Grands réseaux

Multi-services network security

Cédric Llorens

Some references

Les cours sont disponibles à :

https://sites.google.com/site/courscedricllorens/home

Quelques références Internet:

http://www.ripe.net/
http://www.nanog.org/

Pratique de la gestion de réseau :

Bonnes pratiques de configuration de BGP, ANSSI

Le Journal MISC :

http://www.miscmag.com/

Some references

Les Tableaux de bord de la sécurité réseau, 3ème édition, 562 pages, C.Llorens, L.Levier, D.Valois, B.Morin, Eyrolles, 2010, http://www.eyrolles.com

Mesure de la sécurité "logique" d'un réseau d'un opérateur de télécommunications, http://pastel.paristech.org/archive/00001492/

Méthodes d’analyse et d’ évaluation des risques

Quelques références

Les cours sont disponibles à :

https://sites.google.com/site/courscedricllorens/home

http://groups.google.fr/group/tableau-de-bord-de-la-securite-reseau

National Institute of Standards and Technology

Risk Management Guide for Information Technology Systems

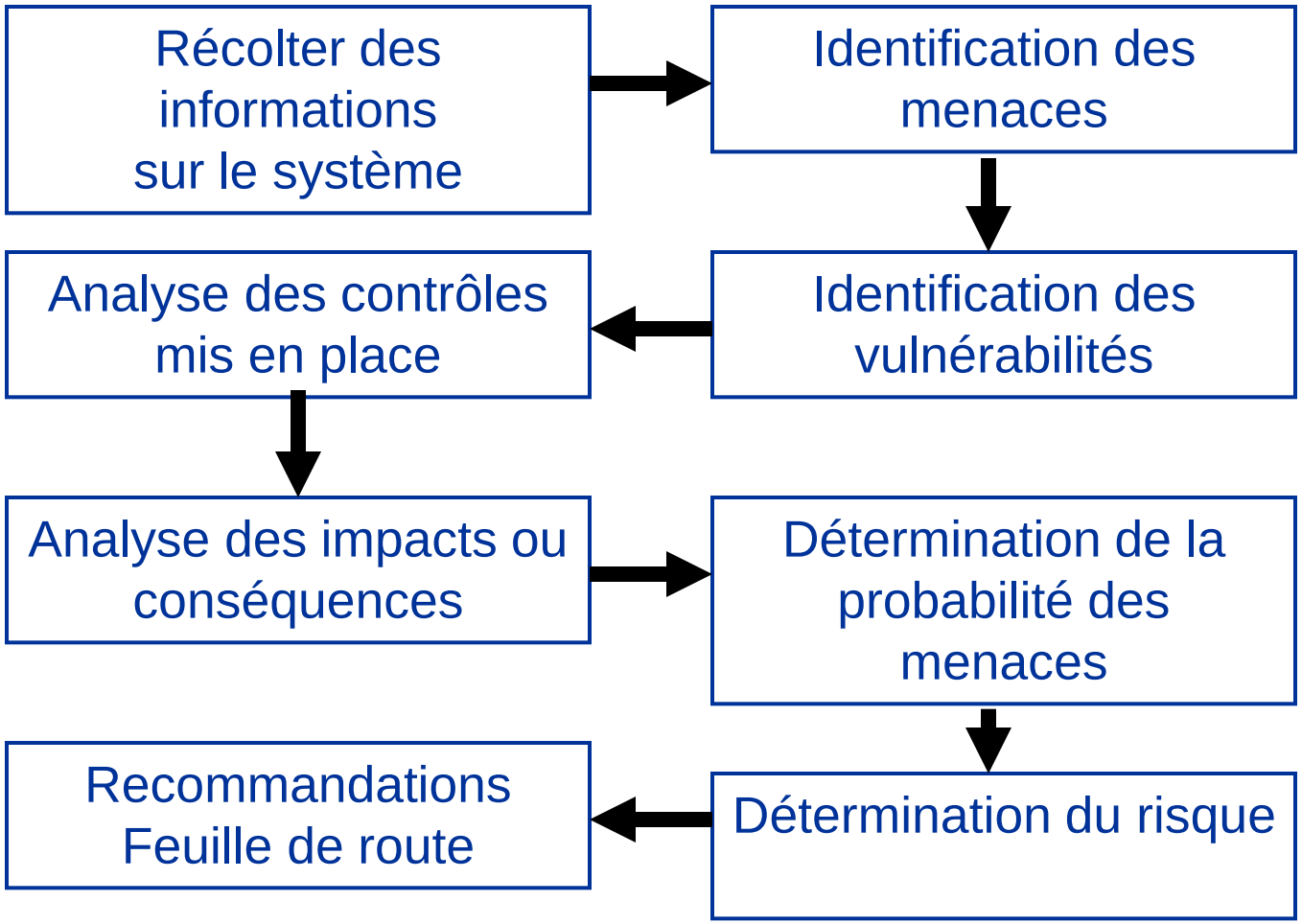
http://www.nist.org

National Aeronautics ans Space Administration

Probabilistic Risk Assessment methodology

http://www.nasa.gov

Analyse & évaluation du risque



Récolter des informations sur le système

Il faut déterminer le périmètre et le contenu du système, il s'agit donc de réaliser un inventaire exhaustif de ce système et des ressources associées:

- Les locaux.
- Les composants hardware et software.
- Les réseaux.
- Les données.
- Les utilisateurs & interfaces (flowchart, application, etc.).
- Les documents (diagrammes réseaux, politiques de sécurité, etc.).

Les moyens pour y parvenir sont nombreux, on retiendra plus particulièrement :

- Les questionnaires électroniques (orientés évaluation du risque).
- Les interviews de personnes clés (récolte d'information dans leur contexte).
- L'utilisation d'outils de détection (méthodes proactives).

Identification des menaces

Il faut déterminer les sources de menace possibles qui peuvent utiliser une vulnérabilité de sécurité. Parmi les sources de menace les plus classiques, nous retiendrons :

• Les menaces naturelles : inondations, tremblements de terre, tornades, etc.

• Les menaces humaines : intentionnelles ou non intentionnelles, lancer des attaques, faire des erreurs, etc.

• Les menaces environnementales : perte de courant au niveau d'une région ou d'un pays, pollution, etc.

Identification des menaces

Source de menace	Motivation	Actions
Hacker, cracker	Challenge	Hacking, social engineering, etc.
Computer Criminal	Money	System intrusion, fraudulent act, etc.
Terrorist	Destruction Revenge	Bomb, System penetration, information warfare, etc.
Industrial espionage	Economic Money	Information theft, social engineering, Unauthorised system access
Personnel de l'entreprise	Curiosité Ego Money	Fraud, system penetration, system unauthorised access, theft, etc.

Analyse & évaluation du risque

Identification des vulnérabilités

Il faut identifier les vulnérabilités du système par des techniques très variées selon la nature du système:

• Récupérer les anciens audits de sécurité, ou analyses de risques, rapports d'anomalies si ils existent.

• Mener un audit de sécurité:

  • Interne: on se place à l'intérieur du système avec des droits d'administration (System Security Scanner pour analyser la sécurité interne d'un système d'exploitation)

  • Externe: on se place à l'extérieur du système sans droits spécifiques (Internet Security Scanner ou Nessus pour analyser la robustesse d'un système face à une pénétration externe).

Analyse & évaluation du risque

A Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization (NIST).

In other words, a Risk is a combination of :

- Threat (menace),
- Vulnerability (vulnérabilité),
- Consequence (conséquence).

Risk (T_i, V_i, C_i)

Analyse & évaluation du risque

- Find the vulnerabilities.
  - V1, V2, …
- Associate an impact status to each vulnerability:
  - Define impact status : High-Impact, Medium-Impact, Low-Impact, No-Impact
  - Associate : V1 -> High-Impact, V2 -> Low-Impact, etc.
- Compute probabilities associated to impact status:
  - P(High-Impact), P(Medium-Impact), P(Low-Impact), P(No-impact)
- Associate a consequence value for each impact status probability:
  - P(High-Impact)1 -> C1, P(Medium-Impact)2 -> C2 ….
- Compute a risk:
  - Sum (i) (Pi * Ci)

Détermination de la probabilité des menaces

Bienvenue dans le monde des probabilités !!

On a T_i, V_i, mais quelle est la probabilité P_i qu'une menace T_i exploite une vulnérabilité de sécurité V_i?

Quelques rappels :

Soit (O,R) un espace probabilisable, une probabilité P est une application de R sur R+ tel que P(O)=1 (axiomatique de Kolmogorov), pour tout A<R, B<R

P(AuB) = P(A)+P(B) - P(A^B)

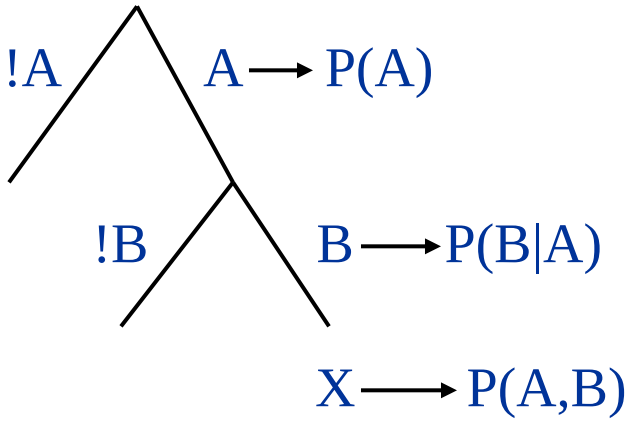
P(AuB) = P(A)+P(B) si P(A^B) = 0, A et B sont alors mutuellement exclusifs (ne peut pas arriver en même temps).

P(AuB) = P(A)+P(B)-P(A)*P(B), A et B sont indépendants.

Analyse & évaluation du risque

Détermination de la probabilité des menaces

Théorème de Bayes et construction d'arbre d'événements !!



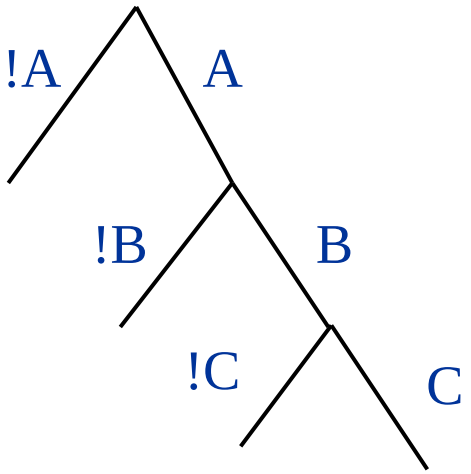
P(A,B)= P(B|A) * P(A) si dépendance de B par rapport à A

Sinon, P(A,B) = P(B) * P(A), A et B sont indépendants.

Analyse & évaluation du risque

Détermination de la probabilité des menaces

Généralisation du théorème de Bayes et construction d'arbre d'événements !!



(1) P(A,B,C) = P(A) * P(B,C/A) d'après la formule de bayes

On a aussi P(B,C) = P(B) * P(C/B) d'après la même formule de bayes. Si on conditionne par rapport à l'événement A, on obtient :

(2) P(B,C/A) = P(B/A) * P(C/B,A)

D'où en combinant (1) et (2), on a : P(A,B,C) = P(A) * P(B/A) * P(C/B,A)

Analyse & évaluation du risque

Détermination de la probabilité des menaces

Exercice :

Un individu accédant un routeur (telnet ou ssh) et essayant un « mot de passe » au hasard est refoulé 999 sur 1000.

Sachant que le routeur accepte trois essais de « mot de passe » avant de couper la connexion, quelle est la probabilité de se connecter au routeur par hasard ?

Analyse & évaluation du risque

On peut alors définir le risque comme:

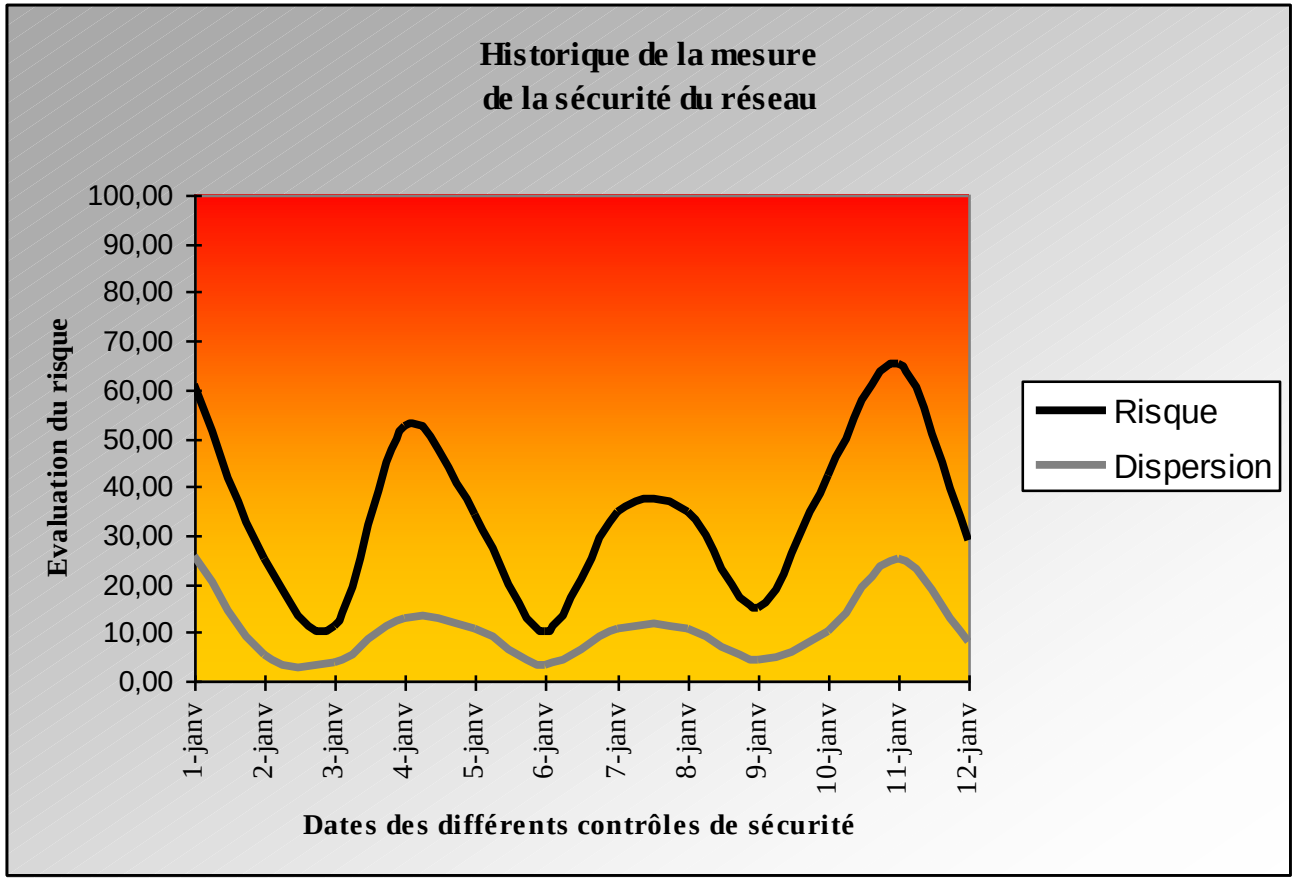
$$Risk = \sum_{i=1}^{n} P_i * C_i$$

$$E(X) = \sum_{i=1}^{n} P_i(X = x_i) * x_i$$

Probabilité de la menace	Conséquence (Impact faible) (10)	Conséquence (Impact moyen) (50)	Conséquence (Impact fort) (100)
Forte (1.0)	Risque Faible 10*1.0=10	Risque Moyen 50*1.0=50	Risque Fort 100*1.0=100
Moyen (0.5)	Faible 10*0.5=5	Moyen 50*0.5=25	Risque Moyen 100*0.5=50
Faible (0.1)	Risque Faible 10*0.1=10	Risque Faible 50*0.1=5	Risque Faible 100*0.1=10

Analyse & évaluation du risque

Détermination du risque



$$E(X) = \sum_{i=1}^{n} P_i(X = x_i) * x_i$$

$$\sigma(X) = \sqrt{E(X) - E(X)^2}$$

Analyse & évaluation du risque

Recommandations
Feuille de route

Exercice : Estimation du risque d'un routeur

- Soit V1 un bug de la fonction SSH permettant d'avoir un accès au routeur et pouvant générer un impact fort.
- Soit V2 un bug de la fonction BGP permettant d'avoir un accès au routeur et pouvant générer un impact fort.
- Soit V3 des droits d'accès mal positionnés permettant d'avoir accès au système de fichiers et pouvant générer un impact moyen.

En considérant qu'une attaque peut échouée, donner l'arbre d'événements ainsi qu'une valeur de risque pour le routeur :

- on notera que les événements sont équiprobables à chaque branche.
- on prendra les valeurs de conséquence du tableau précédent.

Eléments de sécurité d'une réseau multi-services

Agenda

- Security principles

- Security of the routing protocols

- Security by routing high availibility

- Security mechanisms at level 2

- Security mechanisms at level 3

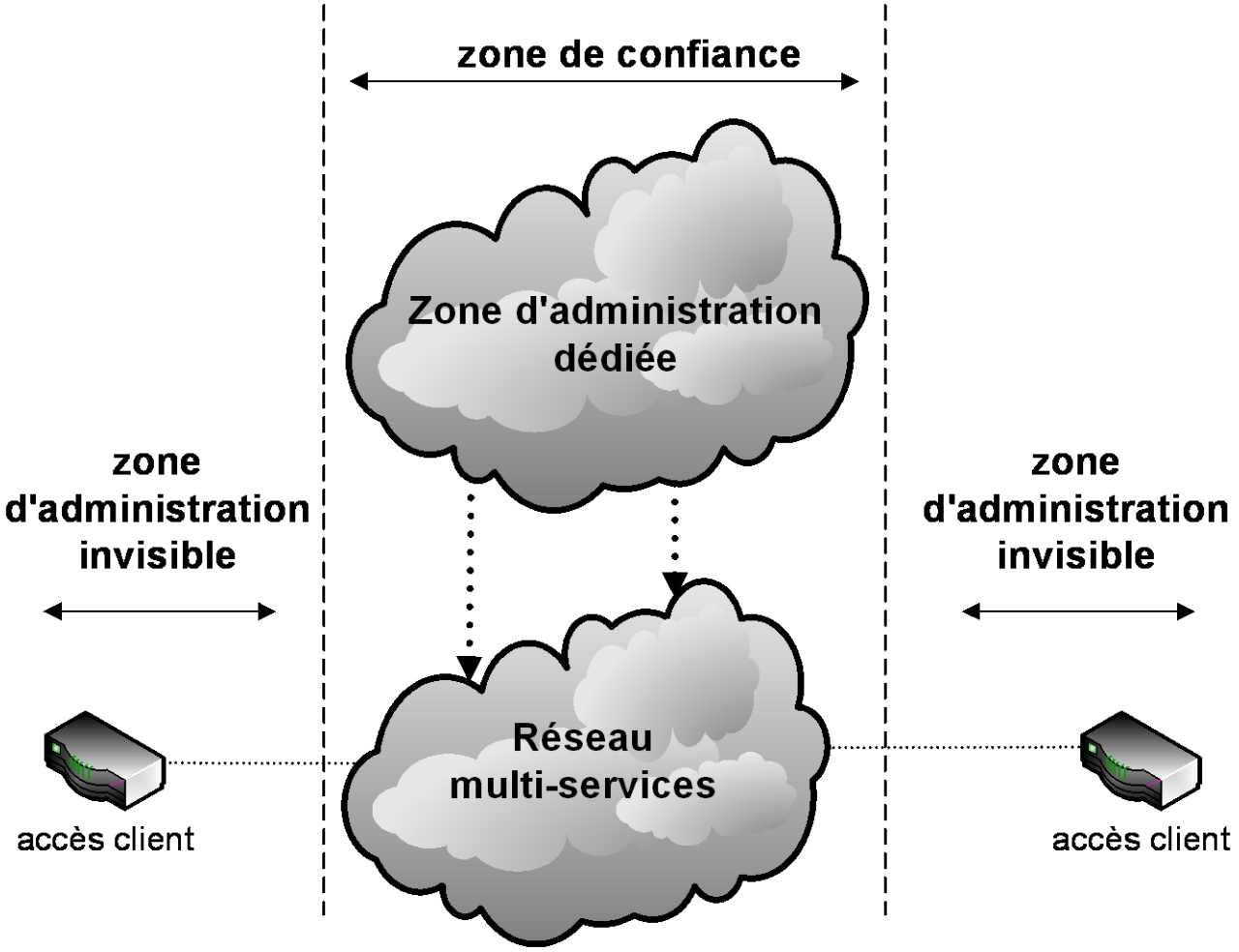
Agenda

Security principles

of a multi-services network

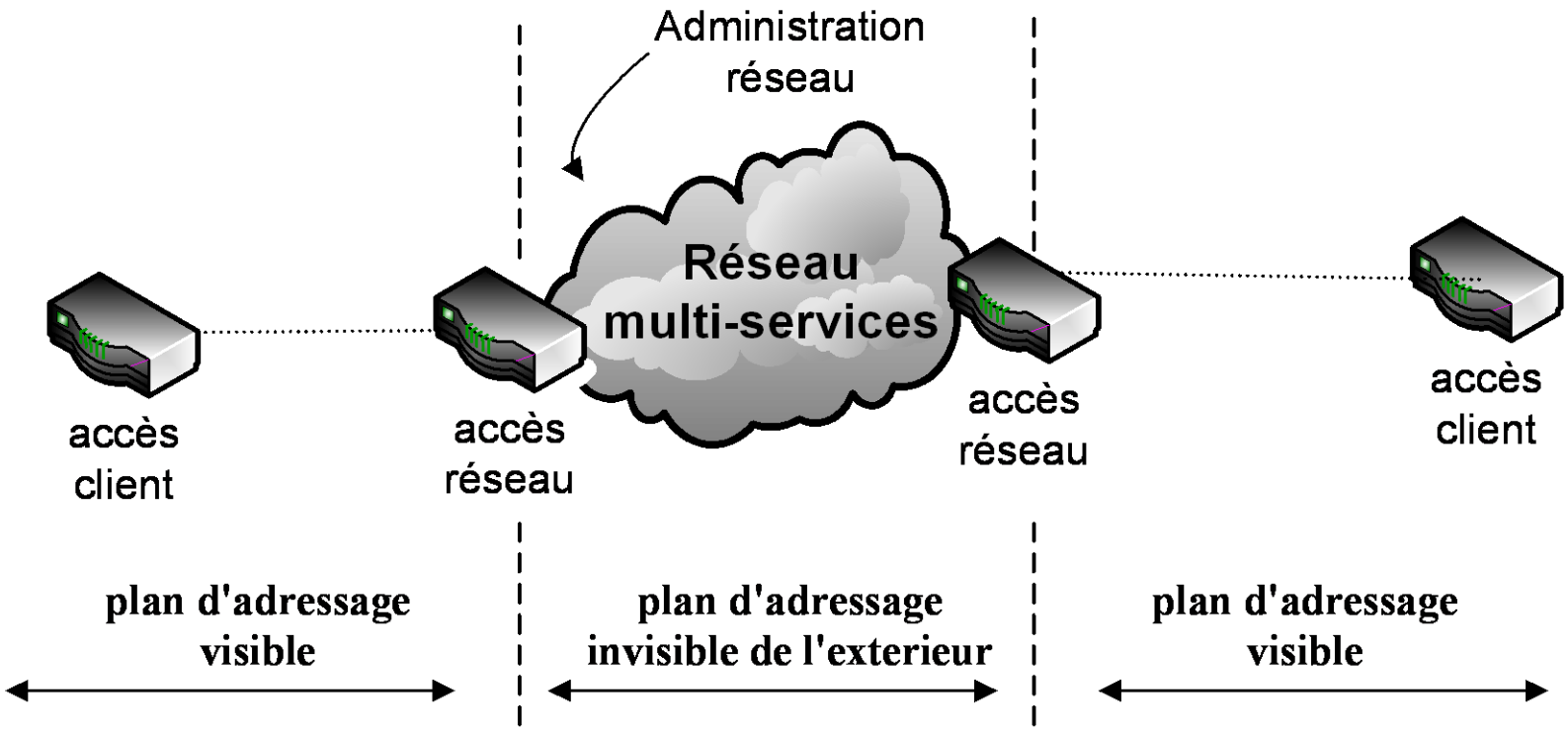
Security principles of a multi-services network

(Indépendance de la zone d ’administration)

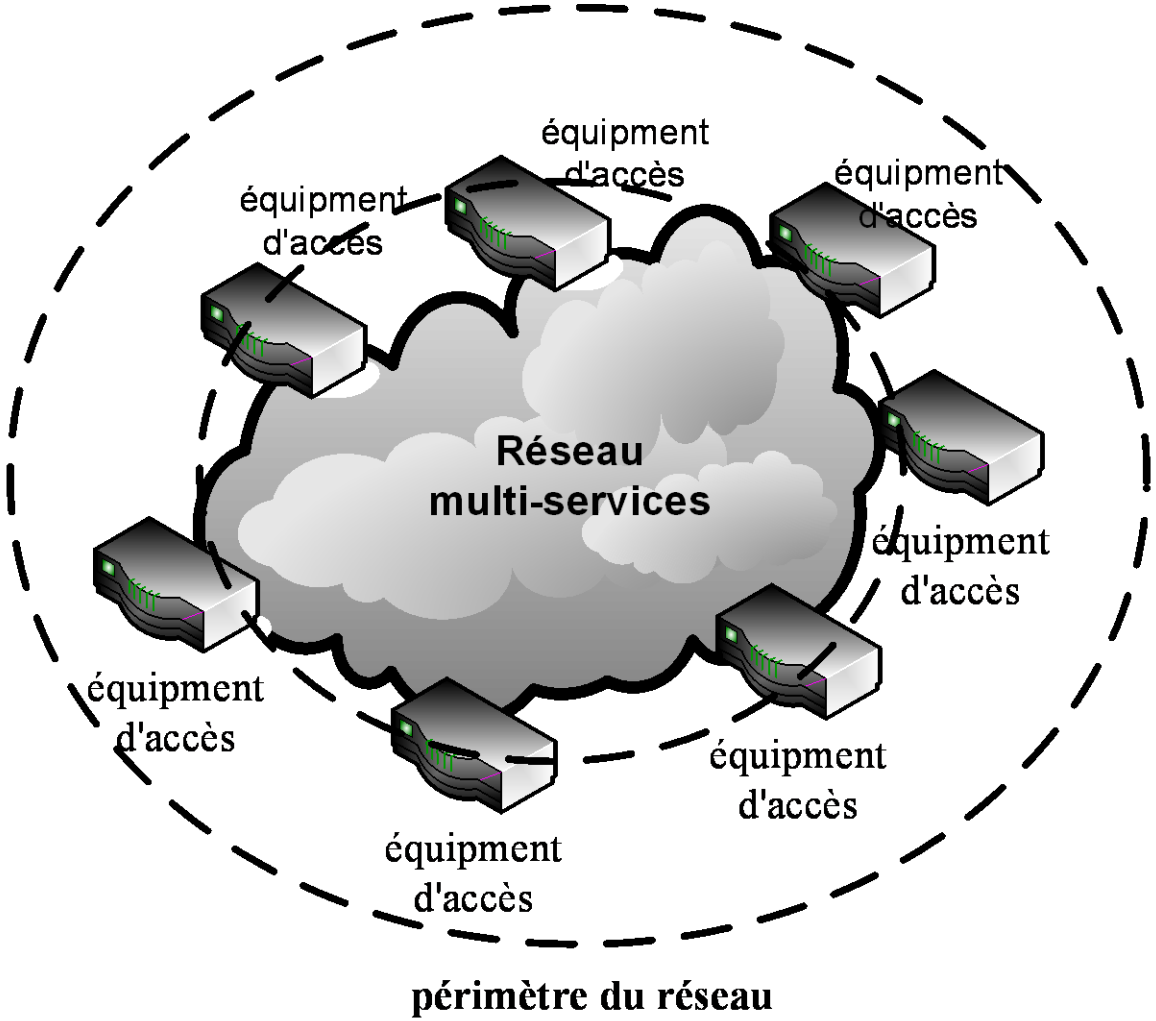


Security principles of a multi-services network

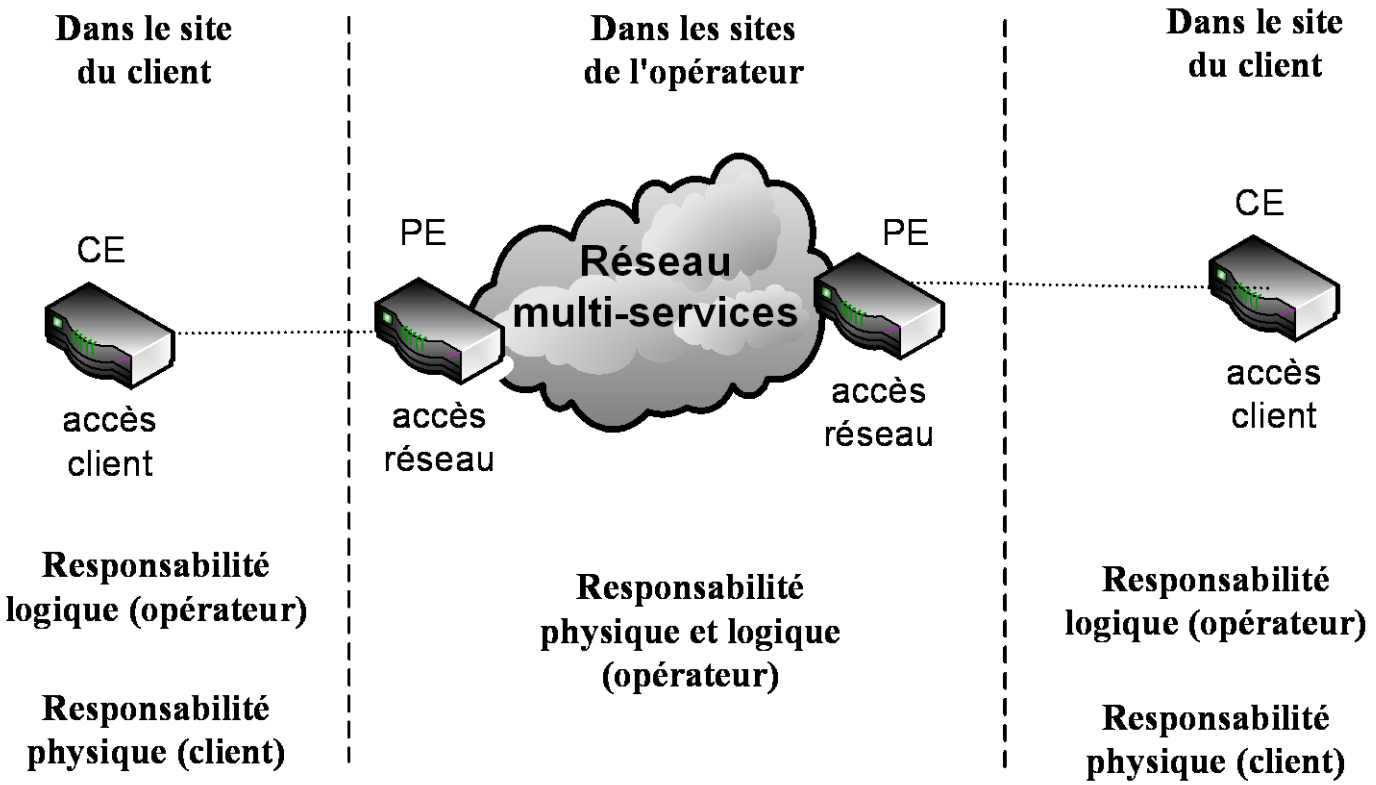
(Invisibilité du cœur de réseau)



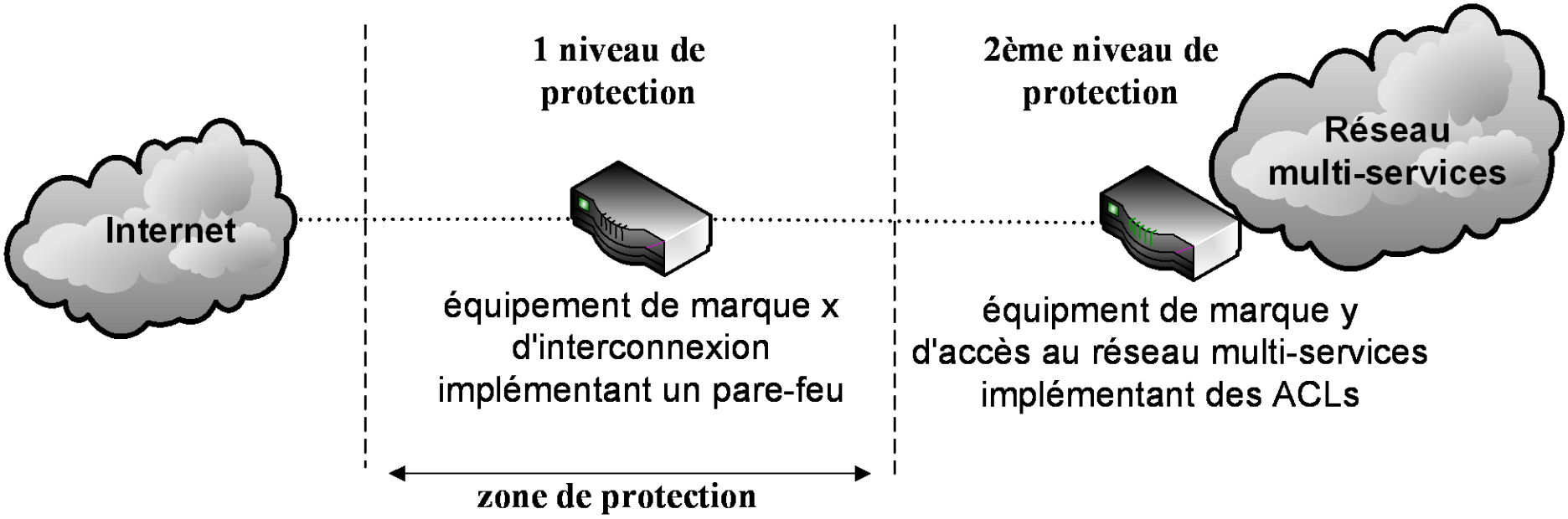
Security principles of a multi-services network
(Le maillon le plus faible)



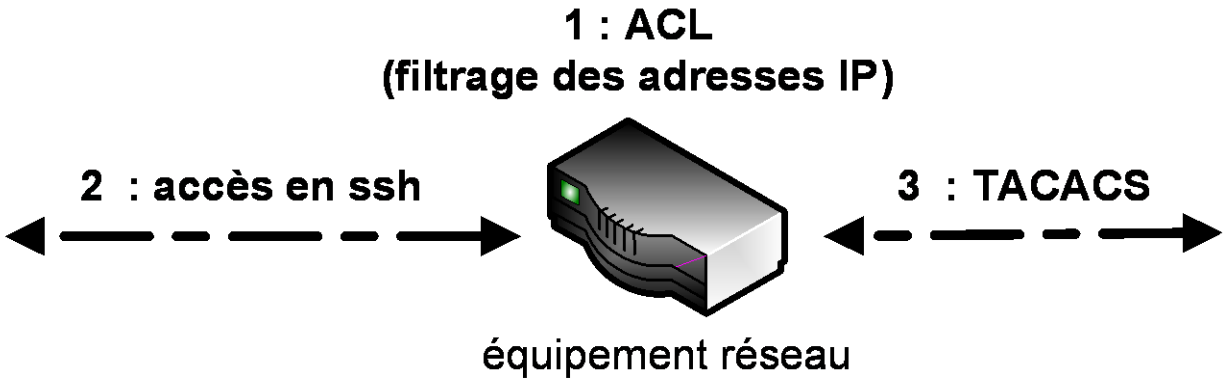
Security principles of a multi-services network
(La responsabilité physique et logique)



Security principles of a multi-services network
(La variété des protections)

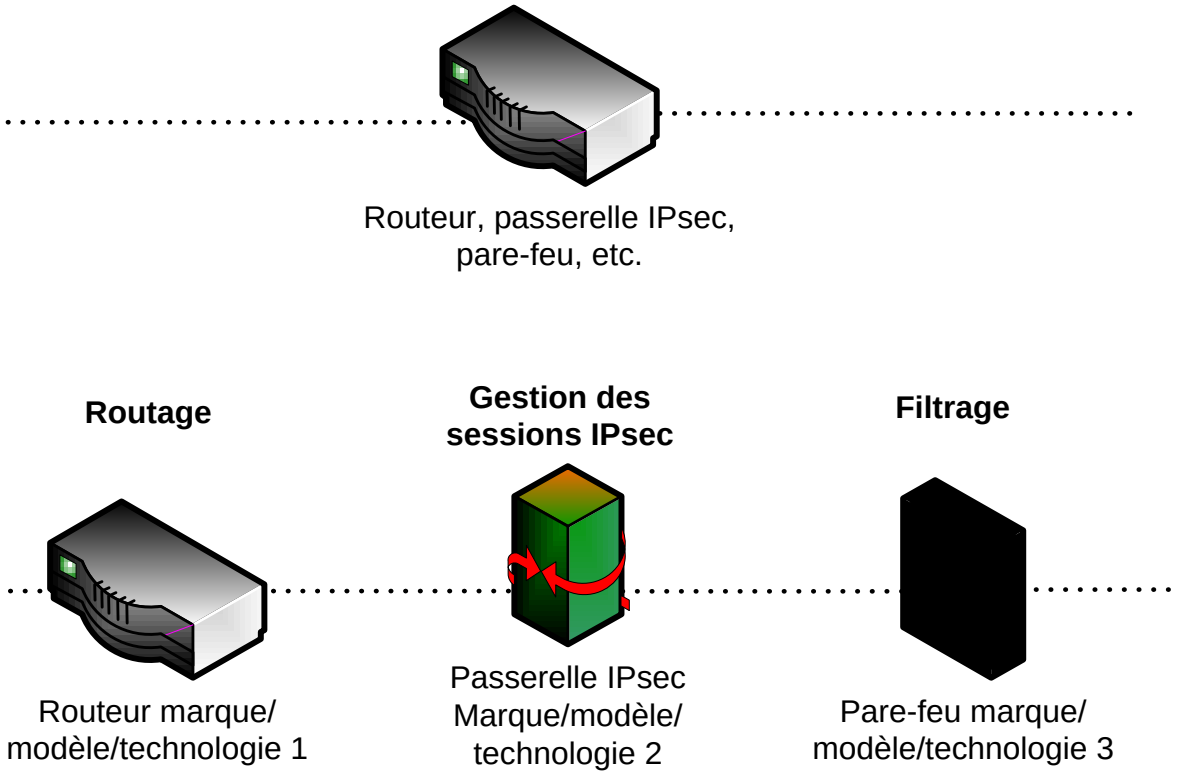


Security principles of a multi-services network
(La sécurité en profondeur)



- Un premier élément de sécurité filtre les adresses IP accédant à un équipement réseau par le biais d'ACL (Access Control List).
- Un deuxième élément de sécurité force l'accès à un équipement réseau à l'aide d'algorithmes de chiffrement tel que SSH (Secure Shell) afin d'assurer la confidentialité des données échangées.
- Un troisième élément de sécurité réalise une authentification liée à un profil d'accès et qui permet de générer des traces sur les commandes réalisées. La protocole TACACS permet de mettre en œuvre les trois AAA (Authentication Autorisation Accounting).

Security principles of a multi-services network
(La séparation des mécanismes de sécurité)



Security of the routing protocols

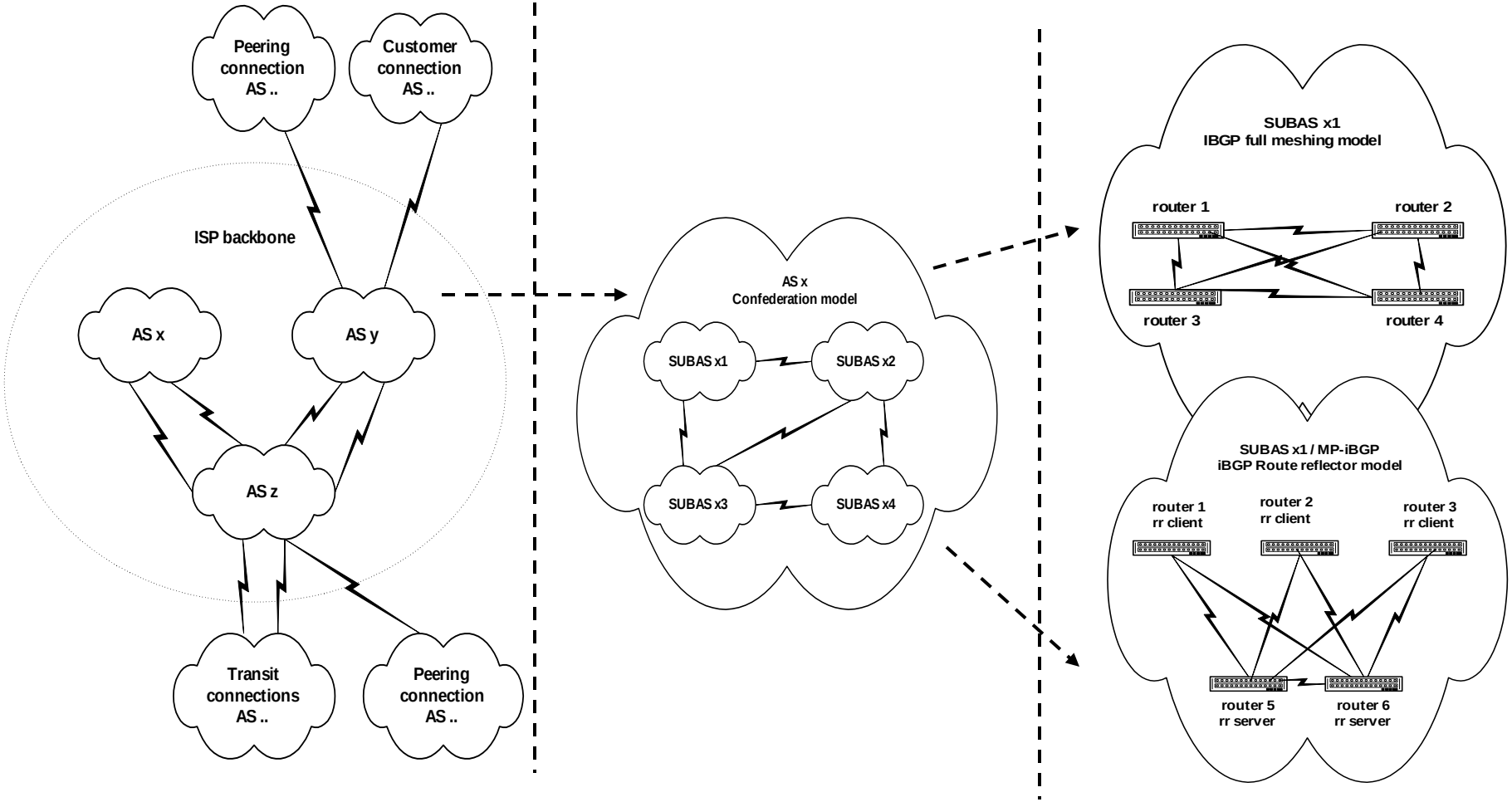
Présentation et sécurité du protocole **Exterior Gateway Protocol BGP**

Architecture et politique de routage interne & externe

Topology level 1

Topology level 2

Topology level 3



La sécurité du protocole BGP
Quels sont les moyens de protection actuels ?

neighbor {ip-address | peer-group-name} password string
Permet de définir un mot de passe pour une session BGP

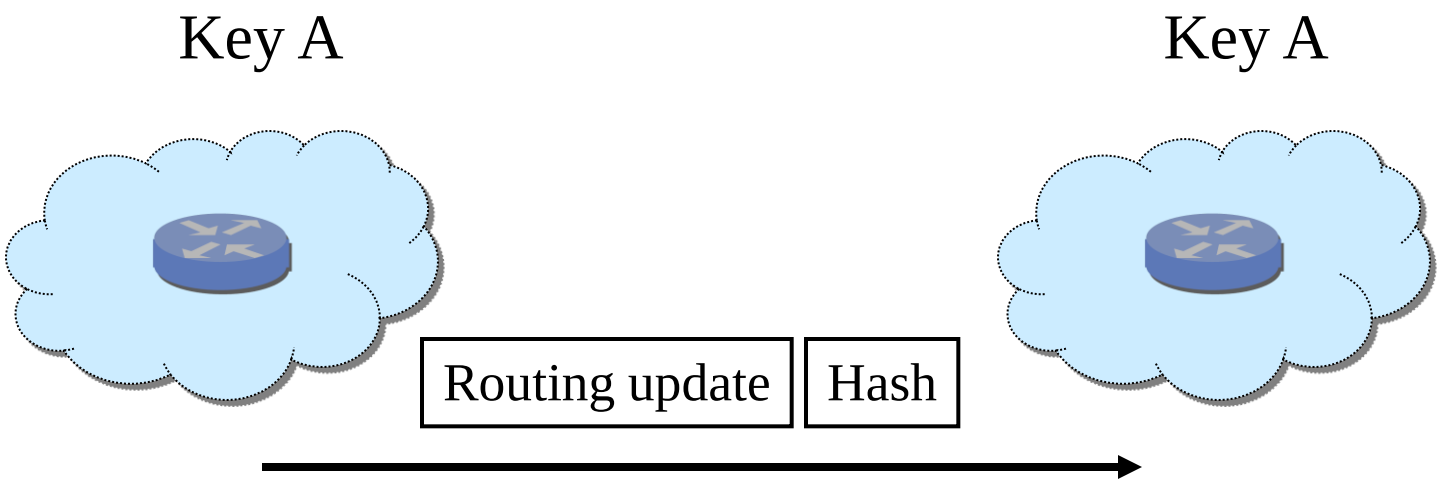
neighbor {ip-address | peer-group-name} filter-list access-list-number {in | out}
Permet de définir un filtre sur les systèmes autonomes pour une session BGP

neighbor {ip-address | peer-group-name} prefix-list prefix-listname {in | out}
Permet de définir un filtre sur les adresses IP pour une session BGP

neighbor {ip-address | peer-group-name} maximum-prefix maximum [threshold]
Limite le nombre de préfixes IP annoncés

neighbor {ip-address | peer-group-name} route-map route-map-name {in | out}
Permet d'appliquer une politique de route-map sur une session BGP
(note : it allows the network operator to configure and organize more modular policy definitions)

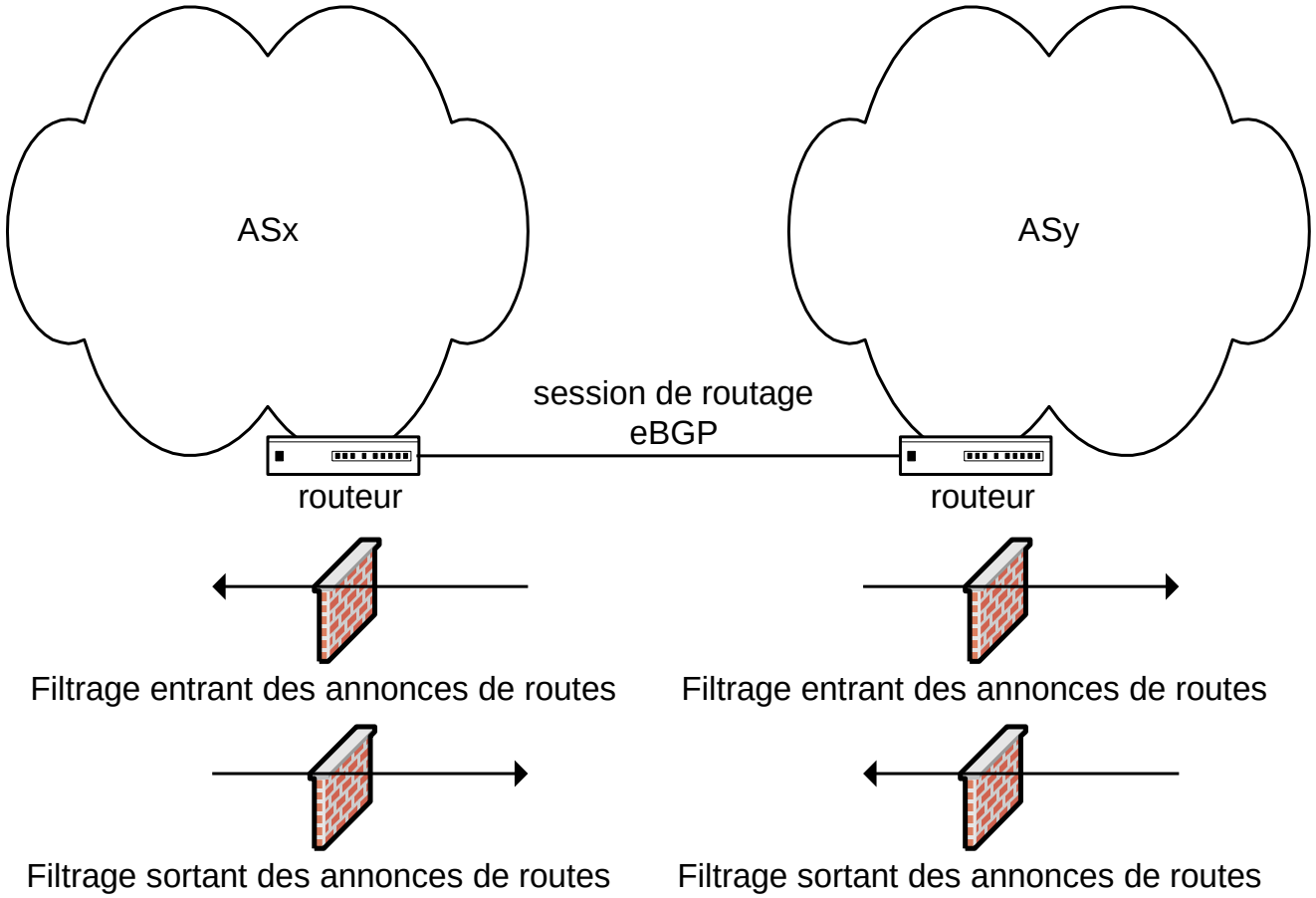
La sécurité du protocole BGP
Quels sont les moyens de protection actuels ?



Hash = MD5(Routing update, Key A)

Hash1 = MD5(Routing update, Key A)
Hash = Hash1 ?

La sécurité du protocole BGP
Quels sont les moyens de protection actuels ?



Suppression des AS privés, suppression des adresses privées, filtrage sur AS_PATH, etc.

La sécurité du protocole BGP
Quels sont les moyens de protection actuels ?

neighbor ip-address ttl-security hops hop-count
Permet de filtrer selon le TTL les mises à jour de routage.

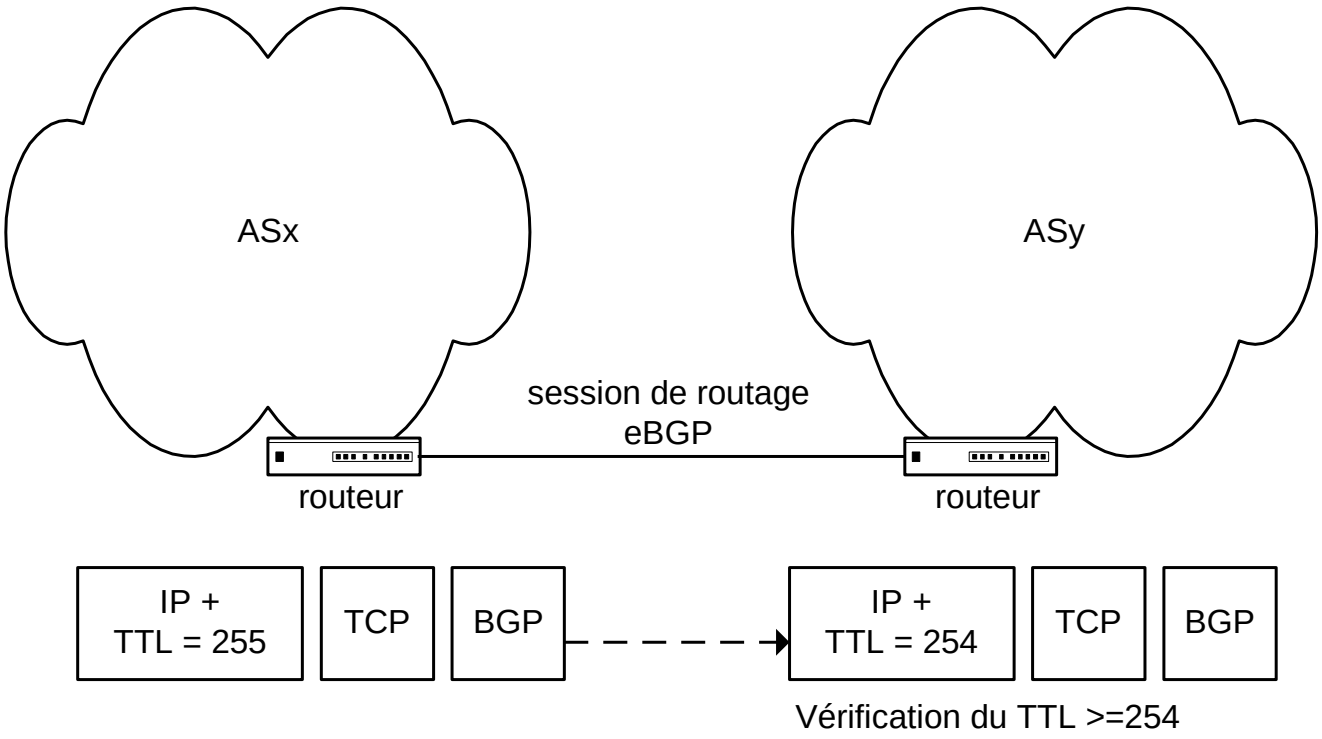
bgp dampening [half-life reuse suppress max-suppress-time] [route-map map]
Permet de définir une politique prenant en compte les instabilités des mises à jour de route

ip verify unicast reverse-path
Permet de prévenir l'usurpation d'adresses IP basé sur la table de routage. Elle s'applique sur une ou plusieurs interfaces réseaux :

```
interface FastEthernet 1
        ip address @ip1
        ip verify unicast reverse-path
```

La sécurité du protocole BGP
Quels sont les moyens de protection actuels ?

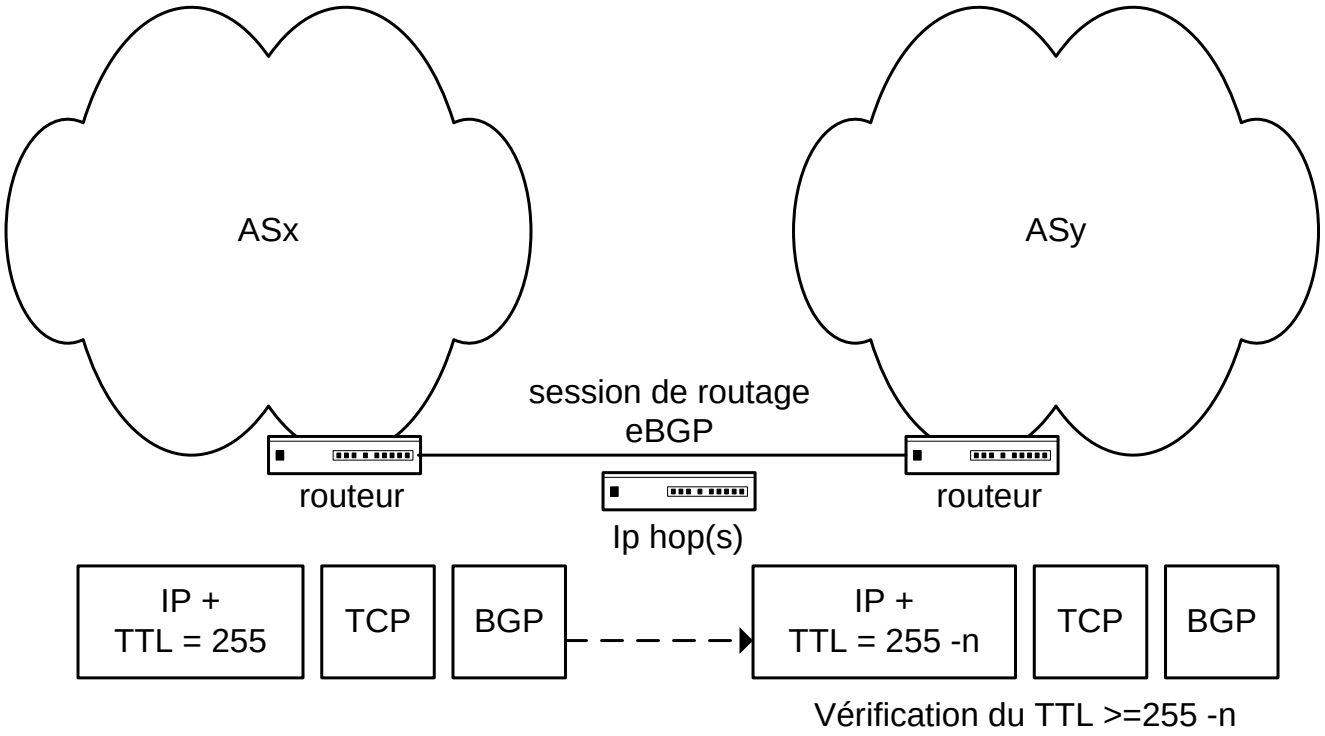
Vérification stricte du TTL : connexion directe avec le peer



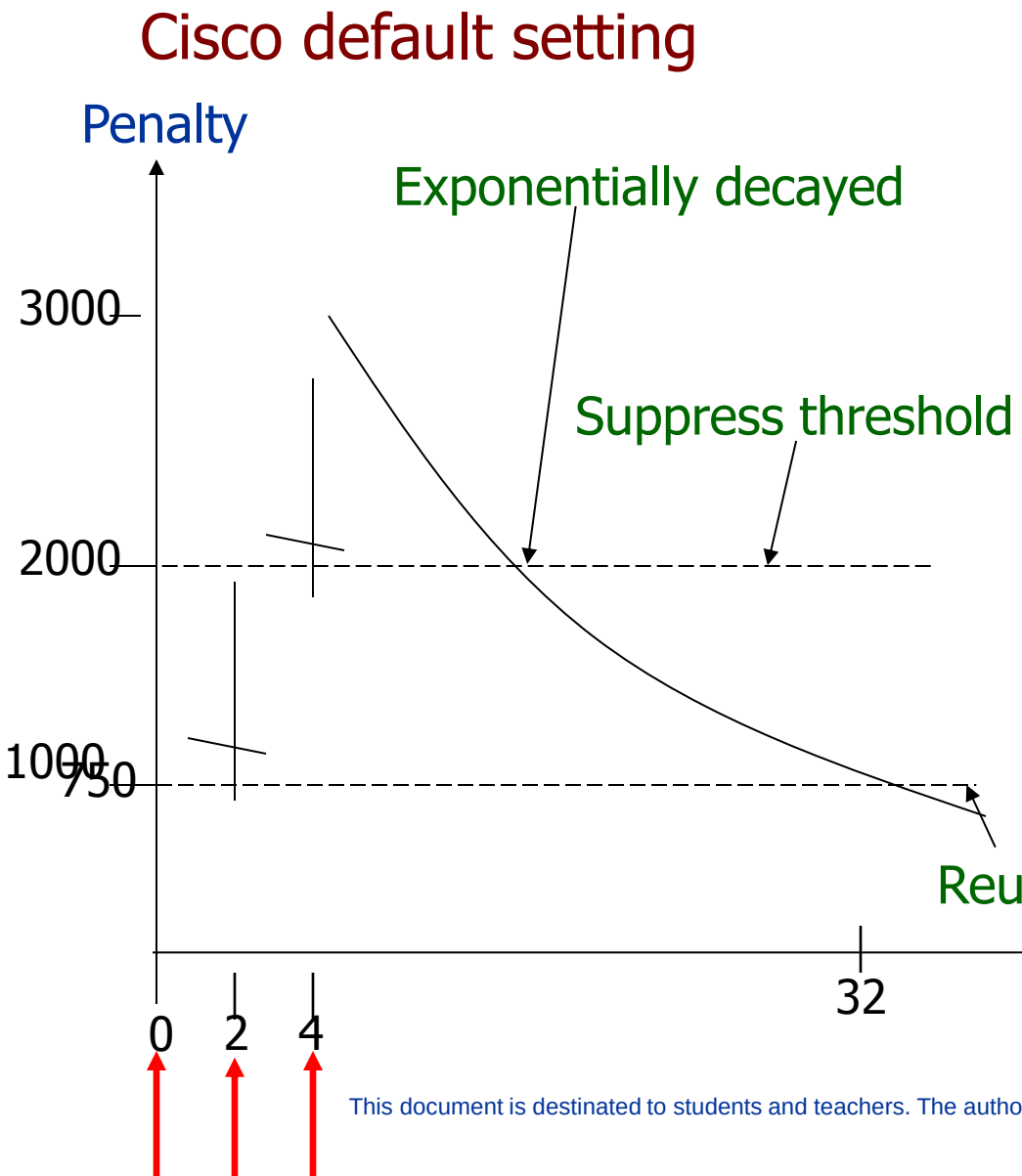
La sécurité du protocole BGP
Quels sont les moyens de protection actuels ?

Generalized TTL Security Mechanism

Vérification large du TTL : connexion ayant n hops avec le peer



La sécurité du protocole BGP
Quels sont les moyens de protection actuels ?



Route flap damping

Scope

- Inbound external routes
- Per neighbor, per destination

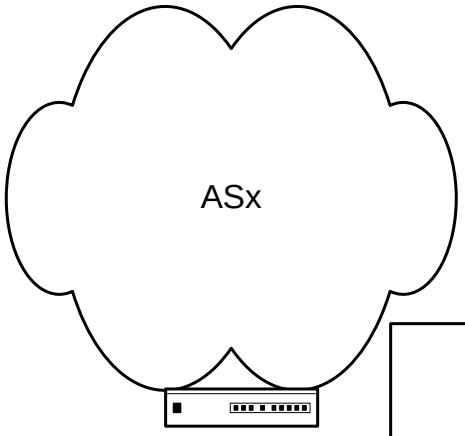
Penalty

- **Flap**: route change
- Increases for each flap
- Decays exponentially

$$P(t') = P(t)e^{-\lambda(t'-t)}$$

La sécurité du protocole BGP
Quels sont les moyens de protection actuels ?

Unicast Reverse Path Forwarding



The packet must come on the same interface where the return packet will be sent based on the converged routing table

ROUTING TABLE

Strict : appear in the routing table and linked to interface

Loose : appear in the routing table

La sécurité du protocole BGP
Les initiatives …

- **S-BGP (Secure BGP),** crypto, topology authentication = strong, Path authentication = strong, Origin Authen = strong

- **So-BGP (Secure Origin),** crypto, topology authentication = strong, Path authentication = none, Origin Authen = strong

- **Pretty Good BGP,** route scanning analysis.

- **Route Origin Authentication,** crypto, Origin Authen = strong

La sécurité du protocole BGP
S-BGP

S-BGP makes use of:

- **IPsec** to secure point-to-point communication of BGP control traffic
- **Public Key Infrastructure** to provide an authorization framework representing address space and AS # “ownership”
- **Attestations** (digitally-signed data) to bind authorization information to UPDATE messages

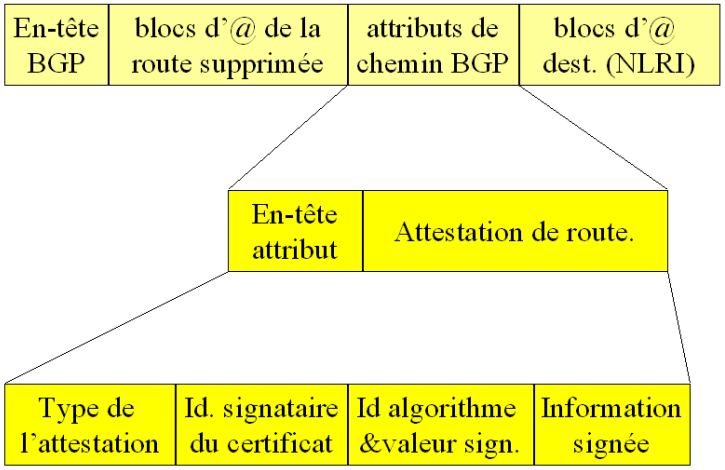
S-BGP requires routers to:

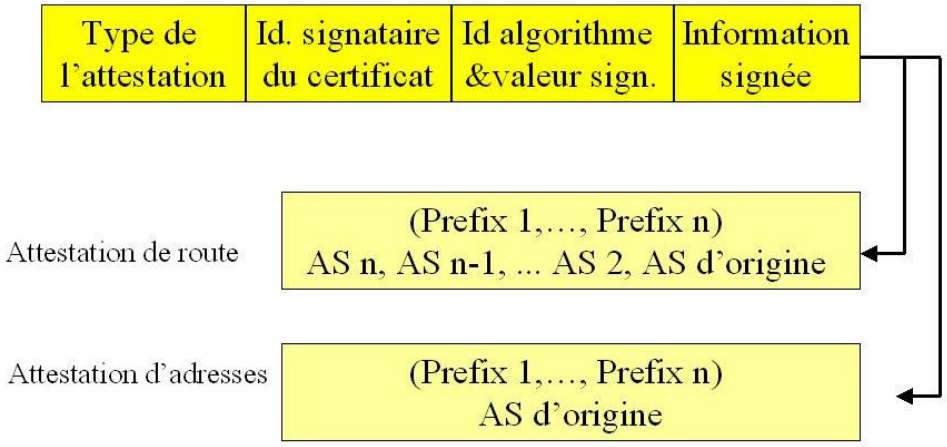
- **Generate** an attestation when generating an UPDATE for another S-BGP router
- **Validate** attestations associated with each UPDATE received from another S-BGP router

La sécurité du protocole BGP
S-BGP & Address & Route

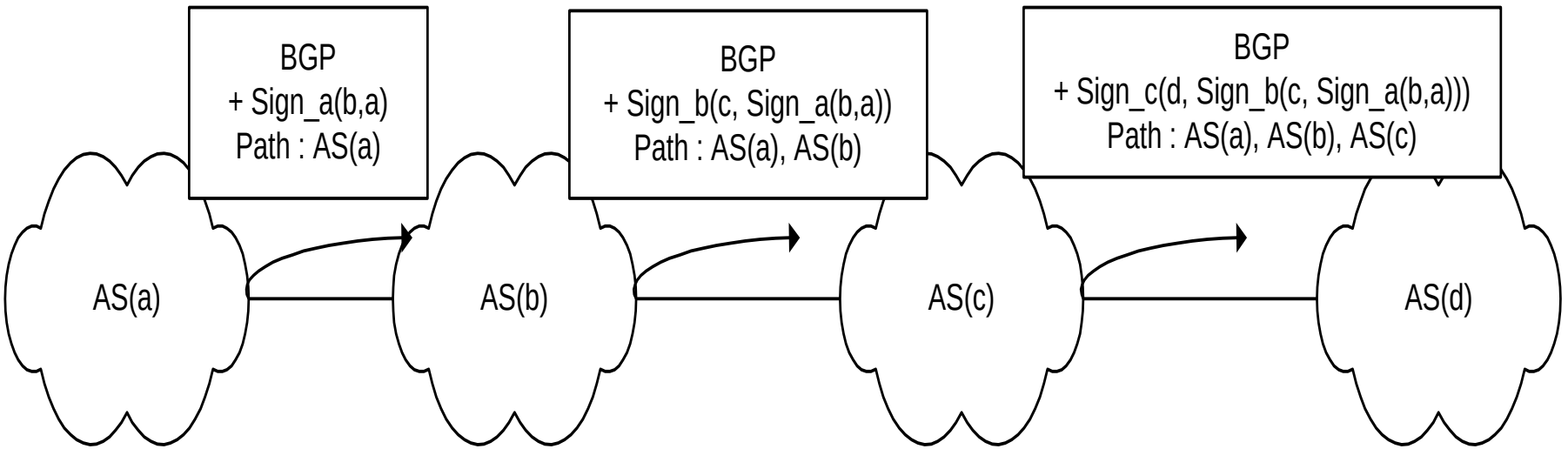
Un routeur recevant un message UPDATE peut vérifier que chaque AS du chemin spécifié a bien été autorisé à publier la route par l'AS le précédant.

Il s'assure aussi que l'AS d'origine détient bien le droit de publier les adresses correspondant à la route. Si une seule de ces différentes vérifications échoue, le message BGP UPDATE sera rejeté.





La sécurité du protocole BGP
S-BGP & Route Consistency



Route Attestation : Les signatures se superposent comme les couches d'un oignon.

La sécurité du protocole BGP
S-BGP & current issues

- Deployment issues especially for PKI.
- Signature computation and verification.
- Additional bandwidth & memory for signatures and certificates.
- Key distribution depends on correctness of BGP itself.

La sécurité du protocole BGP
So-BGP (Secure Origin BGP)

S-BGP: Secure BGP

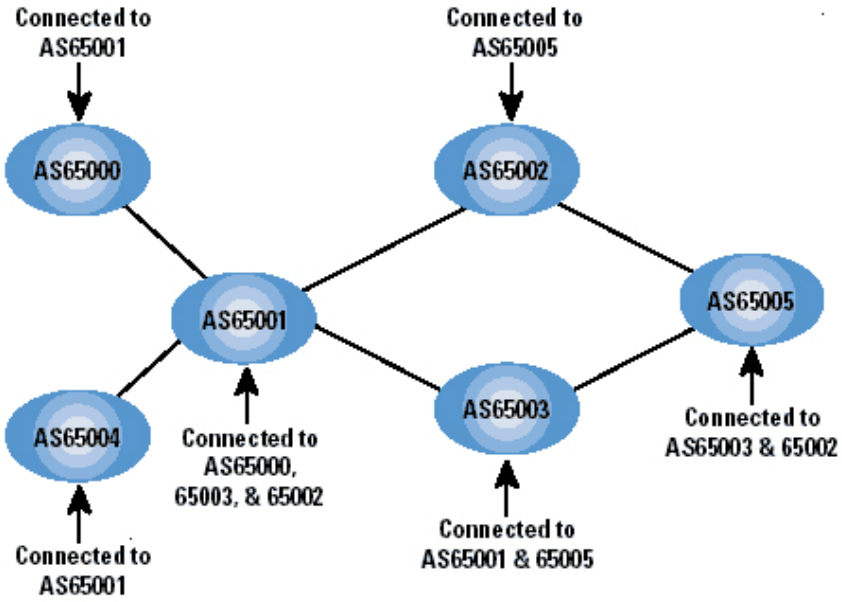
- PKI-based
- Address and route attestations
- Peer(s) connection : ipsec

soBGP: “Secure Origin” BGP

- Use a “web of trust “rather than a PKI-based
- Address and route attestations done via a set of certificates
- Peer(s) connection : shared secret and hash authentication

La sécurité du protocole BGP
So-BGP (Secure Origin BGP)

- **To avoid computational overhead of validating signatures,** So-BGP authenticates long-term structural routing elements prior to participating in BGP (*PolicyCert*).



La sécurité du protocole BGP
So-BGP (Secure Origin BGP)

- **In S-BGP, route attestations are sent dynamically** in the BGP update message (the peer has a real time view of the path taken by the message).

- **In so-BGP, route attestations can be done if each router has built a complete topology graph** based previous on exchanges of SECURITY messages (new set of BGP message). **In other words, attestations are static in So-BGP.**

- **Synchronisation issues** between the topology graph and the realtime BGP UPDATE messages. Cannot validate that the update actually traversed the path (!)

Pretty Good BGP

Main Ideas:

- Lower the local preference of suspicious routes
- Only inform the operators involved with the hijacked route of the problem. Nobody else can authoritatively answer.

Benefits

- Network has a chance to stop an attack before it spreads
- Accidental short-term routes do no harm
- Low operator overhead
- No loss in reachability
- Adaptive
- Simple

Identifying Prefix Hijacks

How does PGBGP spot a prefix hijack?

- Keep track of the origin ASs of each prefix that have been seen in the RIB and updates over the last 10 days.
- If an update contains a new origin AS for a prefix, it's potentially a prefix hijack. Label it as suspicious.
- UNLESS: A recently seen origin AS of the prefix is on the AS Path of the update. Then it's clean.

How does PGBGP *stop* a prefix hijack?

- Lower the local preference of suspicious routes for 24 hours.
- After 24 hours, promote the suspicious route to its normal preference, and add it to the history of known origin ASs for the prefix if it's still in the RIB.

Identifying Sub-Prefix Hijacks

What is a sub-prefix hijack?

- A sub-prefix hijack occurs when AS originates a prefix that it does not own and the space is originated elsewhere *and its space is wholly contained within another announced prefix block*

How can we spot a sub-prefix hijack?

- Keep a list of all recently seen prefixes. If a new prefix appears in an update, it *could* be a sub-prefix hijack

How does PGBGP spot a sub-prefix hijack?

- Keep track of each prefix that has been seen in the RIB and updates over the last 10 days.
- If an update contains a new prefix, and it's a sub-prefix of a recently seen prefix it's potentially a sub-prefix hijack. Label it as suspicious.
- UNLESS: The supernet's origin AS is on the AS Path of the update. Then it's clean.

ROA (Route Origin Authentication) Association of Addresses to AS#s

Create a new type of digitally signed object, a Route Origin Authorization (ROA)

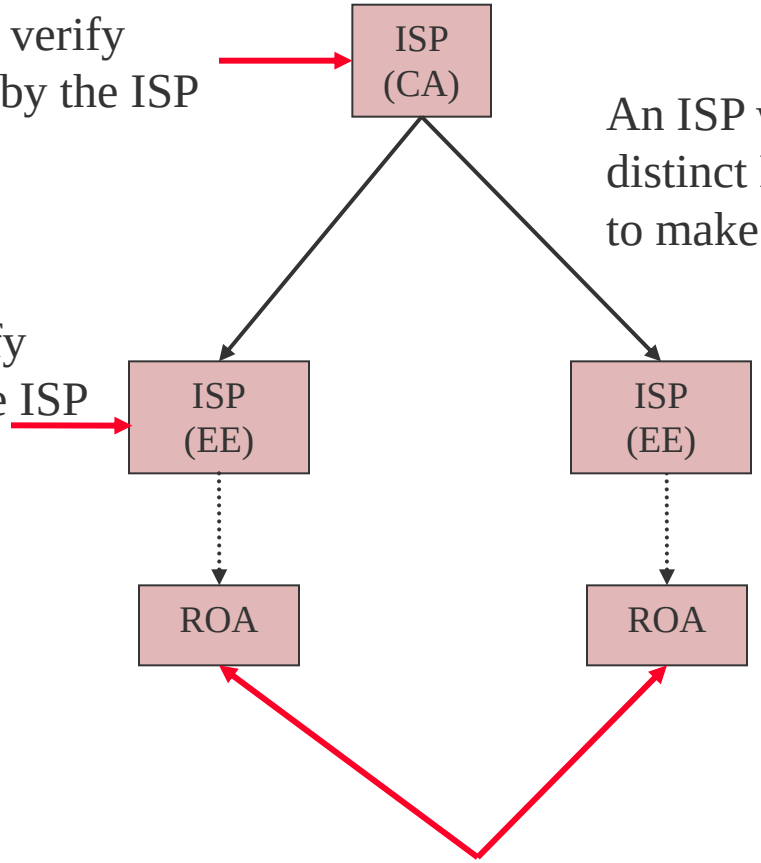
Every ROA is signed by an address space holder and contains:

- The AS# of the ISP
- The IP address block(s)
- An expiration date

ROA allows an address space holder to identify an AS number that is authorized to originate a route for one or more IP address blocks

ROA (Route Origin Authentication)
ROAs & Certificates

Public key used to verify certificates issued by the ISP



An ISP will usually create a distinct EE certificate per ROA, to make ROA revocation easy

Public key used to verify a ROA generated by the ISP

Signed objects authorizing route origination

ROA (Route Origin Authentication) Validation in the RPKI

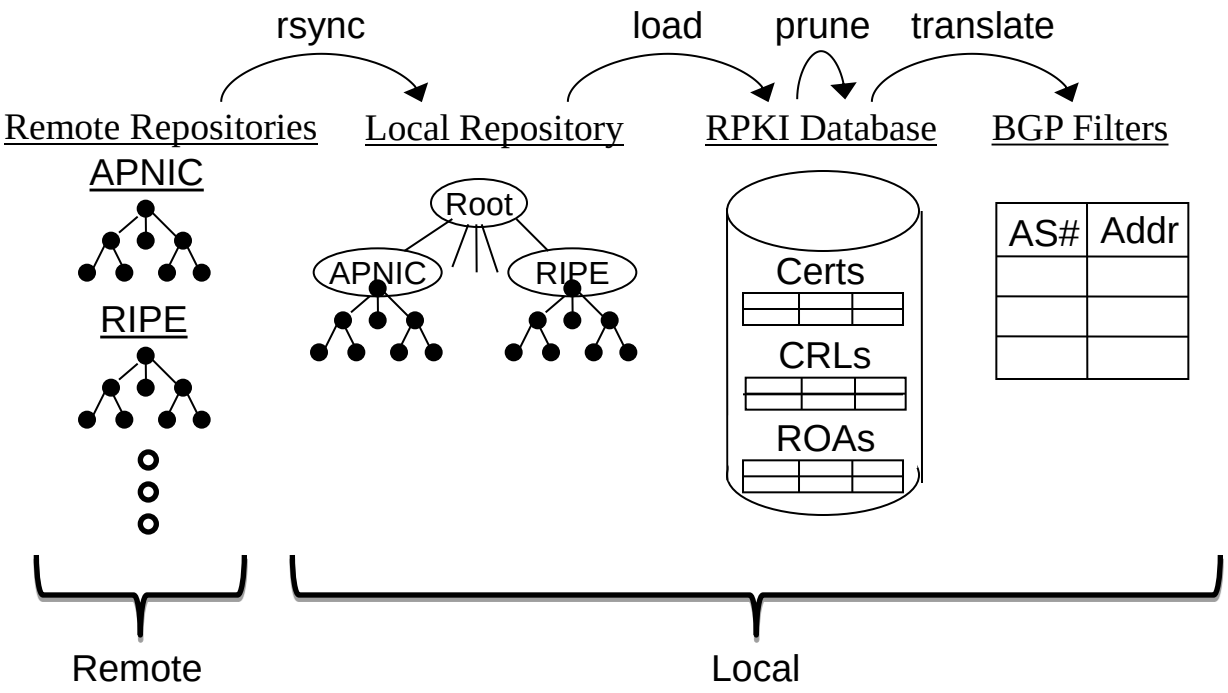
Typical PKI application context

- A relying party (RP) receives an End Entity (EE) certificate which must be validated
- It discovers a certification path to a trust anchor (TA)
- Only a small fraction of all the certificates in the PKI will need to be validated in a given time interval by a given RP

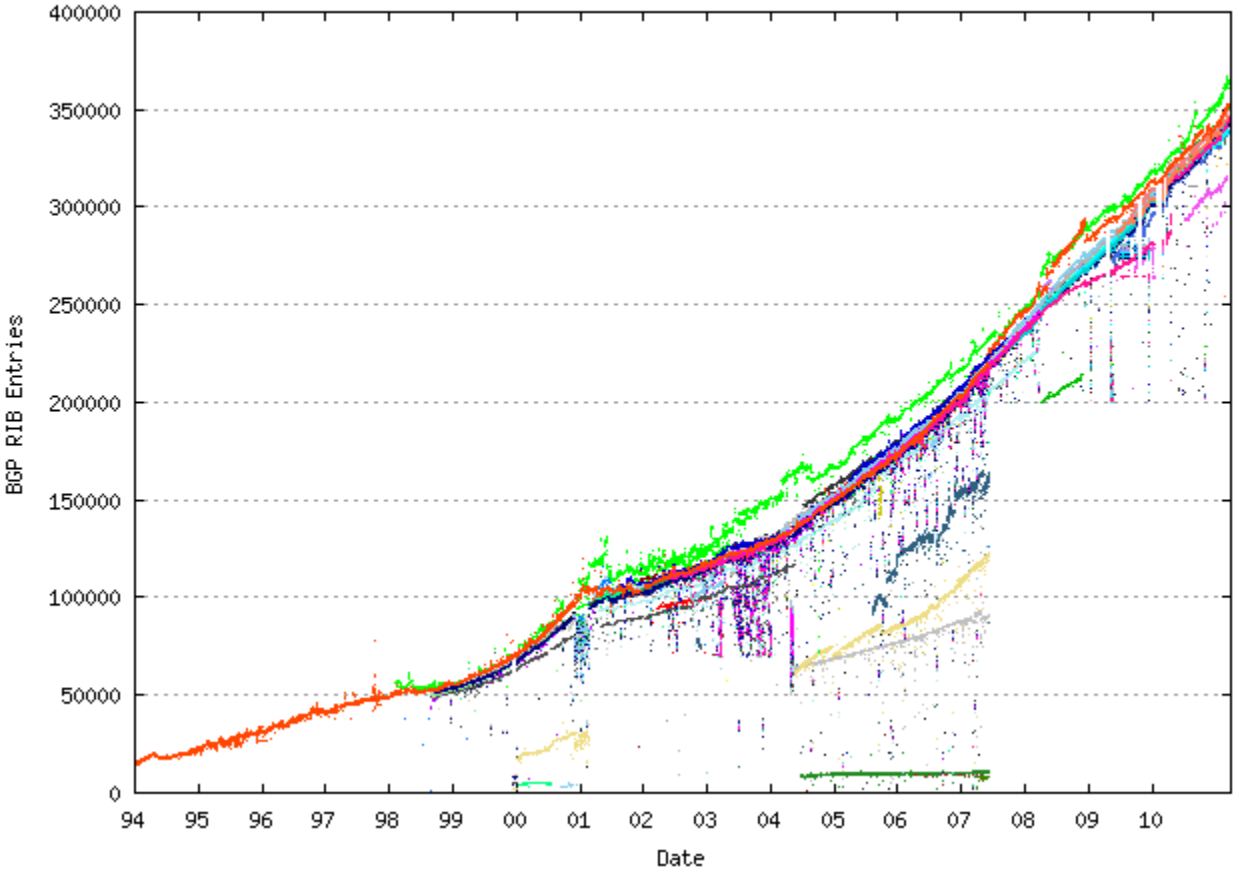
Resource PKI context

- The complete collection of valid ROAs is needed in order to generate BGP routing filters
- Every relying party must validate every certificate within a given time interval (nominally 1 day)
- Each ROA needs a certification path to a TA in order to be validated
- This is an authorization PKI, not an identification PKI

RPKI Software Architecture
ROA (Route Origin Authentication)



La sécurité du protocole BGP
L'explosion du nombre de routes visibles sur Internet



Explosion du nombre d'entrées avec l'arrivée de ipv6

Routing high availibility

High Availability

GR: Graceful Restart

- Capability exchanged between routing protocol speakers to indicate ability to do NSF

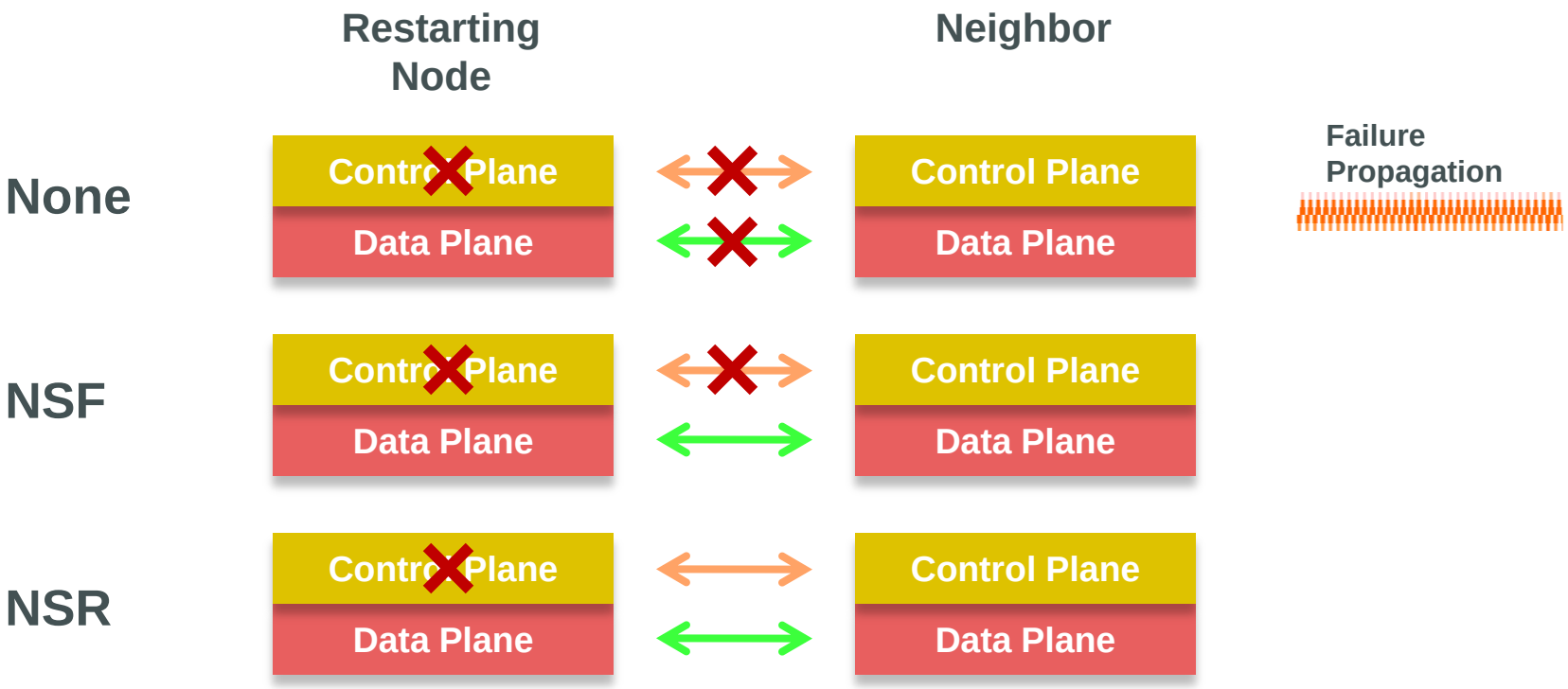
NSF: Non-Stop Forwarding

- Ability for a router with independent control and forwarding planes to forward traffic across a control plane restart
- FIB preserves routes/forwarding info

NSR: Non-Stop Routing

- Feature where routing protocols explicitly checkpoint state from the active RP to the standby RP to maintain routing information across a switchover

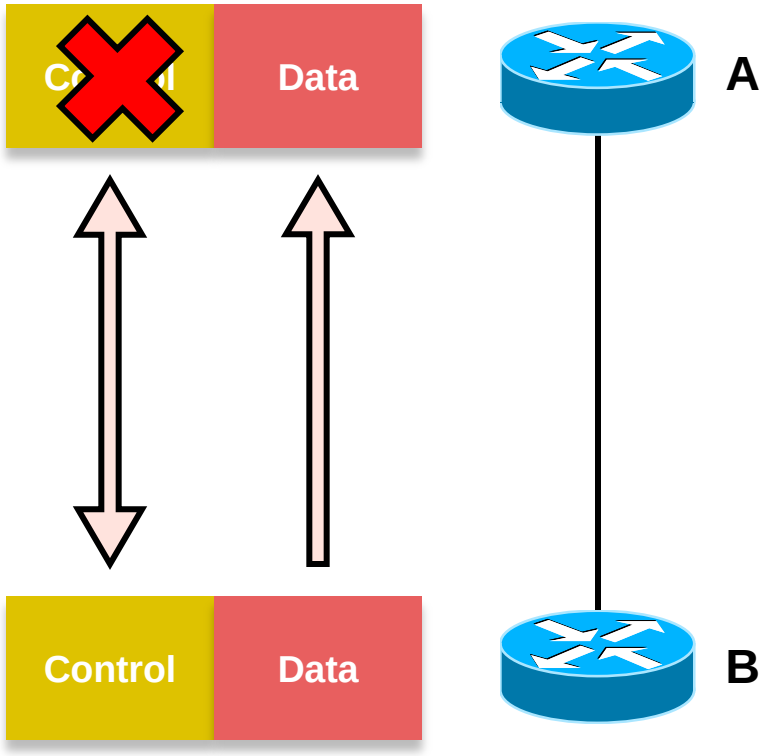
Routing HA Evolution



Behaviour without NSF

Router A loses its control plane for some period of time

It will take some time for Router B to recognize this failure, and react to it

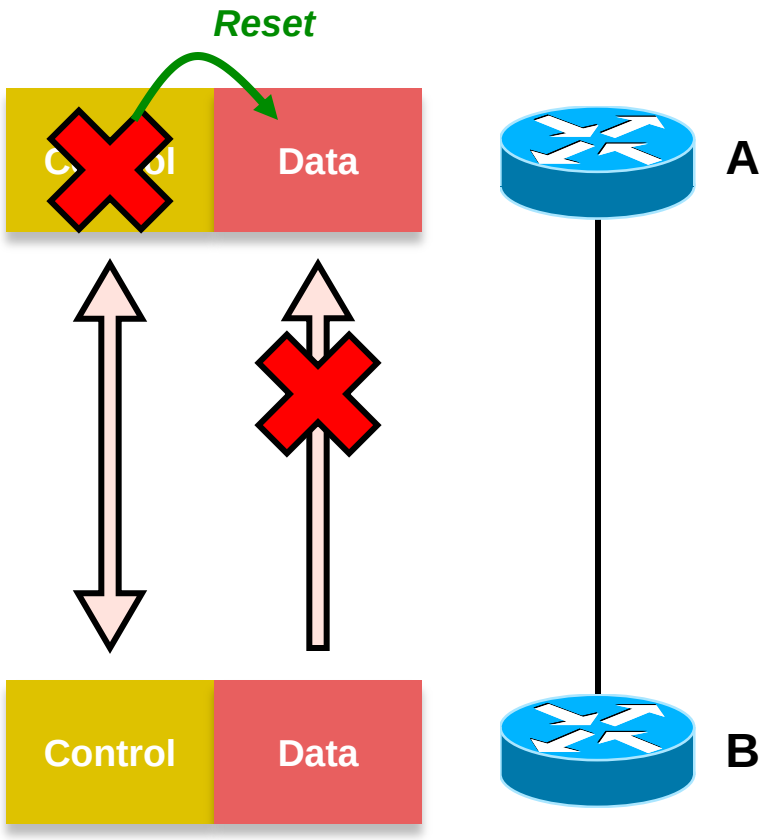


Behaviour without NSF

During the time that A has failed, and B has not detected the failure, B will continue forwarding traffic through A

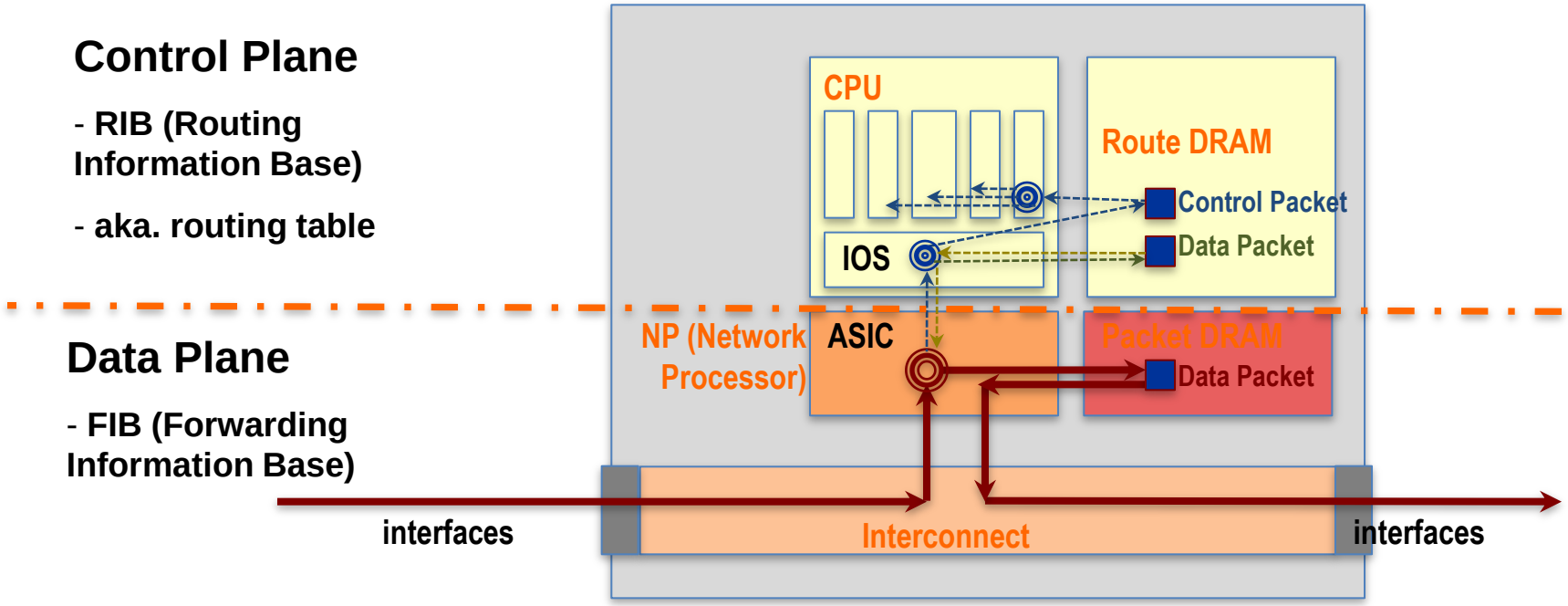
Once the control plane resets, the data plane will reset as well, and this traffic will be dropped

NSF reduces or eliminates the traffic dropped while A's control plane is down



Prerequisite : Separated Forwarding Plane

- Concept of separated control- and forwarding plane essential for routing HA
- Routing HA maintains the forwarding plane while the control plane restarts/recovers



Prerequisite 2: Stateful Switch Over (SSO)

- Any routing HA requires one important mechanism:
  The link and its line protocol need to stay up

  If not, all neighbours would re-route across the restarting node

- Can be trivial: Keep the linecard up and laser on, for example for POS/HDLC

- Keeping physical link active is easy with Ethernet as well, but need to sync ARP/v6ND/adjacency information

- Can be complex: PPP, ATM or FrameRelay require state to be maintained when failing over the control-plane, sync needed as well

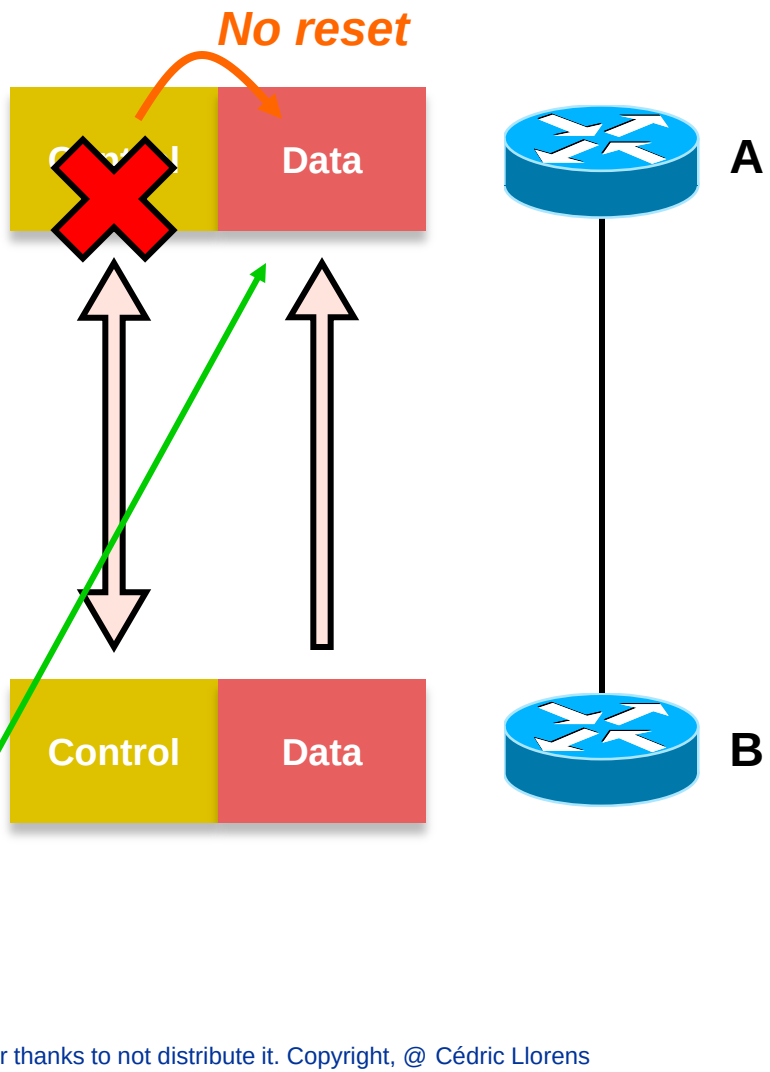
GR/NSF Fundamentals

If A is NSF capable, the control plane will not reset the data plane when it restart

Instead, the forwarding information in the data plane is marked as stale

Any traffic B sends to A will still be switched based on the last known forwarding information

This is the *Non-Stop Forwarding* behaviour



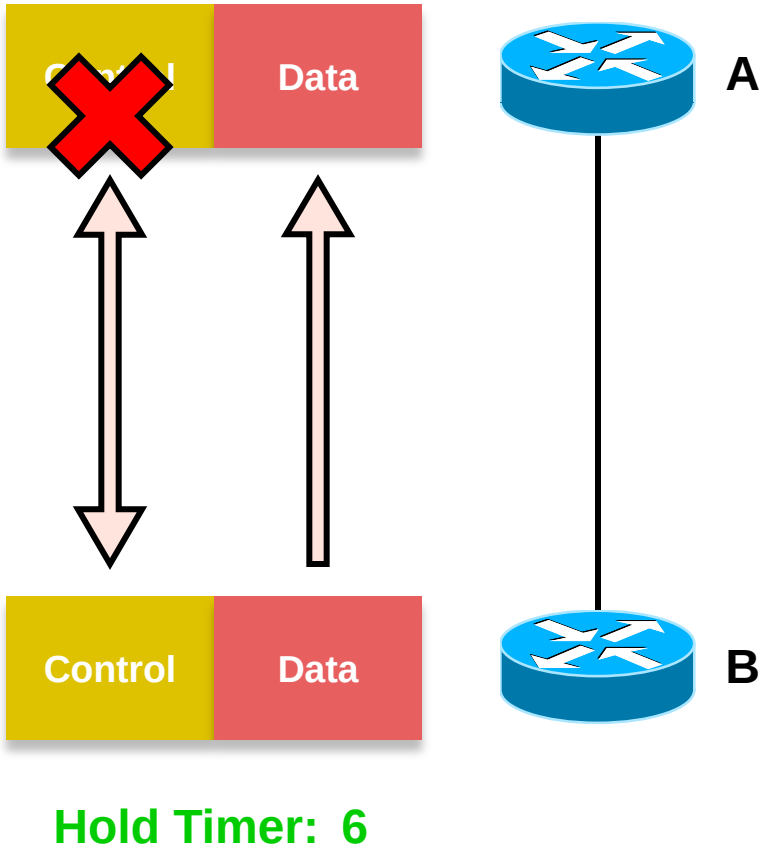
GR/NSF Fundamentals

While A's control plane is down, the routing protocol hold timer on B counts down....

A has to come back up and signal B before B's hold timer expires, or B will route around it

When A comes back up, it signals B that it is still forwarding traffic, and would like to resync

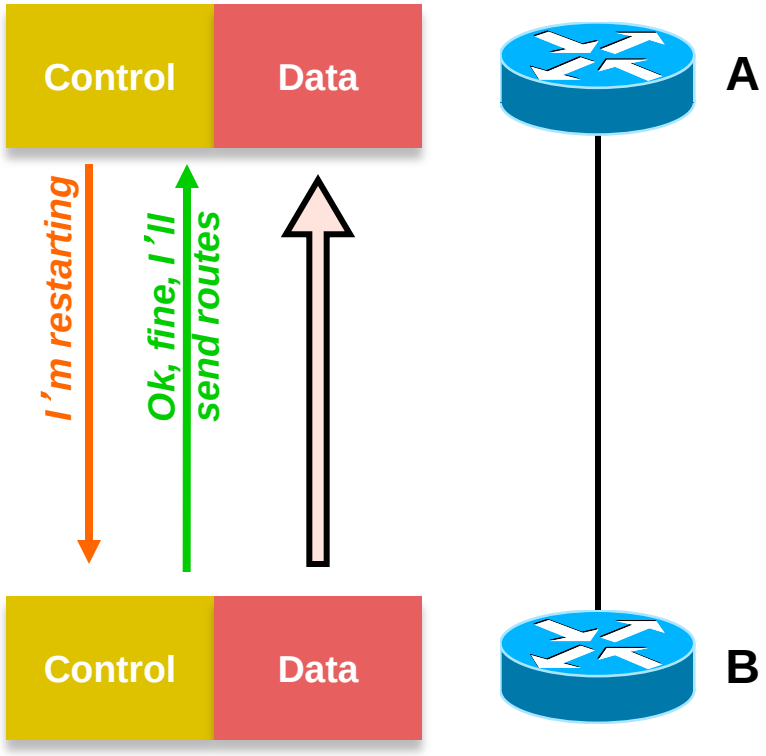
This is the first step in *Graceful Restart* (GR)



GR/NSF Fundamentals

The second GR phase deals with neighbors updating the restarting router's routing table

This involves new protocol mechanisms



Non-stop Routing – NSR

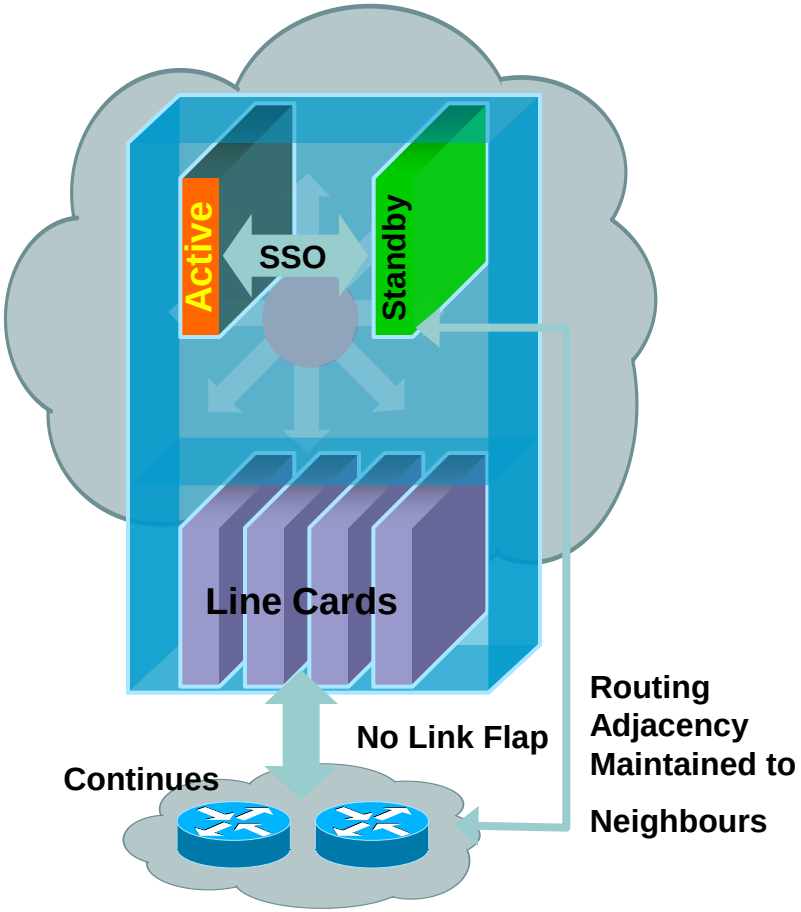
Idea: Why not sync all routing protocol state to the standby RP (or standby process)?

Restarting RP could pick up right where the primary left off

No need to refresh any information, no need for the neighbour to know that anything happened

Easy idea – challenging implementation ☺

- Now we absolutely need to avoid anything to let the neighbour know



High Availability Alphabet Soup

SSO: Stateful Switchover

- Failover from the active RP (crashing or reloading) to the standby RP (now taking over active role) where state is preserved and the router was in **hot standby** mode before the switchover

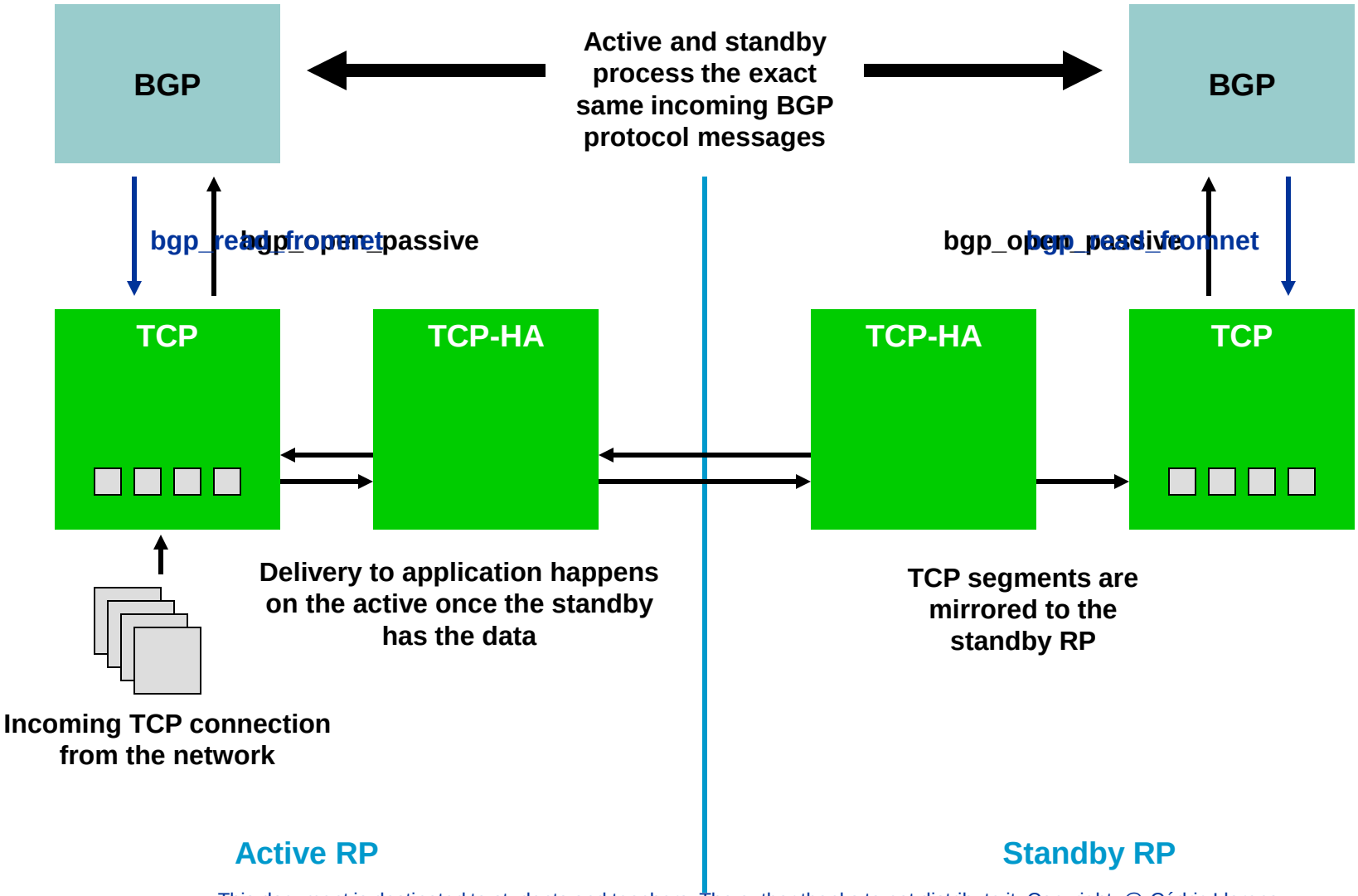
Hot Standby

- Redundancy **operating mode** where standby RP is fully initialized and able to checkpoint state from the active RP

RPR+

- Route Processor Redundancy operating mode – standby RP is partially initialized but there is no synchronization of state

NSR Symmetric Startup



Bidirectional Forwarding Detection

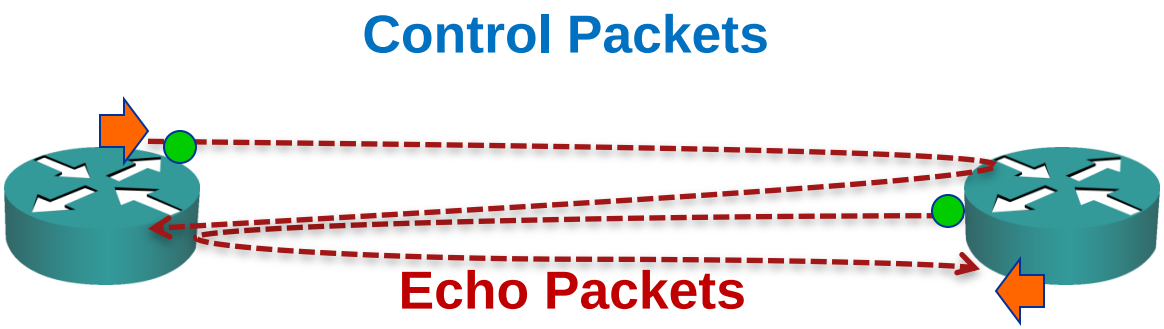
Control Packets and Echo Mode

If echo function is not negotiated

- control packets sent at high rate to achieve Detection Time

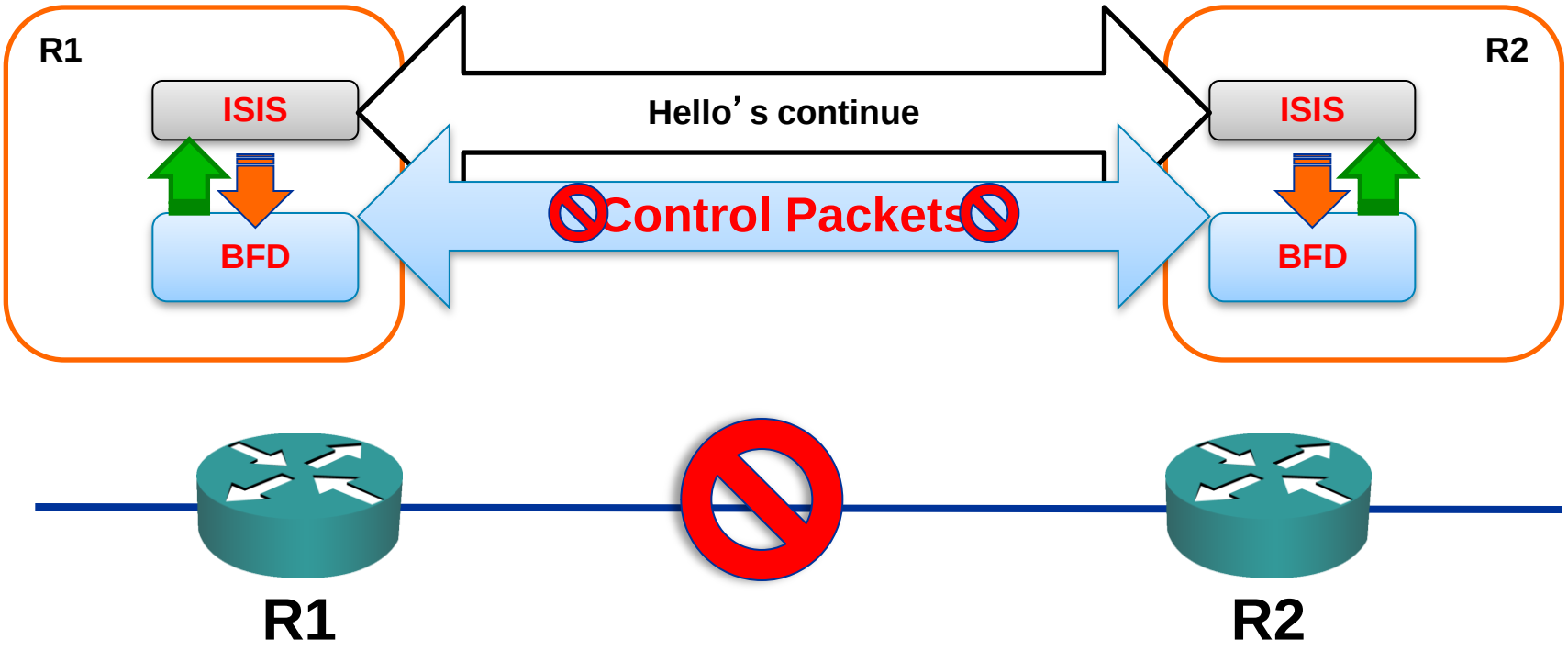
If echo function is negotiated

- control packets sent at a slow rate (Negotiated Rate)
  self directed echo packets sent at high rate (Min Echo Rx Interval)



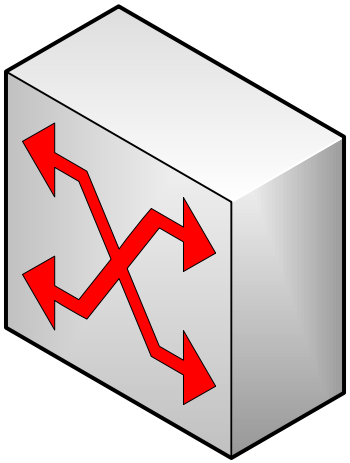
BFD with a ISIS session

- **BFD notifies ISIS of failure**
- **ISIS declares neighbor dead**



Security features at level 2 of a multi-services network

Some protection elements



- **DHCP snooping protection feature (real DHCP server connected to a trusted port).**

- **Dynamic ARP inspection feature (analysis of ARP packets per port, control of IP and MAC address per port).**

- **Port security feature (security policy per port : number of MAC address, violation policy, release of MAC address policy, etc.).**

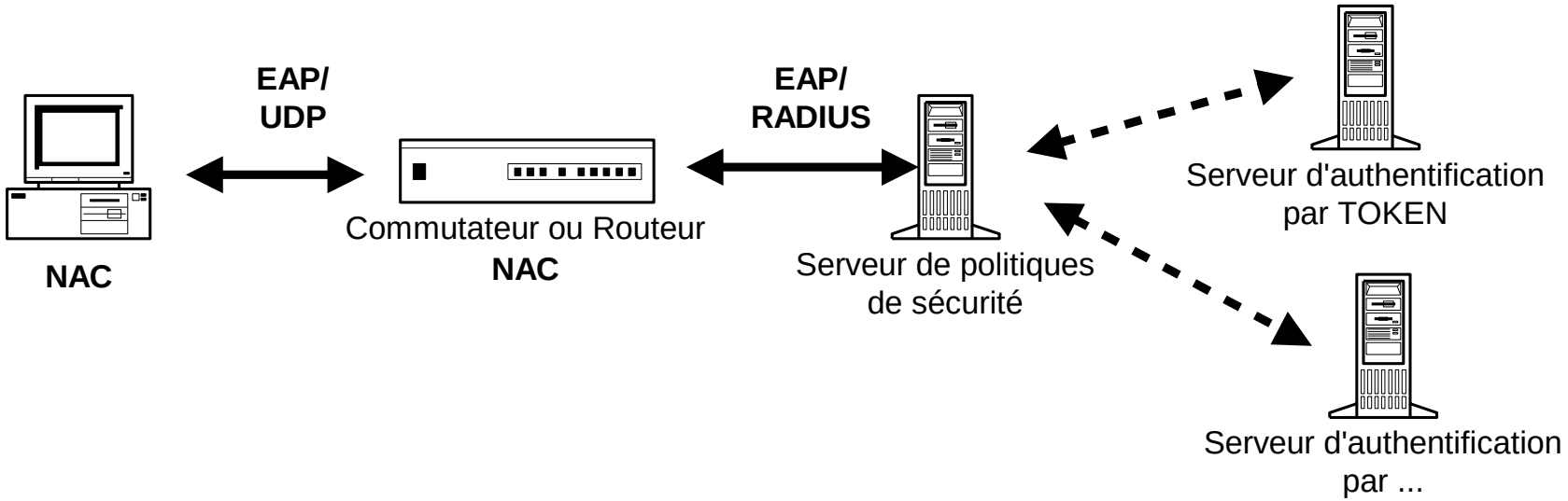
- **PACL (port ACL) : for level 2, VACL (VLAN ACL) : for intra and inter VLAN, RACL (routed ACL) : for routed port and inter VLAN.**

- **etc.**

Some protection elements

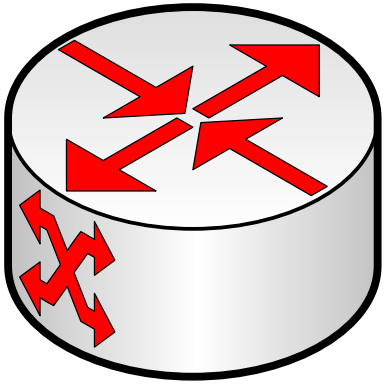
NAC : Network Access Control (Cisco initiative)

Allows to control the access to a network for a computer from a layer 2 point of view.



Security features at level 3 of a multi-services network

Some protection elements



- **rACL (receive ACL)**
- **Control Plane Policing (CoPP)**

Some protection elements

rACL (receive ACL)

La rACL est gérée par le RP du routeur. La rACL se doit de couvrir tout le trafic à destination ou initié par le routeur comme client : protocoles de routage (BGP et OSPF par exemple), protocoles de supervision (SNMP par exemple), accès pour la gestion (telnet et TACACS par exemple), protocole liés à MPLS (LDP par exemple), etc.

! autoriser SNMP en sortie (traps)
access-list 101 permit udp host <nous> any eq snmp
! autoriser les sources SNMP (serveurs)
access-list 101 permit udp <serveurs de supervision) any eq snmp
etc.

Some protection elements

Control Plane Policing CoPP) : gestion du plan de contrôle

CoPP consiste à protéger le plan de contrôle du routeur contre toute surcharge de travail. Si la CPU d'une LC ou la CPU du RP sont à la peine, c'est tout le routeur qui est mis à mal. Le but d'une politique CoPP est de limiter autant que possible le trafic qui sera passé vers le haut (« punt »).

Il ne fait sens de déployer une politique CoPP que sur des équipements qui traitent la majorité des opérations au niveau matériel vu que sur un routeur dont les opérations sont purement logicielles CoPP pourrait avoir un impact négatif en cas de déni de service.

Une rACL fait logiquement partie d'une politique CoPP, mais elle ne traite que les paquets destinés au routeur, alors que CoPP concerne tous les paquets (y compris du trafic « en transit ») qui vont être passés à la CPU du RP. Une rACL et une politique CoPP sont complémentaires.

Some protection elements

Control Plane Policing CoPP) : gestion du plan de contrôle

```
access-list 101 permit icmp any any
access-list 102 permit ip any any eq ssh
access-list 102 permit ip any any eq snmp

class-map ICMP
        match access-group 101
class-map MGMT
        match access-group 102
policy-map control-plane-policy
        class ICMP
                police 64000 conform-action transmit exceed-action drop
        class MGMT
                police 32000 conform-action transmit exceed-action drop
control-plane
        service-policy input control-plane-policy
```

Some protection elements

Control Plane Policing CoPP) : gestion du plan de contrôle

```
access-list 101 permit icmp any any
access-list 102 permit ip any any eq ssh
access-list 102 permit ip any any eq snmp

class-map ICMP
        match access-group 101
class-map MGMT
        match access-group 102
policy-map control-plane-policy
        class ICMP
                police 64000 conform-action transmit exceed-action drop
        class MGMT
                police 32000 conform-action transmit exceed-action drop
control-plane
        service-policy input control-plane-policy
```

Agenda

Questions ?