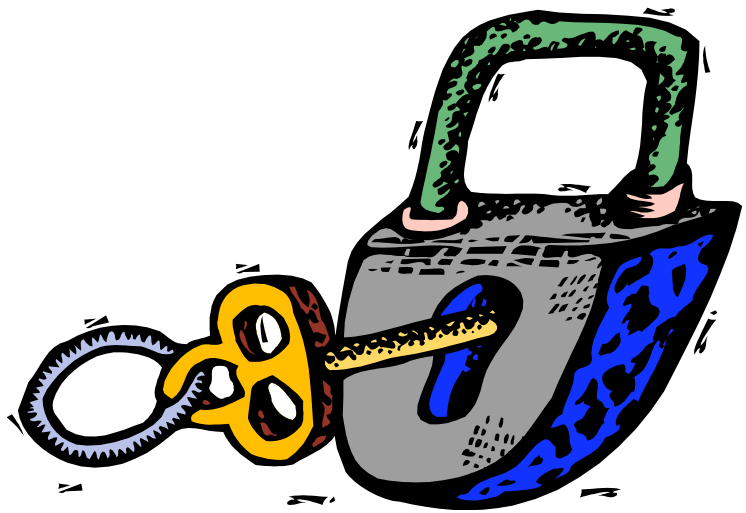
Agenda

- La Muerte de Alice
- Componentes de la Seguridad
- Astrid y Bernard
- **Conclusiones**

www.6sos.org

Conclusiones (1/2)

- Especificar políticas conpatibles con el contenido, el contenedor y con el marco
- Establecer sistemas de seguridad configurables, plurales y orientados al contexto
- Diseñar nuevos protocolos/marcos de seguridad
- Introducir seguridad en un mundo abierto y heterogéneo



www.6sos.org

Conclusiones (2/2)

- IPv6 crea el marco adecuado para establecer nuevos modelos de seguridad
- Integra de forma natural y como parte del protocolo la seguridad
- Soporta necesidades de direcciones para la vuelta al modelo E2E

No debemos pensar que todo esta resuelto pero se ha avanzado

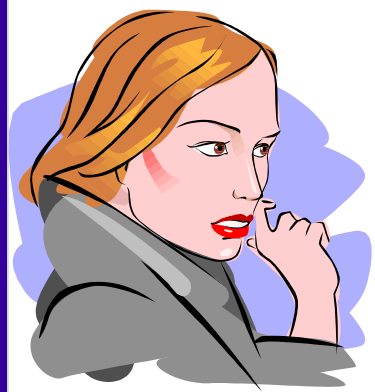
www.6sos.org

SI a comunicar NO a ...

Alice

Bernard

Astrid



Seguridad

Bob