

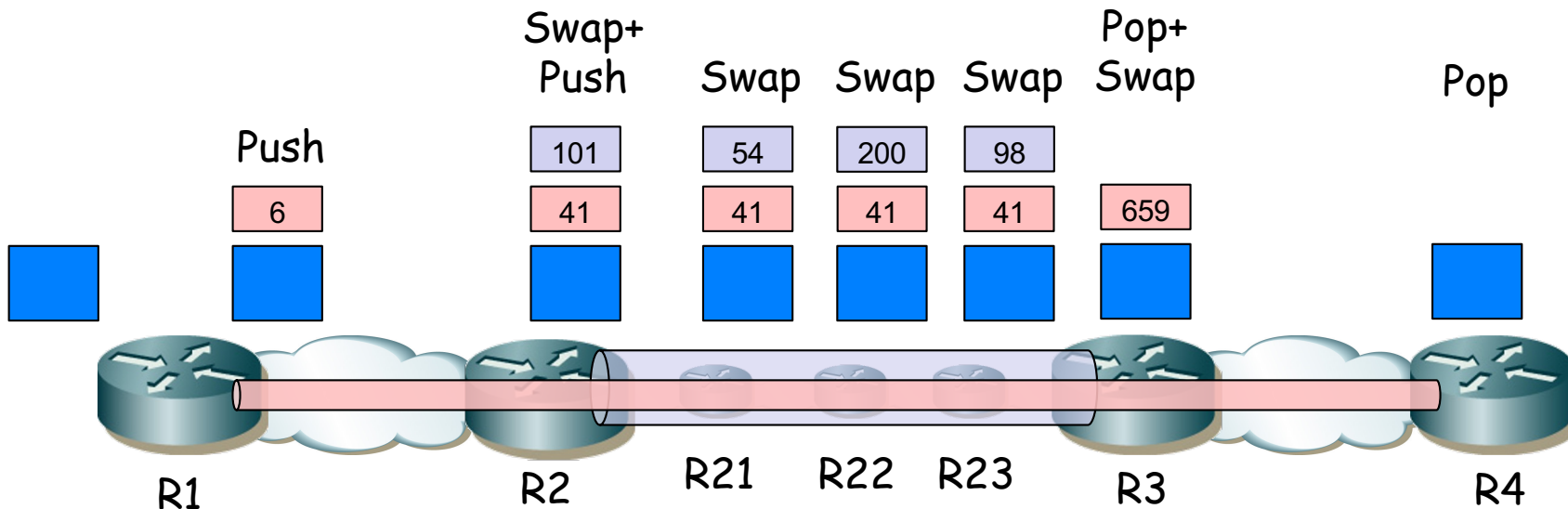
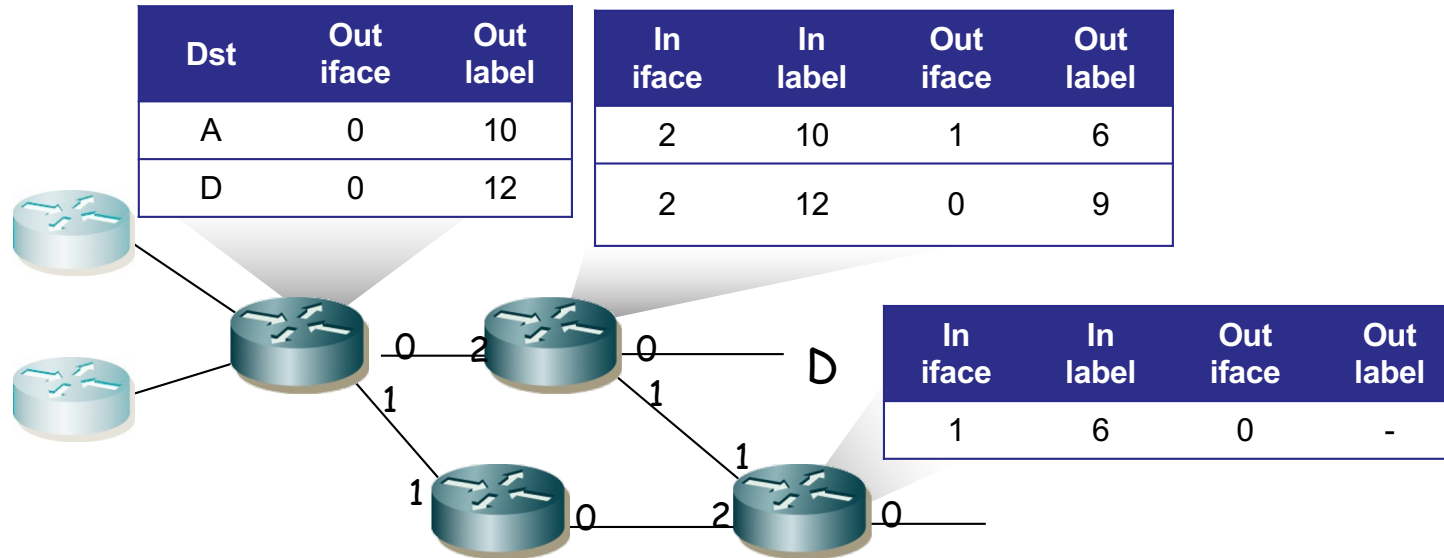
upna

Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

Redes de Nueva Generación
Área de Ingeniería Telemática

MPLS

LSP Tunnels dentro de LSPs



upna

Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

Redes de Nueva Generación
Área de Ingeniería Telemática

MPLS

upna

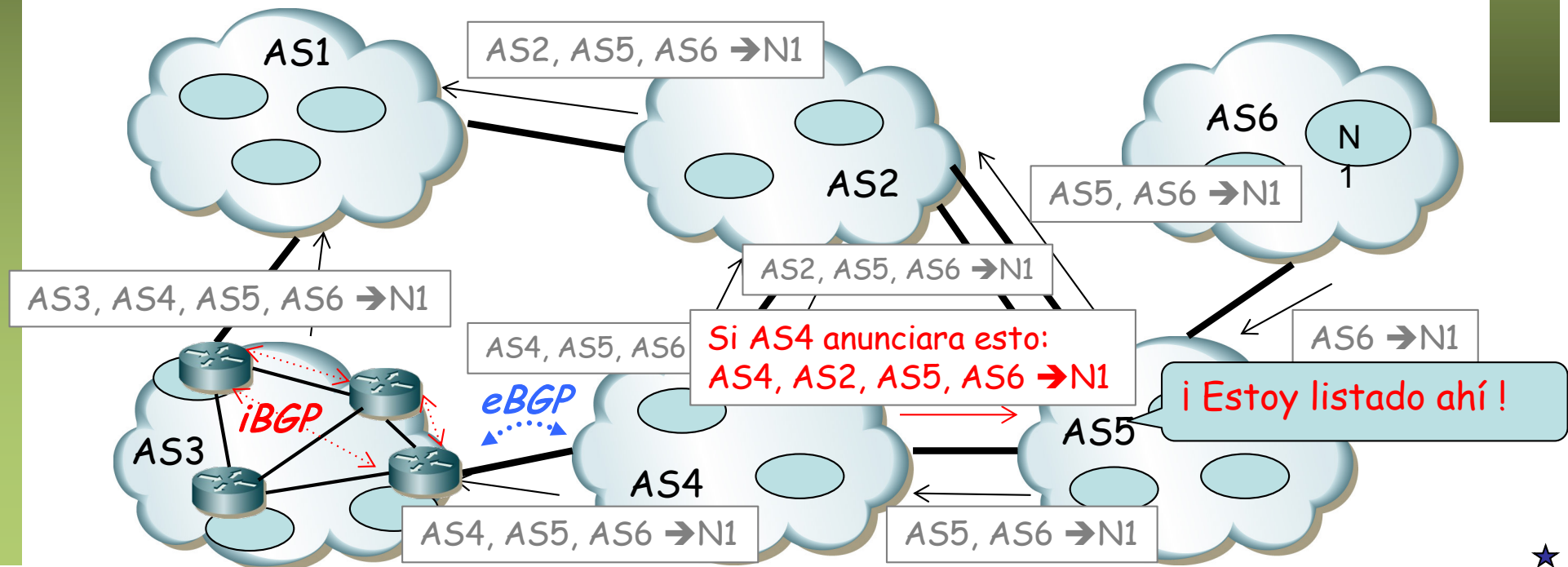
Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

Redes de Nueva Generación
Área de Ingeniería Telemática

BGP-4

BGP

- Path Vector: Anunciar el camino permite evitar los ciclos
- En otro AS: *external peer* \Rightarrow **eBGP**, mismo AS: *internal peer* \Rightarrow **iBGP**
- En el mismo AS el *peering* iBGP forma una malla porque...
 - iBGP permite que otros ASBRs aprendan los prefijos a anunciar
 - No se pasan por iBGP prefijos aprendidos por iBGP
 - No interesa difundir todas las rutas al IGP (escalabilidad)



upna

Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

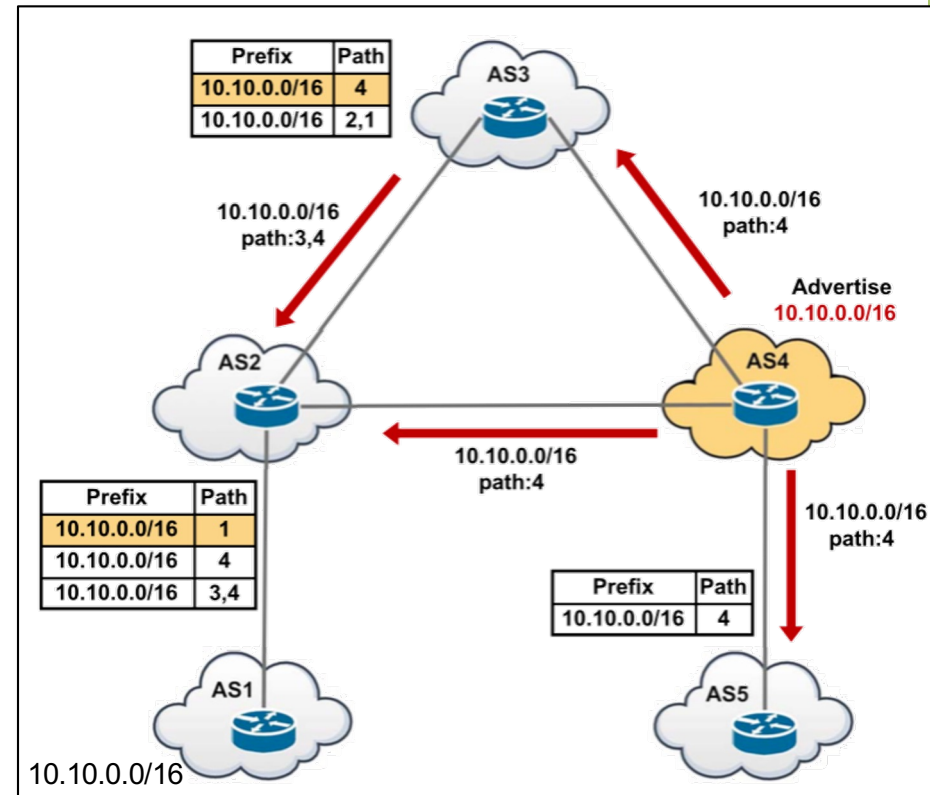
Redes de Nueva Generación
Área de Ingeniería Telemática

BGP - Problemas

BGP – (Sub-)Prefix hijacking

Ejemplos de problemas

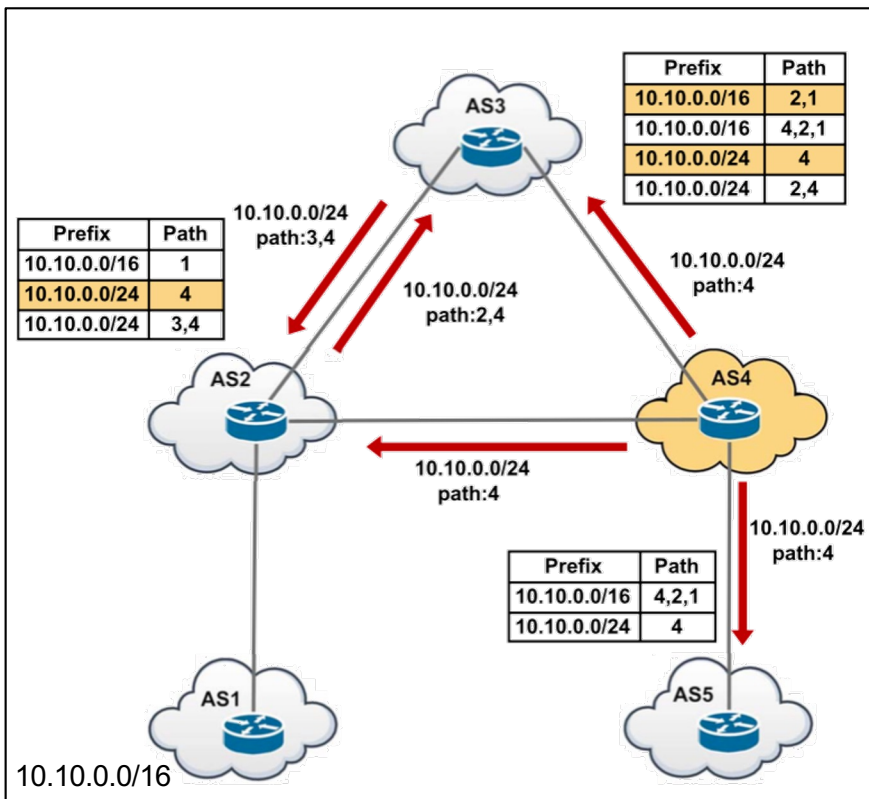
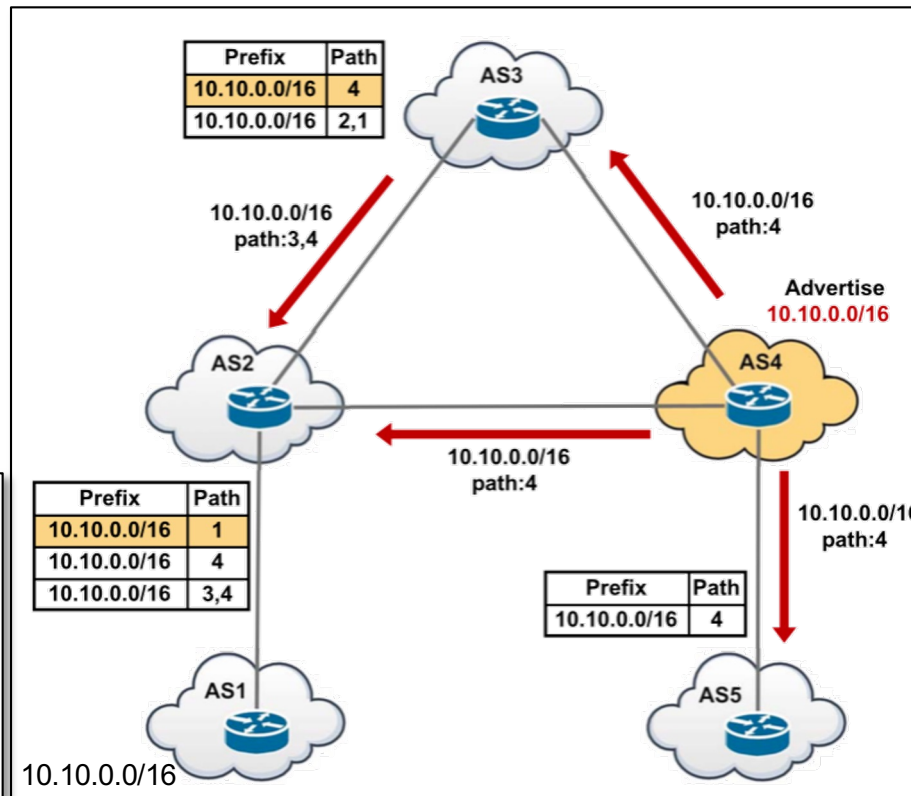
- Prefix hijacking



10.10.0.0/16

Ejemplos de problemas

- Prefix hijacking
- Sub-prefix hijacking

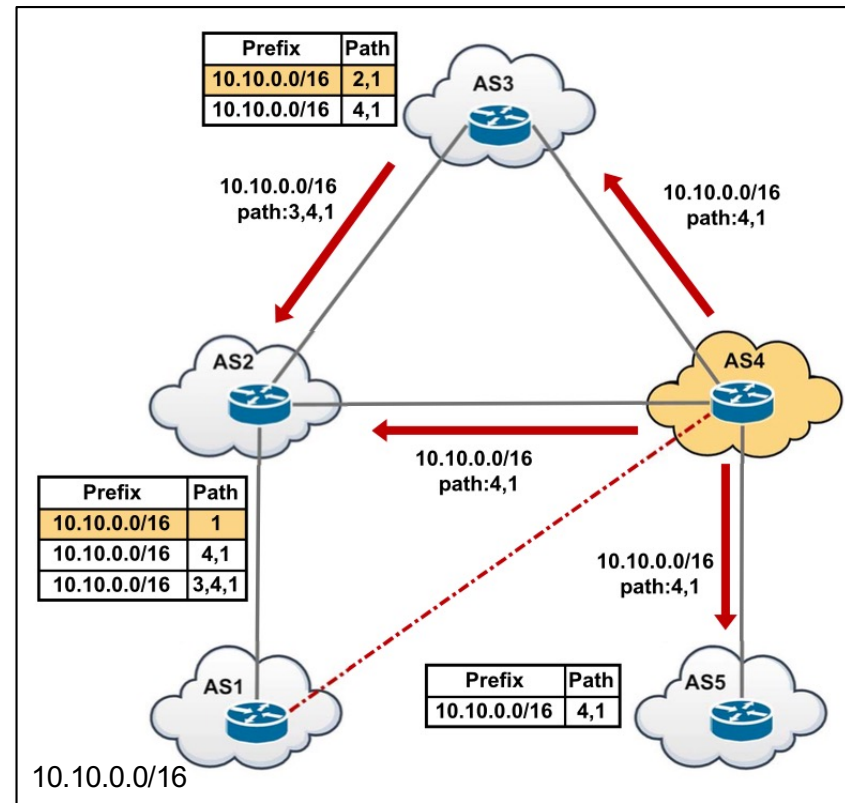


BGP – (Sub-)Prefix hijacking

BGP – (Sub-)Prefix and its AS hijacking

Ejemplos de problemas

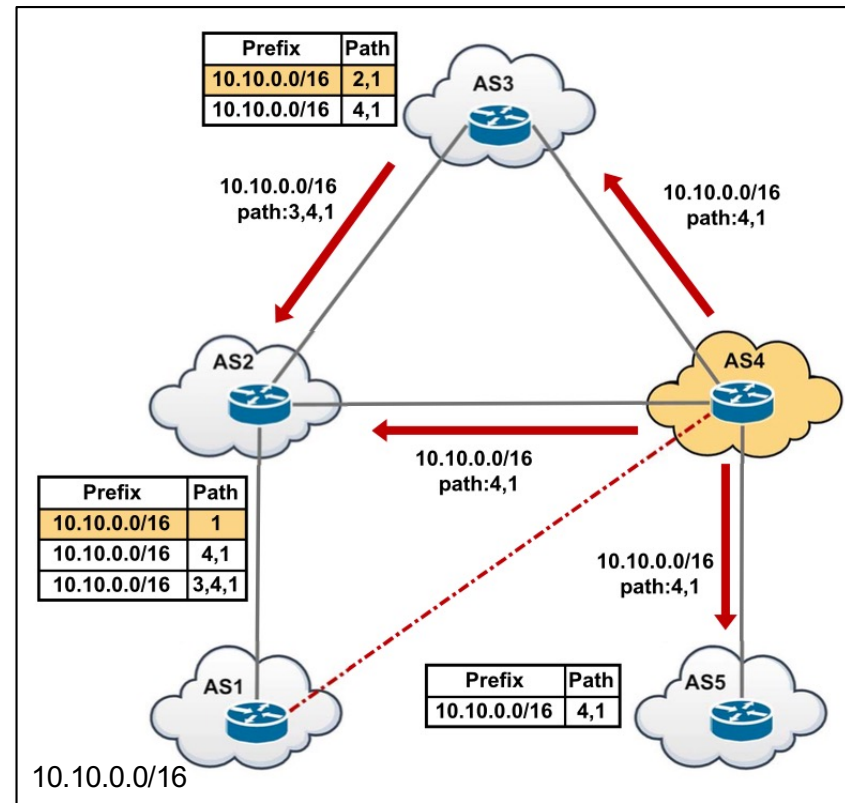
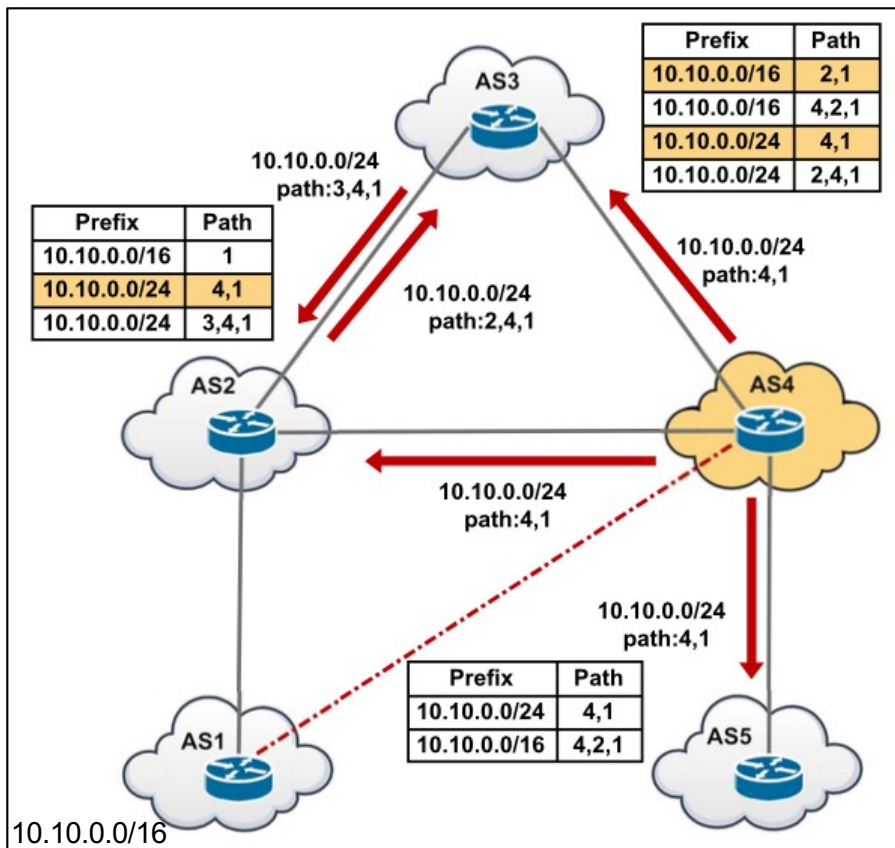
- Prefix and its AS hijacking



10.10.0.0/16

Ejemplos de problemas

- Prefix and its AS hijacking
- Sub-prefix and its AS hijacking



Ejemplo de secuestro

- YouTube Hijacking: A RIPE NCC RIS case study
 - <https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study>
 - <https://youtu.be/lzLPKuAOe50>

The screenshot shows the RIPE NCC website interface. At the top left is the RIPE NCC logo (RIPE NETWORK COORDINATION CENTRE). To the right is a search bar for the RIPE Database (Whois) and a link to the Website. Below the header is a navigation menu with items: Manage IPs and ASNs, Analyse, Participate, Get Support, and Publications. A breadcrumb trail reads: You are here: Home > Publications > News > Industry Developments > YouTube Hijacking: A RIPE NCC RIS case study. On the left sidebar, there are sections for Publications (with a left arrow) and News (with a down arrow). Under Publications are links for RIPE Document Store, RIPE NCC Organisational Documents, IPv6 Info Centre, and Member Update. Under News are links for RSS News Feeds, Industry Developments, NRO News, Call for Comments for a Draft Internet Number Community Review, and Committee Charter. The main content area features the article title 'YouTube Hijacking: A RIPE NCC RIS case study' in a large font. Below the title is a yellow warning box: 'You're viewing an archived page. It is no longer being updated.' The article begins with an 'Introduction' section, stating: 'On Sunday, 24 February 2008, Pakistan Telecom (AS17557) started an unauthorised announcement of the prefix 208.65.153.0/24. One of Pakistan Telecom's upstream providers, PCCW Global (AS3491) forwarded this announcement to the rest of the Internet, which resulted in the hijacking of YouTube traffic on a global scale.' It continues: 'In this report we show how the events were seen by RIPE NCC's Routing Information Service (RIS) and how, in general, one can use the RIS tools to obtain hard data on network events.' Below the introduction is an 'Event Timeline' section with two bullet points:

- **Before, during and after Sunday, 24 February 2008:** AS36561 (YouTube) announces 208.65.152.0/22. Note that AS36561 also announces other prefixes, but they are not involved in the event.
- **Sunday, 24 February 2008, 18:47 (UTC):** AS17557 (Pakistan Telecom) starts announcing 208.65.153.0/24. AS3491 (PCCW Global) propagates the announcement. Routers around the world receive the announcement, and YouTube traffic is redirected to Pakistan.

Más ejemplos

- <https://youtu.be/HnCfQUzMzFM>

How Pakistan knocked YouTube offline (and how to make sure it never happens again)
YouTube becoming unreachable isn't the first time that Internet addresses were hijacked. But if it spurs interest in better security, it may be the last.
BY DECLAN MCCULLOUGH · FEBRUARY 25, 2008 4:28 PM PST

BORDER GATEWAY PROTOCOLS — How 3ve's BGP hijackers eluded the Internet—and made \$29M
3ve used addresses of unsuspecting owners—like the US Air Force.
DAN GOODIN · 12/21/2018, 12:30 PM

BORDER GATEWAY PROTOCOLS ATTACK — Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency
Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.
DAN GOODIN · 4/24/2018, 2:00 PM

Criminals, Nation-States Keep Hijacking BGP and DNS
While Exploitable Protocols and Processes Persist, Adoption of Secure Fixes Lags
Matthew J. Schwartz · February 18, 2019

Why BGP Hijacking Remains a Security Scourge
Cyber criminals are stepping up their attacks against routing protocols, creating new problems for network operators.

OmanTel hijacking of IP space
Jared Mauch [jared at puck.nether.net](mailto:jared@puck.nether.net)
Wed Jan 11 15:50:49 UTC 2017

- Previous message (by thread): [Advice re network compromise and "law enforcement" \(PCI certification\)](#)
- Next message (by thread): [OmanTel hijacking of IP space](#)
- Messages sorted by: [\[date\]](#) | [\[thread\]](#) | [\[subject\]](#) | [\[author\]](#)

There is an ongoing pattern of OmanTel hijacking IP space and advertising it to many of their peers here/42000/you

IPv4 and IPv6 hijacking by AS 6

Matt Harris [matt at netfire.net](mailto:matt@netfire.net)
Thu Apr 12 16:34:31 UTC 2018

- Previous message (by thread): [\[date\]](#) | [\[thread\]](#) | [\[subject\]](#) | [\[author\]](#)
- Next message (by thread): [IPv4](#)
- Messages sorted by: [\[date\]](#) | [\[thread\]](#) | [\[subject\]](#) | [\[author\]](#)

AS 6 is now announcing a like I'm not alone. Does anyone else see this? The hijacking is tremendous. The phone is non-functional. I've seen (Mike Abbott and John Lu) not optimistic.

198.154.60.0/22 bogon/hijacked?

Jeremy Parsons [jeremyp at gmx.us](mailto:jeremyp@gmx.us)
Mon Nov 14 00:49:29 UTC 2016

AS3266: BitCanal hijack factory, courtesy of Cogent, GTT, and Level3

Ronald F. Guilmette [rfg at tristatelogic.com](mailto:rfg@tristatelogic.com)
Tue Jun 26 04:49:15 UTC 2018

- Previous message (by thread): [Call for presentations RIPE 77](#)
- Next message (by thread): [AS3266: BitCanal hijack factory, courtesy of Cogent, GTT, and Level3](#)
- Messages sorted by: [\[date\]](#) | [\[thread\]](#) | [\[subject\]](#) | [\[author\]](#)

AS9498 Bharti BGP hijacks

George William Herbert [george.herbert at gmail.com](mailto:george.herbert@gmail.com)
Sat Apr 1 18:19:55 UTC 2017

- Next message (by thread): [AS9498 Bharti BGP hijacks](#)
- Messages sorted by: [\[date\]](#) | [\[thread\]](#) | [\[subject\]](#) | [\[author\]](#)

Hey, Bharti, knock that off.

Prefix hijack by INDOSAT AS4795 / AS4761

Randy amps [amps at djab.com](mailto:amps@djab.com)
Thu Mar 26 14:08:20 UTC 2015

- Previous message: [booster to gain distance above 60km](#)
- Next message: [Prefix hijack by INDOSAT AS4795 / AS4761](#)
- Messages sorted by: [\[date\]](#) | [\[thread\]](#) | [\[subject\]](#) | [\[author\]](#)

(going) we are seeing
else seeing similar or

1436 29889
1436 29889

BGP – (Sub-)Prefix and its AS hijacking

upna

Universidad Pública de Navarra
Nafarroako Unibertsitate Publikoa

Redes de Nueva Generación
Área de Ingeniería Telemática

BGP-4