



MANRS



Cooperación Latino Americana de Redes Avanzadas



Al servicio y fortalecimiento
de la educación superior

ASOCIACIÓN NACIONAL DE UNIVERSIDADES
E INSTITUCIONES DE EDUCACIÓN SUPERIOR



Corporación Universitaria para el Desarrollo de Internet A.C.
Internet 2 - México



UNIVERSIDAD DE
GUADALAJARA
Administración General

Normas Mutuamente
Acordadas para el
Enrutamiento Seguro en
Internet

Acción 2 – Anti-Spoofing

Jaime Olmos

ASn 2549

IPv4 148.202.0.0/16 200.39.160/19 207.249.224/19

IPv6 2001:1210::/32

Agenda



¿Qué es IP address Spoofing?

Paquetes con una dirección IP de origen falsa o suplantada

- Mala configuración
Problema de software
- Simulación y Pruebas
Pruebas de rendimiento
- Intentos maliciosos
Oculta la identidad del origen
Hacerse pasar por otro host

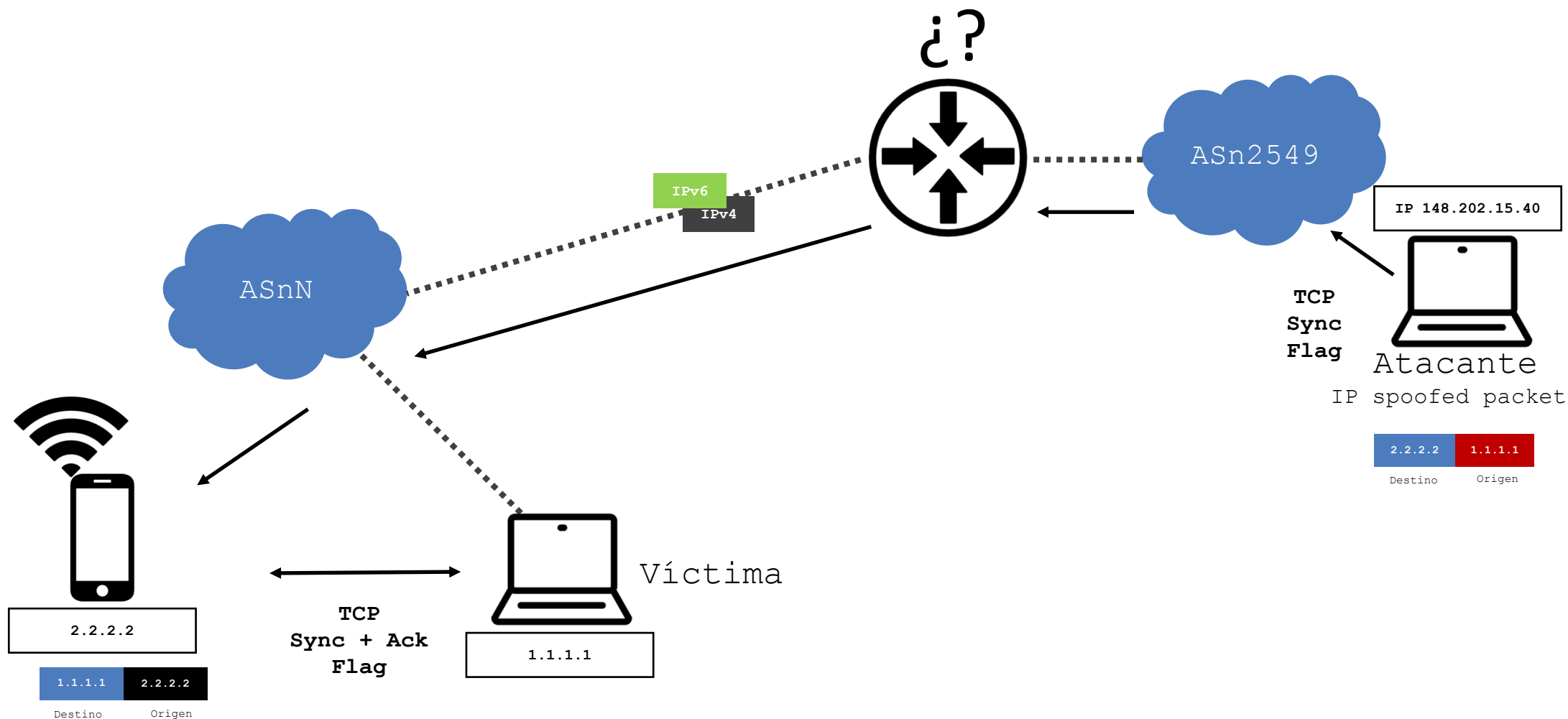
Utilizado con mayor frecuencia para ataques de denegación de servicio DDoS

- ¡Cualquiera puede ser una víctima!

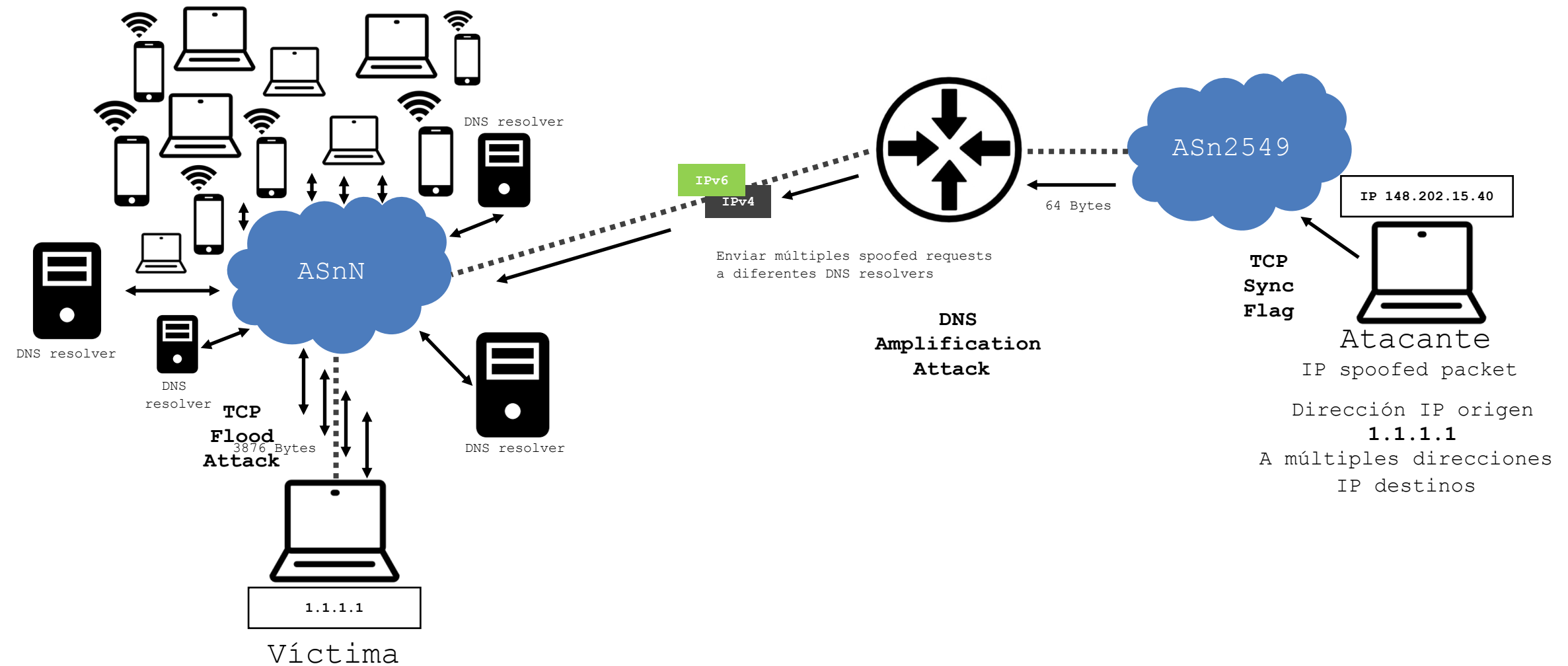
Soluciones

- ACLs
- uRPF
- SAVI

Comprender un IP Spoofing



Distribute Denial of Service





Algunas Soluciones

De ingreso Access Lists

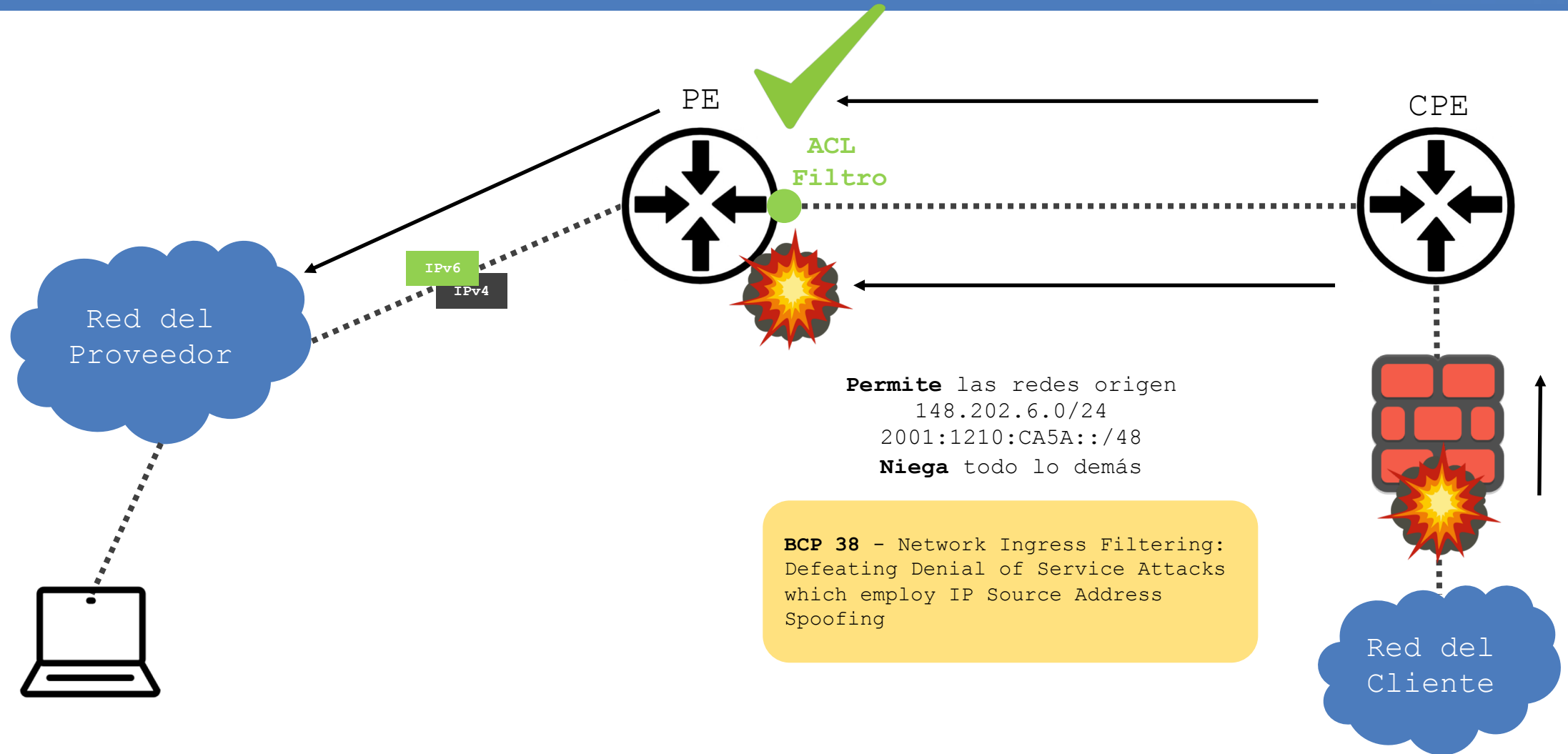
- Access Control List - ACLs

Unicast Reverse Path Forward (uRPF)

- Strict Mode
- Loose Mode
- Feasible Path
- VRF Mode

Source Address Validation Improvement (SAVI)

Access Control List



Filtro de Ingreso en router PE



CISCO

```
interface GigabitEthernet0/1
ip access-group FILTRO-CLIENTE-V4 in
ipv6 traffic-filter FILTRO-CLIENTE-V6 in
...
ip access-list extended FILTRO-CLIENTE-V4
! Una dirección IP del cliente
permit ip 148.202.5.3 0.0.0.0 any
! Un rango de direcciones IP del cliente
permit ip 148.202.6.0 0.0.0.255 any
! Rechazar todas las demás
deny ip any any
...
ipv6 access-list extended FILTRO-CLIENTE-V6
! Una dirección IP del cliente
permit ipv6 2001:1210:C0C0:10C0::2/128 any
! Un rango de direcciones IPv6 del cliente
permit ipv6 2001:1210:CA5A::/48 any
! Rechazar todas las demás
deny ipv6 any any
```

Filtro de Ingreso en router PE



JUNIPER

```
interfaces {
  ge-0/0/0 {
    unit 0 {
      family inet {
        filter {
          input CLIENT-V4;
        }
      }
      family inet6 {
        filter {
          input CLIENTES-V6;
        }
      }
    }
  }
}
```

```
policy-options {
  prefix-list FILTRO-CLIENTE-V4{
    /* Una dirección IP del cliente */
    148.202.5.3/32;
    /* Un rango de direcciones IP del cliente */
    148.202.6.0/24;
  }
  prefix-list FILTRO-CLIENTE-V6{
    /* Una dirección IPv6 del cliente */
    2001:1210:C0C0:10C0::2/128;
    /* Un rango de direcciones IPv6 del cliente */
    2001:1210:CA5A::/48;
  }
}
```

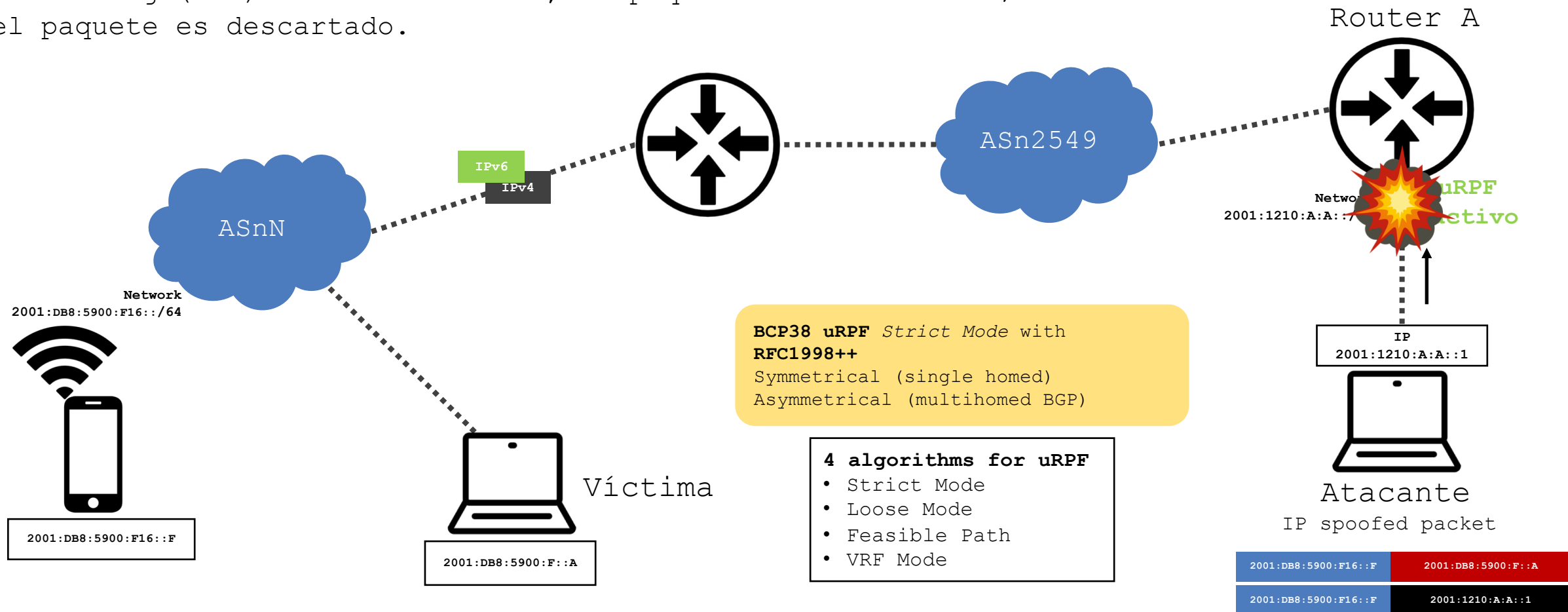
```
firewall {
  family inet6 {
    filter CLIENTES-V6{
      term 1 {
        from {
          source-prefix-list {
            FILTRO-CLIENTE-V6;
          }
        }
        then {
          accept;
        }
      }
      term DEFAULT{
        then {
          discard;
        }
      }
    }
  }
}
```

```
firewall {
  family inet {
    filter CLIENTES-V4{
      term 1 {
        from {
          source-prefix-list {
            FILTRO-CLIENTE-V4;
          }
        }
        then {
          accept;
        }
      }
      term DEFAULT{
        then {
          discard;
        }
      }
    }
  }
}
```


Unicast Reverse Path Forward



El **Router A** busca una entrada para la dirección origen en su tabla de forwarding (FIB). Si la encuentra, el paquete es transmitido; de otra manera el paquete es descartado.



Unicast Reverse Path Forward



CISCO

```
ip cef
ipv6 cef
interface GigabitEthernet0/1
ip verify unicast source reachable-via rx
ipv6 verify unicast source reachable-via rx
```

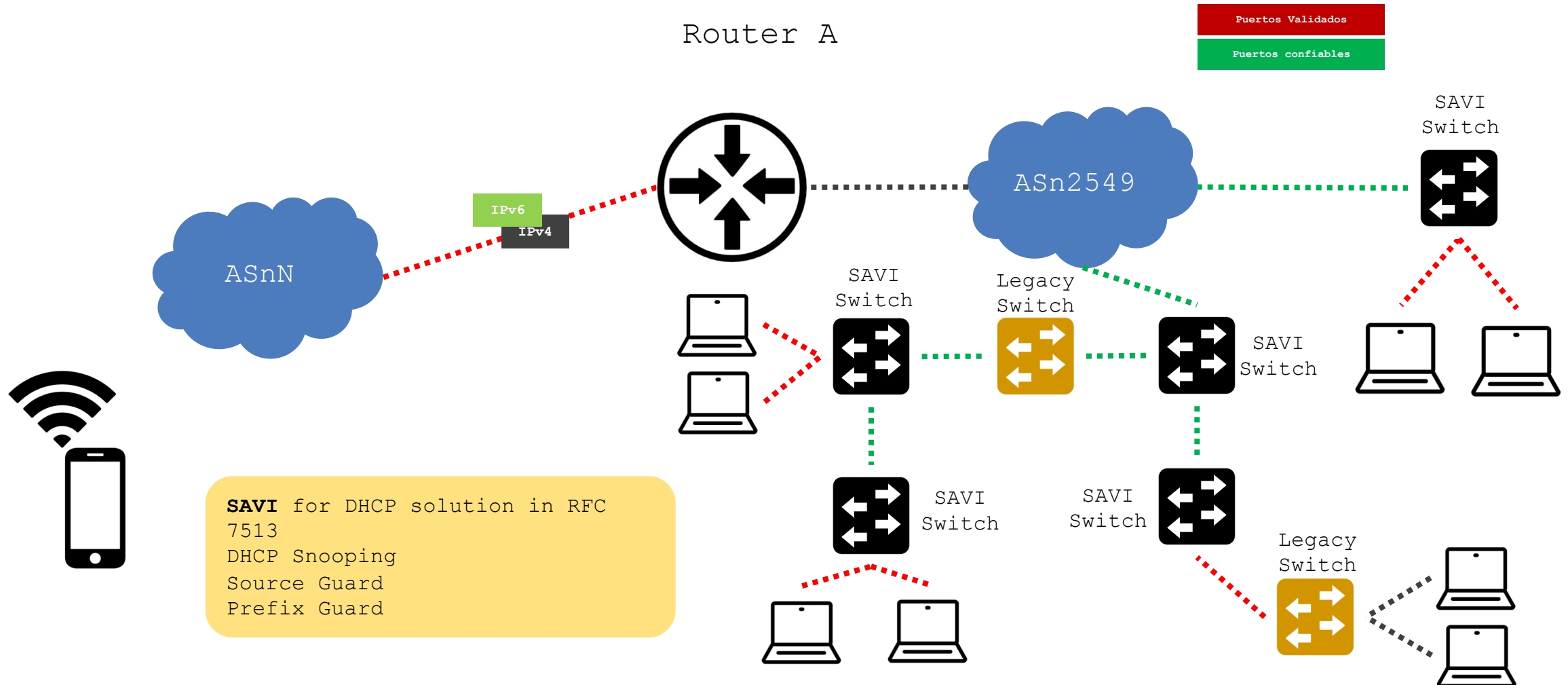
Unicast Reverse Path Forward



JUNIPER

```
interfaces {  
  ge-0/0/0 {  
    unit 0 {  
      family inet {  
        rpf-check;  
      }  
    }  
  }  
}
```

```
interfaces {  
  ge-0/0/0 {  
    unit 0 {  
      family inet6 {  
        rpf-check;  
      }  
    }  
  }  
}
```



Lecturas adicionales



- **RIPE Anti-Spoofing Task Force HOW-TO**
<https://www.ripe.net/publications/docs/ripe-431>
- **Source Address Validation Improvements (SAVI) Solution for DHCP**
<https://tools.ietf.org/html/rfc7513>
- **Setting Access Lists with Radius**
<http://blog.ipspace.net/2010/09/setting-access-lists-with-radius.html>
- **Cisco: IPv6 First-Hop Security Configuration Guide**
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-sy/ipv6f-15-sy-book.html
- **Cisco: Configuring DHCP Snooping, IP Source Guard, and IPSG for Static Hosts**
<http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4500/12-2/15-02SG/configuration/guide/config/dhcp.html>
- **Cisco: Configuring DHCP Features and IP Source Guard**
http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_53_se/configuration/guide/2960scg/swdhcp82.html
- **Cisco: Cable Source-Verify and IP Address Security**
<http://www.cisco.com/c/en/us/support/docs/broadband-cable/cable-security/20691-source-verify.html>



DUDAS



ASOCIACIÓN NACIONAL DE UNIVERSIDADES
E INSTITUCIONES DE EDUCACIÓN SUPERIOR



UNIVERSIDAD DE
GUADALAJARA
Administración General



MANRS



¡Gracias!

Jaime Olmos – UdeG

Emmanuel Serrano – UADY