Protocol Deep Dive: SSH and Telnet

THE SECURE SHELL (SSH) PROTOCOL

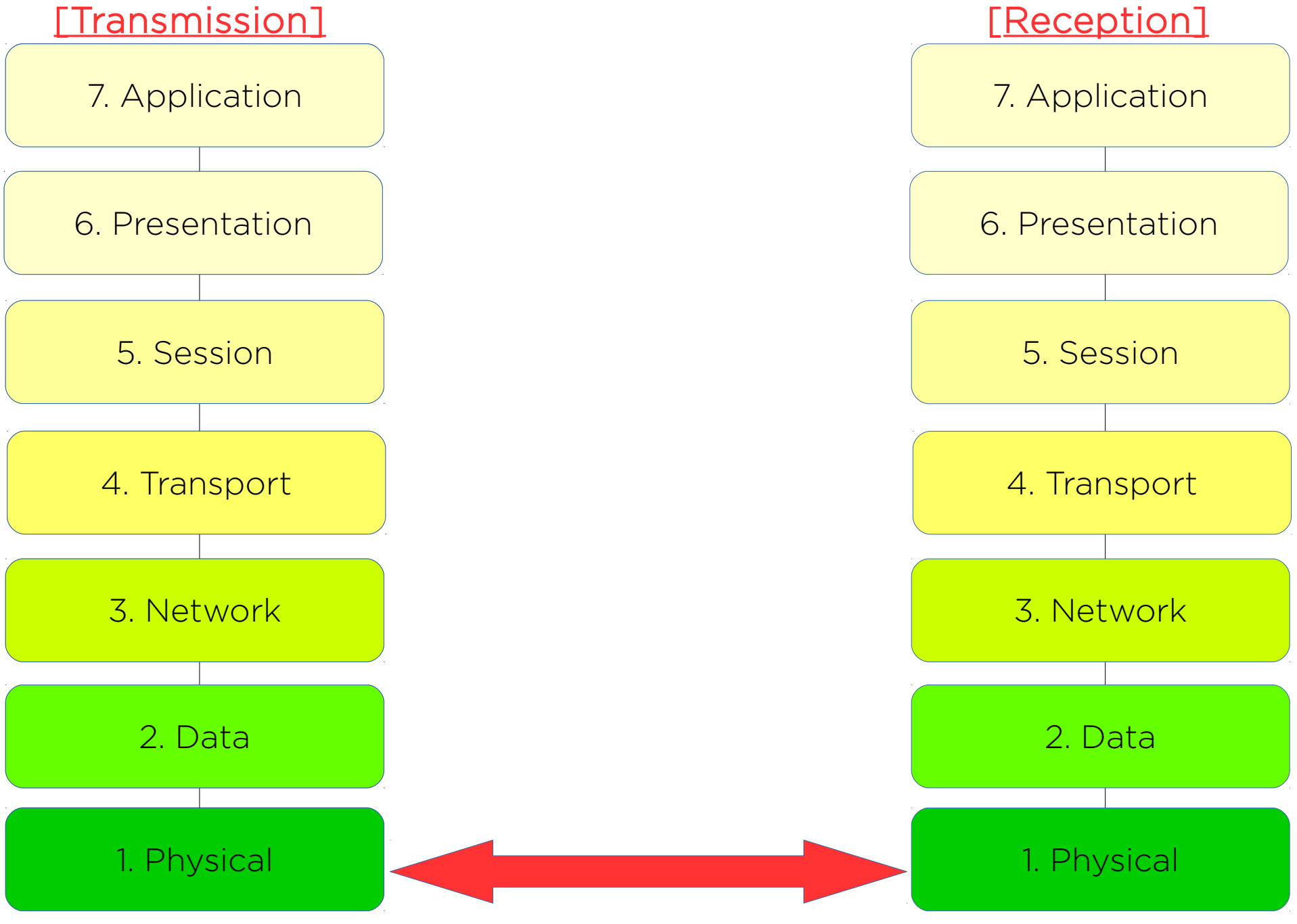
David Clinton
LINUX SYSTEM ADMINISTRATOR

www.bootstrap-it.com/networking | www.bootstrap-it.com/blog

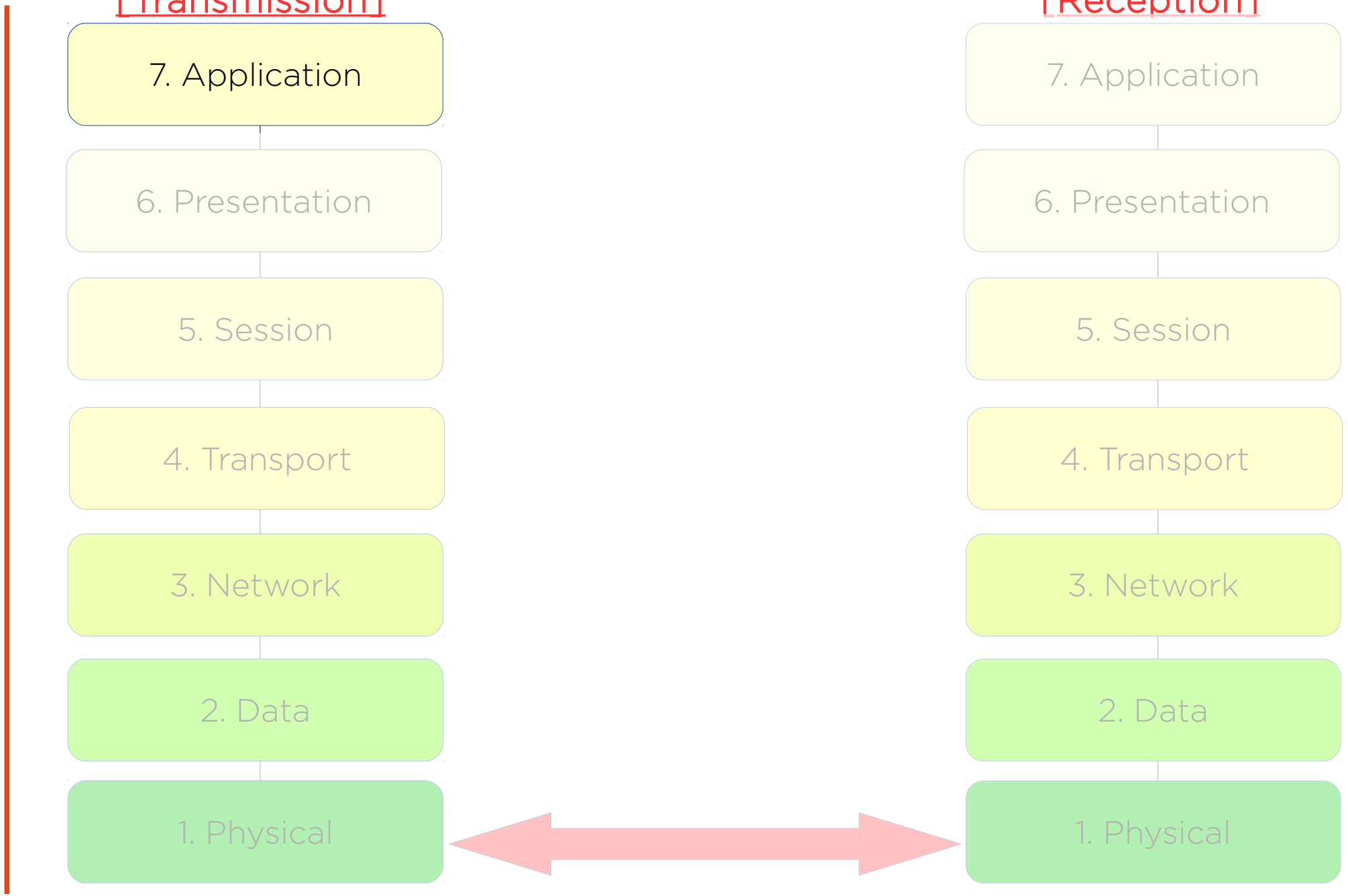
Communication Protocol

"Accepted rules that establish the synchronization methodology and syntax that parties to a communication session will use to govern their exchanges."

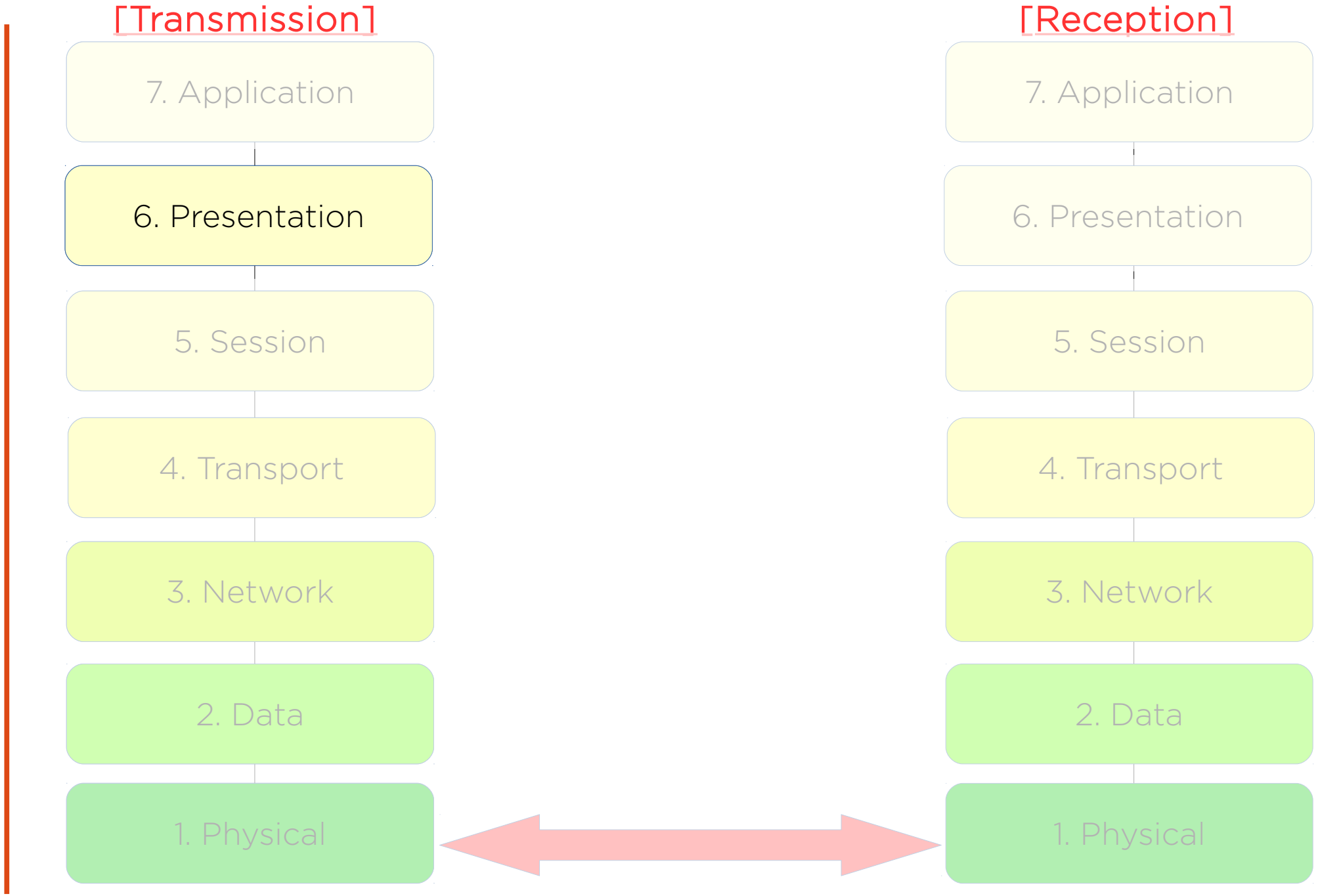
The OSI Model



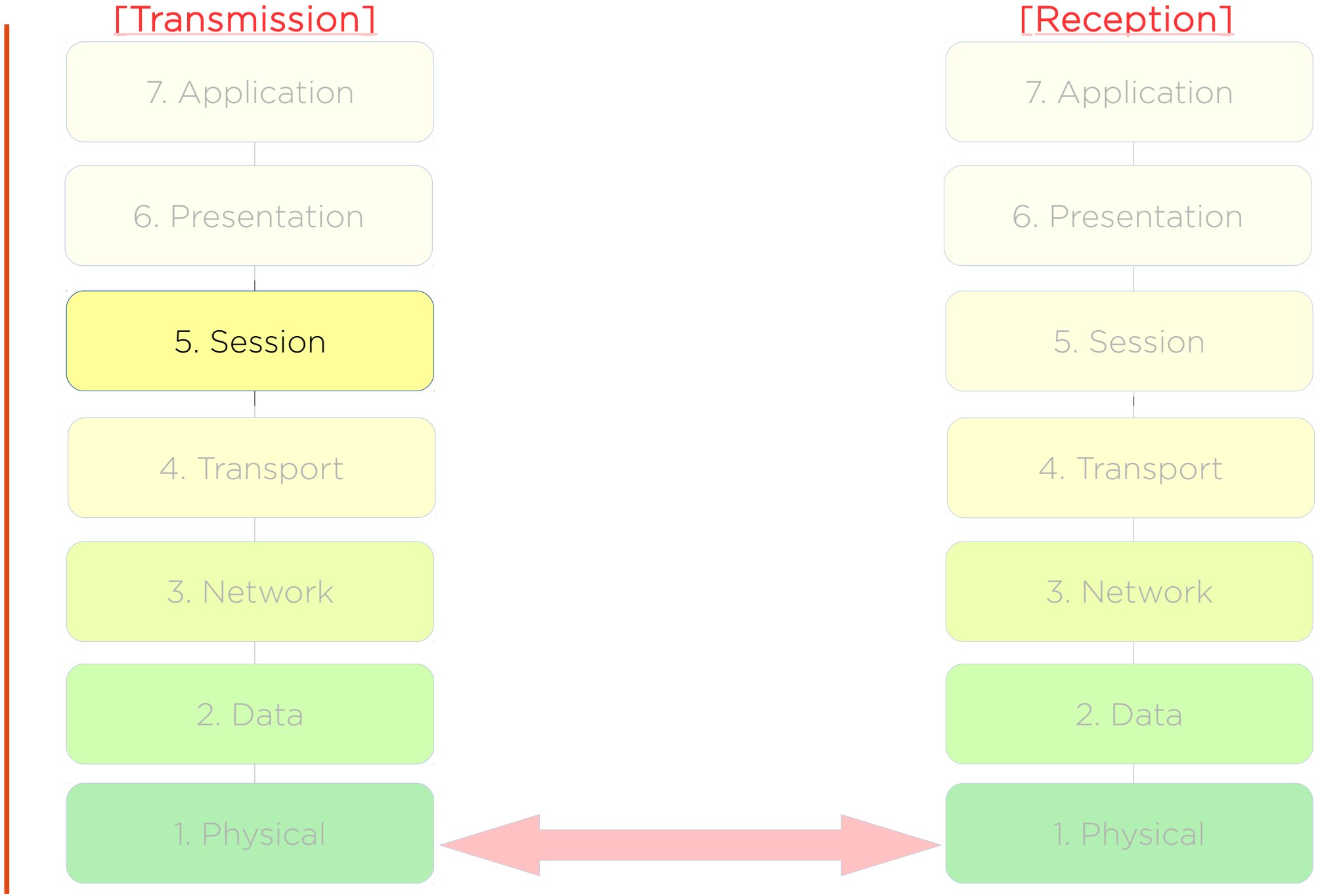
The OSI Model



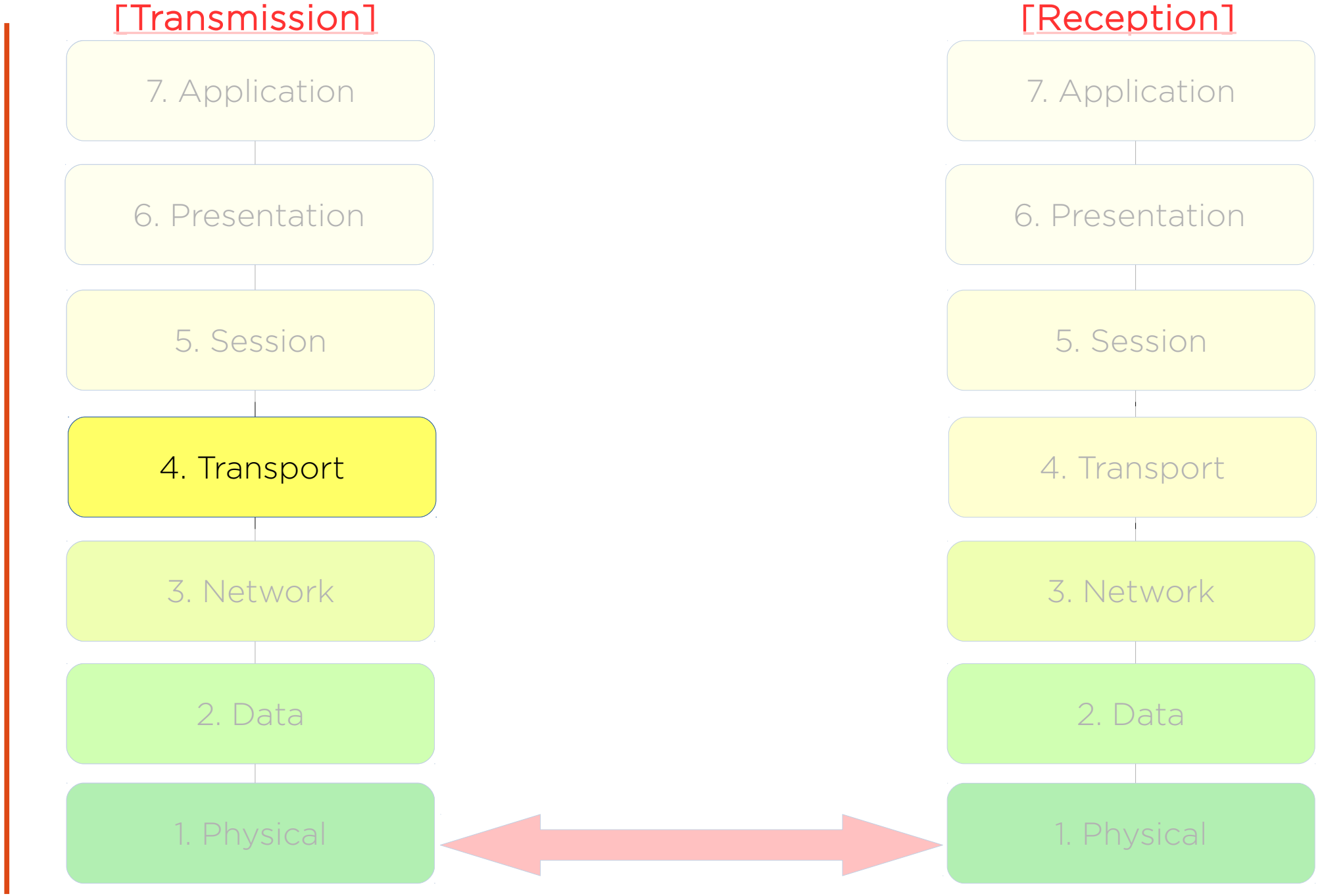
The OSI Model

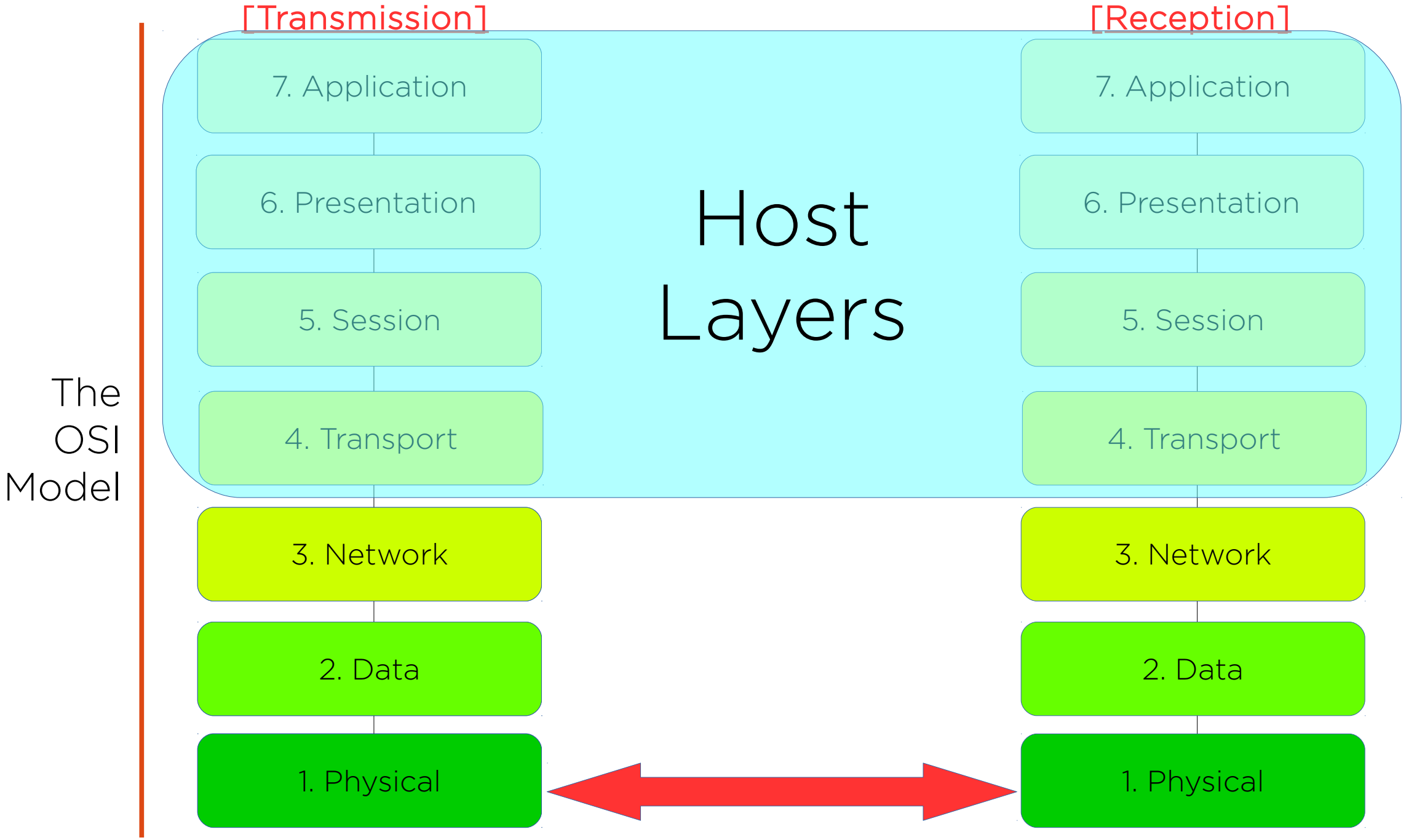


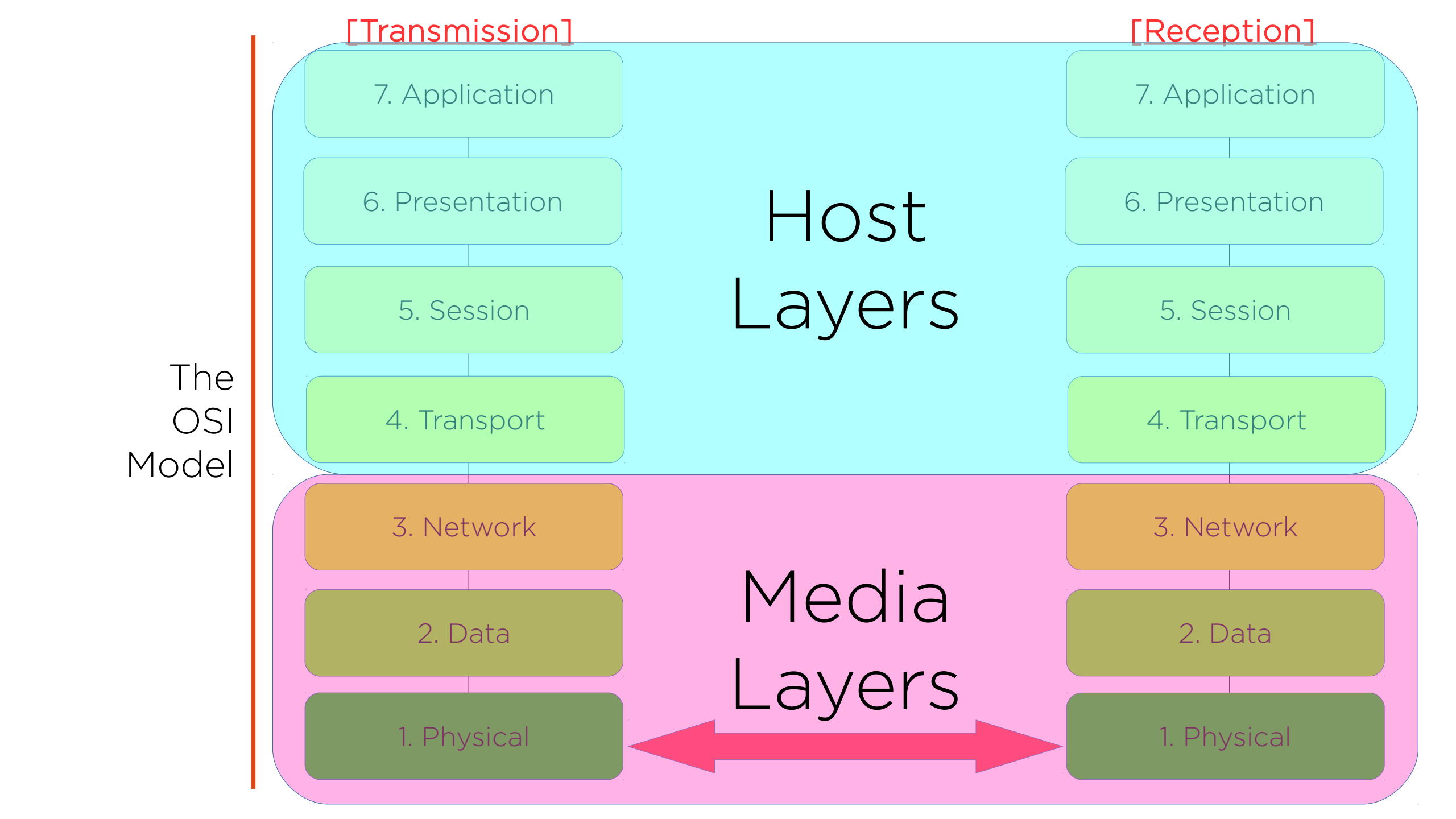
The OSI Model



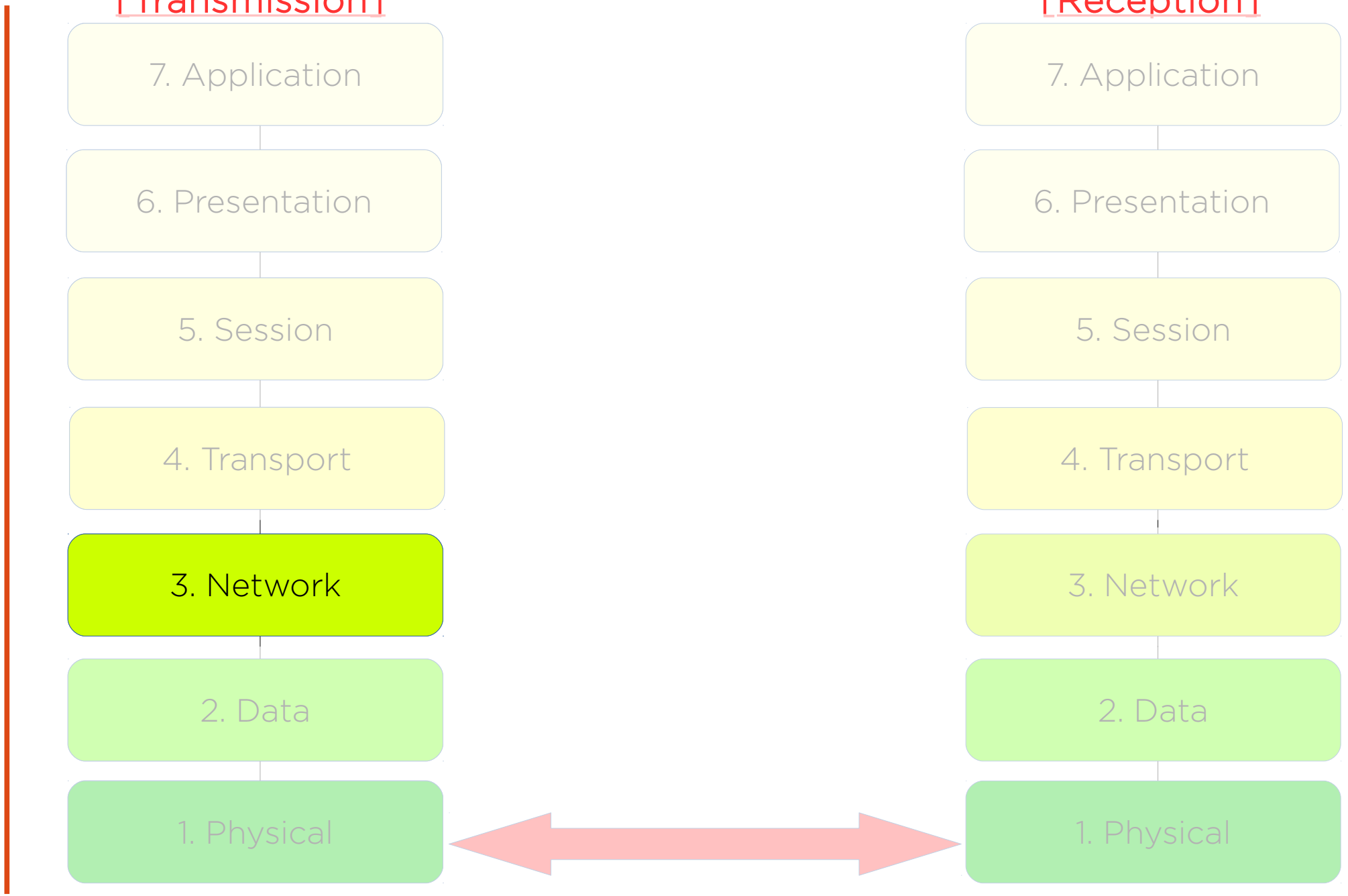
The OSI Model



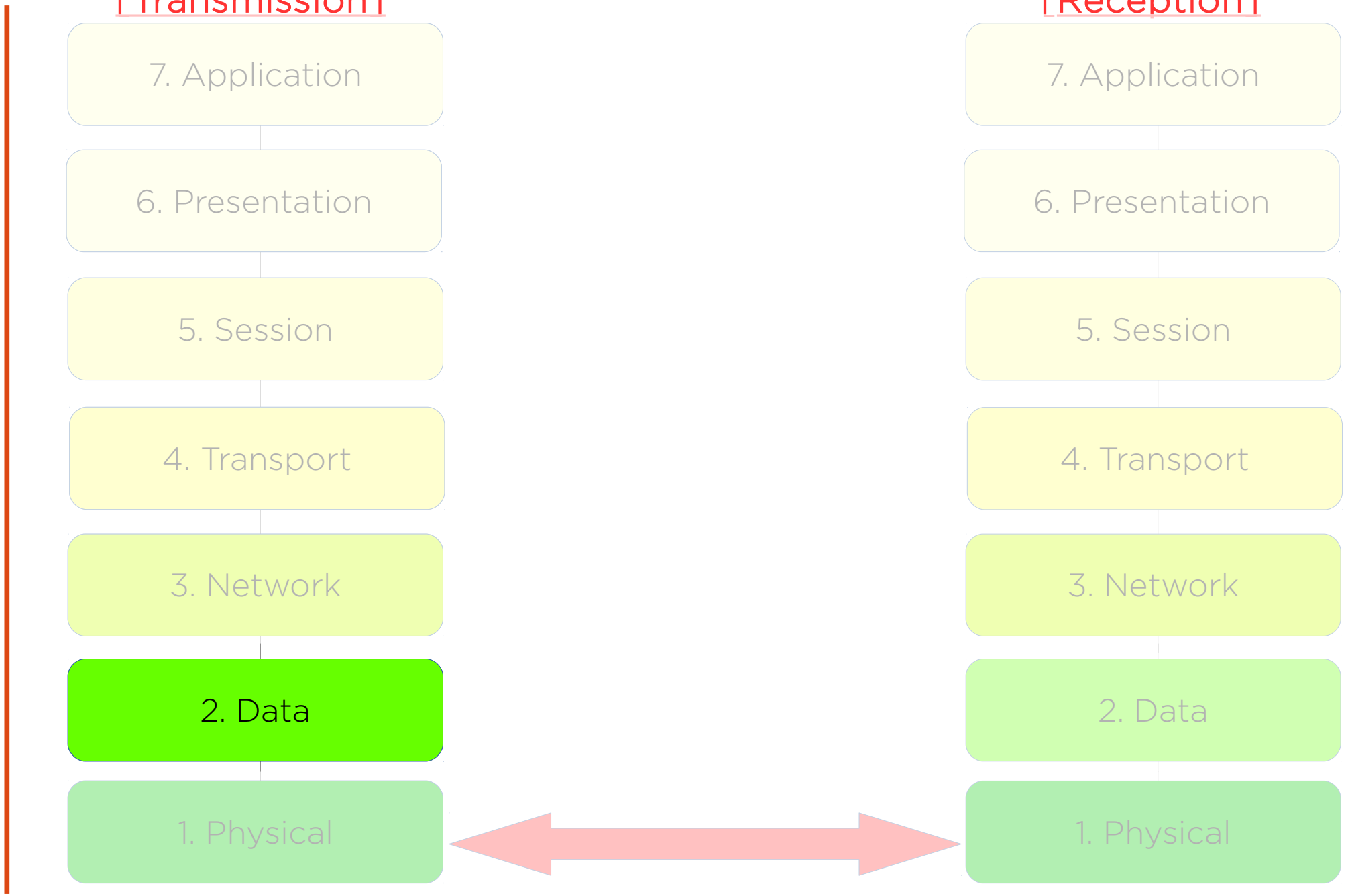

[Transmission]
[Reception]
The OSI Model
7. Application
6. Presentation
5. Session
4. Transport
Host Layers
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data
1. Physical
3. Network
2. Data
1. Physical


[Transmission]
[Reception]
The OSI Model
7. Application
6. Presentation
5. Session
4. Transport
Host Layers
7. Application
6. Presentation
5. Session
4. Transport
3. Network
2. Data
1. Physical
Media Layers
3. Network
2. Data
1. Physical

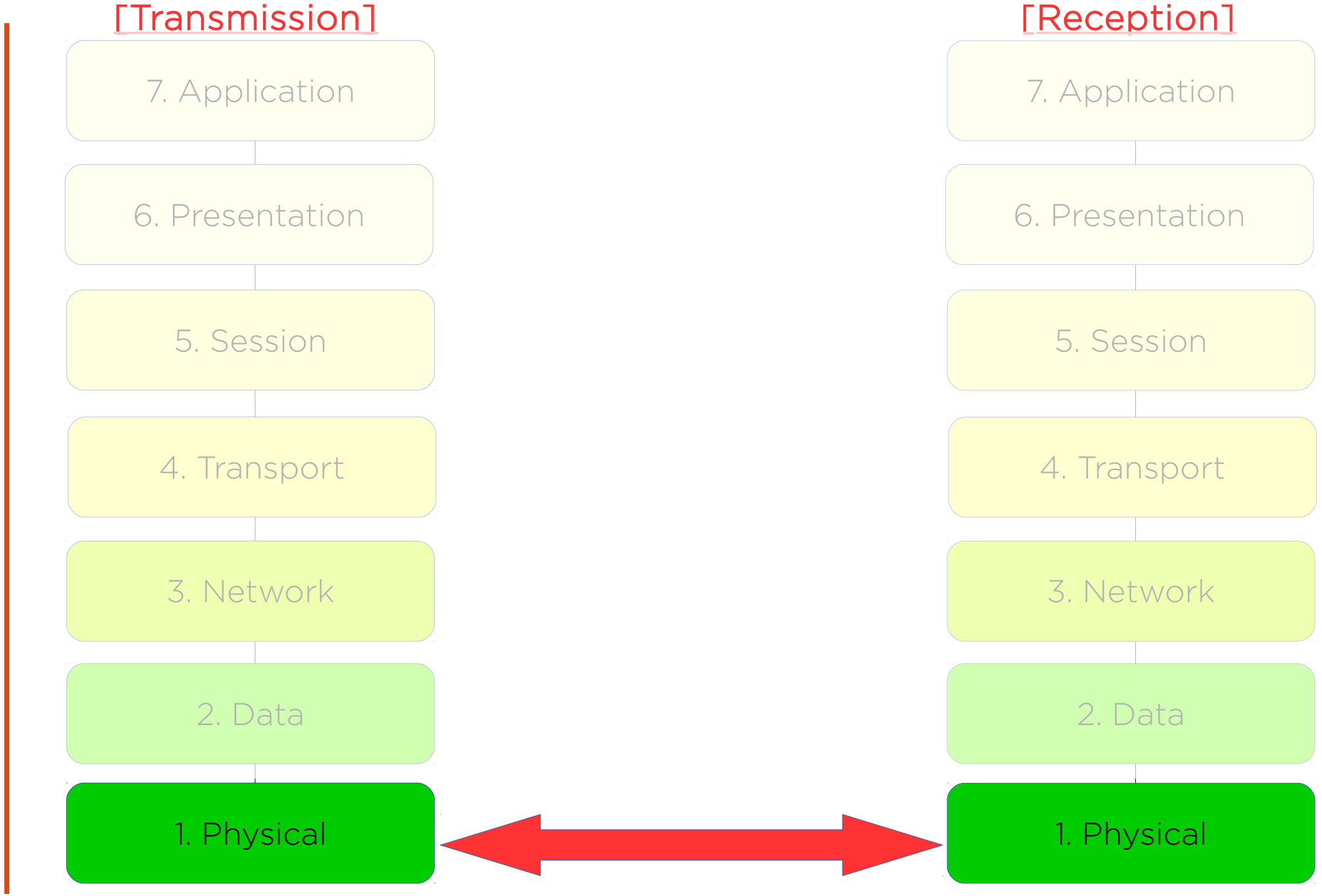
The OSI Model



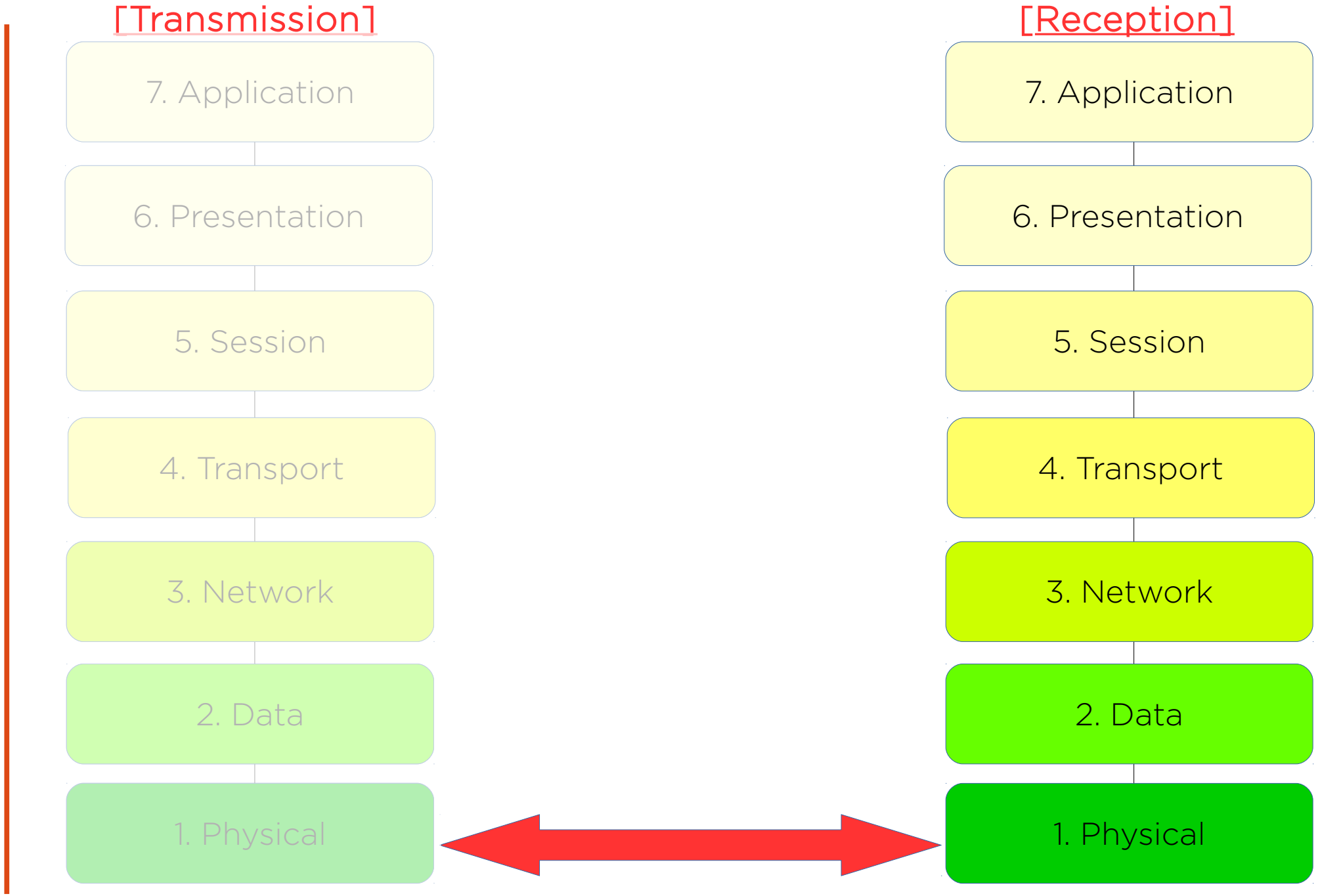
The OSI Model



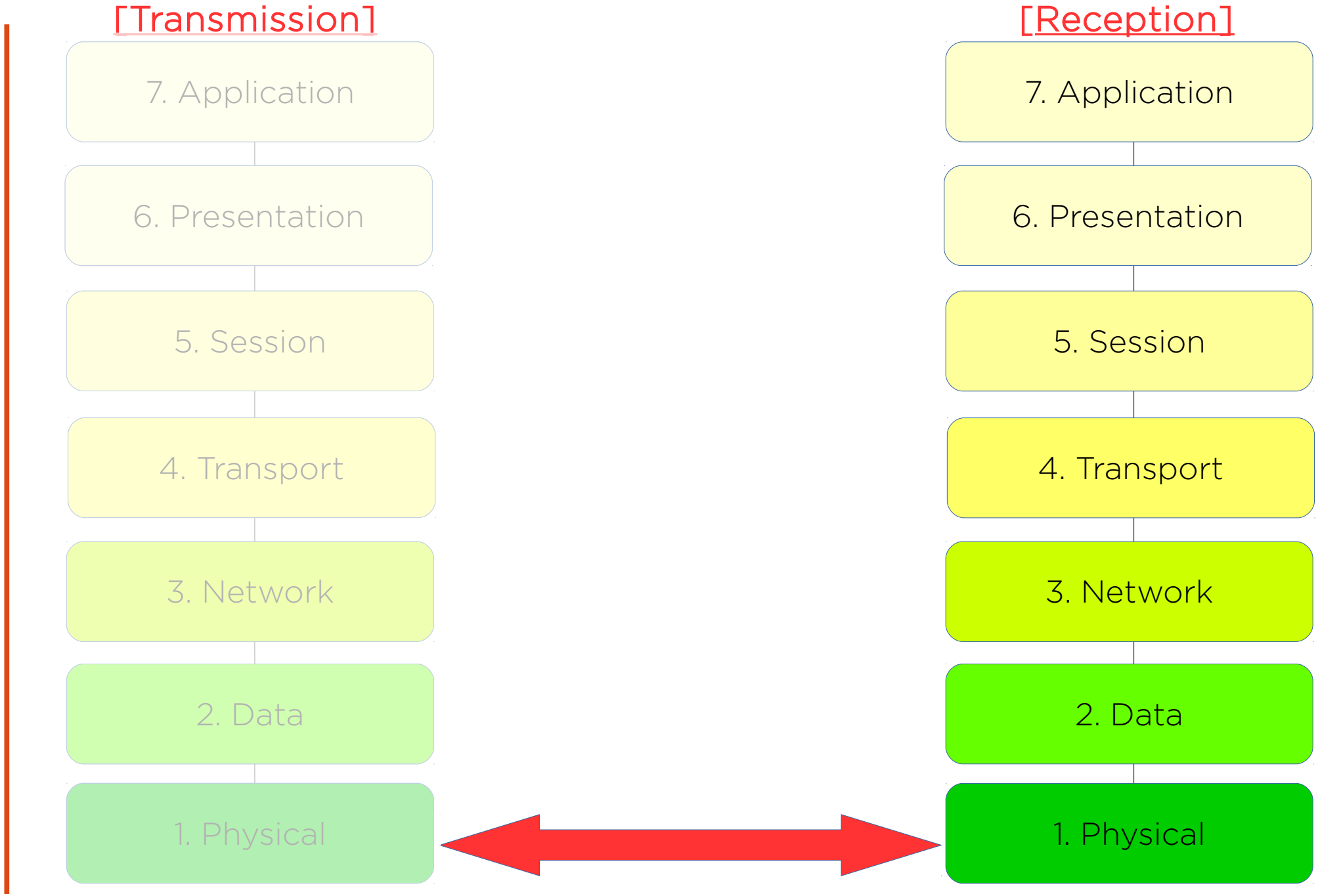
The OSI Model



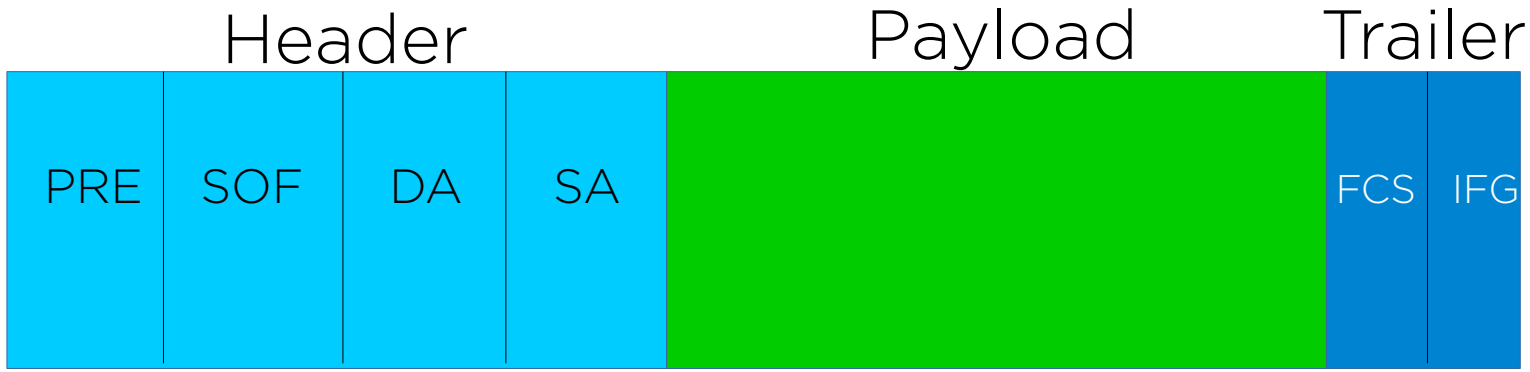
The OSI Model



The OSI Model



Ethernet IEEE 802.3 Data Frame Structure



Header
- Preamble (PRE)
- Start of Frame Delimiter (SOF)
- Destination Address (DA)
- Source Address (SA)
- Type

Payload

Trailer
- Frame Check Sequence (FCS)
- Interframe Gap (IFG)

SSH: The Secure Shell

SSH Session Types

1. RSA rhost authentication
2. Private/public keypair authentication
3. Password authentication

SSH Session Types

1. RSA rhost authentication

   /etc/hosts.equiv

   /etc/ssh/shosts.equiv

2. Private/public keypair authentication
3. Password authentication

SSH Session Types

1. RSA rhost authentication
   - /etc/hosts.equiv
   - /etc/ssh/shosts.equiv
   - /home/username/.rhosts
   - /home/username/.shosts
2. Private/public keypair authentication
3. Password authentication

SSH Session Types

1. RSA rhost authentication
   - /etc/hosts.equiv
   - /etc/ssh/shosts.equiv
   - /home/username/.rhosts
   - /home/username/.shosts
2. Private/public keypair authentication
3. Password authentication

SSH Session Types

1. RSA rhost authentication
   - /etc/hosts.equiv
   - /etc/ssh/shosts.equiv
   - /home/username/.rhosts
   - /home/username/.shosts
2. Private/public keypair authentication
3. Password authentication

SSH Session Types

1. RSA rhost authentication
   - /etc/hosts.equiv
   - /etc/ssh/shosts.equiv
   - /home/username/.rhosts
   - /home/username/.shosts
2. Private/public keypair authentication
3. Password authentication

   algorithms: RSA, DSA, OpenPGP

SSH Files (Linux)

SSH user keys location:

/home/username/.ssh/

SSH system keys location:

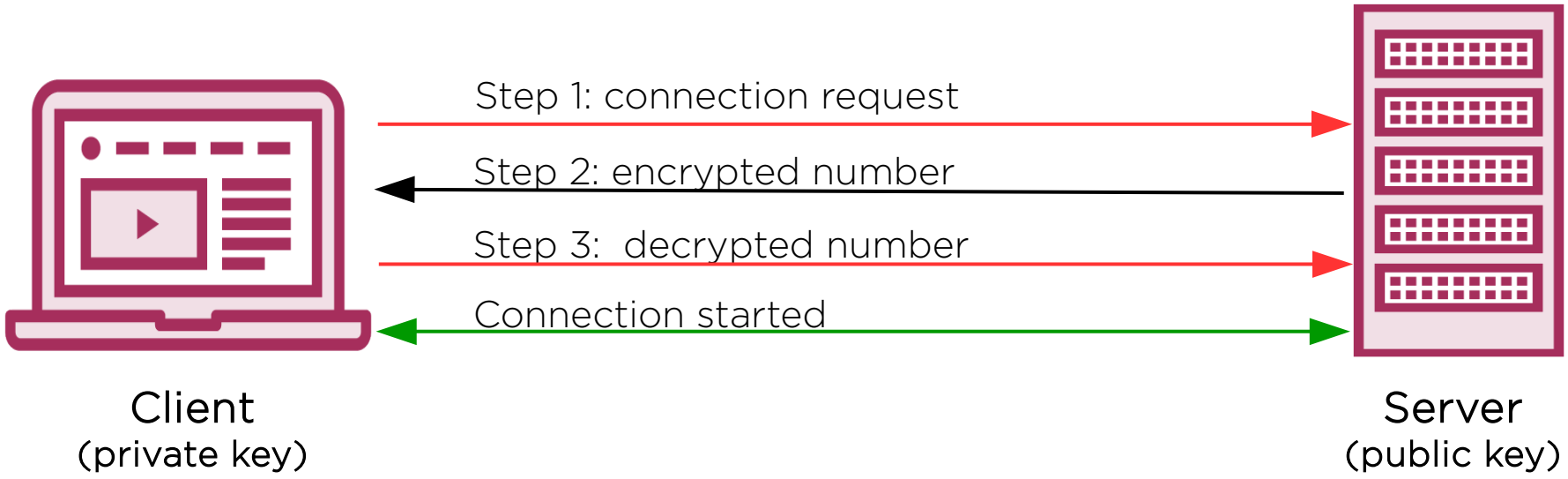
/etc/ssh/

SSH configuration files:

/etc/ssh/ssh_config (Control client behavior)

/etc/ssh/sshd_config (Control server behavior)

SSH Key Exchange

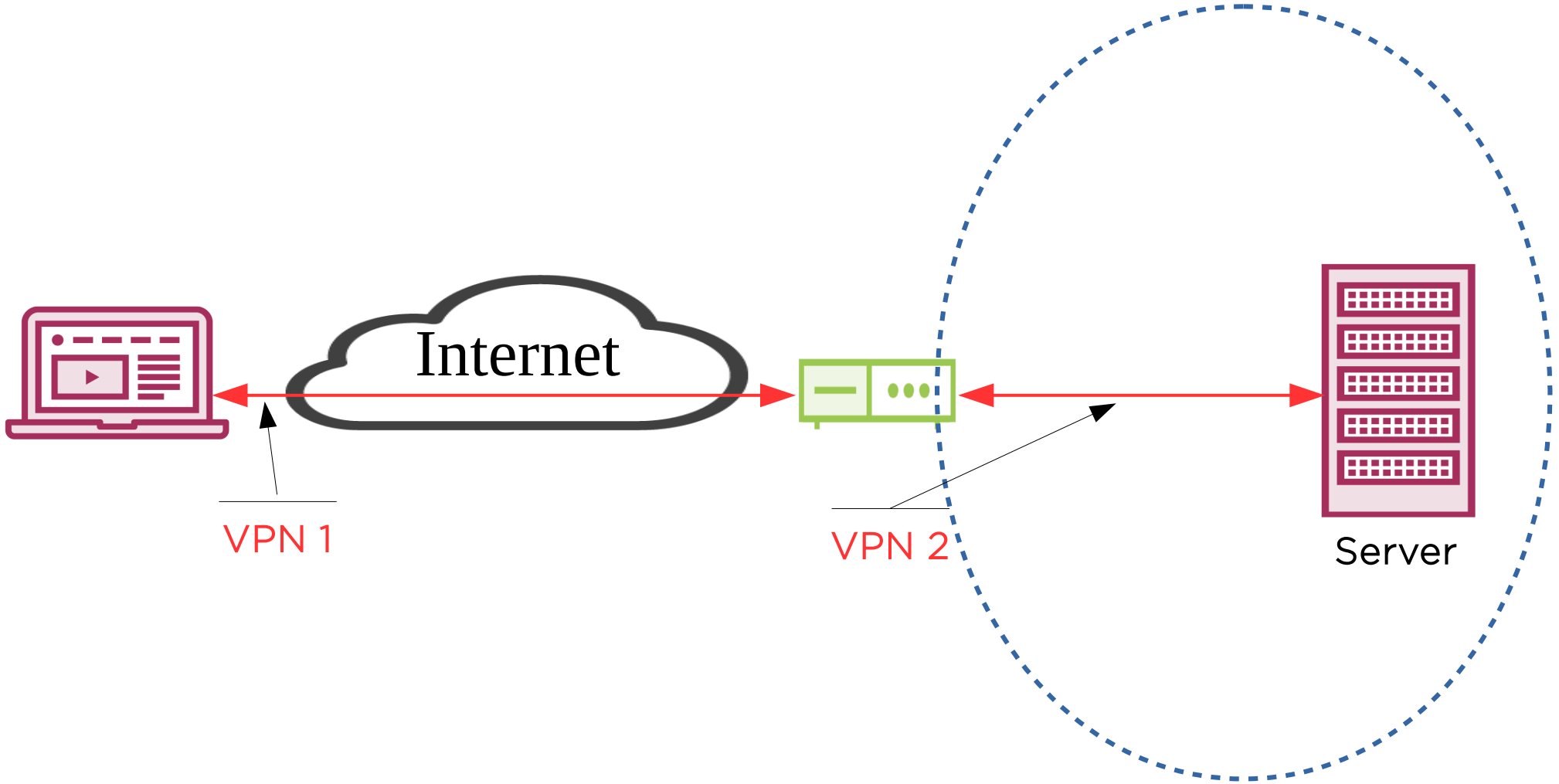


SSH: Debugging Tools

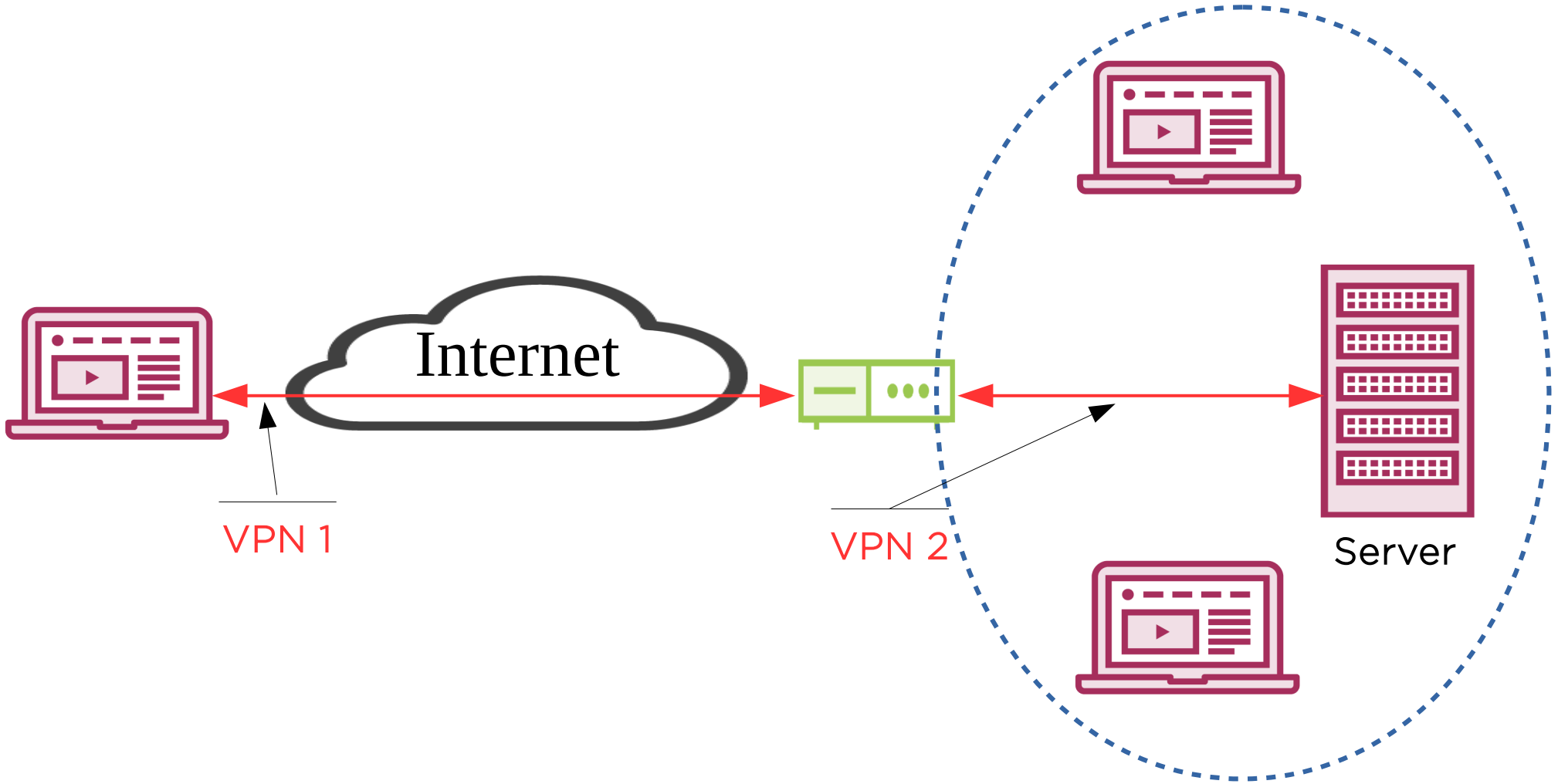
Troubleshooting: Usage Errors

Troubleshooting: Scenarios

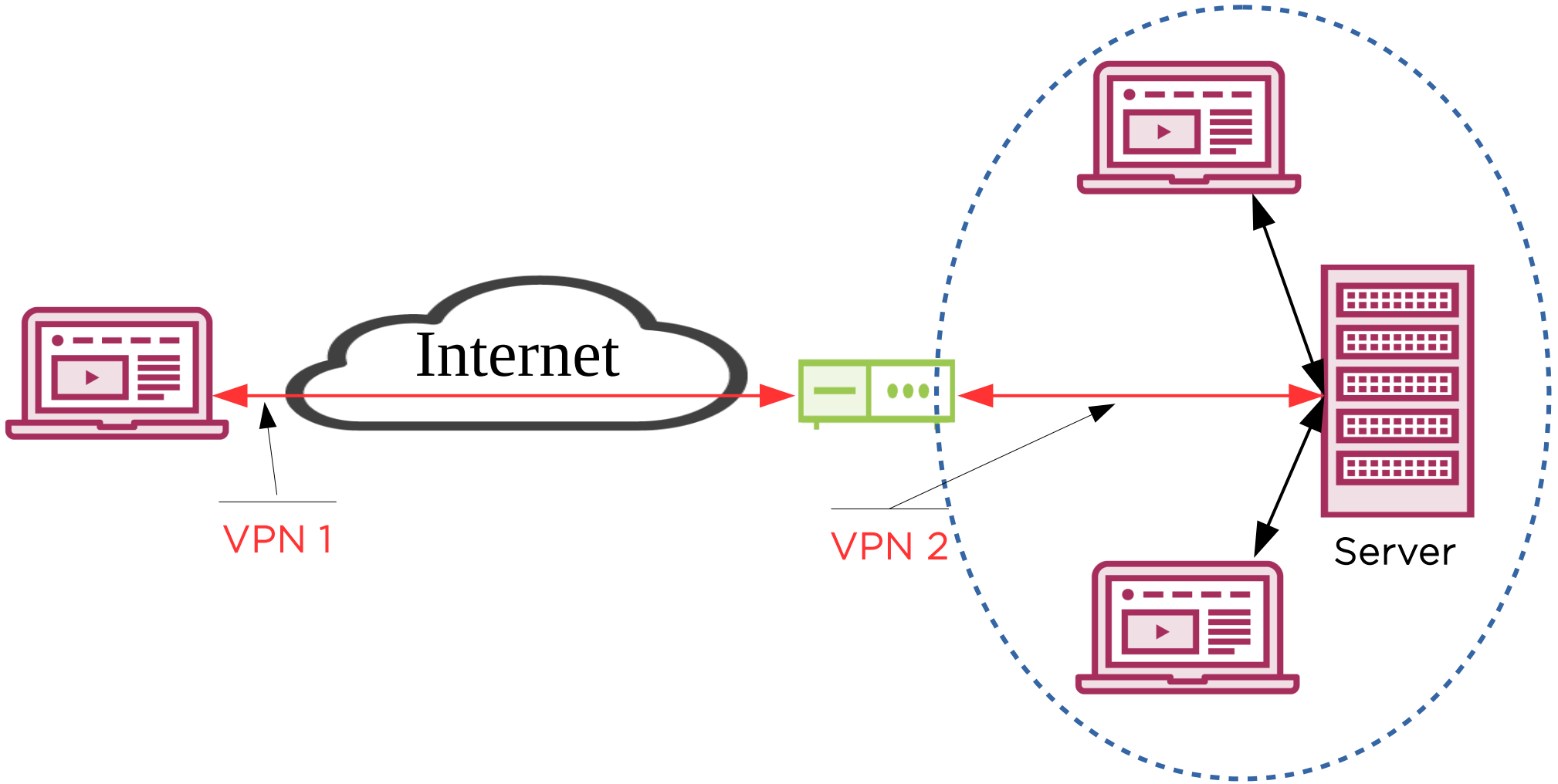
Multiple VPNs



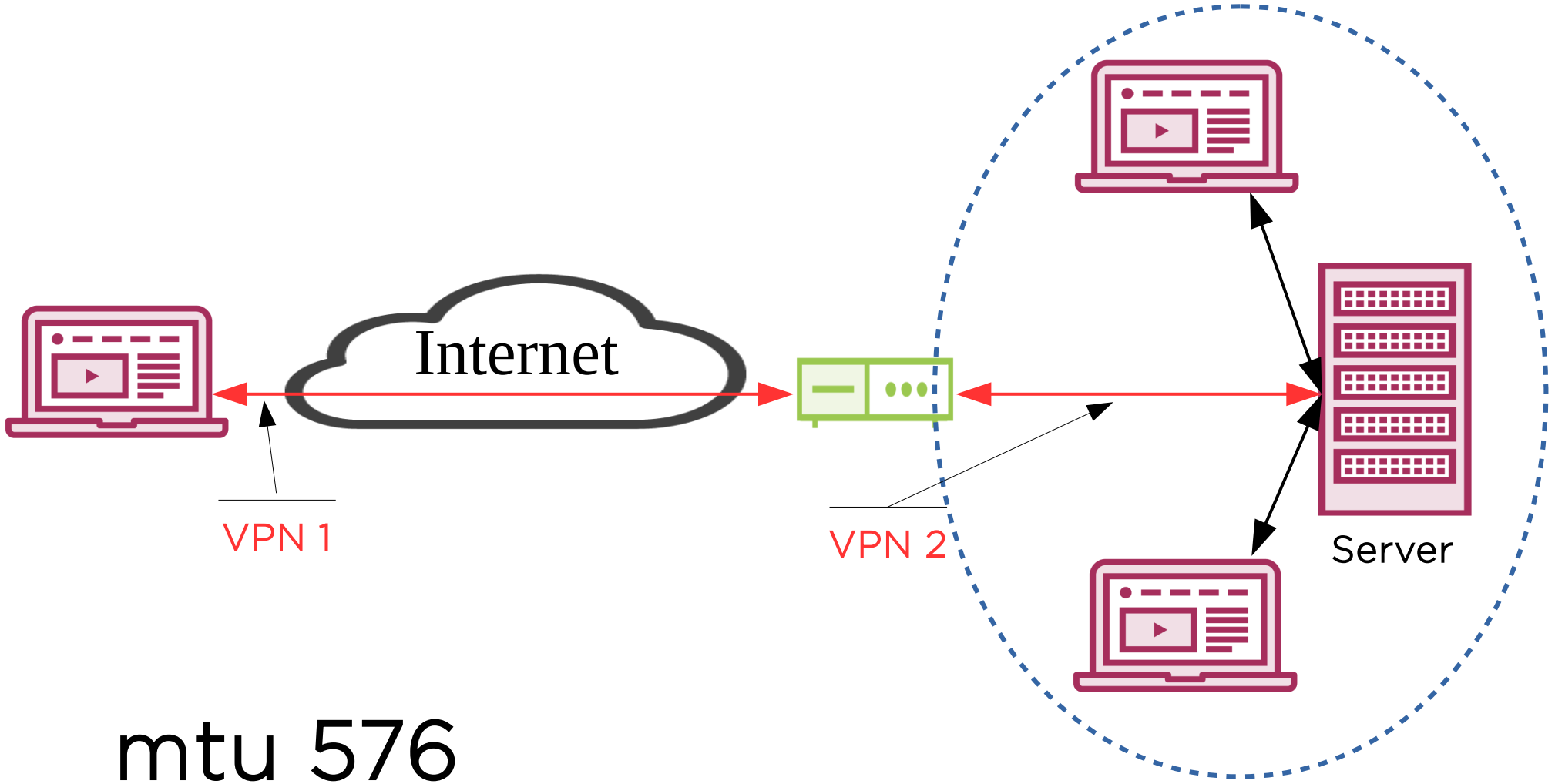
Multiple VPNs



Multiple VPNs



Multiple VPNs



mtu 576

Review

OSI Session Layer (5)

SSH authentication: RSA rhost

SSH authentication: public/private keypair

SSH authentication: password

ssh-add ~/.ssh/id_rsa

/home/username/.ssh/known_hosts

/etc/ssh/sshd_conf

/etc/ssh/ssh_conf

Wireshark | Follow TCP Stream

Review

OSI Session Layer (5)

SSH authentication: RSA rhost

SSH authentication: public/private keypair

SSH authentication: password

ssh-add ~/.ssh/id_rsa

/home/username/.ssh/known_hosts

/etc/ssh/sshd_conf

/etc/ssh/ssh_conf

Wireshark | Follow TCP Stream

Review

OSI Session Layer (5)

SSH authentication: RSA rhost

SSH authentication: public/private keypair

SSH authentication: password

ssh-add ~/.ssh/id_rsa

/home/username/.ssh/known_hosts

/etc/ssh/sshd_conf

/etc/ssh/ssh_conf

Wireshark | Follow TCP Stream

Review

OSI Session Layer (5)

SSH authentication: RSA rhost

SSH authentication: public/private keypair

SSH authentication: password

ssh-add ~/.ssh/id_rsa

/home/username/.ssh/known_hosts

/etc/ssh/sshd_conf

/etc/ssh/ssh_conf

Wireshark | Follow TCP Stream

Review

OSI Session Layer (5)

SSH authentication: RSA rhost

SSH authentication: public/private keypair

SSH authentication: password

ssh-add ~/.ssh/id_rsa

/home/username/.ssh/known_hosts

/etc/ssh/sshd_conf

/etc/ssh/ssh_conf

Wireshark | Follow TCP Stream

Review

OSI Session Layer (5)

SSH authentication: RSA rhost

SSH authentication: public/private keypair

SSH authentication: password

ssh-add ~/.ssh/id_rsa

/home/username/.ssh/known_hosts

/etc/ssh/sshd_conf

/etc/ssh/ssh_conf

Wireshark | Follow TCP Stream

Review

OSI Session Layer (5)

SSH authentication: RSA rhost

SSH authentication: public/private keypair

SSH authentication: password

ssh-add ~/.ssh/id_rsa

/home/username/.ssh/known_hosts

/etc/ssh/sshd_conf

/etc/ssh/ssh_conf

Wireshark | Follow TCP Stream

Review

OSI Session Layer (5)

SSH authentication: RSA rhost

SSH authentication: public/private keypair

SSH authentication: password

ssh-add ~/.ssh/id_rsa

/home/username/.ssh/known_hosts

/etc/ssh/sshd_conf

/etc/ssh/ssh_conf

Wireshark | Follow TCP Stream

Review

OSI Session Layer (5)

SSH authentication: RSA rhost

SSH authentication: public/private keypair

SSH authentication: password

ssh-add ~/.ssh/id_rsa

/home/username/.ssh/known_hosts

/etc/ssh/sshd_conf

/etc/ssh/ssh_conf

Wireshark | Follow TCP Stream

Review

journalctl | grep sshd

sudo /usr/sbin/sshd -d -p 2020

systemctl status sshd

ping 192.1.68.0.100

sudo tcpdump -n -i enp0s3 tcp port 22 and host 192.168.0.100

TCPKeepAlive yes

chmod 600 id_rsa

mtu 576

Review

journalctl | grep sshd

sudo /usr/sbin/sshd -d -p 2020

systemctl status sshd

ping 192.1.68.0.100

sudo tcpdump -n -i enp0s3 tcp port 22 and host 192.168.0.100

TCPKeepAlive yes

chmod 600 id_rsa

mtu 576

Review

journalctl | grep sshd

sudo /usr/sbin/sshd -d -p 2020

systemctl status sshd

ping 192.1.68.0.100

sudo tcpdump -n -i enp0s3 tcp port 22 and host 192.168.0.100

TCPKeepAlive yes

chmod 600 id_rsa

mtu 576

Review

journalctl | grep sshd

sudo /usr/sbin/sshd -d -p 2020

systemctl status sshd

ping 192.1.68.0.100

sudo tcpdump -n -i enp0s3 tcp port 22 and host 192.168.0.100

TCPKeepAlive yes

chmod 600 id_rsa

mtu 576

Review

journalctl | grep sshd

sudo /usr/sbin/sshd -d -p 2020

systemctl status sshd

ping 192.1.68.0.100

sudo tcpdump -n -i enp0s3 tcp port 22 and host 192.168.0.100

TCPKeepAlive yes

chmod 600 id_rsa

mtu 576

Review

journalctl | grep sshd

sudo /usr/sbin/sshd -d -p 2020

systemctl status sshd

ping 192.1.68.0.100

sudo tcpdump -n -i enp0s3 tcp port 22 and host 192.168.0.100

TCPKeepAlive yes

chmod 600 id_rsa

mtu 576

Review

journalctl | grep sshd

sudo /usr/sbin/sshd -d -p 2020

systemctl status sshd

ping 192.1.68.0.100

sudo tcpdump -n -i enp0s3 tcp port 22 and host 192.168.0.100

TCPKeepAlive yes

chmod 600 id_rsa

mtu 576

Review

journalctl | grep sshd

sudo /usr/sbin/sshd -d -p 2020

systemctl status sshd

ping 192.1.68.0.100

sudo tcpdump -n -i enp0s3 tcp port 22 and host 192.168.0.100

TCPKeepAlive yes

chmod 600 id_rsa

mtu 576