Escenarios de implementación sobre SDN e IPv6

CASO DE UNA RED UNIVERSITARIA

UNIVERSIDAD DE GUADALAJARA

Red Universitaria e Institución Benemérita de Jalisco

CGTI

COORDINACIÓN GENERAL DE TECNOLOGÍAS DE INFORMACIÓN

NIC MÉXICO

RESUMEN

- **IPv6** – implica un enorme espacio de direcciones, comunicación de extremo a extremo, características de seguridad, etc.
- Requiere un contexto de integración / automatización de dispositivos e infraestructura de red, para la transición a IPv6.
- La Red Definida por Software (SDN) define un nuevo concepto para separar el control y proporcionar elementos abstractos de dispositivos de red.
- **IPv6 / SDN no** tienen mucho en común; pero tienen un potencial de revolucionar el diseño de red, construir y lograr una operación de la red empresarial más eficiente.
- Presentaremos las principales arquitecturas de SDN e ilustraremos cómo la UdeG implementa e integra ambas tecnologías IPv6 / SDN, utilizando mecanismos: OpenFlow, Web API, NETCONF, SSH, SNMP, entre otras.

UNIVERSIDAD DE GUADALAJARA

Red Universitaria e Institución Benemérita de Jalisco

Consideraciones generales en IPv6

La red Internet será mucho más compleja durante un tiempo:

- Mayor uso de NAT44 para IPv4
- Mayor uso de NAT64 para IPv6
- Mayor uso de túneles
- Uso de otras tecnologías de transición co-existencia

así y todo es la única opción para permanecer en Internet

Mitos IPv6

REUNIÓN DE OPERADORES DE REDES MÉXICO

- PENSAR EN UN MUNDO SOLO IPv4, Y NO TENGO QUE PREOCUPARME POR IPv6.
  - MAYORÍA DE LOS S.O. TIENEN ACTIVO IPv6 POR DEFECTO.
- IPv6 ES MÁS SEGURO QUE IPv4.
  - IPSEC
    - ALGUNA ESPECIE DE ESTRATEGIA DE PROMOCIÓN, AL FINAL FUE CONTRAPRODUCENTE POR QUE NO FUE TAN CIERTO.
    - FUE UN REQUISITO EL SOPORTE IPSEC EN LOS NODO.
    - EN LA PRÁCTICA NO SE LLEVO DE MANERA GENERALIZADA.
- ESTOY EXPUESTO A ATAQUES SI NO USO NAT, SIN DIRECCIONES PRIVADAS.
  - NO ES CIERTO POR QUE NO ESTAMOS OBLIGADOS PERMITIR TRÁFICO A CUALQUIER PARTE DE NUESTRA RED.
- IPv6 ES ALGO MUY NUEVO PARA SER ATACADO.
  - SE HAN DETECTADO HERRAMIENTAS Y ATAQUES CON IPV6 (COMO DOS).

Limite o frontera de un nibble

REUNIÓN DE OPERADORES DE REDES MÉXICO

EN EL CONTEXTO DE IPv6, EL LÍMITE DE UN NIBBLE SE REFIERE A 4 bits. CUALQUIER CAMBIO EN MÚLTIPLOS DE 4 bits ES FÁCIL DE CALCULAR:

DIGAMOS QUE TENEMOS UNA ASIGNACIÓN: **2001:1210::/32**. TOMAR RODAJAS DE ESTE GRUPO DENTRO DE UN LÍMITE DE 4 bits ES BASTANTE FÁCIL, QUE CON DECIMALES EN IPv4.

APNIC - How to: calculating IPv6 subnets outside the nibble boundary

N bits	M bits	32-N-M bits = 4,294,967,296 subnets
Global Routing Prefix	Subnet ID	Mask bits
2001:1210:	0000:0000:	/48
2001:1210:	FFFF:FFFF:	/48

Direcciones IPv6 Global Unicast

REUNIÓN DE OPERADORES DE REDES MÉXICO

64 bits IID

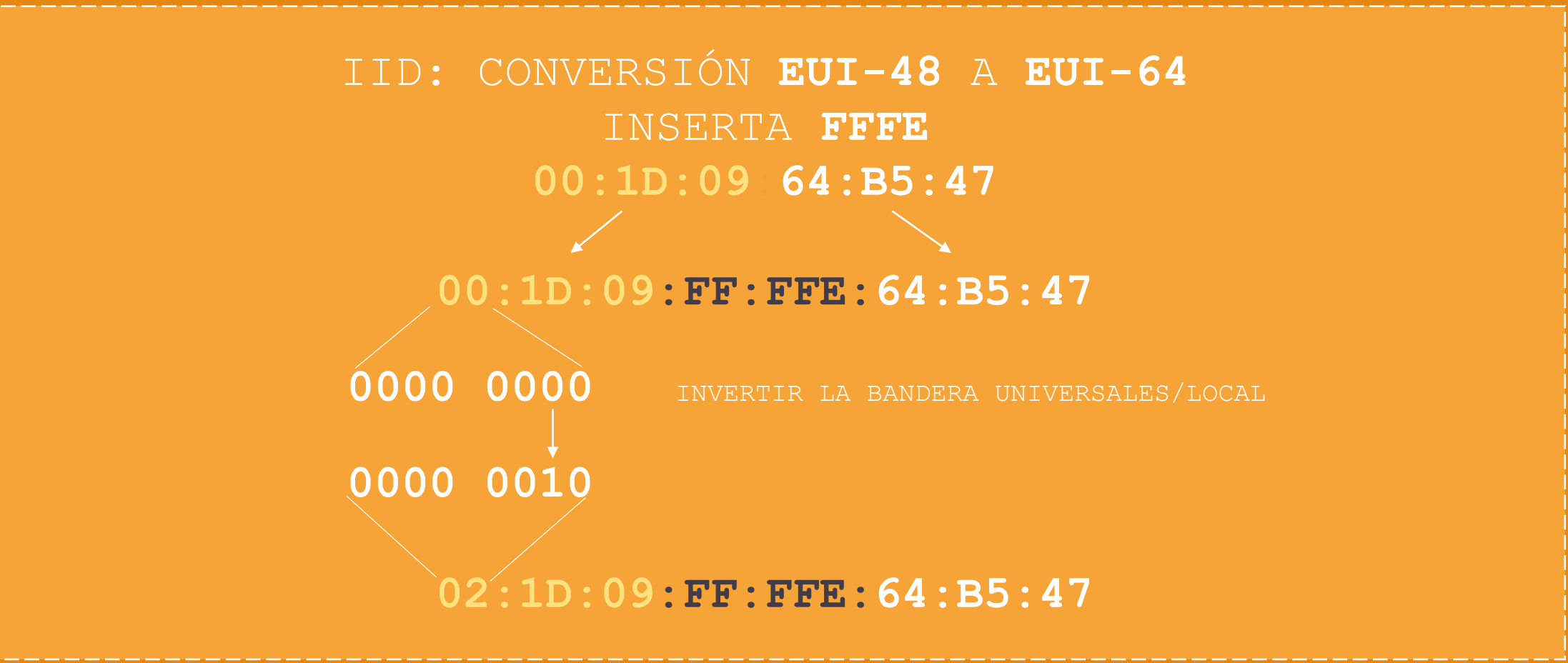
N bits	M bits	((128 – N) – M) bits
Global Routing Prefix	Subnet ID	Interface ID
2001:1210:0100:	0001:	021d:09ff:fe64:b547

64 bits

- **GLOBAL ROUTING PREFIX** (**GRP**)Y **SUBNET ID** (**SID**) SIMILARES A IPv4.
- EL **INTERFACE ID** (**IID**) ANÁLOGO AL HOST-ID DE IPv4 (PERO DE 64 bits).
- SE PUEDE SELECCIONAR CON DIFERENTES CRITERIOS:
  - MODIFIED EUI-64 IDENTIFIERS (STATELESS ADDRESS AUTOCONFIGURATION O **SLAAC**, AUTOCONFIGURACIÓN DE DIRECCIÓN SIN ESTADO **TRADICIONAL**)
  - IDENTIFICADORES ALEATORIOS (DIRECCIONES TEMPORALES)
  - CONFIGURADOS MANUALMENTE
  - DE ACUERDO A LO ESPECIFICADO POR TECNOLOGÍAS DE TRANSICIÓN

Implicaciones de seguridad en el direccionamiento IPv6

REUNIÓN DE OPERADORES DE REDES MÉXICO



Implicaciones de seguridad en el direccionamiento IPv6

REUNIÓN DE OPERADORES DE REDES MÉXICO

CORRELACIÓN DE ACTIVIDADES EN EL TIEMPO

- LOS IID DE IPv6 SON “GLOBALMENTE ÚNICOS” Y ESTABLES.
  - EJEMPLO:
    - DÍA 1: ACTIVIDAD DE 2001:1210:1::**021D:09**FF:FE**64:B547**/64
    - DÍA 2: ACTIVIDAD DE 2001:1210:1::**021D:09**FF:FE**64:B547**/64
    - EL IID “**021D:09FF:FE64:B547**” REVELA LA IDENTIDAD DEL NODO
      - POR LO TANTO PUEDO HACER CORRELACIÓN DE ACTIVIDADES

Implicaciones de seguridad en el direccionamiento IPv6

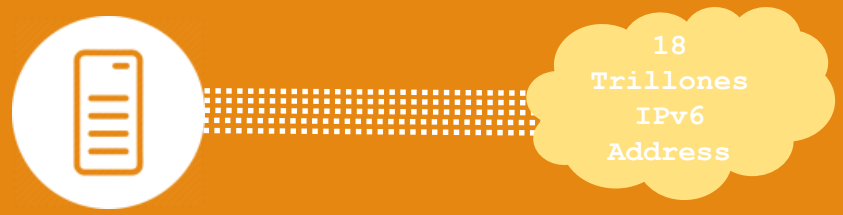
REUNIÓN DE OPERADORES DE REDES MÉXICO

EN LA RED 1: EL HOST AUTOCONFIGURA:
2001:1200:5A25:021D:09FF:FE64:B547/64

Implicaciones de seguridad en el direccionamiento IPv6

REUNIÓN DE OPERADORES DE REDES MÉXICO

- **RECONOCIMIENTO DE RED**
  - SE ASUME QUE LOS ATAQUES DE ESCANEO DE DIRECCIONES IPv6 SON **IMPOSIBLES**.



SI SE PUDIERA ESCANEAR **UN MILLÓN** DE DIRECCIONES CADA SEGUNDO ¡NECESITARÍA UNOS **584,555 AÑOS** PARA ESCANEAR SÓLO UN **/64**!

  - LAS DIRECCIONES IPv6 SIGUEN PATRONES.
    - ¡EL ESPACIO DE BÚSQUEDA NO ES 2^{64}!
  - SI BIEN EL ESCANEO POR FUERZA BRUTA ES “IMPOSIBLE”.
    - **LOS ATAQUES DE ESCANEO QUE EXPLOTAN PATRONES EN LAS DIRECCIONES IPv6 SON POSIBLES.**

Mitigaciones de seguridad en el direccionamiento IPv6

REUNIÓN DE OPERADORES DE REDES MÉXICO

```
Last login: Tue Jul 11 11:08:20 on console
249-15:~ operaciones$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
        options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
        inet 127.0.0.1 netmask 0xff000000
        inet6 ::1 prefixlen 128
        inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
        nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=10b<RXCSUM,TXCSUM,VLAN_HWTAGGING,AV>
        ether 00:3e:e1:be:ec:bb
        inet6 fe80::898:10f:5275:569b%en0 prefixlen 64 secured scopeid 0x4
        inet6 2001:1210:100:15:9d:77d5:9586:2cf2 prefixlen 64 autoconf secured
        inet 148.202.15.249 netmask 0xffffff00 broadcast 148.202.15.255
        inet6 2001:1210:100:15::249 prefixlen 64 dynamic
        inet6 2001:1210:100:15:c7b:432f:a484:ae0 prefixlen 64 deprecated autoconf temporary
        inet6 2001:1210:100:15:cca5:c057:a76f:560a prefixlen 64 deprecated autoconf temporary
        inet6 2001:1210:100:15:a89a:5bcf:e55a:d835 prefixlen 64 deprecated autoconf temporary
        inet6 2001:1210:100:15:d82b:7747:707b:b3f5 prefixlen 64 deprecated autoconf temporary
        inet6 2001:1210:100:15:8015:6266:3ca:4e50 prefixlen 64 deprecated autoconf temporary
        inet6 2001:1210:100:15:ed08:a16c:8f95:25cf prefixlen 64 deprecated autoconf temporary
        inet6 2001:1210:100:15:c071:4f75:d413:b4b5 prefixlen 64 autoconf temporary
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect (1000baseT <full-duplex>)
        status: active
```

ONEXIONES

Mitigaciones de seguridad en el direccionamiento IPv6

REUNIÓN DE OPERADORES DE REDES MÉXICO

DIRECCIONES **IPv6**	**Fijas**	**Temporales**
Predecibles	IEEE ID-derived	N/A
No predecibles	RFC 7217	RFC 4941

- **DIRECCIONES AUTO-CONFIGURADAS**
  - **RFC 7217** (STABLE PRIVACY-ENHANCED IPv6 ADDRESSES):
    - REEMPLAZA A LAS DIRECCIONES TRADICIONALES, BASADAS EN IEEE IDS.
    - EN BUENA MEDIDA ES ORTOGONAL A LAS DIRECCIONES TEMPORALES.
    - PROBABLEMENTE “LO SUFICIENTEMENTE BUENO” INCLUSO SIN

RFC 7217 Algoritmo

REUNIÓN DE OPERADORES DE REDES MÉXICO

- **Genera el Interface IDs mediante :**
  - `F(`*`Prefix`*`, Net_Iface, Network_ID, Counter,` **`Secret_Key`**`)`
- DONDE:
  - F() ES UNA PSEUDO-RANDOM FUNCTION (PRF).
    - POR EJEMPLO UNA FUNCIÓN DE HASHING.
  - *Prefix* ES EL PREFIJO SLAAC O EL PREFIJO LINK-LOCAL
  - Net_Iface ES (ALGUNO) EL IDENTIFICADOR DE INTERFAZ
  - Network_ID PODRÍA SER EL SSID DE UNA RED WIRELESS
  - Counter SE UTILIZA PARA RESOLVER COLISIONES
  - **Secret_Key** ES DESCONOCIDO PARA EL ATACANTE (Y GENERADO ALEATORIAMENTE POR DEFECTO)

RFC 7217 Propiedades

REUNIÓN DE OPERADORES DE REDES MÉXICO

En la red 2; el host autoconfigura:

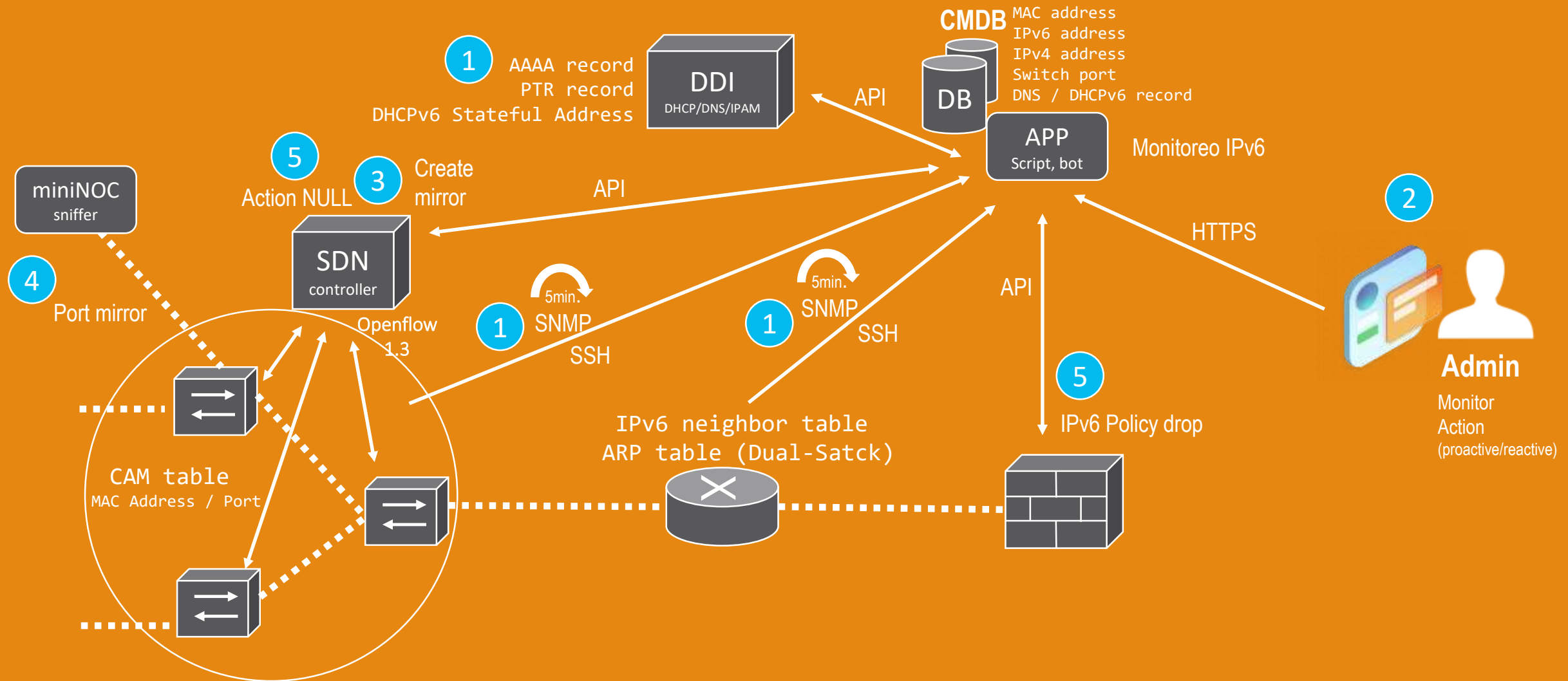
2001:1210:50A:2548:5ABC:AECB:FD5A:E14/64

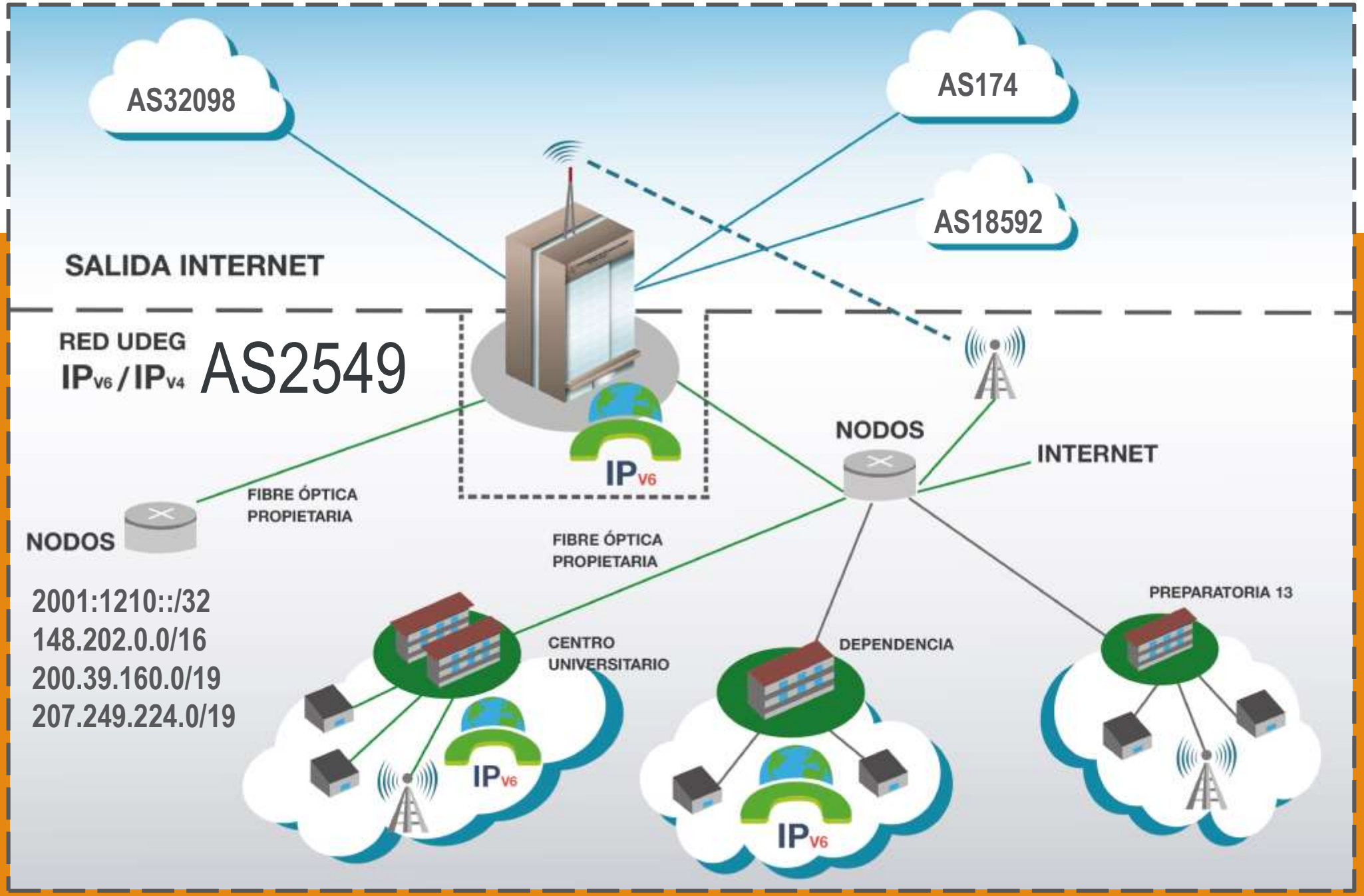
REUNIÓN DE OPERADORES DE REDES MÉXICO

¿ADMIN VS. DIRECCIONES IPv6 NO PREDECIBLES?

1. Escenario IPv6 neighbors

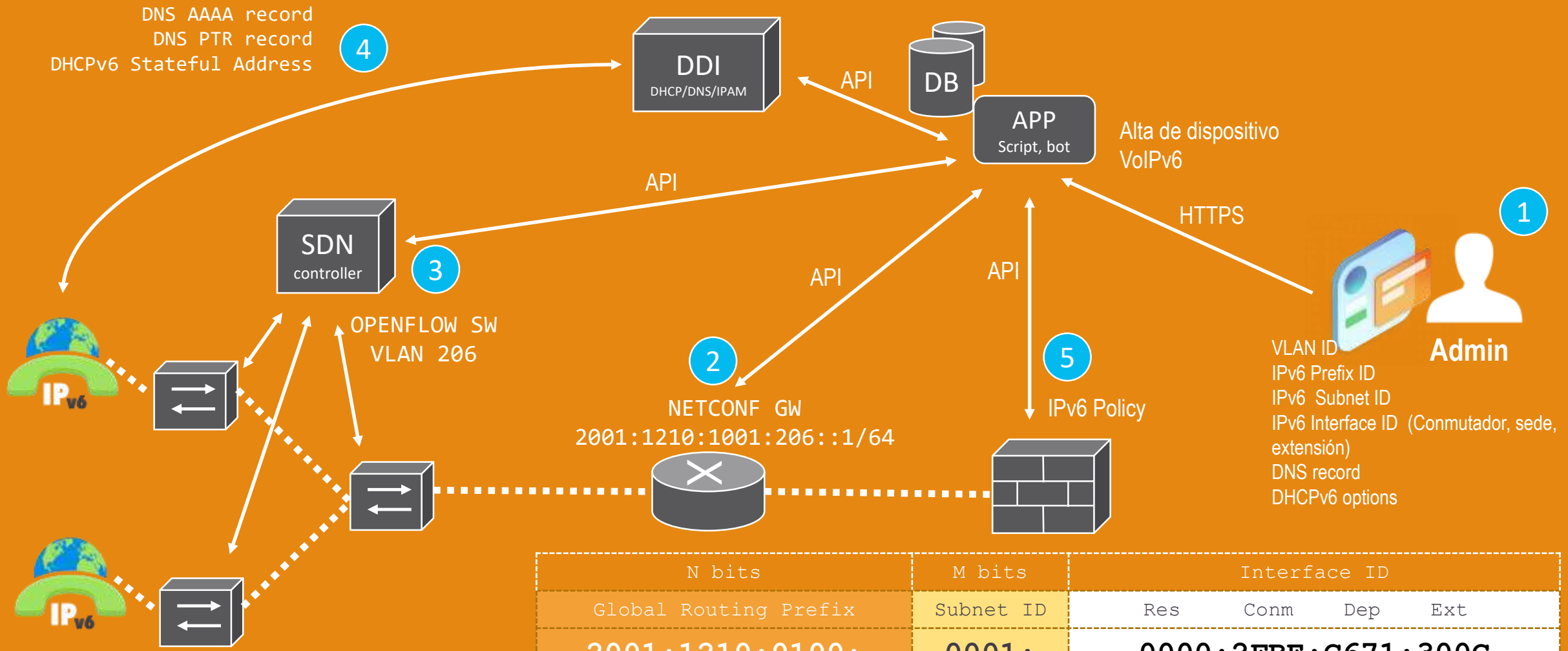
REUNIÓN DE OPERADORES DE REDES MÉXICO




AS32098
AS174
AS18592
SALIDA INTERNET
RED UDEG
IPV6 / IPV4
AS2549
IPV6
NODOS
INTERNET
FIBRE ÓPTICA
PROPIETARIA
NODOS
FIBRE ÓPTICA
PROPIETARIA
2001:1210::/32
148.202.0.0/16
200.39.160.0/19
207.249.224.0/19
CENTRO
UNIVERSITARIO
IPV6
DEPENDENCIA
IPV6
PREPARATORIA 13

2. Escenario VoIPv6

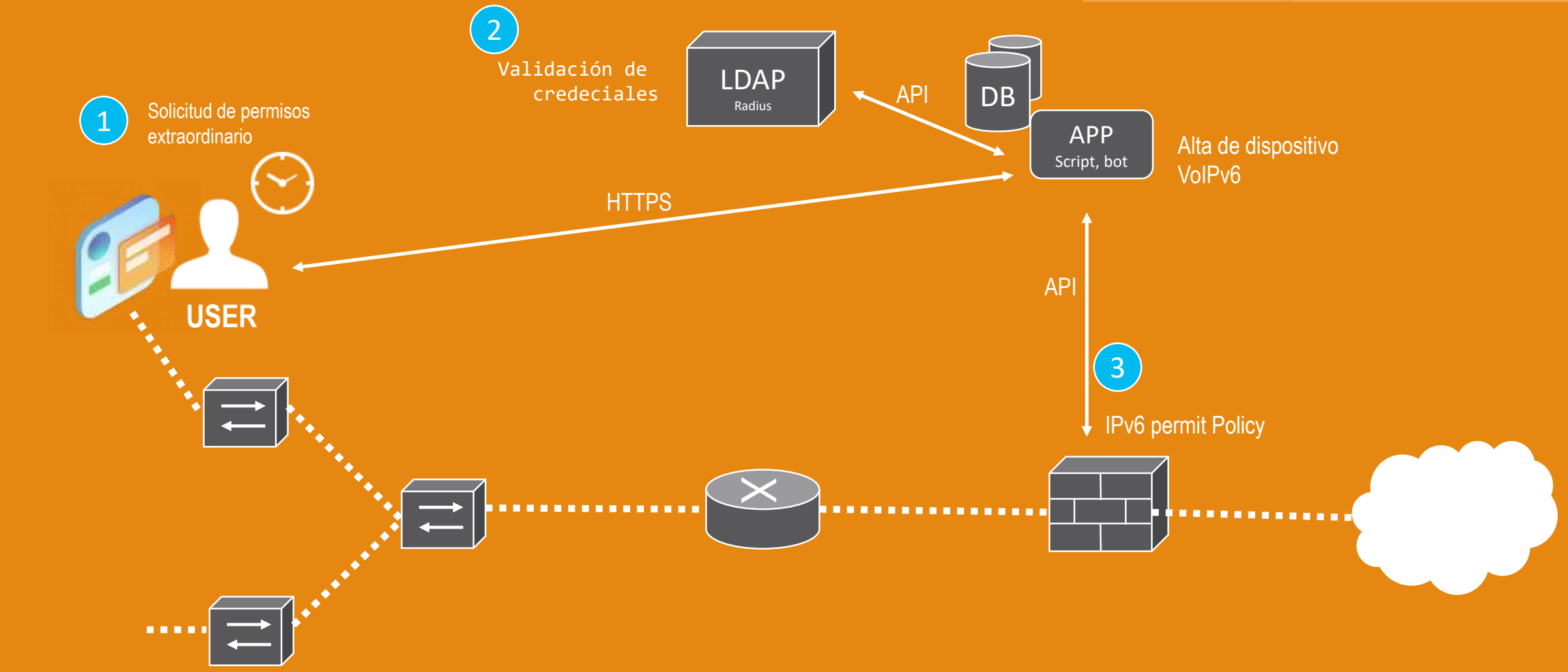
REUNIÓN DE OPERADORES DE REDES MÉXICO



N bits	M bits	Interface ID
Global Routing Prefix	Subnet ID	Res Conm Dep Ext
2001:1210:0100:	0001:	0000:2FBE:C671:300C

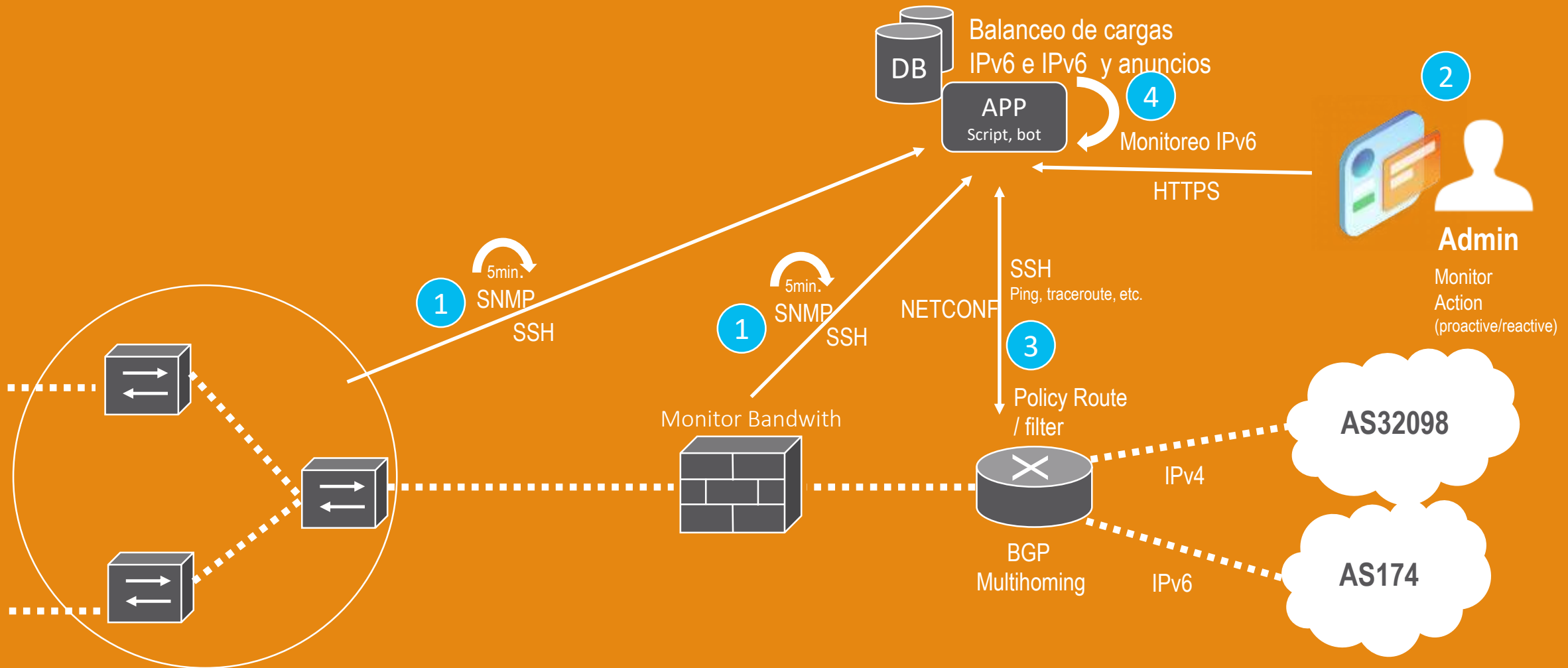
3. Escenario Firewall

permit policy



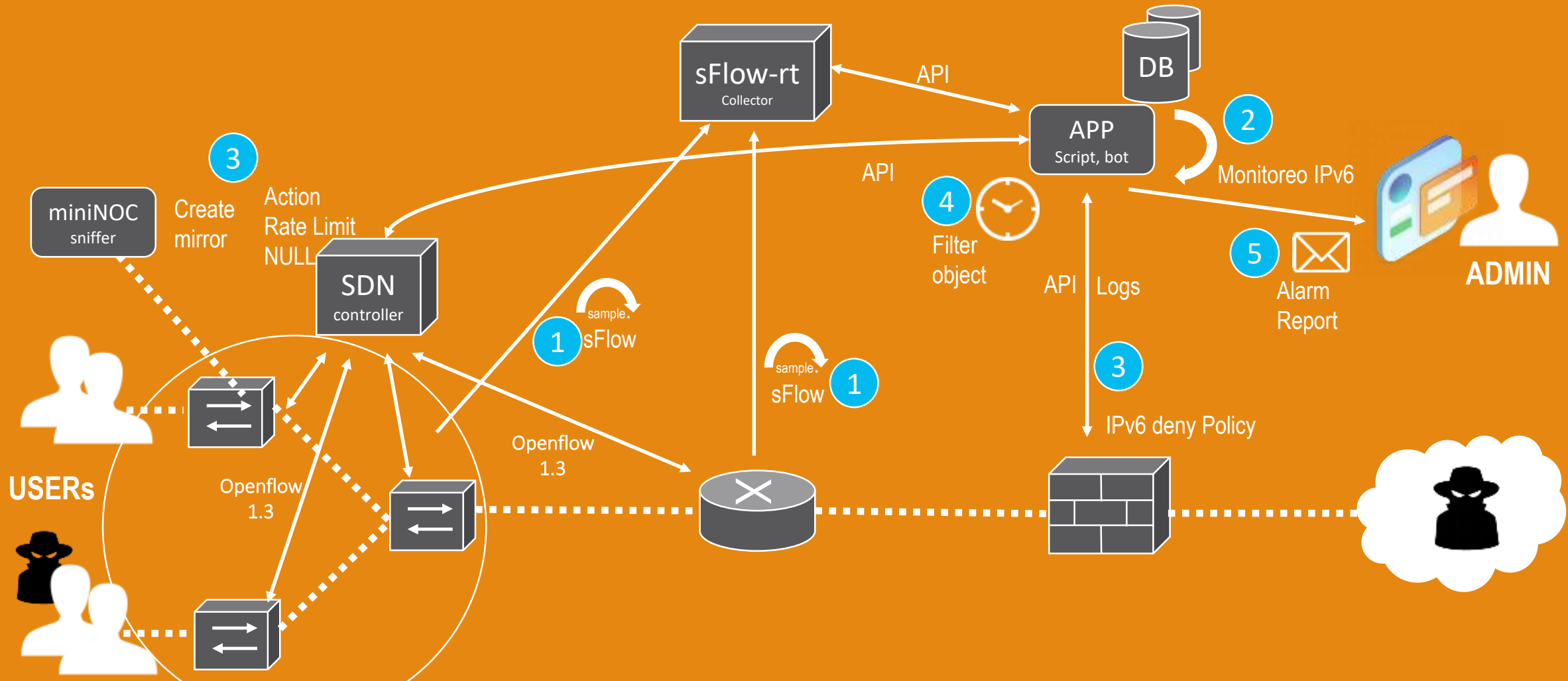
4. Escenario WAN

REUNIÓN DE OPERADORES DE REDES MÉXICO



5. Escenario Firewall
Attacks (DDoS, Virus, etc.)

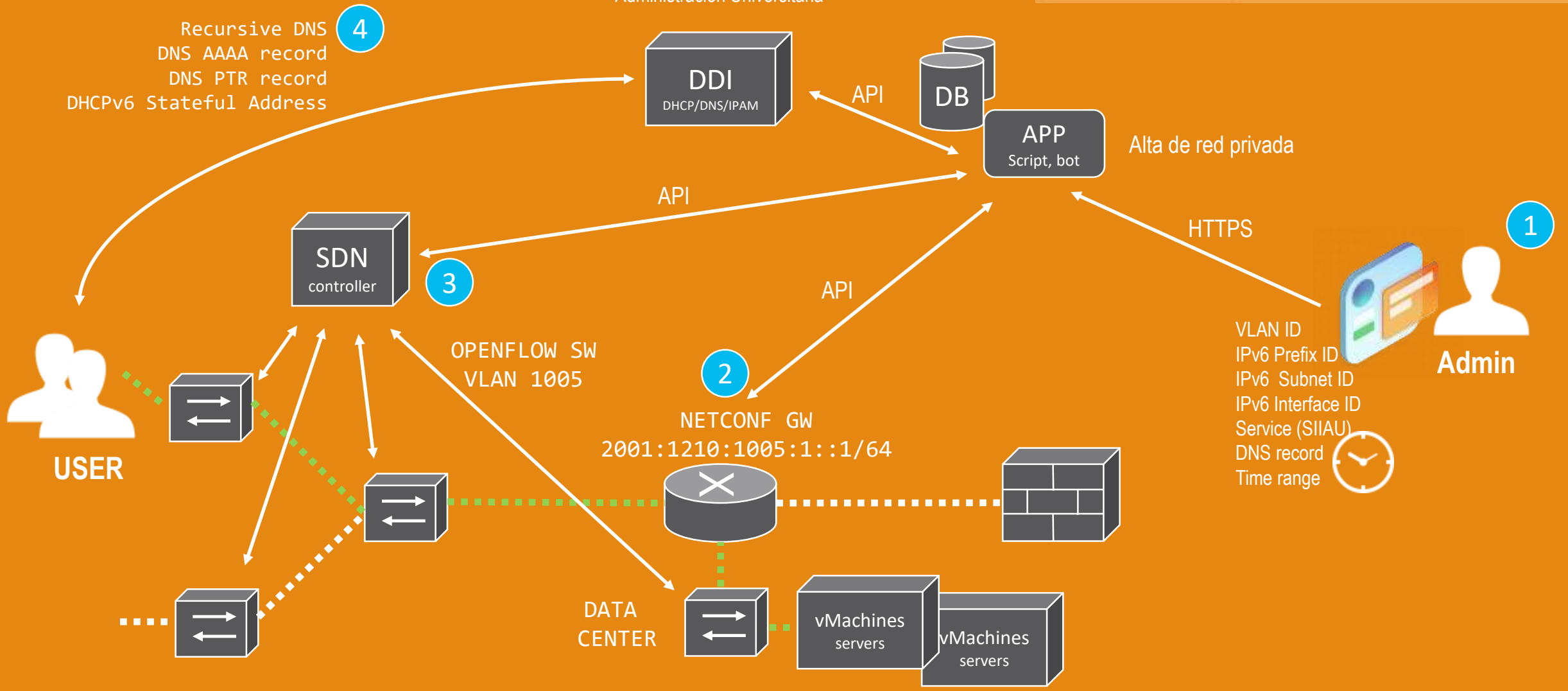
REUNIÓN DE OPERADORES DE REDES MÉXICO



6. Escenario ERP (SIIAU)

REUNIÓN DE OPERADORES DE REDES MÉXICO

Sistema Integral de Información y Administración Universitaria



¡GRACIAS!

REUNIÓN DE OPERADORES DE REDES MÉXICO

UNIVERSIDAD DE GUADALAJARA
Red Universitaria e Institución Benemérita de Jalisco

CGTI
COORDINACIÓN GENERAL DE TECNOLOGÍAS DE INFORMACIÓN

JAIME OLMOS DE LA CRUZ
RESPONSABLE DEL NOC-UDEG
HTTP://OLMOSv6.BLOGSPOT.MX/
HTTP://WWW.IPv6.UDG.MX
HTTP://IPv6TEST.UDG.MX
JAIME@NOC.UDG.MX
@OLMOSV6