INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Université Polytechnique HAUTS-DE-FRANCE

LE ROUTAGE

v

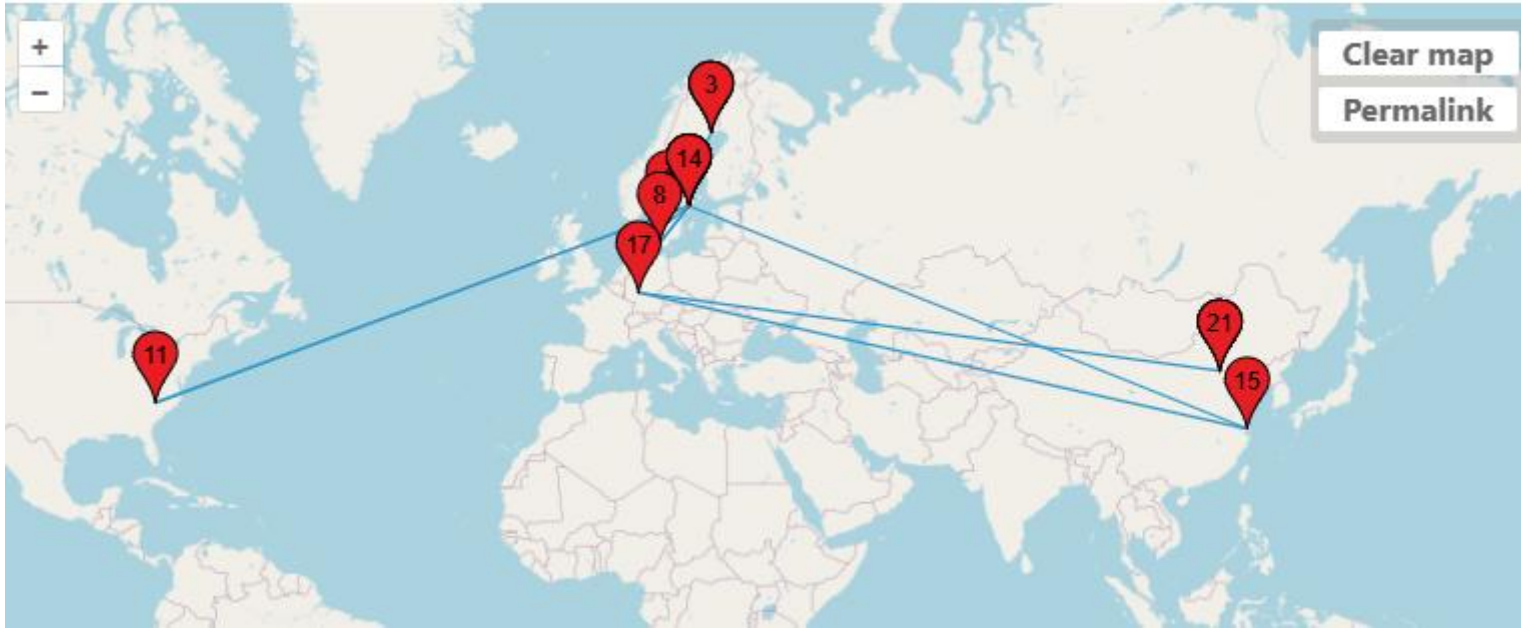
INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Université Polytechnique HAUTS-DE-FRANCE

Rappel : fonctionnement d’internet

- (37) Comment fonctionne Internet ? - YouTube
- Submarine Cable Map
- Tracert
- Traceroute

Traceroute à partir de la suède



Traceroute vers free.fr

1 4 ms 4 ms 4 ms 10.4.0.4

2 7 ms 8 ms 9 ms 193.51.250.113

3 7 ms 7 ms 7 ms vl445-be4-ren-nr-lille-rtr-091.noc.renater.fr [193.51.186.200]

4 9 ms 9 ms 12 ms xe1-1-7-paris1-rtr-131.noc.renater.fr [193.51.177.61]

5 9 ms 9 ms 9 ms et-5-0-1-ren-nr-paris2-rtr-131.noc.renater.fr [193.55.204.195]

6 10 ms 9 ms 9 ms free-vl30-ae9-ren-nr-paris2-rtr-131.noc.renater.fr [193.51.187.209]

7 10 ms 11 ms 10 ms p19-6k-2-v900.intf.nra.proxad.net [78.254.255.206]

8 * * * Délai d'attente de la demande dépassé.

9 10 ms 10 ms 9 ms www.free.fr [212.27.48.10]

I. Introduction

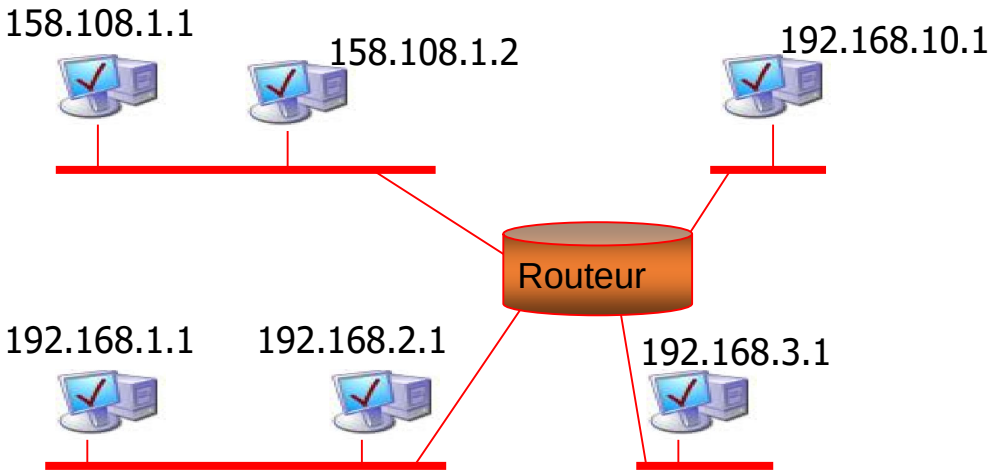
Définition du routage et de son rôle dans les réseaux de communication

- Le routage est le processus de **transmission de données** entre les réseaux.

- Les routeurs sont des équipements de réseau qui sont conçus pour **acheminer** les paquets de données d'un point à un autre.

- Le routage est essentiel dans les réseaux de communication car il permet de **connecter différents réseaux** et de les faire communiquer entre eux.

5.1 : Réseaux et routage

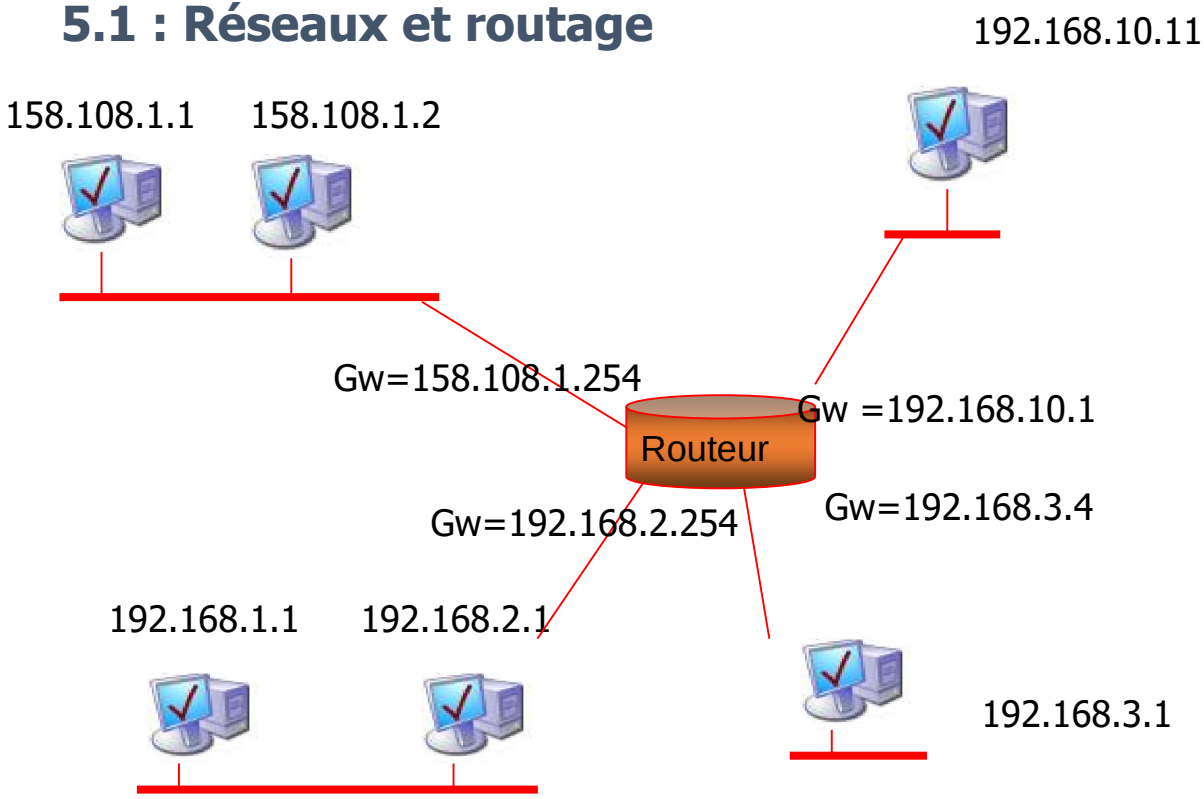


5.2 : Routage en sous-réseau

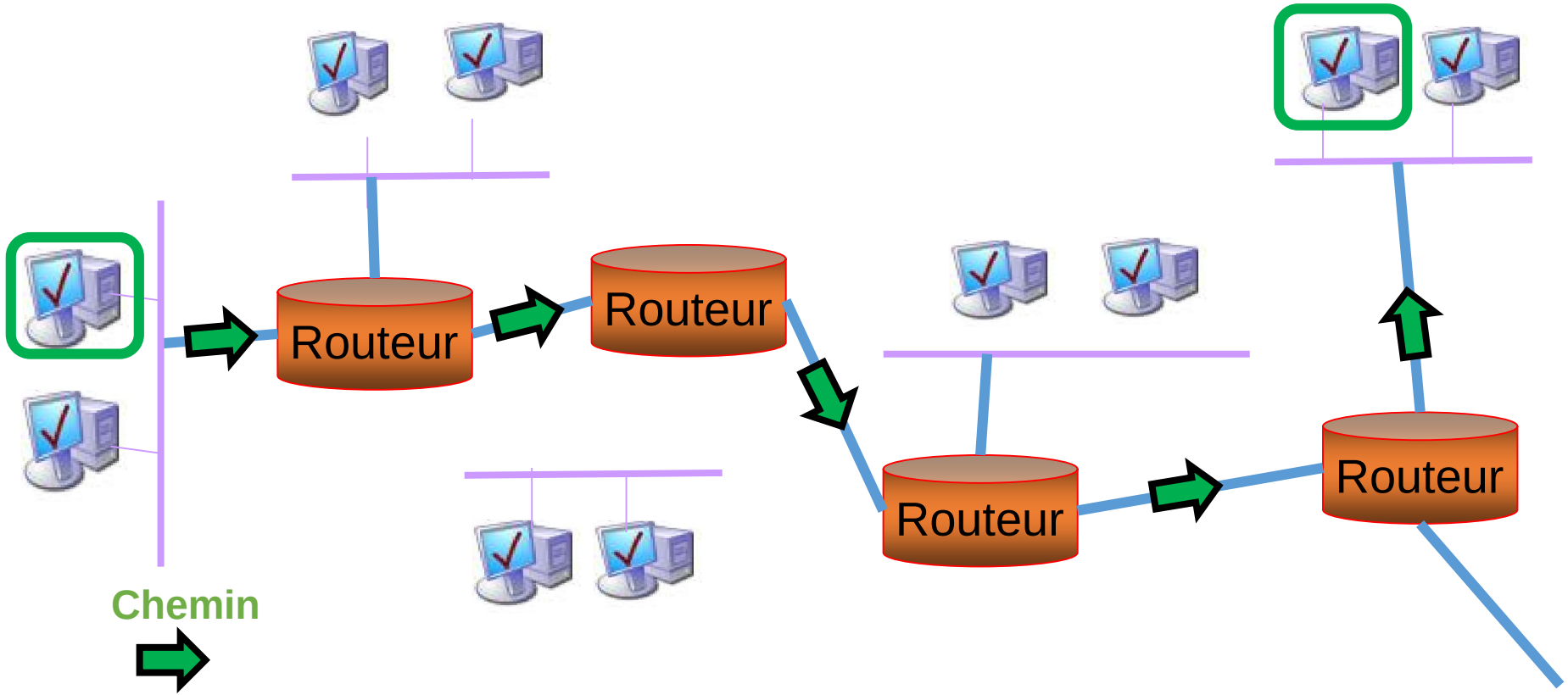
- Dans chaque station le traffic est dirigée selon l'algorithme suivant :

```
Si (adr.IP_dest && masque == adr.IP_locale && masque)
      // adr.IP dest est dans le même sous-réseau
      envoyer le paquet sur le sous-réseau
Sinon
      // adr.IP dest est dans un autre sous-réseau
       envoyer le paquet au routeur
```

5.1 : Réseaux et routage



Définition du routage et de son rôle dans les réseaux de communication

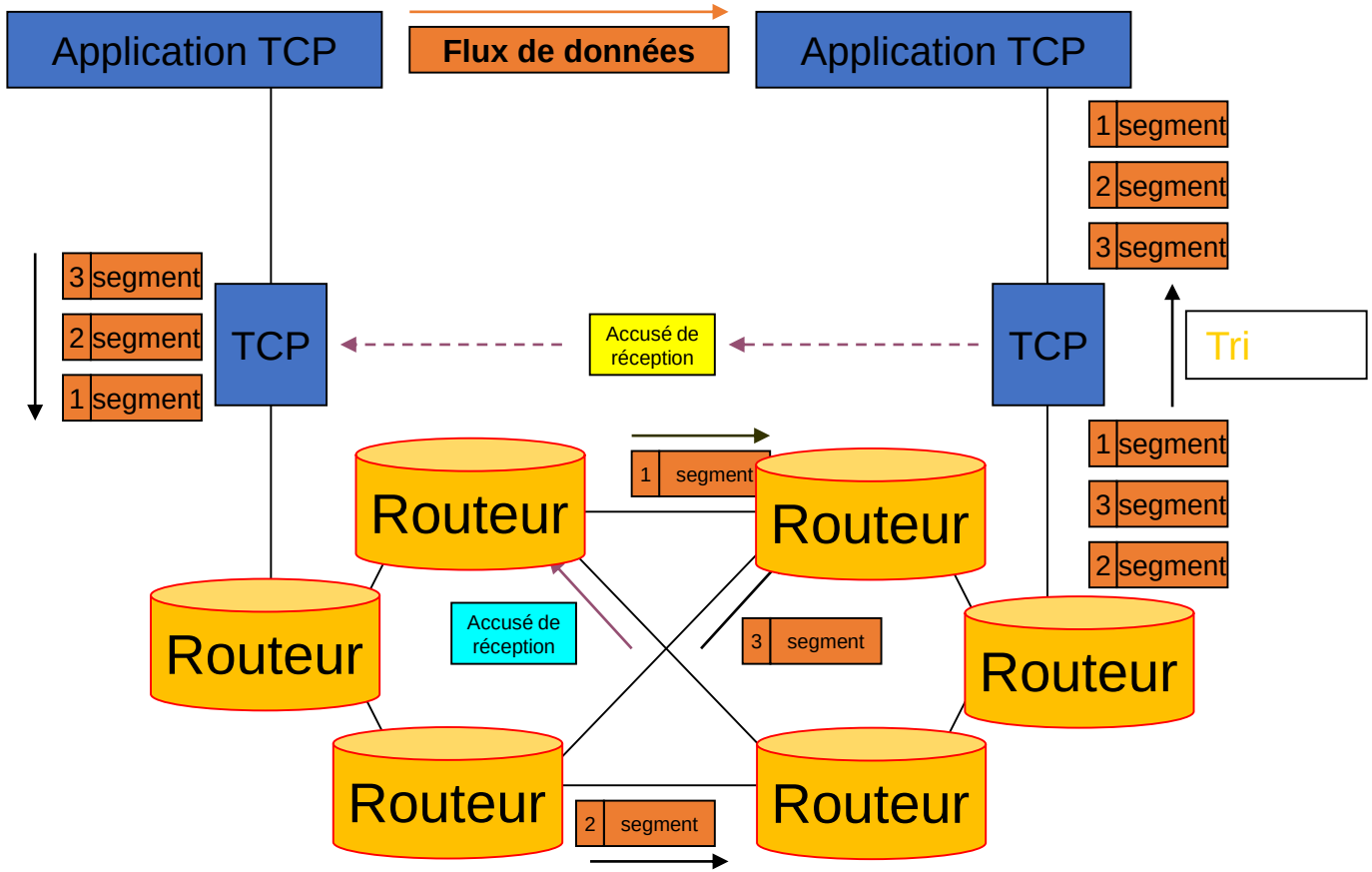


Importance du routage dans les réseaux à grande échelle

- en acheminant les paquets de données de **manière efficace et fiable** à travers le réseau,
- tout en **évitant les congestions et**
- **les goulots d'étranglement**.

- Il permet également **d'optimiser** l'utilisation des ressources du réseau en **répartissant la charge**
  - de manière équitable entre les différents chemins de transmission disponibles.
- Il permet de maintenir la connectivité du réseau en redirigeant le trafic
  - en cas de **défaillance** d'un élément du réseau

Une données = plusieurs paquets



II. Présentation d'un routeur

Format d'un routeur : matériel

- **nombre de ports** Ethernet inférieur.
- **puissants, à plusieurs cœurs**.
- **pare-feu et la détection d'intrusion**.

Routeur

- Les routeurs peuvent être **montés en rack** et équipés de **modules d'extension** pour ajouter des fonctionnalités supplémentaires.

- Les marques les plus utilisées en entreprise sont **Cisco, Fortinet, Hewlett Packard et Ubiquiti Networks**.

Switch

- Les routeurs professionnels peuvent coûter
  - 20 000 € ou plus

Les routeurs logiciels : une alternative économique et flexible

- **Des logiciels de routage**
- **Linux** ou **Windows**
- Utiles pour **les petits réseaux** et les environnements de test
- **Moins performants**
  - mais offrent des avantages en termes de flexibilité
  - de facilité de déploiement
  - et de coûts
- **Dépendance du processeur**,
  - de la mémoire
  - et de la bande passante
- Des exemples de routeurs logiciels populaires comprennent **pfSense**, VyOS, OpenWrt et DD-WRT
- **pare-feu** pour protéger le réseau.

Services proposées par les routeurs : tolérance aux pannes

- **tolérance aux pannes**

  - Les routeurs peuvent fournir des chemins de communication ***redondants***
    - en cas de panne d'un lien ou d'un routeur.

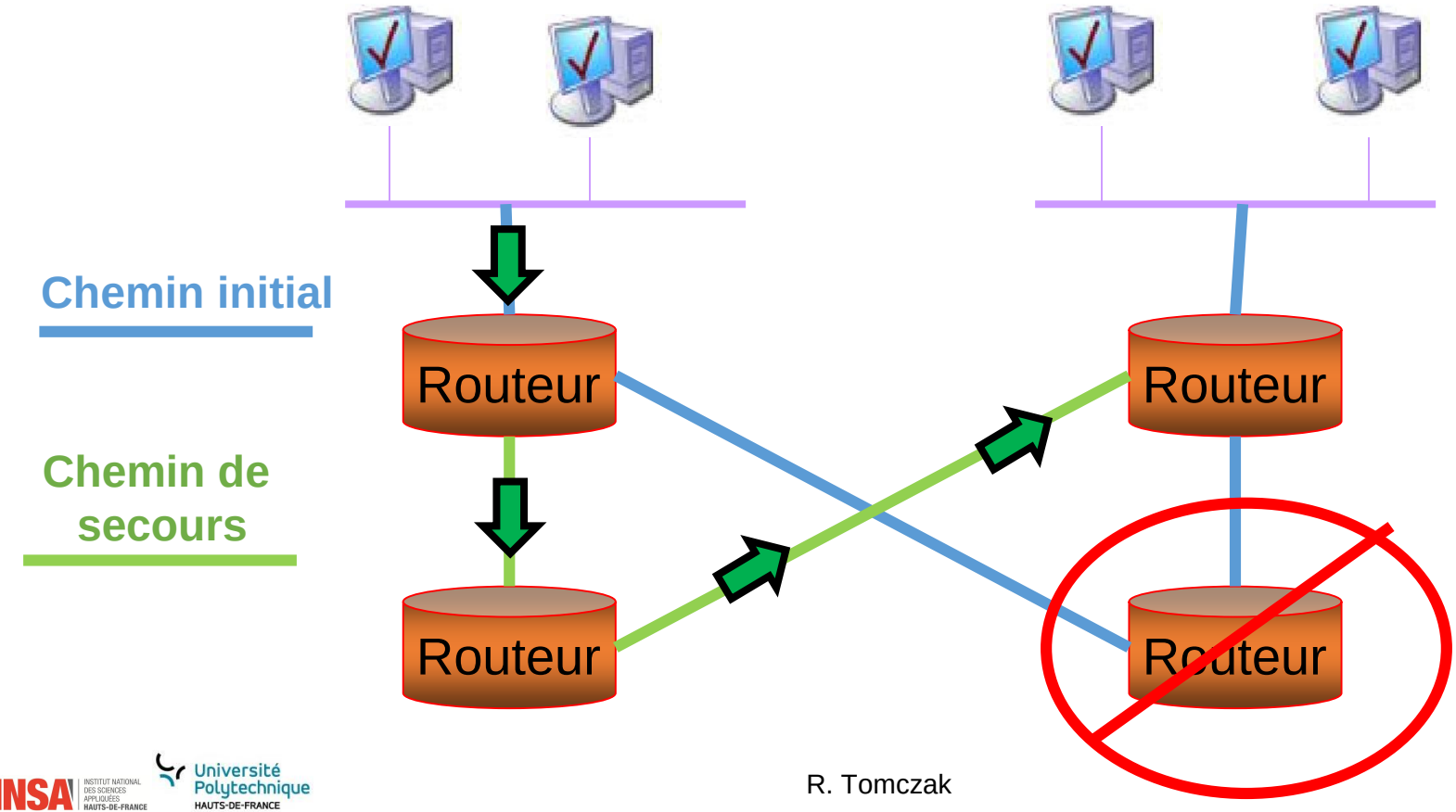
  - Les protocoles de routage avancés, tels que OSPF :
    - **Chemins les plus fiables**
    - et détecter les **pannes**.

Routeur et passerelle

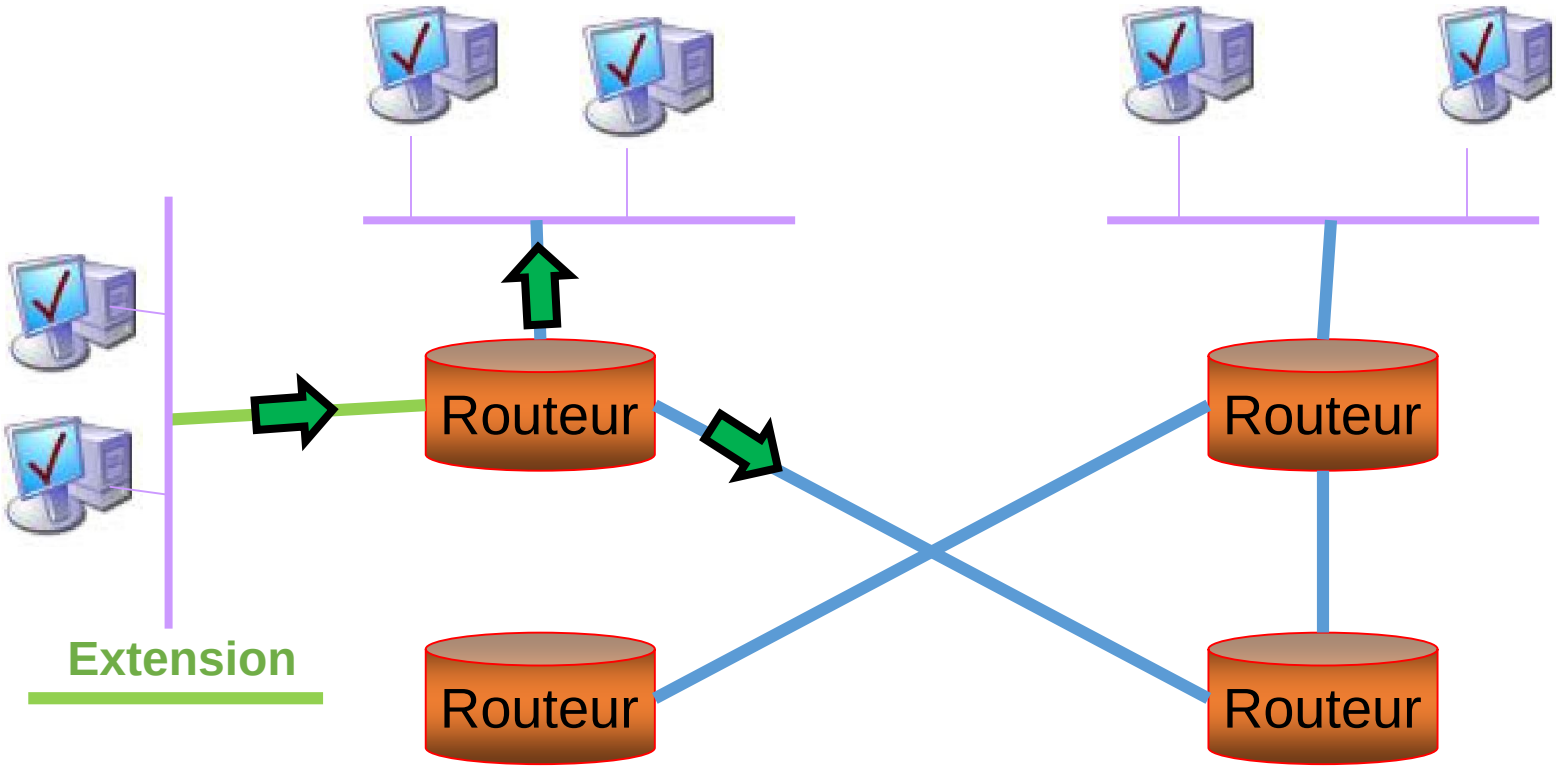
- **Passerelle = point d'entrée** pour relier deux réseaux différents
- Peut être **physique ou logicielle**, travaille sur les couches 3, 4 et au-delà

- Pour l'Ethernet, la **passerelle est l'appareil (ou plutôt l'adresse)**
  - se trouvant dans le réseau
  - qui permet de sortir de ce réseau.
  - Dans la plupart des cas, cet appareil est un **routeur**.

Services proposées par les routeurs : tolérance aux pannes



Services proposées par les routeurs : évolutivité



Services proposées par les routeurs : QoS

- Les routeurs permettent la **qualité de service (QoS) :**
  - Attribuent des priorités aux différents types de trafic
  - Par exemple, voix et vidéo considérées comme prioritaires
  - Les données sont considérées comme moins importantes

- Garantissent une bande passante suffisante :
  - pour les flux de trafic prioritaires, même en cas de congestion

- la voix sur IP
- et la vidéoconférence.

Services proposées par les routeurs : sécurisation

- Fonctionnalités de sécurité qui permettent de mieux protéger les réseaux contre les attaques et les intrusions malveillantes

1. **Pare-feu** qui filtrent le trafic entrant et sortant du réseau et bloquent les paquets malveillants ou non autorisés.
2. **Séparation de réseaux** diviser les réseaux en plusieurs sous-réseaux, afin de limiter la propagation des attaques et de séparer les zones de confiance.
3. **Accès distant sécurisé** : un accès distant sécurisé, tel que les connexions **VPN**, qui permettent aux utilisateurs de se connecter à distance au réseau de l'entreprise de manière sécurisée.
4. **Détection d'intrusion** : surveillent le trafic réseau pour identifier les activités suspectes et les tentatives d'intrusion.
5. **Contrôle d'accès** : limiter l'accès aux ressources du réseau en fonction des identifiants d'utilisateur, des adresses IP

III. Le routage statique

Configuration des routes statiques dans les routeurs

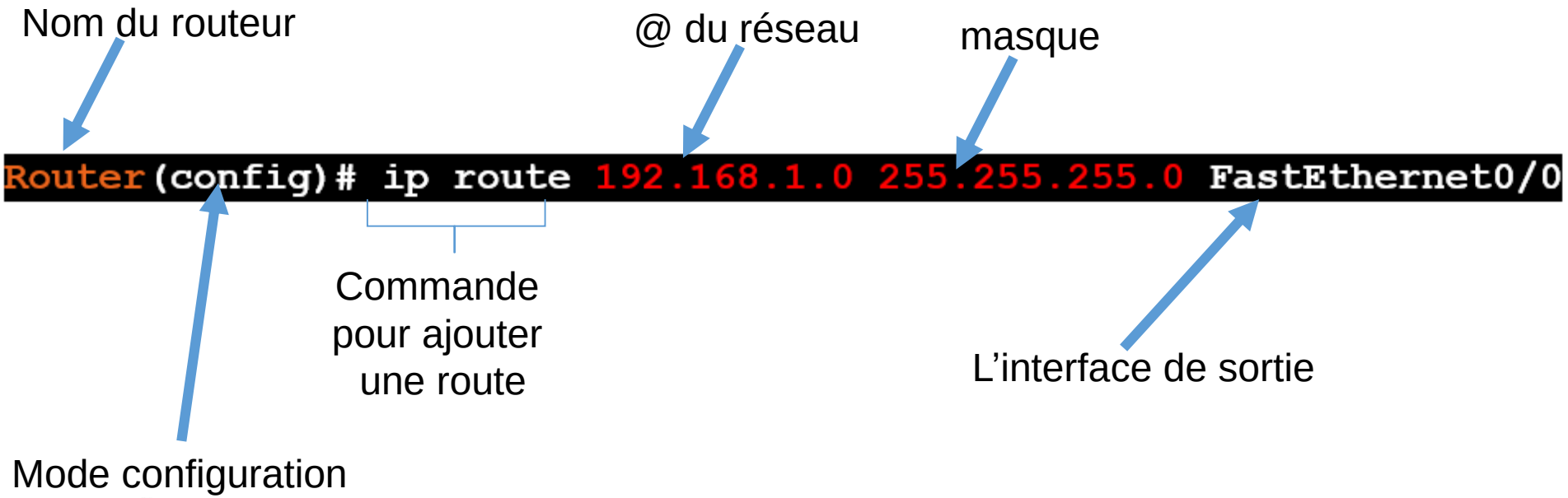
- Le routage **statique** = les routes sont **définies manuellement**

- l'administrateur réseau doit :
  - déterminer **les routes optimales pour chaque destination**
  - et les configurer dans les **tables de routage** des routeurs.

- Les routes statiques :
  - peuvent être configurées pour **les destinations qui changent rarement**,
  - ou pour les connexions point à point

Configuration des routes statiques dans les routeurs

- **utilise l'interface de ligne de commande**
- **Par ex:** ajouter une route statique vers le réseau de destination 192.168.1.0/24 via l'interface FastEthernet0/0



Avantages

- **Facile** à configurer et à maintenir

- **Moins de trafic** sur le réseau car les routes sont configurées manuellement dans chaque routeur

- **Moins de ressources nécessaires** pour exécuter le routage car il n'y a pas de processus de routage dynamique

- **Moins de vulnérabilités** de sécurité car il n'y a pas de diffusion de trafic de routage

inconvénients

- **Inconvénients** :
  - Configuration manuelle **fastidieuse** pour les grands réseaux

  - **Moins flexible**, moins adaptable aux changements dans la topologie du réseau
  - **Moins de tolérance aux pannes** et aux problèmes de connectivité car les routes sont statiques et ne peuvent pas s'adapter aux changements dans le réseau
  - **Plus de risques d'erreur humaine** dans la configuration des routes

Table de routage des routeurs

Linux et iOs

Soit la table de routage :

Table de Routage

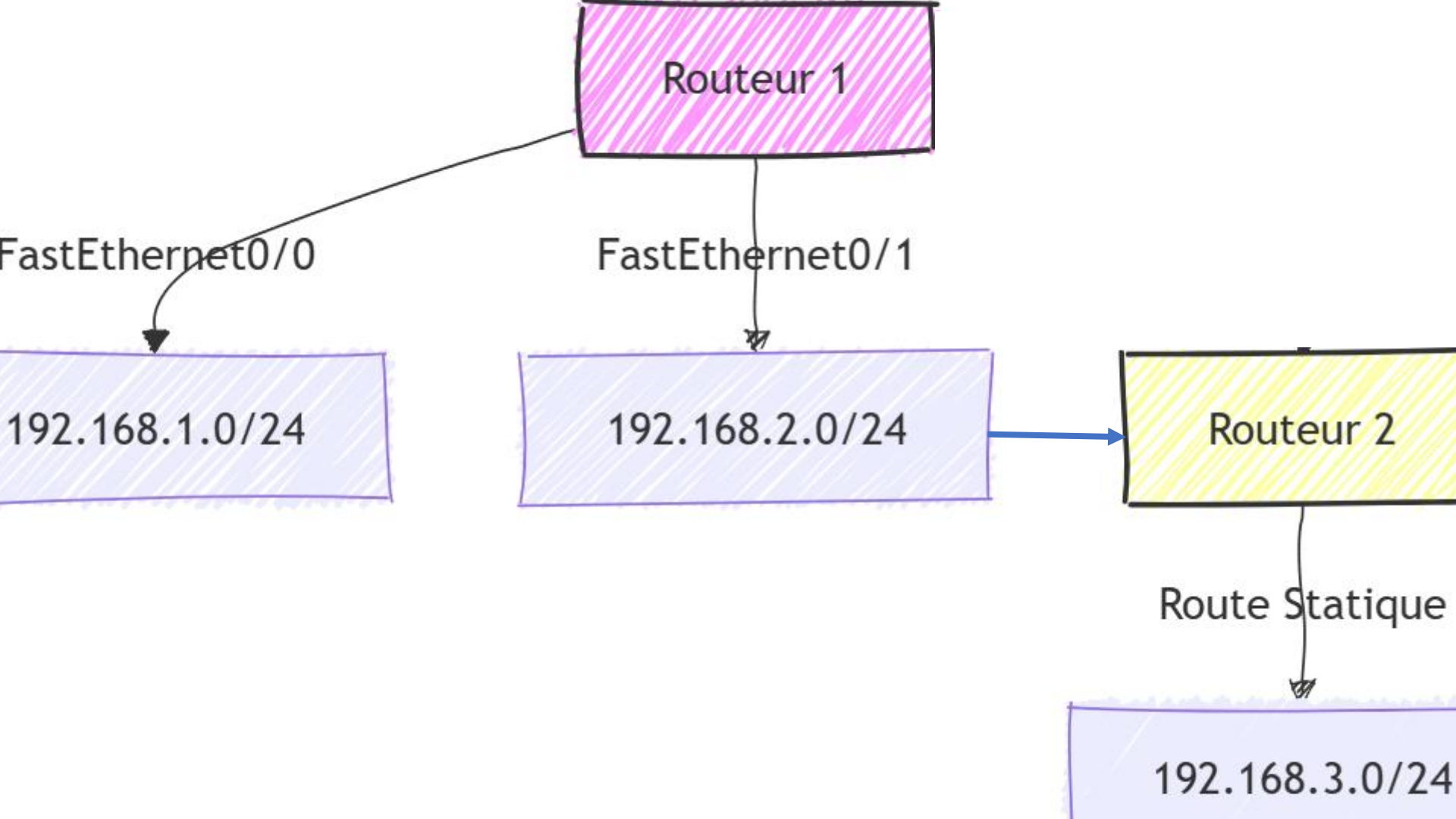
Destination	Masque de sous-réseau	Prochain saut	Interface	Distance administrative	Métrique (Coût)
192.168.1.0	255.255.255.0	N/A	FastEthernet0/0	N/A	N/A
192.168.2.0	255.255.255.0	N/A	FastEthernet0/1	N/A	N/A
192.168.3.0	255.255.255.0	192.168.2.1	FastEthernet0/3	1	0
0.0.0.0	0.0.0.0	192.168.2.1	FastEthernet0/3	1	0

explications

Table de Routage

Destination	Masque de sous-réseau	Prochain saut	Interface	Distance administrative	Métrique (Coût)
192.168.1.0	255.255.255.0	N/A	FastEthernet0/0	N/A	N/A
192.168.2.0	255.255.255.0	N/A	FastEthernet0/1	N/A	N/A
192.168.3.0	255.255.255.0	192.168.2.1	FastEthernet0/3	1	0
0.0.0.0	0.0.0.0	192.168.2.1	FastEthernet0/3	1	0

•**Destination** : Le réseau de destination ou l'adresse IP que vous souhaitez atteindre.
•**Masque de sous-réseau** : Le masque de sous-réseau qui détermine la plage d'adresses pour la destination.
•**Prochain saut** : L'adresse IP du prochain routeur ou périphérique auquel les paquets doivent être envoyés pour atteindre la destination.
•**Interface** : L'interface réseau sur le périphérique de routage utilisée pour envoyer les paquets vers la destination ou le prochain saut.
•**Distance administrative** : Une valeur indiquant la fiabilité de la route. Plus la distance est faible, plus la route est fiable. Les routes connectées ont une distance administrative de 0, les routes statiques ont généralement une distance de 1, etc.
•**Métrique (Coût)** : Une valeur utilisée pour déterminer la "meilleure" route en cas de routes multiples. Elle peut être affectée par des protocoles de routage comme RIP, OSPF ou EIGRP. Une métrique plus faible indique une route préférée.


Routeur 1
FastEthernet0/0
FastEthernet0/1
192.168.1.0/24
192.168.2.0/24
Routeur 2
Route Statique
192.168.3.0/24

- 1 Définir la passerelle par défaut :

- Directement connecté
- ip addr add 192.168.1.100/24 dev eth0
- ip addr add 192.168.2.100/24 dev eth1

- Route statique
- ip route add 192.168.3.0/24 via 192.168.2.1 dev eth1

Linux

- $ ip route show

default via 192.168.1.1 dev eth0
192.168.1.0/24 dev eth0 scope link src 192.168.1.100
192.168.2.0/24 dev eth1 scope link src 192.168.2.100
192.168.3.0/24 via 192.168.2.1 dev eth1

Cisco

```
ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip route 192.168.1.0 255.255.255.0 Ethernet0
ip route 192.168.2.0 255.255.255.0 Ethernet1
ip route 192.168.3.0 255.255.255.0 192.168.2.1
```

Cisco

- **Router**# show ip route

Gateway of last resort is 192.168.1.1 to network 0.0.0.0

S* 0.0.0.0/0 [1] via 192.168.1.1
C 192.168.1.0/24 is directly connected, Ethernet0
C 192.168.2.0/24 is directly connected, Ethernet1
S 192.168.3.0/24 [1] via 192.168.2.1

Explication des codes dans la table de routage Cisco :

- **C** : Connectée (réseau directement connecté).
- **S** : Statique (route configurée manuellement).

AS ?

Introduction aux AS (Autonomous Systems) 🌍

📌 Définition :

- Un **AS (Autonomous System)** est un ensemble de réseaux sous une même administration.
- Chaque AS est identifié par un numéro unique appelé **ASN (Autonomous System Number)** 🔢.
- Internet est composé de **milliers d'AS** interconnectés.

📡 Pourquoi sont-ils importants ?

- Ils assurent **le bon fonctionnement du routage sur Internet**.
- Ils permettent aux **FAI, entreprises et organisations** d'échanger du trafic efficacement.

Exemples d'AS 📶

- 📡 **Quelques exemples de grands AS :**
- **Google** 🌐 → AS15169 ☐
- **Facebook (Meta)** 📘 → AS32934 🟢
- **Cloudflare** ☁️☐ → AS13335 ☐
- **Orange** 📶 → AS3215 ☐

Pourquoi les AS sont essentiels ? ☐

- 🔗 **Les AS sont indispensables pour :**

✅ **L'interconnexion mondiale d'Internet.**
✅ **L'optimisation des routes et la redondance.**
✅ **Le contrôle du routage par les entreprises et fournisseurs.**

- 📡 **En résumé** : Sans AS, **Internet ne fonctionnerait pas** !

Informations générales sur l'AS15169

- **Nom de l'organisation** : Google LLC
- **Pays d'origine** : États-Unis
- **Site web** : https://about.google

- **Détails techniques**
- **Nombre de préfixes IPv4 annoncés** : 1 158
- **Nombre de préfixes IPv6 annoncés** : 107
- **Nombre total d'adresses IPv4** : 9 127 424
- **Nombre total d'adresses IPv6** : $1{,}82 \times 10^{38}$
- **Type d'ASN** : Hébergement

Détails techniques du réseau de Google 📡

- 📌 **Nombre de préfixes annoncés**
  - **IPv4** : **1 158 préfixes**
  - **IPv6** : **107 préfixes**
- 👉 Un **préfixe IP** est une plage d'adresses IP appartenant à un réseau donné. Google annonce **1 158 blocs IPv4** et **107 blocs IPv6**, ce qui montre son infrastructure étendue.

- 📌 **Nombre total d'adresses IP**
  - **IPv4** : **9 127 424 adresses** 🏠
  - **IPv6** : **1,82 × 10^{38} adresses** (presque illimité 😲)

- 👉 **Pourquoi autant d'adresses ?**
  - Google possède **un des plus grands réseaux au monde**, nécessitant des millions d'adresses pour ses serveurs, services cloud et datacenters.
  - En **IPv4**, 9 millions d'adresses, c'est énorme ! Mais Google doit optimiser car IPv4 est limité à **4,3 milliards d'adresses au total**.
  - En **IPv6**, le nombre d'adresses est **quasi-infini** grâce à sa conception, permettant une évolutivité sans contrainte.

Chaque **AS** identifié par un **Numéro de Système Autonome (ASN)**

- En France :

ASN	Organisation
AS3215	Orange S.A.
AS5410	Bouygues Telecom S.A.
AS15557	SFR S.A.
AS30781	Jaguar Network SAS
AS35655	Owentis SARL
AS2486	Société Française du Radiotéléphone S.A.
AS2200	RENATER (Réseau National de télécommunications pour la Technologie, l'Enseignement et la Recherche)
AS16276	**OVH SAS**

INSA INSTITUT NATIONAL DES SCIENCES APPLIQUÉES HAUTS-DE-FRANCE

Université Polytechnique HAUTS-DE-FRANCE

IV. Le routage dynamique

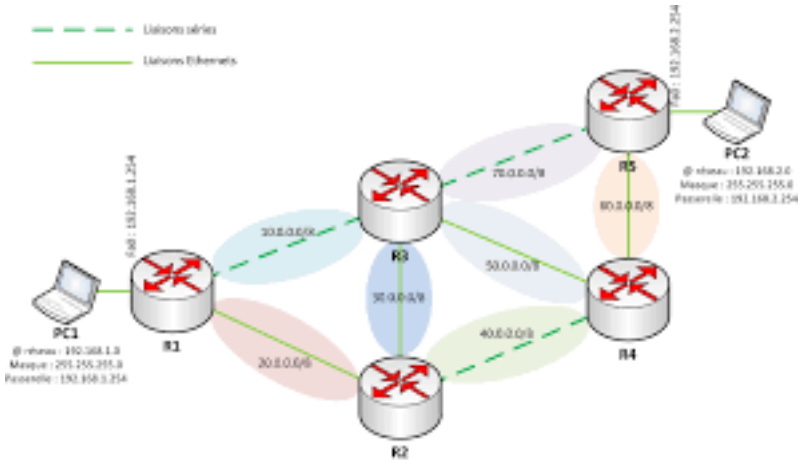
Définition et principe de fonctionnement

- Le **routage dynamique** =
  - **trouver le meilleur chemin**

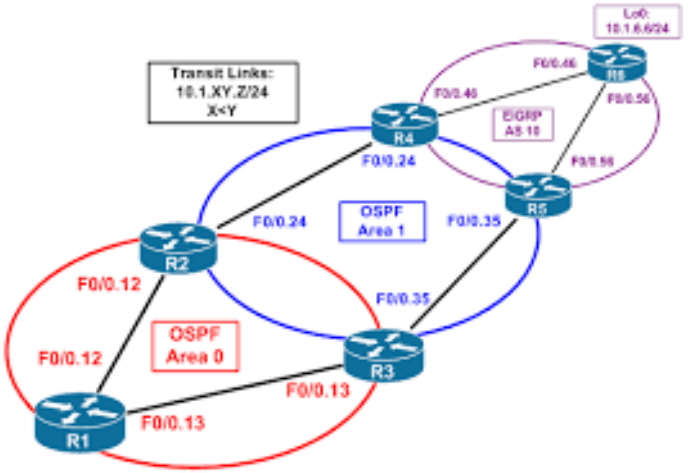
- Il repose sur des **algorithmes de routage** qui permettent aux routeurs de
  - découvrir les réseaux
  - de choisir le meilleur chemin pour y accéder.
  - **de s'échanger des informations de routage** en temps réel
- **protocoles de routage dynamique** :
  - **RIP** (Routing Information Protocol),
  - **OSPF** (Open Shortest Path First) ou
  - **BGP** (Border Gateway Protocol)

RIP (Routing Information Protocol)

- un protocole de routage **à vecteur de distance**
- qui utilise le **nombre de sauts**
- RIP est **simple** à configurer et à utiliser,
- mais peut avoir des performances limitées dans les réseaux de grande taille.



OSPF (Open Shortest Path First)



- **OSPF** (Open Shortest Path First) :
- c'est un protocole de routage **à état de lien**
  - qui utilise la bande passante
  - et la qualité de service
  - **OSPF est plus complexe** à configurer que RIP, mais il est plus performant et évolutif.

- Plus loin :
  - BGP (Border Gateway Protocol),
  - EIGRP (Enhanced Interior Gateway Routing Protocol)
  - IS-IS (Intermediate System to Intermediate System),

Avantages

- **Avantages :**
  - **plus facile à configurer**
    - ✓ car les informations de routage sont **automatiquement** échangées entre les routeurs.
  - plus résilient aux pannes,
    - ✓ car les routeurs peuvent **adapter**
- **Inconvénients**
  - **temps de convergence** plus longs en cas de changements dans le réseau, car les **routeurs doivent échanger des informations** de routage pour rétablir les meilleurs chemins de routage.
  - **plus difficile à configurer et à administrer**

inconvénients du routage dynamique

- **Inconvénients**
  - **temps de convergence** plus longs en cas de changements dans le réseau,
    - ✓ les **routeurs doivent échanger des informations** de routage pour rétablir les meilleurs chemins de routage.
  - **plus difficile à configurer et à administrer**

V. Le routage intra et inter-domaine

Intra-domaine vs inter-domaine

- Le **routage inter-domaine : réseaux appartenant à des domaines différents**, c'est-à-dire à des **organisations ou entreprises distinctes**.

  ➢ préférences de routage et les changements de topologie de réseau.

- **En résumé** :

- une même organisation (routage **intra-domaine**)
- organisations différentes (routage **inter-domaine**).

Intra-domaine

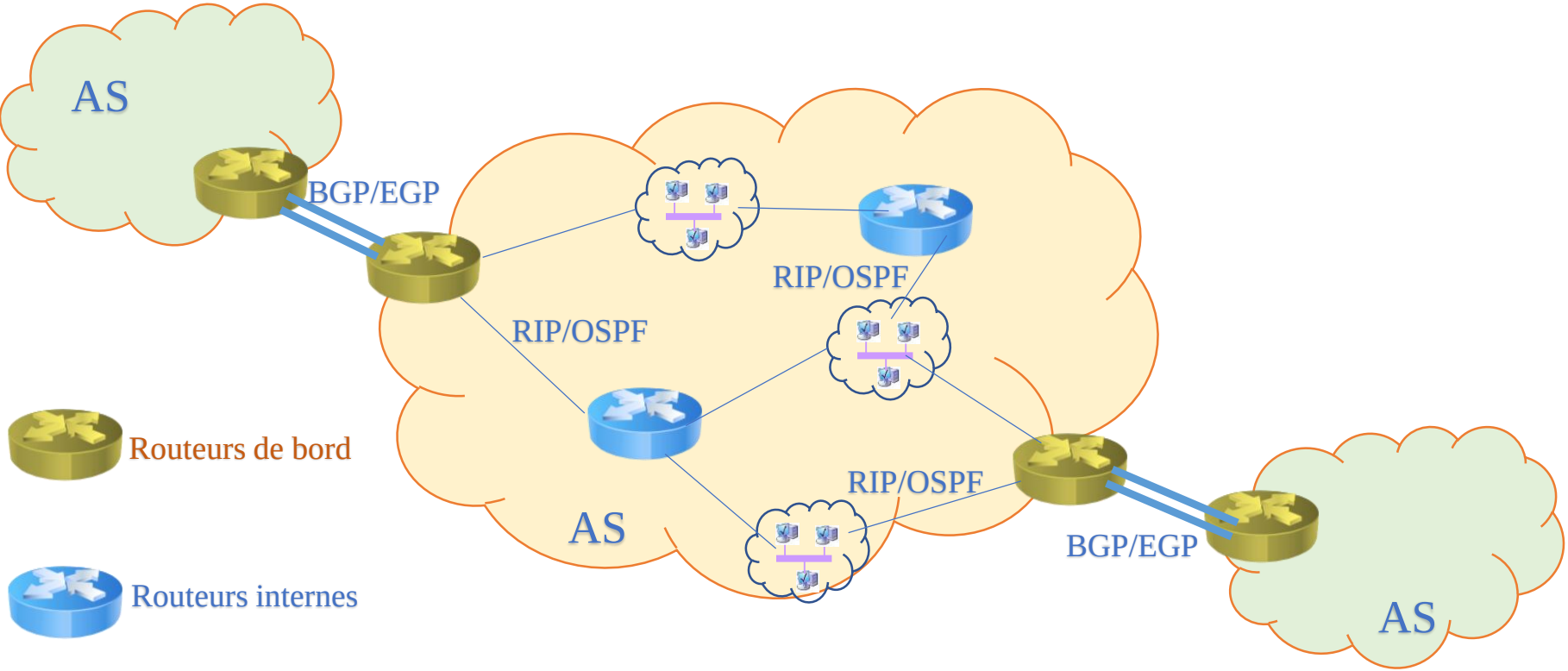
- Le **routage intra-domaine :**
  - transmission des paquets entre les réseaux appartenant à **un même domaine**,
  - c'est-à-dire à une même **entreprise, organisation, des universités**
  - gèrent leur propre infrastructure de réseau.

- Officiellement, ces types de domaine de routage sont appelés **systèmes autonomes** (AS – Autonomous System)
  - Domaine de routage lié à un découpage de l'Internet
  - Responsabilité d'une autorité, un numéro attribuée par l'ICANN identifie de façon unique le domaine.
  - Les protocoles de routage interne ou intra-domaine sont appelés **IGP** (Interior Gateway Protocols) et on y trouve **RIP** et **OSPF**.

Les protocoles de routage inter-domaine (BGP, EIGRP, etc.)

- Les protocoles de routage inter-domaine les plus courants sont **BGP** (Border Gateway Protocol) et **EIGRP** (Enhanced Interior Gateway Routing Protocol).
- **BGP** est le protocole de routage inter-domaine standard pour l'Internet
- **EIGRP** est largement utilisé dans les environnements de réseau d'entreprise.
- Deux approches différentes
  - **BGP** utilise un **algorithme de routage vecteur-distance** pour déterminer les meilleurs chemins entre les réseaux différents
  - **EIGRP** : protocole de routage **hybride** qui utilise une combinaison de techniques de routage de **vecteur-distance** et de **routage à état** de liens

Le routage sur Internet



VII. Sécurité du routage

Les attaques de routage et leurs impacts

- Les attaques peuvent avoir des **impacts importants** sur le fonctionnement du réseau,
  - en **perturbant** le trafic,
  - en **interceptant** les données,
  - en **redirigeant** le trafic vers des destinations non autorisées.

- Pour **prévenir** ces attaques, les entreprises mettent en place :
  - **l'authentification** des **routeurs**,
  - la **surveillance** des **tables de routage**,
  - la **configuration de règles de filtrage**,
  - l'utilisation de **protocoles de routage sécurisés**.
- mettre en place **des plans de continuité d'activité** pour réduire les impacts

Les attaques de routage et leurs impacts

- Les attaques de routage les plus courantes sont :

a) le déni de service (DoS)

- Le DoS consiste à **surcharger le réseau** avec une quantité importante de trafic, ce qui rend le réseau indisponible pour les utilisateurs légitimes.

a) le détournement de trafic (hijacking)

- Le détournement de trafic consiste à **rediriger le trafic** vers des destinations non autorisées, ce qui peut permettre à un hacker d'intercepter les données échangées ou d'usurper l'identité d'un utilisateur.

a) la pollution de la table de routage (route poisoning).

- La pollution de la table de routage consiste à **envoyer de fausses informations de routage** dans le réseau, ce qui peut entraîner des erreurs de routage ou des boucles de routage.

La mise en place de la sécurité du routage dans les réseaux

- la première mesure de sécurité consiste **à limiter l'accès à l'interface de configuration des routeurs** en
  - utilisant des mots de passe forts,
  - des listes de contrôle d'accès (ACL)
  - et des connexions chiffrées.

- Dans le cas de OSPF : **sécurisation de son protocole de contrôle d'admission**

- **clé publique** (PKI) : **l'authenticité des messages échangés entre les routeurs**.

- **tunnels VPN (Virtual Private Network)** connexion chiffrées entre les **différents sites d'une entreprise**.

Les protocoles de sécurité de routage (BGPSEC, RPKI, etc.)

- Les protocoles de sécurité de routage visent à garantir que les **messages de routage sont authentiques** .

- **BGPSEC (Border Gateway Protocol Secure)**

  - une extension du protocole **BGP**, qui est utilisé pour l'échange de messages de routage entre les systèmes autonomes.

  - ajoute des fonctionnalités de sécurité pour empêcher les attaques de type **homme du milieu**

  - pour garantir que les messages de routage sont **authentiques** et n'ont pas été modifiés en transit.

Les protocoles de sécurité de routage (BGPSEC, RPKI, etc.)

- **RPKI** (**Resource Public Key Infrastructure**)
  - ➢ système de **certificats** numériques utilisé pour vérifier **l'authenticité des préfixes IP** annoncés par les routeurs.
  - ➢ Les routeurs peuvent ensuite utiliser RPKI pour vérifier que les préfixes annoncés sont bien authentiques et qu'ils sont autorisés à les annoncer.
- En plus de BGPSEC et RPKI, il existe d'autres
  - ➢ **S-BGP (Secure Border Gateway Protocol)**
  - ➢ **SOBGP (Secure Origin BGP)**.
    - ✓ renforcer la sécurité de BGP et à protéger contre les attaques telles que le détournement de trafic ou la manipulation de messages de routage

Incident Pakistan Telecom et YouTube - 2008

Blocage de Youtube

- En février 2008, Pakistan Telecom a tenté de bloquer l'accès à YouTube
- pour ses utilisateurs locaux
  - en réponse à un ordre gouvernemental.

- Leur intention était de censurer le contenu jugé offensant.

- Pour ce faire, ils ont annoncé des routes BGP spécifiques pour l'adresse IP de YouTube :
  - ,prétendant que ces adresses étaient accessibles via leur réseau
  - "blackholing" (mise en trou noir) du trafic destiné à YouTube

Youtube inaccesible

- au lieu de rester confiné à Pakistan Telecom,
  - ➢ l'annonce a été propagée sur l'Internet global.

- En raison de la façon dont BGP fonctionne :
  - ➢ (les routeurs font confiance aux annonces qu'ils reçoivent sans vérification de l'origine

- beaucoup de trafic Internet mondial destiné à YouTube a été détourné vers Pakistan Telecom :
  - ➢ ce qui a effectivement rendu YouTube inaccessible pour une grande partie du monde pendant plusieurs heures.

VIII. Conclusion

Résumé des points clés sur le routage

- En résumé, le routage est un **élément clé** dans la mise en place et la gestion d'un réseau informatique.
  - Il permet de **diriger** le trafic entre différents réseaux et d'optimiser les performances du réseau.
- Le routage est une **fonctionnalité de la couche 3 du modèle OSI**, c'est-à-dire la couche réseau.
  - C'est cette couche qui gère les adresses IP et les mécanismes de routage qui permettent de **transférer les paquets entre les différents réseaux**.
- Les protocoles de routage (couche 3) , tels que **OSPF, BGP ou RIP**, permettent aux dispositifs de
  - communiquer entre eux pour **échanger** des informations de routage
  - prendre des **décisions** quant aux **meilleurs chemins** pour acheminer les **paquets**.

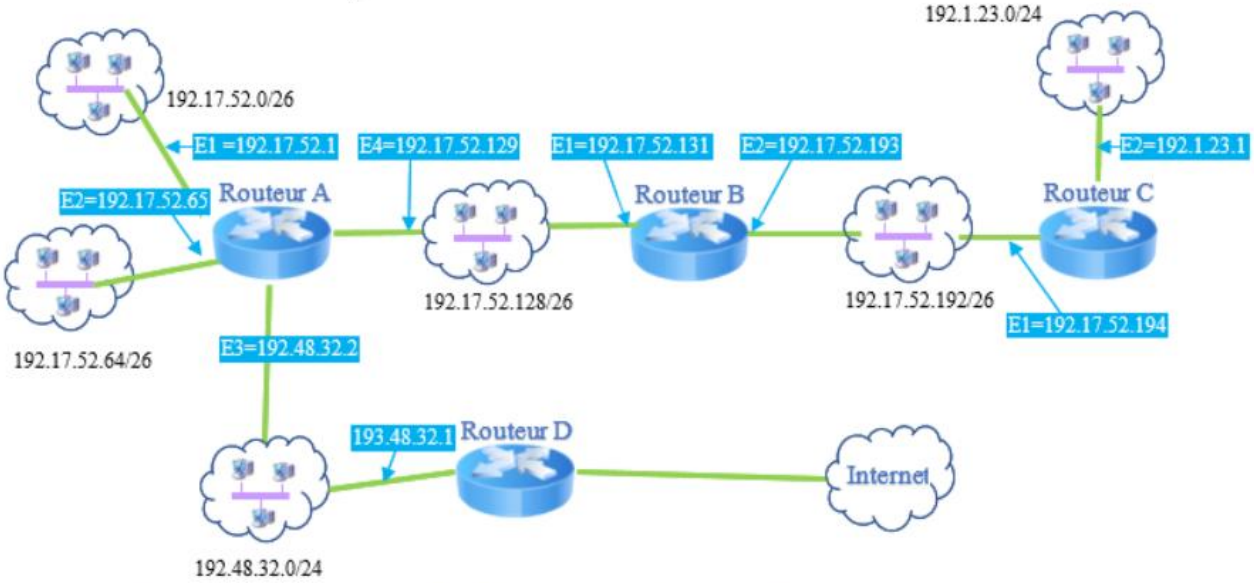
Résumé des points clés sur le routage

- Le **routage avancé**, tel que le **MPLS**, le routage **IPv6** et les **VPN**, permet **d'optimiser les performances** du réseau
- Enfin, le routage est un domaine en constante évolution,
  - avec **l'apparition de nouveaux protocoles**,
  - de **nouveaux équipements**
  - de **nouveaux services** de communication,
  - la **transition vers IPv6**,
  - l'adoption de technologies de routage **avancé et sécurisé**
  - sont autant de défis et d'opportunités pour les professionnels des réseaux informatiques.

Exercice N°2

Exercice N° 2. Table de routage IP

Soit le schéma réseau d'une entreprise :



Question a. Donnez la table de routage du routeur A

Adresse du réseau destination	Masque du réseau destination	Adresse du prochain routeur	Interface	Nb sauts
192.17.52.128	…	…	4	0
…	…	…	…	…


INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
HAUTS-DE-FRANCE
FIN
Université
Polytechnique
HAUTS-DE-FRANCE

Prise de conscience de la sécurité

- Raison ?
- absence de mécanismes de sécurité de BGP
  - pour vérifier l'exactitude des annonces de route.

- RPKI (Resource Public Key Infrastructure)
  - pour aider à valider l'origine des annonces BGP
  - prévenir les détournements de route malveillants ou accidentels.
  - utilise la cryptographie à clé publique
    - pour associer les blocs d'adresses IP (préfixes) aux AS (Autonomous Systems) autorisés à les annoncer

Conclusion

- BGP est un protocole **hybride** : mi à vecteur d'états (Poids OSPF) mi vecteur de distance (sauts RIP)
- c'est plutôt un protocole **à état de liens** :

- Contrairement à d'autres protocoles de routage, il n'y a **pas de transmission périodique** des meilleures routes mais uniquement lors de changement
- Ce protocole permet de stocker toutes les routes vers **toutes les destinations**, en décrivant le chemin emprunté avec une liste des systèmes autonomes (**AS**) traversés.
- Les **caractéristiques** des réseaux internes traversés sont utilisées pour **pondérer** le chemin vers une destination.


INSA
INSTITUT NATIONAL
DES SCIENCES
APPLIQUÉES
HAUTS-DE-FRANCE
FIN
Université
Polytechnique
HAUTS-DE-FRANCE