

Internet infrastructure

Virtual Private Networking

Prof. dr. ir. André Mariën

Virtual Private Network

- Why VPN?
 - Use of network with insufficient protection
 - To provide communication on top of another, untrusted, communication network
- Supports one or more of the following:
 - Integrity
 - Authentication
 - Confidentiality

VPN uses

- Between organization entities
 - Maintain illusion of one network
 - Cost reduction compared to real private networks (leased lines)
- Between organization and individuals
 - Part of remote access solutions
 - “work as if in the office”
 - Risks:
 - physical security different (lower?)
 - social control different (absent?)

VPN uses: partner connections

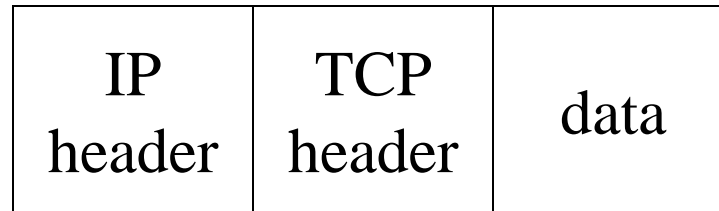
- Incoming:
 - Service companies
 - Maintenance
 - Access: high risk (management and monitoring activities, configurations)
- Commercial
 - Suppliers (delivery)
 - Customers (orders)
- Integrated processes
 - Industry standard solutions

IPsec

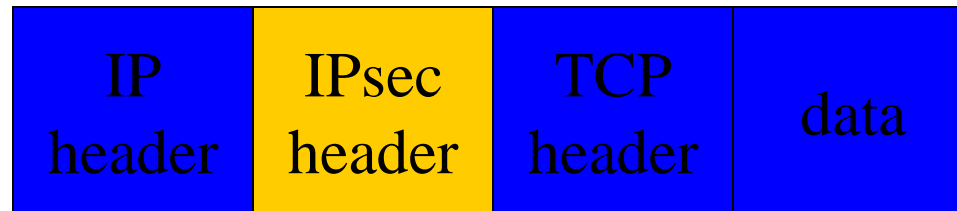
- Architecture: RFC 2401
- What is IPsec? Two protocols:
 - Authentication Header(AH): RFC 2402
 - Integrity and authentication
 - Encapsulating Security Payload (ESP) : RFC 2406
 - Integrity and confidentiality
- How does IPsec work? Two modes of operation:
 - transport mode: point-to-point
 - tunnel mode

Modes of operation

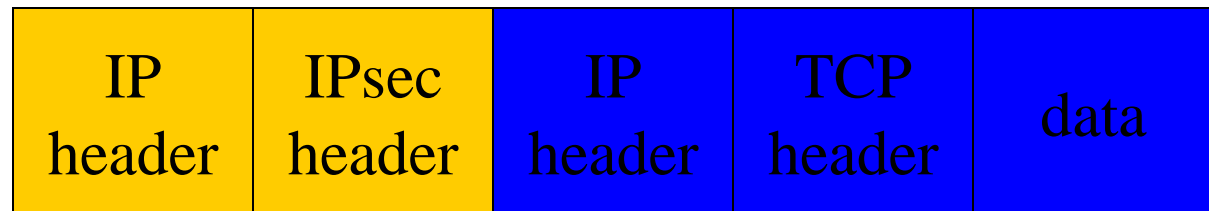
Normal
IP packet



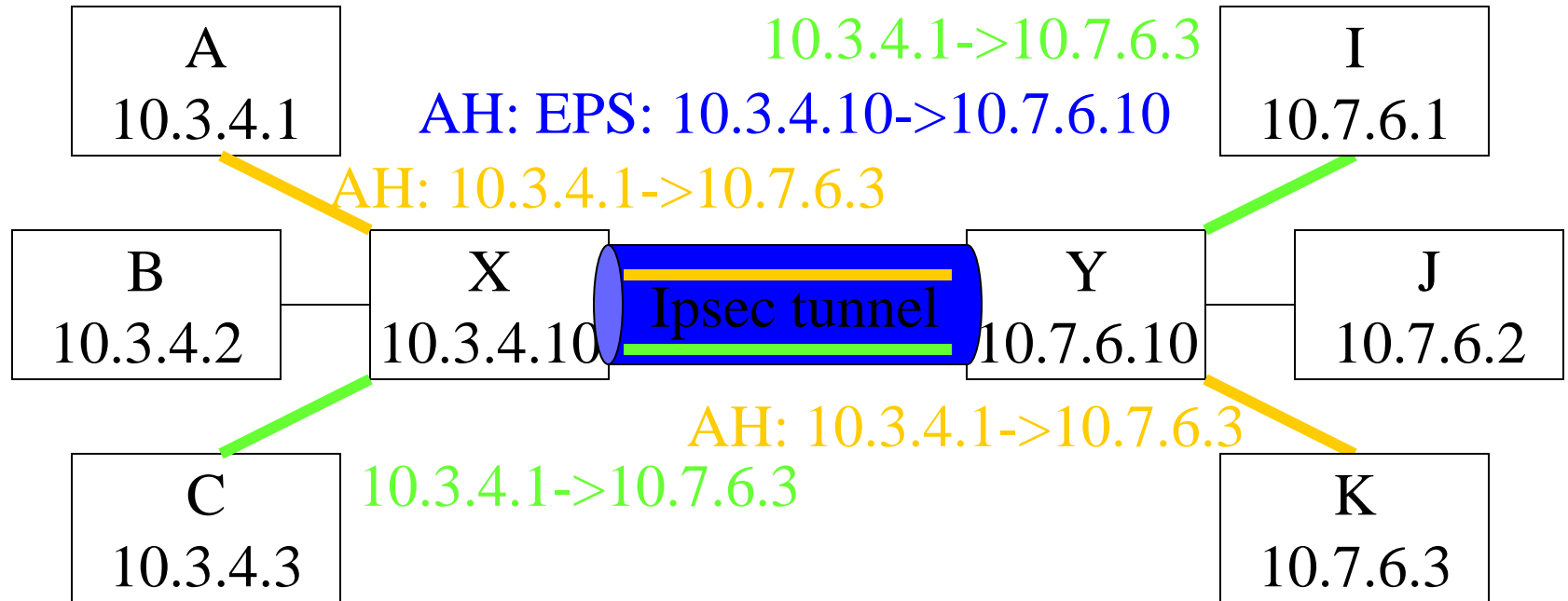
Transport mode
packet



Tunnel mode
packet



Modes of operation



A authenticates towards K (IPsec A & K)

X authenticates towards Y (IPsec X & Y)

X protects communication from 10.3.4.* to 10.7.6.* (Ipsec X & Y)

Security policy

- Defines security services for connections
- Starting point to negotiate the Security Associations
- Policy is defined by:
 - source & destination IP
 - DNS name
 - protocol
 - source & destination port (if applicable)

Security Association (SA)

- SA = communication parameter agreement
 - $SA_{out}(A) = SA_{in}(B)$
 - $SA_{in}(A) = SA_{out}(B)$
- ID: Security Parameter Index (SPI)
- Parameters: generic or protocol specific (AH/ESP)
- SA DataBase (SADB)
- SA management

Internet Key Exchange: IKE

- RFC 2409
- Diffie-Hellman key exchange
 - Exchange messages that allow both parties to compute shared secret
- Authentication include:
 - shared secret, ex: HMAC-SHA
 - DSA / RSA signatures

Generic Routing Encapsulation

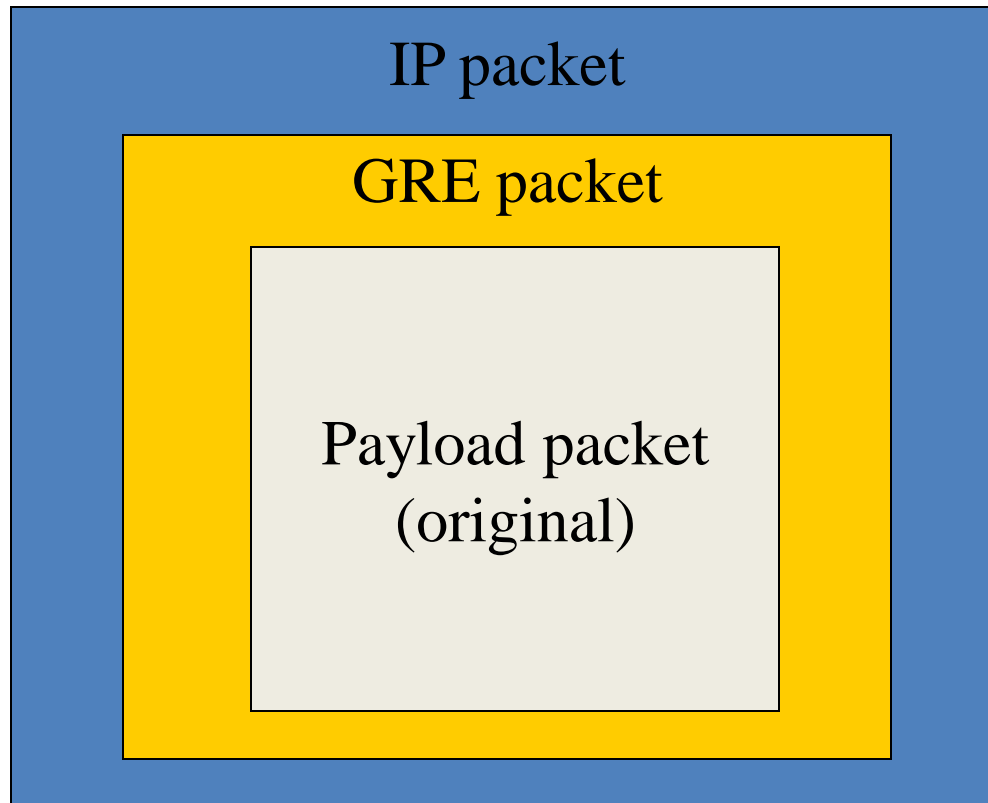
Generic Routing Encapsulation (GRE)

- Need to encapsulate protocols in other protocols
 - Example: IPX over TCP/IP
 - Example: broadcast across a VPN tunnel
- Request for Comments: 2784

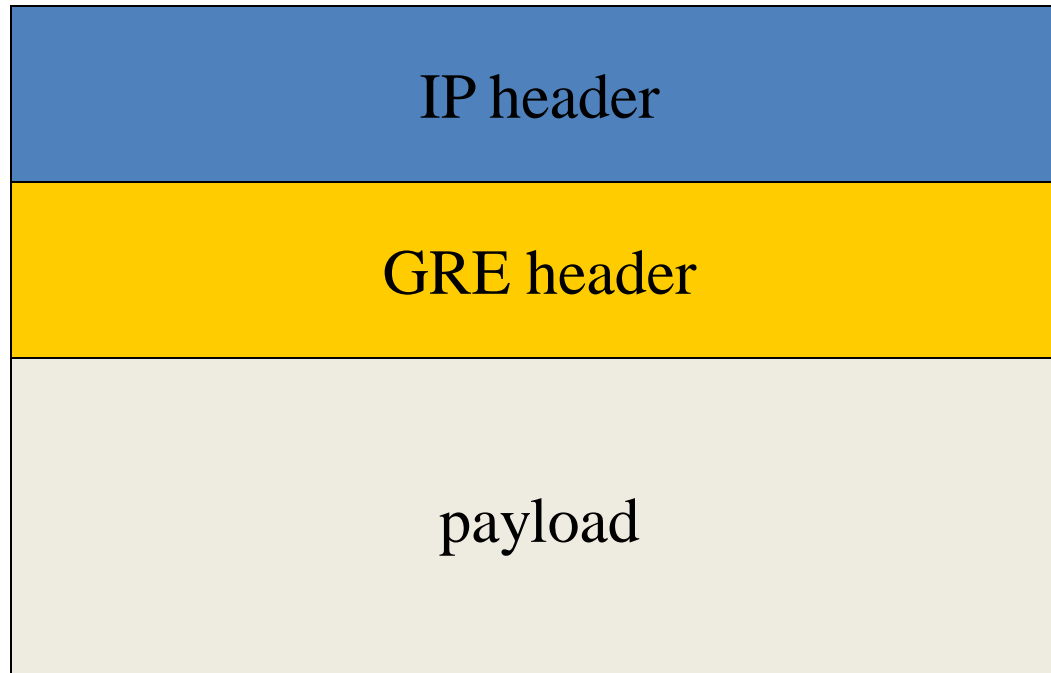
GRE encapsulation

- Original packet: payload packet
- Payload packet is wrapped with a GRE header
- Other protocol , carrier protocol, is used to deliver the packet
- Focus on IPv4 as carrier protocol

GRE packet



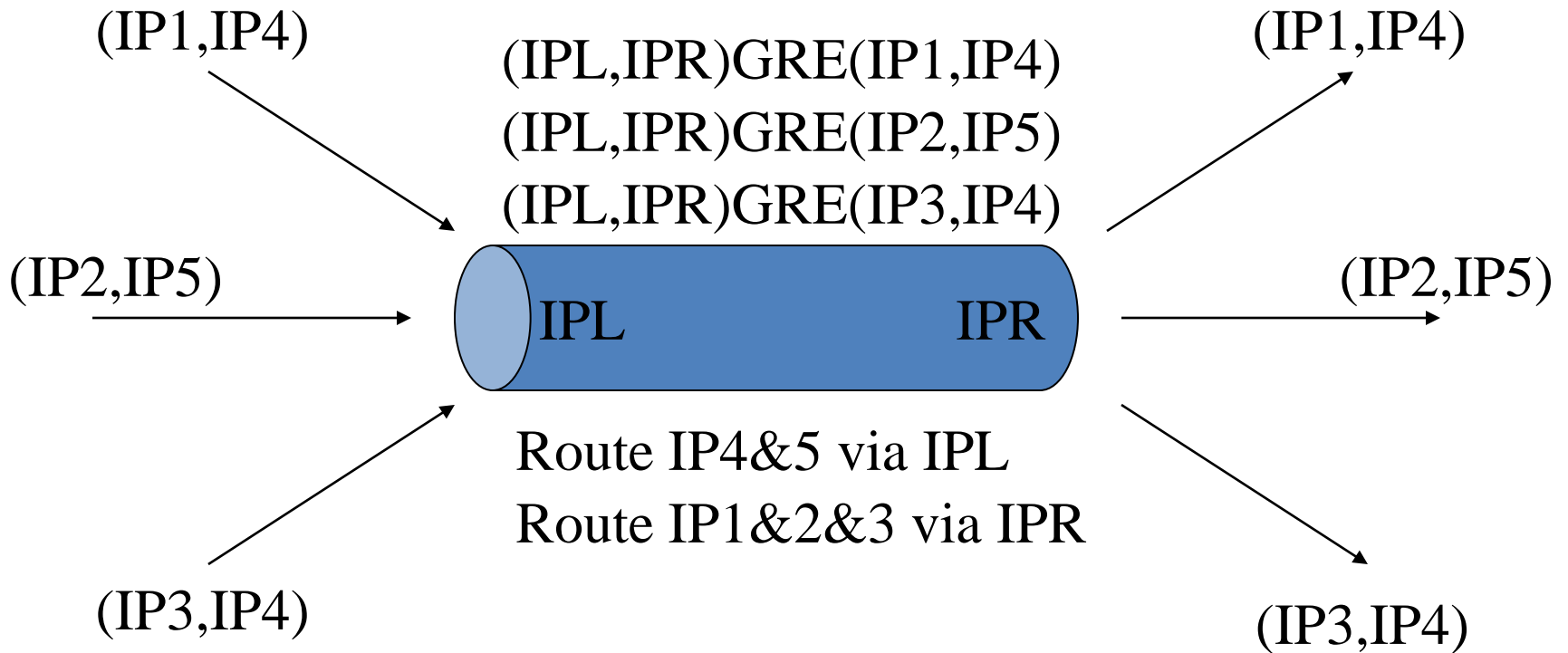
Linear form with IPv4 carrier



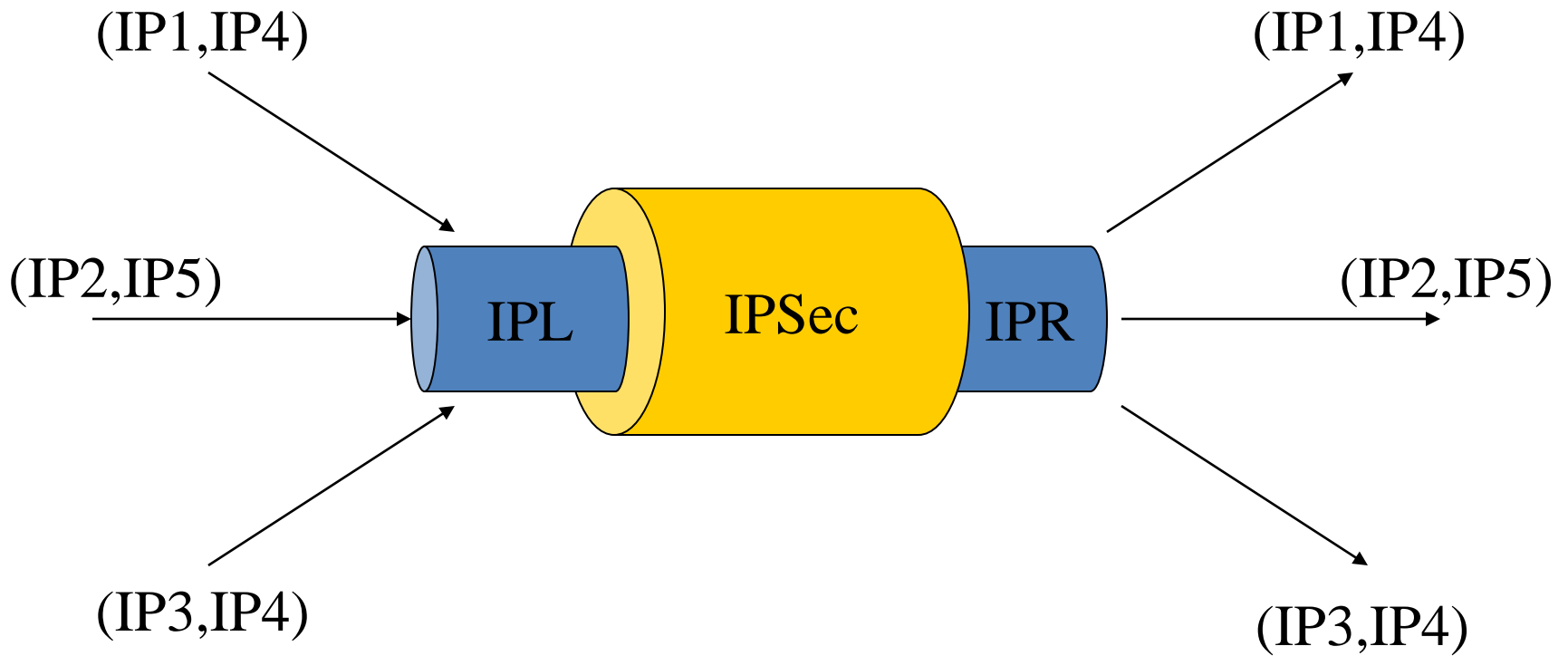
GRE header

- Protocol version; 0x800: IP
 - Note: IP protocol ID for GRE is 47
- Optional checksum

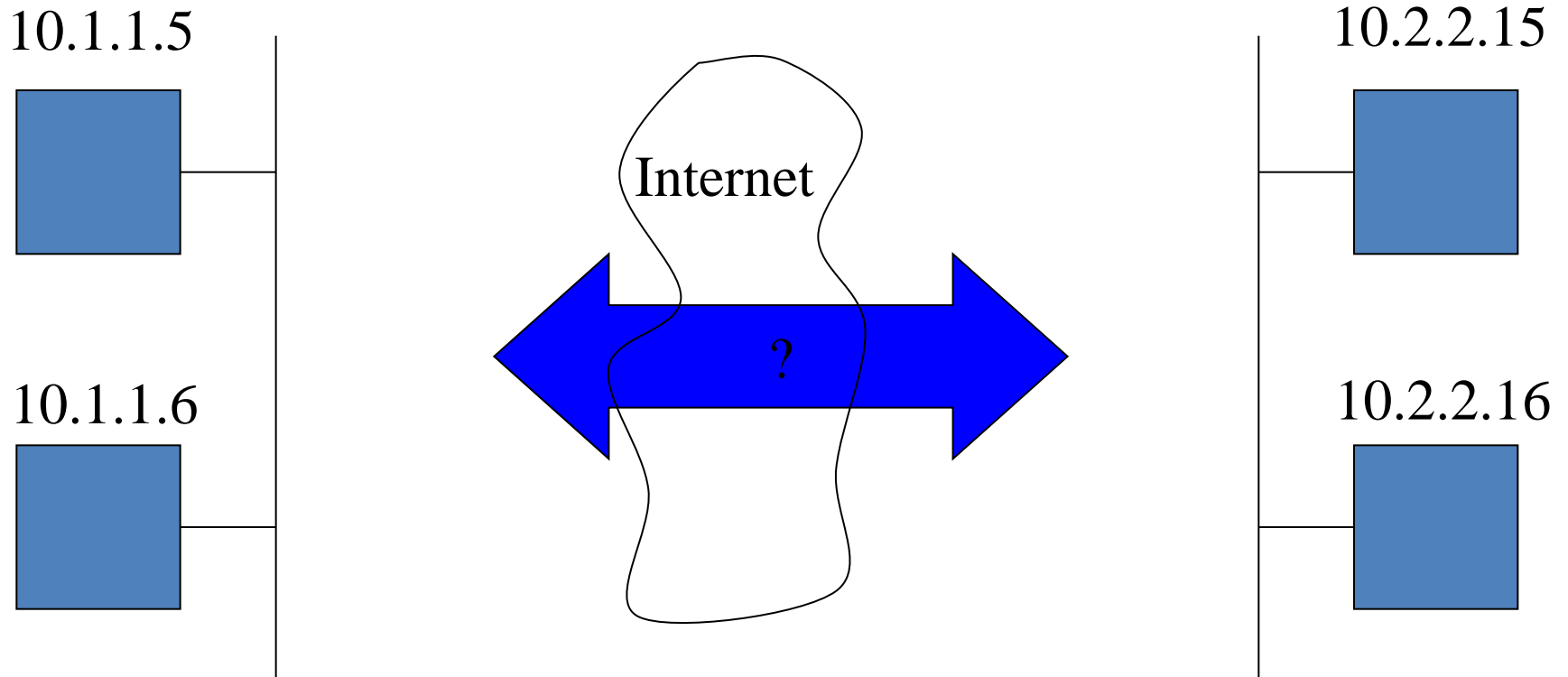
GRE usage



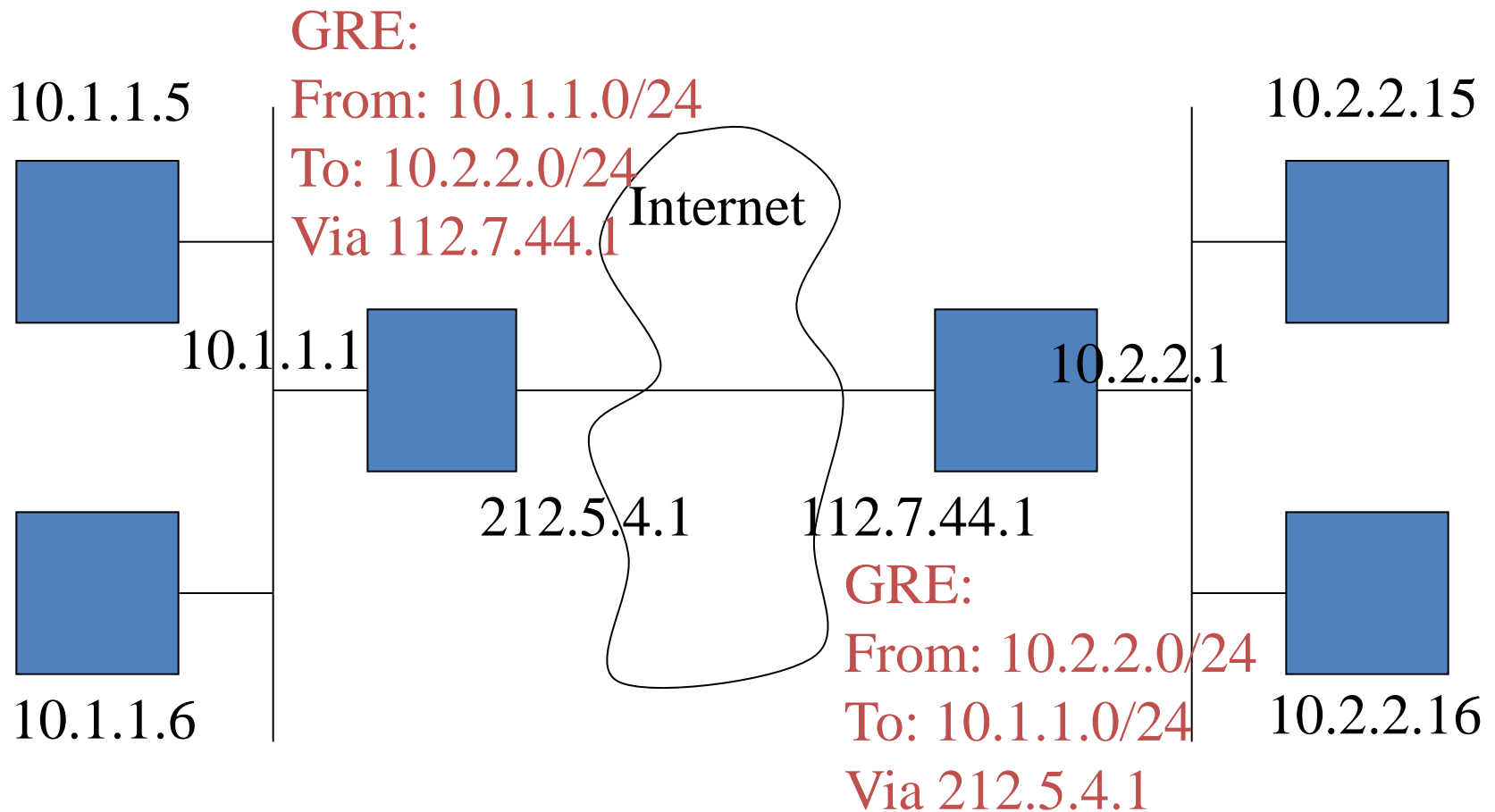
GRE + IPSec usage



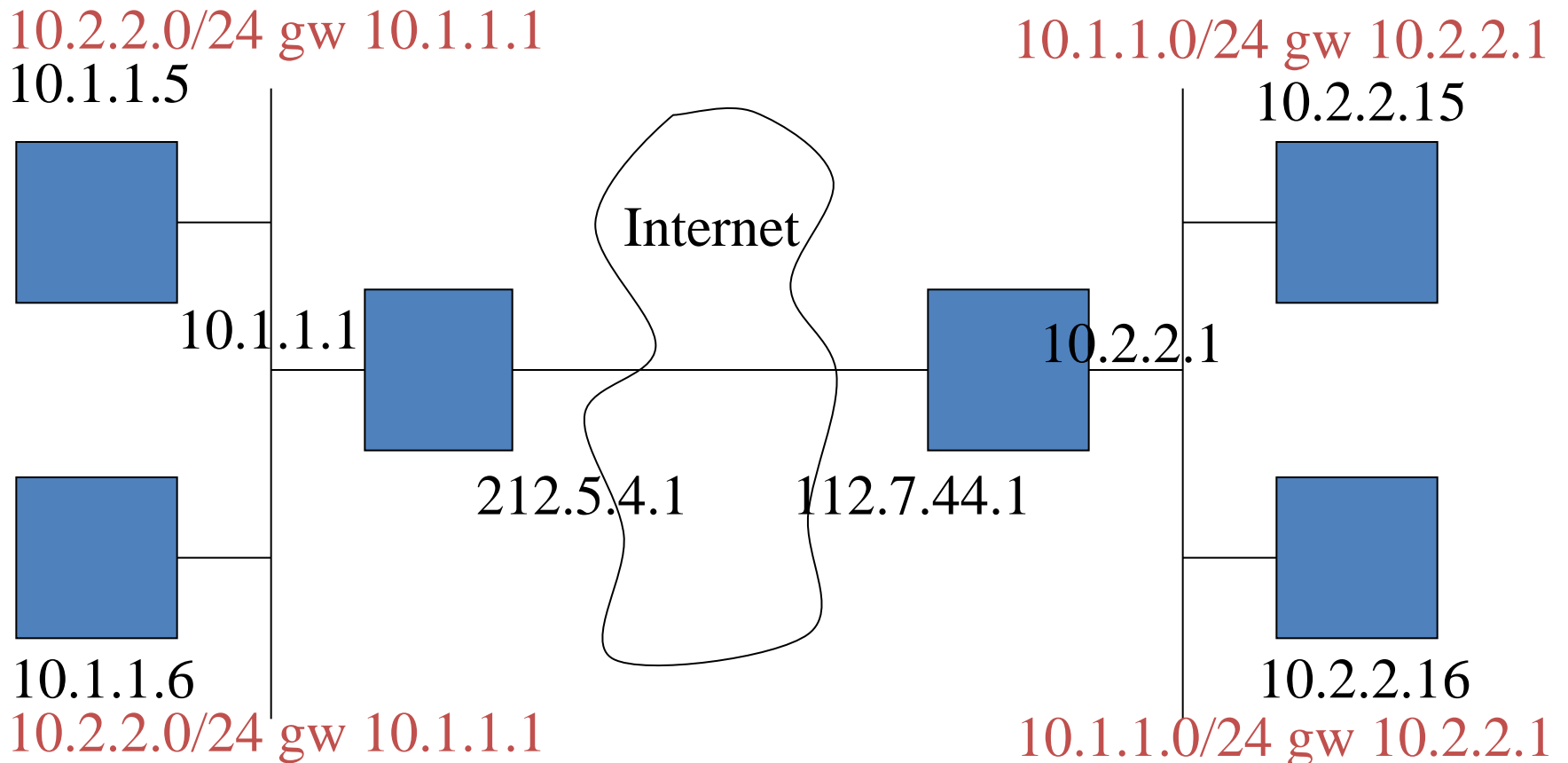
GRE example: problem



GRE example: configuration



GRE example: routing



Other VPN: PPTP

- PPTP: point to point tunneling protocol
- Extension of PPTP to allow VPN

PPTP protocol tasks

- Queries the status of communications servers
- Provides in-band management
- Allocates channels and places outgoing calls
- Notifies server of incoming calls
- Transmits and receives user data with bidirectional flow control
- Notifies server of disconnected calls
- Assures data integrity
- Coordinating packet flow

PPTP packets

Ethernet addresses: mac from, mac to

Ip addresses: IP from, IP to

GRE information

PPP information

Tunneled data

Exercise: RFC 1027

- read and understand

Exercise: RFC 925

- read and understand

References

- Microsoft Virtual Private Networking: Using Point-to-Point Tunneling Protocol for Low-Cost, Secure, Remote Access Across the Internet
- <http://www.alliedtelesyn.co.nz/documentation/ar800/241/pdf/gre.pdf>