Compromis performance/sécurité des passerelles très haut débit pour Internet.

Ludovic Jacquin

Mercredi 20 novembre 2013

Dr Olivier Festor, Rapporteur.

Pr Jean-Marc Pierson, Rapporteur.

Pr Christophe Bidan, Examinateur.

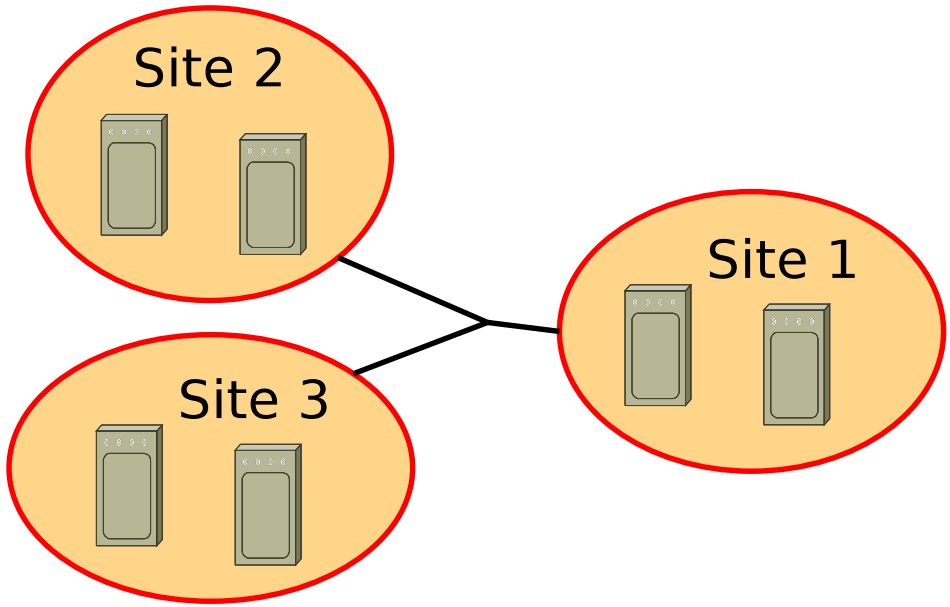
Dr Claude Castelluccia, Directeur de thèse.

Dr Vincent Roca, Co-Directeur de thèse.

Dr Jean-Louis Roch, Co-Directeur de thèse.

Financements : Projet SHIVA (FUI № 09-2-93-0473) et ATER à temps plein, IUT2 Université Pierre–Mendès France.

Problématique



Interconnexion sécurisée entre sites

Comment protéger les échanges numériques d'une institution/entreprise ?

Sécurité des communications réseau

Deux types de réseau privé

Physique Création d'un réseau indépendant.

Logique Utilisation d'un réseau partagé.

Quatres objectifs de sécurité

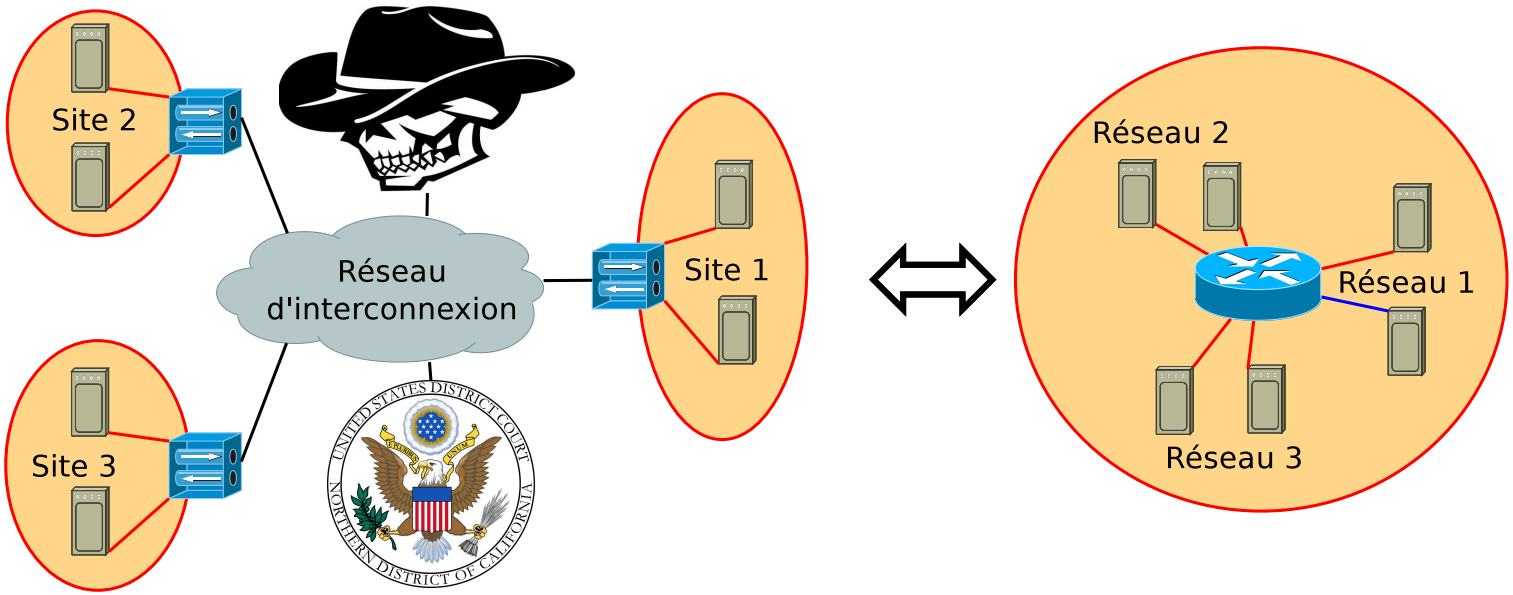
Confidentialité Protection des données contre l'écoute par des tiers.

Authenticité Authentification des flux.

Intégrité Non modification des données par les tiers.

Disponibilité Mise à disposition de toutes les capacités du réseau.

Réseau privé virtuel



Vue physique du réseau

Vue logique d'un utilisateur

Trois problématiques pour les passerelles

- **Sécuriser les communications** sur le réseau d'interconnexion.
- **Sécuriser les accès** aux réseaux des sites.
- **Supporter la charge** due à la bande passante.

Contexte général de la thèse

Le projet SHIVA (FUI)

Définition et implantation d'une passerelle sécurisé IPsec à 10 Gb/s.

Contributions

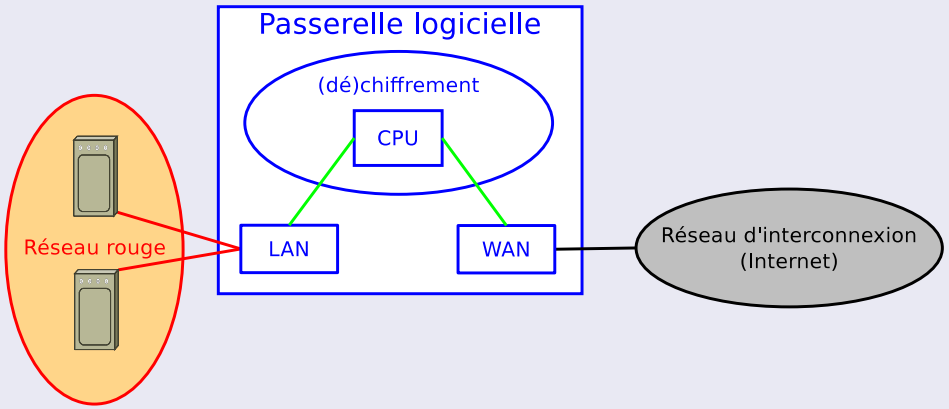
Conception et évaluation d'un système de sécurité "en rupture".
Caractérisation des routeurs et trous noirs ICMP.
Attaque ICMP contre des architectures de sécurité.

Plan

Plan

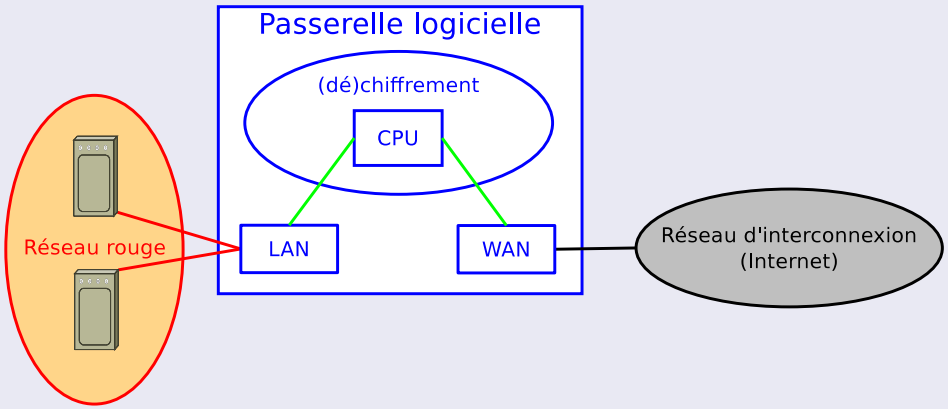
Architecture classiques

Architecture logicielle (OpenVPN, OpenSSH, OpenConnect)

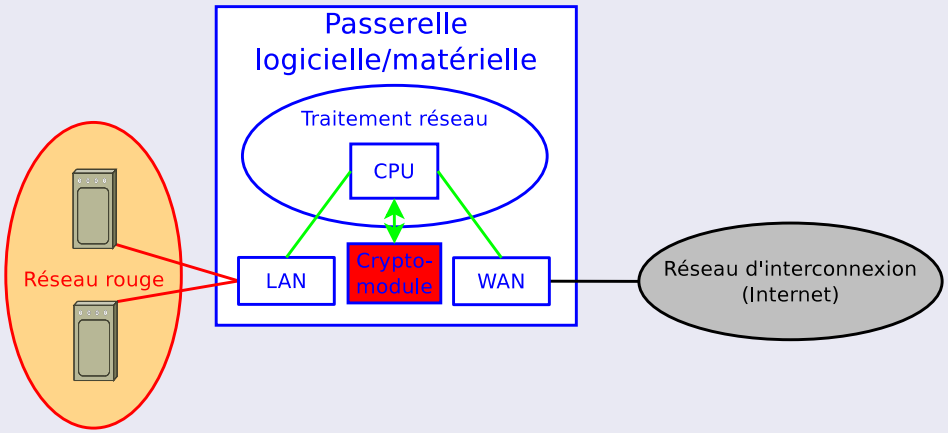


Architecture classiques

Architecture logicielle (OpenVPN, OpenSSH, OpenConnect)

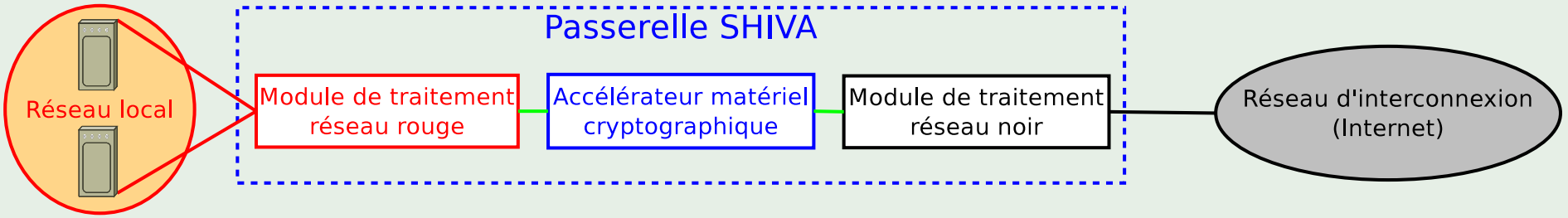


Architecture logicielle/matérielle (Cisco, module matériel de sécurité)

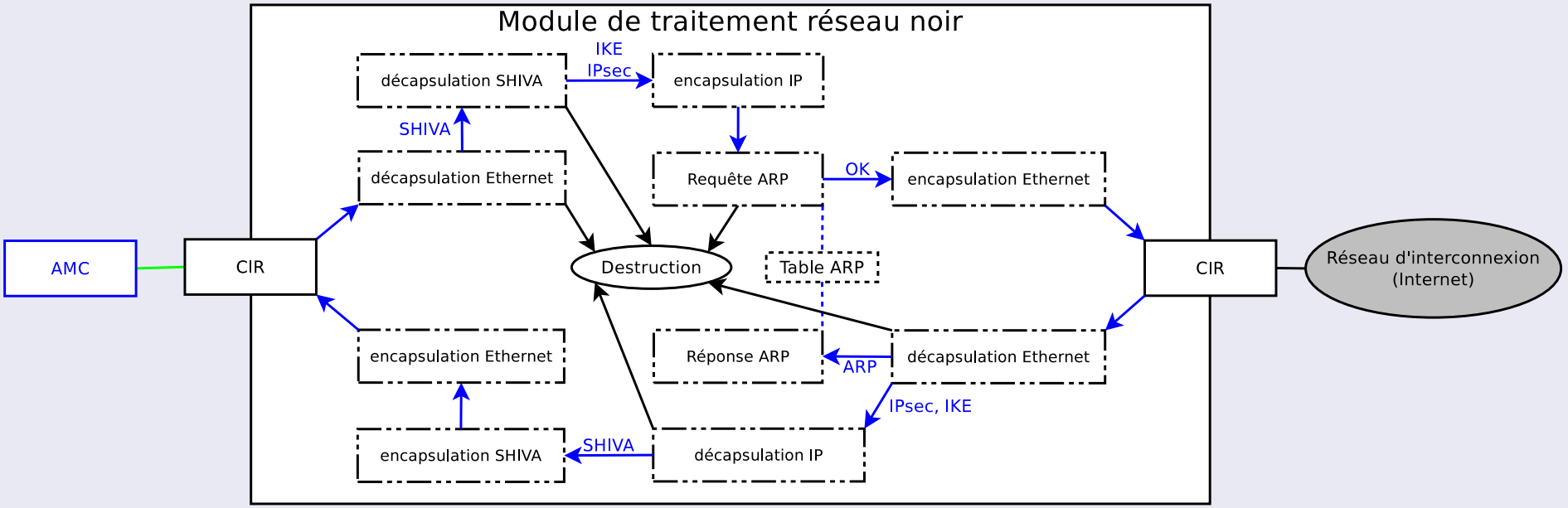


Architecture SHIVA

Architecture en rupture (chapitre 4)



Module de traitement réseau noir



Choix technologiques

Click, un "routeur" logiciel modulaire (Kohler)

Mise au point d'une pile réseau sur mesure.
Click 2.0.1 sur Debian 6.0.2 (Linux 3.2.1).

Dernières évolutions du matériel sur étagère

- Cartes réseaux multiqueues (CIR Intel, Myricom).
- Architecture parallèle des ordinateurs (Intel Nehalem, QPI, IOH).

Choix technologiques

Click, un "routeur" logiciel modulaire (Kohler)

Mise au point d'une pile réseau sur mesure.
Click 2.0.1 sur Debian 6.0.2 (Linux 3.2.1).

Dernières évolutions du matériel sur étagère

- Cartes réseaux multiqueues (CIR Intel, Myricom).
- Architecture parallèle des ordinateurs (Intel Nehalem, QPI, IOH).

Portage de notre pile sur Click

La mise en œuvre initiale est limitée à 1,3 Gb/s.

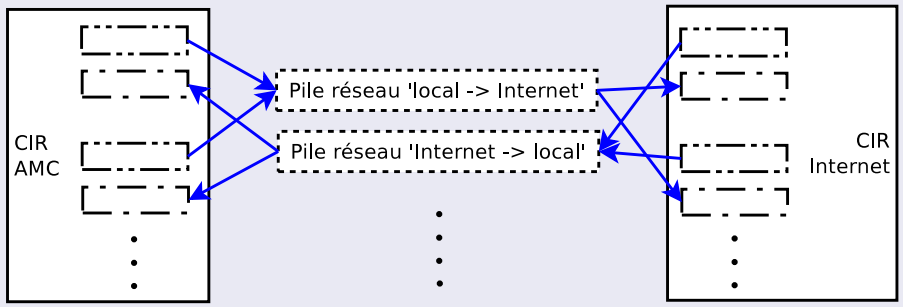
Spécificité des traitements réseau

Sans optimisation, une passerelle minimale de niveau 2 est limitée à 3 Gb/s.

Performances de l'architecture en rupture

Parallélisation

- Séparer les traitements par direction du trafic.
- Instancier plusieurs piles réseau.
- Utilisation des queues physiques.



Banc de validation des performances

2000 connexions utilisateurs (objectif SHIVA).
Moyenne du débit sur 10 tests.

La seule mise en place d'un tel banc de test est complexe.

Résultats obtenus

2,75 Gb/s pour des paquets de 1 500 octets.

Contributions

Architecture en rupture **Définition d'une nouvelle architecture** de passerelle et développement d'un prototype.

Accélérateur cryptographique Le matériel sur étagère ne peut pas traiter le chiffrement à 10 Gb/s.

Point critique Nombre de paquets traités par seconde.
Grâce aux optimisations on obtient un débit de 5 Gb/s.

Publication

"Parallel arithmetic encryption for high-bandwidth communications on multicore/GPGPU platforms"
L. Jacquin, V. Roca, J.-L. Roch et M. Al Ali. *International Workshop on Parallel and Symbolic Computation (PASCO'10)*, 2010.

Trois délivrables pour le projet SHIVA (dont spécification et implantation).

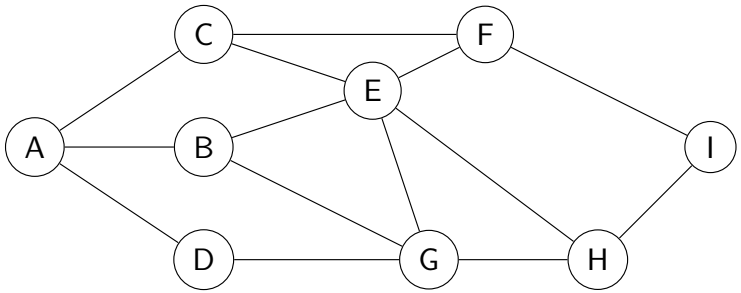
Performances et taille maximale de paquets

Définition d'un réseau

Graphe d'hôtes connectés :

Nœuds Ordinateurs, routeurs.

Arêtes Liens physiques entre nœuds.



Une propriété des liens physiques (RFC 894)

MTU = taille maximale supportée le lien.

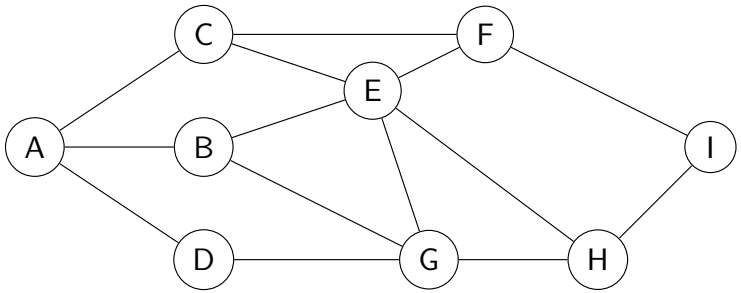
Performances et taille maximale de paquets

Définition d'un réseau

Graphe d'hôtes connectés :

Nœuds Ordinateurs, routeurs.

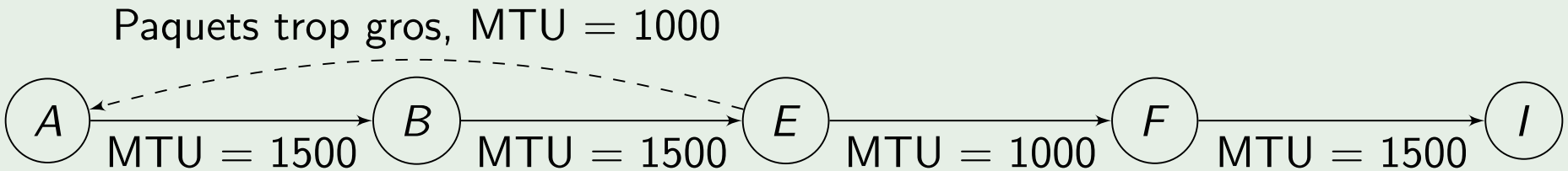
Arêtes Liens physiques entre nœuds.



Une propriété des liens physiques (RFC 894)

MTU = taille maximale supportée le lien.

Découverte de la taille maximale des paquets sur une route (PMTUd, RFC 1191 et 1981)



Présentation d'ICMP

Un protocole fondamental (RFC 792 et 4443)

Transmet les **messages de contrôles et d'erreurs** des routeurs pour les protocoles Internet.

Protocole de la couche réseau (niveau 3)

- ICMP se situe au même niveau qu'IP ;
- ICMP ne fait pas de routage, il **utilise IP pour l'acheminement** ;
- existe en 2 versions : ICMP et ICMPv6.

Le protocole ICMP en détail

Format général de l'en-tête ICMP

0-7	8-15	16-31
Type	**Code**	Somme de contrôle
Données ou bourrage		
Optionnel : données (longueur variable)		

Deux catégories de types ICMP

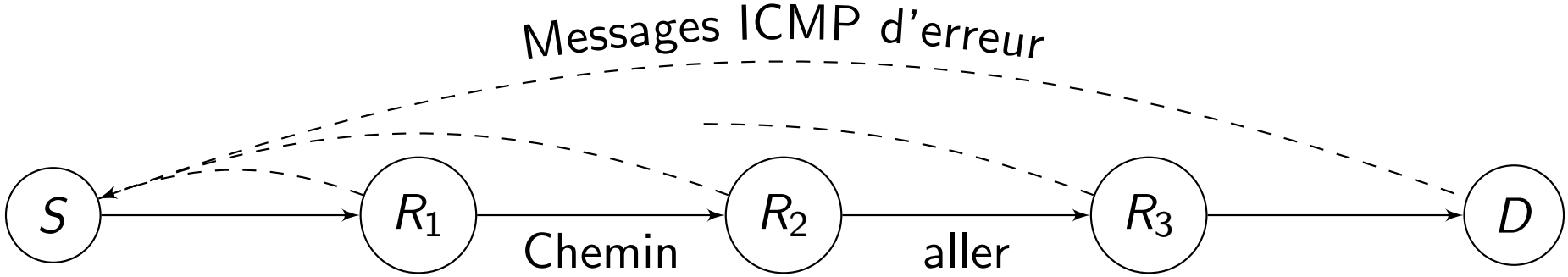
Messages d'erreur destination non atteignable (dont paquet trop gros) ;
extinction de la source ;
redirection ;
dépassement du temps ;
problèmes de paramétrage.

Messages d'information requête/réponse d'echo ;
gestion des routes, multicast.

ICMP et la topologie réseau

Traceroute

Trouver les routeurs intermédiaires en générant des messages ICMP "dépassement du temps" (champ TTL à 0 dans l'en–tête IP).



Numéro de saut	IP du Routeur	Round-Trip Time
1 (R1)	11.11.11.11	0.3 ms
2 (R2)	22.22.22.22	0.4 ms
3	* * *	
4 (D)	44.44.44.44	1 ms

Utilisations majeures d'ICMP

Découverte de la topologie du réseau

Évaluer l'état des routes du réseau (Traceroute).

Gestion des "erreurs" des paquets

Informer les émetteurs en cas de problème avec leurs paquets (PMTUd).

Utilisations majeures d'ICMP

Découverte de la topologie du réseau

Évaluer l'état des routes du réseau (Traceroute).

Gestion des "erreurs" des paquets

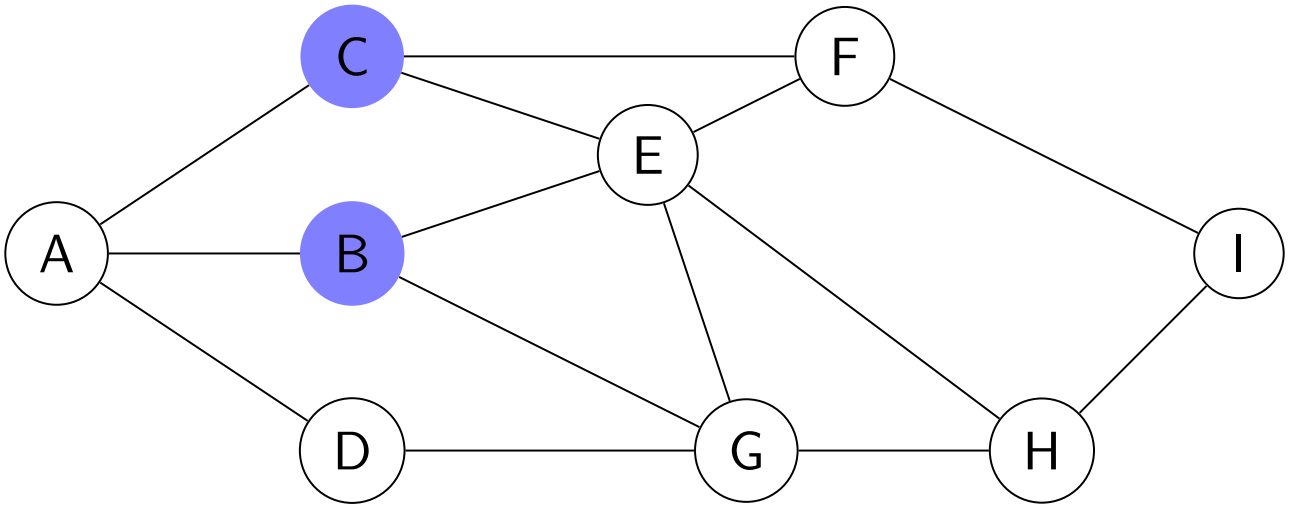
Informer les émetteurs en cas de problème avec leurs paquets (PMTUd).

Un vecteur d'attaque classique

Utilisation possible pour mener des attaques, en particulier de **Déni de Service Distribué** (cf 3ème partie).

Plan

Motivations d'IBTrack



Trous noirs ICMP

Parties du réseau détruisant les messages ICMP.
Multiples justifications (filtrage, administration).

Deux objectifs majeurs

- **Détection** des trous noirs ICMP.
- **Analyse du comportement** des routeurs associés à ces trous noirs.

Travaux associés

MERLIN (Mérindol et al., 2011)

Découverte de la topologie "multicast" du réseau.

Hubble (Katz-Bassett et al., 2008)

Mise en évidence les trous noirs ICMP (**sondage périodique**).

Reverse Traceroute (Katz-Bassett et al., 2010)

Découverte du chemin retour pour une destination donnée.

Travaux associés

MERLIN (Mérindol et al., 2011)

Découverte de la topologie "multicast" du réseau.

Hubble (Katz-Bassett et al., 2008)

Mise en évidence les trous noirs ICMP (**sondage périodique**).

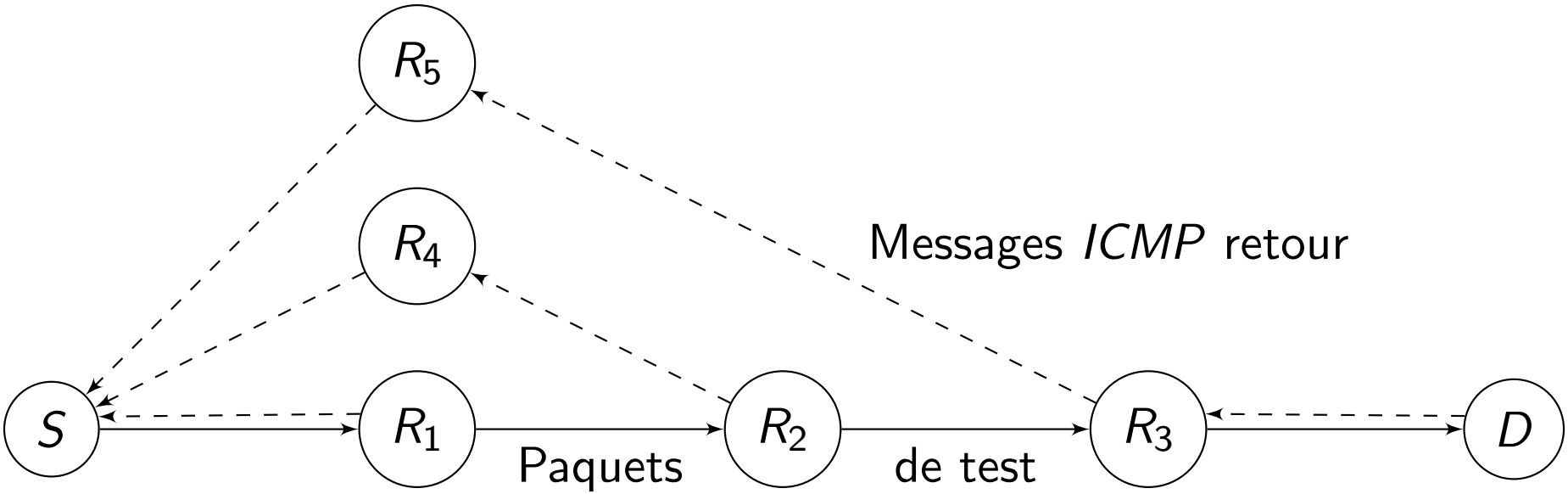
Reverse Traceroute (Katz-Bassett et al., 2010)

Découverte du chemin retour pour une destination donnée.

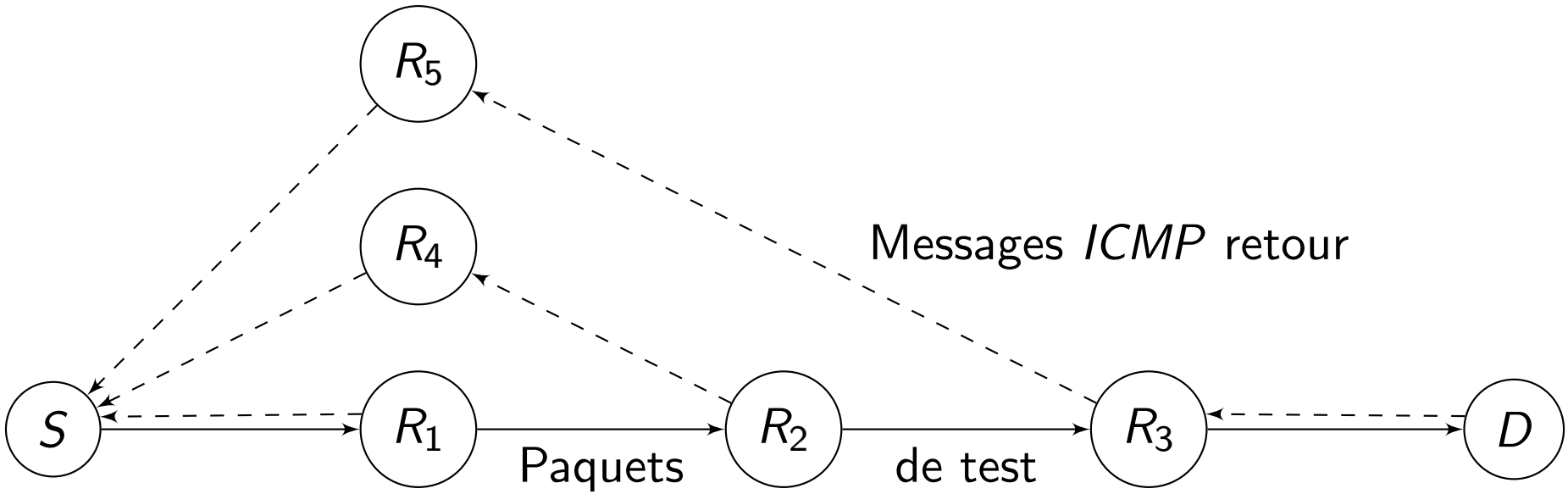
IBTrack (chapitre 6)

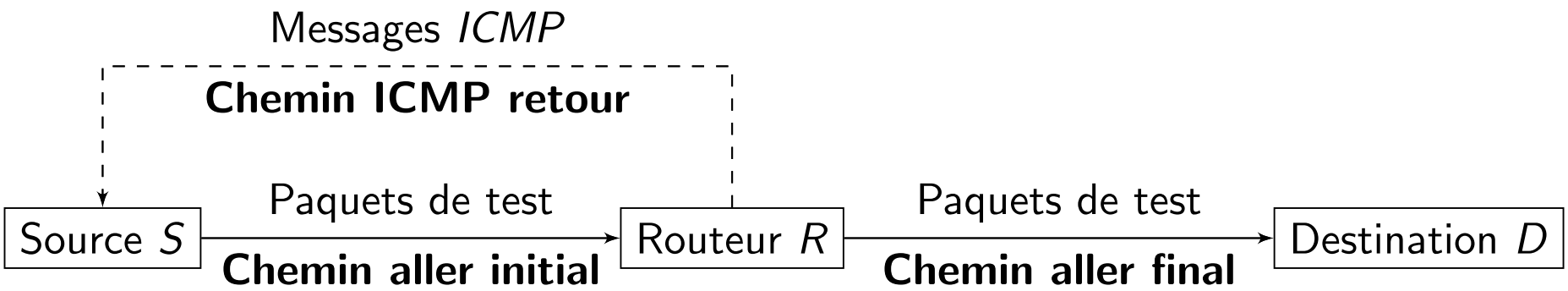
Caractérisation du comportement des routeurs et des trous noirs ICMP.

Définitions



Définitions

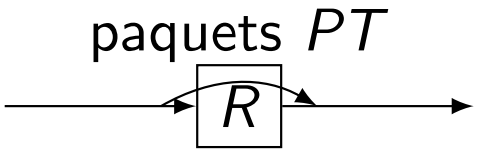




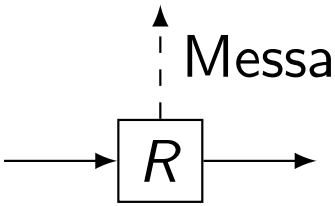
Propriétés d'un routeur

Propriétés d'un routeur R, du point de vue de S, pour un protocole de test PT donné (UDP, TCP, etc.) :

Propriété 1 R **transmet** les paquets PT.

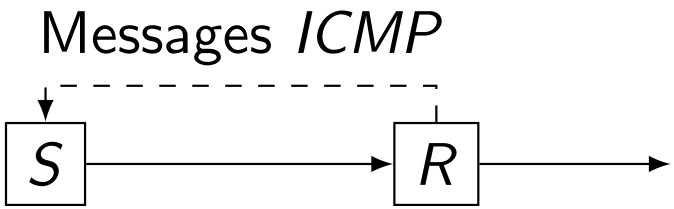


Propriété 2 R est "**coopératif**" pour les paquets PT.



R crée les messages $ICMP$ déclenchés par les paquets PT.

Propriété 3 Les messages $ICMP$ créés par R sont reçus par S.



Algorithme initial

Principe

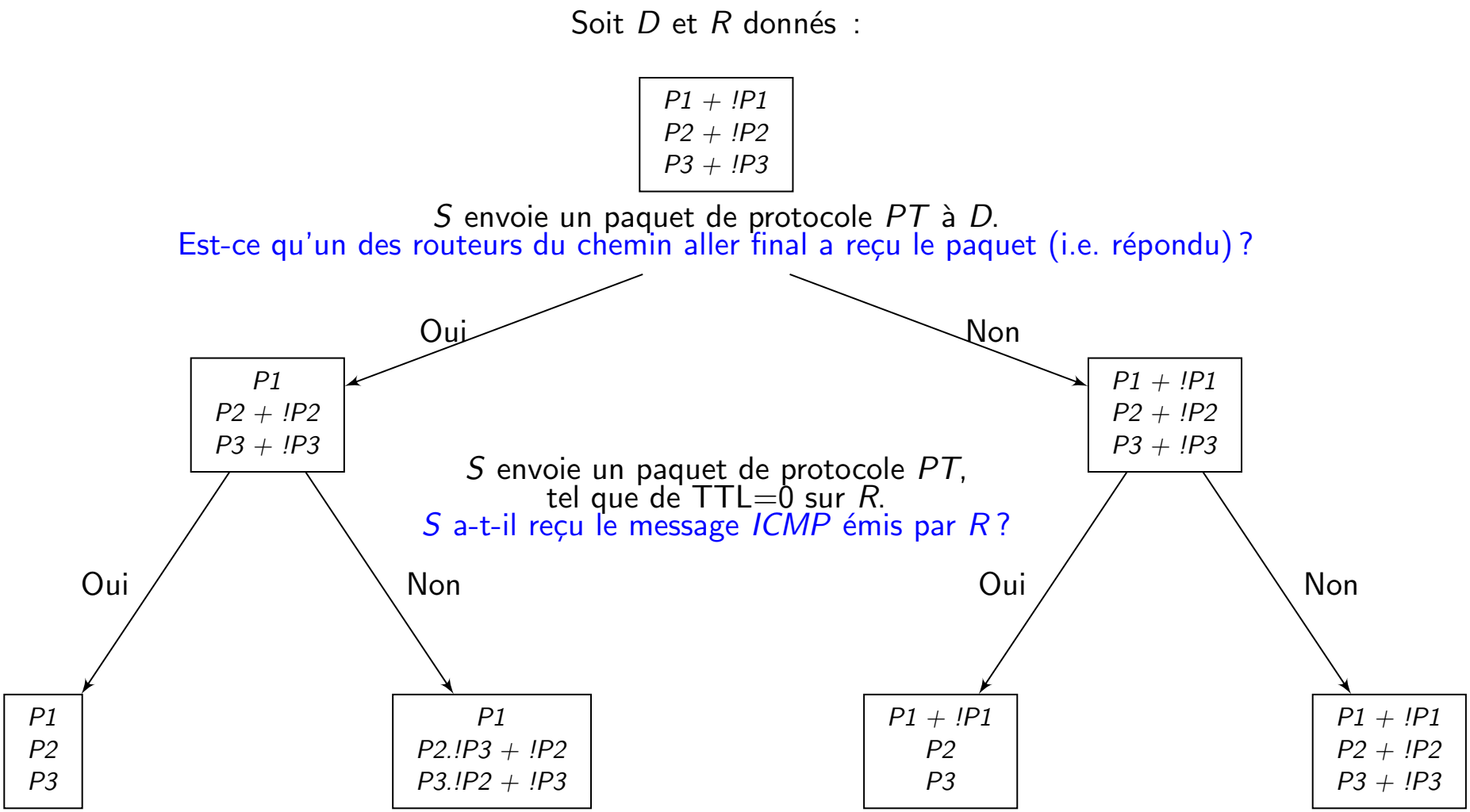
Caractériser le comportement de chaque routeur d'un chemin en fonction des **éléments mesurables** par l'utilisateur.

Deux étapes majeures pour chaque routeur R :

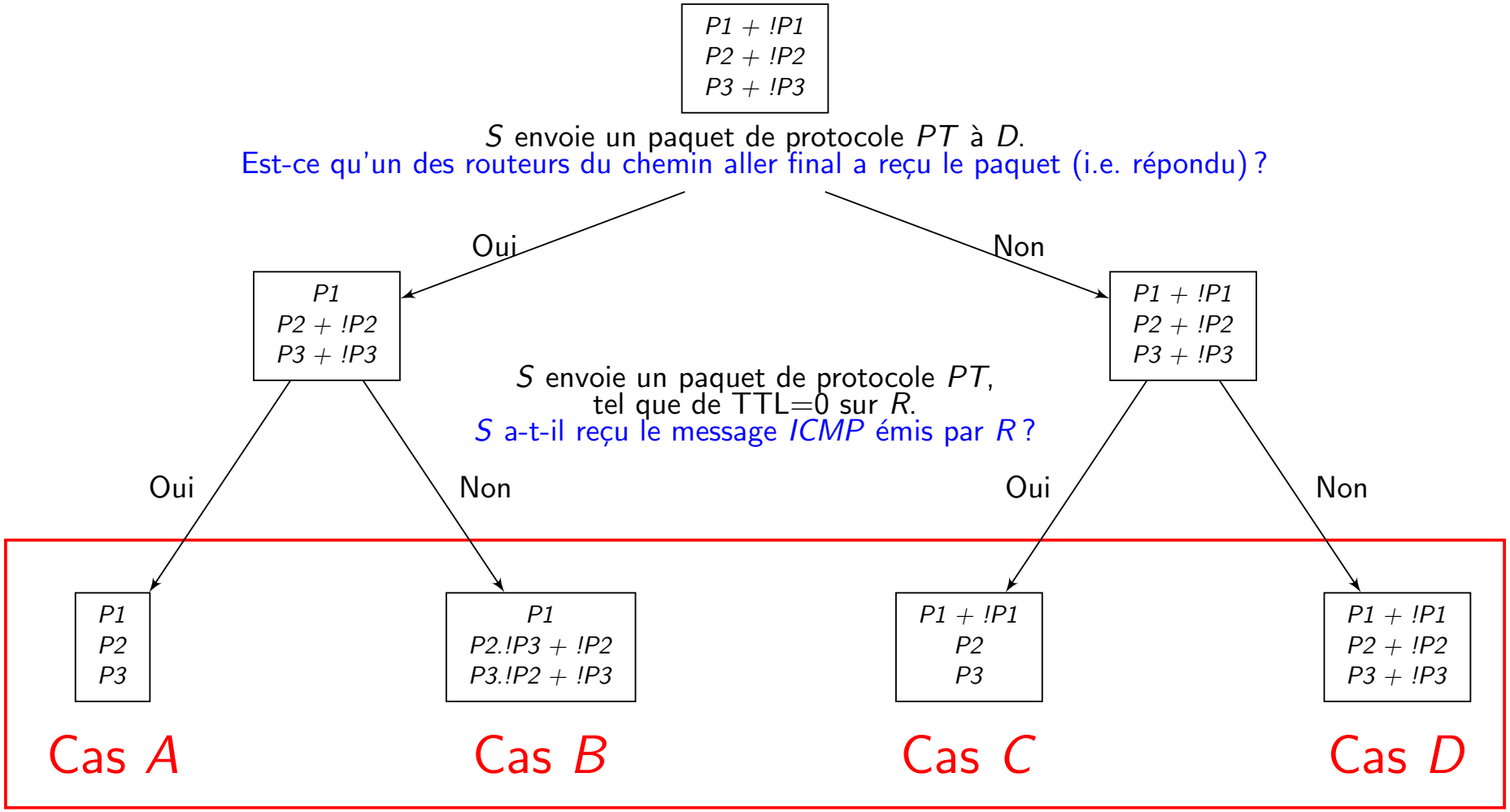
Chemin aller à travers R : mesurable par la réception d'une réponse d'un routeur du chemin aller final (propriété *P1*).

Chemin ICMP retour depuis R : mesurable par la réception d'un message *ICMP* de R (propriétés *P2* et *P3*).

Mise en œuvre de l'algorithme initial



Classification initiale



Principe de raffinement des catégories

Une des propriétés est indépendante du protocole des paquets de test.

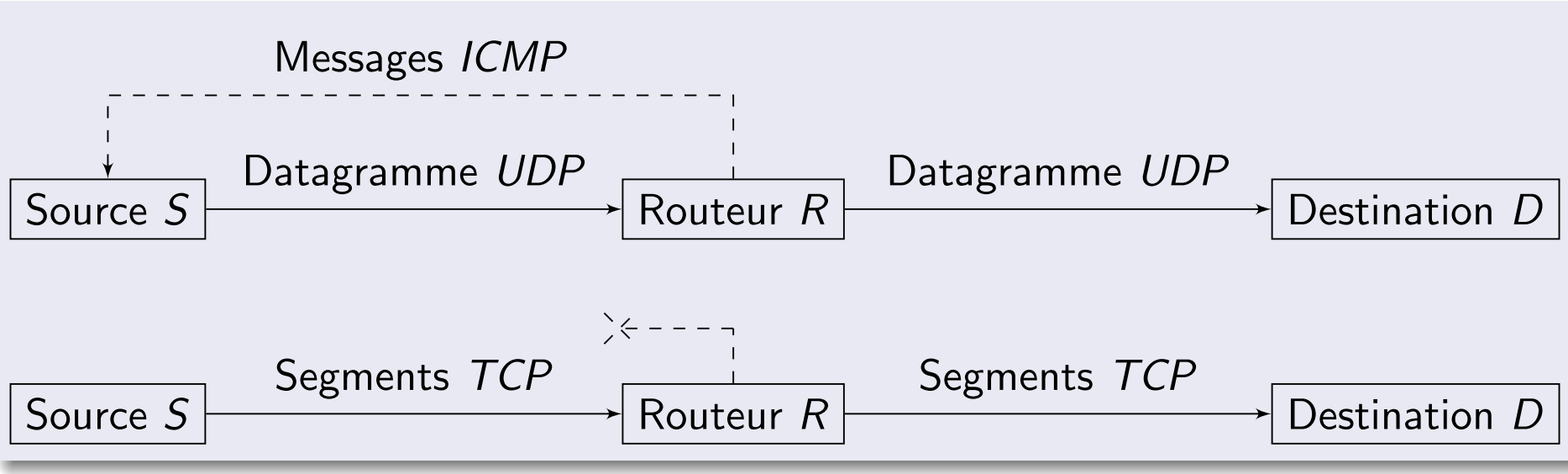
Propriété 3 : les messages *ICMP* créés par *R* sont reçus par *S*.

Algorithme de raffinement

IBTrack compare la propriété *P3* pour **plusieurs protocoles de test**.

Traceroute		IBTrack	Traceroute		IBTrack
Saut	UDP	Cas UDP	Saut	TCP	Cas TCP
...	...		...	...	
3	33.33.33.33	A	3	33.33.33.33	A
4	44.44.44.44	A	4	* * *	B
5	55.55.55.55	A	5	55.55.55.55	A
6	66.66.66.66	A	6	66.66.66.66	A
...	...		...	...	

Exemple de raffinement



Raffinement

Le test *UDP* permet d'affirmer que **le chemin ICMP retour n'abandonne pas les messages ICMP**.

Déduction

Le routeur **R ne crée pas le message ICMP pour le protocole TCP**.

Mesures grande échelle sur Internet

Sources Des nœuds *Planet-lab* et un accès FAI.
31 points de mesure autour du globe (majoritairement en Europe).

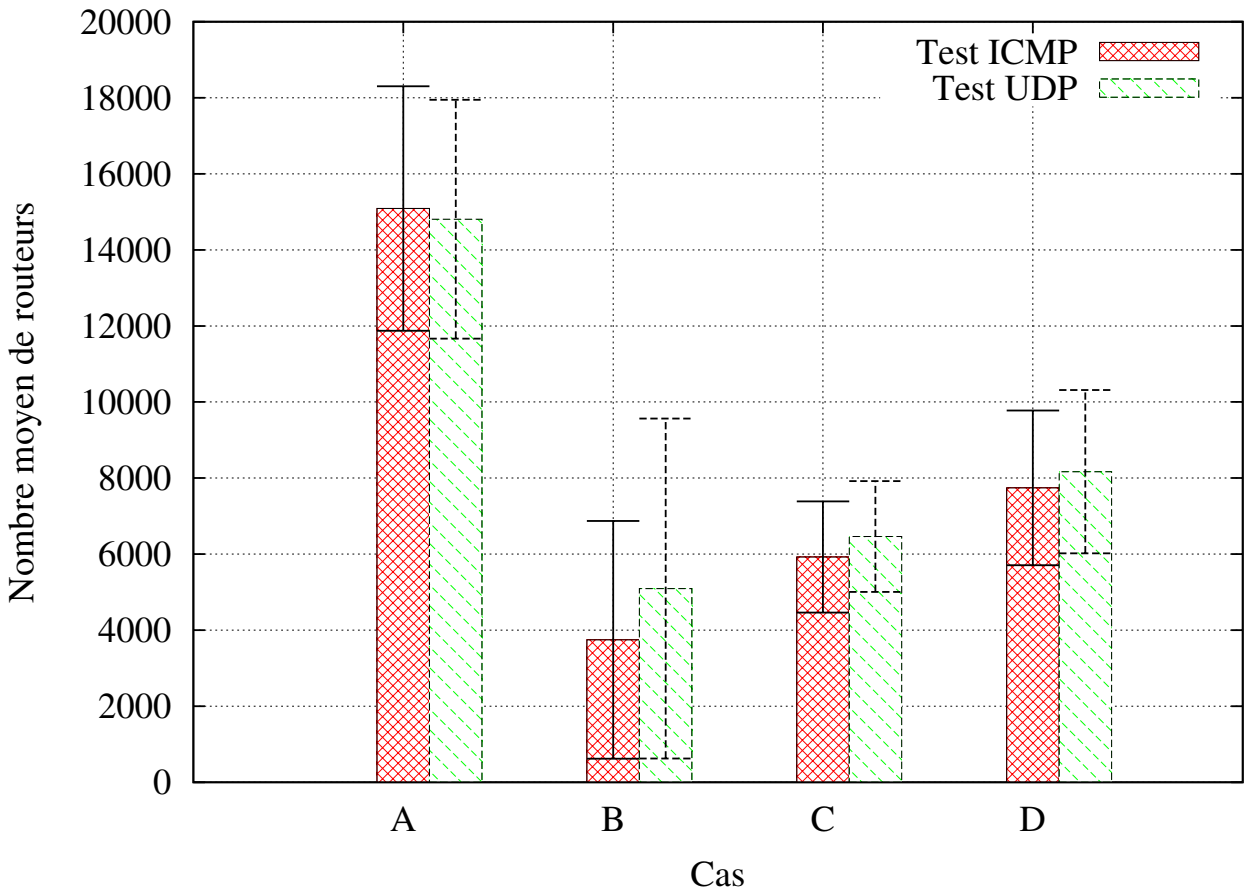
Destinations Jeu de données *CAIDA*.
$\approx$ 10 000 adresses IPv4 routable.

Methodologie Mesures type *traceroute*.
Chaque source sonde chacune des adresses IP destinations avec *ICMP*, *UDP* (et *TCP*).

Challenge

Identifier que deux routes sont identiques (**même suite de routeurs**) pour le raffinement (paragraphe 6.3).

Classification initiale des routeurs



Seulement la moitié des routeurs rencontrés ($\approx$ 33 000) fonctionnent correctement vis-à-vis d'ICMP.

Contributions

Formalisation Définition des parties du réseau et **caractérisation d'un routeur par trois propriétés** mesurables par un utilisateur seul.

IBTrack Classifie le comportement des routeurs, avec un **raffinement possible pour les situations problématiques**.

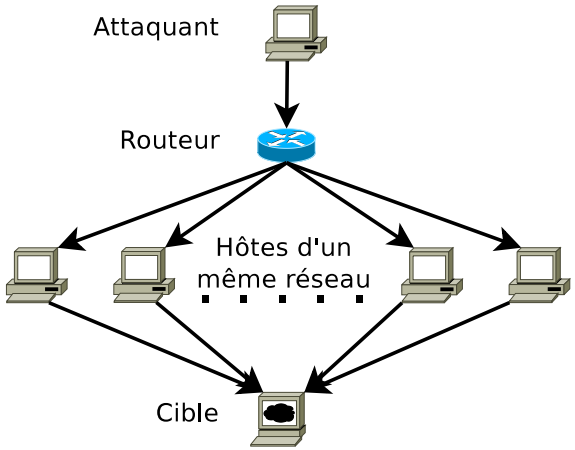
Mesures Classification à grande échelle des routeurs d'Internet.

Publication

"IBTrack : An ICMP Black holes Tracker"
L. Jacquin, V. Roca, M. Ali Kaafar, J.-L. Roch, et F. Schuler. *IEEE Global Communications Conference (GLOBECOM'12)*, 2012.

Plan

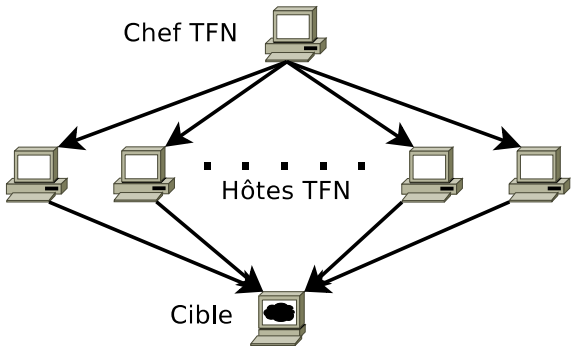
ICMP comme vecteur d'attaque (1/2)



Attaque Smurf, Déni de Service Distribué (DDoS) (CERT Advisory CA-1998-01)

- trouver un routeur autorisant ICMP sur l'adresse de diffusion ;
- envoyer un message ICMP "echo request" en usurpant l'IP source par l'adresse de la cible ;
- toutes les machines du sous–réseau répondent un message ICMP "echo reply" à la cible.

ICMP comme vecteur d'attaque (2/2)



Attaque "Tribe Flood Network" (botnet ICMP - DDoS) (CERT Incident Note IN-99-04)

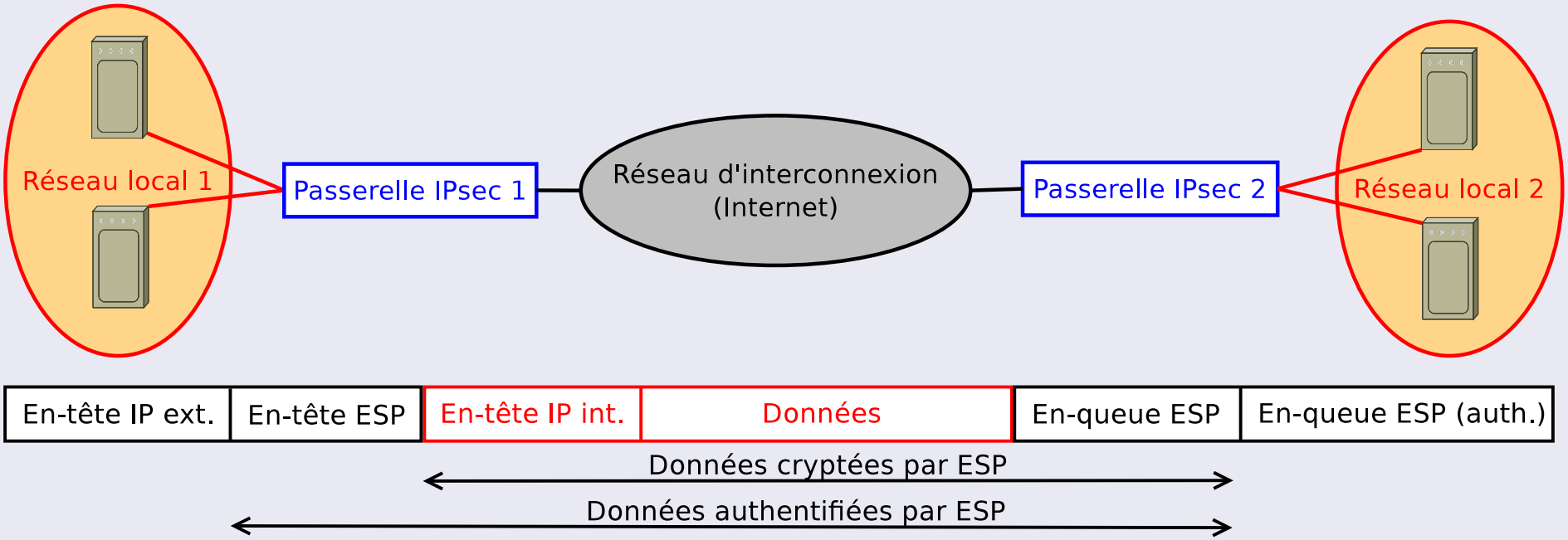
Le chef synchronise les hôtes pour l'attaque sur la cible.

Et bien d'autres encore...

"Ping of Death" (Hacking : the art of exploitation, 2nd edition).
Attaques ICMP sur les connexions TCP (RFC 5927).

Présentation d'IPsec

Cas d'utilisation SHIVA : mode tunnel et protocole ESP



Précédentes attaques sur IPsec (Paterson et al.)

Essentiellement des attaques sur les primitives cryptographiques.

Modèle de l'attaquant

Ni cryptanalyse, ni force brute

Primitives cryptographiques sûres.

Protocoles d'échanges de clés robustes.

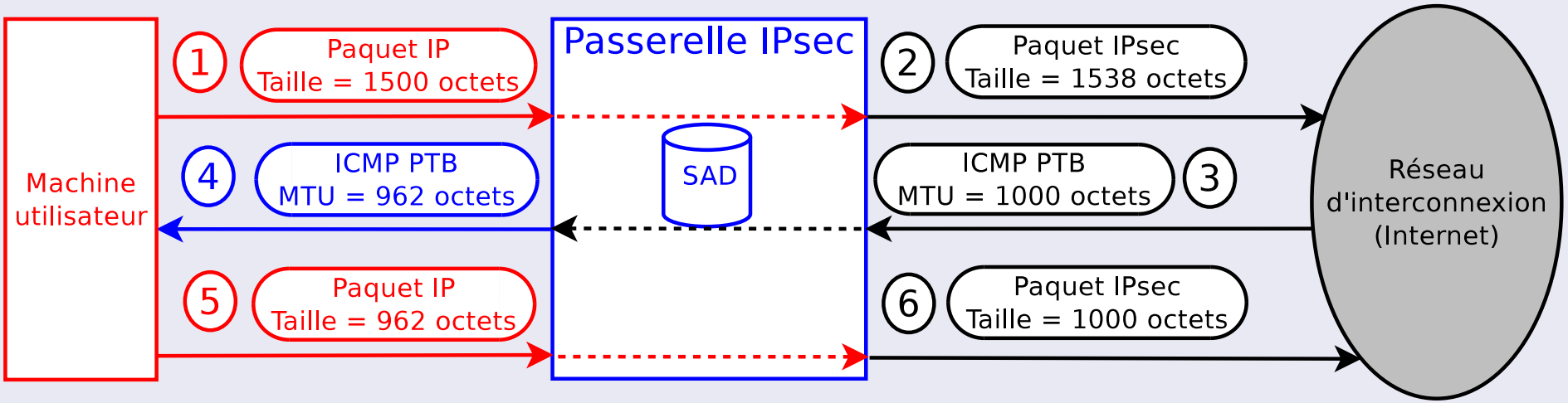
Possibilité sur le réseau

Écoute des communications.

Émission de paquets.

PMTUd dans le cas d'IPsec

Échanges ICMP pour le PMTUd avec une passerelle IPsec (RFC 4301)

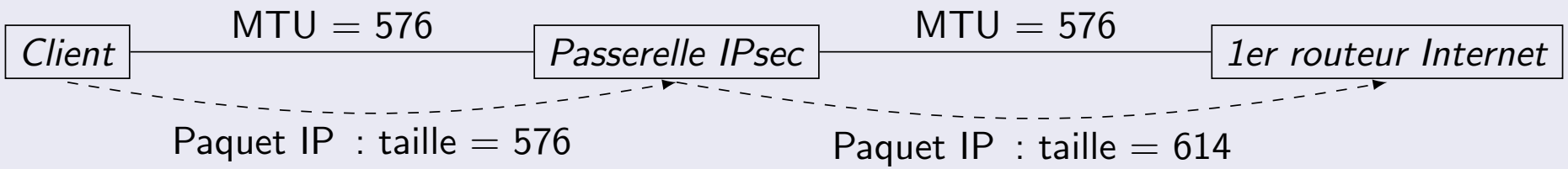


Taille des en–têtes IPsec/ESP dans notre configuration : 38 octets.

Stockage du PMTU dans la SAD par IPsec.

Fondement de notre attaque

Cas d'un réseau physique limité



Cas légitime de blocage dû à la présence d'un tunnel en IPv4.
Valable aussi en IPv6.

Défaut dans les normes de l'IETF

Pas de prise en compte du **surcoût des en–têtes d'un tunnel** dans IP/ICMP.

But de l'attaquant (chapitre 7)

Faire croire que le réseau est dans ce cas limite.

Principe de notre attaque

Deux étapes majeures

Réduction du PMTU du tunnel : mise à une valeur arbitraire du PMTU stocké dans la SAD.

Propagation du PMTU arbitraire : la passerelle IPsec crée des messages ICMP PTB si les paquets IP sont trop gros.

Principe de notre attaque

Deux étapes majeures

Réduction du PMTU du tunnel : mise à une valeur arbitraire du PMTU stocké dans la SAD.

Propagation du PMTU arbitraire : la passerelle IPsec crée des messages ICMP PTB si les paquets IP sont trop gros.

Mécanisme de protection d'IPsec

IPsec vérifie que les messages ICMP reçus par la passerelle ont été déclenchés par des paquets issus du tunnel.

Solution pour l'attaquant

Compléter les messages ICMP PTB par du trafic chiffré.

Illustration de l'attaque

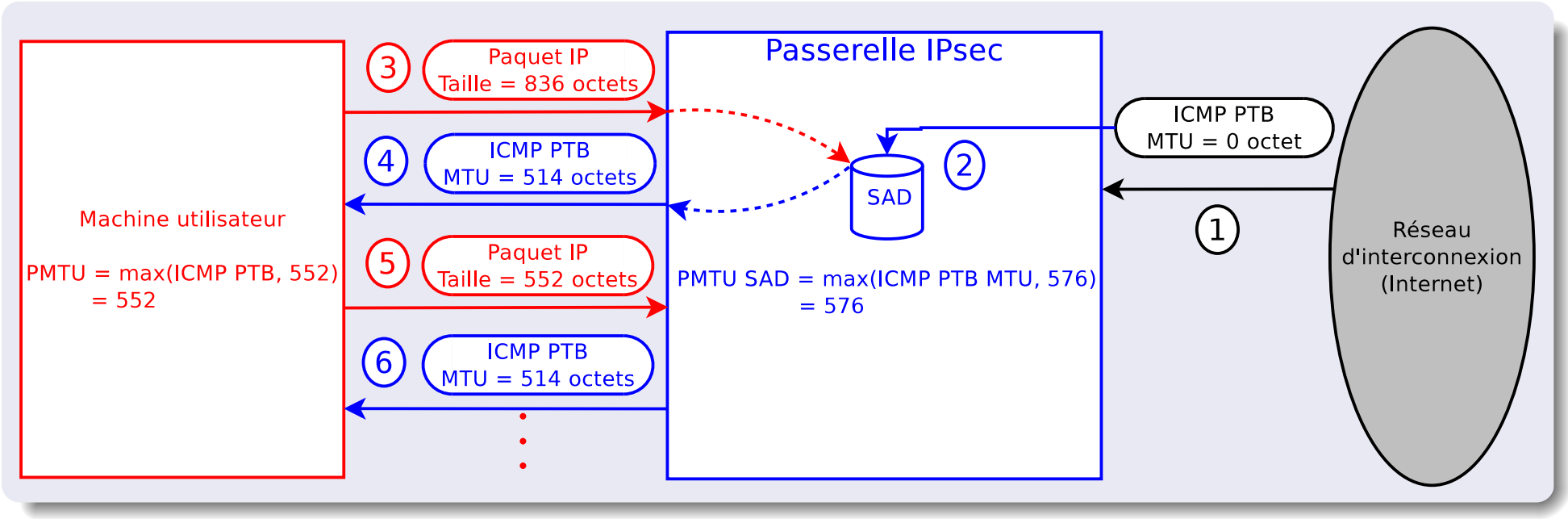
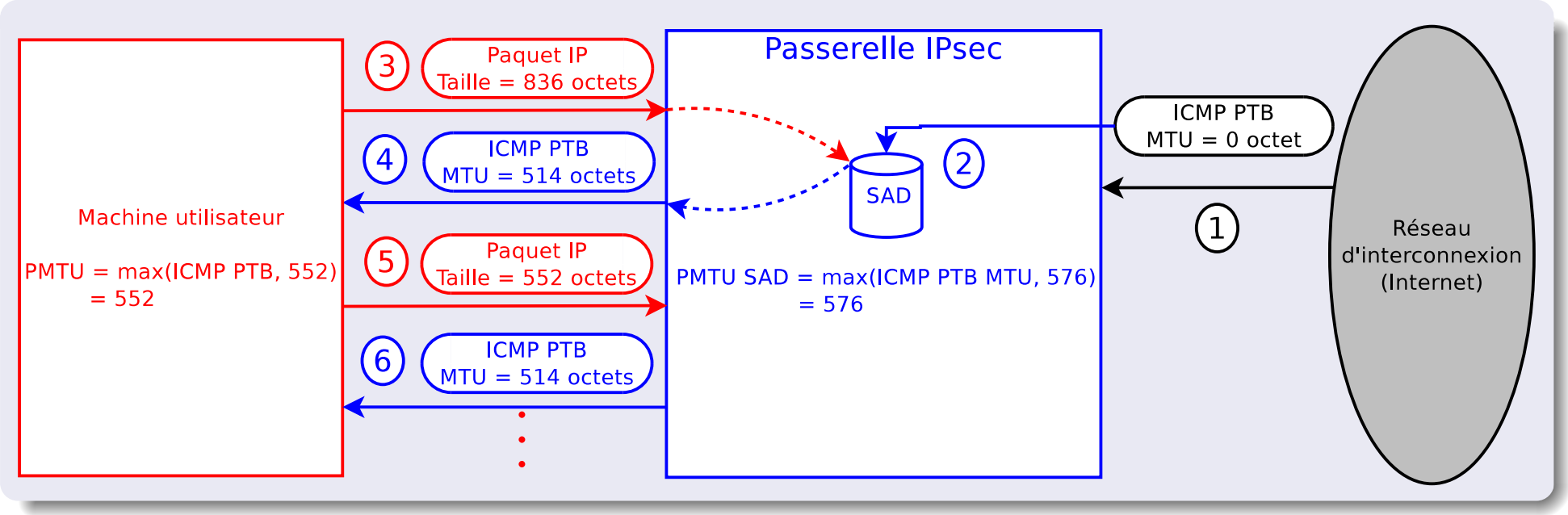


Illustration de l'attaque



Mise en œuvre de l'attaque sur Debian "Squeeze" (Linux 3.2.1)

Impossibilité d'établir une connexion SSH via un tunnel IPsec.

Contre-mesures existantes

Bit DF (RFC 791)

Autoriser la fragmentation par les routeurs (uniquement en IPv4).

PLPMTUd (RFC 4821)

Ne plus utiliser les messages ICMP PTB pour évaluer le PMTU.
Introduit un délai de 6 secondes lors de l'établissement de la connexion.

Configuration de la machine utilisateur

Prendre en compte la taille des en–têtes du tunnel (**à condition de la connaître**).

Contre-mesures existantes

Bit DF (RFC 791)

Autoriser la fragmentation par les routeurs (uniquement en IPv4).

PLPMTUd (RFC 4821)

Ne plus utiliser les messages ICMP PTB pour évaluer le PMTU.
Introduit un délai de 6 secondes lors de l'établissement de la connexion.

Configuration de la machine utilisateur

Prendre en compte la taille des en–têtes du tunnel (**à condition de la connaître**).

Dégradation des performances

Plus de déni de service, mais une forte **réduction du débit** utilisable.

Nos propositions de contre-mesures

Authentification des messages ICMP

Mise en place d'une architecture du réseau permettant de garantir l'**authenticité des messages ICMP**.

Nouvelle évaluation du PMTU dans IPsec

Sondage du PMTU entre passerelles IPsec ne reposant pas sur les messages ICMP PTB du réseau.

Contributions

Analyse de sécurité Découverte d'un **défaut dans les normes IP/ICMP**.

Mise en place de l'attaque **Déni de service** ou réduction du débit selon la configuration de l'utilisateur.

Contre–mesures Sécuriser Internet.
Évaluation du PMTU sans messages ICMP dans IPsec.

Publication

"ICMP : an Attack Vector against IPsec Gateways"
L. Jacquin, V. Roca et J.-L. Roch. En cours de soumission à *IEEE International Conference on Communications (ICC'14)*.

Plan

Conclusions

Conception et développement de l'architecture en rupture

Implantation d'un prototype avec un accélérateur matériel cryptographique.

ICMP pour la performance des communications réseau

Conception et développement d'IBTrack.
Mesures à grande échelle sur Internet.

ICMP comme vecteur d'attaque des communications réseau sécurisées

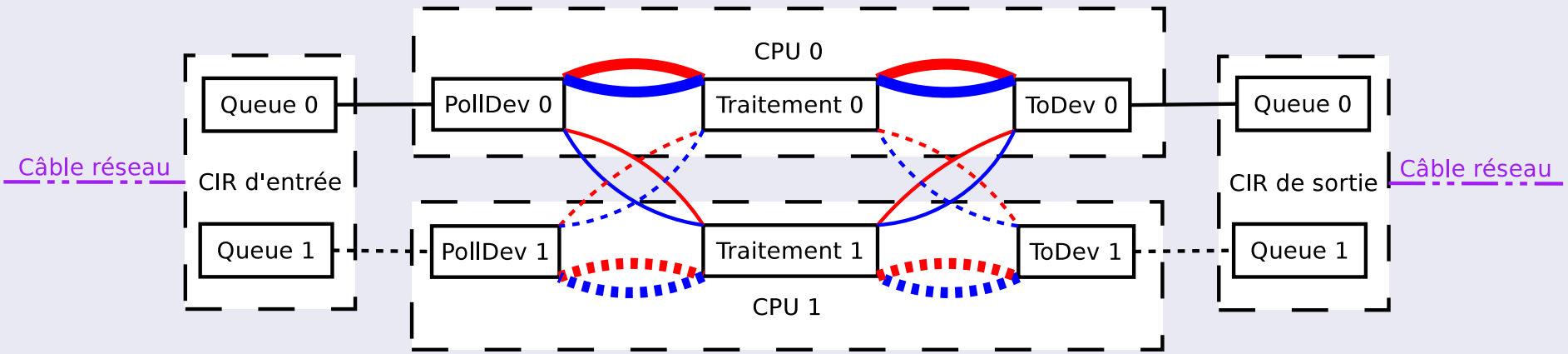
Mise en évidence et implantation d'une attaque par message ICMP
PTB sur les passerelles IPsec en mode tunnel.

Perspectives

Sécurisation des communications

L'ubiquité d'Internet (et de ses menaces) nécessite la mise en place de solutions de sécurité.

Parallélisation des traitements réseau par vol de travail



Vers une couche réseau (IP) uniquement de routage

Considérer un réseau non sécurisé comme une boite noire.