75.43 Introducción a los Sistemas Distribuidos
75.60 Redes y Aplicaciones Distribuidas
TA048 Redes

Tema: Capa de Red (IV)

Capítulo 5: desde el apartado *5.4 Routing Among the ISPs: BGP* hasta el final del mismo, del libro *Computer Networking : A Top-Down Approach. James Kurose and Keith Ross. Publisher: Pearson Edition: 8th, 2021.*
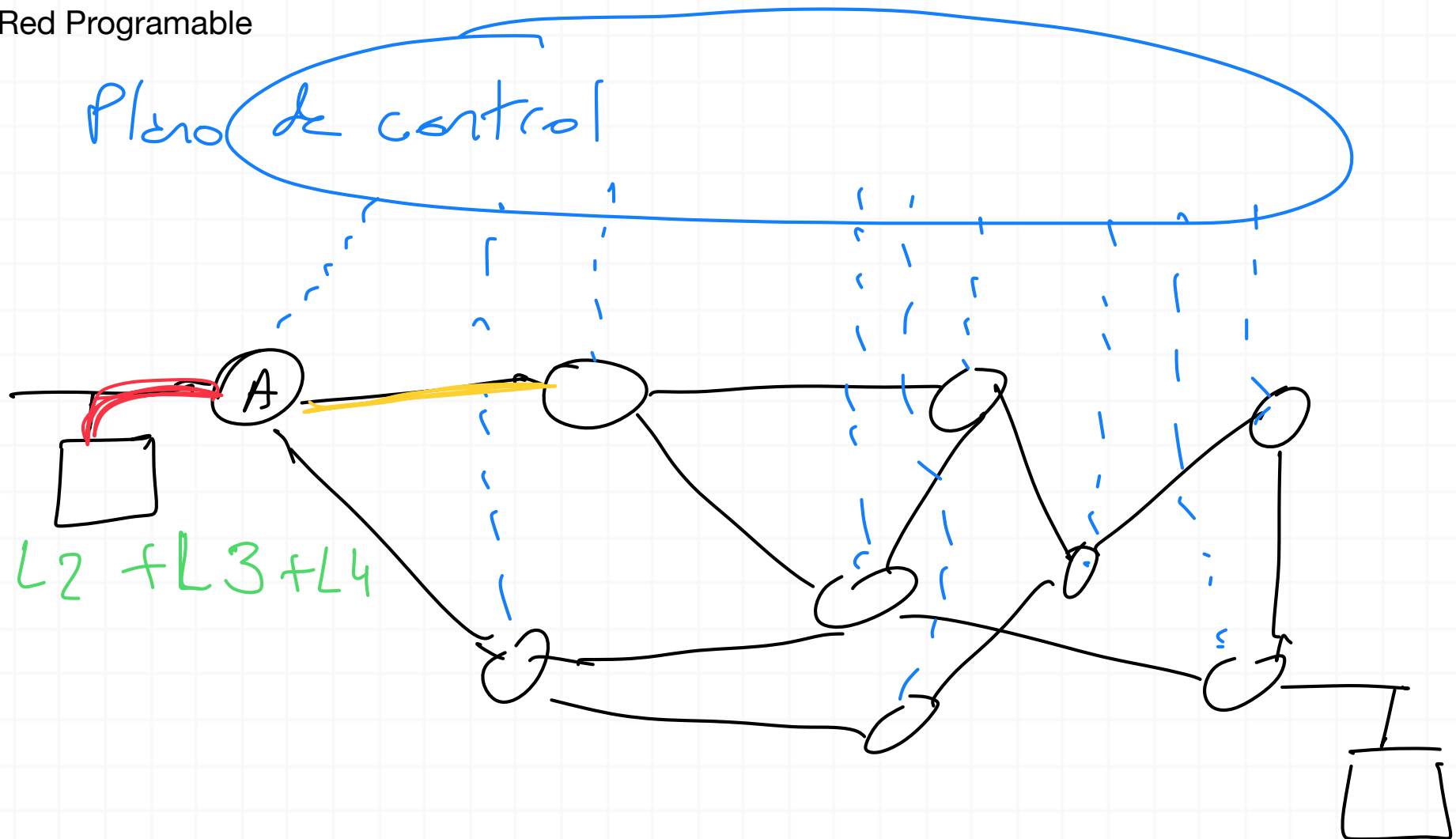
Dr. Ing. J. Ignacio Alvarez-Hamelin

Clase de hoy

- *SDN Control Plane*

- BGP (*Border Gateway Protocol*)

- ICMP (*Internet Control Message Protocol*)

SDN (*Software Defined Networks*), Plano de Control

- Reenvío basado en flujos

- Separación del plano de datos y de control

- Control de Red: externo a los conmutadores

- Red Programable

NAT Routing Access Firewall
               Control
                                    Norte
- - - - - - - - - - - - - - - -

┌─────────────────────────────┐
│ App. SDN   │
└─────────────────────────────┘

┌─────────────────────────────┐
│ SDN   │
│ Controlador   │
└─────────────────────────────┘

┌─────────────────────────────┐
│ Comunicación   │
└─────────────────────────────┘

- - - - - - - - - - - - - - -
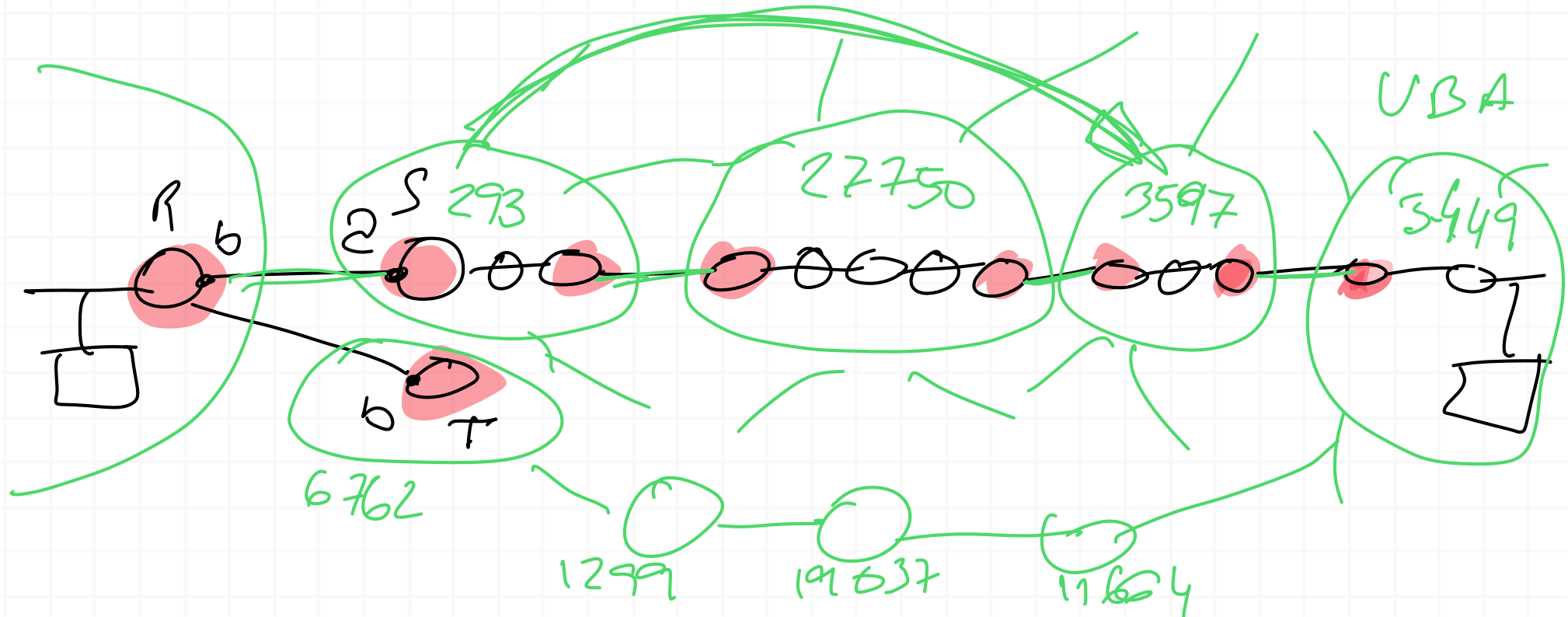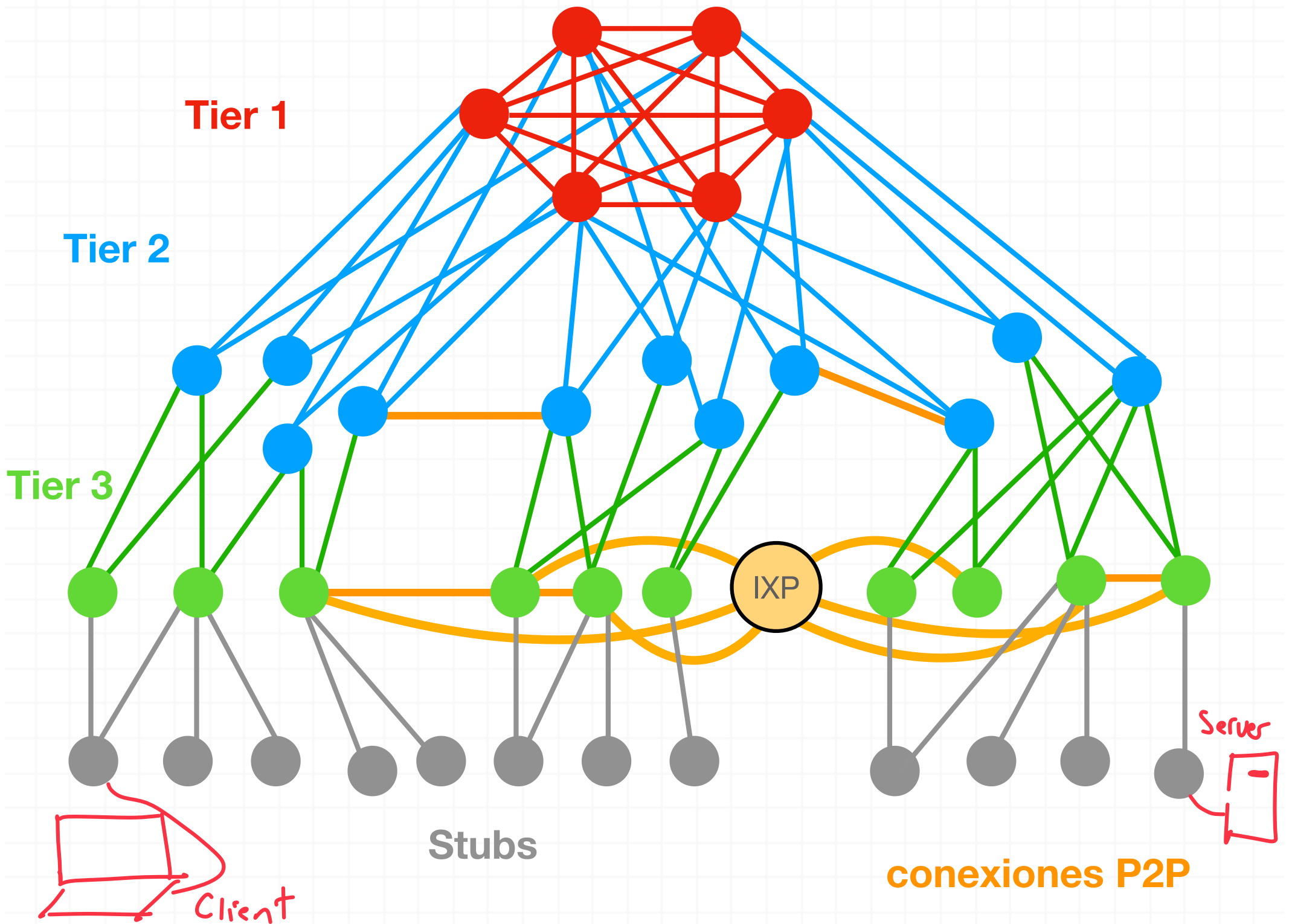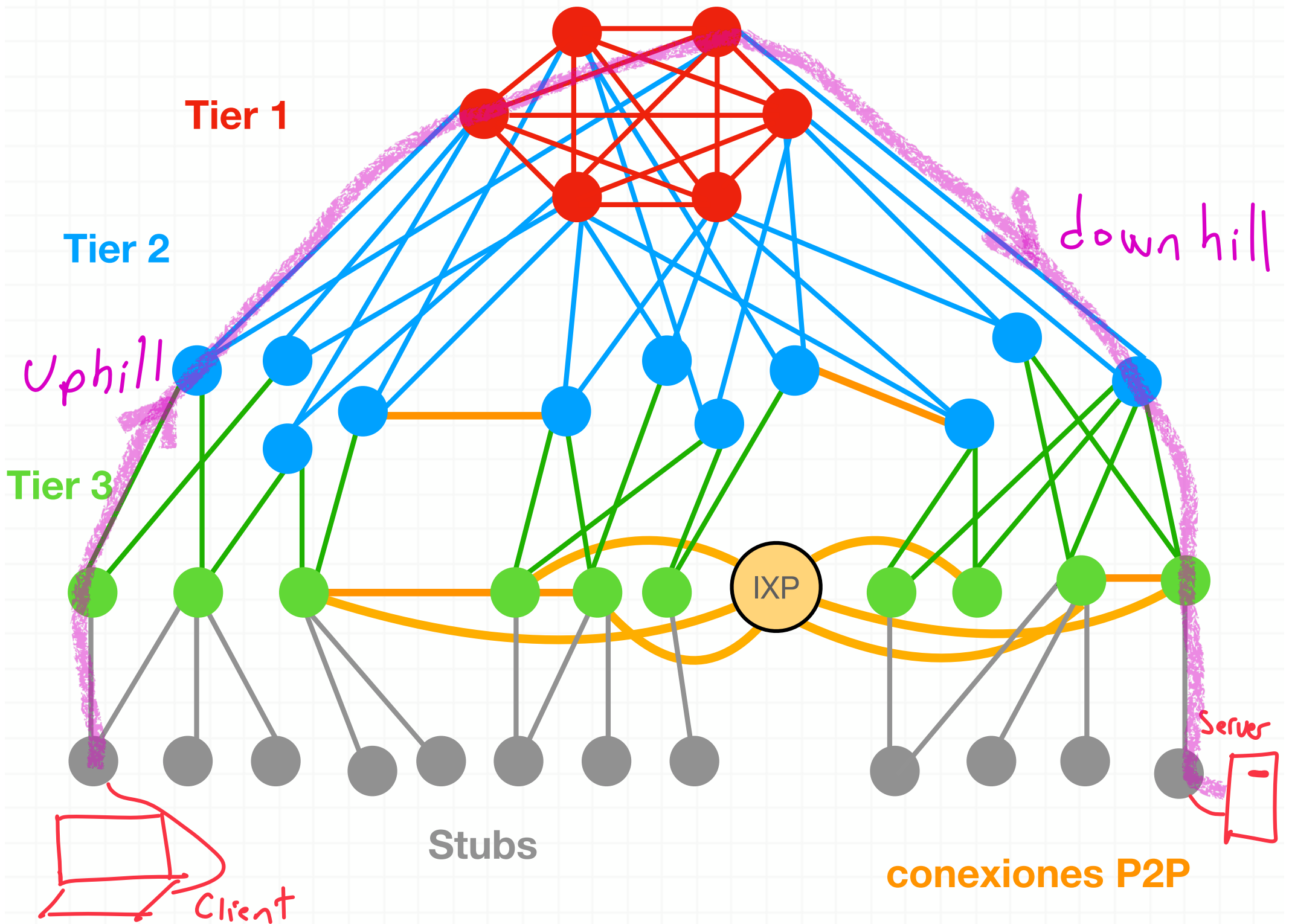   Sur

BGP (Border Gateway Protocol)

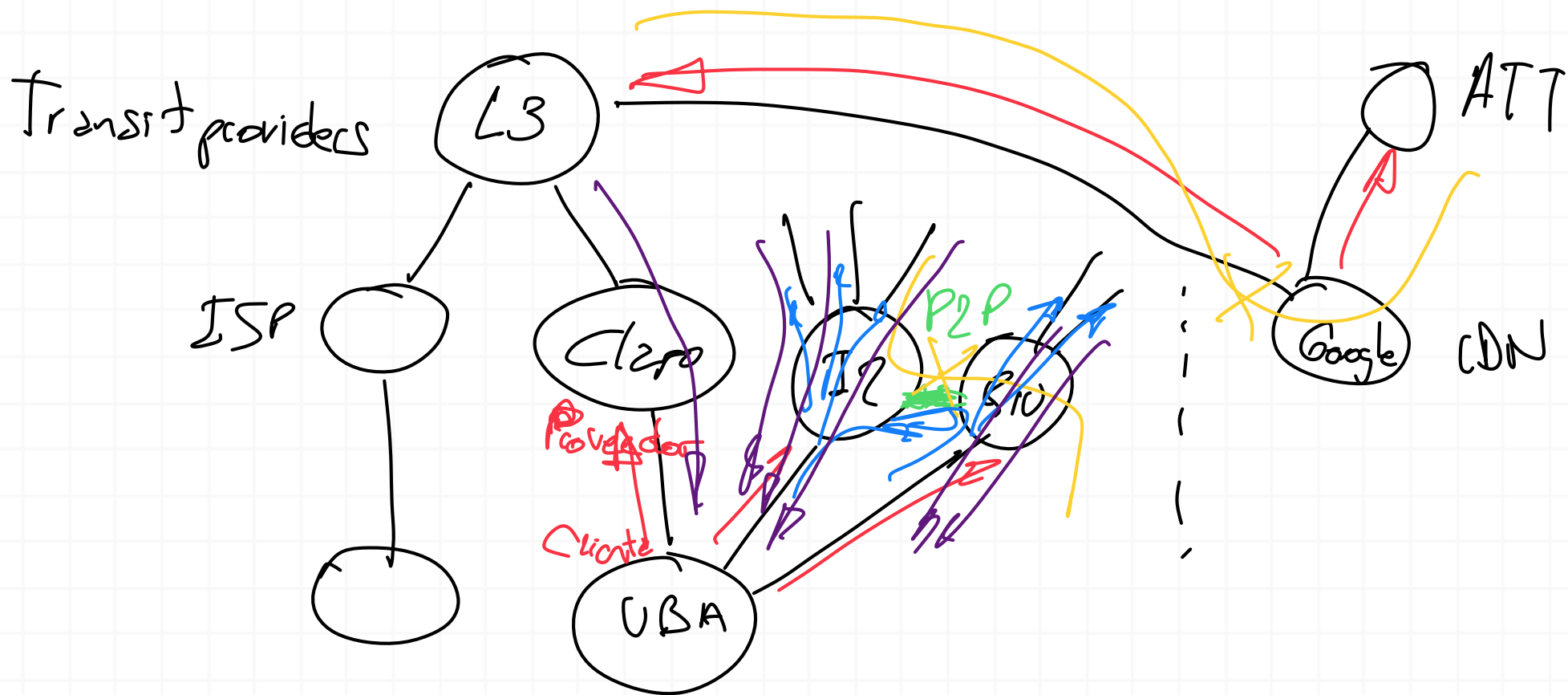- **Uso y aplicación**
- **Funcionamiento**
- **Implementación de Políticas**

Red Destino	Next hop	AS-path	L.P
✱ 157.92.0.0/16	S.a	293, 27750, 3597, 3449	
157.82.0.0/16	T.b	6762, 1299, 19037, 11664, 3449	

Tier 1

Tier 2

Tier 3

IXP

Stubs

Client

Server

conexiones P2P

Tier 1

Tier 2

down hill

Uphill

Tier 3

IXP

Stubs

Client

Server

conexiones P2P

Tier 1

Tier 2

Tier 3

IXP

Stubs

Client

Server

conexiones P2P

Transit providers

L3

ISP

Claro

Proveedor

Cliente
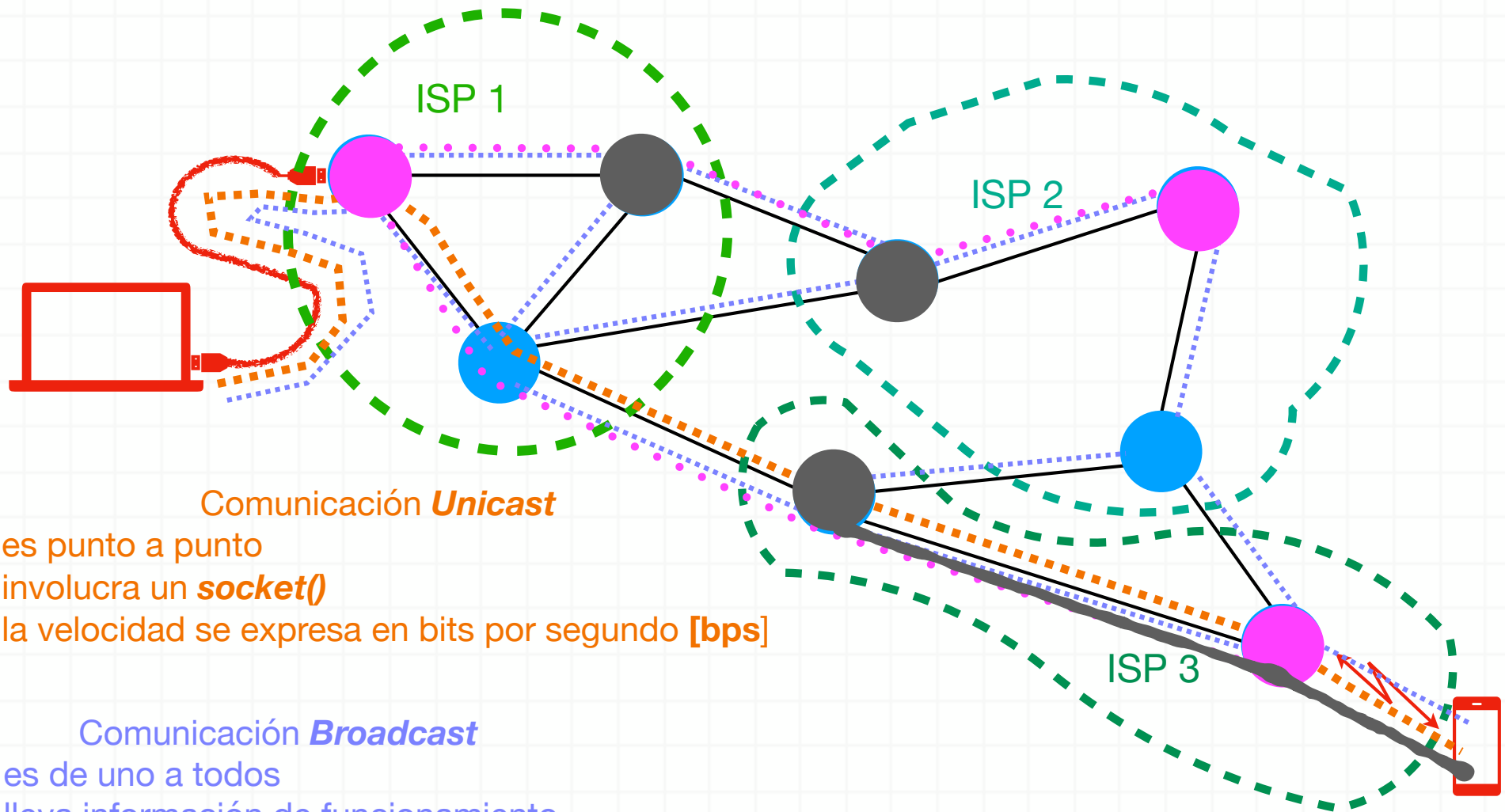
UBA

P2P

I2

G10

Google

ATT

CDN

ISP 1

ISP 2

ISP 3
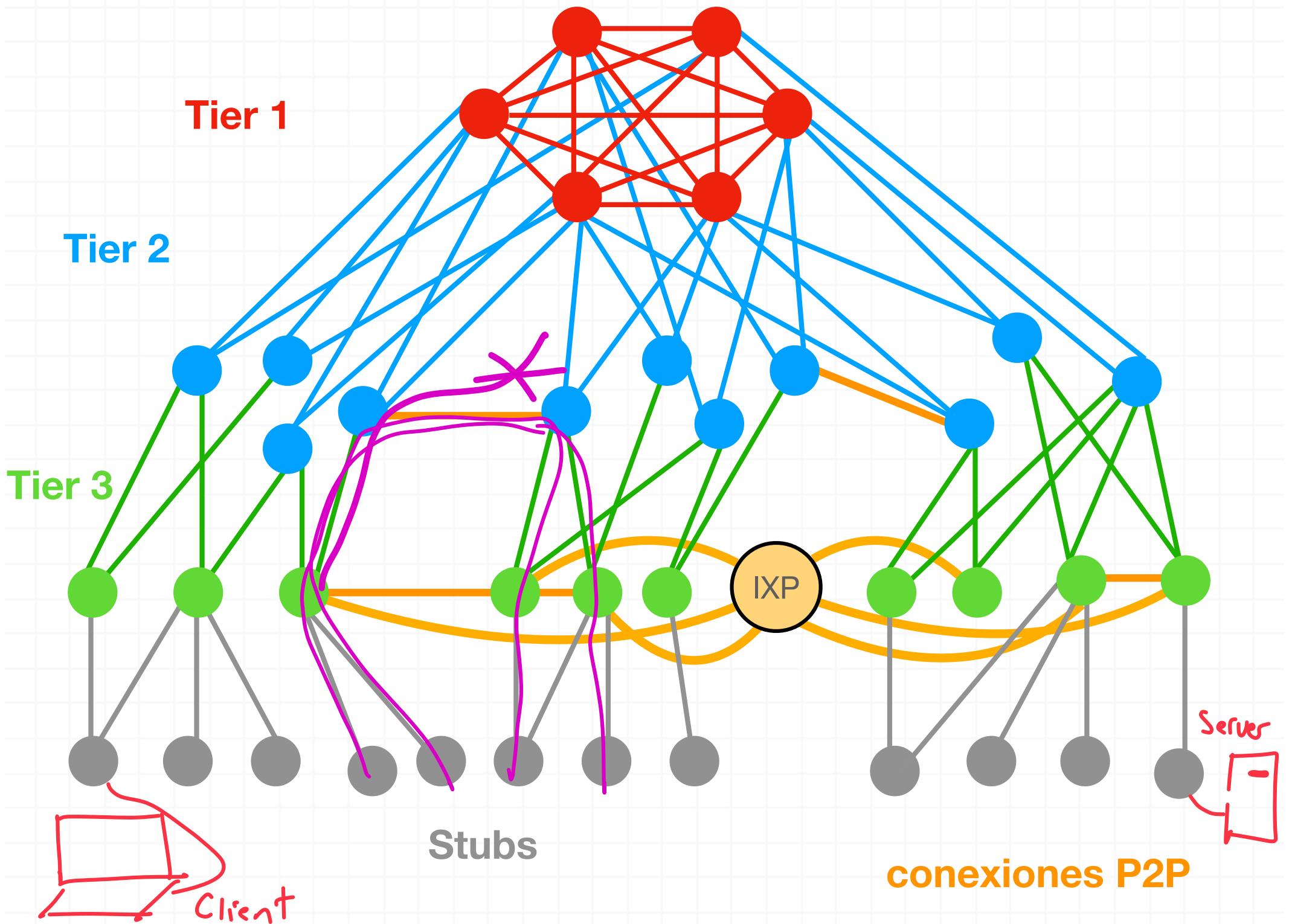
Comunicación *Unicast*
- es punto a punto
- involucra un *socket()*
- la velocidad se expresa en bits por segundo **[bps]**

Comunicación *Broadcast*
- es de uno a todos
- lleva información de funcionamiento

Comunicación *Multicast*
- es de uno a un grupo
- lleva información que sólo es necesaria para ese grupo

Comunicación *Anycast*
- es al más cercano
- lleva información que está replicada en la red

Mutually Agreed Norms for Routing Security

1. Filtering – Preventing propagation of incorrect routing information.
   - Network operator defines a clear routing policy and implements a system that ensures correctness of their own announcements and announcements from their customers to adjacent networks with prefix and AS-path granularity.
   - Network operator is able to communicate to their adjacent networks which announcements are correct.
   - Network operator applies due diligence when checking the correctness of their customer's announcements, specifically that the customer legitimately holds the ASN and the address space it announces.
2. Anti-Spoofing – Preventing traffic with spoofed source IP addresses.
   - Network operator implements a system that enables source address validation for at least single-homed stub customer networks, their own end-users and infrastructure. Network operator implements anti-spoofing filtering to prevent packets with an incorrect source IP address from entering and leaving the network.
3. Coordination – Facilitating global operational communication and coordination between network operators.
   - Network operator maintains globally accessible up-to-date contact information.
4. Global Validation – Facilitating validation of routing information on a global scale.
   - Network operator has publicly documented routing policy, ASNs and prefixes that are intended to be advertised to external parties.

ICMP

- Utilidad
- IPv4: **RFC 792**
- IPv6: **RFC 4443**

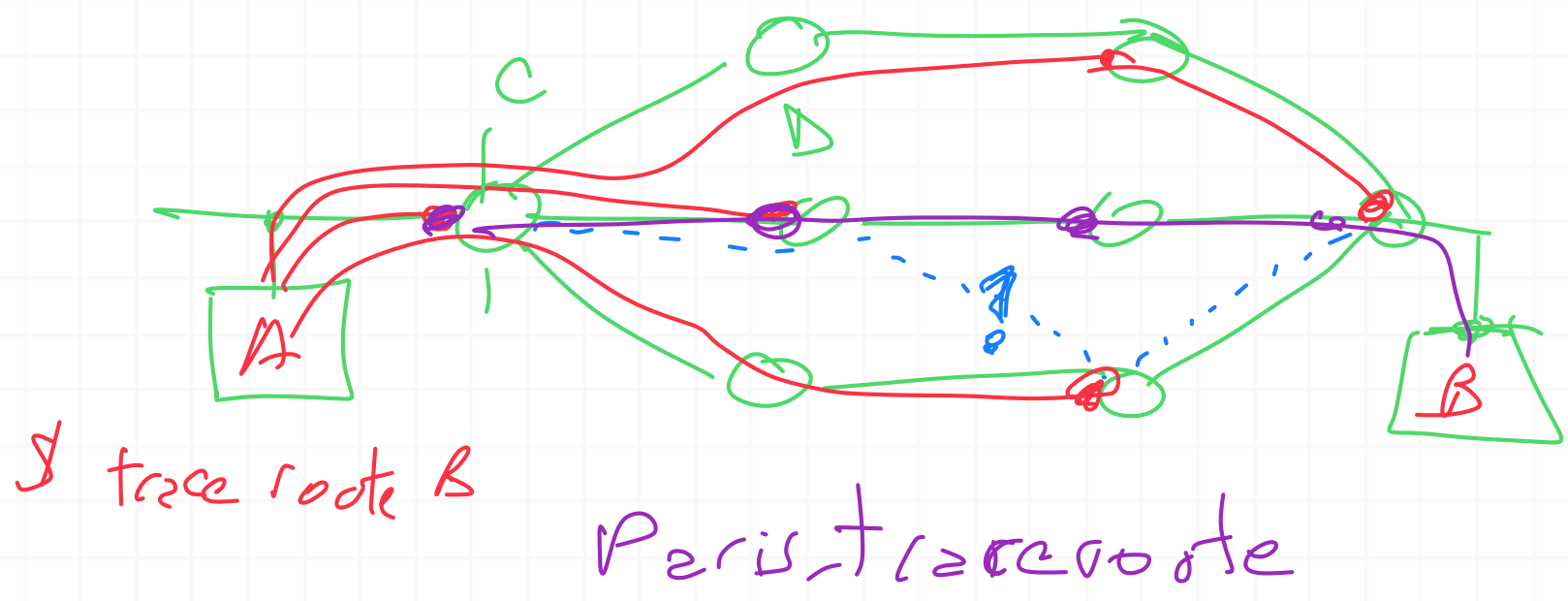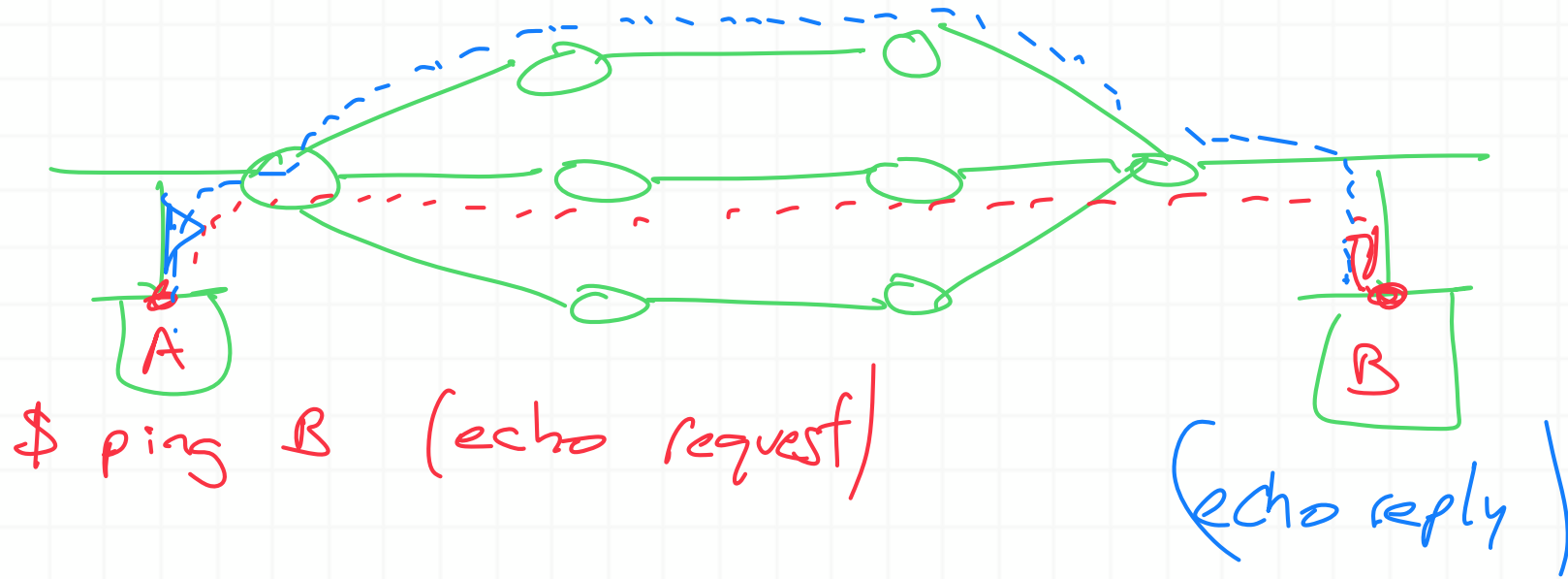| IP	ICMP

<u>Información</u>:

- Echo
  - Request
  - Replay

- Network Information

- Source quench

- Redirect

<u>Errores</u>:

- Destination Unreachable

- Fragmentación
  - IPv4 Fragment needed but DE=1
  - IPv6 Packet too Big

- Packet Corruption

- Time exceded
  - Transit
  - Reasembling

- Parameter Problem

A

$ ping B (echo request)

B

(echo reply)

C

D

A

B

$ traceroute B

Paristraceroute

Análisis de ICMP y *traceroute* en Wireshark

Tarea no obligatoria:

Realizar un captura con el Wireshark de traceroute (si pueden en IPv6) con las opciones TCP y luego con UDP e ICMP, y realizar un informe en PDF.

Lectura para la próxima clase:
Del inicio del **Capítulo 6, hasta *6.3 Multiple Access Links and Protocols* inclusive.**