

**Protocoles internet dans une optique  
sécurité**  
**PROTOCOLES & ARCHITECTURE  
INTERNET**

6/8 janvier 2009

**Gérald Litzistorf**



UNIVERSITÉ DE GENÈVE

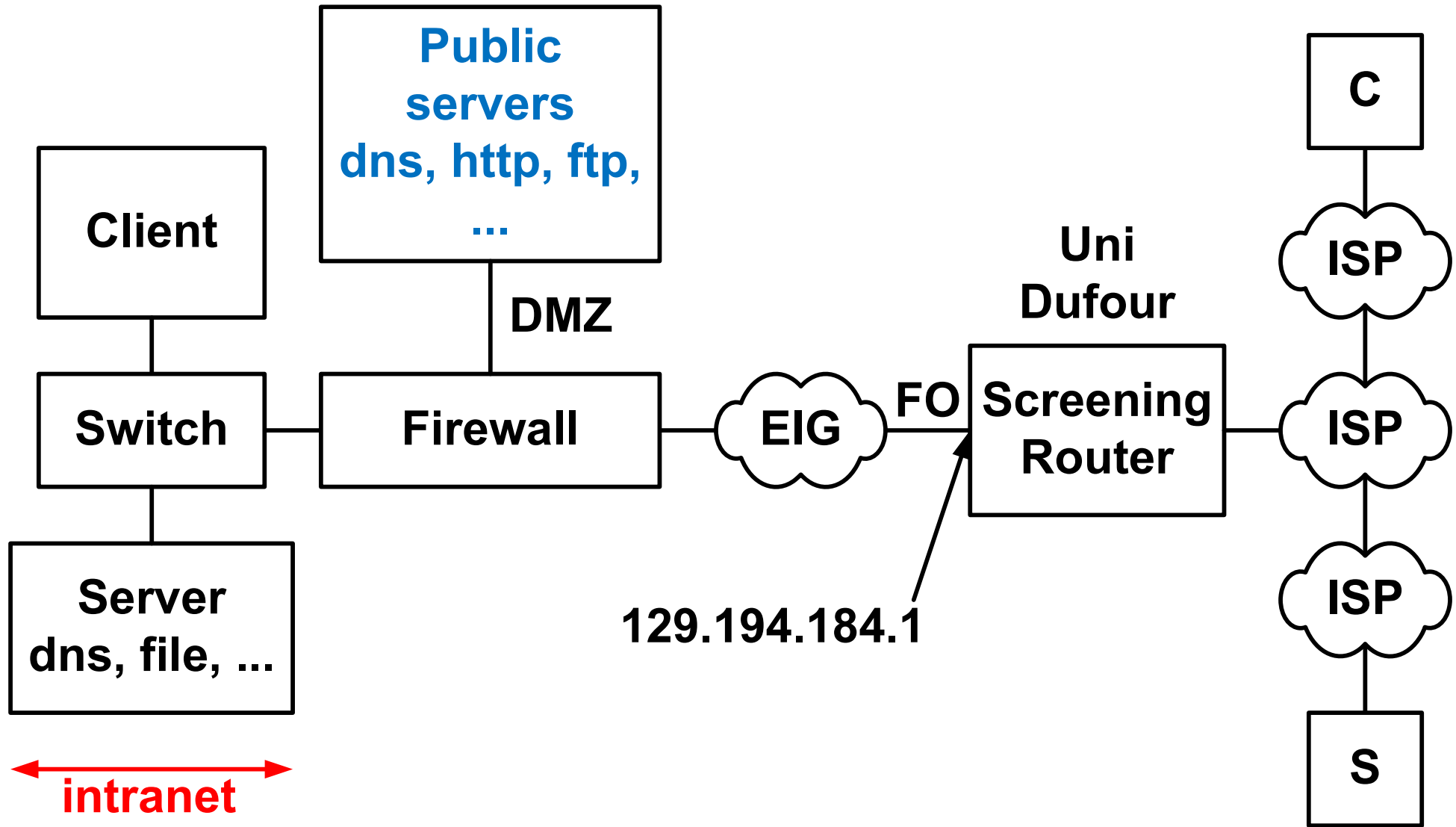
## Contenu

- Liaisons avec modules du DSSI
- *Internet* et mon poste de travail
- Modèle en couches : ..., *switch, router, firewall, proxy*, ...
- *Domain Name System* – FQDN
- *Internet*
- Famille de protocoles TCP/IP ..., IP, TCP, UDP, DNS, HTTP, ...
- Adresse IP, routeur
- Ports TCP
- Topologie : point à point et multipoint, ...
- Réseau d'accès, *dedicated line*, commutation, ADSL
- URLs

- §2 Configuration du poste de travail 10 min
- §3 Commande ping 10 min
- §4 FQDN, adresse IP et résolution DNS 15 min
- §5 Commande traceroute 10 min
- §6 Port TCP / UDP 10 min
- §7 Transfert de fichier ftp 10 min
- §8 Navigateur 10 min

# Infrastructure du labo

1 - 4



**Protocoles internet dans une optique  
sécurité**  
**PROTOCOLES (partie 1)**

13/15 janvier 2009

**Gérald Litzistorf**



UNIVERSITÉ DE GENÈVE

- **Ethernet → slides 3-10**
- **Internet Protocol (IP) → slides 11-16**
- **Address Resolution Protocol (ARP) → slides 17-21**
- **Ping & Internet Control Message Protocol (ICMP)  
→ slides 22-24**
- **User Datagram Protocol (UDP) → slides 25-26**
- **Labo → slide 27**
- **Principales RFCs, livre & URL → slide 28**

- §3      **Commandes arp et ping**      **15 min**
- §4      **Prise en main de Wireshark**      **30 min**  
**Acquisition du trafic ping 10.1.1.1**
- §5      **Protocoles Ethernet, ARP, IP, UDP, DNS**      **20 min**  
**Acquisition du trafic ping www.unige.ch**
- §6      **Wireshark en mode acquisition**      **20 min**  
**avec filtrage d'adresse**

**Protocoles internet dans une optique  
sécurité**  
**PROTOCOLES (partie 2)**

20/22 janvier 2009

**Gérald Litzistorf**



UNIVERSITÉ DE GENÈVE

- *Transmission Control Protocol (TCP)* → slides 3-17
- *User Datagram Protocol (UDP)* → slides 18-19 (rappel)
- *Applications web* → slides 20
- *HyperText Transfer Protocol (http)* → slides 21-27
- *Labo* → slide 28
- *Loopback* → slide 29

- §3      **Protocoles TCP et http**      **40 min**
- §4      **Wireshark en mode statistique**      **10 min**  
**Apprentissage**
- §5      **Wireshark en mode statistique**      **20 min**  
**Trafic EIG**
- §6      **Travail personnel**      **20 min**

# **INTRODUCTION AUX RESEAUX INFORMATIQUES INTERNETWORKING**

27/29 janvier 2009

**Gérald Litzistorf**



**UNIVERSITÉ DE GENÈVE**

- **Hub Ethernet → slides 3-9**
- **Switch Ethernet → slides 10-16**
- **Router, Subnet mask → slides 17-22**
- **Traceroute → slides 23-26**
- **Network scanners → slides 27-37**
- **Labo → slide 38**
- **Configuration dynamique → slides 39-42**

- §3      Indicateurs utiles de l'interface ethernet      **10 min**
- §4      Commutateur ethernet      **10 min**
- §5      Analyse protocole commande ping      **10 min**
- §6      Analyse protocole commande tracert      **15 min**
- §7      Outils TCPView & netstat      **15 min**
- §8      nmap      **15 min**
- §9      Forger un paquet avec Colasoft      **15 min**

**Protocoles internet dans une optique  
sécurité**  
**DOMAIN NAME SYSTEM**

3/5 février 2009

**Gérald Litzistorf**



UNIVERSITÉ DE GENÈVE

- **Rappel** → slides 3-6
- **Fonctionnement** → slides 7-9
- **Root servers** → slides 10
- **Requêtes récursives et itératives** → slides 11-12
- **Config. du labo** → slides 15-17, 23
- **Format des messages** → slides 18-20
- **Cache poisoning** → slides 21
- **nslookup** → slides 24
- **Labo** → slide 31

- §3      **Analyse protocole DNS**      **30 min**  
**Acquisition du trafic ping www.nokia.de**
- §4      **Commande nslookup (Windows XP)**      **20 min**
- §5      **Outils ntop et nagios**      **10 min**
- §6      **Outil netcat**      **20 min**