TÉCNICO LISBOA

Lab 8: Virtual Private Networks (VPNs)

Configuring tunnels and secure VPNs

Goals

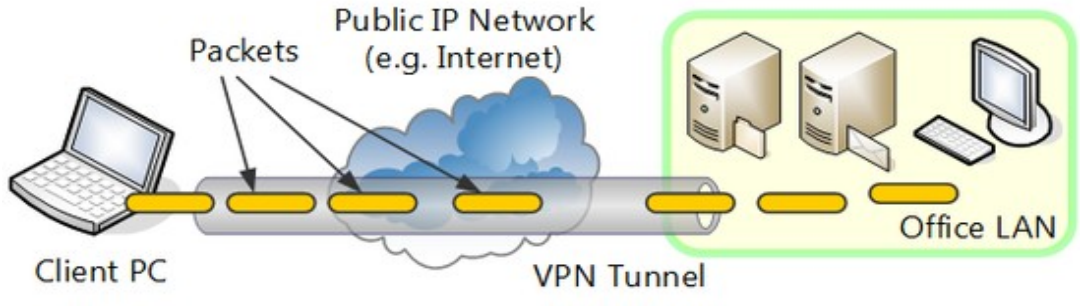
1. Learn the basics of Virtual Private Networks (VPNs)
2. Use GRE to implement simple tunnels
3. Use OpenVPN to implement a secure VPN

Evaluation

- Where
  - *Moodle: Lab 8: Virtual Private Networks*
- Submission due
  - Sunday, December 10, 23h59

Basic concepts

- Extension of a private network over a public network

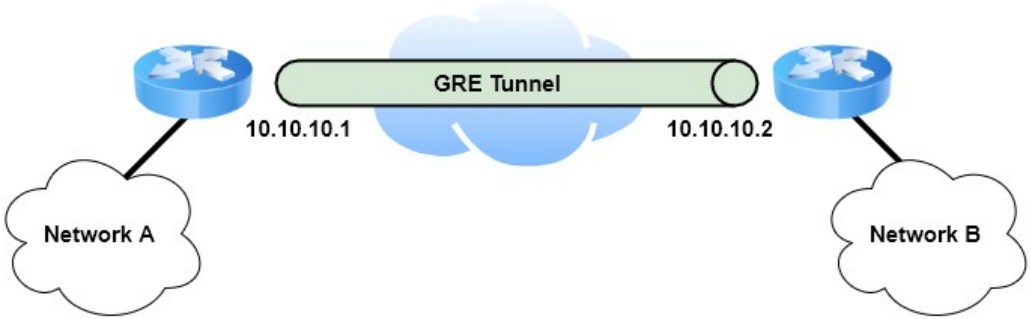


- Hosts appear to be directly connected to the private network through a (secure) point-to-point connection

Unencrypted tunnels

Generic Routing Encapsulation (GRE)

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

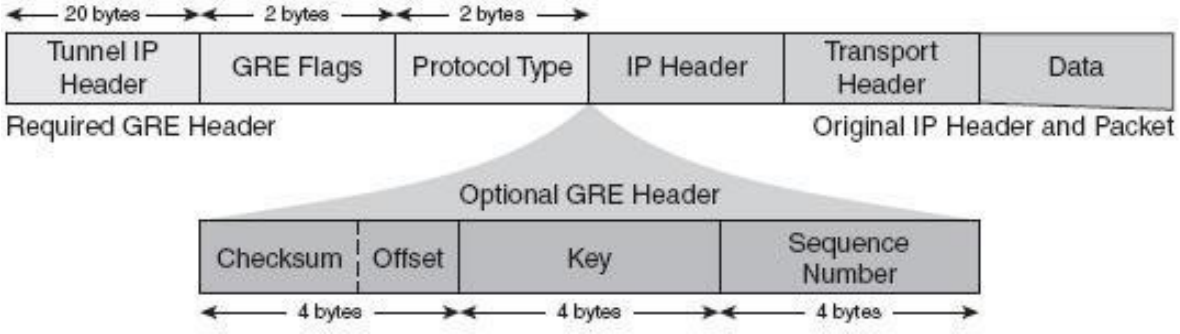


- Each endpoint is assigned a different IPv4 address
  - Packets are tunneled through the endpoints

Unencrypted tunnels

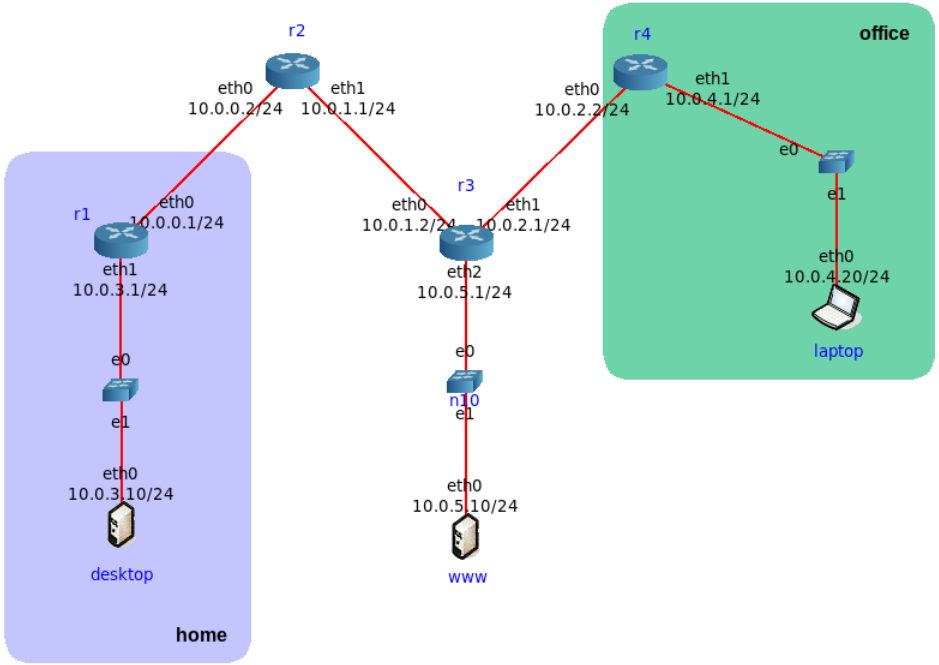
Generic Routing Encapsulation (GRE)

- Encapsulate packets to send other protocols over IP
  - Routers along the way *do not parse inner packets*, only the outer GRE packet



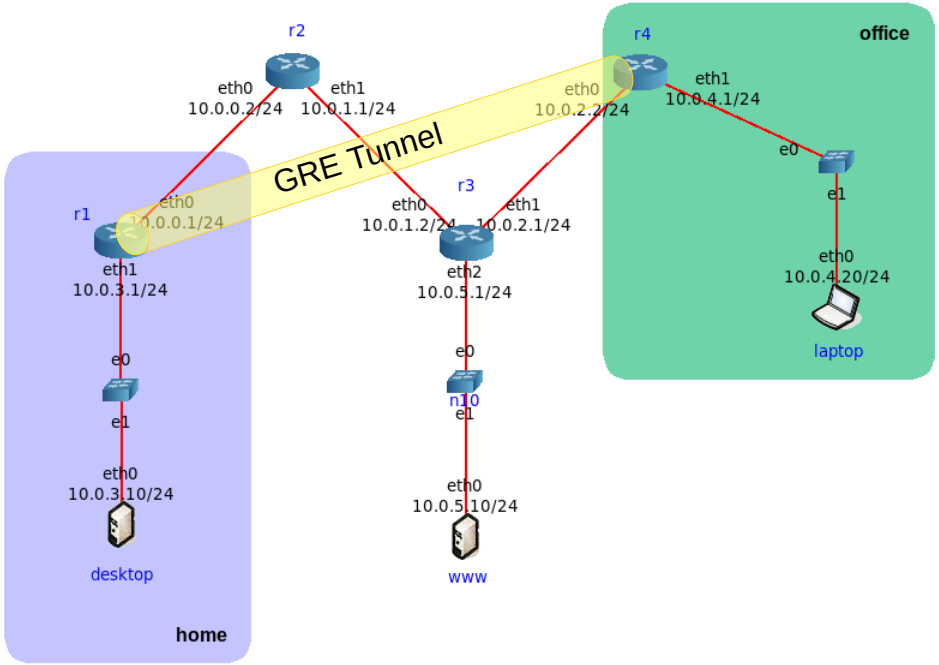
Unencrypted tunnels

Handout exercise



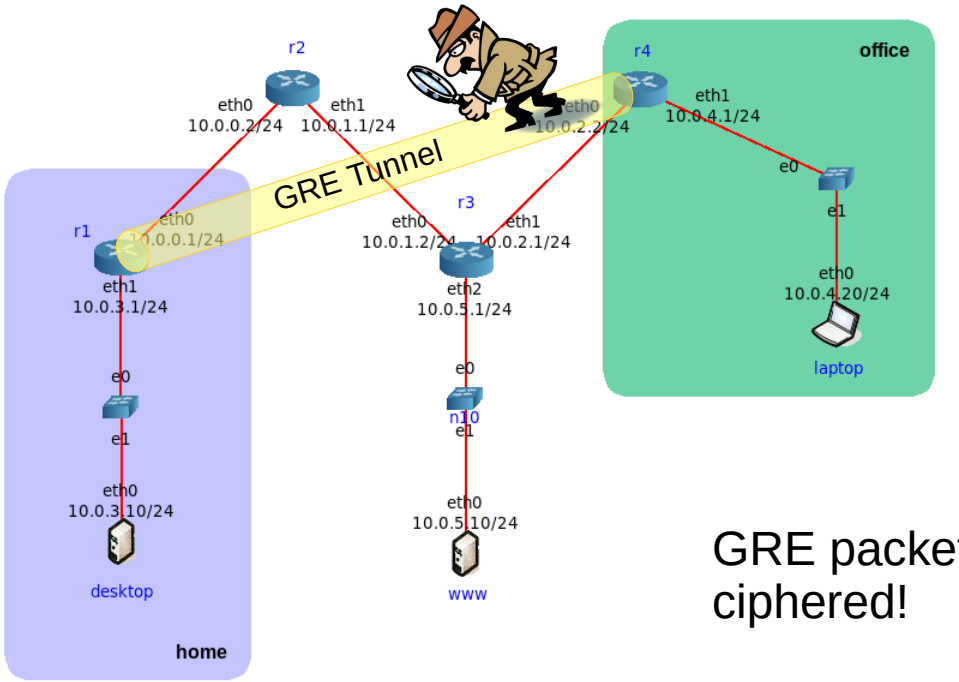
Unencrypted tunnels

Handout exercise



Unencrypted tunnels

Handout exercise

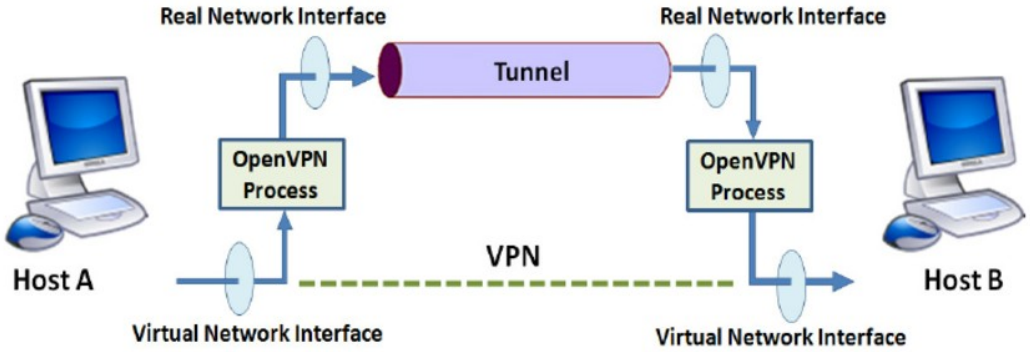


GRE packets are not ciphered!

Encrypted tunnels

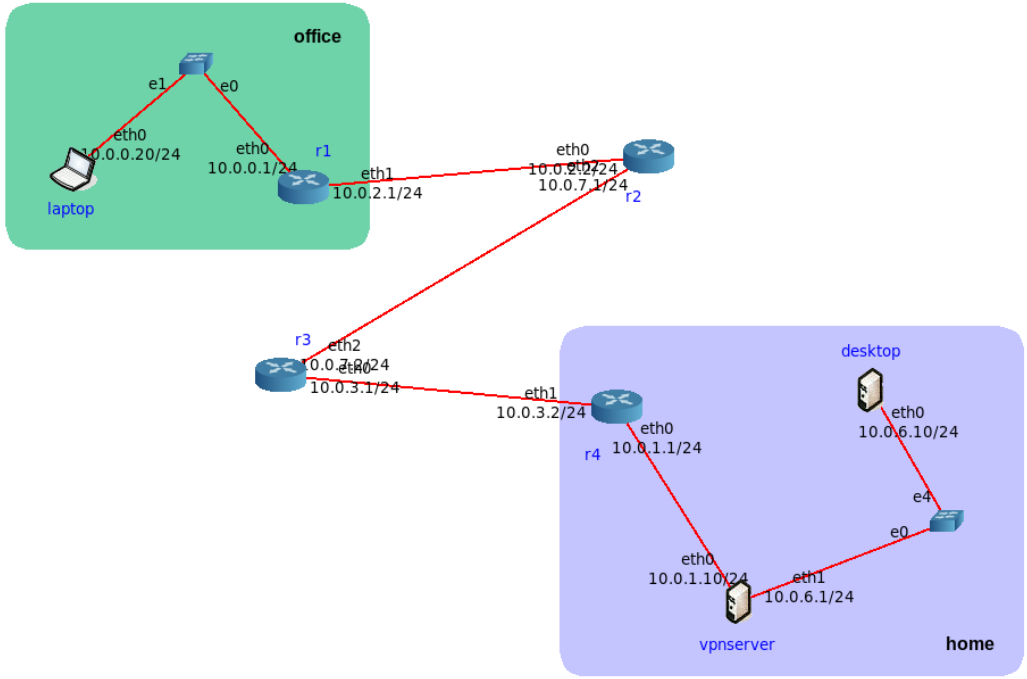
OpenVPN

- Secure point-to-point tunnels over untrusted networks
  - Communication is secured through the use of cryptographic mechanisms



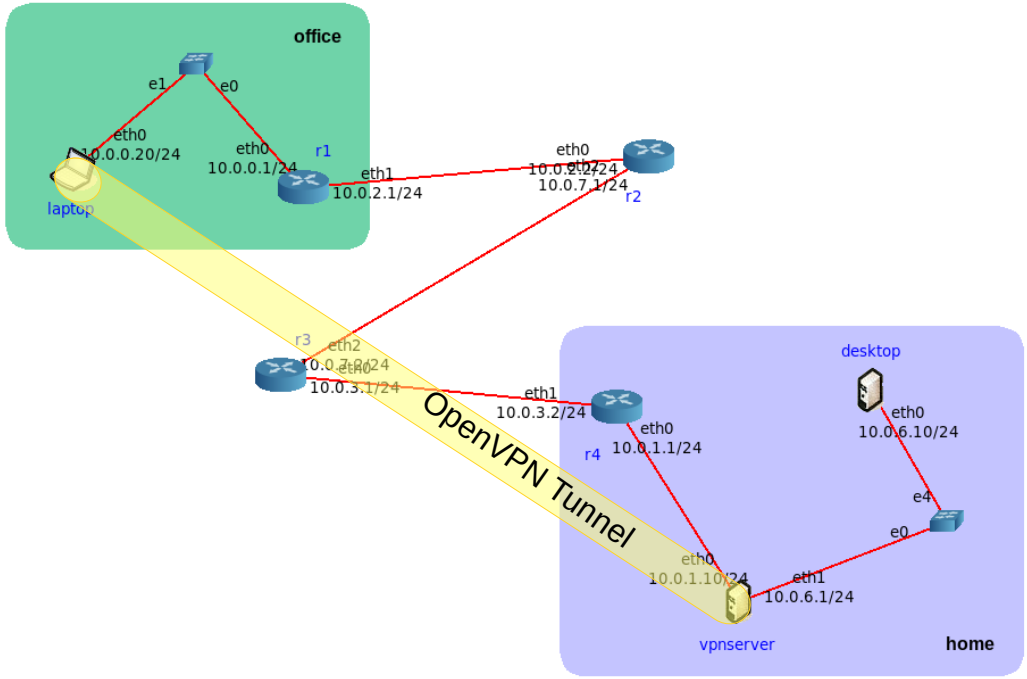
Encrypted tunnels

Handout exercise



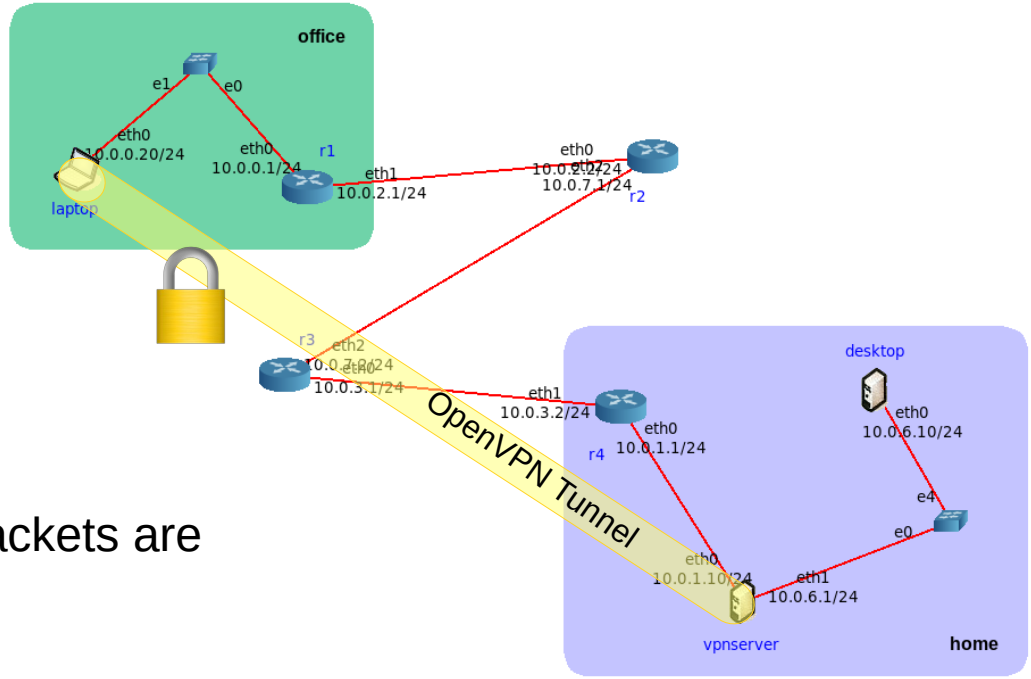
Encrypted tunnels

Handout exercise



Encrypted tunnels

Handout exercise



OpenVPN packets are encrypted!