Protocolos seguros

Recordatorio Problemas

- Criptografía simétrica: Hay que acordar la clave.
- Criptografía asimétrica: Costosa.

Fundamentos

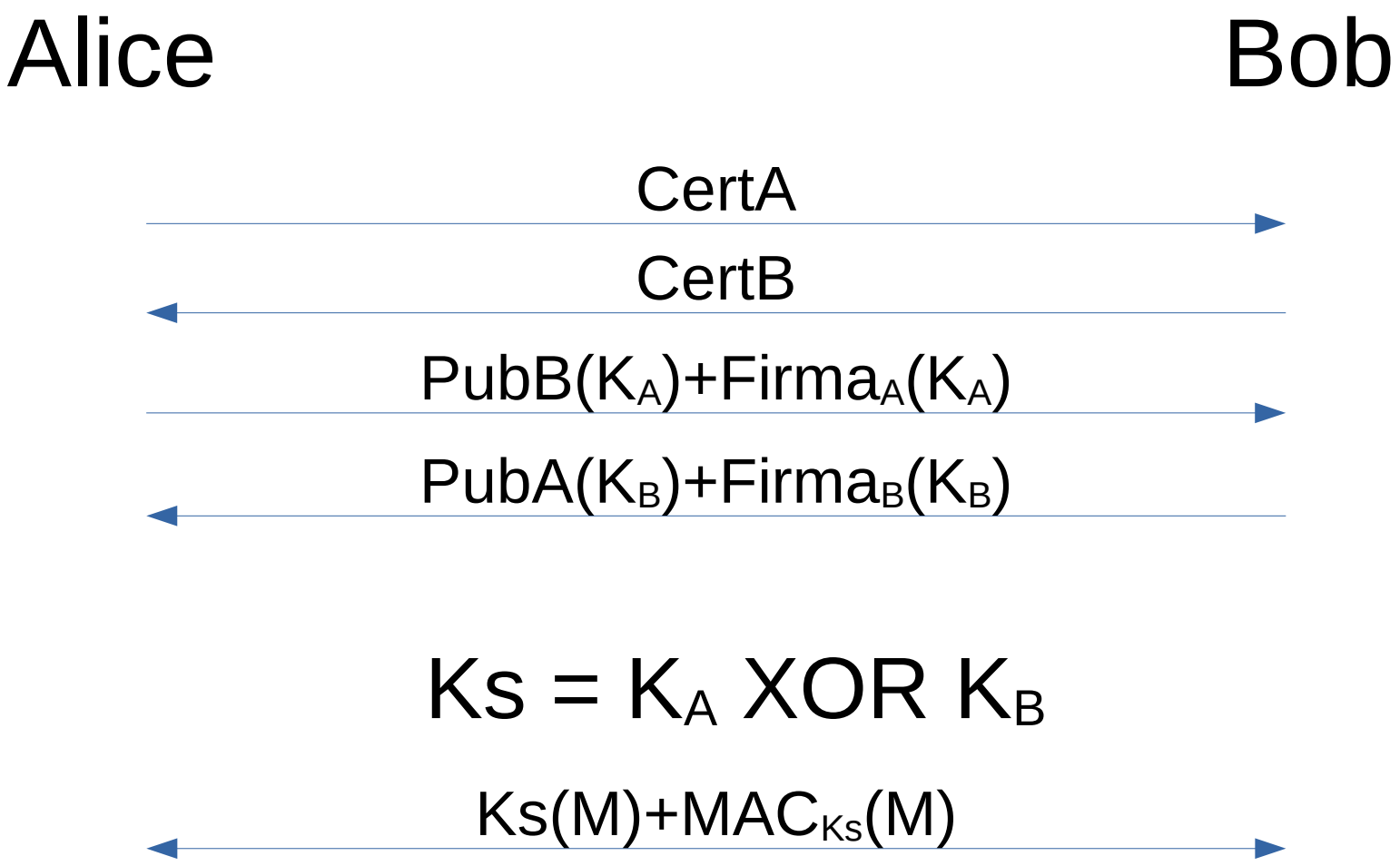
Alice

Bob

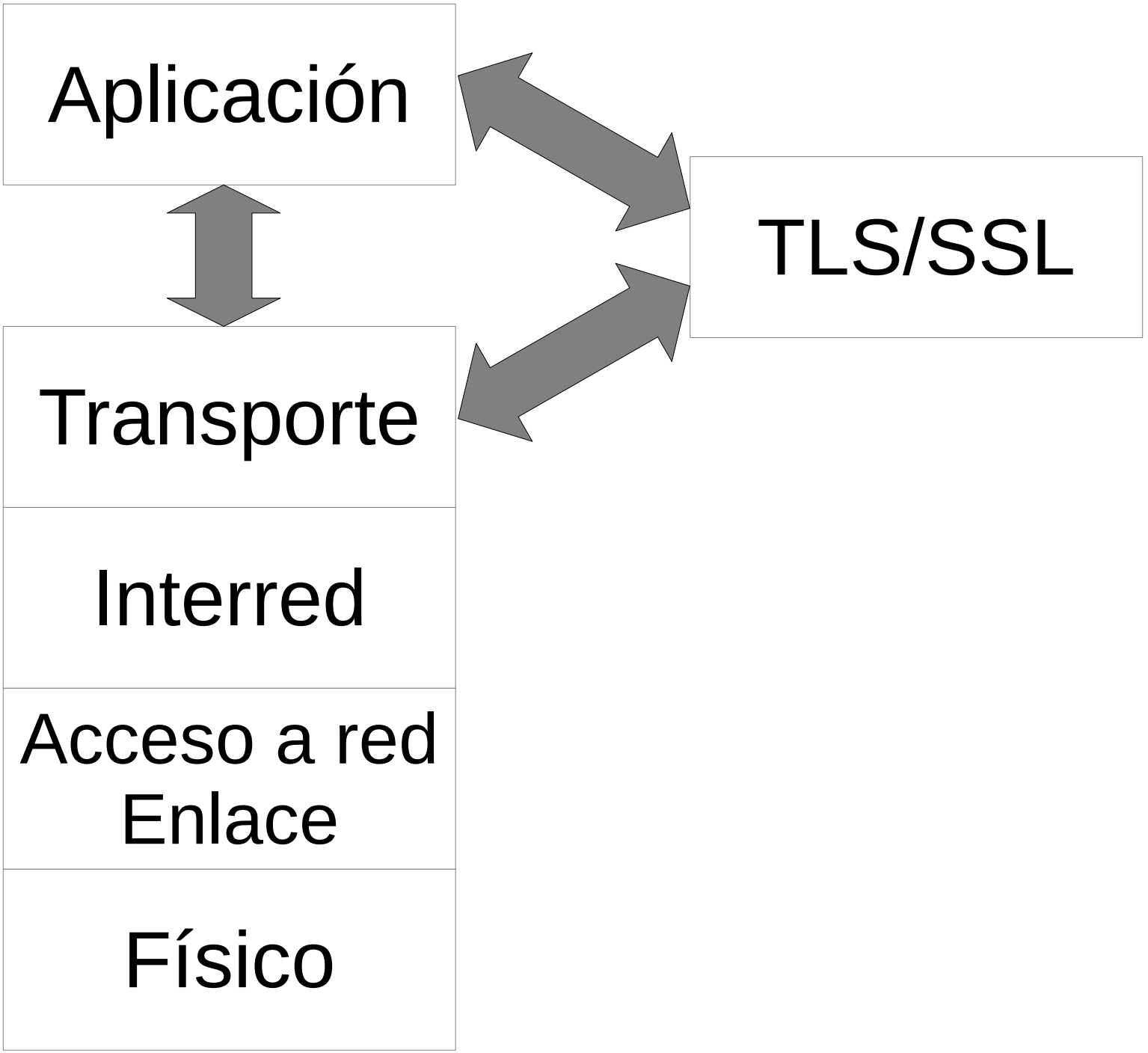
Acordar clave de sesión simétrica
usando criptografía asimétrica

Comunicarse
usando criptografía simétrica

Ejemplo


Alice
Bob
CertA
CertB
PubB(K_A)+Firma_A(K_A)
PubA(K_B)+Firma_B(K_B)
Ks = K_A XOR K_B
Ks(M)+MAC_Ks(M)

TLS/SSL


Aplicación
TLS/SSL
Transporte
Interred
Acceso a red
Enlace
Físico

Saludo TLS

- Acordar algoritmos
- Autenticar servidor (certificado)
- Acordar clave simétrica de sesión
- Opcionalmente, autenticar cliente (certificado).

IPSec

Características IPSec

Seguridad ofrecida:

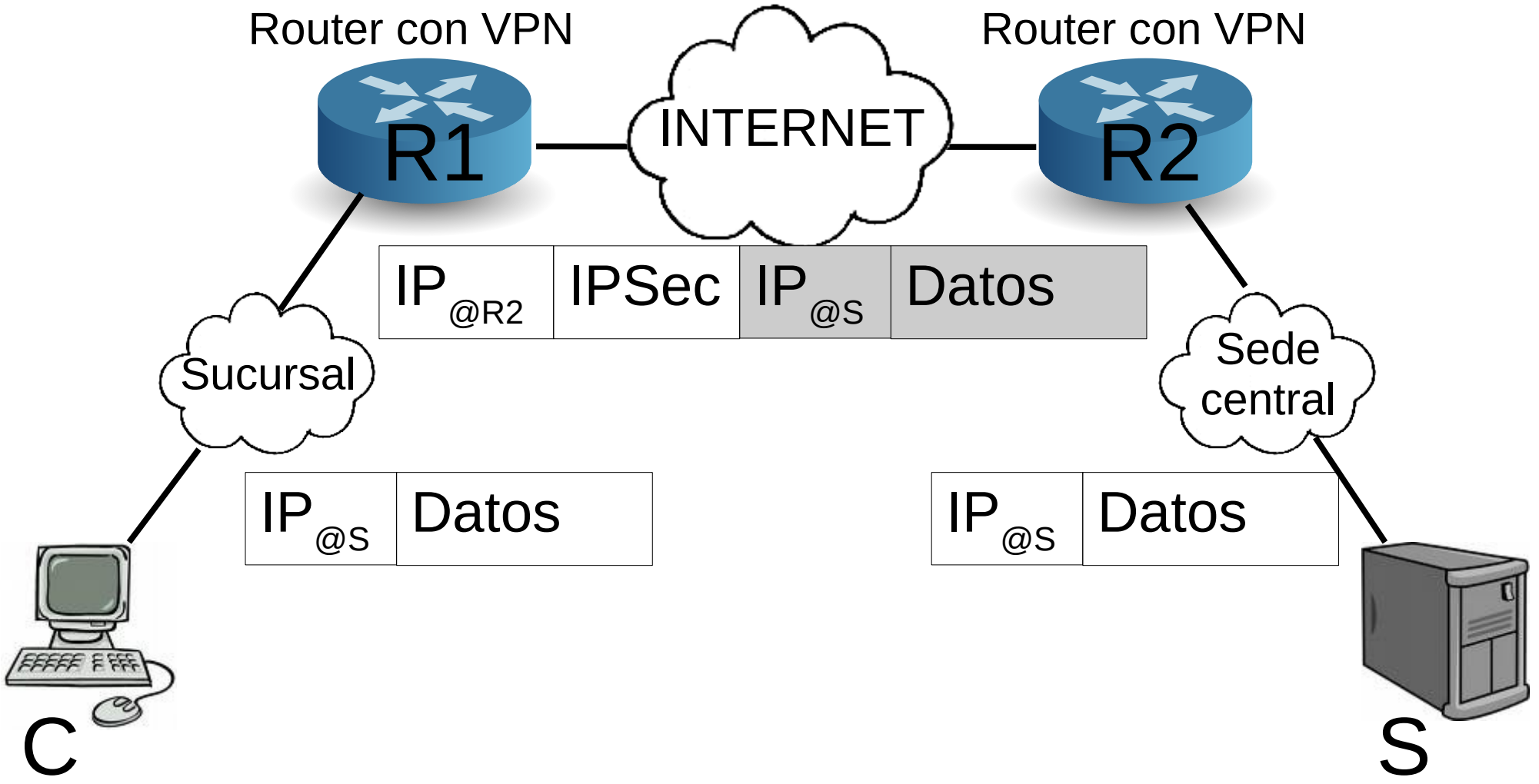
- AH: autenticación e integridad
- ESP: AH + confidencialidad

Parte cifrada:

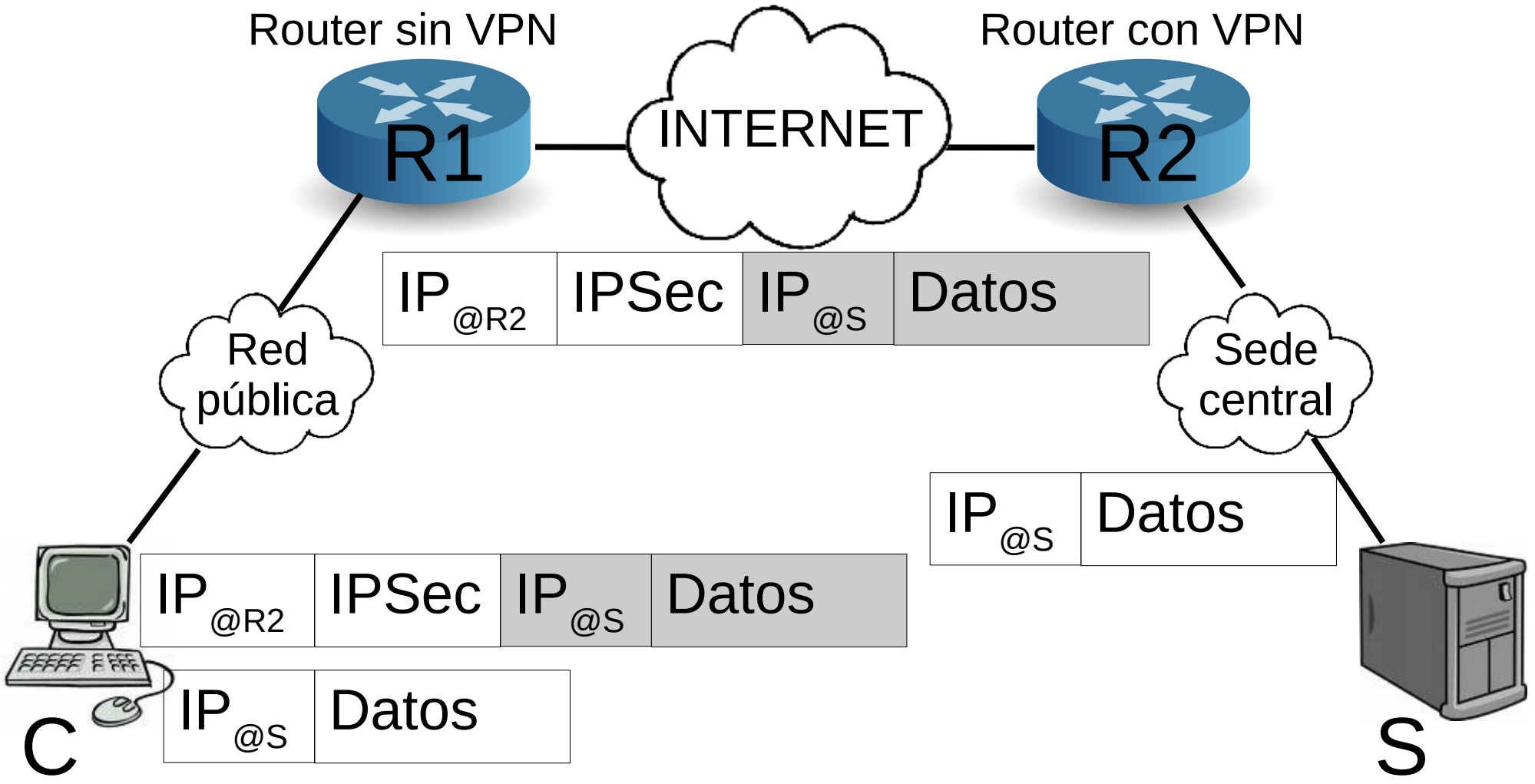
- Datos (payload): Transport
- Datagrama completo: Tunnel

VPN

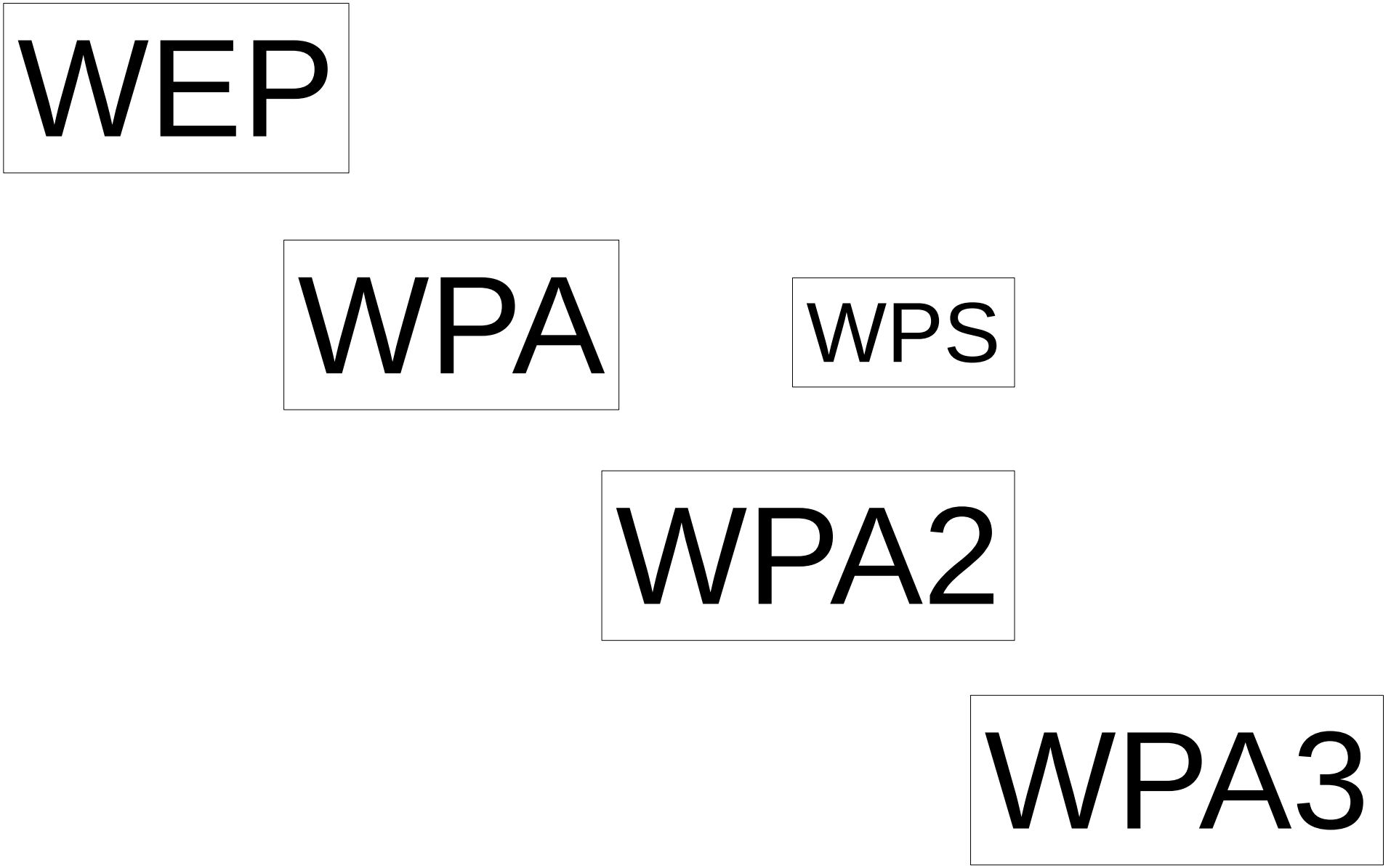
Sede a sede


Router con VPN
Router con VPN
R1
INTERNET
R2
IP@R2
IPSec
IP@S
Datos
Sucursal
Sede central
IP@S
Datos
IP@S
Datos
C
S

Dispositivo a sede



Wifi


WEP
WPA
WPS
WPA2
WPA3