Licence Pro - Sécurité - Séance 2

Université de Caen

Jean Fromentin
mailto:jfroment@info.unicaen.fr
http://www.info.unicaen.fr/~jfroment

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 1 : Physique

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 2 : Liaison

Couche 1 : Physique

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

- Cette couche est chargée de la transmission effective des signaux électriques ou optiques entre les interlocuteurs.

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

- Cette couche est chargée de la transmission effective des signaux électriques ou optiques entre les interlocuteurs. Son service est typiquement limité à l'émission et la réception d'un bit ou d'un train de bits continu.

Exemple protocole : ADSL, 100BaseT, ADSL, Wifi, Bluetooth

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

- Cette couche est chargée de la transmission effective des signaux électriques ou optiques entre les interlocuteurs. Son service est typiquement limité à l'émission et la réception d'un bit ou d'un train de bits continu.

Exemple protocole : ADSL, 100BaseT, ADSL, Wifi, Bluetooth

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

- Cette couche gère les communications entre deux machines adjacentes, directement reliées entre elles par un support physique.

Exemple protocole : Ethernet

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

- Cette couche gère les communications de proche en proche, généralement entre machines : routage et adressage des paquets.

Exemple protocole : IPv4, IPv6, IPX

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

- Cette couche gère les communications de bout en bout entre processus (programmes en cours d'exécution).

Exemple protocole : TCP, UDP

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

- Cette couche gère la synchronisation des échanges et les "transactions", permet l'ouverture et la fermeture de session.

Exemple protocole : NetBios

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

- Cette couche est chargée du codage des données applicatives, précisément de la conversion entre données manipulées au niveau applicatif et chaînes d'octets effectivement transmises.

Exemple protocole : SMB, ASN.1

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

- Cette couche est le point d'accès aux services réseaux.

Exemple protocole : HTTP, SMTP, TELNET

Modèle en couche OSI

- La première version repose sur des spécifications publiées en 1978.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

Couche 3 : Réseau

Couche 2 : Liaison

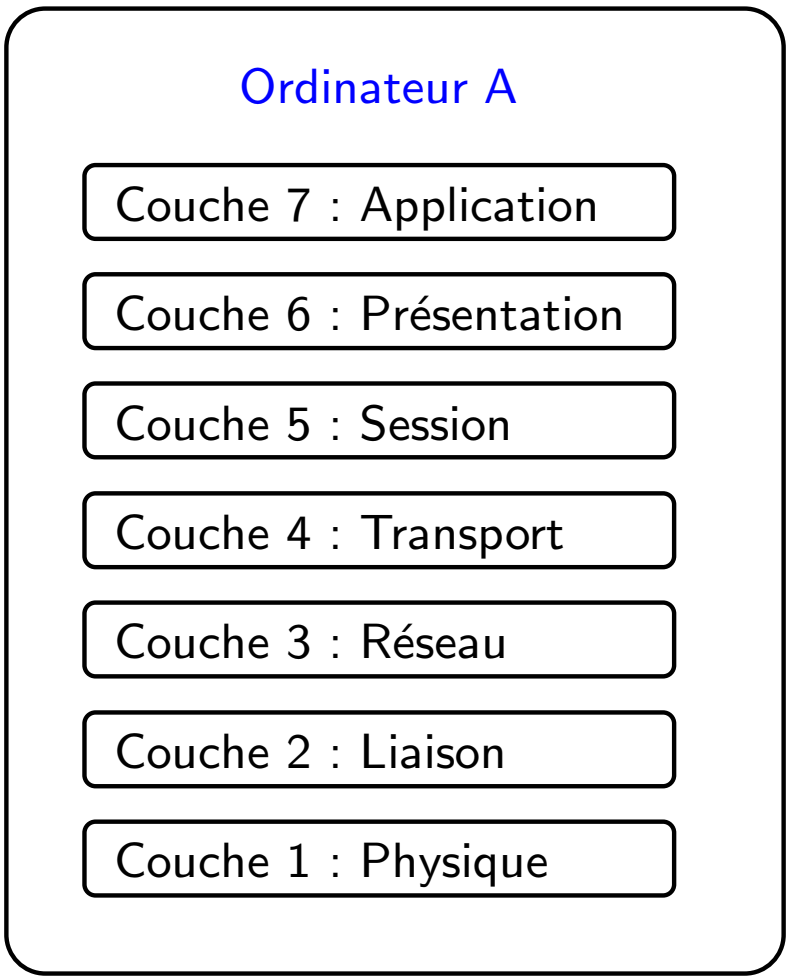
Couche 1 : Physique

Modèle OSI et protocoles

- Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.

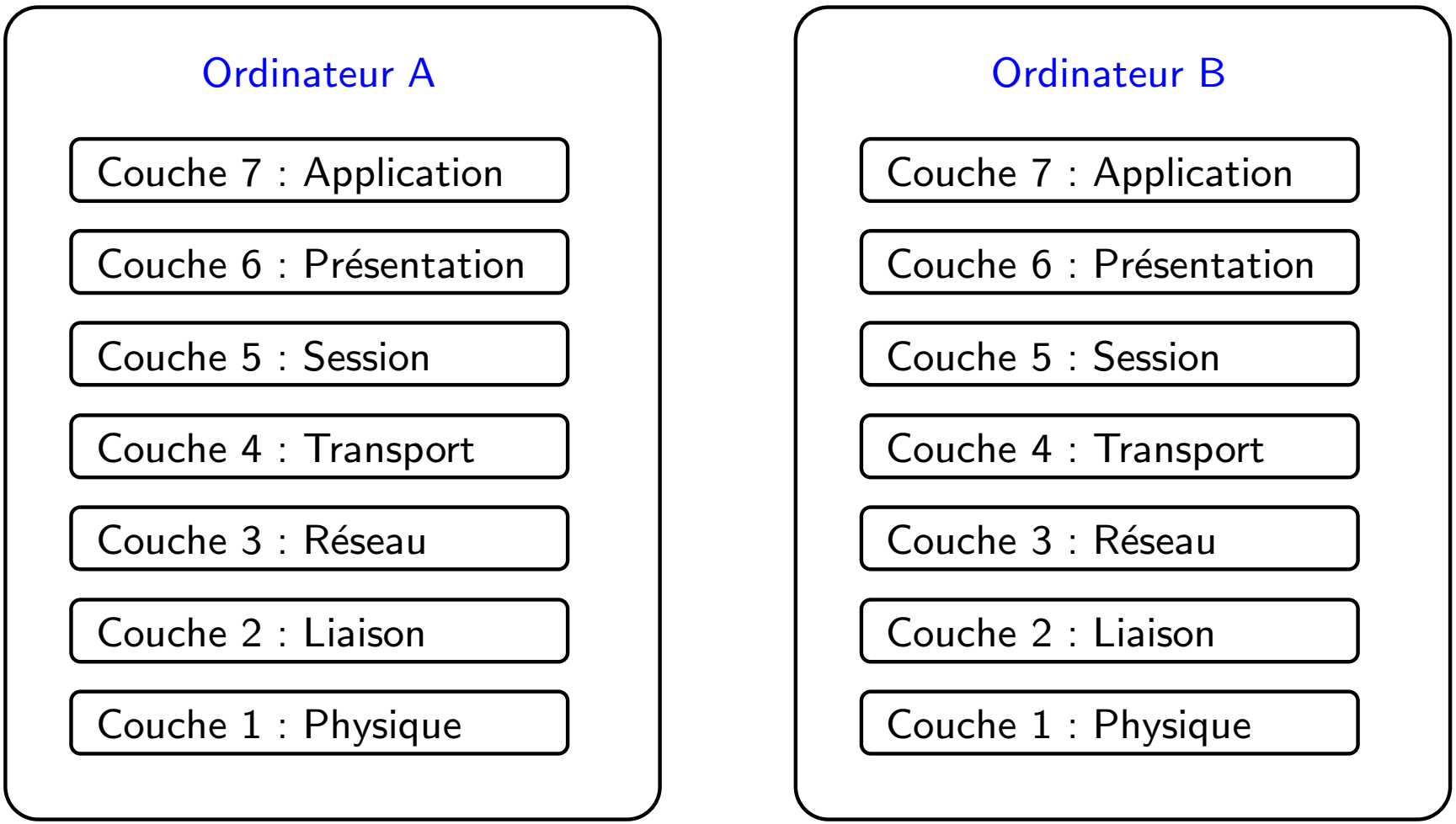
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



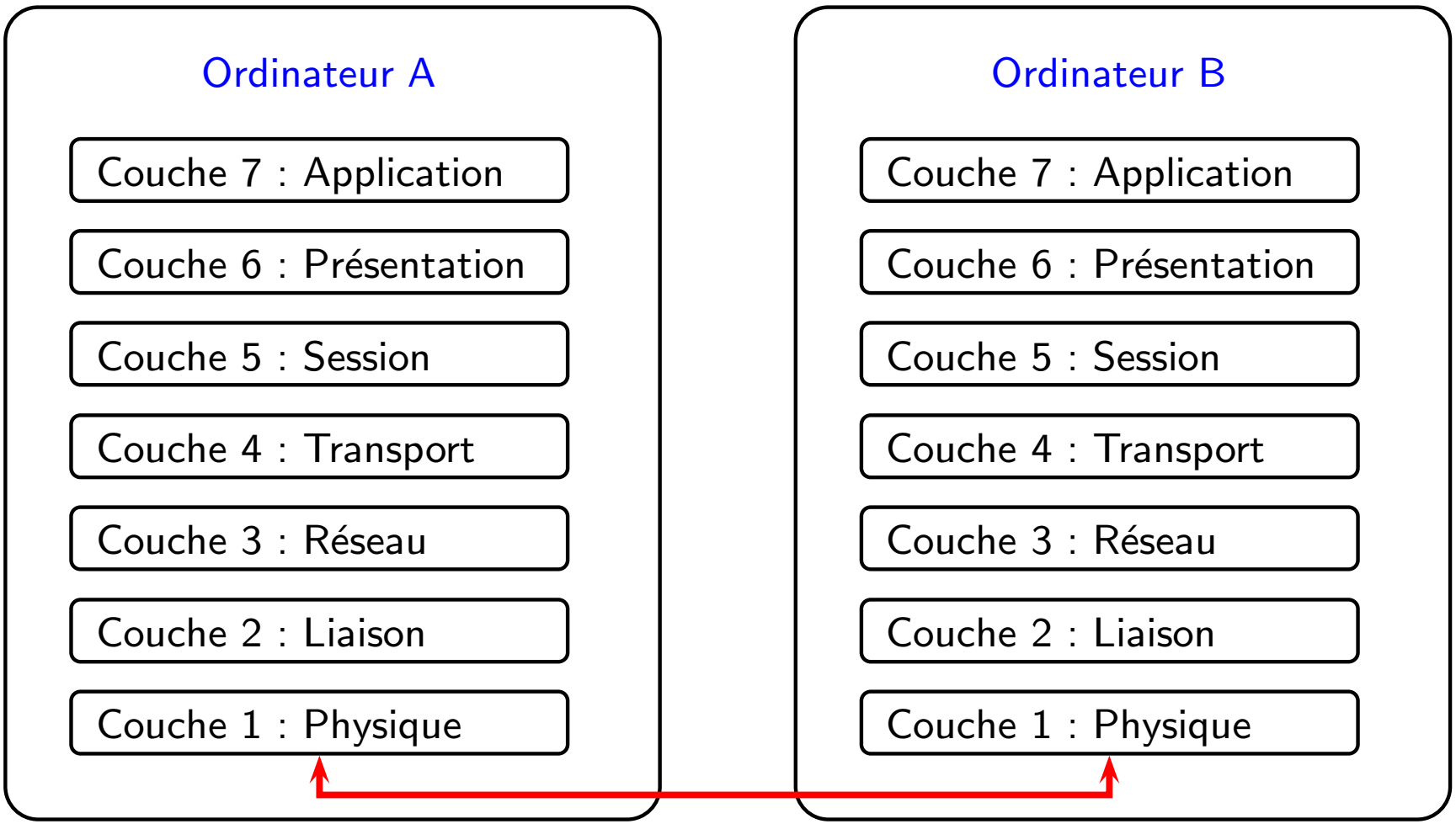
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



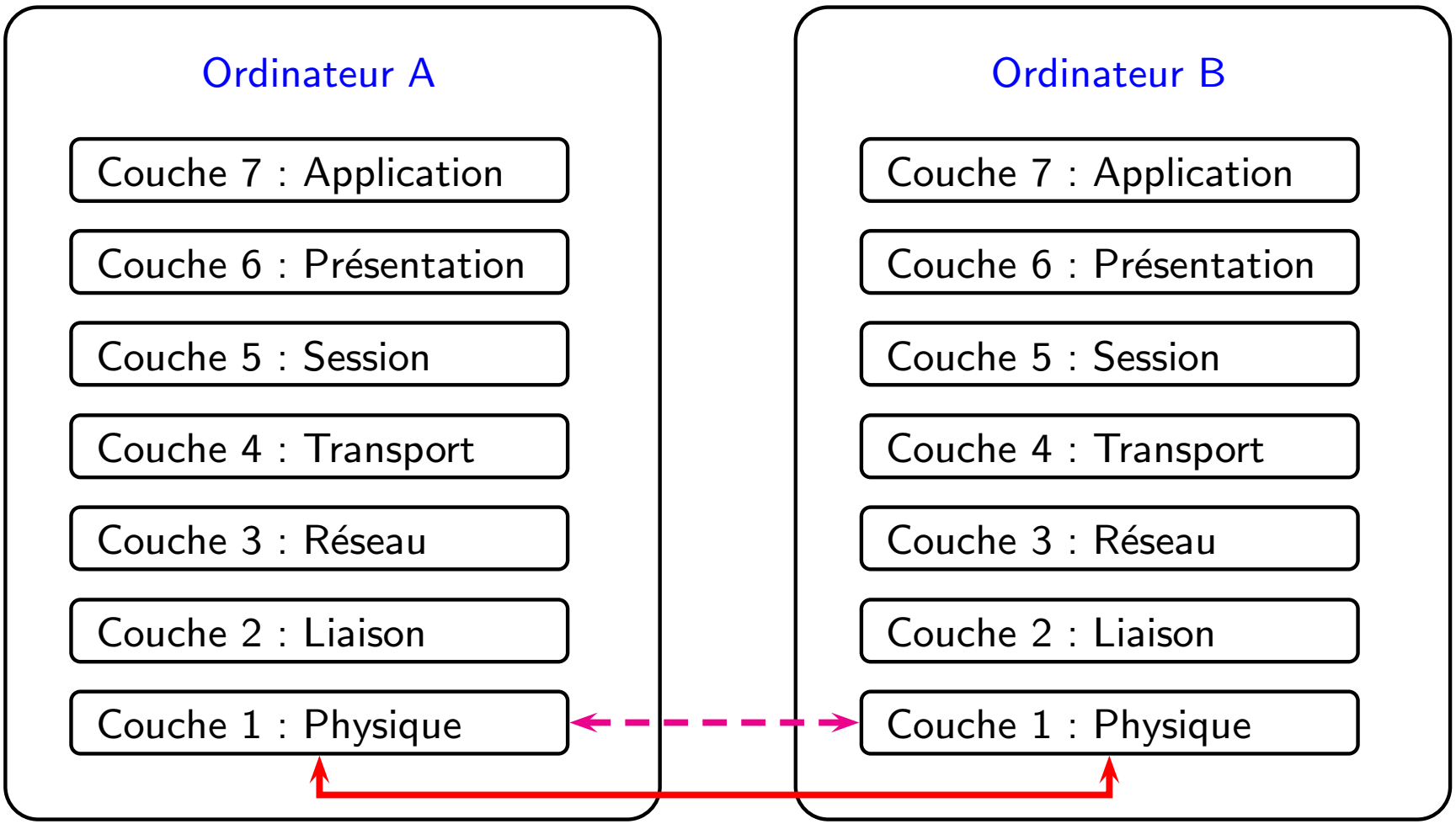
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



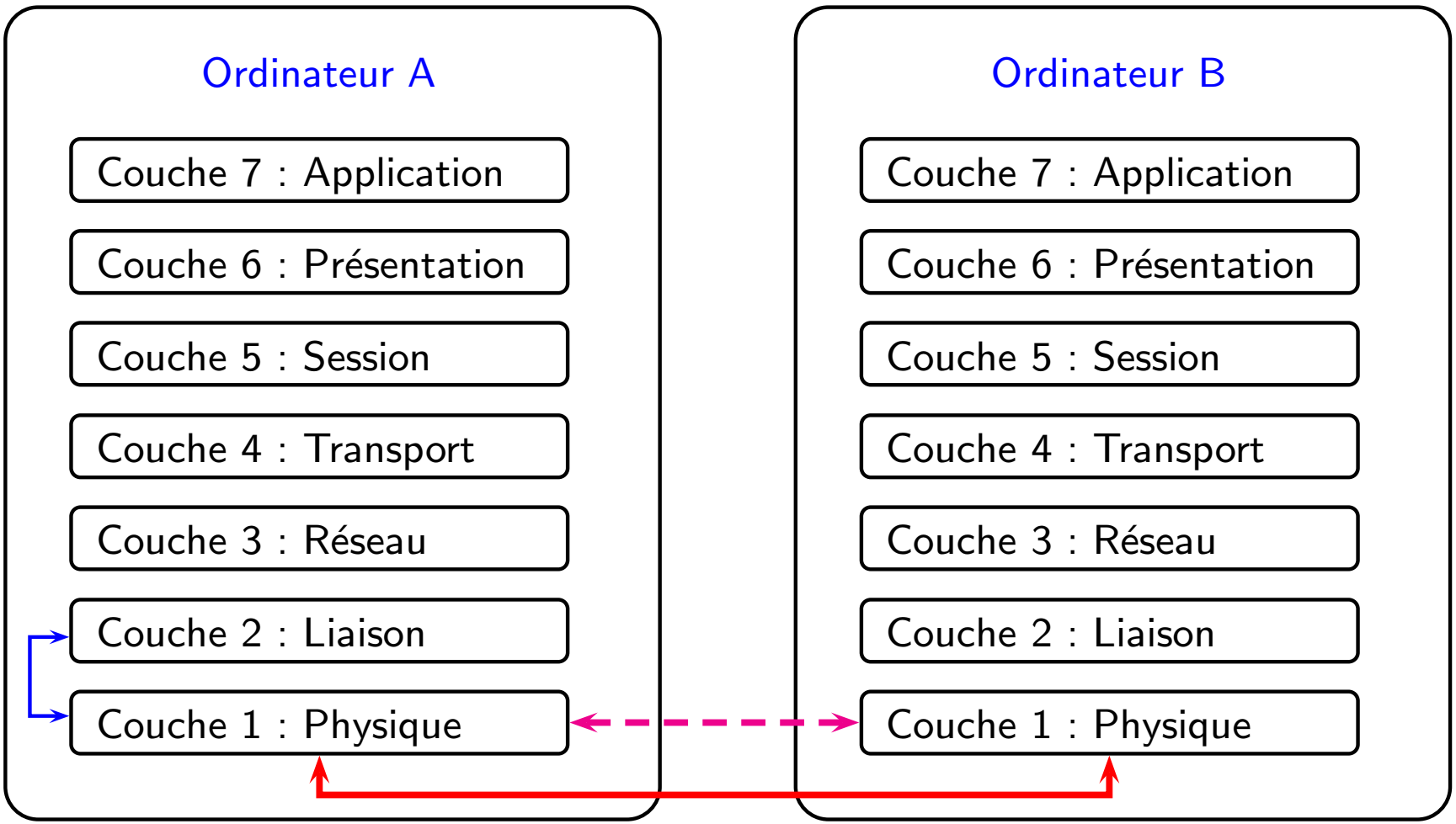
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



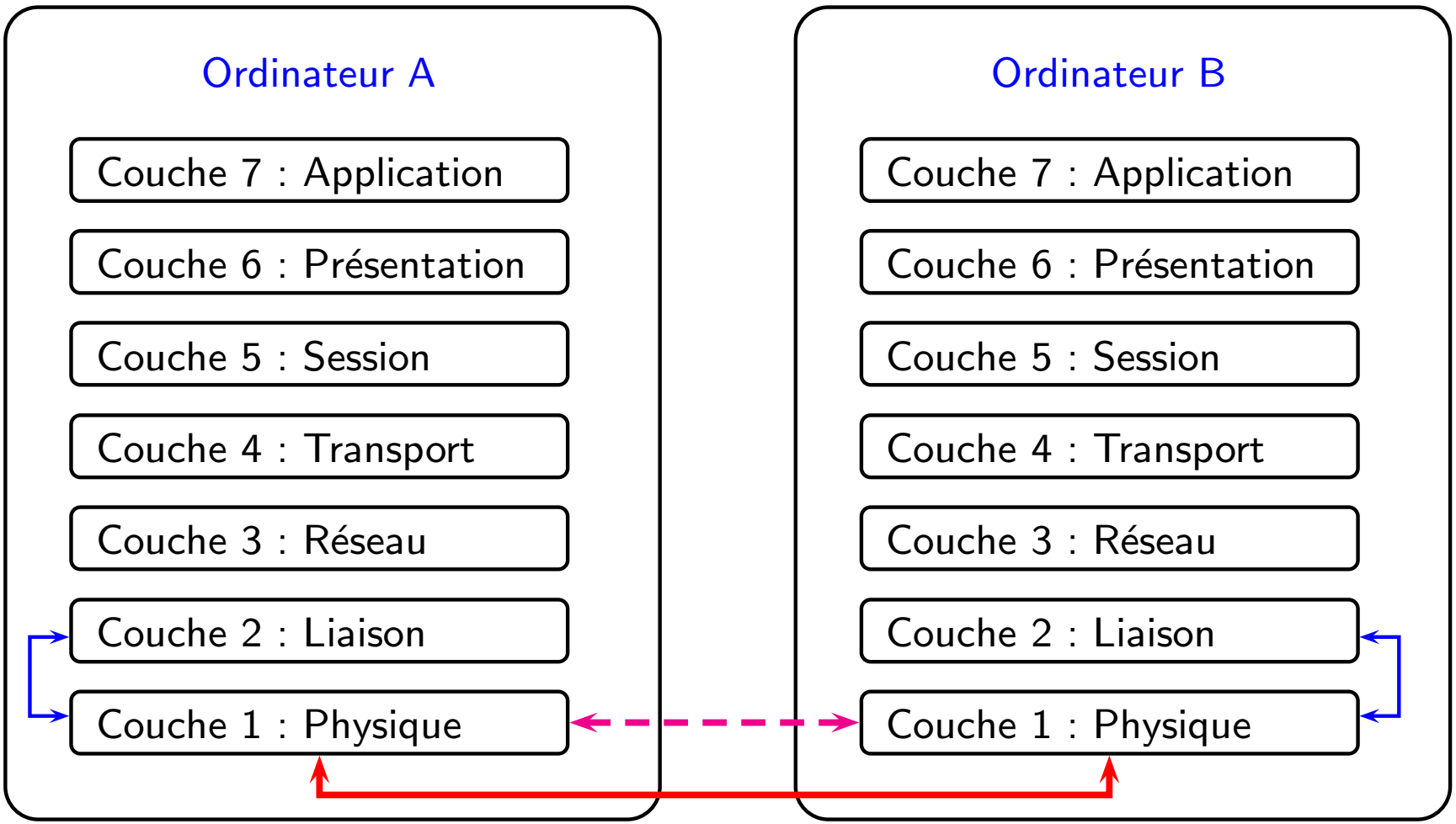
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



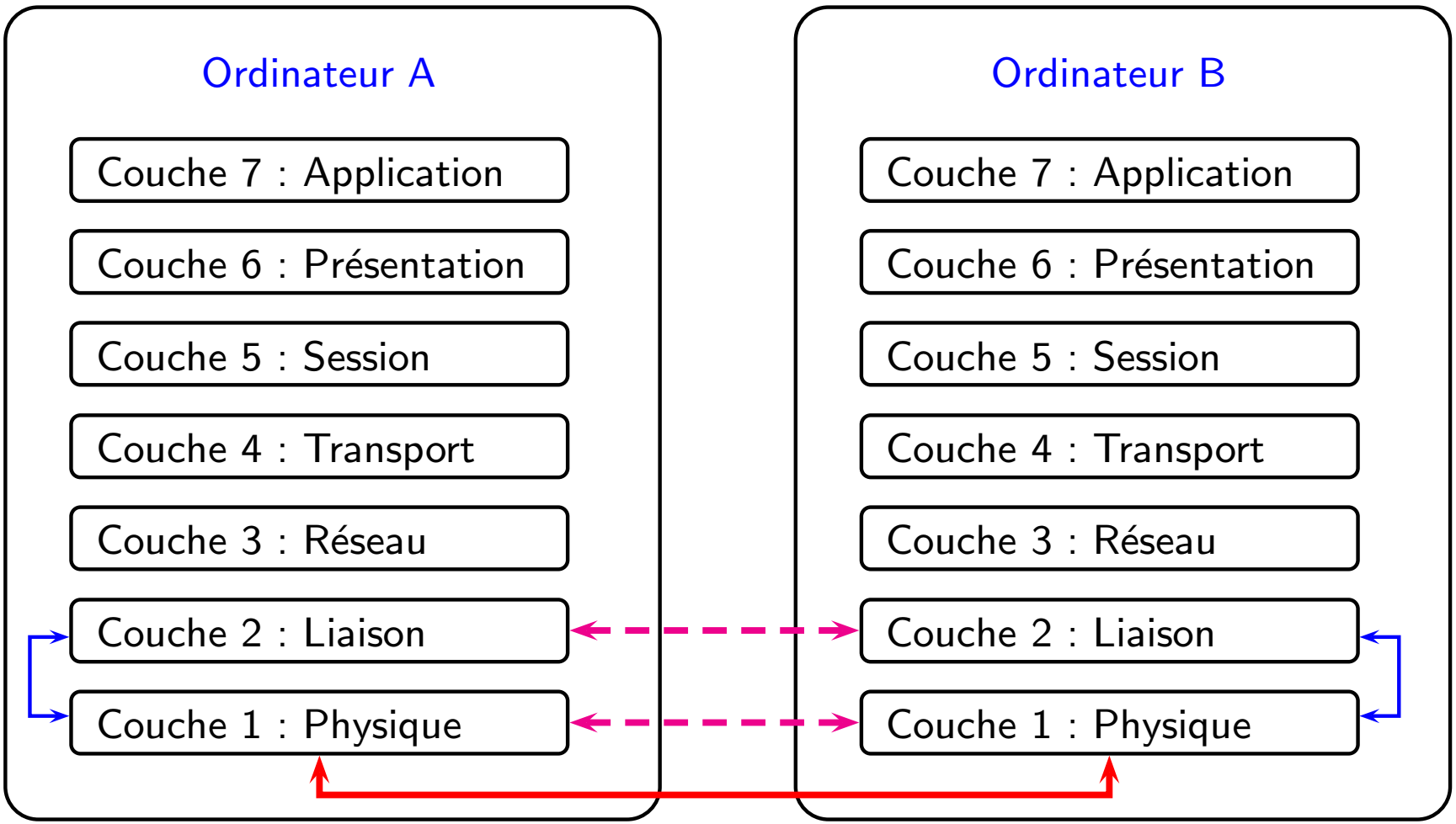
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



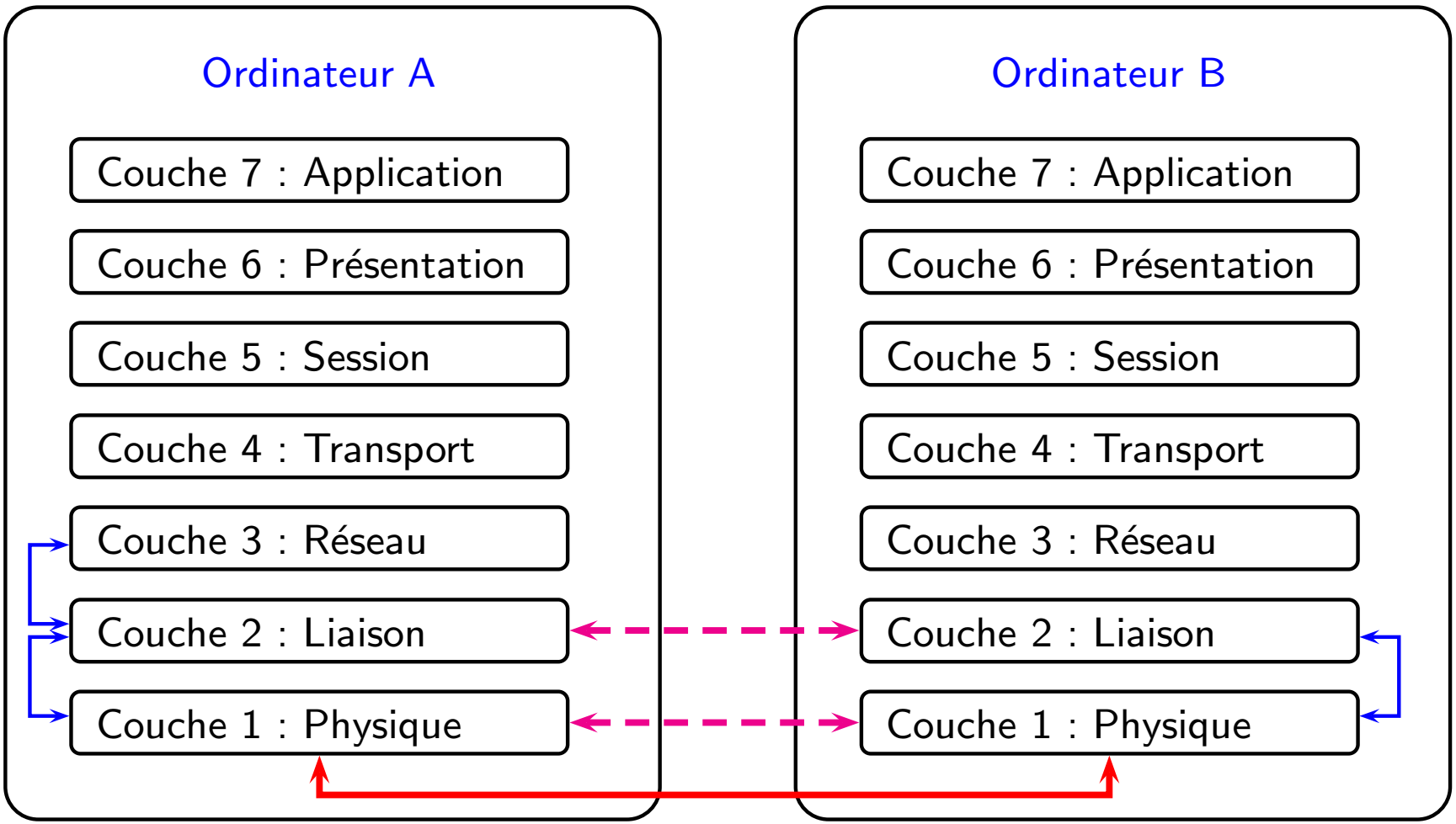
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



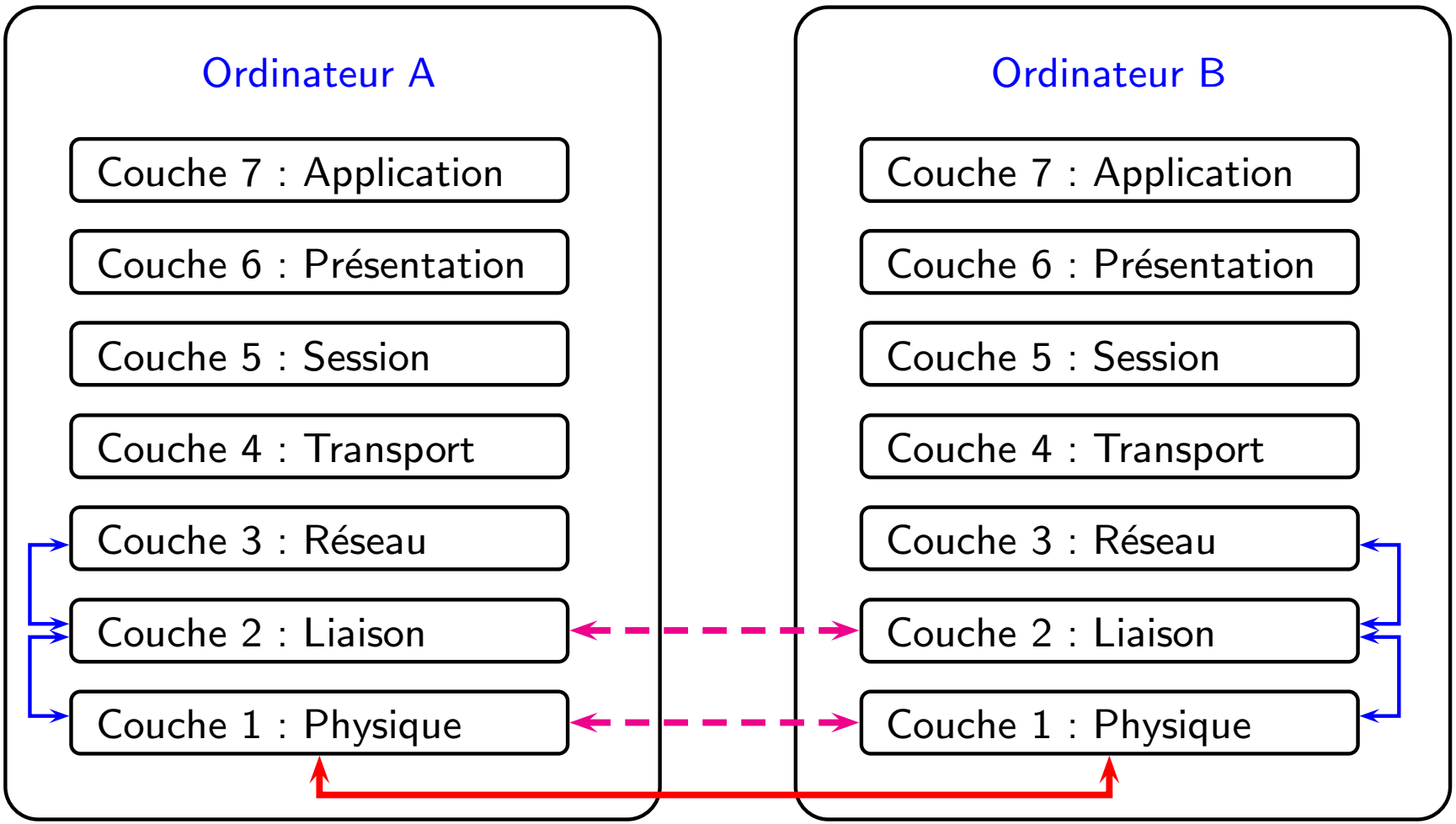
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



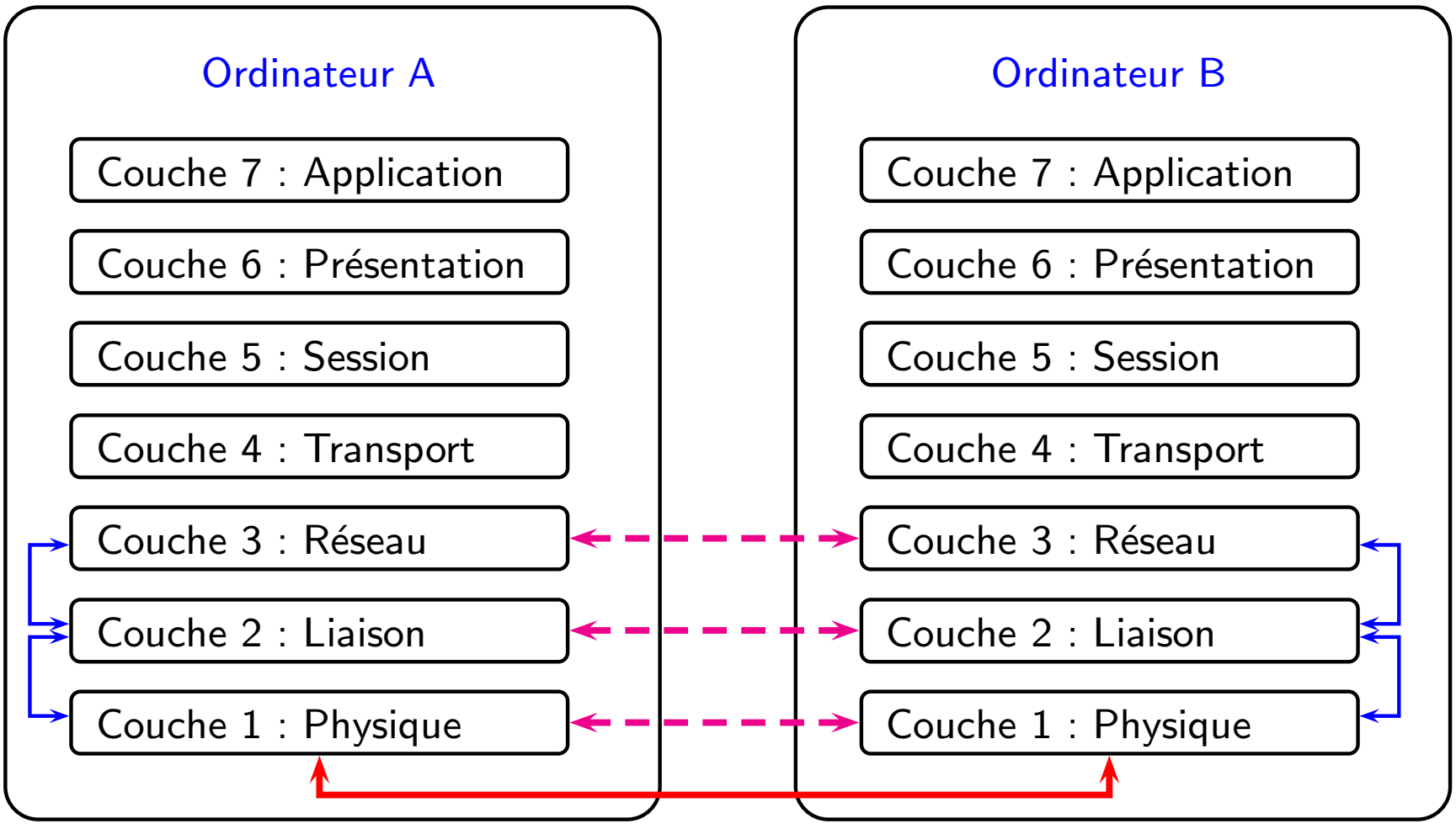
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



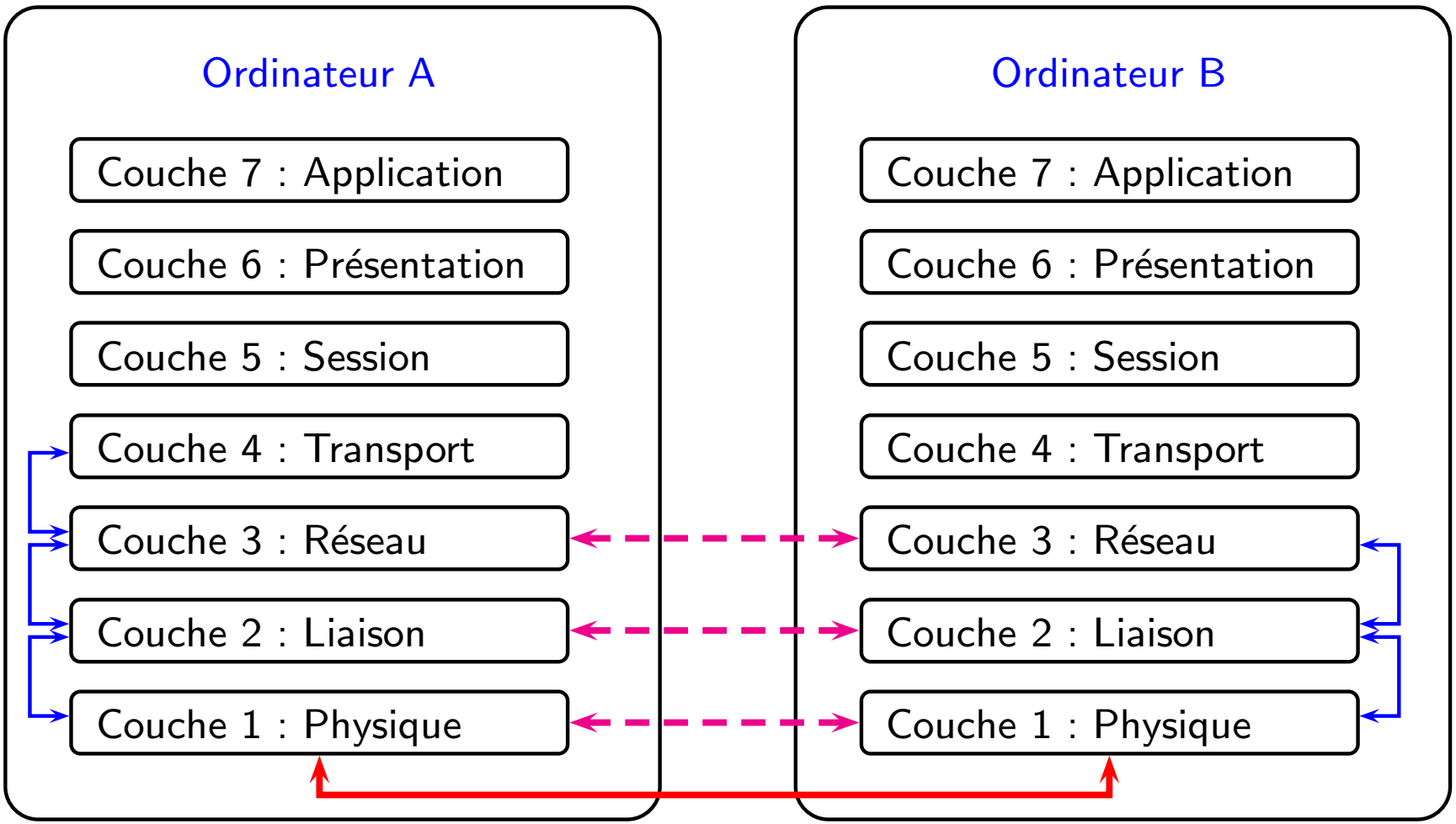
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



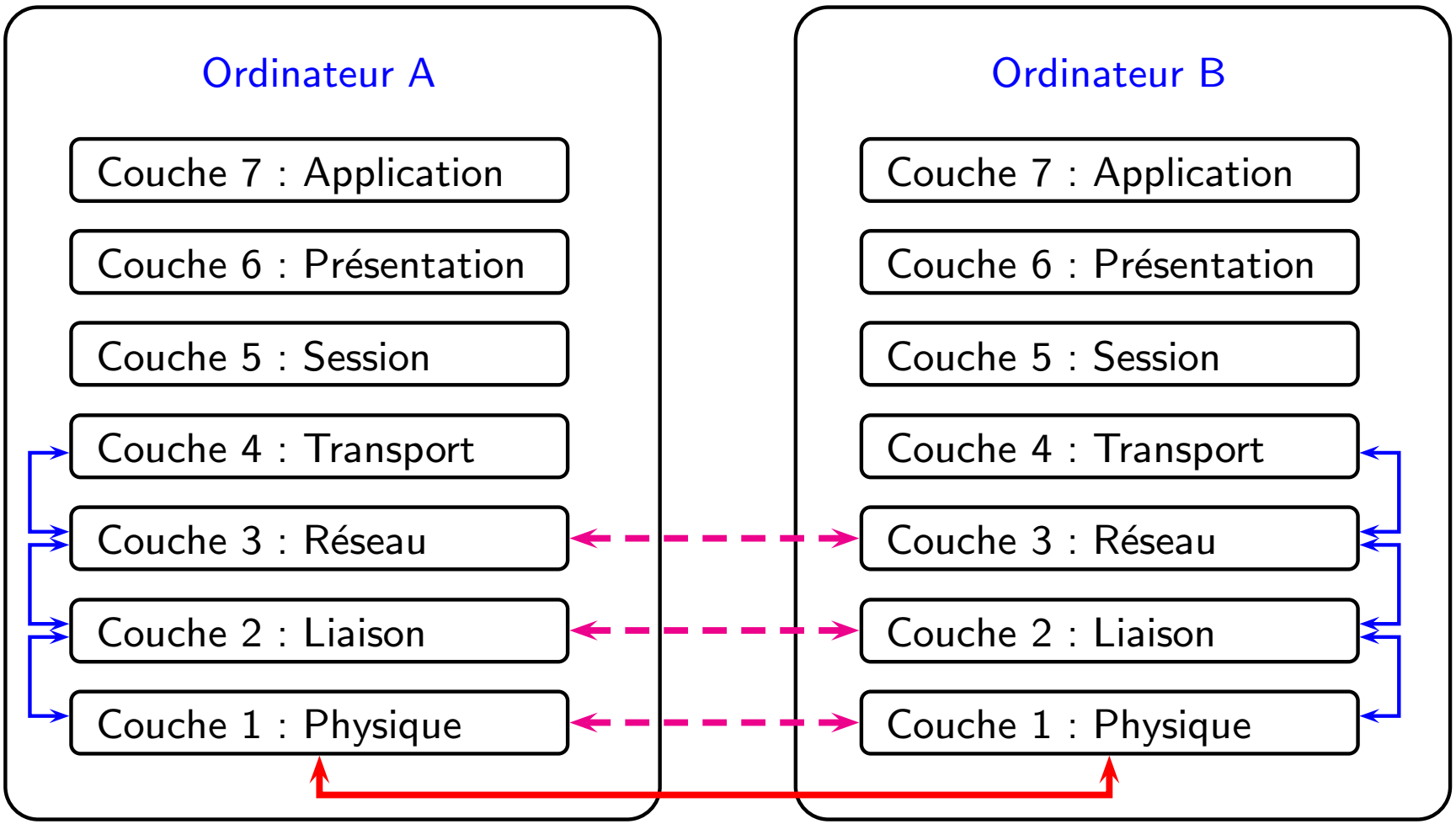
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



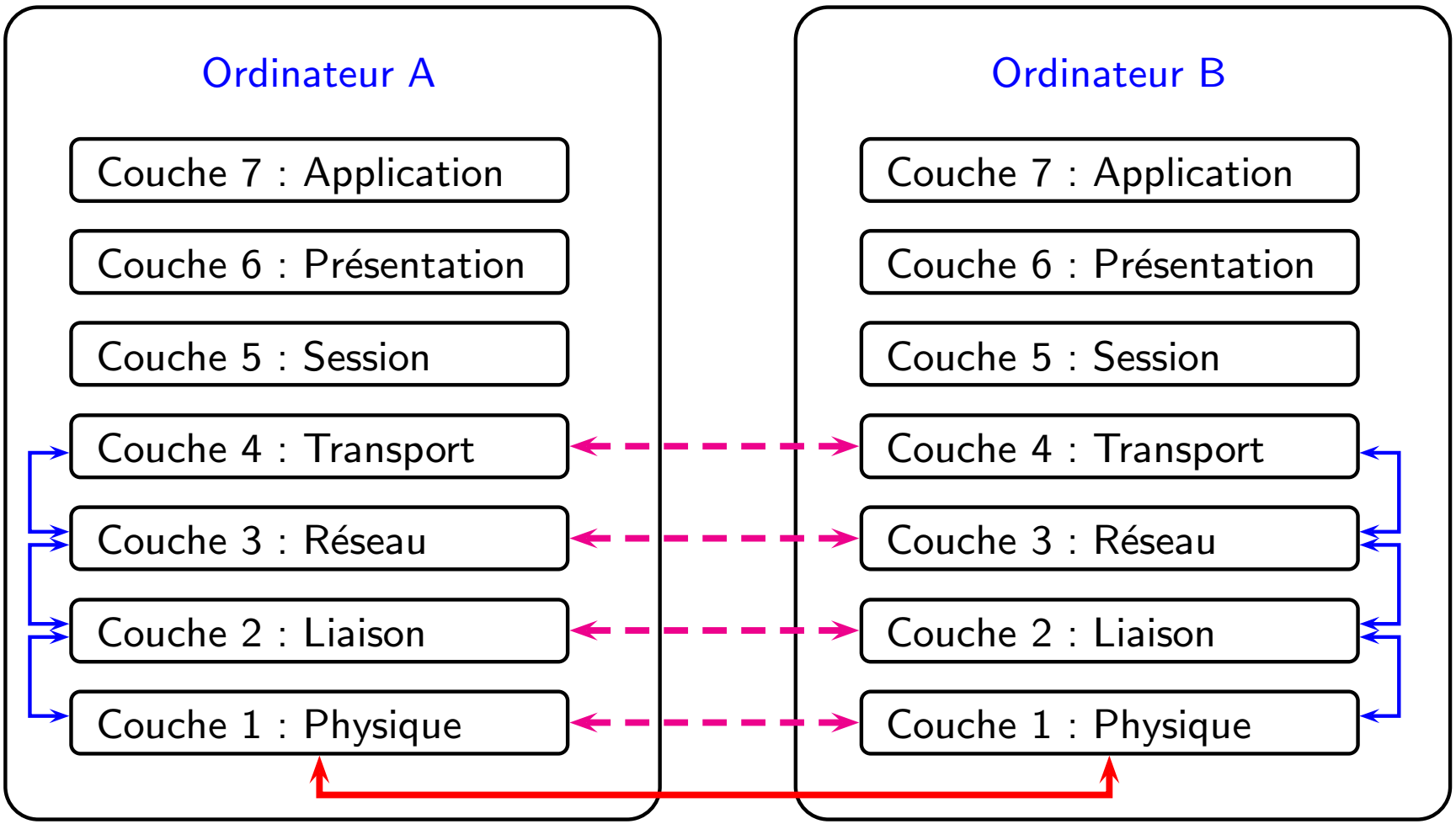
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



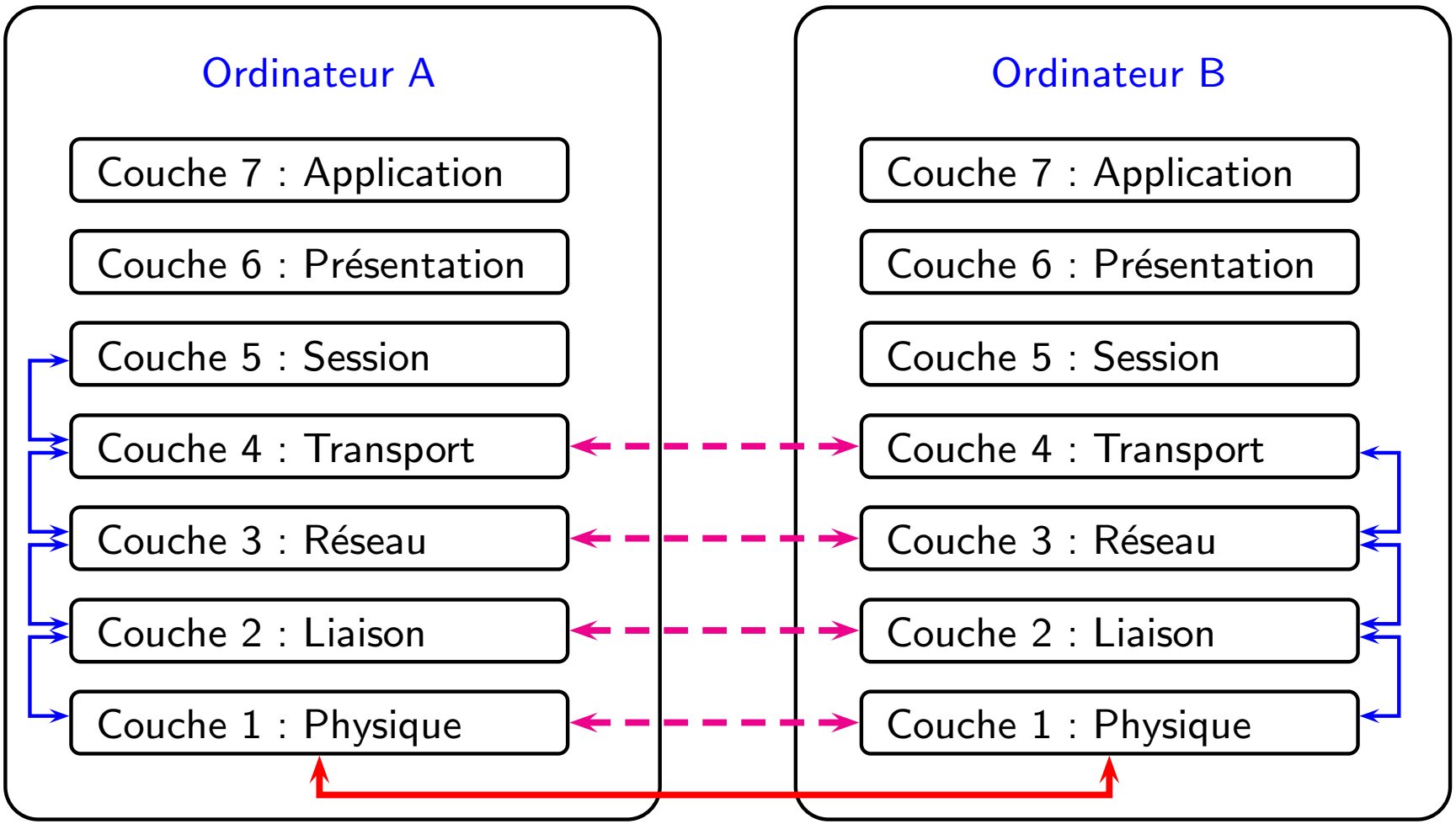
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



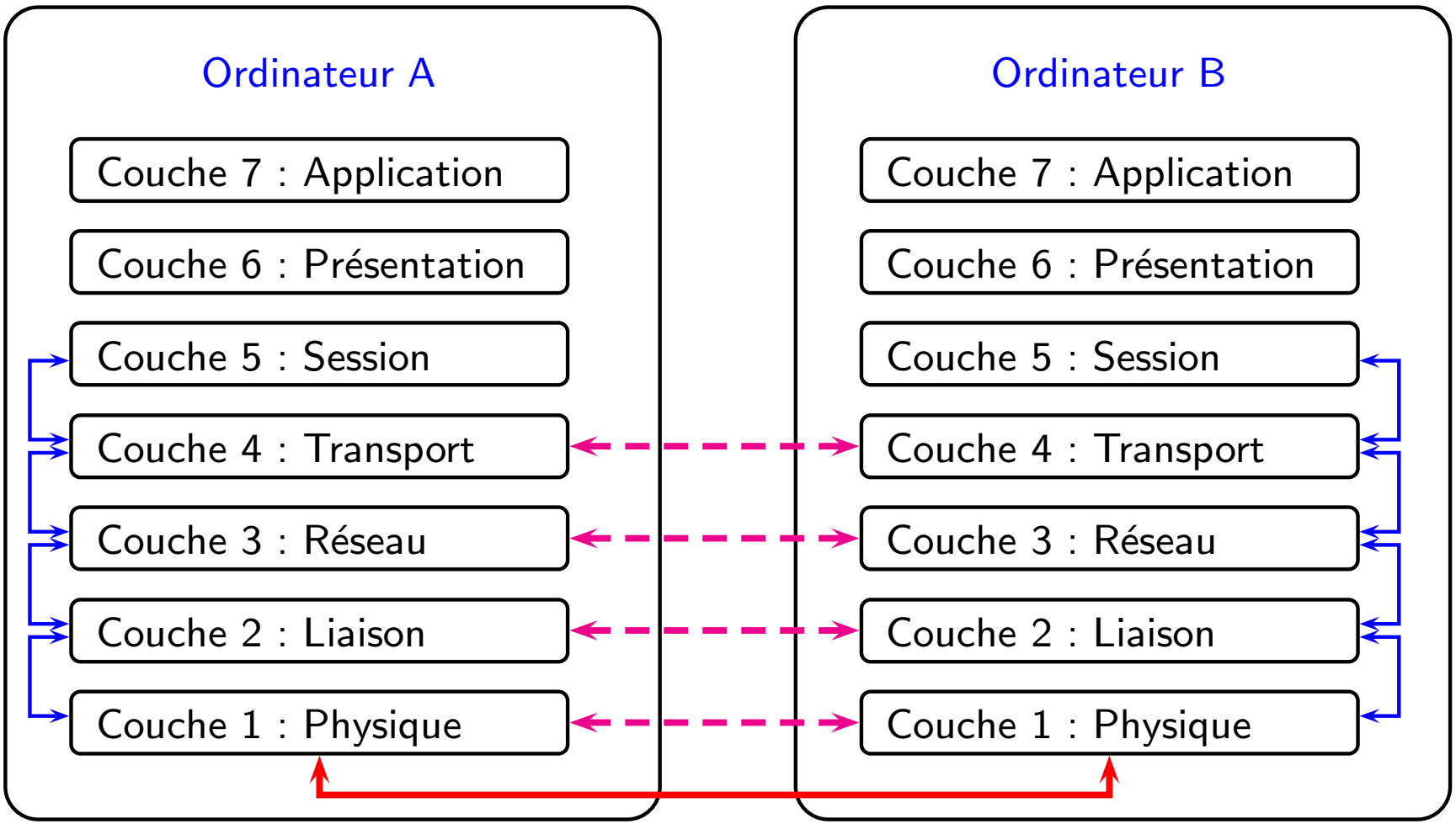
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



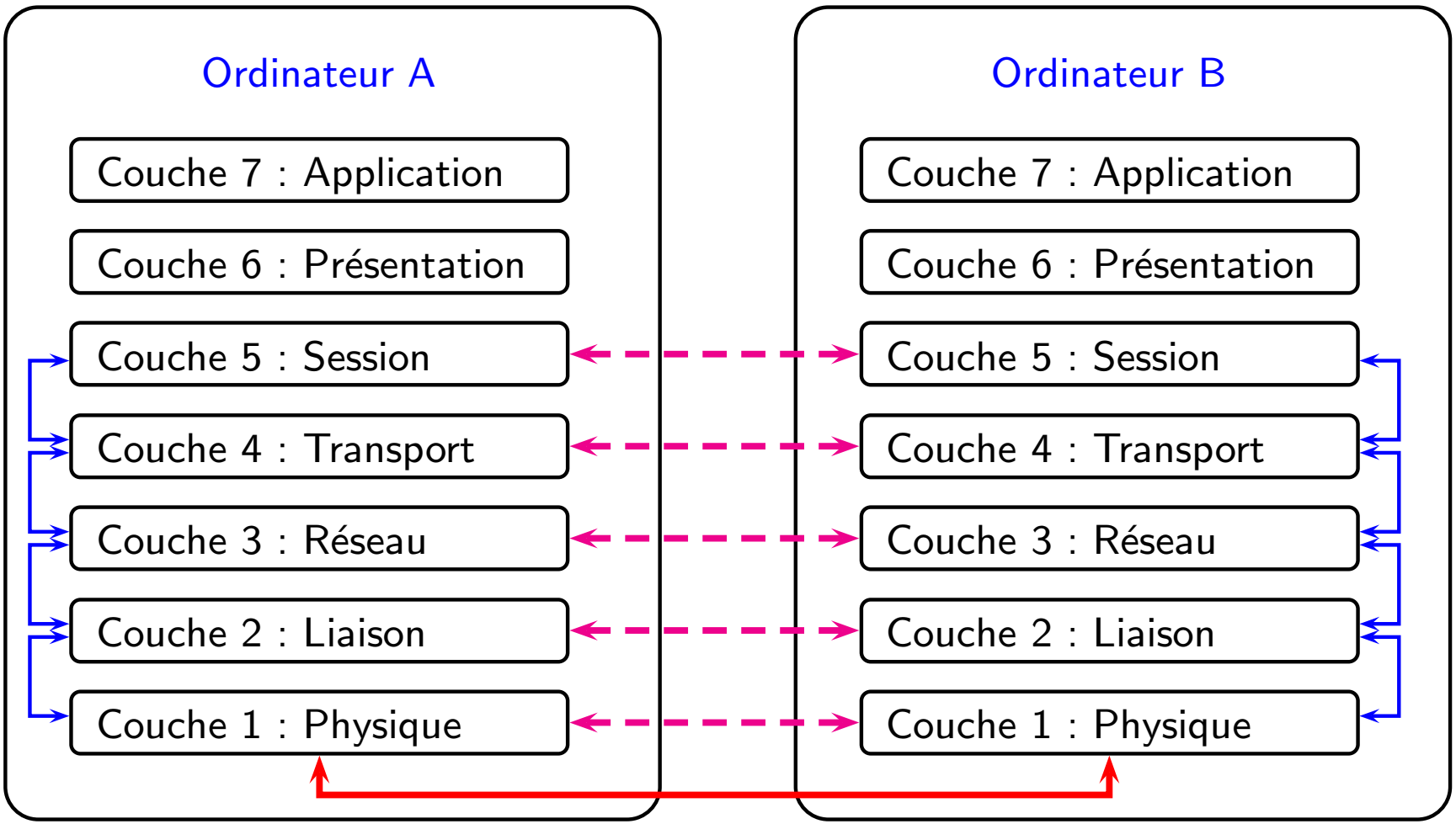
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



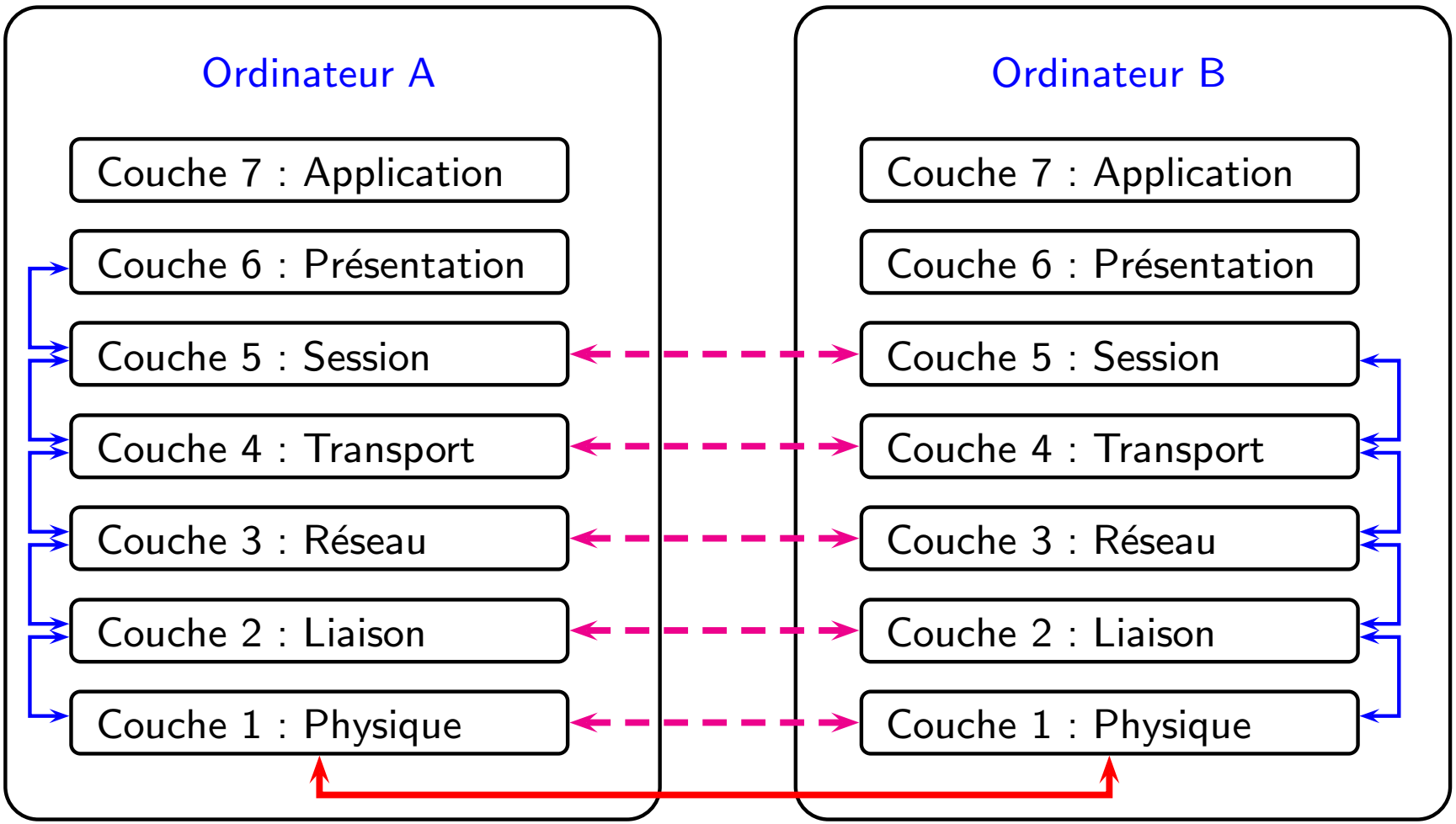
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



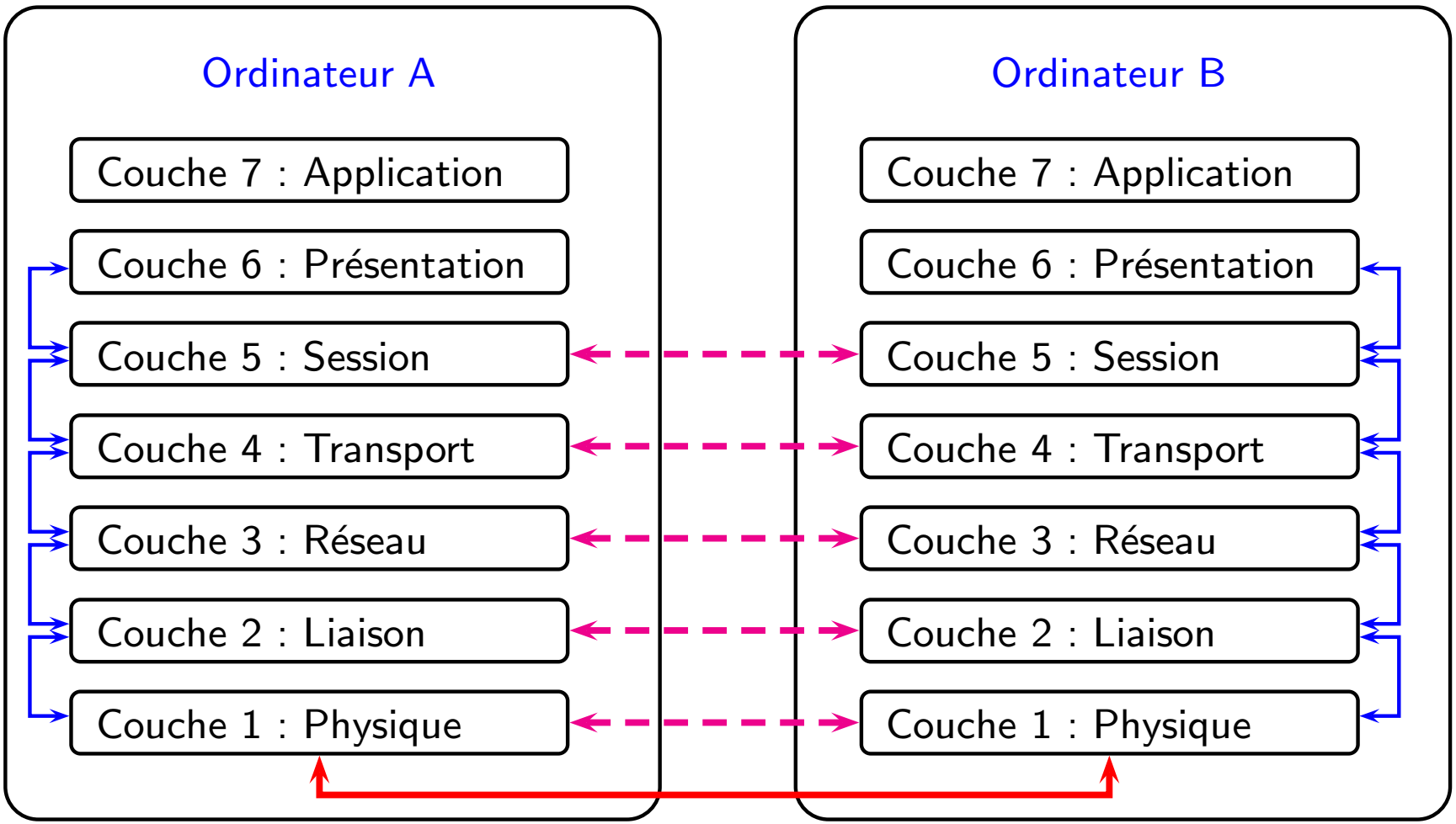
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



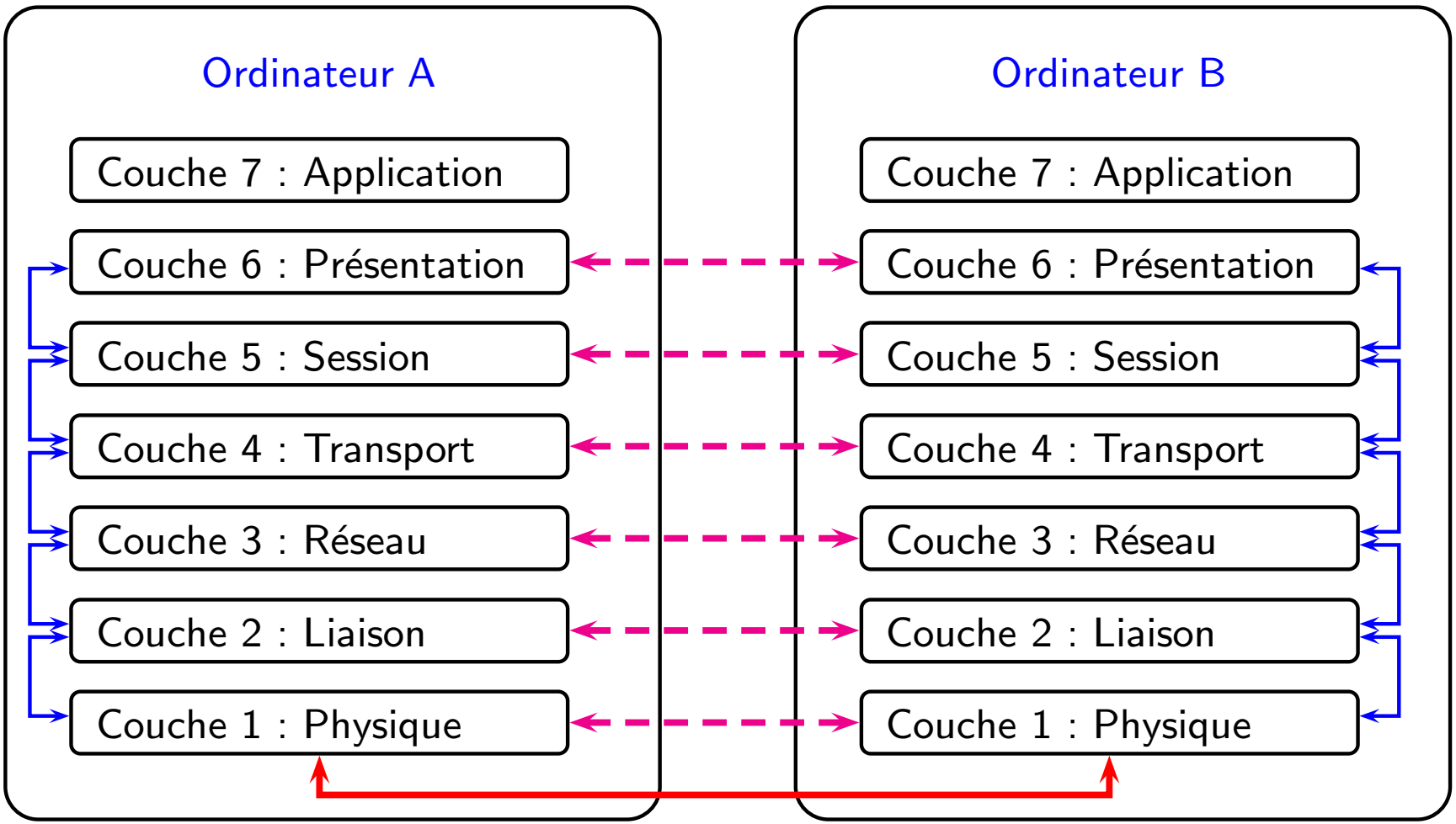
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



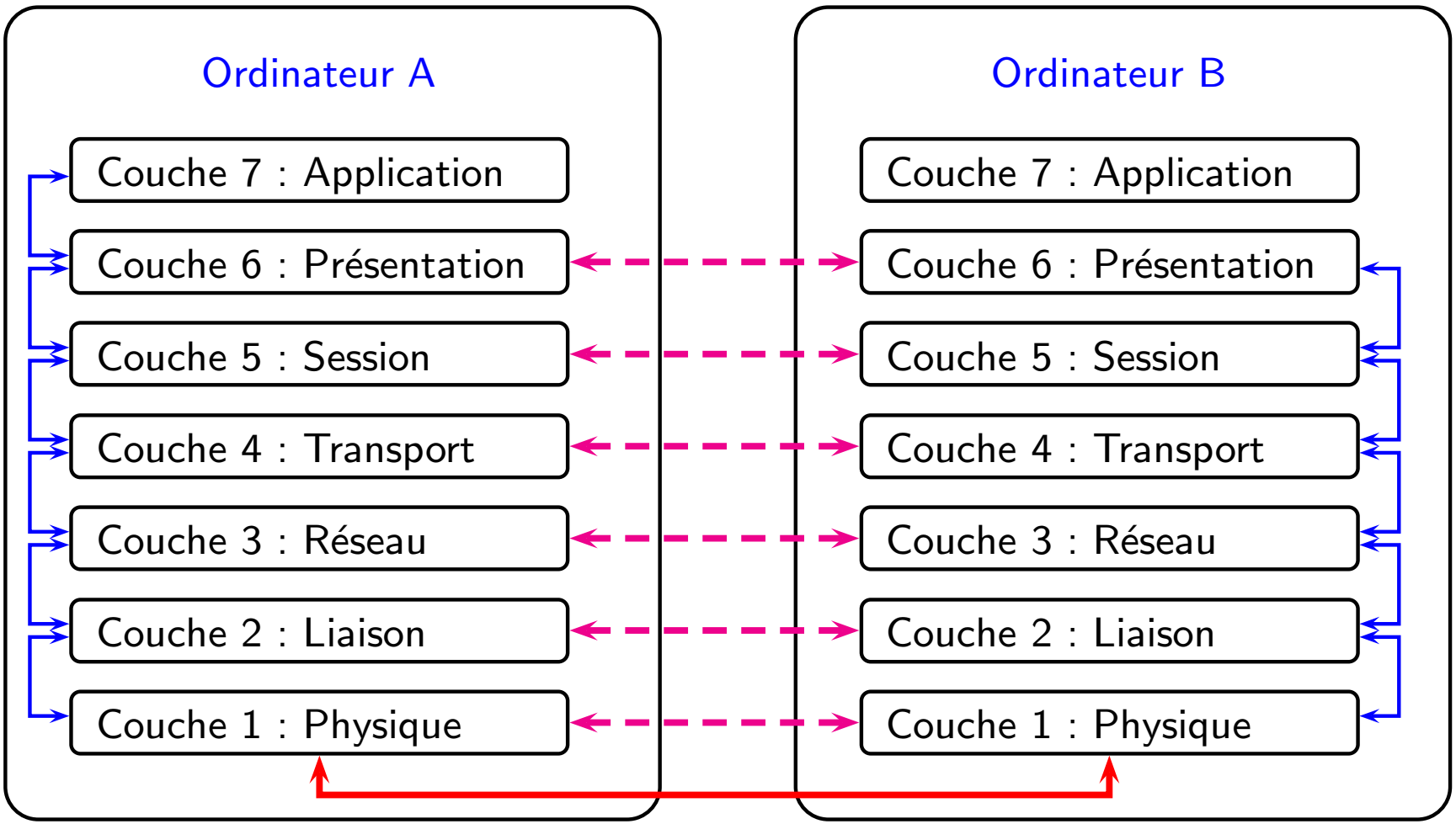
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



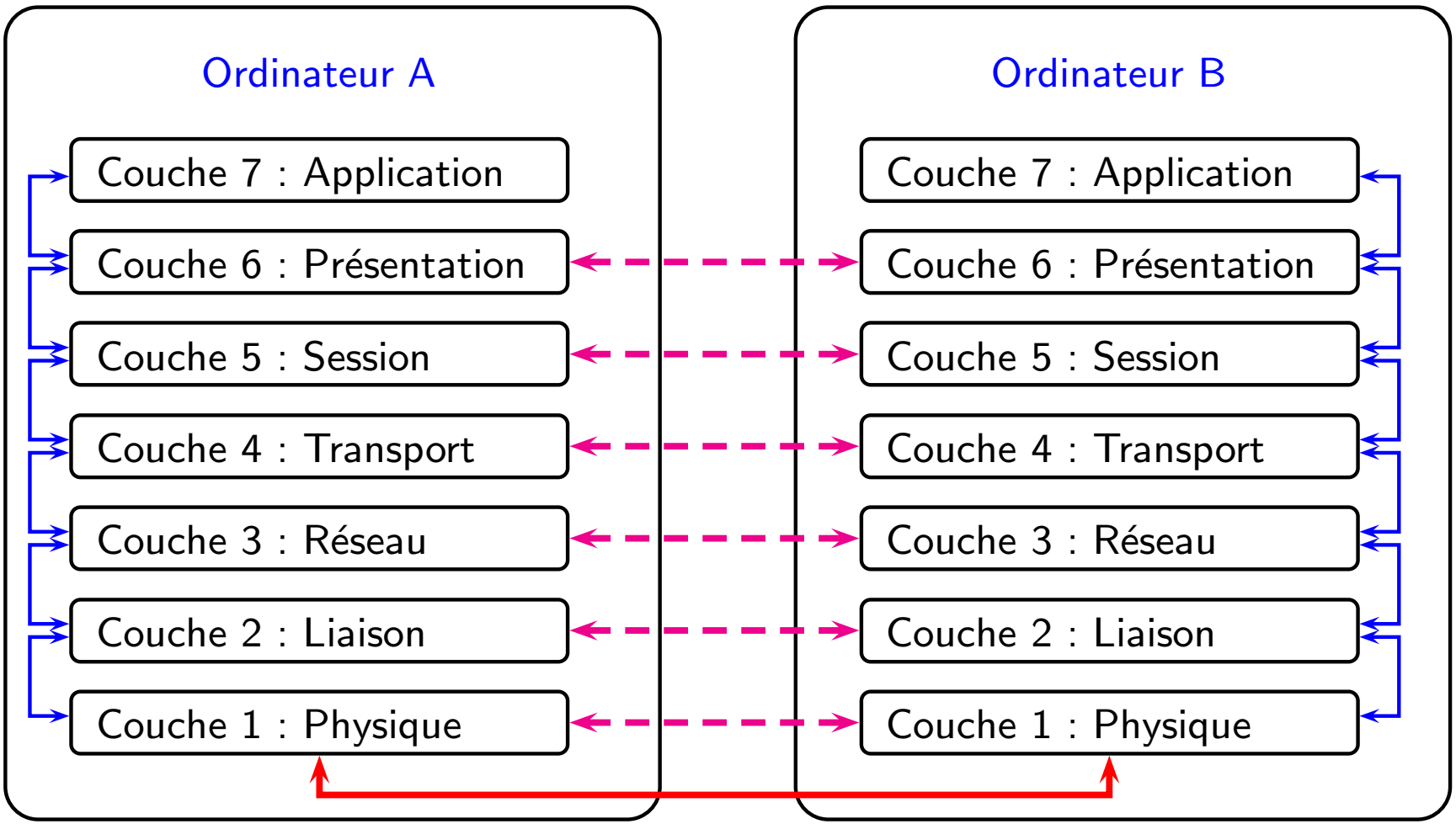
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



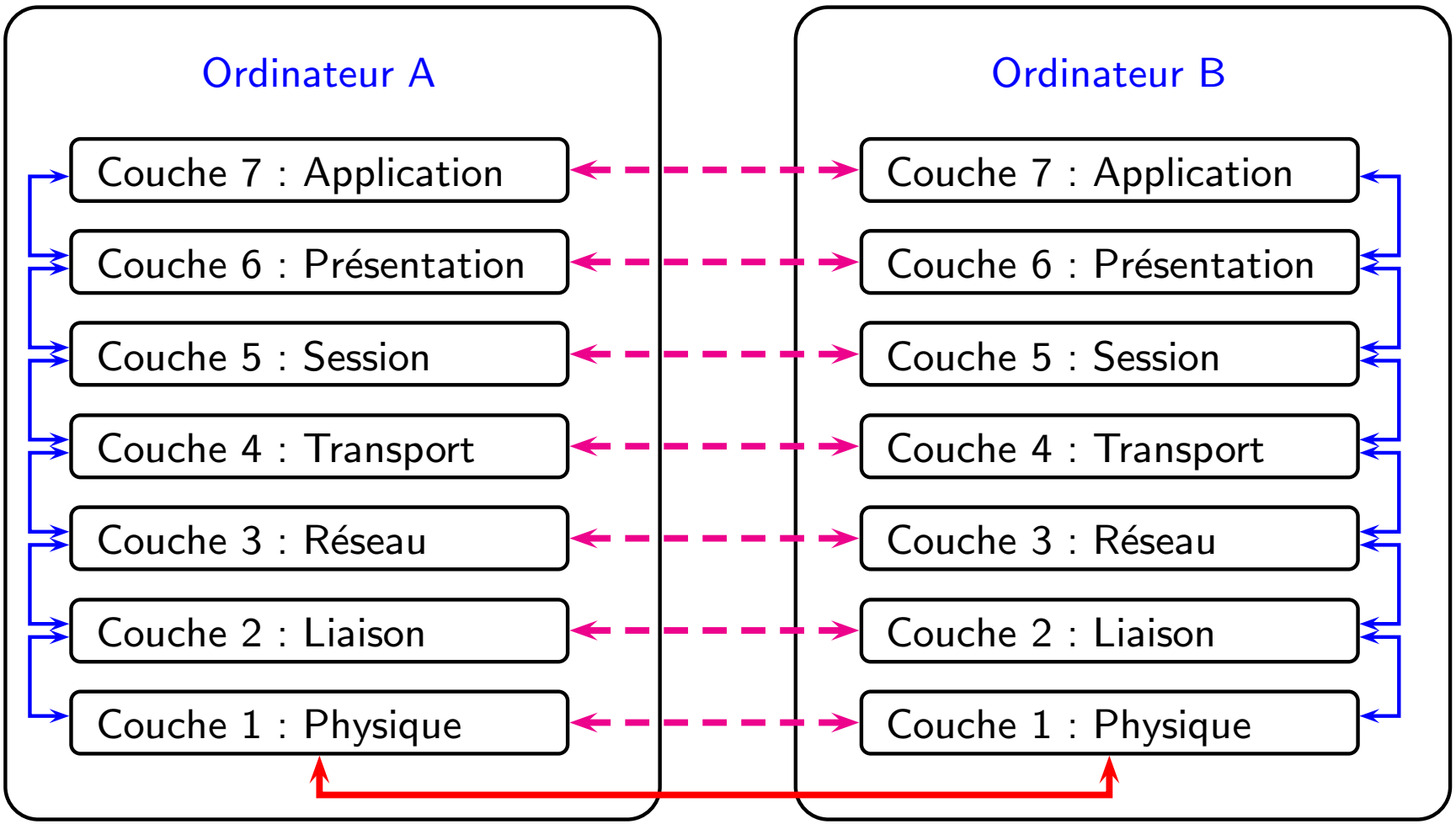
Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



Modèle OSI et protocoles

• Lorsque deux ordinateur entrent en contact, une liaison virtuelle est créée entre leurs couches correspondantes.



Modèle OSI et protocoles : suite

Modèle OSI et protocoles : suite

- Dans le modèle OSI, il y a deux types de communications :

Modèle OSI et protocoles : suite

- Dans le modèle OSI, il y a deux types de communications :
  – une verticale qui correspond aux transferts d'une couche à une autre ; cette communication est réalisée par des primitives de services ;

Modèle OSI et protocoles : suite

- Dans le modèle OSI, il y a deux types de communications :
  – une verticale qui correspond aux transferts d'une couche à une autre ; cette communication est réalisée par des primitives de services ;
  – une horizontale qui, par l'intermédiaire de messages échangés à travers le réseau, transfère, entre couche distantes de même niveau (couches homologues) des données.

Modèle OSI et protocoles : suite

- Dans le modèle OSI, il y a deux types de communications :
  – une verticale qui correspond aux transferts d'une couche à une autre ; cette communication est réalisée par des primitives de services ;
  – une horizontale qui, par l'intermédiaire de messages échangés à travers le réseau, transfère, entre couche distantes de même niveau (couches homologues) des données.

- Une communication entre couches de niveau N constitue un protocole de niveau N.

Modèle OSI et protocoles : suite

- Dans le modèle OSI, il y a deux types de communications :
  – une verticale qui correspond aux transferts d'une couche à une autre ; cette communication est réalisée par des primitives de services ;
  – une horizontale qui, par l'intermédiaire de messages échangés à travers le réseau, transfère, entre couche distantes de même niveau (couches homologues) des données.

- Une communication entre couches de niveau N constitue un protocole de niveau N.

- La couche de niveau N adjoint un en-tête précisant le travail à effectuer par la couche homologue ainsi que des instructions spéciales destiné à la couche inférieur.

Modèle simplifié de OSI

Modèle simplifié de OSI

- Techniquement les couches 5 et 6 du modèle OSI ne sont pas respectées.

Modèle simplifié de OSI

• Techniquement les couches 5 et 6 du modèle OSI ne sont pas respectées.

Couche 7 : Application

Couche 6 : Présentation

Couche 5 : Session

Couche 4 : Transport

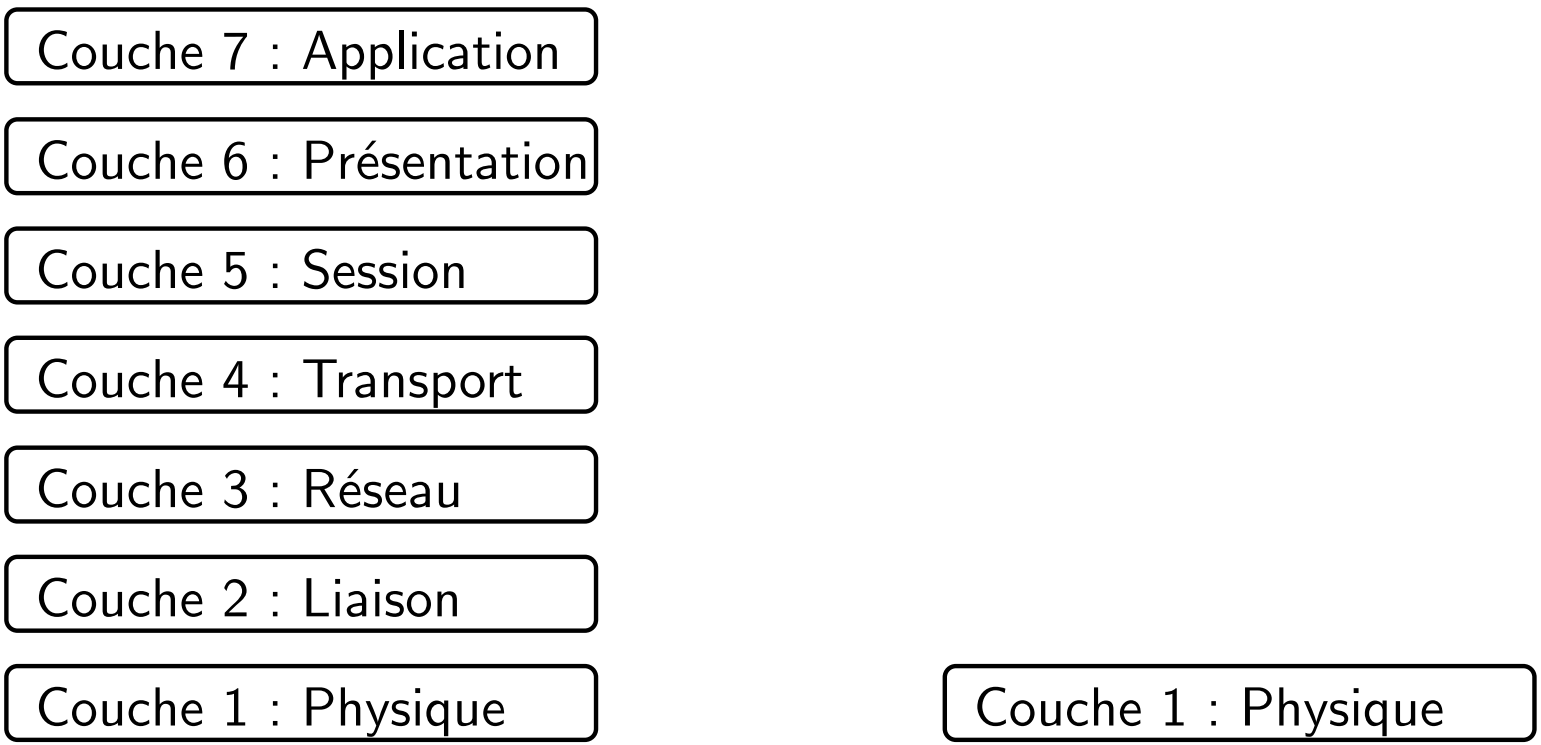
Couche 3 : Réseau

Couche 2 : Liaison

Couche 1 : Physique

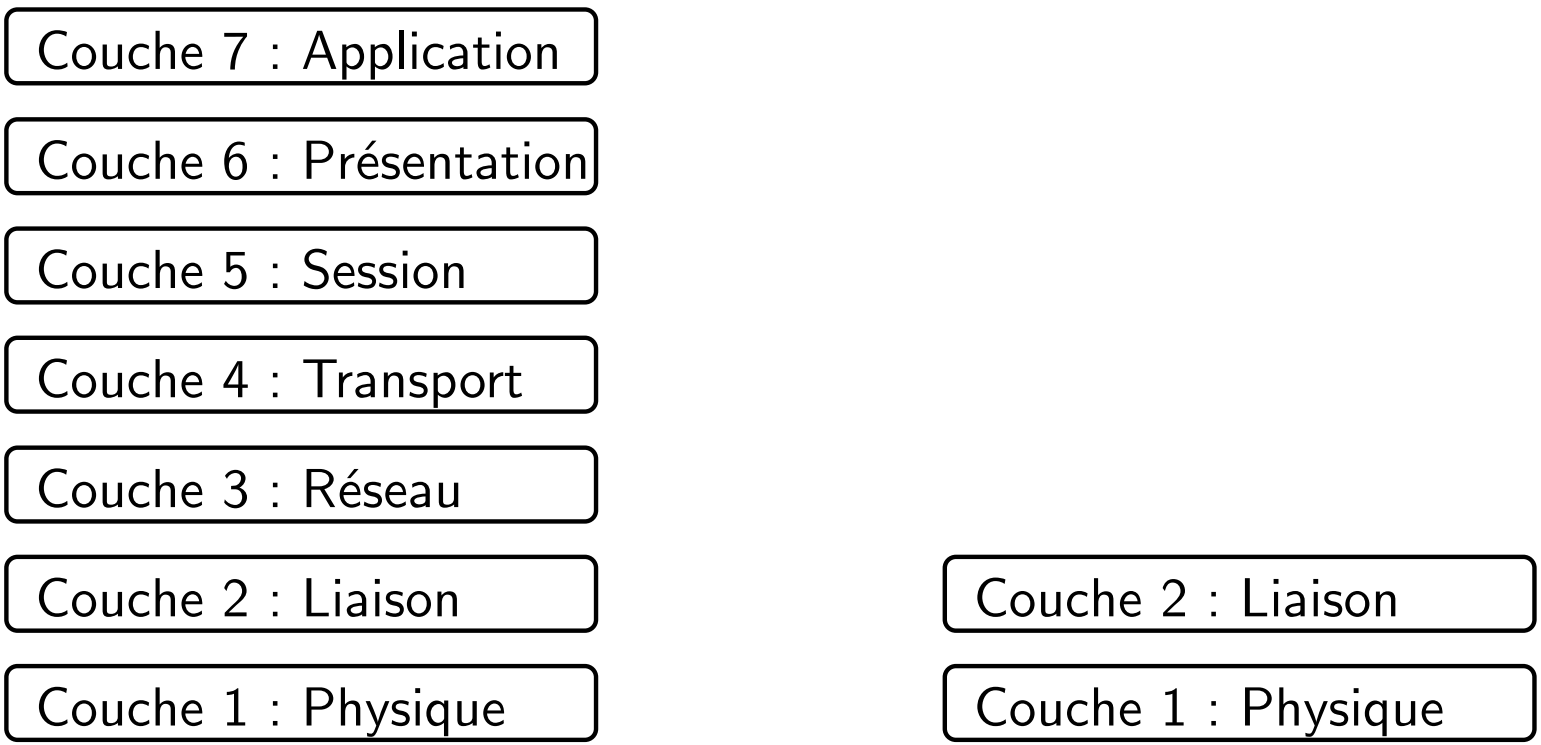
Modèle simplifié de OSI

• Techniquement les couches 5 et 6 du modèle OSI ne sont pas respectées.



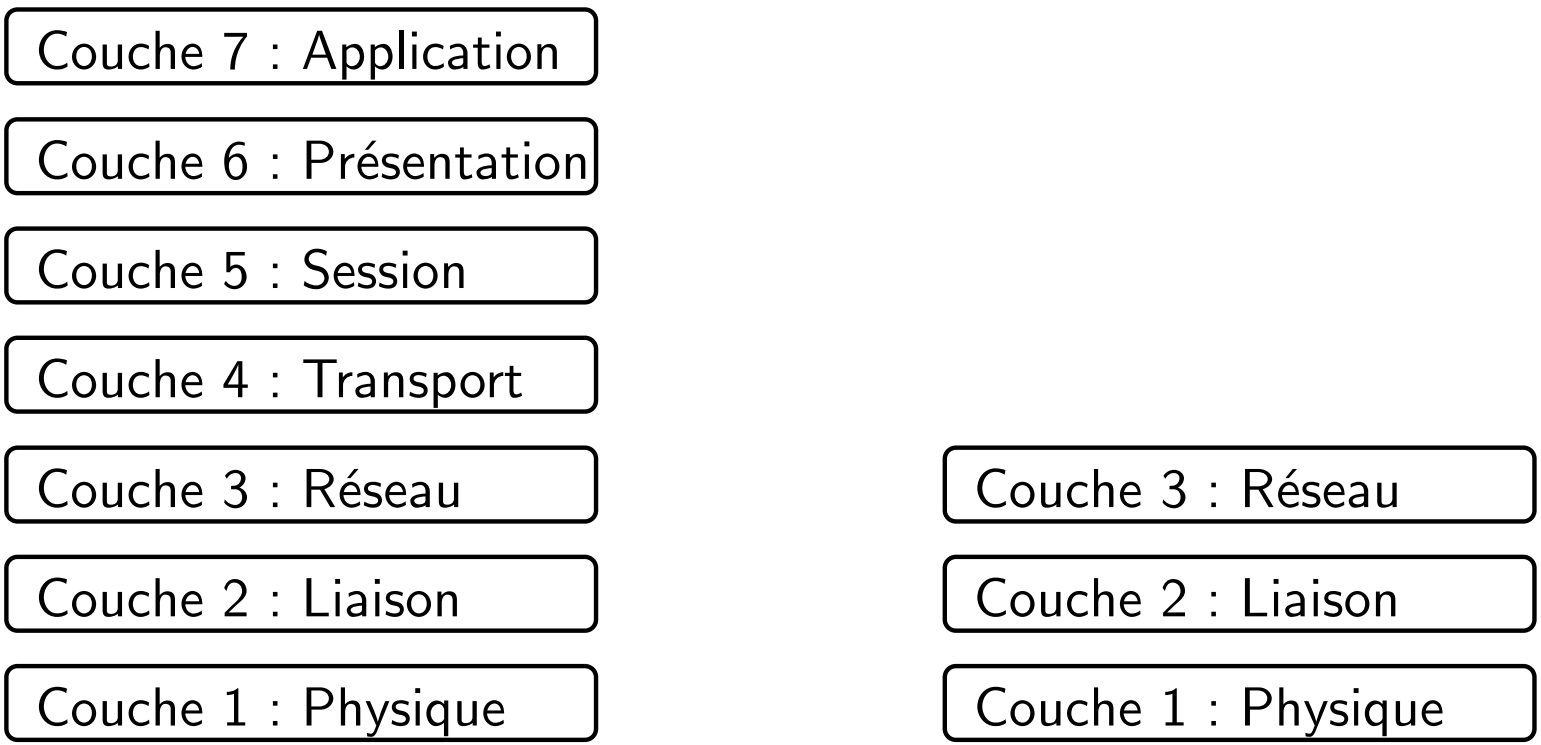
Modèle simplifié de OSI

• Techniquement les couches 5 et 6 du modèle OSI ne sont pas respectées.



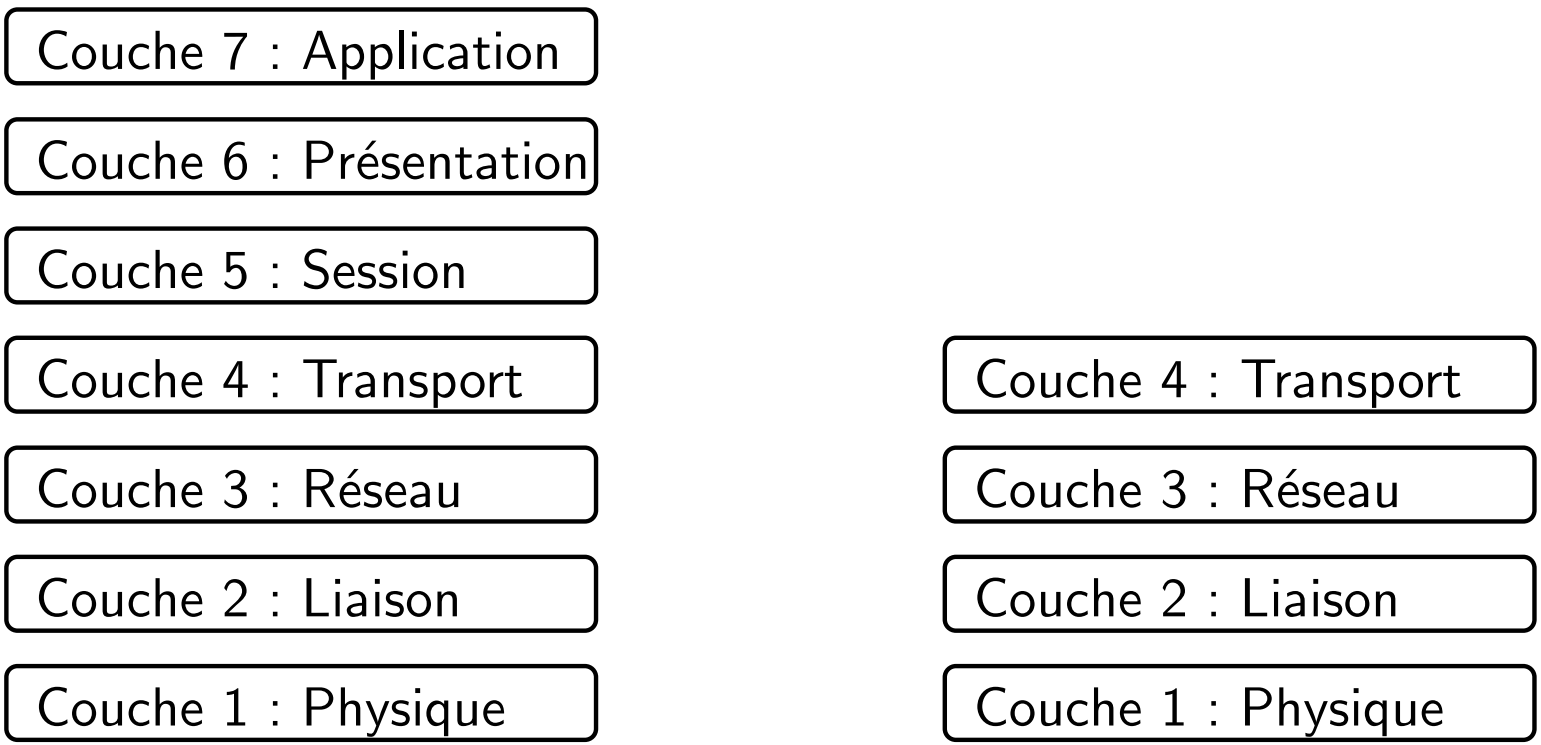
Modèle simplifié de OSI

• Techniquement les couches 5 et 6 du modèle OSI ne sont pas respectées.



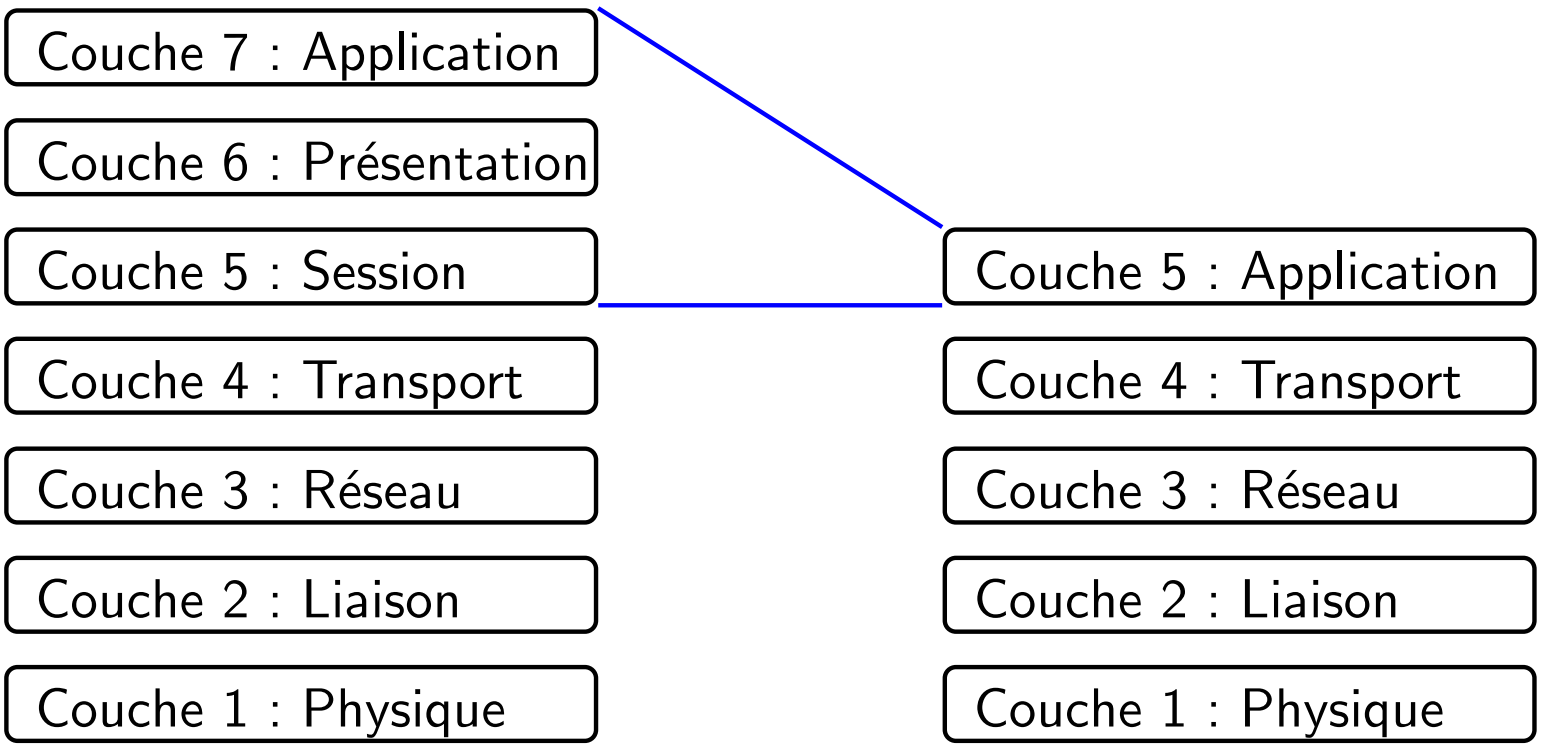
Modèle simplifié de OSI

• Techniquement les couches 5 et 6 du modèle OSI ne sont pas respectées.



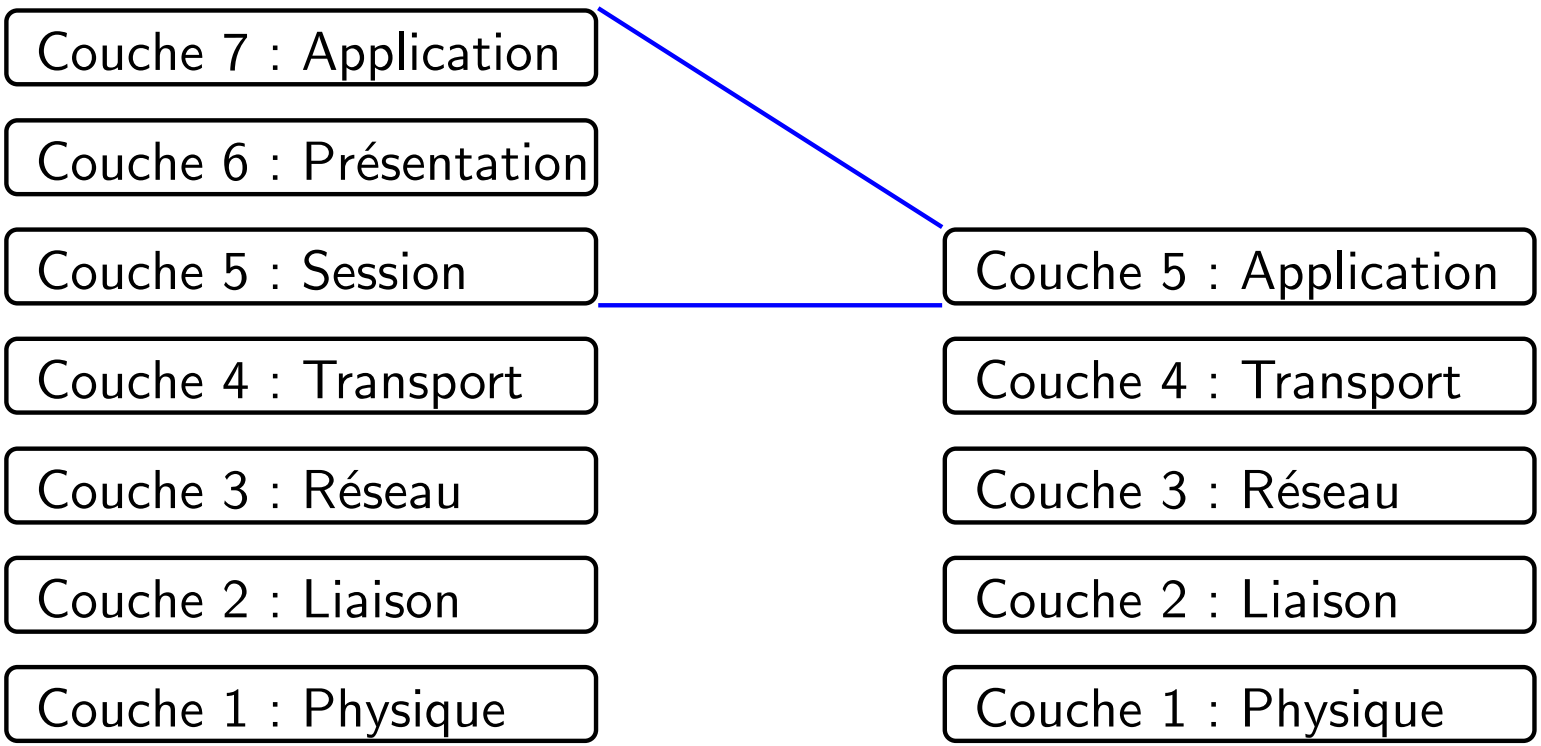
Modèle simplifié de OSI

- Techniquement les couches 5 et 6 du modèle OSI ne sont pas respectées.



Modèle simplifié de OSI

- Techniquement les couches 5 et 6 du modèle OSI ne sont pas respectées.



- Ressemble en modèle en couches de TCP/IP.

Couche et protocoles

Couche et protocoles

- Les couches peuvent délivrer différents service.

Couche et protocoles

- Les couches peuvent délivrer différents service.

- Un protocole est orienté connexion si un contact est établi en préalable à la communication, et si un contrôle de transmission s'effectue durant la communication afin de vérifier la bonne réception des données.

Couche et protocoles

- Les couches peuvent délivrer différents service.

- Un protocole est orienté connexion si un contact est établi en préalable à la communication, et si un contrôle de transmission s'effectue durant la communication afin de vérifier la bonne réception des données.
  $\rightsquigarrow$ TCP est un tel protocole.

Couche et protocoles

- Les couches peuvent délivrer différents service.

- Un protocole est orienté connexion si un contact est établi en préalable à la communication, et si un contrôle de transmission s'effectue durant la communication afin de vérifier la bonne réception des données.
  $\rightsquigarrow$ TCP est un tel protocole.

- Un protocole est non orienté connexion si, lors de l'envoie d'un message de l'émetteur, aucun mécanisme de vérification des données n'est mis en oeuvre.

Couche et protocoles

- Les couches peuvent délivrer différents service.

- Un protocole est orienté connexion si un contact est établi en préalable à la communication, et si un contrôle de transmission s'effectue durant la communication afin de vérifier la bonne réception des données.
  $\rightsquigarrow$ TCP est un tel protocole.

- Un protocole est non orienté connexion si, lors de l'envoie d'un message de l'émetteur, aucun mécanisme de vérification des données n'est mis en oeuvre.
  $\rightsquigarrow$ UDP est un tel protocole.

Faiblesse de TCP

Les protocoles de la couche transport n'assurent par une sécurité acceptable pour les communications. Les informations circulent de fait en clair, et les paquets routés au travers d'Internet peuvent être lus, interceptés, modifiés à chaque noeud traversé.

Faiblesse de TCP

Les protocoles de la couche transport n'assurent par une sécurité acceptable pour les communications. Les informations circulent de fait en clair, et les paquets routés au travers d'Internet peuvent être lus, interceptés, modifiés à chaque noeud traversé.

- L'envoi de cookies n'est pas sûr.

Faiblesse de TCP

Les protocoles de la couche transport n'assurent par une sécurité acceptable pour les communications. Les informations circulent de fait en clair, et les paquets routés au travers d'Internet peuvent être lus, interceptés, modifiés à chaque noeud traversé.

- L'envoi de cookies n'est pas sûr.
- L'authentification par mot de passe classique avec un fichier `.htaccess` n'est pas sûre non plus compte tenu du fait que le mot de passe transite en clair. Des analyseurs réseau tels que `Wireshark` (analyseur de trames) peuvent en effet intercepter ces flux.

Historique de SSL/TLS

SSL a été créé en juillet 1994. Le but était pour Netscape d'offrir un navigateur capable de réaliser des échanges cryptés avec les serveurs de Netscape.

Historique de SSL/TLS

SSL a été créé en juillet 1994. Le but était pour Netscape d'offrir un navigateur capable de réaliser des échanges cryptés avec les serveurs de Netscape.

La version 2 de SSL fut améliorée par Microsoft au niveau d'une couche de sécurité assez similaire, PCT.

Historique de SSL/TLS

SSL a été créé en juillet 1994. Le but était pour Netscape d'offrir un navigateur capable de réaliser des échanges cryptés avec les serveurs de Netscape.

La version 2 de SSL fut améliorée par Microsoft au niveau d'une couche de sécurité assez similaire, PCT.

La version 3, qui reprit les avantages de PCT, fut renommée TLS suite au rachat du brevet de Netscape par l'IETF en 2001. Ce sont essentiellement les mêmes protocoles.

Le rôle de SSL/TLS

Le rôle de SSL/TLS est de fournir l'authentification du serveur (certificats), la confidentialité (chiffrement à clef secrète) et l'intégrité des données transmises (hachage).

Le rôle de SSL/TLS

Le rôle de SSL/TLS est de fournir l'authentification du serveur (certificats), la confidentialité (chiffrement à clef secrète) et l'intégrité des données transmises (hachage).

De manière optionnelle, il peut aussi assurer l'authentification du client par le biais de certificats nuériques.

Le rôle de SSL/TLS

Le rôle de SSL/TLS est de fournir l'authentification du serveur (certificats), la confidentialité (chiffrement à clef secrète) et l'intégrité des données transmises (hachage).

De manière optionnelle, il peut aussi assurer l'authentification du client par le biais de certificats nuériques.

La couche SSL/TLS se situe à l'interface des couches "applications" et "transport" su modèle OSI.

Caractéristiques de SSL/TLS

Caractéristiques de SSL/TLS

- **Séparation des devoirs**. Authentification, chiffrement et intégrité sont des tâches assurées séparément avec différentes clefs secrètes.

Caractéristiques de SSL/TLS

- **Séparation des devoirs**. Authentification, chiffrement et intégrité sont des tâches assurées séparément avec différentes clefs secrètes.
- **Efficacité**. Possibilité de conserver en cache un secret maître.

Caractéristiques de SSL/TLS

- **Séparation des devoirs**. Authentification, chiffrement et intégrité sont des tâches assurées séparément avec différentes clefs secrètes.
- **Efficacité**. Possibilité de conserver en cache un secret maître.
- **Généricité**. Peut fourni une liaison sécurisée à n'importe quelle application :

Caractéristiques de SSL/TLS

- **Séparation des devoirs**. Authentification, chiffrement et intégrité sont des tâches assurées séparément avec différentes clefs secrètes.
- **Efficacité**. Possibilité de conserver en cache un secret maître.
- **Généricité**. Peut fourni une liaison sécurisée à n'importe quelle application :
  1. HTTP -¿ HTTPS

Caractéristiques de SSL/TLS

- **Séparation des devoirs**. Authentification, chiffrement et intégrité sont des tâches assurées séparément avec différentes clefs secrètes.
- **Efficacité**. Possibilité de conserver en cache un secret maître.
- **Généricité**. Peut fourni une liaison sécurisée à n'importe quelle application :
  1. HTTP -¿ HTTPS
  2. SMTP -¿ SSMTP

Caractéristiques de SSL/TLS

- **Séparation des devoirs**. Authentification, chiffrement et intégrité sont des tâches assurées séparément avec différentes clefs secrètes.
- **Efficacité**. Possibilité de conserver en cache un secret maître.
- **Généricité**. Peut fourni une liaison sécurisée à n'importe quelle application :
  1. HTTP -¿ HTTPS
  2. SMTP -¿ SSMTP
  3. POP3 -¿ SPOP3

Caractéristiques de SSL/TLS

- **Séparation des devoirs**. Authentification, chiffrement et intégrité sont des tâches assurées séparément avec différentes clefs secrètes.
- **Efficacité**. Possibilité de conserver en cache un secret maître.
- **Généricité**. Peut fourni une liaison sécurisée à n'importe quelle application :
  1. HTTP -¿ HTTPS
  2. SMTP -¿ SSMTP
  3. POP3 -¿ SPOP3
- **Protection contre les attaques Man in the middle ou replay attack** par l'usage de certificat.

Caractéristiques de SSL/TLS

- **Séparation des devoirs**. Authentification, chiffrement et intégrité sont des tâches assurées séparément avec différentes clefs secrètes.
- **Efficacité**. Possibilité de conserver en cache un secret maître.
- **Généricité**. Peut fourni une liaison sécurisée à n'importe quelle application :
  1. HTTP -¿ HTTPS
  2. SMTP -¿ SSMTP
  3. POP3 -¿ SPOP3
- **Protection contre les attaques Man in the middle ou replay attack** par l'usage de certificat.
- **Compression** possible avec chiffrement des données

Caractéristiques de SSL/TLS

- **Séparation des devoirs**. Authentification, chiffrement et intégrité sont des tâches assurées séparément avec différentes clefs secrètes.
- **Efficacité**. Possibilité de conserver en cache un secret maître.
- **Généricité**. Peut fourni une liaison sécurisée à n'importe quelle application :
  1. HTTP -¿ HTTPS
  2. SMTP -¿ SSMTP
  3. POP3 -¿ SPOP3
- **Protection contre les attaques Man in the middle ou replay attack** par l'usage de certificat.
- **Compression** possible avec chiffrement des données
- **Compatibilité** avec SSLv2

Caractéristiques de SSL/TLS

- **Séparation des devoirs**. Authentification, chiffrement et intégrité sont des tâches assurées séparément avec différentes clefs secrètes.
- **Efficacité**. Possibilité de conserver en cache un secret maître.
- **Généricité**. Peut fourni une liaison sécurisée à n'importe quelle application :
  1. HTTP -¿ HTTPS
  2. SMTP -¿ SSMTP
  3. POP3 -¿ SPOP3
- **Protection contre les attaques Man in the middle ou replay attack** par l'usage de certificat.
- **Compression** possible avec chiffrement des données
- **Compatibilité** avec SSLv2
- **Performances moindres**

Objectifs

Dans cette partie nous aborderons les attaques de bases :

Objectifs

Dans cette partie nous aborderons les attaques de bases :
- usurpation d'identité

Objectifs

Dans cette partie nous aborderons les attaques de bases :

- usurpation d'identité
- attaque par déni de service

Objectifs

Dans cette partie nous aborderons les attaques de bases :

- usurpation d'identité
- attaque par déni de service
- manipulation de données

Objectifs

Dans cette partie nous aborderons les attaques de bases :

- usurpation d'identité
- attaque par déni de service
- manipulation de données

Nous distinguerons les deux modes d'attaques suivant :

Objectifs

Dans cette partie nous aborderons les attaques de bases :
- usurpation d'identité
- attaque par déni de service
- manipulation de données

Nous distinguerons les deux modes d'attaques suivant :
- les méthodes actives (leurres, exploitations de failles de sécurité)

Objectifs

Dans cette partie nous aborderons les attaques de bases :
- usurpation d'identité
- attaque par déni de service
- manipulation de données

Nous distinguerons les deux modes d'attaques suivant :
- les méthodes actives (leurres, exploitations de failles de sécurité)
- les méthodes passives : man in the middle

Usurpation d'identité : But

Le but de cette technique est de récupérer un coupe (identifiant/mot de passe) afin de

Usurpation d'identité : But

Le but de cette technique est de récupérer un coupe (identifiant/mot de passe) afin de

- espionner

Usurpation d'identité : But

Le but de cette technique est de récupérer un coupe (identifiant/mot de passe) afin de

- espionner
- détruire des données

Usurpation d'identité : But

Le but de cette technique est de récupérer un coupe (identifiant/mot de passe) afin de

- espionner
- détruire des données
- vol de donnée

Usurpation d'identité : But

Le but de cette technique est de récupérer un coupe (identifiant/mot de passe) afin de

- espionner
- détruire des données
- vol de donnée
- faire une attaque atcive

Usurpation d'identité : But

Le but de cette technique est de récupérer un coupe (identifiant/mot de passe) afin de

- espionner
- détruire des données
- vol de donnée
- faire une attaque atcive
- ...

Usurpation d'identité : Méthodes astucieuces

• Remarque : Il n'est pas nécessaire de casser le haché d'un mot de passe !

En effet :

Usurpation d'identité : Méthodes astucieuces

• Remarque : Il n'est pas nécessaire de casser le haché d'un mot de passe !

En effet :
- le mot de passe peut être évident

Usurpation d'identité : Méthodes astucieuces

• Remarque : Il n'est pas nécessaire de casser le haché d'un mot de passe !

En effet :
- le mot de passe peut être évident
- il peut y avoir une complicité avec l'attaquant

Usurpation d'identité : Méthodes astucieuces

• Remarque : Il n'est pas nécessaire de casser le haché d'un mot de passe !

En effet :
- le mot de passe peut être évident
- il peut y avoir une complicité avec l'attaquant
- social engineering (l'attaquant se fait passer pour un administrateur)

Usurpation d'identité : Méthodes passives

• Fait : Les mots de passes sont véhiculés par le réseau de la machine de l'utilisateur au serveur d'authentification.

Usurpation d'identité : Méthodes passives

• Fait : Les mots de passes sont véhiculés par le réseau de la machine de l'utilisateur au serveur d'authentification.

⇝ On peut alors récupérer le mot de passe en écoutant le réseau :

Usurpation d'identité : Méthodes passives

• Fait : Les mots de passes sont véhiculés par le réseau de la machine de l'utilisateur au serveur d'authentification.

⇝ On peut alors récupérer le mot de passe en écoutant le réseau : Sniffing.

Usurpation d'identité : Méthodes passives

• Fait : Les mots de passes sont véhiculés par le réseau de la machine de l'utilisateur au serveur d'authentification.

⇝ On peut alors récupérer le mot de passe en écoutant le réseau : Sniffing.

D'autant plus que certains protocole les transmettent en clair :

Usurpation d'identité : Méthodes passives

• Fait : Les mots de passes sont véhiculés par le réseau de la machine de l'utilisateur au serveur d'authentification.

⇝ On peut alors récupérer le mot de passe en écoutant le réseau : Sniffing.

D'autant plus que certains protocole les transmettent en clair :
– telnet

Usurpation d'identité : Méthodes passives

• Fait : Les mots de passes sont véhiculés par le réseau de la machine de l'utilisateur au serveur d'authentification.

⇝ On peut alors récupérer le mot de passe en écoutant le réseau : Sniffing.

D'autant plus que certains protocole les transmettent en clair :
- telnet
- smtp

Usurpation d'identité : Méthodes passives

• Fait : Les mots de passes sont véhiculés par le réseau de la machine de l'utilisateur au serveur d'authentification.

⇝ On peut alors récupérer le mot de passe en écoutant le réseau : Sniffing.

D'autant plus que certains protocole les transmettent en clair :
- telnet
- smtp
- pop sans ssl

Usurpation d'identité : Méthodes passives

• Fait : Les mots de passes sont véhiculés par le réseau de la machine de l'utilisateur au serveur d'authentification.

⇝ On peut alors récupérer le mot de passe en écoutant le réseau : Sniffing.

D'autant plus que certains protocole les transmettent en clair :
- telnet
- smtp
- pop sans ssl
- http

Usurpation d'identité : Méthodes passives

• Fait : Les mots de passes sont véhiculés par le réseau de la machine de l'utilisateur au serveur d'authentification.

⇝ On peut alors récupérer le mot de passe en écoutant le réseau : Sniffing.

D'autant plus que certains protocole les transmettent en clair :
- telnet
- smtp
- pop sans ssl
- http

⇝ L'utilisation de SSL ou de haché augment la sécurité mais n'est pas parfaite.

Usurpation d'identité : Méthodes actives

Un Key-Logger (certain trojan) est un logiciel qui permet d'écouter et d'enregistrer les frappes claviers et (position/clic de la souris). L'attaquant, une fois le logiciel implanté, n' a plus qu'à attendre qu'un utilisateur s'authentifie.

Usurpation d'identité : Méthodes actives

Un Key-Logger (certain trojan) est un logiciel qui permet d'écouter et d'enregistrer les frappes claviers et (position/clic de la souris). L'attaquant, une fois le logiciel implanté, n' a plus qu'à attendre qu'un utilisateur s'authentifie.

Une attaque très répandue consiste à reproduire la page d'authentification d'un site (à l'aide de CSS par ex.) et d'envoyer l'identifiant/mot de passe à la page correspondante su site ainsi que sur une zone de stockage .

Usurpation d'identité : Méthodes actives

Les couples (identifiant/mot de passe) ont une *existence physique* :

Usurpation d'identité : Méthodes actives

Les couples (identifiant/mot de passe) ont une *existence physique* :
- dans les fichiers du serveur d'authentification ;

Usurpation d'identité : Méthodes actives

Les couples (identifiant/mot de passe) ont une *existence physique* :
- dans les fichiers du serveur d'authentification ;
- dans les fichier stockés par des logiciels (cookies, ...)

Usurpation d'identité : Méthodes actives

Les couples (identifiant/mot de passe) ont une *existence physique* :
- dans les fichiers du serveur d'authentification ;
- dans les fichier stockés par des logiciels (cookies, ...)
- dans les fichiers logs (si mauvaise saisie)

Usurpation d'identité : Méthodes actives

Les couples (identifiant/mot de passe) ont une *existence physique* :
- dans les fichiers du serveur d'authentification ;
- dans les fichier stockés par des logiciels (cookies, ...)
- dans les fichiers logs (si mauvaise saisie)

Si l'attaquant met la main sur ces fichiers, il ne lui reste plus qu'à casser les couples (utilisateurs/mot de passes).

Usurpation d'identité : Méthodes actives

Pour cela il existe des logiciels, (exemple : *john the ripper*)

Usurpation d'identité : Méthodes actives

Pour cela il existe des logiciels, (exemple : *john the ripper*)

Attaque de mot de passe :

Usurpation d'identité : Méthodes actives

Pour cela il existe des logiciels, (exemple : *john the ripper*)

Attaque de mot de passe :

- force brute on casser le mot de passe en testant toutes les combinaisons (environ 8^{94} en protection standard).

Usurpation d'identité : Méthodes actives

Pour cela il existe des logiciels, (exemple : *john the ripper*)

Attaque de mot de passe :

- force brute on casser le mot de passe en testant toutes les combinaisons (environ 8^{94} en protection standard).
- par dictionnaire : on va utiliser un dictionnaire des mots et noms de la langue les plus courants, combinés avec des chiffres, des versions modifié, ... (il y a environ 80000 mots dans la langue française).

Attaque par Dénie de Service (DOS)

- Principe : Sollicité un service jusqu'à le rendre indisponible :

Attaque par Dénie de Service (DOS)

- Principe : Sollicité un service jusqu'à le rendre indisponible :
  - arrêt du serveur/service

Attaque par Dénie de Service (DOS)

- Principe : Sollicité un service jusqu'à le rendre indisponible :
  – arrêt du serveur/service
  – consommation des ressources (processeur, mémoire, bande passant, espace disque, ...)

Attaque par Dénie de Service (DOS)

- Principe : Sollicité un service jusqu'à le rendre indisponible :
  – arrêt du serveur/service
  – consommation des ressources (processeur, mémoire, bande passant, espace disque, ...)
  – destruction matérielle ou logicielle

Dénie de service bassique

Les attaques les plus basiques sont :

Dénie de service bassique

Les attaques les plus basiques sont :

- le *mail-bombing* : envoi de mails pour soit rendre inutilisable la boîte mail ou en consommer toute la place

Dénie de service bassique

Les attaques les plus basiques sont :

- le *mail-bombing* : envoi de mails pour soit rendre inutilisable la boîte mail ou en consommer toute la place
- le *flood attack* envoi de message en continu sur un salon de discution ou un forum

Dénie de service bassique

Les attaques les plus basiques sont :

- le *mail-bombing* : envoi de mails pour soit rendre inutilisable la boîte mail ou en consommer toute la place
- le *flood attack* envoi de message en continu sur un salon de discution ou un forum
- bombe logique (`while(1) fork();`)

Attaque par saturation à message unique

Ce genre d'attaque consiste à envoyer un message défectueux à la cible :

Attaque par saturation à message unique

Ce genre d'attaque consiste à envoyer un message défectueux à la cible :

- `Teardrop` : utilisation de la recomposition des messages du protocole TCP/IP ;

Attaque par saturation à message unique

Ce genre d'attaque consiste à envoyer un message défectueux à la cible :

- `Teardrop` : utilisation de la recomposition des messages du protocole TCP/IP ;
- `Ping of death` : envoi d'un ping avec un paquet trop *gros* ;

Attaque par saturation à message unique

Ce genre d'attaque consiste à envoyer un message défectueux à la cible :

- `Teardrop` : utilisation de la recomposition des messages du protocole TCP/IP ;
- `Ping of death` : envoi d'un ping avec un paquet trop *gros* ;
- `LAND` : envoi d'un paquet (*spoofé*) SYN ayant pour destinataire la cible.

Attaque par saturation à message unique

Ce genre d'attaque consiste à envoyer un message défectueux à la cible :

- `Teardrop` : utilisation de la recomposition des messages du protocole TCP/IP ;
- `Ping of death` : envoi d'un ping avec un paquet trop *gros* ;
- `LAND` : envoi d'un paquet (*spoofé*) SYN ayant pour destinataire la cible.

$\rightsquigarrow$ d'autre méthode existent : SYN flood, SMURFING, ...

Modification de données : but

Les motifs classiques de la modification de données sont généralement :

Modification de données : but

Les motifs classiques de la modification de données sont généralement :

- l'ajout de publicité sur un site ;

Modification de données : but

Les motifs classiques de la modification de données sont généralement :

- l'ajout de publicité sur un site ;
- le discrédit d'un site web commerciale ou d'un portail d'un gros organisme ;

Modification de données : but

Les motifs classiques de la modification de données sont généralement :

- l'ajout de publicité sur un site ;
- le discrédit d'un site web commerciale ou d'un portail d'un gros organisme ;
- la destruction de données.

Modification de données : attaques pas injection

• Définition : Une attaque par injection consiste à injecter du code à l'aide d'une faille de sécurité ou d'un programme pour :

Modification de données : attaques pas injection

• Définition : Une attaque par injection consiste à injecter du code à l'aide d'une faille de sécurité ou d'un programme pour :

- forcer le programme à afficher des données qu'il ne devait pas ;

Modification de données : attaques pas injection

• Définition : Une attaque par injection consiste à injecter du code à l'aide d'une faille de sécurité ou d'un programme pour :

- forcer le programme à afficher des données qu'il ne devait pas ;
- récupérer la main sur la machine hébergeant le programme ;

Les attaques par injections les plus fréquentes sont les suivantes :

Modification de données : attaques pas injection

• Définition : Une attaque par injection consiste à injecter du code à l'aide d'une faille de sécurité ou d'un programme pour :

- forcer le programme à afficher des données qu'il ne devait pas ;
- récupérer la main sur la machine hébergeant le programme ;

Les attaques par injections les plus fréquentes sont les suivantes :

- Injection système : Unix, Windows, ... ;

Modification de données : attaques pas injection

• Définition : Une attaque par injection consiste à injecter du code à l'aide d'une faille de sécurité ou d'un programme pour :

- forcer le programme à afficher des données qu'il ne devait pas ;
- récupérer la main sur la machine hébergeant le programme ;

Les attaques par injections les plus fréquentes sont les suivantes :

- Injection système : Unix, Windows, ... ;
- Injection SQL : Accès à des base de données de manières détournées ;

Modification de données : attaques pas injection

• Définition : Une attaque par injection consiste à injecter du code à l'aide d'une faille de sécurité ou d'un programme pour :

- forcer le programme à afficher des données qu'il ne devait pas ;
- récupérer la main sur la machine hébergeant le programme ;

Les attaques par injections les plus fréquentes sont les suivantes :

- Injection système : Unix, Windows, ... ;
- Injection SQL : Accès à des base de données de manières détournées ;
- Injection sur les variables globales de type `GET` ;

Modification de données : attaques pas injection

• Définition : Une attaque par injection consiste à injecter du code à l'aide d'une faille de sécurité ou d'un programme pour :

- forcer le programme à afficher des données qu'il ne devait pas ;
- récupérer la main sur la machine hébergeant le programme ;

Les attaques par injections les plus fréquentes sont les suivantes :

- Injection système : Unix, Windows, ... ;
- Injection SQL : Accès à des base de données de manières détournées ;
- Injection sur les variables globales de type `GET` ;
- Cross Site Scripting.