TÉCNICO
LISBOA

Lab 8: Virtual Private Networks (VPNs)

Configuring (un)encrypted VPNs

Virtual Private Networks

- Goals:
  1. Learn the basics of Virtual Private Networks (VPNs)
  2. Use unencrypted tunnels to implement a VPN (GRE)
  3. Use encrypted tunnels to implement a VPN (OpenVPN)

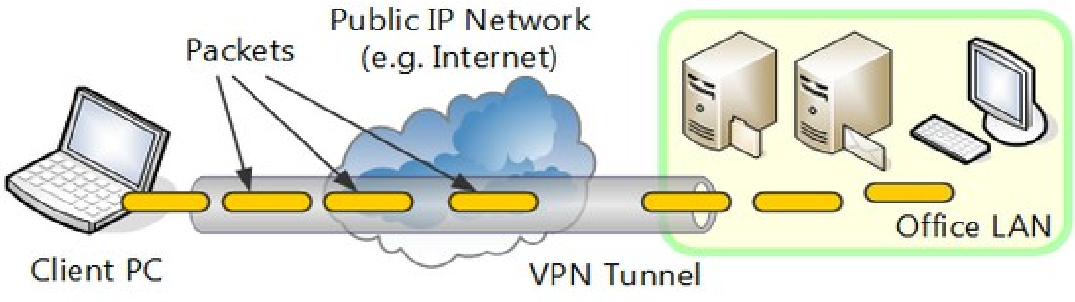
Evaluation

- Where
  - *Lab 8: VPNs* on Moodle (already opened)
- Submission due
  - Sunday, January 23, 23h59
- Comments due
  - Thursday, January 27, 23h59

Virtual Private Networks

Basic concepts

- Extension of a private network over a public network

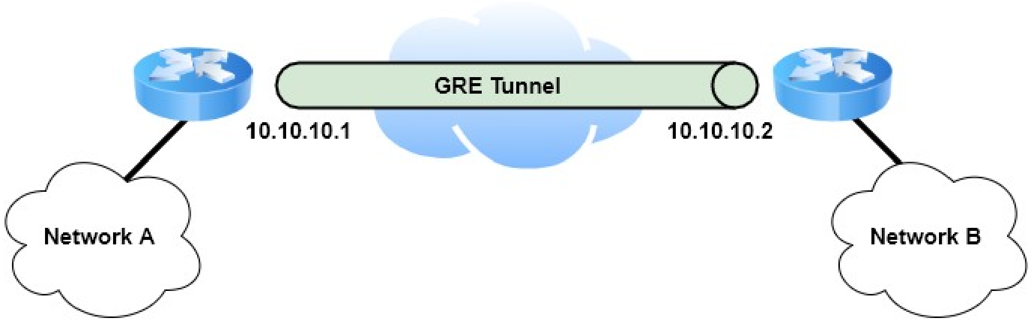


- Hosts appear to be directly connected to the private network through a secure point-to-point connection

Unencrypted tunnels

Generic Routing Encapsulation (GRE)

- A private point-to-point connection (a GRE tunnel) is created between the two routers

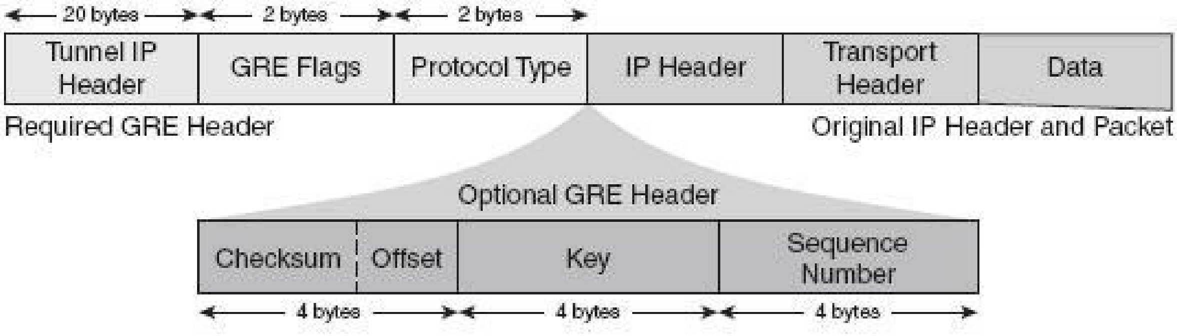


- Each endpoint is assigned a different IPv4 address
  - Packets are tunneled through the endpoints

Unencrypted tunnels

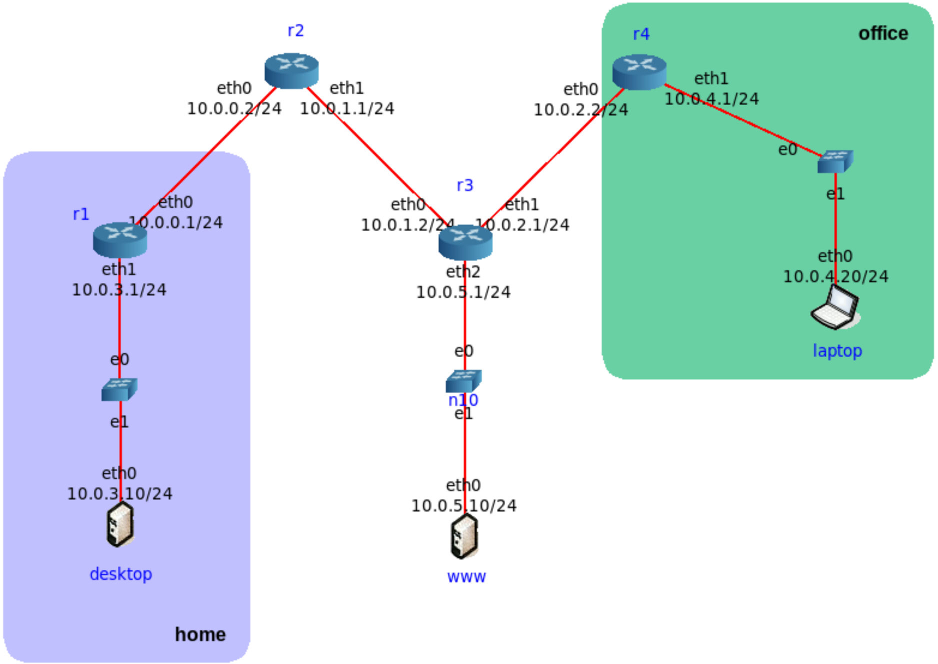
Generic Routing Encapsulation (GRE)

- GRE encapsulates packets to route other protocols over IP
  - Routers along the way do not parse inner packets, only the other GRE packet



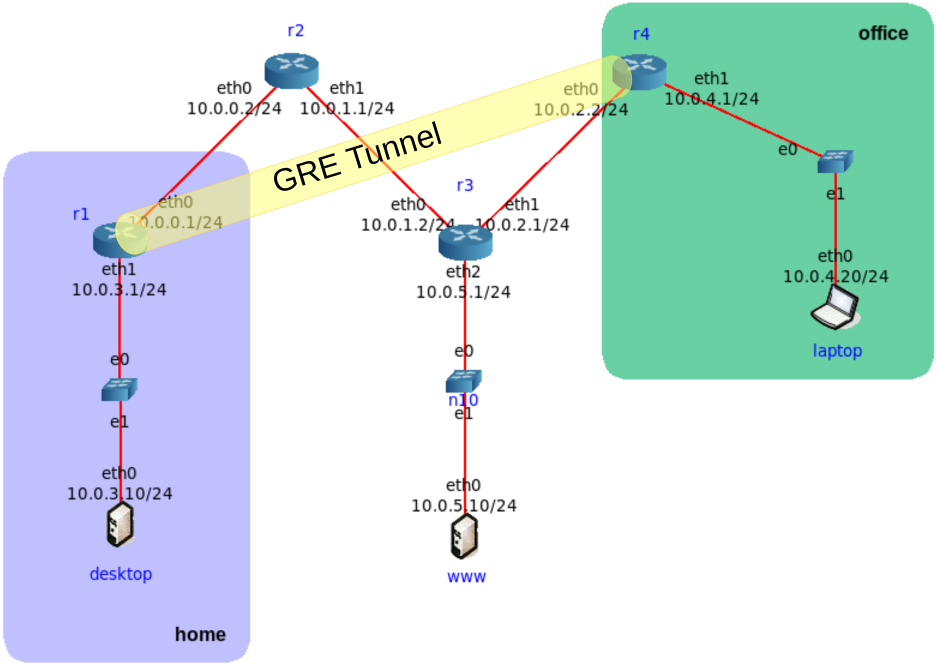
Unencrypted tunnels

Handout exercise



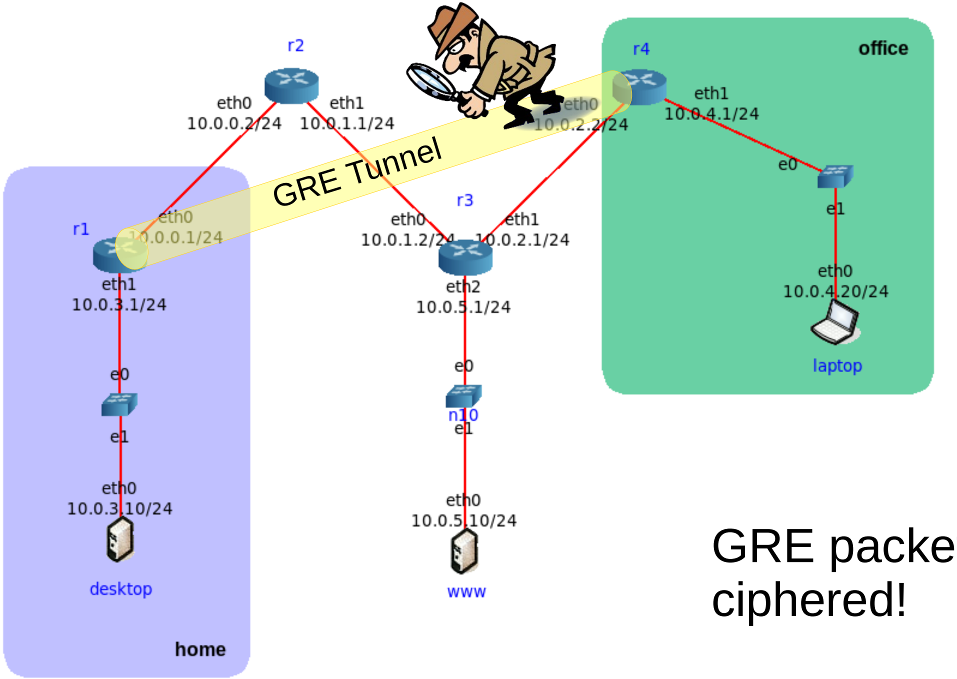
Unencrypted tunnels

Handout exercise



Unencrypted tunnels

Handout exercise

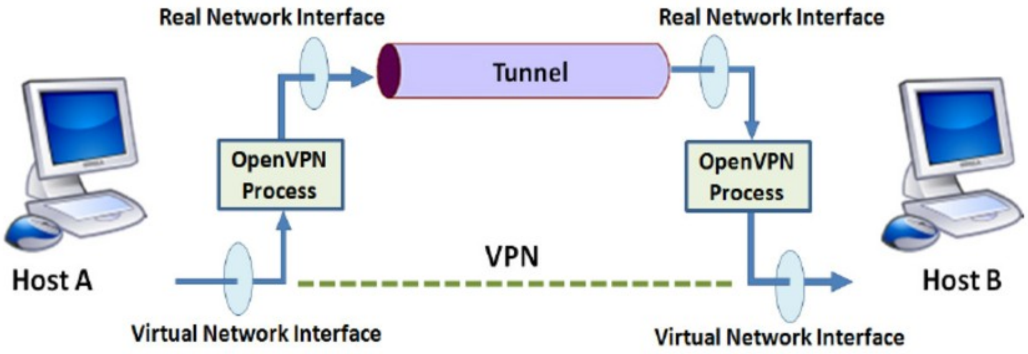


GRE packets are not ciphered!

Encrypted tunnels

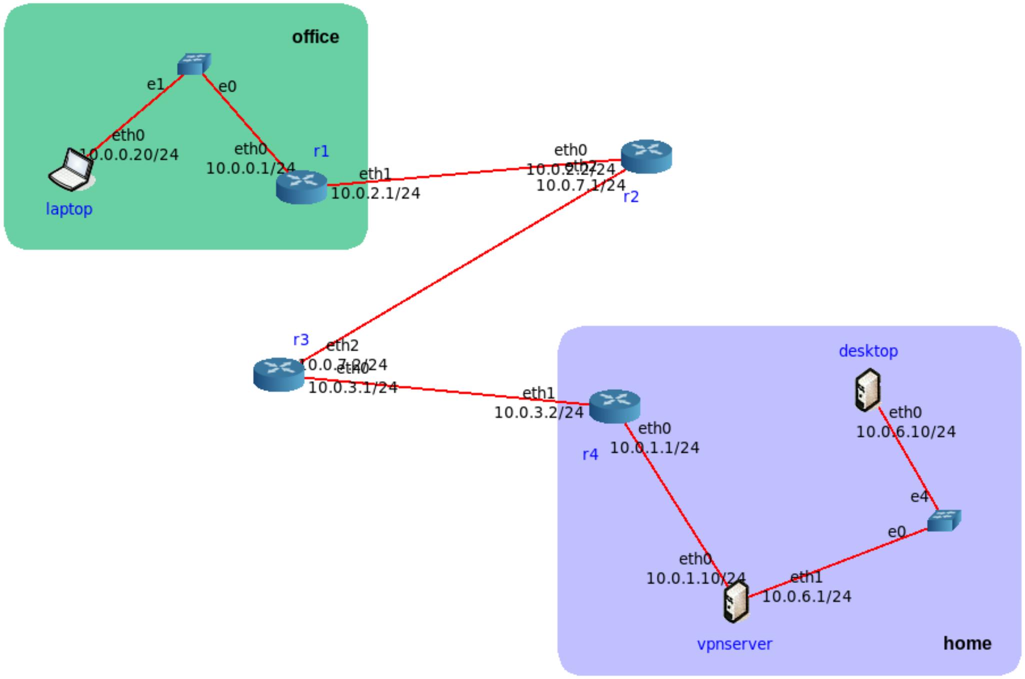
OpenVPN

- System that allows to create secure point-to-point tunnels over untrusted networks
  - Does not involve packet encapsulation
  - Communication is secured through the use of cryptographic mechanisms



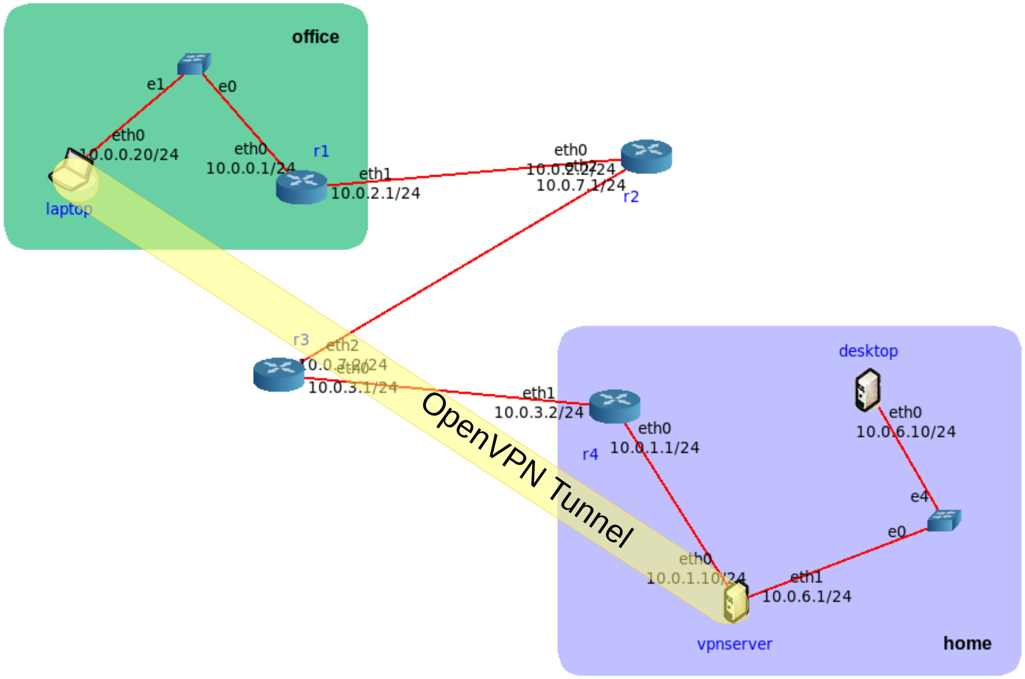
Encrypted tunnels

Handout exercise



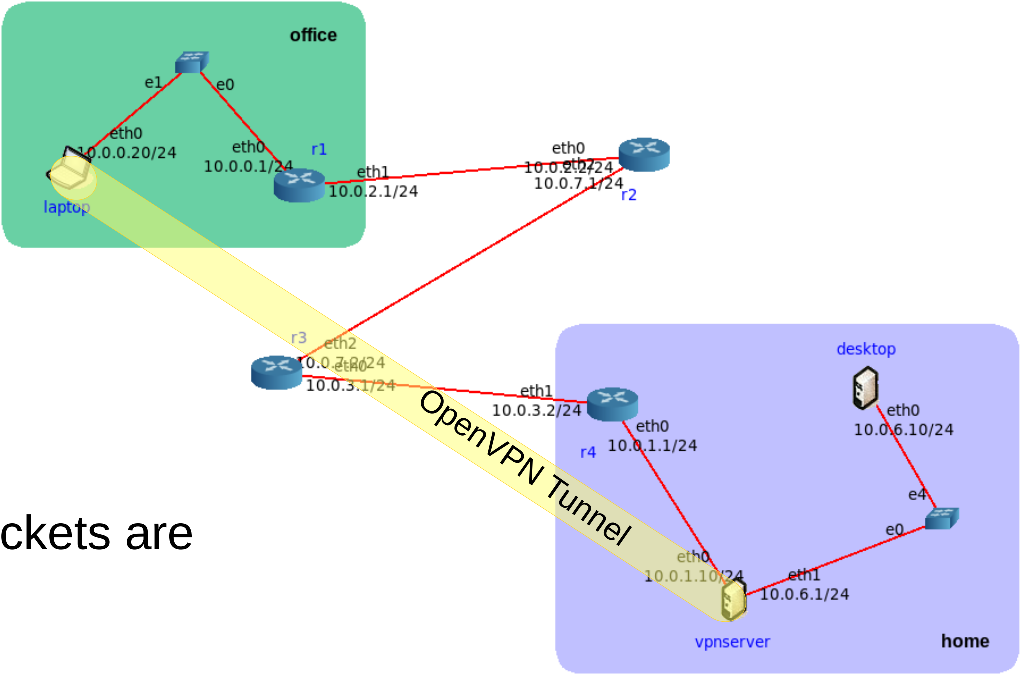
Encrypted tunnels

Handout exercise



Encrypted tunnels

Handout exercise



OpenVPN packets are ciphered!