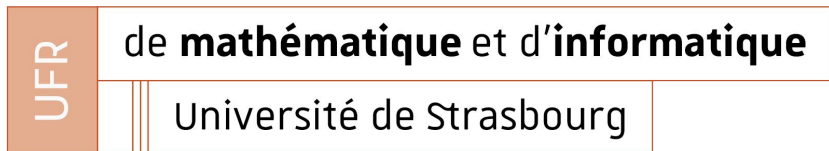


# Les NAT sont-ils infranchissables ?

L2S4 PRDS



Par Carine Wakim & Maxime Zingraff, 10.04.2024

# Rappel de la séance précédente :

Séance précédente:

- Les différents méthodes (*théoriques*) de contournement

→ Aujourd'hui : Comment sont implémentées ces méthodes de contournement ?

# Les technologies de contournement : 2 familles

## 1. Port Forwarding

UPnP, PCP

## 2. Relaying et Hole Punching : ICE PAC/TCP (STUN & TURN)

UPnP : Universal Plug and Play

PCP : Port Control Protocol

ICE PAC : Interactive Connectivity Establishment Patiently Awaiting Connectivity (pour UDP)

ICE TCP : TCP Candidates with Interactive Connectivity Establishment

STUN : Session Traversal Utilities for NAT

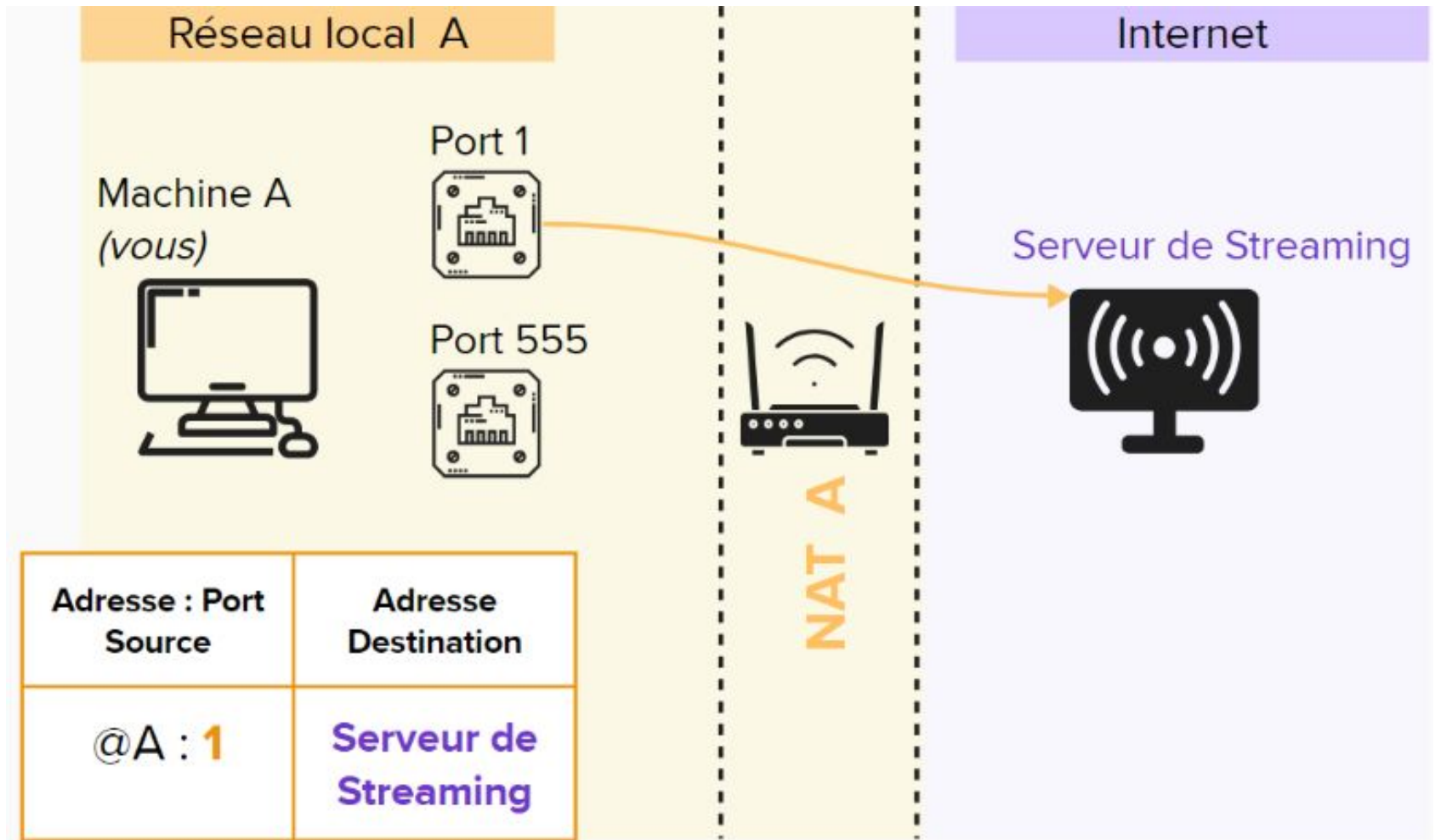
TURN : Traversal Using Relays around NAT

# Le Port Forwarding avec UPnP

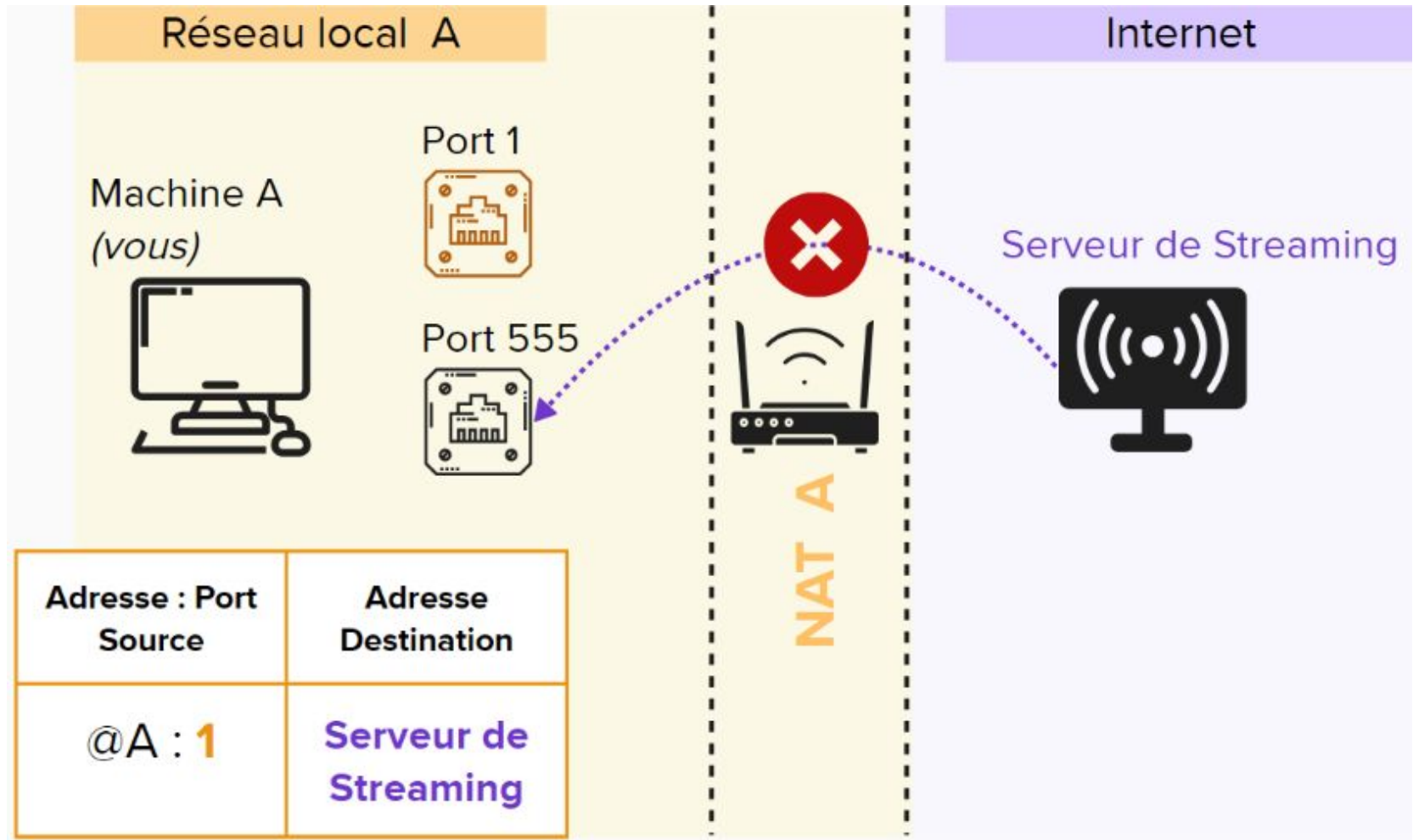
Exemple : Accès à un stream

- NAT Address and Port Dependent (*le plus restrictif*)

# Le Port Forwarding avec UPnP



# Le Port Forwarding avec UPnP



# Le Port Forwarding avec UPnP

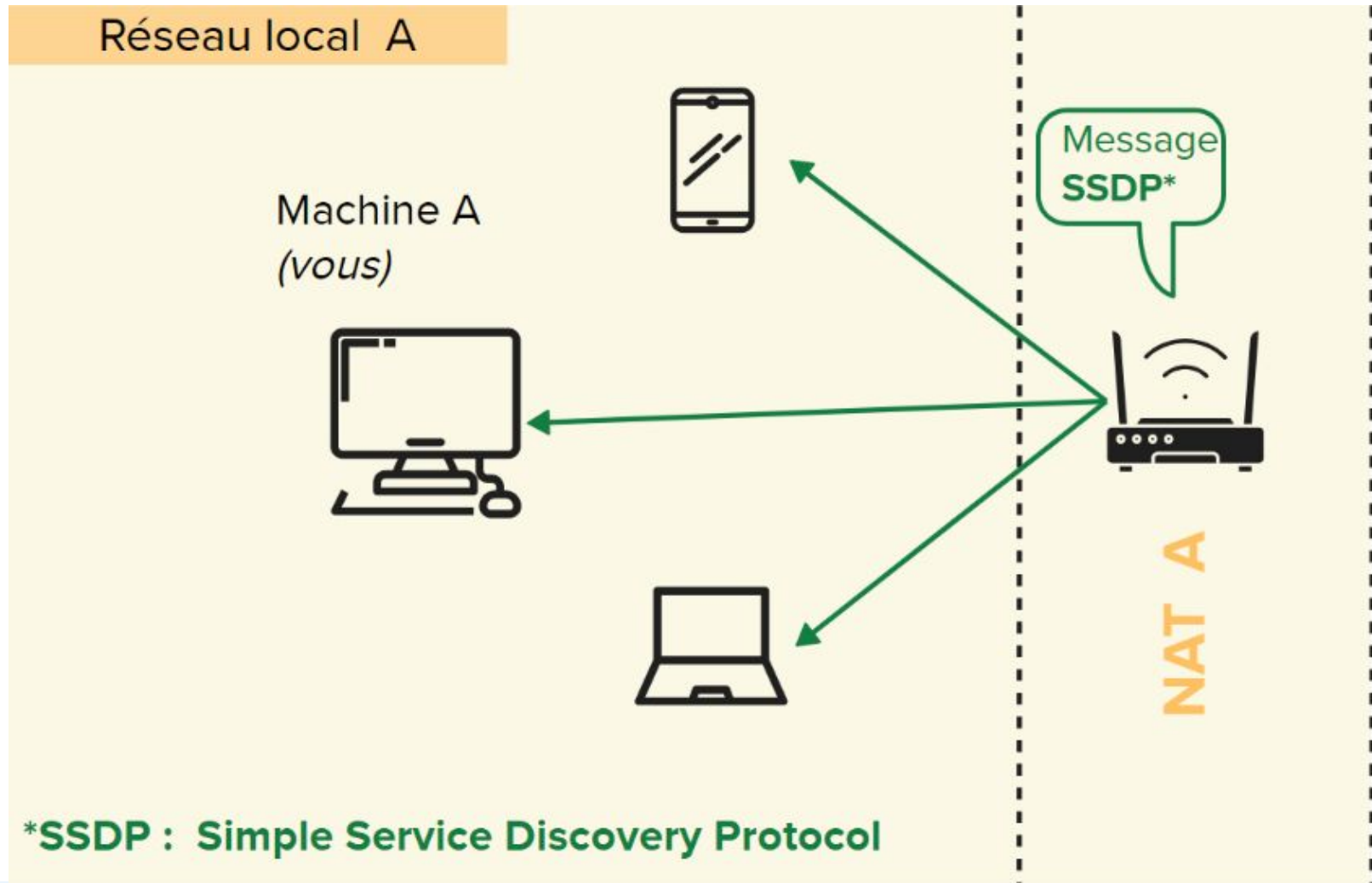
Universal Plug and Play (UPnP) :

➤ Ensemble de protocoles

BUT :

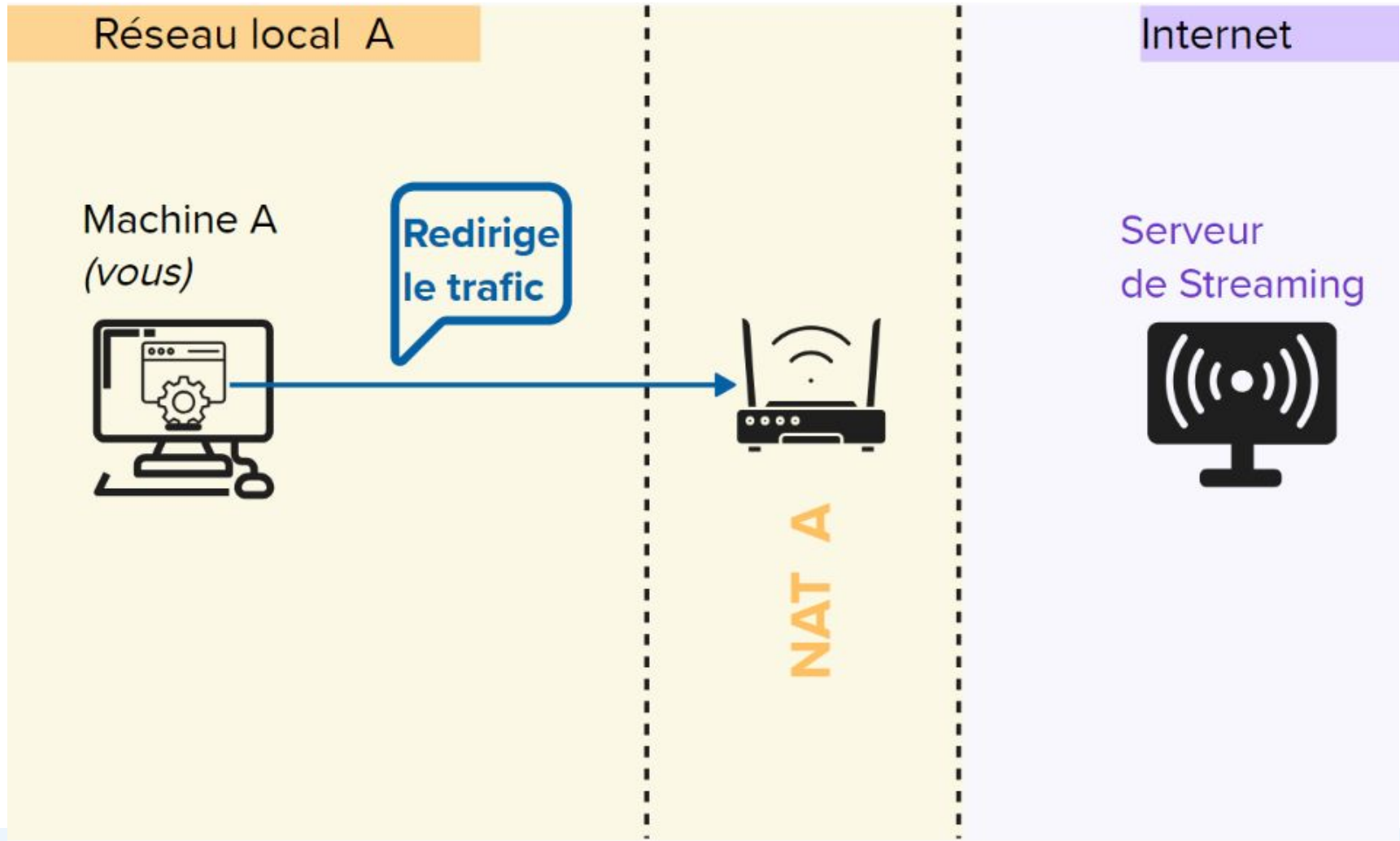
Permettre aux machines d'un réseau local d'interagir automatiquement

# Le Port Forwarding avec UPnP

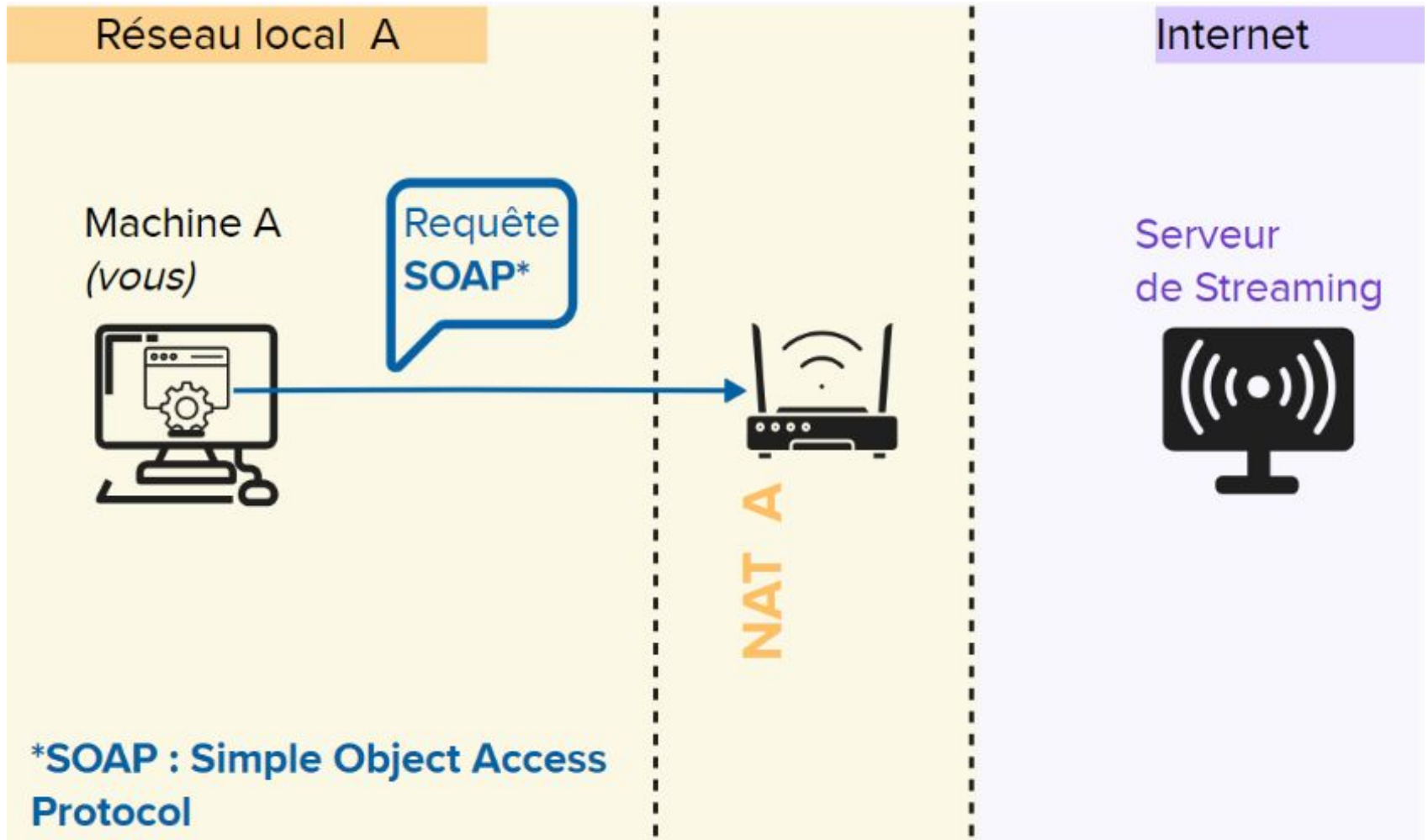




# Le Port Forwarding avec UPnP



# Le Port Forwarding avec UPnP

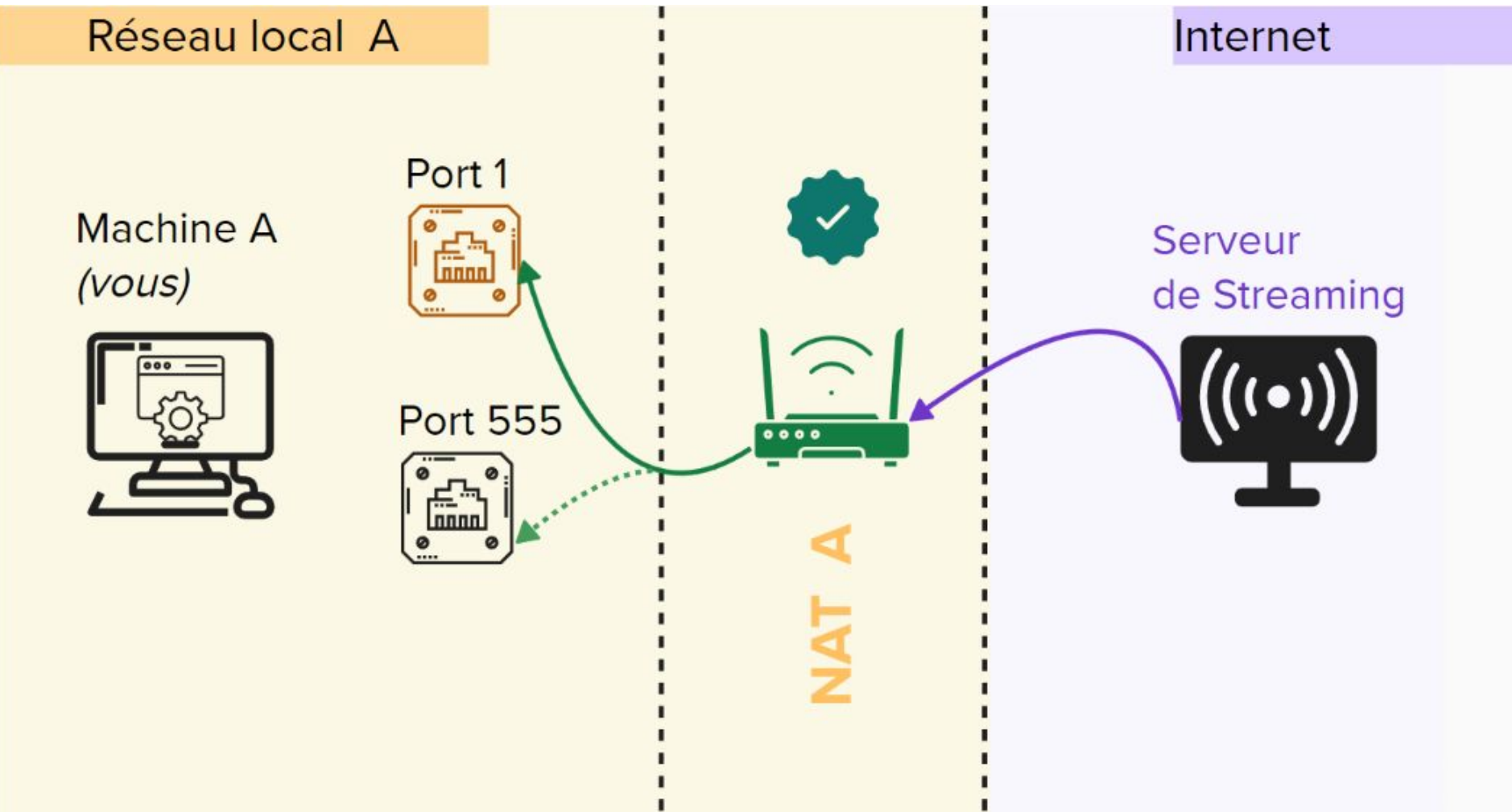


# Le Port Forwarding avec UPnP

## Requête SOAP

```
<?xml version="1.0"?>
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
  SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
    <m:AddPortMapping xmlns:m="urn:schemas-upnp-org:service:WANIPConnection:1">
      <NewRemoteHost></NewRemoteHost>
      <NewExternalPort>555</NewExternalPort>
      <NewProtocol>TCP</NewProtocol>
      <NewInternalPort>1</NewInternalPort>
      <NewInternalClient>192.168.1.100</NewInternalClient>
      <NewEnabled>1</NewEnabled>
      <NewPortMappingDescription>Port Forwarding</NewPortMappingDescription>
      <NewLeaseDuration>0</NewLeaseDuration>
    </m:AddPortMapping>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

# Le Port Forwarding avec UPnP



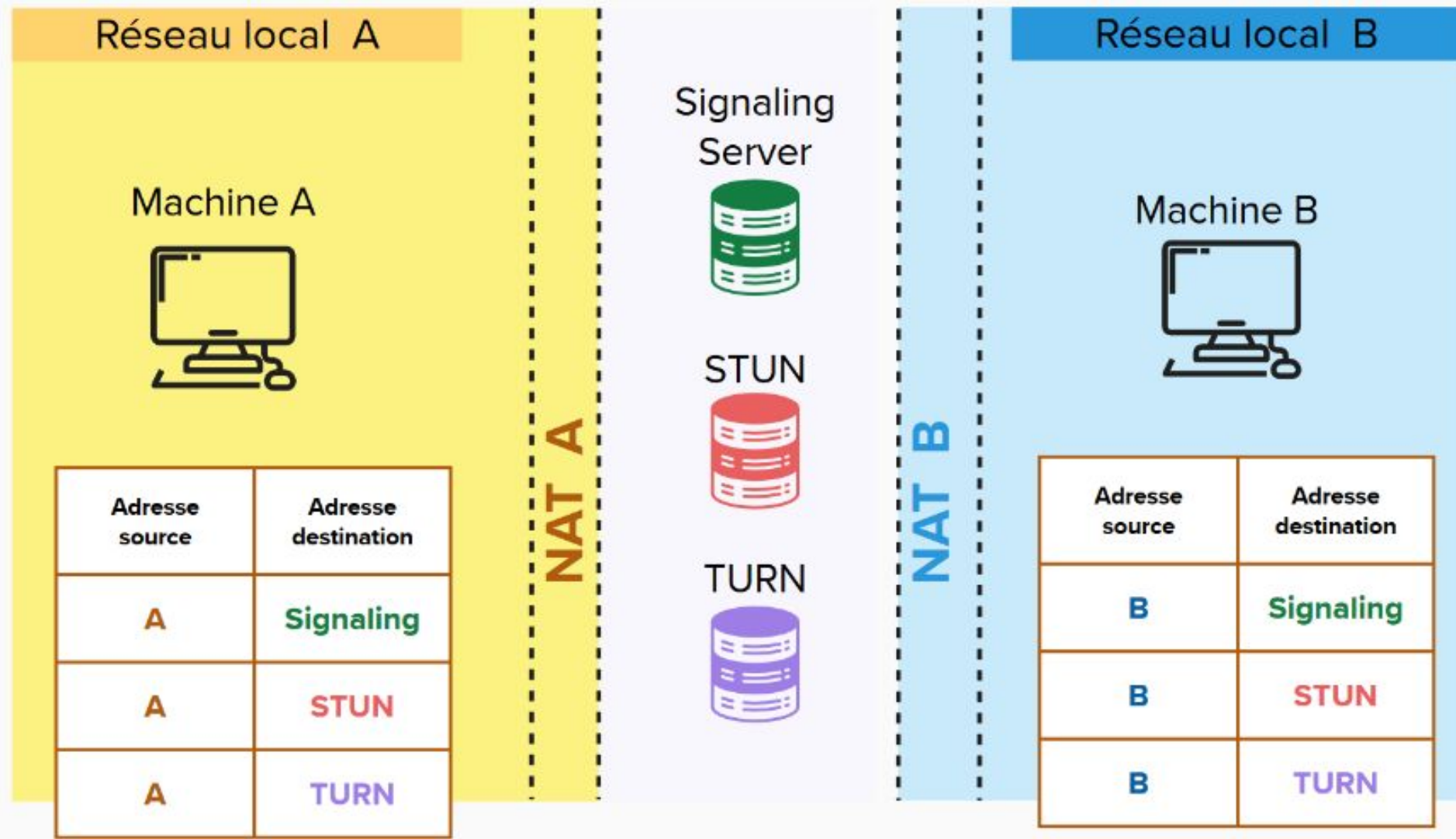
# ICE PAC/TCP (Hole Punching & Relaying)

- Rappel de la dernière présentation :
  - Hole Punching : créer des entrées dans la table NAT de A et de B grâce à un serveur intermédiaire (*STUN*)
  - Relaying : tous les paquets transitent par un serveur intermédiaire (*TURN*)

# ICE PAC/TCP (Hole Punching & Relaying)

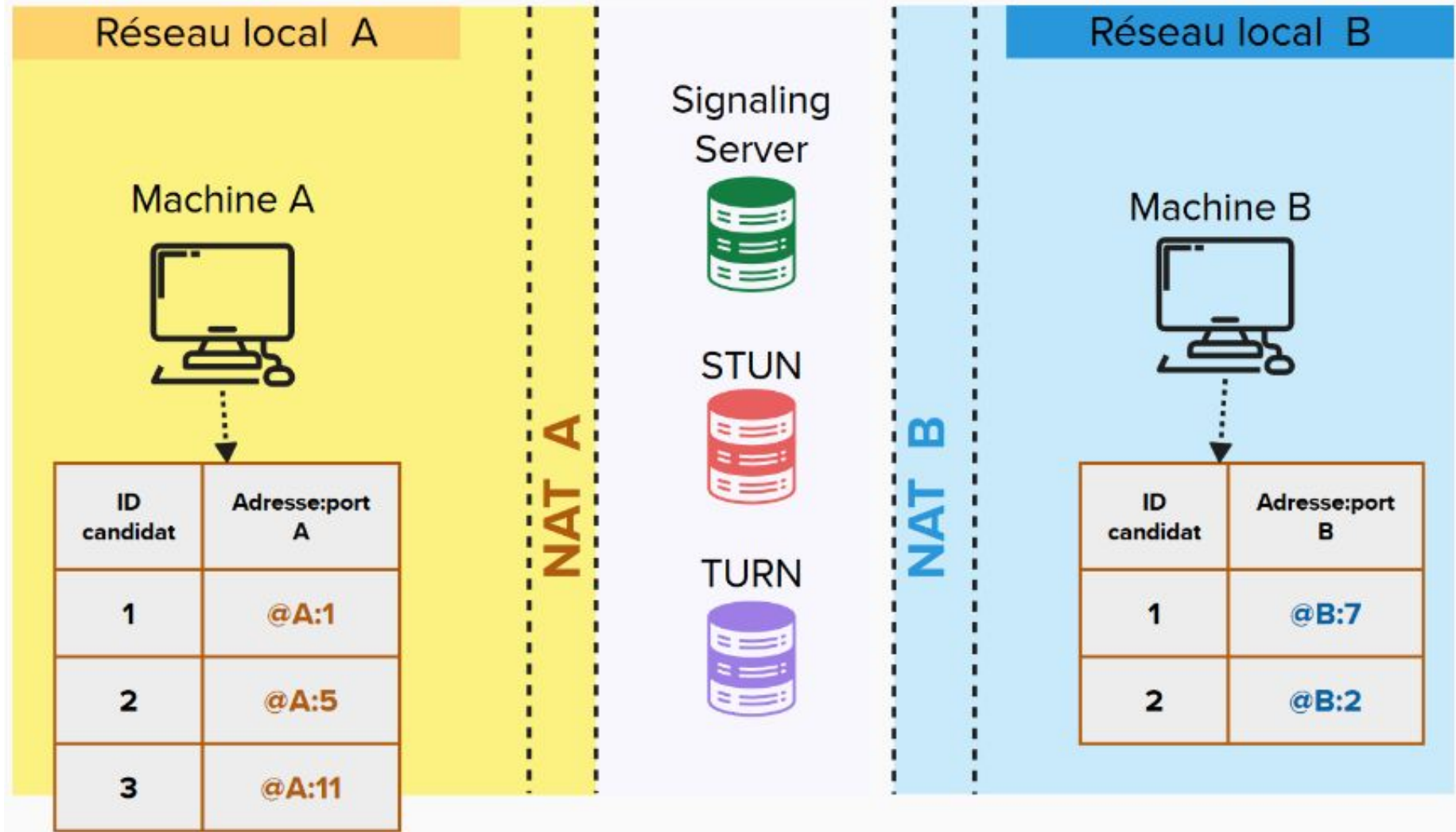
- Rappel de la dernière présentation :
  - Hole Punching : créer des entrées dans la table NAT de A et de B grâce à un serveur intermédiaire (*STUN*)
  - Relaying : tous les paquets transitent par un serveur intermédiaire (*TURN*)
- ICE  $\Rightarrow$  combinaison de STUN (prioritaire) et TURN (secondaire)

# ICE PAC/TCP (Hole Punching & Relaying)



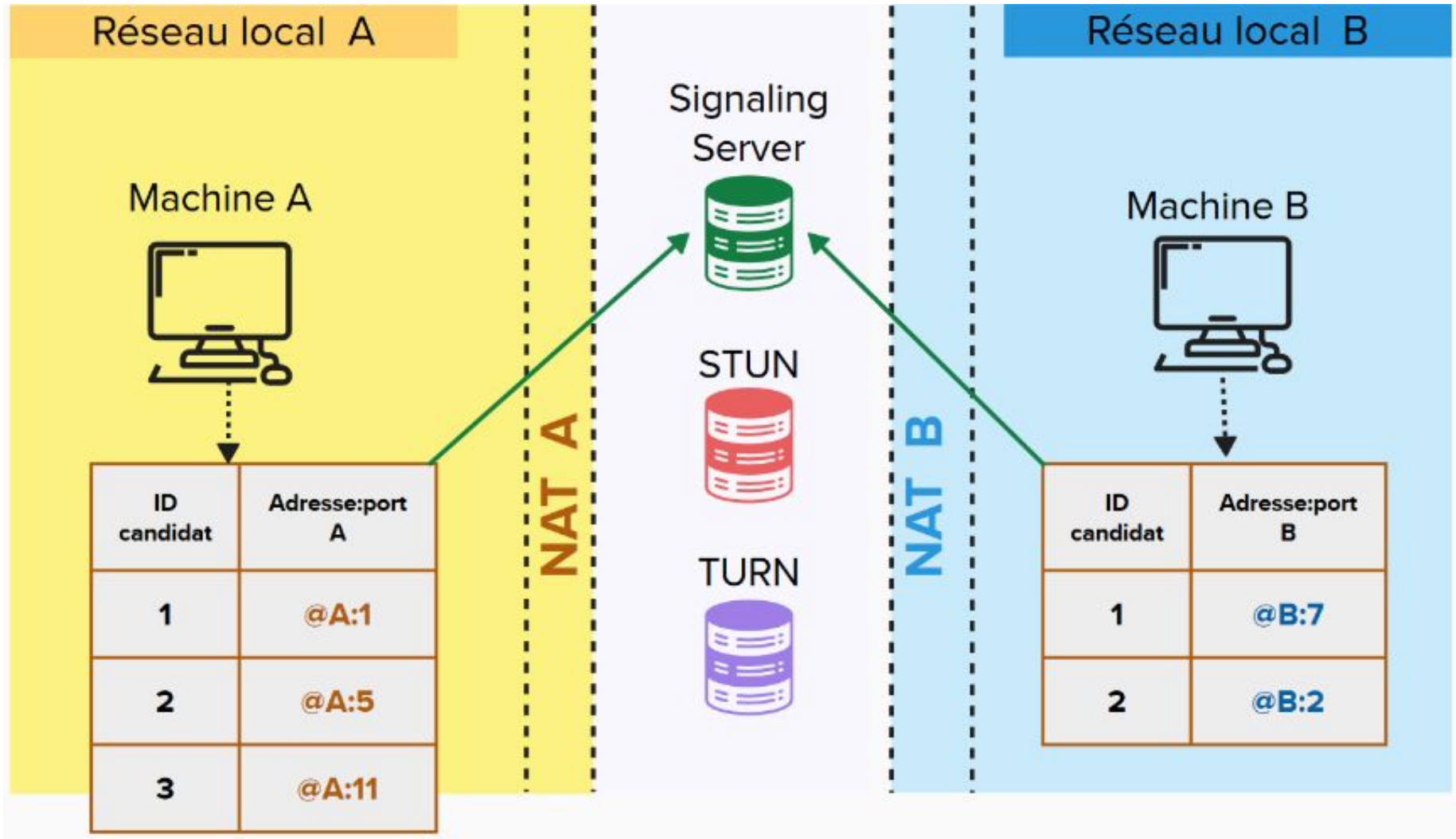


# ICE PAC/TCP (Hole Punching & Relaying)

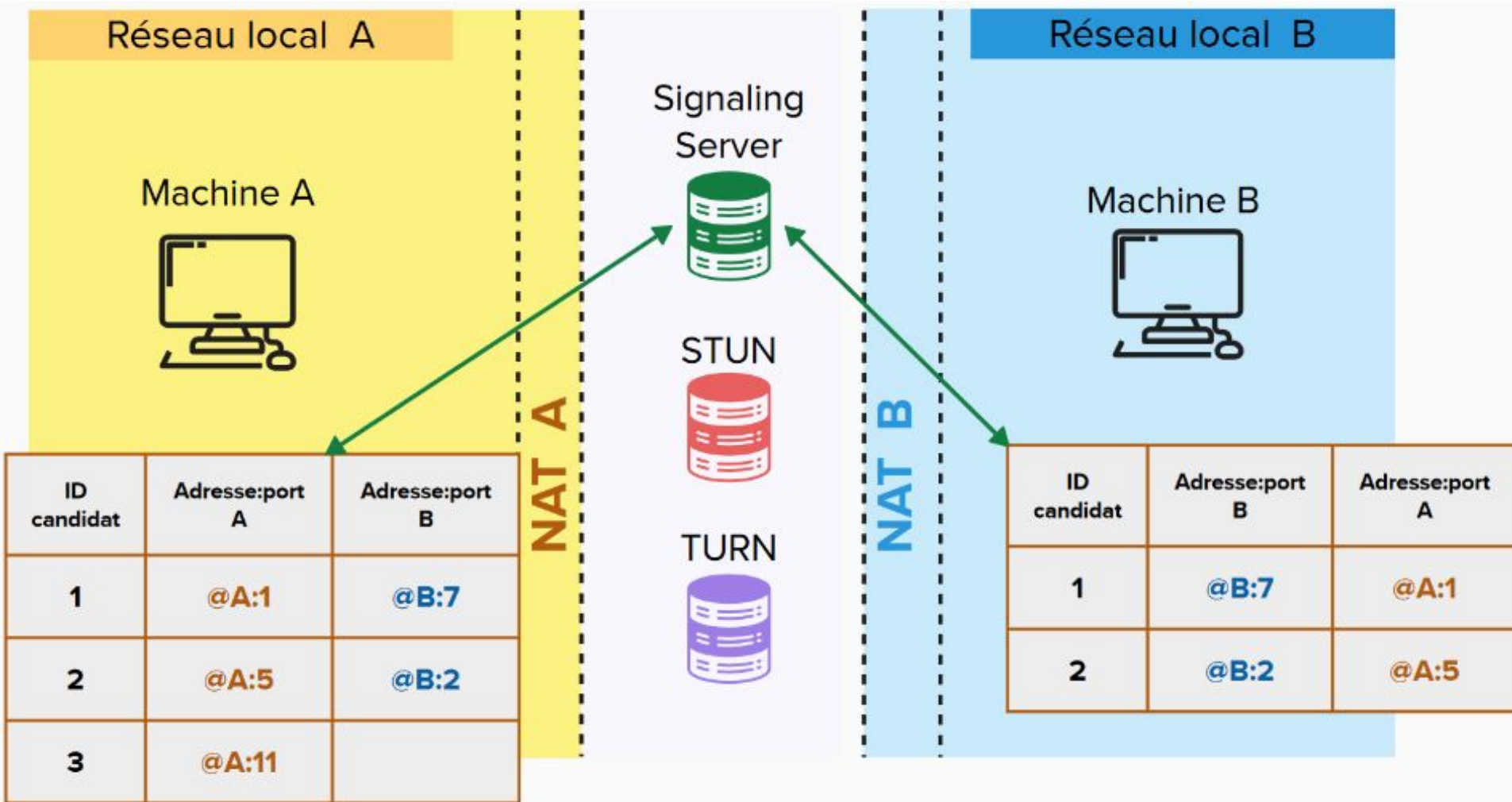




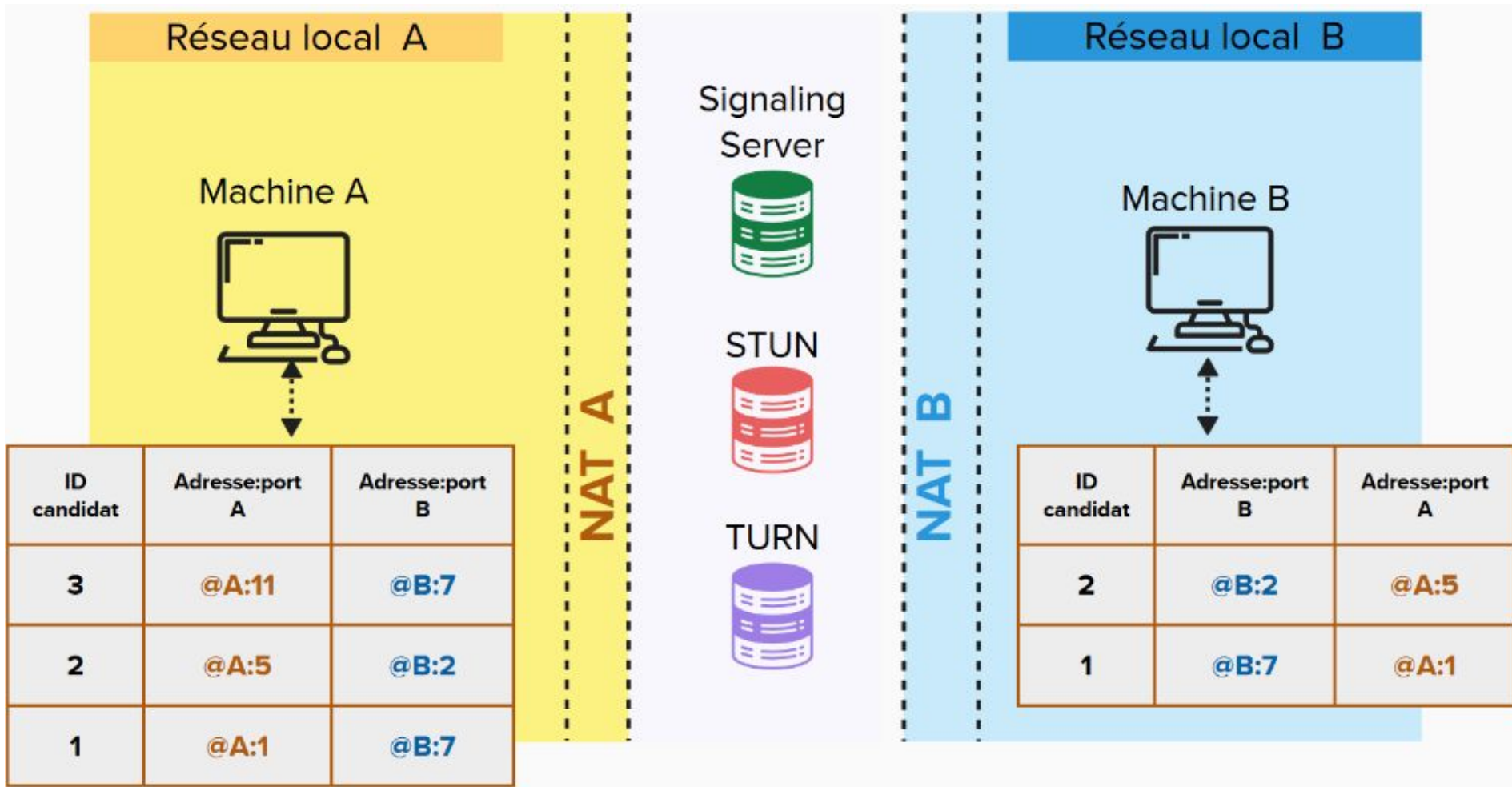
# ICE PAC/TCP (Hole Punching & Relaying)



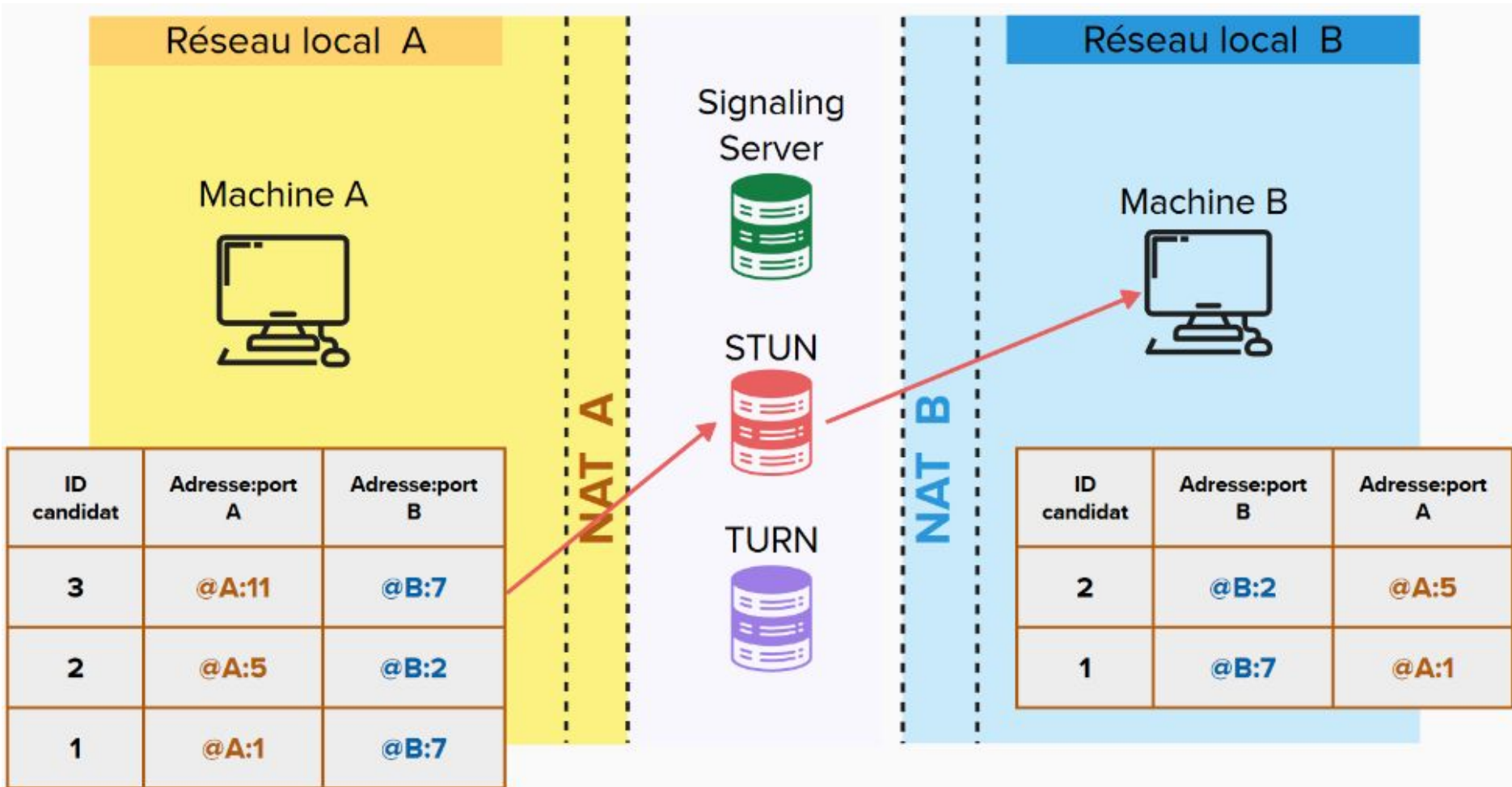
# ICE PAC/TCP (Hole Punching & Relaying)



# ICE PAC/TCP (Hole Punching & Relaying)

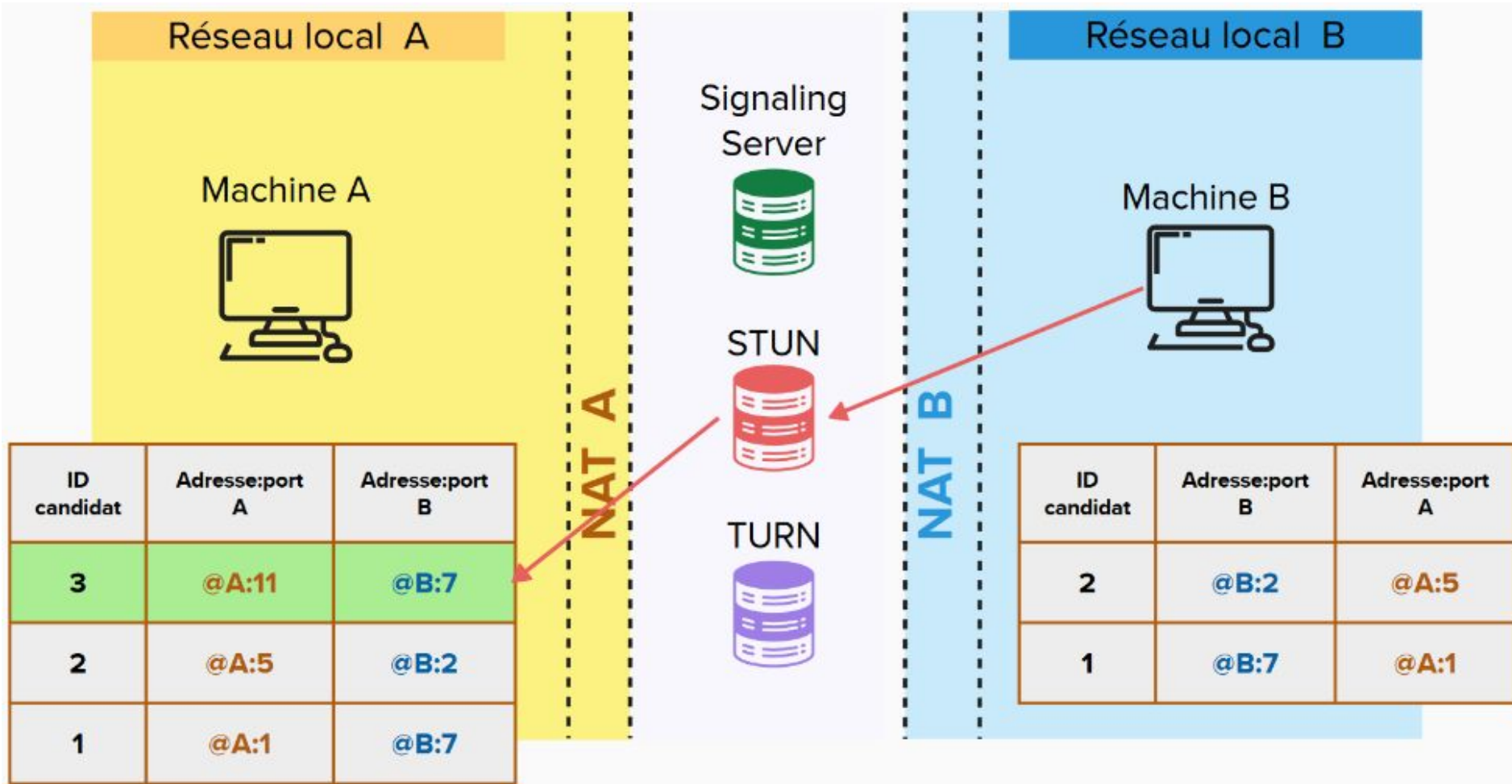


# ICE PAC/TCP (Hole Punching & Relaying)

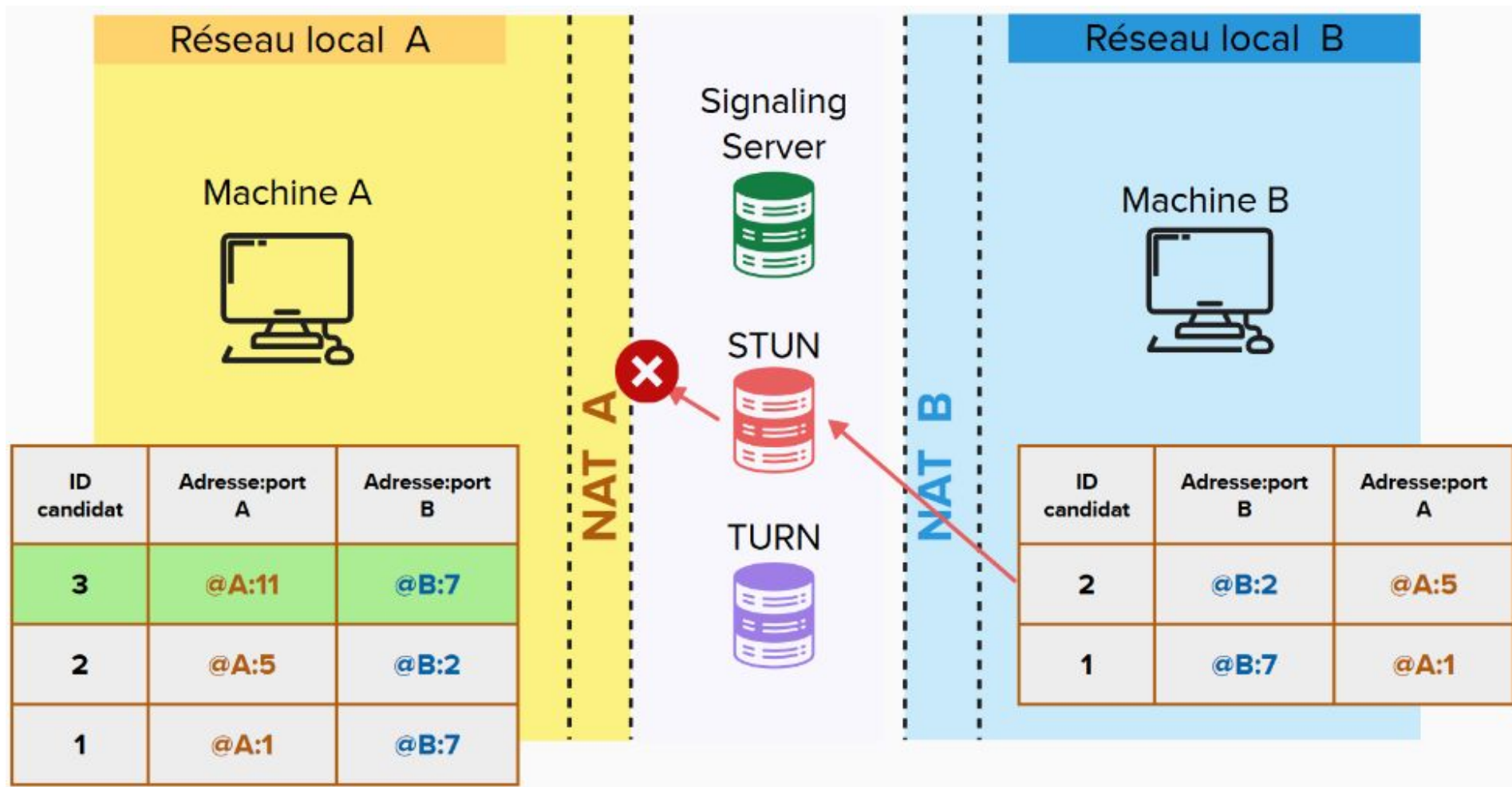




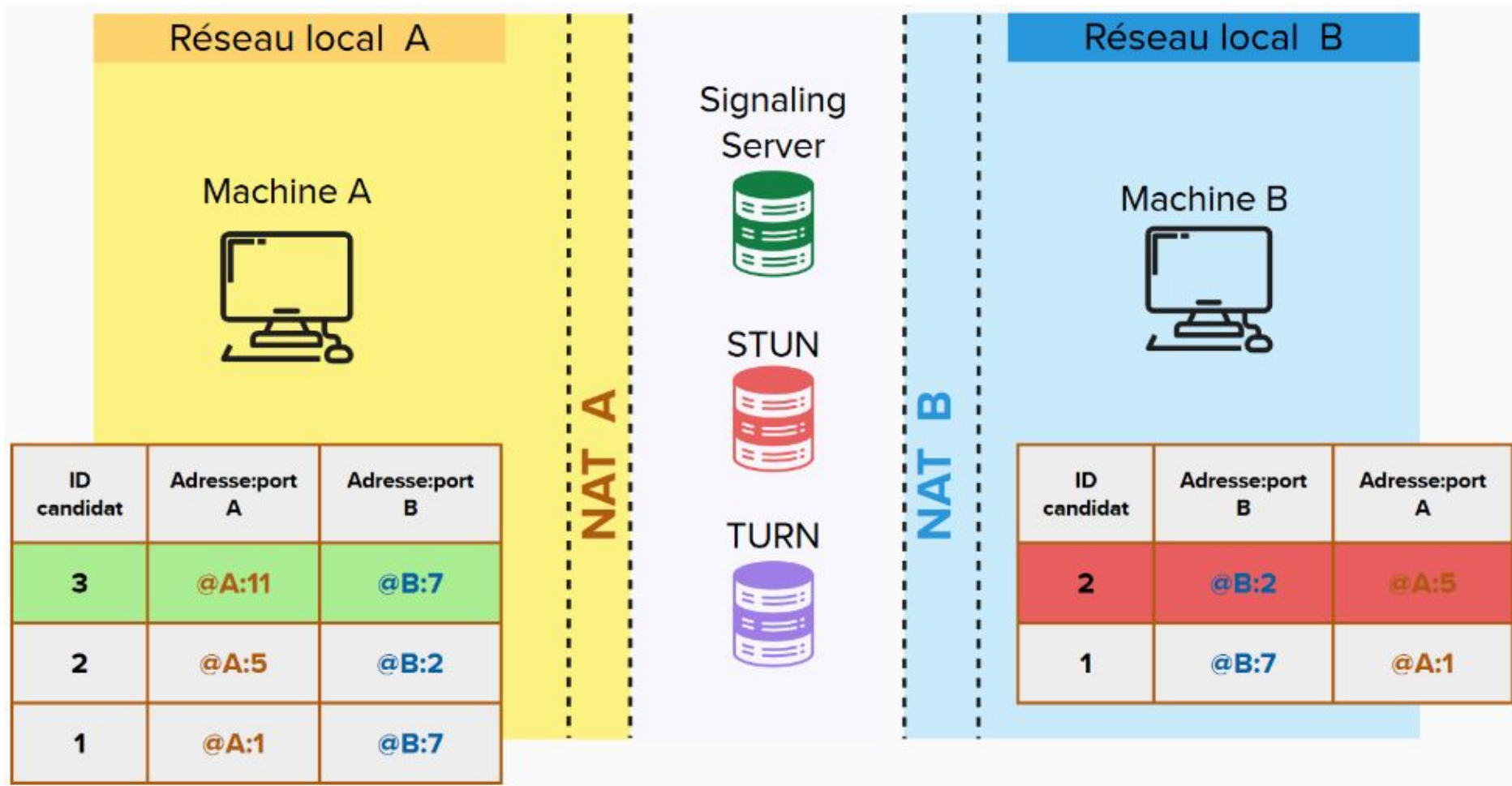
# ICE PAC/TCP (Hole Punching & Relaying)



# ICE PAC/TCP (Hole Punching & Relaying)



# ICE PAC/TCP (Hole Punching & Relaying)

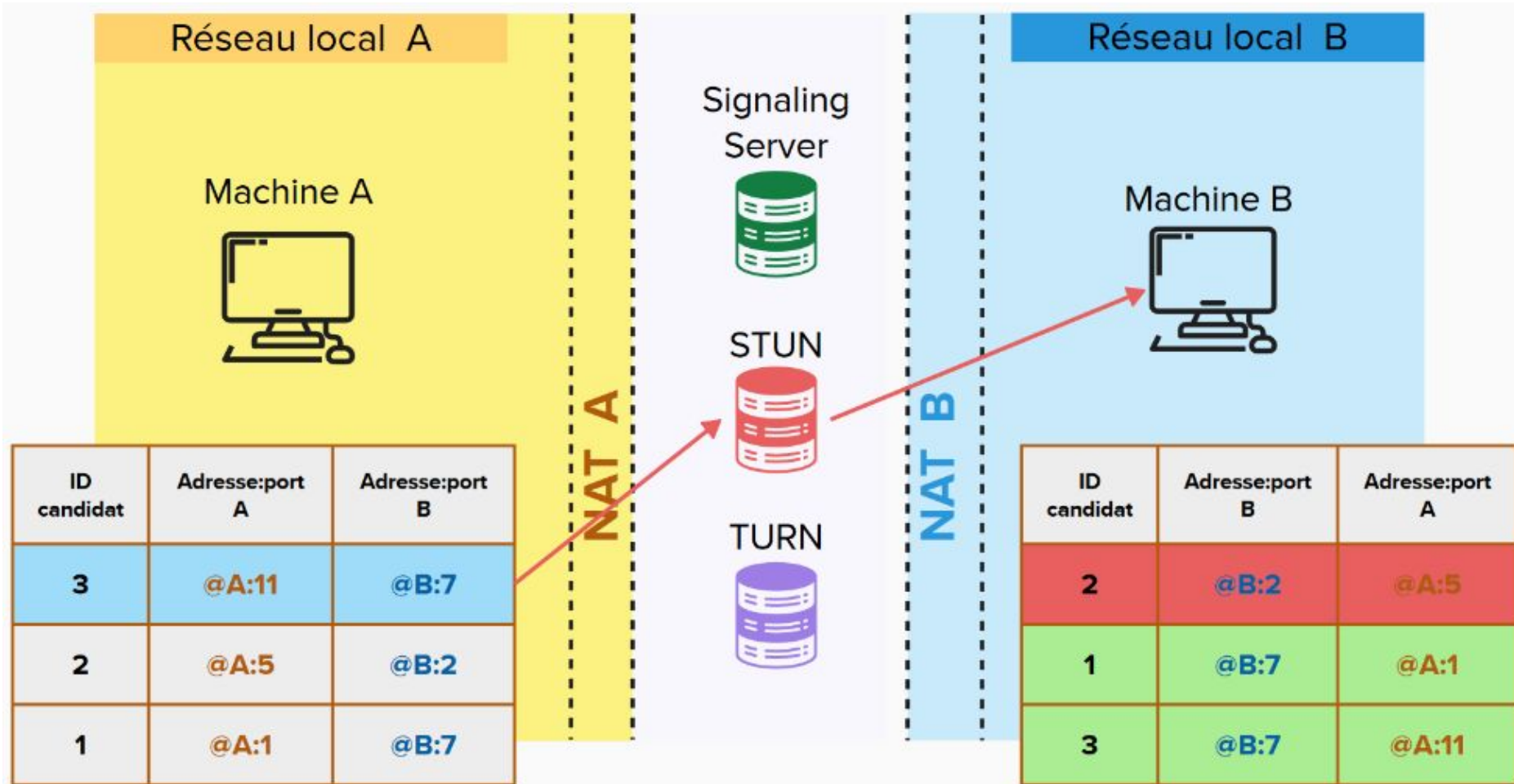


# ICE PAC/TCP (Hole Punching & Relaying)

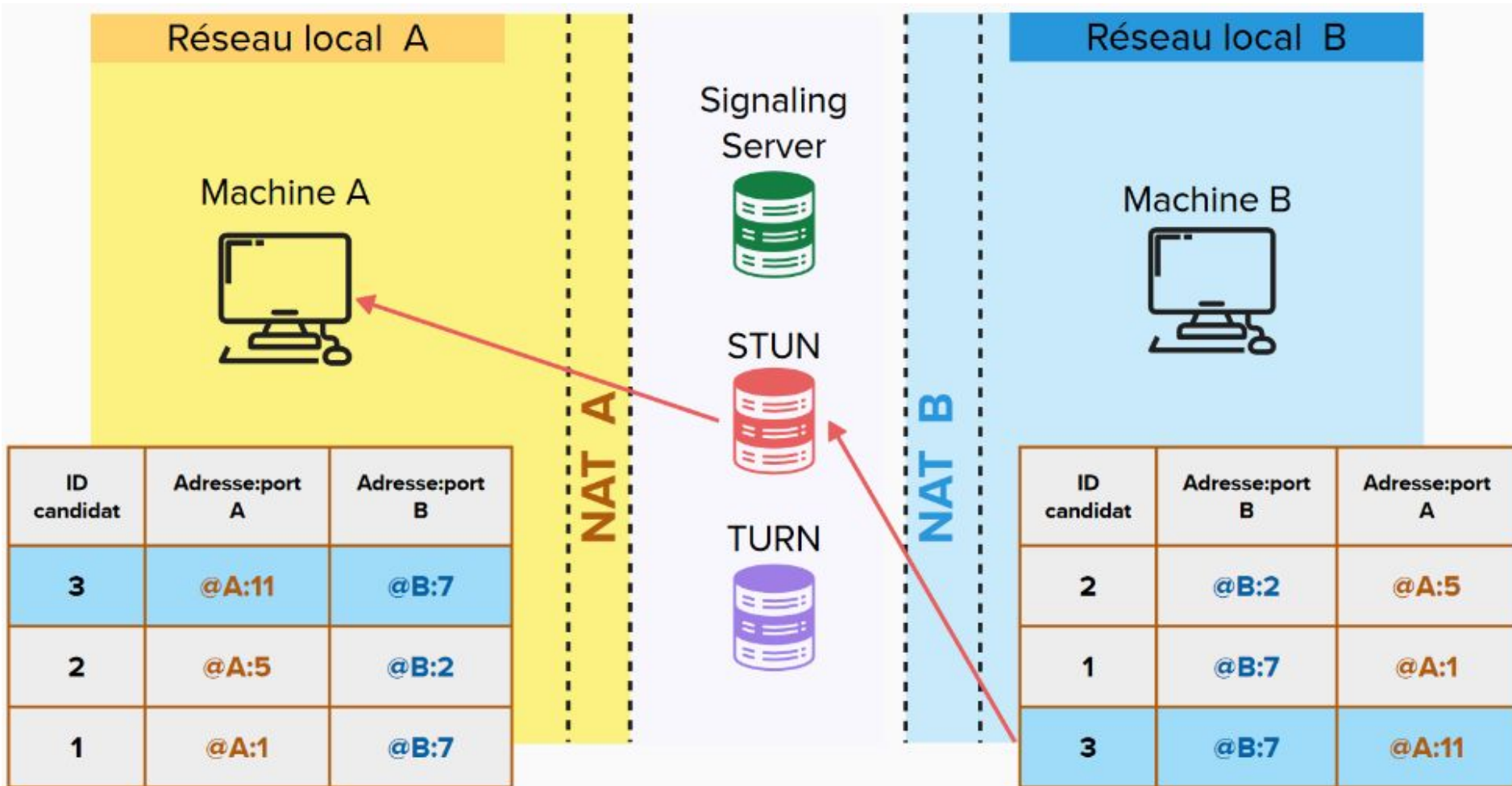




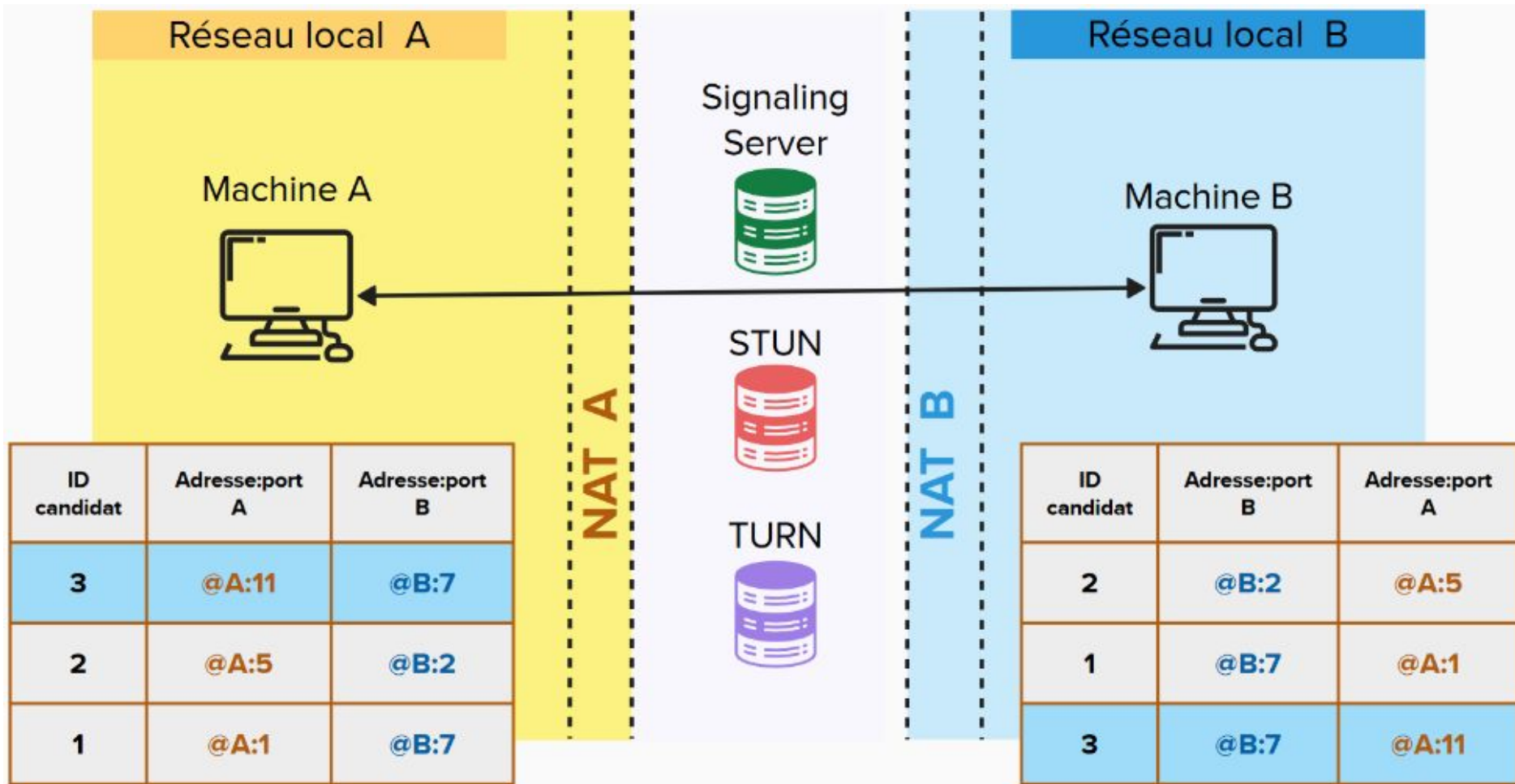
# ICE PAC/TCP (Hole Punching & Relaying)



# ICE PAC/TCP (Hole Punching & Relaying)



# ICE PAC/TCP (Hole Punching & Relaying)



# Conclusion & axes de travail

- À venir :
  - Apports sécuritaires des NATs

# Bibliographie

Keränen, Ari, Christer Holmberg, and Jonathan Rosenberg. "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal." Request for Comments. Internet Engineering Task Force, July 2018. <https://doi.org/10.17487/RFC8445>.

Holmberg, Christer, and Justin Uberti. "Interactive Connectivity Establishment Patiently Awaiting Connectivity (ICE PAC)." Request for Comments. Internet Engineering Task Force, January 2021. <https://doi.org/10.17487/RFC8863>.

Rosenberg, Jonathan, Christian Huitema, Rohan Mahy, and Joel Weinberger. "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)." Request for Comments. Internet Engineering Task Force, March 2003. <https://doi.org/10.17487/RFC3489>.

Matthews, Philip, Jonathan Rosenberg, and Rohan Mahy. "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)." Request for Comments. Internet Engineering Task Force, April 2010. <https://doi.org/10.17487/RFC5766>.

P. Srisuresh, B. Ford, D. Kegel. "RFC 5128 - State of Peer-to-Peer (P2P) Communication across Network Address Translators (NATs)", *Internet Engineering Task Force* (Mars 2008), <https://datatracker.ietf.org/doc/html/rfc5128>

J. Dordoigne, "Réseaux informatiques - Notions fondamentales" 9ème édition, *ENI Editions* (2022)

UPnP Device Architecture 1.0 , *UPnP Forum*, Document Revision (15 October 2008)  
<https://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.0.pdf>