Introduction à openVPN

David Lebrun – Thibault Gerondal

Louvilug

Jeudi 28 octobre 2010

Petite histoire des réseaux virtuels privés

définition d'un réseau privé virtuel

Un VPN est un ensemble d'outils qui permettent à différents réseaux, à différents endroits, d'être connectés entre eux de façon sécurisée en utilisant un réseau public comme couche de transport.

- Les sociétés à l'époque auraient dépensé des milliers de dollars par mois pour des circuits privés.

Petite histoire des réseaux virtuels privés

définition d'un réseau privé virtuel

Un VPN est un ensemble d'outils qui permettent à différents réseaux, à différents endroits, d'être connectés entre eux de façon sécurisée en utilisant un réseau public comme couche de transport.

- Les sociétés à l'époque auraient dépensé des milliers de dollars par mois pour des circuits privés.
- En même temps se déployait le réseau internet vendant de la bande passante peu chère mais où les données passaient en clair.

Petite histoire des réseaux virtuels privés

définition d'un réseau privé virtuel

Un VPN est un ensemble d'outils qui permettent à différents réseaux, à différents endroits, d'être connectés entre eux de façon sécurisée en utilisant un réseau public comme couche de transport.

- Les sociétés à l'époque auraient dépensé des milliers de dollars par mois pour des circuits privés.
- En même temps se déployait le réseau internet vendant de la bande passante peu chère mais où les données passaient en clair.
- Le concept du VPN était alors de créer virtuellement des circuits dédiés en les faisant passer par internet et en les sécurisant à l'aide de la cryptographie.

Petite histoire des réseaux virtuels privés

définition d'un réseau privé virtuel

Un VPN est un ensemble d'outils qui permettent à différents réseaux, à différents endroits, d'être connectés entre eux de façon sécurisée en utilisant un réseau public comme couche de transport.

- Les sociétés à l'époque auraient dépensé des milliers de dollars par mois pour des circuits privés.
- En même temps se déployait le réseau internet vendant de la bande passante peu chère mais où les données passaient en clair.
- Le concept du VPN était alors de créer virtuellement des circuits dédiés en les faisant passer par internet et en les sécurisant à l'aide de la cryptographie.
- En 1995 sort la première technologie VPN : IPSec.

Quelques exemples d’utilisation

- Utilisation en entreprise pour permettre aux employés d’accéder au réseau intranet de la société à partir de chez eux.

Quelques exemples d’utilisation

- Utilisation en entreprise pour permettre aux employés d’accéder au réseau intranet de la société à partir de chez eux.
- Contourner la restriction d’un jeux qui offre un mode multijoueur en "réseau local”. (principe de Hamachi)

Quelques exemples d’utilisation

- Utilisation en entreprise pour permettre aux employés d’accéder au réseau intranet de la société à partir de chez eux.
- Contourner la restriction d’un jeux qui offre un mode multijoueur en "réseau local”. (principe de Hamachi)
- Contourner un firewall trop restrictif en utilisant une passerelle (gateway) sur le VPN.

Une histoire de tunnels

Les clients connectés à un serveur openVPN créent des tunnels. Les informations passant dans ces derniers sont chiffrées.

définition d'un tunnel

Un tunnel est une encapsulation de données d'un protocole réseau dans un autre.

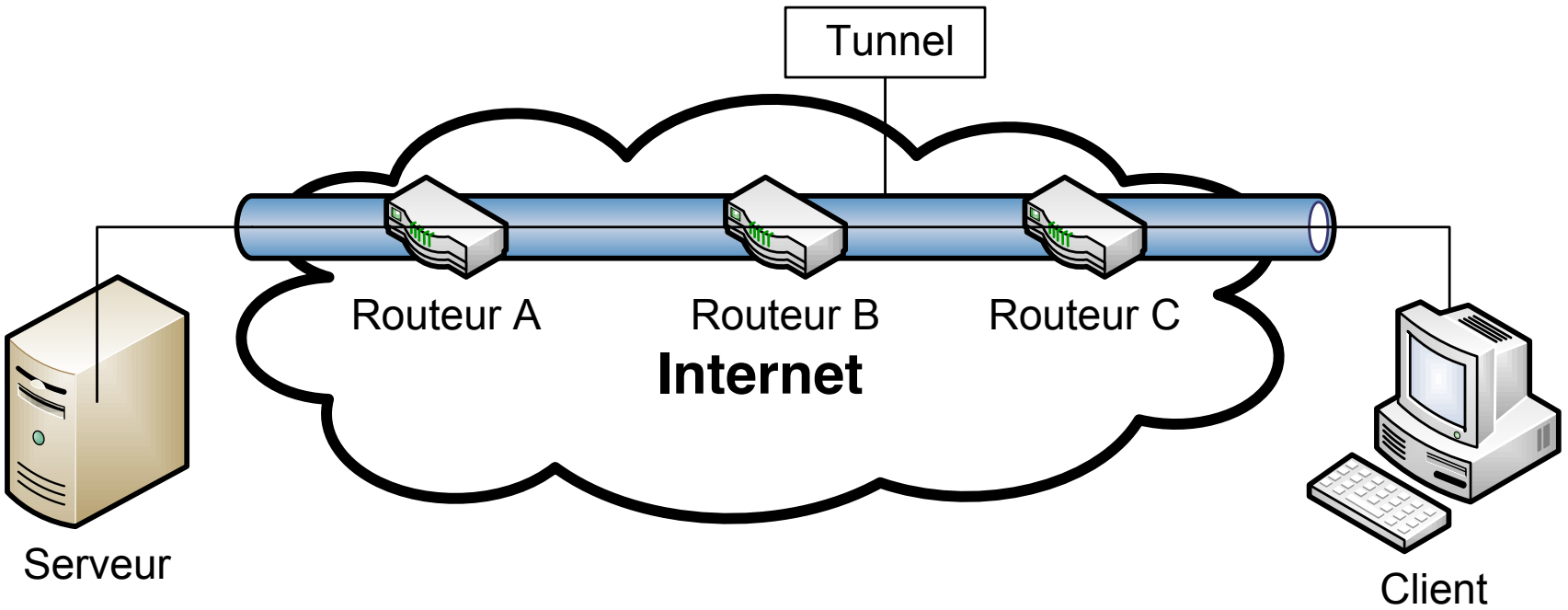


Figure: Tunnelisation

Gestion des clients

- Chaque client connecté sur le réseau virtuel privé se voit attribuer une adresse IP : statique ou dynamique.

Organisation d’un réseau openVPN simple

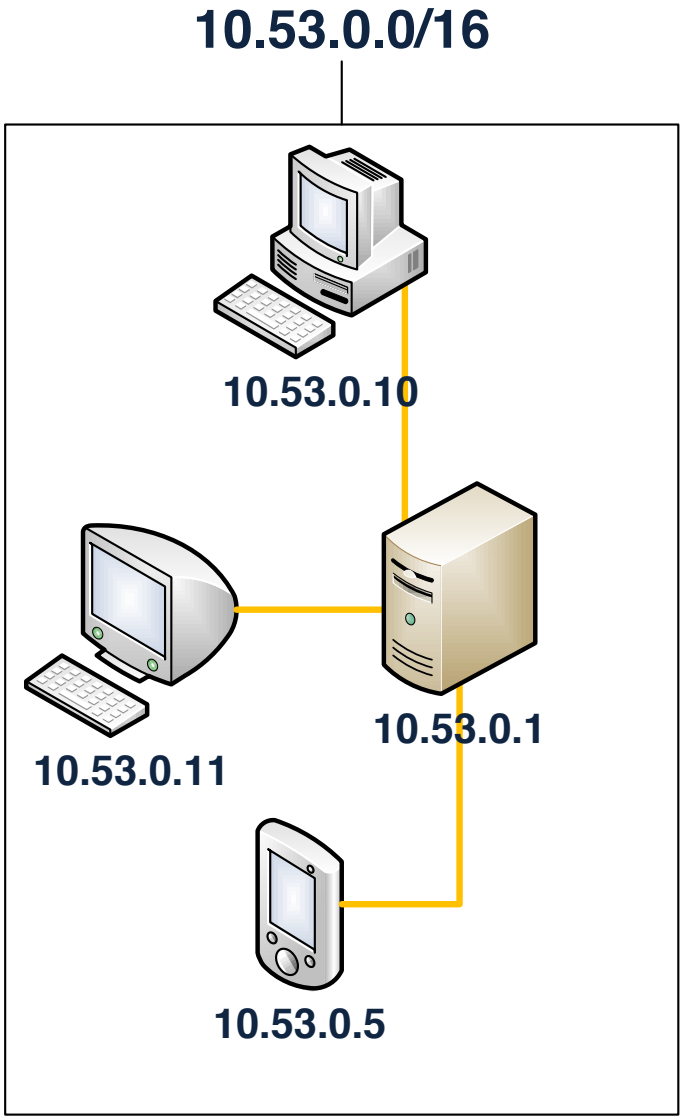


Figure: Exemple d’une réseau virtuel privé openVPN

Gestion des clients

- Chaque client connecté sur le réseau virtuel privé se voit attribuer une adresse IP : statique ou dynamique.
- L'adresse IP du serveur openVPN sur le réseau virtuel privé est fixe.

Organisation d’un réseau openVPN simple

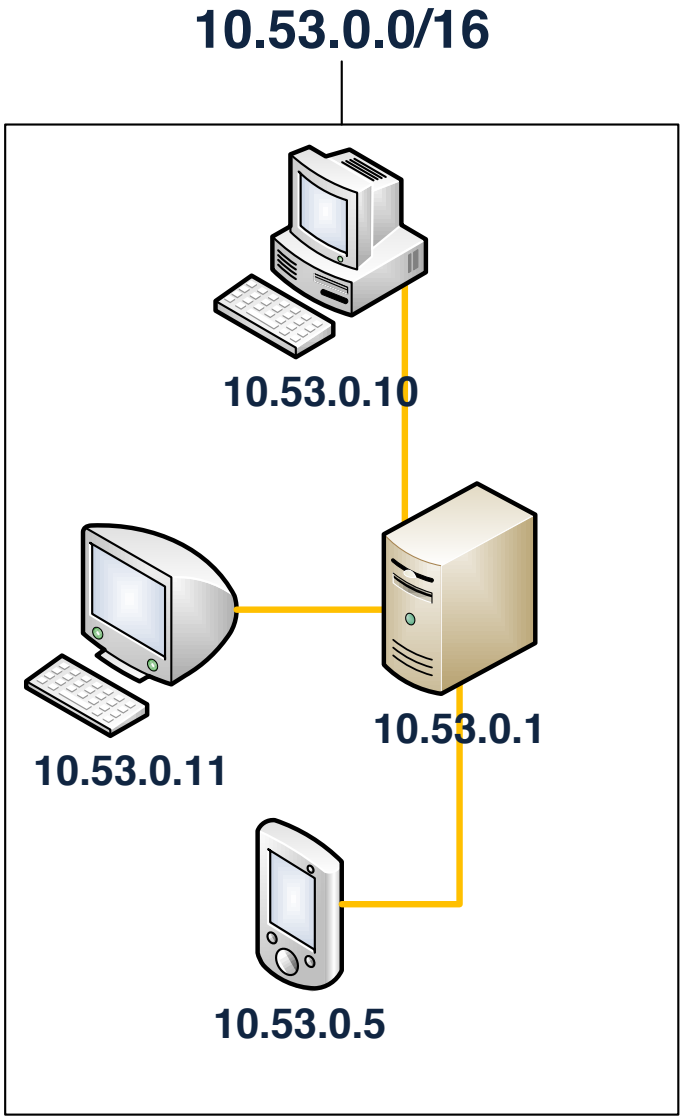


Figure: Exemple d’une réseau virtuel privé openVPN

Gestion des clients

- Chaque client connecté sur le réseau virtuel privé se voit attribuer une adresse IP : statique ou dynamique.
- L'adresse IP du serveur openVPN sur le réseau virtuel privé est fixe.
- Le réseau virtuel privé peut être interconnecté à d'autres.

Organisation d’un réseau avec plusieurs serveurs

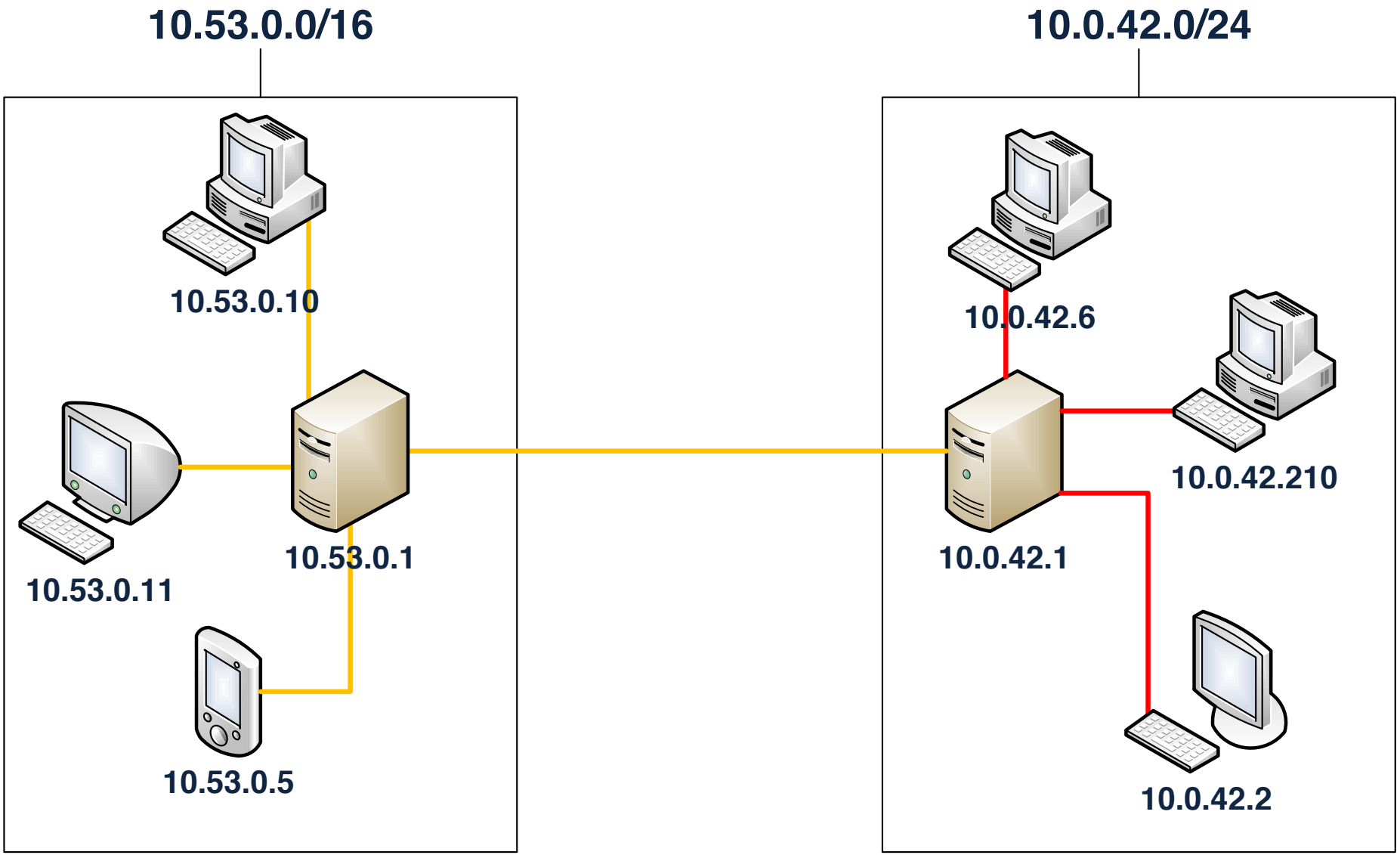


Figure: Exemple d’une interconnexion entre deux VPNs

Principe de la cryptographie asymétrique

- La cryptographie asymétrique est fondée sur l'existence d'une fonction à sens unique.

Principe de la cryptographie asymétrique

- La cryptographie asymétrique est fondée sur l'existence d'une fonction à sens unique.
- Appliquée à un message, il est extrêmement difficile de retrouver le message original.

Principe de la cryptographie asymétrique

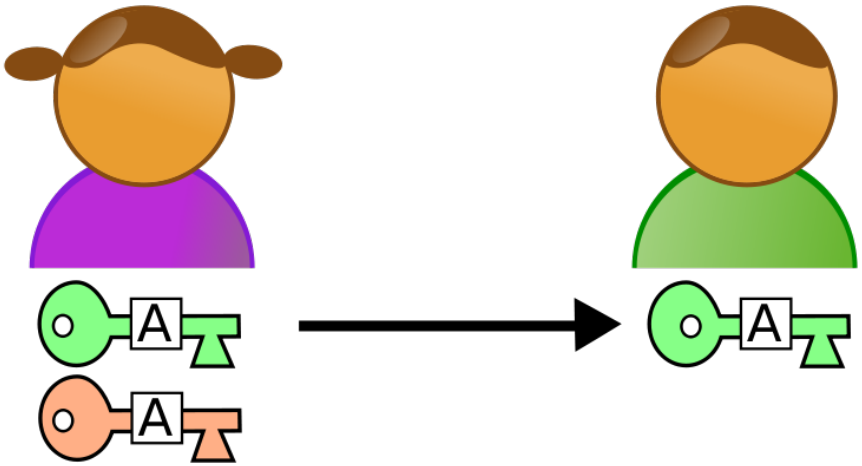
- La cryptographie asymétrique est fondée sur l'existence d'une fonction à sens unique.
- Appliquée à un message, il est extrêmement difficile de retrouver le message original.
- Seul le possesseur d'une information particulière, tenue secrète, nommée clé privée peut déchiffrer le message.

Principe de la cryptographie asymétrique

- La cryptographie asymétrique est fondée sur l'existence d'une fonction à sens unique.
- Appliquée à un message, il est extrêmement difficile de retrouver le message original.
- Seul le possesseur d'une information particulière, tenue secrète, nommée clé privée peut déchiffrer le message.
- Exemple : RSA : Rivest Shamir Adleman.

À partir d'une telle fonction, voici comment se déroulent les choses :

a Alice génère deux clés. La clé publique (verte) qu'elle envoie à Bob et la clé privée (rouge) qu'elle conserve sans la divulguer à quiconque.

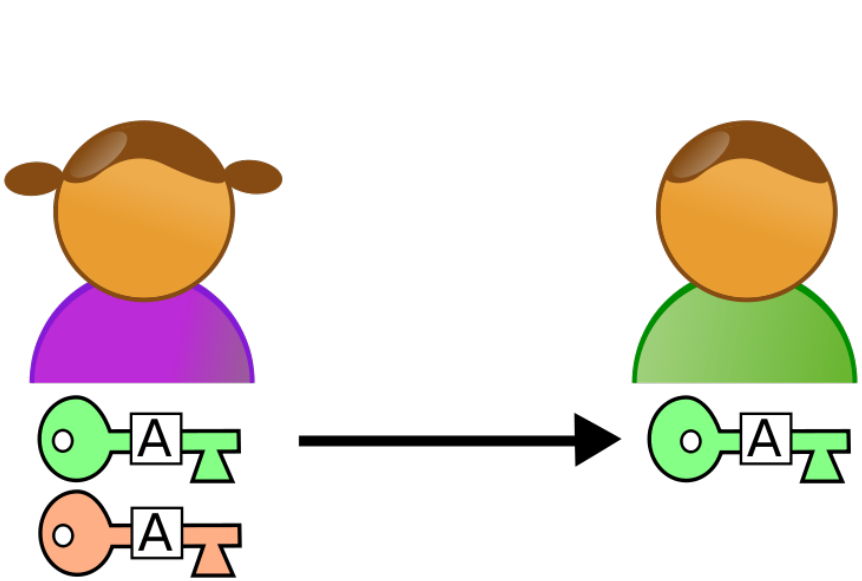


(a) Génération des clés

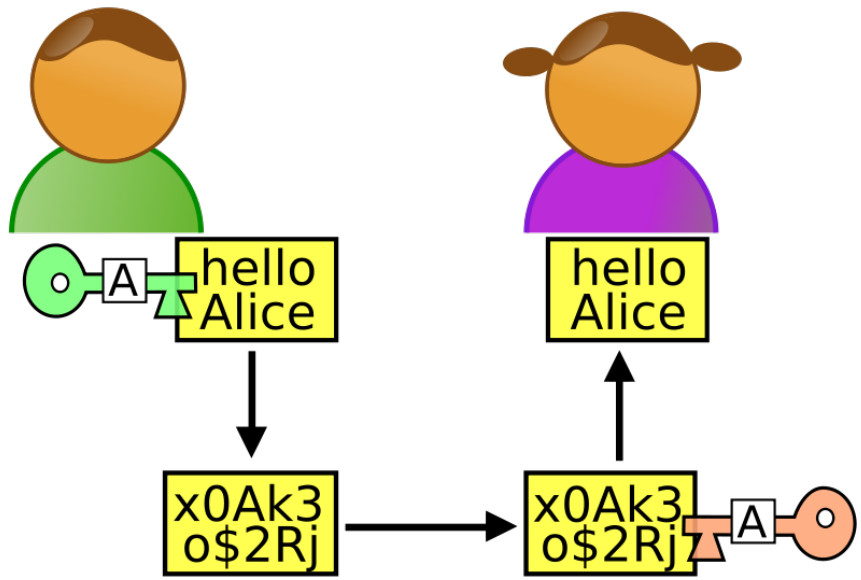
À partir d'une telle fonction, voici comment se déroulent les choses :

a Alice génère deux clés. La clé publique (verte) qu'elle envoie à Bob et la clé privée (rouge) qu'elle conserve sans la divulguer à quiconque.

b Bob chiffre le message en combinant sa clé privée avec la clé publique d'Alice et envoie le texte chiffré. Alice déchiffre le message grâce à sa clé privée.

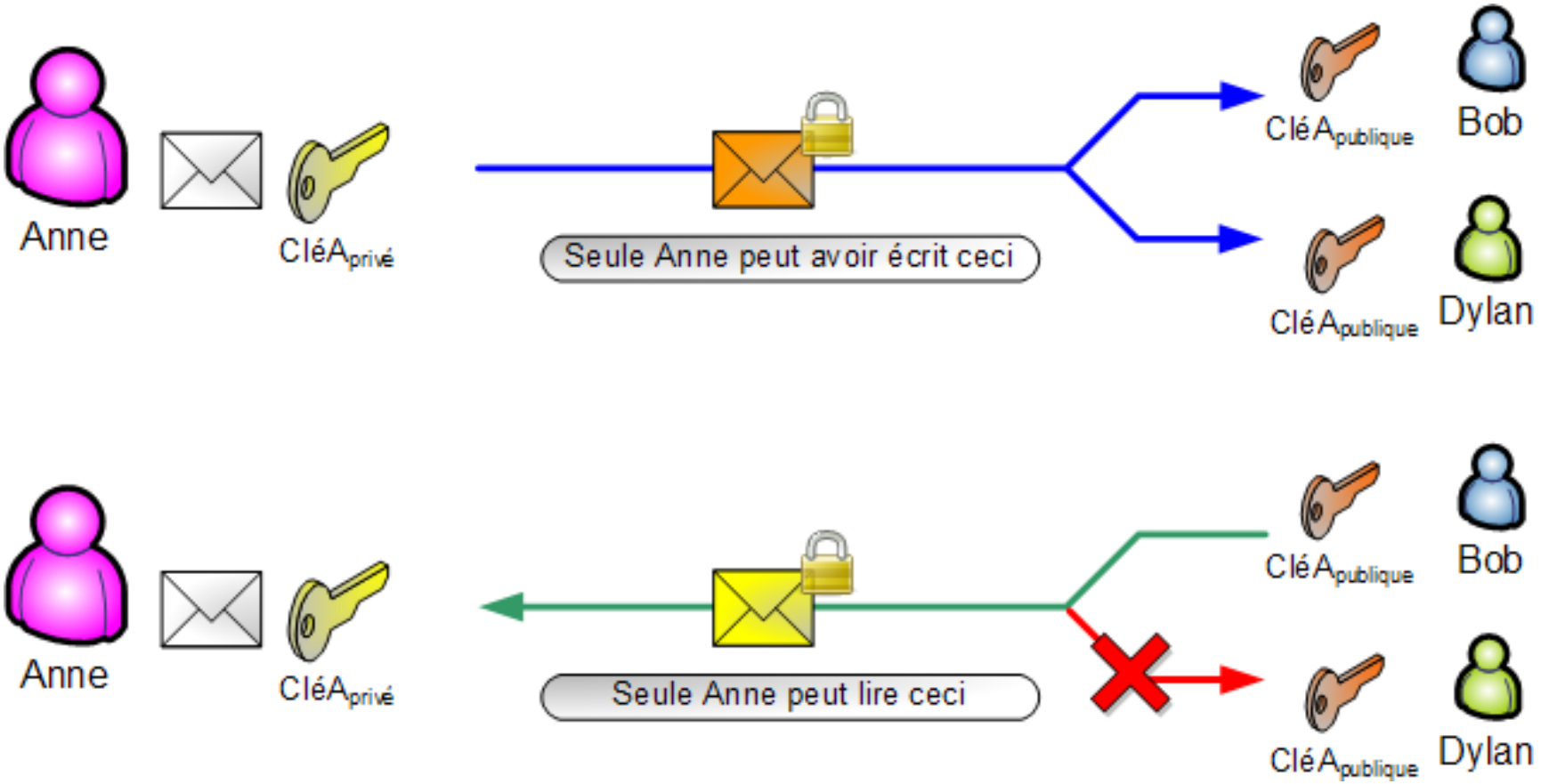


(c) Génération des clés



(d) Chiffrage et déchiffrage

Conséquence



Certificat électronique

Certificat dans openVPN

Un certificat est un fichier permettant de contenir la clé publique ainsi que d'autres informations. Le certificat ajoute une notion de confiance à un référant, générateur du certificat racine, l'Autorité de Certification (AC).

On dit que openVPN est un ensemble d'outils clés en main de création de réseau virtuel privé basé sur la technologie SSL (Secure Socket Layout). Actuellement renommé en TLS (Transport Layer Security).

Certificats d'authentification

- OpenVPN se base sur une infrastructure de **c**lés **p**ubliques (**ICP**, PKI en anglais)

Certificats d'authentification

- OpenVPN se base sur une infrastructure de **c**lés **p**ubliques (**ICP**, PKI en anglais)
- Ce système ne sert qu'à l'authentification.

Certificats d'authentification

- OpenVPN se base sur une infrastructure de **c**lés **p**ubliques (**ICP**, PKI en anglais)
- Ce système ne sert qu'à l'authentification.
- Authentification bidirectionnelle.

Certificats d'authentification

- OpenVPN se base sur une infrastructure de **c**lés **p**ubliques (**ICP**, PKI en anglais)
- Ce système ne sert qu'à l'authentification.
- Authentification bidirectionnelle.
- A partir de ce moment, une confiance mutuelle peut être établie. (tunnel)

Certificats d'authentification

- OpenVPN se base sur une infrastructure de **c**lés **p**ubliques (**ICP**, PKI en anglais)
- Ce système ne sert qu'à l'authentification.
- Authentification bidirectionnelle.
- A partir de ce moment, une confiance mutuelle peut être établie. (tunnel)
- Si la clé privée d'un client est compromise, possibilité de révoquer le certificat.

Exemple

Soit un serveur et un client, alors la liste des certificats et des clés devra ressembler à celui-ci :

Fichier	Possesseur	Description	Secret ?
ca.crt	Serveur et Clients	Certificat racine de l'AC [1]	Non
ca.key	Clé signant la machine seulement	Clé racine de l'AC	Oui
dh1024.pem	Serveur seulement	Paramètre du diffie Hellman	Non
server.crt	Serveur seulement	Certificat serveur	Non
server.key	Serveur seulement	Clé serveur	Oui
client1.crt	Client1 seulement	Certificat client 1	Non
client1.key	Client 1 seulement	Clé client 1	Oui

1. Autorité de Certification

Exemple simple

Pour mieux comprendre comment fonctionne openVPN, nous allons prendre un exemple.

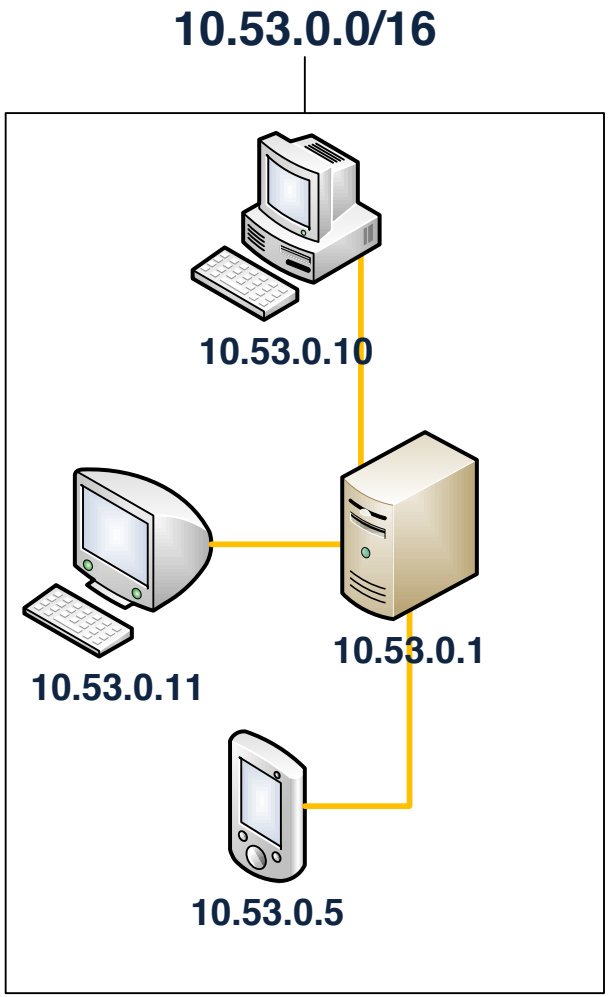


Figure: Exemple d'infrastructure d'un VPN

Configuration côté serveur

```
port 64001
proto udp
dev tap4
ca lug/ca.crt
cert lug/server.crt
key lug/server.key
dh lug/dh1024.pem
server 10.53.0.0 255.255.0.0
client-to-client
user openvpn
group openvpn
cipher AES-256-CBC
```

Configuration côté client

```
client
dev tap3
proto udp
remote tycale.be 64001
ca lug/ca.crt
cert lug/client1.crt
key lug/client1.key
cipher AES-256-CBC
```

Des petits tests côté client

```
    $ ifconfig tap3
tap3: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        ether ea:b2:fc:a9:ae:da
        inet 10.53.0.2 netmask 0xffff0000 broadcast 10.53.255.255
        open (pid 28928)

     $ traceroute tycale.be
traceroute to tycale.be (94.23.150.63), 64 hops max, 52 byte packets
 1  192.168.3.1 (192.168.3.1)  6.331 ms  7.784 ms  7.008 ms
 2  10.183.0.1 (10.183.0.1)  6.477 ms  7.916 ms  8.257 ms
 3  78.129.125.41 (78.129.125.41)  26.299 ms  9.024 ms  6.596 ms
 ...
10  ams-1-6k.nl.eu (94.23.122.129)  80.825 ms  146.522 ms  299.099 ms
11  vss-1-6k.fr.eu (94.23.122.70)  22.731 ms  26.998 ms  29.398 ms
12  tycale.be (94.23.150.63)  21.046 ms  18.866 ms  19.643 ms

     $ traceroute 10.53.0.1
traceroute to 10.53.0.1 (10.53.0.1), 64 hops max, 52 byte packets
 1  10.53.0.1 (10.53.0.1)  53.887 ms  20.966 ms  24.508 ms
```

Organisation d'un réseau avec plusieurs openVPN

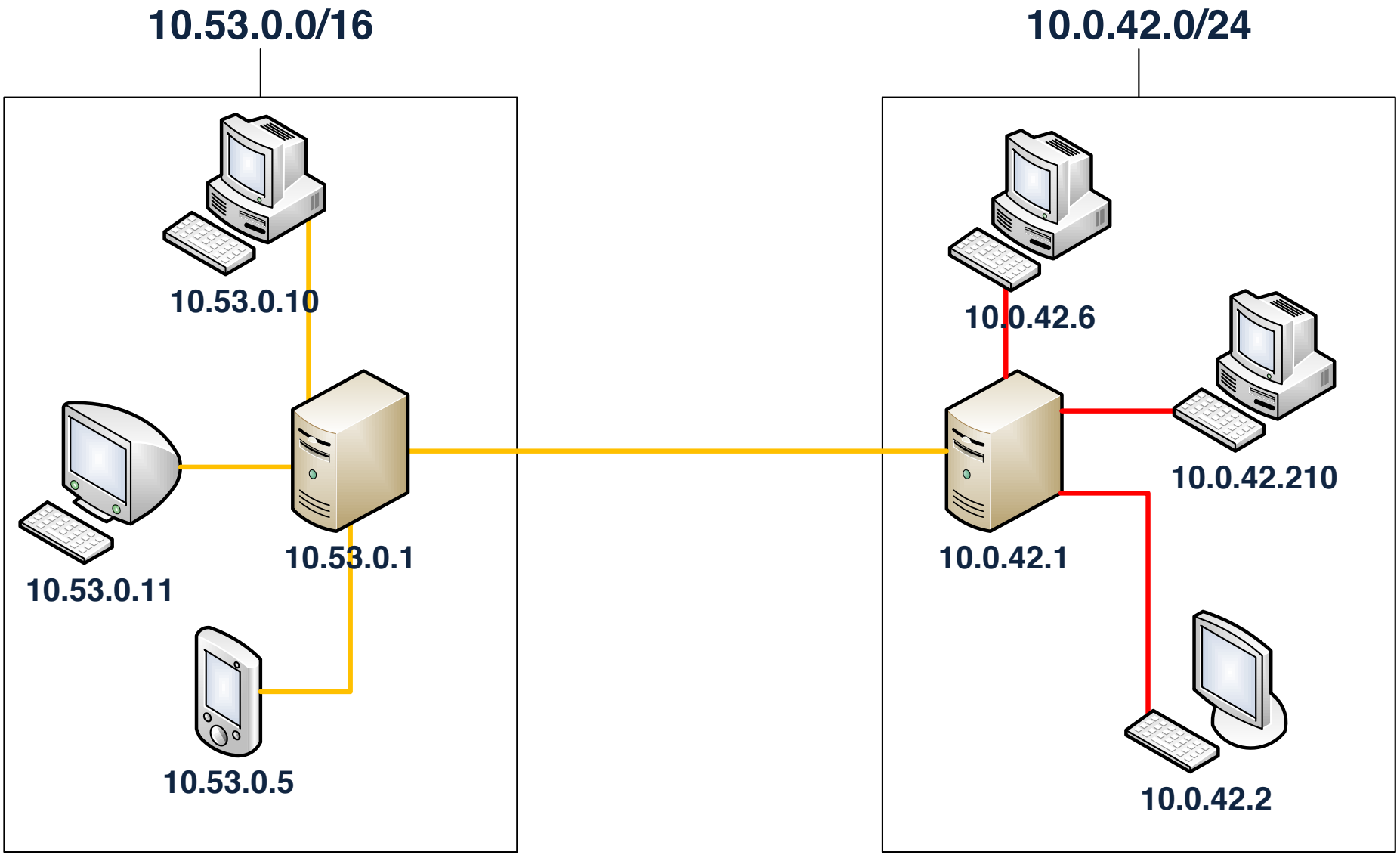


Figure: Exemple d'une interconnexion entre deux VPNs

Comment gérer un réseau avec plusieurs openVPN

- On définit un serveur du réseau virtuel privé comme étant client d'un autre serveur d'un autre réseau virtuel privé.

Comment gérer un réseau avec plusieurs openVPN

- On définit un serveur du réseau virtuel privé comme étant client d'un autre serveur d'un autre réseau virtuel privé.
- Les serveurs doivent annoncer à ses clients la nouvelle parcelle de réseau qui vient d'être ajoutée.

Comment gérer un réseau avec plusieurs openVPN

- On définit un serveur du réseau virtuel privé comme étant client d'un autre serveur d'un autre réseau virtuel privé.
- Les serveurs doivent annoncer à ses clients la nouvelle parcelle de réseau qui vient d'être ajoutée.
- Quand un client d'un réseau openVPN voudra contacter le client d'un autre réseau openVPN il passera donc par minimum deux serveurs openVPN.

Comment gérer un réseau avec plusieurs openVPN

- On définit un serveur du réseau virtuel privé comme étant client d'un autre serveur d'un autre réseau virtuel privé.
- Les serveurs doivent annoncer à ses clients la nouvelle parcelle de réseau qui vient d'être ajoutée.
- Quand un client d'un réseau openVPN voudra contacter le client d'un autre réseau openVPN il passera donc par minimum deux serveurs openVPN.
- Possibilité d'aller encore plus loin avec BGP : Border Gateway Protocol.

Option tun/tap

- option dev (qui veut dire device) en tant que tap : ethernet ou en tant que tun : tunnel.

Option tun/tap

- option dev (qui veut dire device) en tant que tap : ethernet ou en tant que tun : tunnel.

TUN simule un dispositif de couche réseau et opère au 3e niveau de la couche OSI : couche réseau. Comme des paquets IP par exemple.

Option tun/tap

- option dev (qui veut dire device) en tant que tap : ethernet ou en tant que tun : tunnel.

TUN simule un dispositif de couche réseau et opère au 3e niveau de la couche OSI : couche réseau. Comme des paquets IP par exemple.

TAP simule une carte réseau ethernet et opère au 2e niveau de la couche OSI : couche liaison.

Option tun/tap

- option dev (qui veut dire device) en tant que tap : ethernet ou en tant que tun : tunnel.

TUN simule un dispositif de couche réseau et opère au 3e niveau de la couche OSI : couche réseau. Comme des paquets IP par exemple.

TAP simule une carte réseau ethernet et opère au 2e niveau de la couche OSI : couche liaison.

- tap permet de travailler à plus bas niveau et offre donc plus de possibilités.

Option tun/tap

- option dev (qui veut dire device) en tant que tap : ethernet ou en tant que tun : tunnel.

TUN simule un dispositif de couche réseau et opère au 3e niveau de la couche OSI : couche réseau. Comme des paquets IP par exemple.

TAP simule une carte réseau ethernet et opère au 2e niveau de la couche OSI : couche liaison.

- tap permet de travailler à plus bas niveau et offre donc plus de possibilités.
- il est impossible de faire tourner DHCP, ipV6 (dans un tun ipV4), etc. avec l'option dev tun.

OSI Model			
	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation,encryption and decryption,convert machine dependent data to machine independent data
		5. Session	Interhost communication
	Segments	4. Transport	End-to-end connections and reliability,Flow control
Media layers	Packet	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing
	Bit	1. Physical	Media, signal and binary transmission

Figure: Le modèle OSI

Encapsuler du TCP dans du TCP I

- option proto de openVPN nous laisse choisir le protocole à utiliser pour encapsuler nos paquets

Encapsuler du TCP dans du TCP I

- option proto de openVPN nous laisse choisir le protocole à utiliser pour encapsuler nos paquets
- Choix entre du TCP ou de l'UDP

Encapsuler du TCP dans du TCP I

- option proto de openVPN nous laisse choisir le protocole à utiliser pour encapsuler nos paquets
- Choix entre du TCP ou de l'UDP

TCP *(Transmission Control Protocol)* a été conçu pour pouvoir fonctionner sur des réseaux non fiables de sorte à s'assurer que tous les paquets ont été intégralement transmis. Fonctionne en mode connecté. Ex : HTTP, FTP, Telnet, SMTP, etc.

Encapsuler du TCP dans du TCP I

- option proto de openVPN nous laisse choisir le protocole à utiliser pour encapsuler nos paquets
- Choix entre du TCP ou de l'UDP

TCP *(Transmission Control Protocol)* a été conçu pour pouvoir fonctionner sur des réseaux non fiables de sorte à s'assurer que tous les paquets ont été intégralement transmis. Fonctionne en mode connecté. Ex : HTTP, FTP, Telnet, SMTP, etc.

UDP *(User Datagram Protocol)* fonctionne en mode non-connecté. C'est à dire qu'il n'y a aucun moyen pour savoir si les paquets sont bien arrivés. C'est le protocole qui est utilisé dans les jeux vidéo, en visioconférence, etc. Ex : DNS, TFTP, UT2004, etc.

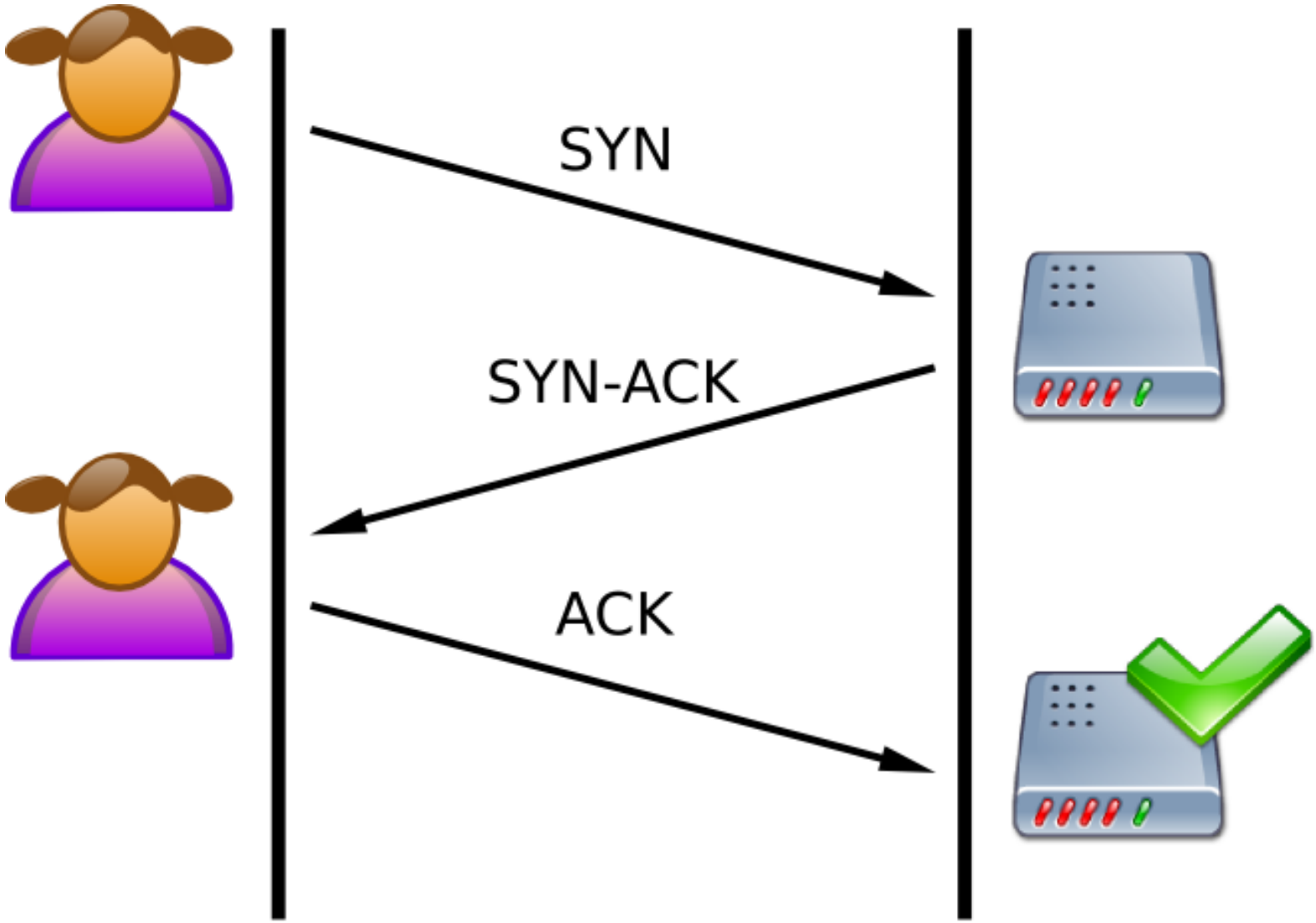


Figure: Le mode connecté du TCP

Encapsuler du TCP dans du TCP II

- Encapsuler du TCP dans du TCP est une mauvaise idée.

Encapsuler du TCP dans du TCP II

- Encapsuler du TCP dans du TCP est une mauvaise idée.
- Redondance au niveau des headers.

Encapsuler du TCP dans du TCP II

- Encapsuler du TCP dans du TCP est une mauvaise idée.
- Redondance au niveau des headers.
- Redondance au niveau du checksum.

Encapsuler du TCP dans du TCP II

- Encapsuler du TCP dans du TCP est une mauvaise idée.
- Redondance au niveau des headers.
- Redondance au niveau du checksum.
- On préfèrera donc l'UDP au TCP.

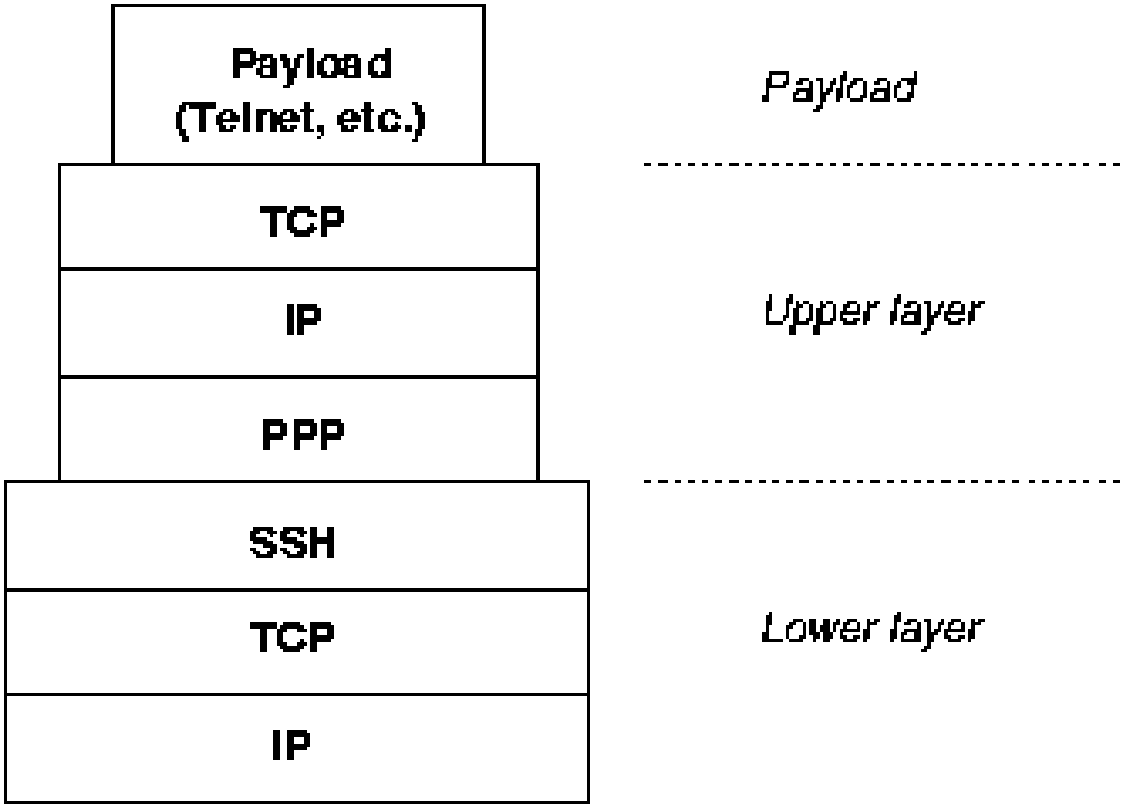


Figure: TCP dans TCP, mauvaise idée.

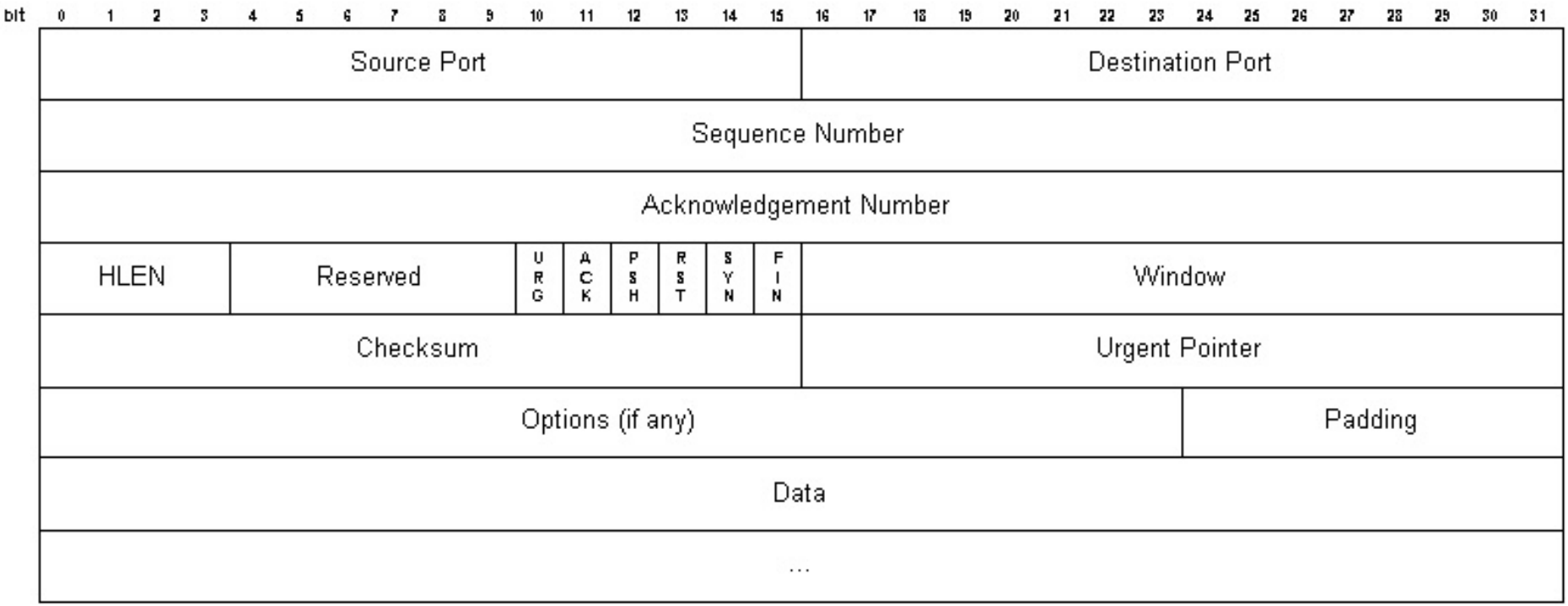


Figure: Header d'un paquet TCP

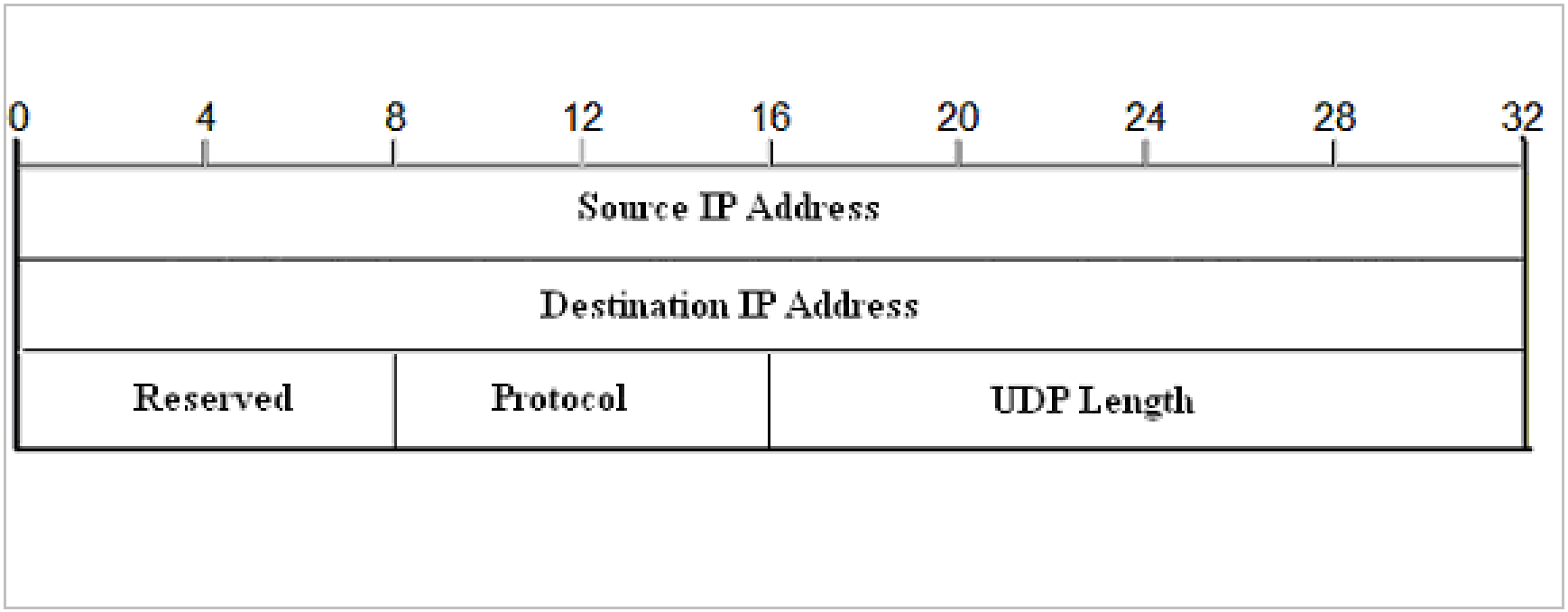


Figure: Header d'un paquet UDP