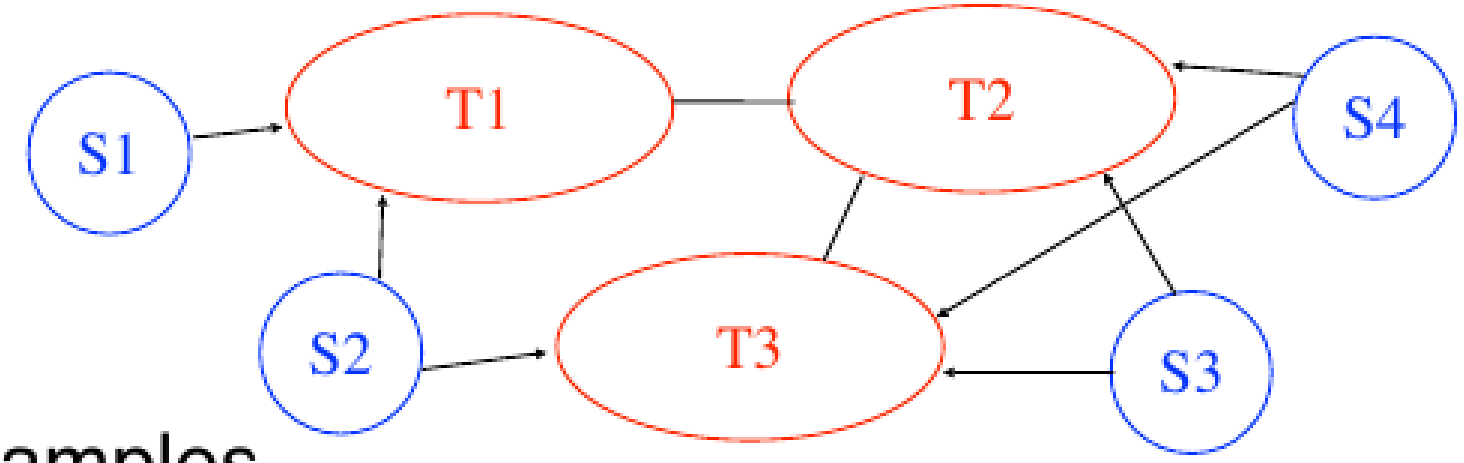
Internet, Principes et Protocoles (IPP)

Table of Contents

Recap

Transit domain

A transit domain allows external domains to use its own infrastructure to send packets to other domains



Examples

UUNet, OpenTransit, GEANT, Internet2, RENATER, EQUANT, BT, Telia, Level3,...

Recap

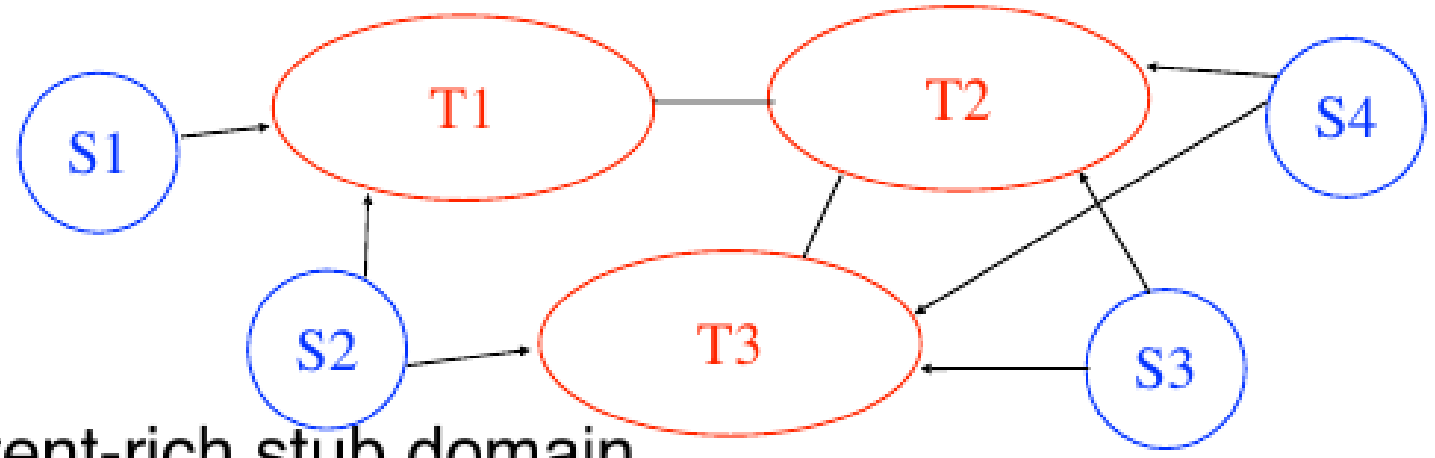
Stub domain

A stub domain does not allow external domains to use its infrastructure to send packets to other domains

A stub is connected to at least one transit domain

Single-homed stub : connected to one transit domain

Dual-homed stub : connected to two transit domains



Content-rich stub domain

Large web servers : Yahoo, Google, MSN, TF1, BBC,...

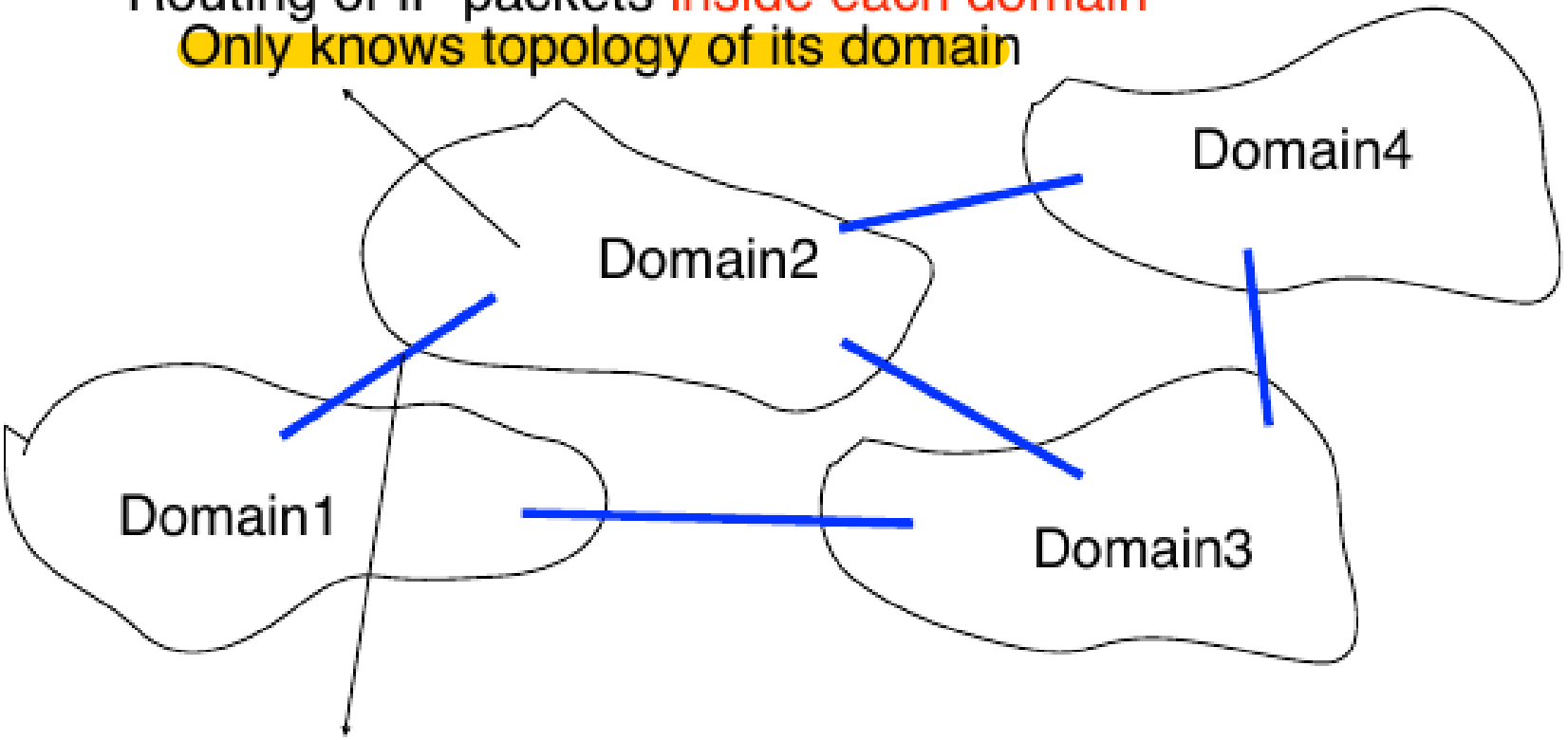
Access-rich stub domain

ISPs providing Internet access via CATV, ADSL, ...

Interior Gateway Protocol (IGP)

Routing of IP packets inside each domain

Only knows topology of its domain



Exterior Gateway Protocol (EGP)

Routing of IP packets between domains

Each domain is considered as a blackbox

Interior Routing Protocols

- Static routing
  - Only useful in very small domains
- Distance vector routing
  - Routing Information Protocol (RIP)
    - Still widely used in small domains despite its limitations
- Link-state routing
  - Open Shortest Path First (OSPF)
    - Widely used in enterprise networks
  - Intermediate System- Intermediate-System (IS-IS)
    - Widely used by ISPs

OSPF

Standardised link state routing protocol

Operation
- Router startup
  - HELLO packets to discover neighbours
- Update of routing tables
  - Link state packets
    - acknowledgements, sequence numbers, age
  - periodic transmission
  - transmission upon link changes
- Database description
  - provides the list of sequence numbers of all LSPs stored by router
- Link state Request
  - used when a router boots to request link state packets from neighbours

OSPF

OSPF in large networks
- avoid too large routing tables in OSPF routers

Solution
- Divide network in areas
- Backbone area : network backbone
  - all routers connected to two or more areas belong to the backbone area
- All non-backbone areas must be attached to the backbone area
  - at least one router inside each area must be attached to the backbone

OSPF routing must allow any router to send packets to any other router

Interdomain routing - BGP

Goals

Allow to transmit IP packets along the best path towards their destination through several transit domains while taking into account the routing policies of each domain without knowing the detailed topology of those domains

From an interdomain viewpoint, best path often means *cheapest* path

Each domain is free to specify inside its routing policy the domains for which it agrees to provide a transit service and the method it uses to select the best path to reach each destination

Border Gateway Protocol (BGP)

- Used as routing protocol between different domains.
- BGP may be used for routing within an autonomous system. (Interior Border Gateway Protocol/ iBGP).
- In contrast, the Internet application of the protocol may be referred to as Exterior Border Gateway Protocol, or eBGP.

Border Gateway Protocol (BGP)

- By design, routers running BGP accept advertised routes from other BGP routers by default.
- Allows for automatic/dynamic routing across the internet
- Allows for any BGP router to advertise any route.
- Problem?

BGP

Public incidents [edit]

- April 1997: The "AS 7007 incident"[7]
- December 24, 2004: TTNet in Turkey hijacks the Internet[8]
- May 7, 2005: Google's May 2005 Outage[9]
- January 22, 2006: Con Edison Communications hijacks big chunk of the Internet[10]
- February 24, 2008: Pakistan's attempt to block YouTube access within their country takes down YouTube entirely.[11]
- November 11, 2008: The Brazilian ISP CTBC - Companhia de Telecomunicações do Brasil Central leaked their internal table into the global BGP table.[12] It lasted over 5 minutes. Although, it was detected by a RIPE route server and then it was not propagated, affecting practically only their own ISP customers and few others.
- April 8, 2010: Chinese ISP hijacks the Internet[13]
- July 2013: The Hacking Team aided Raggruppamento Operativo Speciale (ROS - Special Operations Group of the Italian National Military police) in regaining access to Remote Access Tool (RAT) clients after they abruptly lost access to one of their control servers when the Santrex IPv4 prefix *46.166.163.0/24* became permanently unreachable. ROS and the Hacking Team worked with the Italian network operator Aruba S.p.A. (AS31034) to get the prefix announced in BGP in order to regain access to the control server.[14]
- February, 2014: Canadian ISP used to redirect data from ISPs.[15] - In 22 incidents between February and May a hacker redirected traffic for roughly 30 seconds each session. Bitcoin and other crypto-currency mining operations were targeted and currency was stolen.
- January 2017: Iranian pornography censorship.[16]
- April 2017: Russian telecommunication company Rostelecom (AS12389) originated 37 prefixes[17] for numerous other Autonomous Systems. The hijacked prefixes belonged to financial institutions (most notably MasterCard and Visa) other telecom companies, and a variety of other organizations.[18] Even though the possible hijacking lasted no more than 7 minutes it is still not clear if the traffic got intercepted or modified.
- December 2017: Eighty high-traffic prefixes normally announced by Google, Apple, Facebook, Microsoft, Twitch, NTT Communications, Riot Games, and others, were announced by a Russian AS, DV-LINK-AS (AS39523).[19][20]
- April 2018: Roughly 1300 IP addresses within Amazon Web Services space, dedicated to Amazon Route 53, were hijacked by eNet (or a customer thereof), an ISP in Columbus, Ohio. Several peering partners, such as Hurricane Electric blindly propagated the announcements.[21]
- July 2018: Iran Telecommunication Company (AS58224) originated 10 prefixes of Telegram Messenger.[22]
- November 2018: US-based China Telecom site originated Google addresses.[23]
- May 2019: Traffic to a public DNS run by Taiwan Network Information Center (TWNIC) was rerouted to an entity in Brazil (AS268869).[24]
- June 2019: Large European mobile traffic was rerouted through China Telecom (AS4134)[25][26]

Adress Resolution Protocol

- Upper level protocols (TCP, UDP, HTTP,...) use IP addresses
- Network hardware must use hardware address for delivery (MAC address).
- IP address must be translated into hardware address for delivery
    - The translation is local to a network

Adress Resolution Protocol

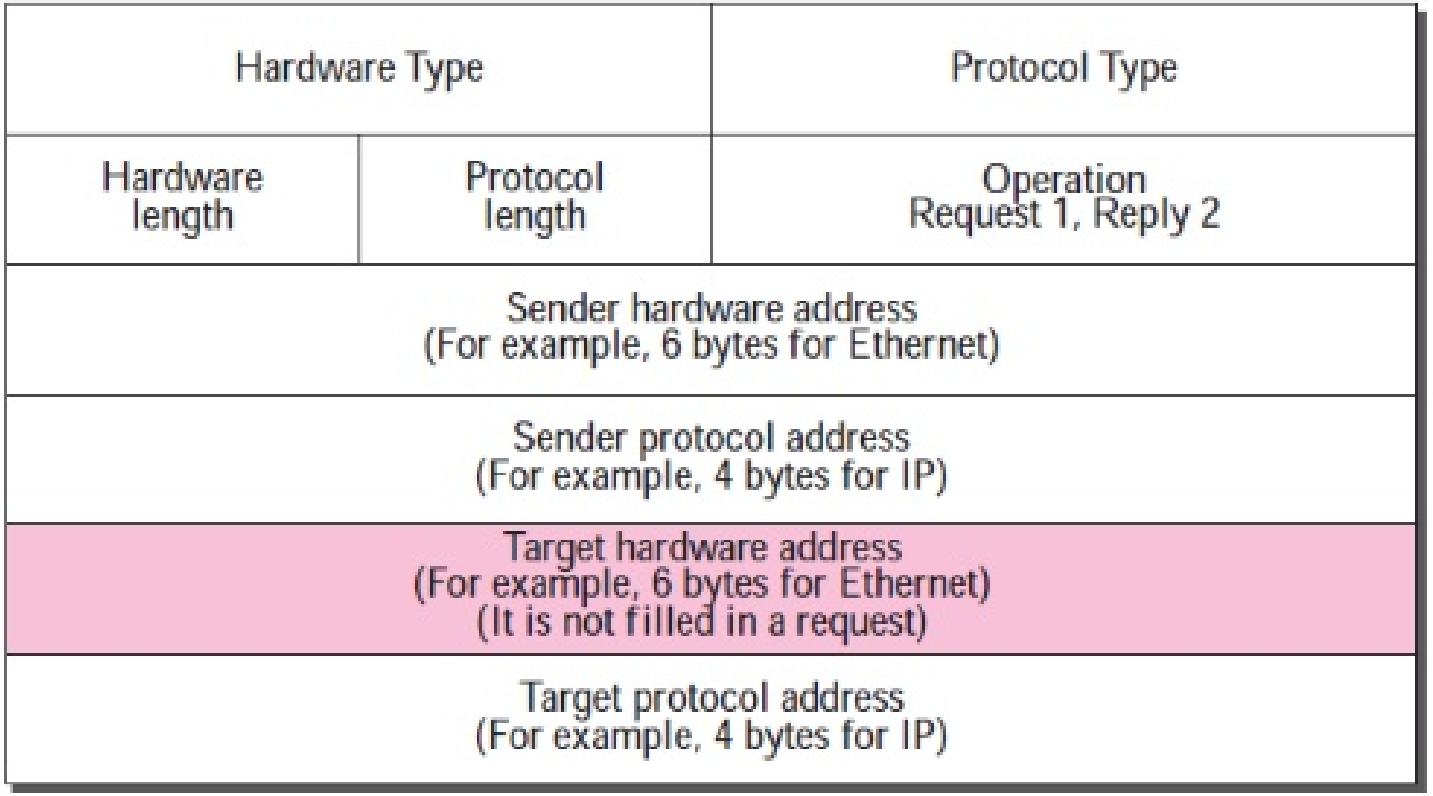
- A host A wants to send a packet to 192.168.1.23
- IP layer, OK, but Datalink layer does not understand IP addresses. It uses MAC addresses (hardware address)
- Address Resolution Protocol (ARP) “translates” IP addresses into MAC, and *vice-versa.*

ARP

- Host A searched his ARP cache, for the resolution of to the IP 192.168.1.23
- If not in cache, A uses ARP to find the MAC address.
- ARP is in 2 parts:
  - Request from source asking for MAC
  - Reply from destination with the MAC
- If no MAC address for the destination, how can the source send the message to the right host?
  - Broadcast Message

ARP

- Source broadcasts message “Who has IP 192.168.1.23”
- The host with the right IP answers with his MAC in unicast mode.



ARP

- Hosts sometimes automatically cache any ARP reply that it receives (even valid entries will be overwritten).
- No authentication method.

- What happens if Bob sends Alice and ARP Reply linking the IP address of the router and the MAC address of Bob?

ARP Poisoning

- What happens if Bob sends Alice and ARP Reply linking the IP address of the router and the MAC address of Bob?
- Alice will send all her traffic to Bob, thinking Bob is the router.
- Bob can forward Alice’s traffic to the router, putting himself in the middle. In this position, he can drop, spy on, modify Alice’s traffic.

Man-In-The-Middle attack