AMRES
Serbian Academic Network

BELGRADE SECURITY WORKSHOP 2015

IP(v6) security

Matěj Grégr

Brno University of Technology, Faculty of Information Technology

Slides adapted from Ing. Tomáš Podermański

GÉANT

What is IP security?

- Encryption?
- Authentication?
- Authorization?
- Surveillance?
- Protection against forgery?

- What should be secure?
  - Routing protocols?
  - Address configuration?
  - Data delivery?

IPv4 – address autoconfiguration

No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

Autoconfiguration & neighbor discovery

DHCP

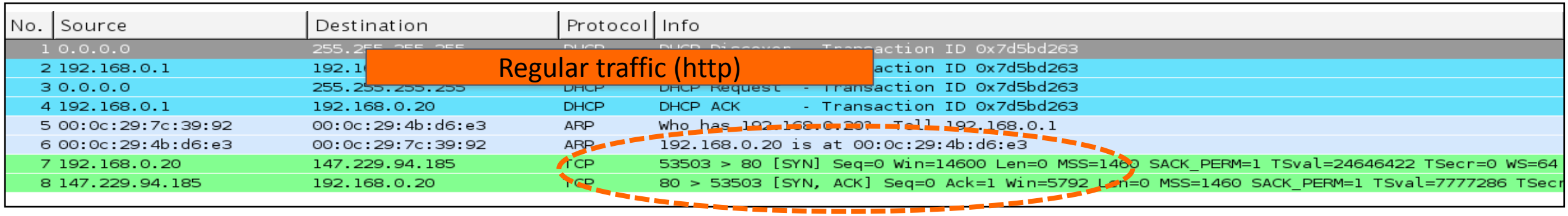
No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

Autoconfiguration & neighbor discovery

No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

ARP

Autoconfiguration & neighbor discovery



Importance of first hop security

- “Stealing” IP address assigned to another device
- Source IP address spoofing
- Source MAC address spoofing
- ARP poisoning

- Rogue DHCP server
  - **Trojan.Flush.M,**
  - **Trojan:W32/DNSChanger**

- The trend is to build and operate “flat” networks
- 2 or 4 C-blocks joined into one subnet

First hop security in IPv4 ①

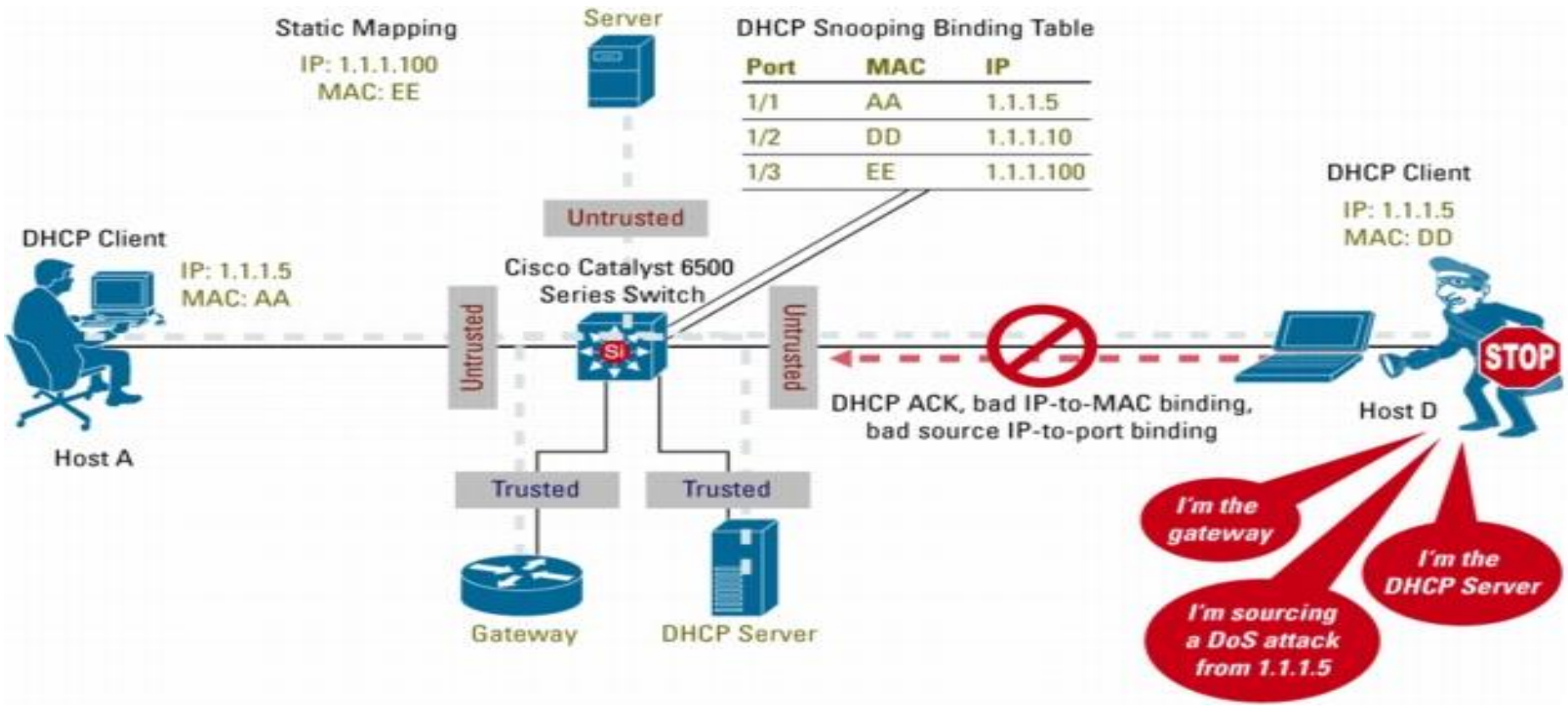
- Port security
  - Only pre-configured MAC addresses are allowed
  - Limit number of MAC addresses per port
  - Protection against MAC flooding

```
S2#
S2#show port-security int fa0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 2
Total MAC Addresses        : 2
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 2
Last Source Address:Vlan   : 0201.0000.0000:30
Security Violation Count   : 0

S2#show port-security int fa0/18 addr
            Secure Mac Address Table
------------------------------------------------------------------------
Vlan    Mac Address       Type                          Ports   Remaining Age
                                                                  (mins)
----    -----------       ----                          -----   -------------
  30    0026.b97f.751e    SecureSticky                  Fa0/18        -
  30    0201.0000.0000    SecureSticky                  Fa0/18        -
------------------------------------------------------------------------
Total Addresses: 2
```

First hop security in IPv4 ②

- DHCP snooping
  - Allows client access only if they obtain address from DHCP server



First hop security in IPv4 ③

- ARP protect
  - Take advantage of DHCP snooping database
  - Protect against MAC spoofing

- IP lockdown
  - Take advantage of DHCP snooping database
  - Protect against IP spoofing

First hop security in IPv4 - summary

- Port security + DHCP snooping + ARP protect + IP lockdown
- Only clients allowed on DHCP server are allowed to access network
- Protect against:
  - attackers
  - misconfiguration
  - faulty network card drivers
  - Worms/Viruses

IPv6

- Different autoconfiguration methods
  - Stateless address autoconfiguration
  - DHCPv6

- Different address assignment
- Interface is allowed to have more IPv6 addresses

Autoconfiguration & neighbor discovery

No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

- IPv6 – DAD, RS/RA, DHCPv6, MLDv2, ND

No.	Source	Destination	Protocol	Info
1	::	ff02::16	ICMPv6	Multicast Listener Report Message v2
2	::	ff02::1:ff4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3
3	fe80::20c:29ff:fe4b:d6e3	ff02::2	ICMPv6	Router Solicitation from 00:0c:29:4b:d6:e3
4	fe80::a:39	ff02::1	ICMPv6	Router Advertisement from 00:0c:29:7c:39:92
5	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Solicit XID: 0x8d6417 CID: 000100011550b198000c294bd6e3
6	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Advertise XID: 0x8d6417 IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b19800
7	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Request XID: 0xad993c CID: 000100011550b198000c294bd6e3 IAA: fd00:b0b0:bebe::f8ca:5391:b4
8	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Reply XID: 0xad993c IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000c294
9	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
10	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
11	::	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2
12	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3 from 00:0c:29:7c:39:92
13	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Advertisement fe80::20c:29ff:fe4b:d6e3 (sol)
14	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
15	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Solicitation for fe80::a:46 from 00:0c:29:4b:d6:e3
16	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Advertisement fe80::a:46 (rtr, sol)
17	fd00:b0b0:bebe::f8ca:539	2001:67c:1220:efff::b	TCP	44423 > 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=24641428 TSecr=0 WS=64
18	fe80::a:46	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 from 00:0c:29:7c:39:92
19	fd00:b0b0:bebe::f8ca:539	fe80::a:46	ICMPv6	Neighbor Advertisement fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 (sol, ovr) is at 00:0c:29:4b:c
20	2001:67c:1220:efff::b	fd00:b0b0:bebe::f8ca:539	TCP	80 > 44423 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 SACK_PERM=1 TSval=7772697 TSecr

Autoconfiguration & neighbor discovery

No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

- IPv6 – DAD, RS/RA, DHCPv6, MLDv2, ND

No.	Source	Destination	Protocol	Info
1	::		ICMPv6	Multicast Listener Report Message v2
2	::		ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3
3	fe80::20c:29ff:fe4b:d6e3	ff02::2	ICMPv6	Router Solicitation from 00:0c:29:4b:d6:e3
4	fe80::a:39	ff02::1	ICMPv6	Router Advertisement from 00:0c:29:7c:39:92
5	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Solicit XID: 0x8d6417 CID: 000100011550b198000c294bd6e3
6	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Advertise XID: 0x8d6417 IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b19800
7	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Request XID: 0xad993c CID: 000100011550b198000c294bd6e3 IAA: fd00:b0b0:bebe::f8ca:5391:b4
8	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Reply XID: 0xad993c IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000c294
9	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
10	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
11	::	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2
12	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3 from 00:0c:29:7c:39:92
13	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Advertisement fe80::20c:29ff:fe4b:d6e3 (sol)
14	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
15	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Solicitation for fe80::a:46 from 00:0c:29:4b:d6:e3
16	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Advertisement fe80::a:46 (rtr, sol)
17	fd00:b0b0:bebe::f8ca:539	2001:67c:1220:efff::b	TCP	44423 > 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=24641428 TSecr=0 WS=64
18	fe80::a:46	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 from 00:0c:29:7c:39:92
19	fd00:b0b0:bebe::f8ca:539	fe80::a:46	ICMPv6	Neighbor Advertisement fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 (sol, ovr) is at 00:0c:29:4b:c
20	2001:67c:1220:efff::b	fd00:b0b0:bebe::f8ca:539	TCP	80 > 44423 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 SACK_PERM=1 TSval=7772697 TSecr

MLDv2

G: ff02::1:ff4b:d6e3

G: ff02::1:ff4b:d6e3

Autoconfiguration IPv4 x IPv6

No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

- IPv6 – DAD, RS/RA, DHCPv6, MLDv2, ND

No.	Source	Destination	Protocol	Info
1	::	ff[illegible]	ICMPv6	Multicast Listener Report Message v2
2	::	ff[illegible]	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3
3	fe80::20c:29ff:fe4b:d6e3	ff02::2	ICMPv6	Router Solicitation from 00:0c:29:4b:d6:e3
4	fe80::a:39	ff02::1	ICMPv6	Router Advertisement from 00:0c:29:7c:39:92
5	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Solicit XID: 0x8d6417 CID: 000100011550b198000c294bd6e3
6	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Advertise XID: 0x8d6417 IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b19800
7	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Request XID: 0xad993c CID: 000100011550b198000c294bd6e3 IAA: fd00:b0b0:bebe::f8ca:5391:b4
8	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Reply XID: 0xad993c IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000c294
9	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
10	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
11	::	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2
12	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3 from 00:0c:29:7c:39:92
13	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Advertisement fe80::20c:29ff:fe4b:d6e3 (sol)
14	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
15	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Solicitation for fe80::a:46 from 00:0c:29:4b:d6:e3
16	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Advertisement fe80::a:46 (rtr, sol)
17	fd00:b0b0:bebe::f8ca:539	2001:67c:1220:efff::b	TCP	44423 > 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=24641428 TSecr=0 WS=64
18	fe80::a:46	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 from 00:0c:29:7c:39:92
19	fd00:b0b0:bebe::f8ca:539	fe80::a:46	ICMPv6	Neighbor Advertisement fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 (sol, ovr) is at 00:0c:29:4b:d
20	2001:67c:1220:efff::b	fd00:b0b0:bebe::f8ca:539	TCP	80 > 44423 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 SACK_PERM=1 TSval=7772697 TSecr

DAD

Autoconfiguration IPv4 x IPv6

No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

- IPv6 – DAD, RS/RA, DHCPv6, MLDv2, ND

No.	Source	Destination	Protocol	Info
1	::	ff02::16	ICMPv6	Multicast Listener Report Message v2
2	::	ff02::1:ff4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3
3	fe80::20c:29ff:fe4b:d6e3	[illegible]	ICMPv6	Router Solicitation from 00:0c:29:4b:d6:e3
4	fe80::a:39	[illegible]	ICMPv6	Router Advertisement from 00:0c:29:7c:39:92
5	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Solicit XID: 0x8d6417 CID: 000100011550b198000c294bd6e3
6	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Advertise XID: 0x8d6417 IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b19800
7	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Request XID: 0xad993c CID: 000100011550b198000c294bd6e3 IAA: fd00:b0b0:bebe::f8ca:5391:b4
8	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Reply XID: 0xad993c IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000c294
9	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
10	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
11	::	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2
12	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3 from 00:0c:29:7c:39:92
13	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Advertisement fe80::20c:29ff:fe4b:d6e3 (sol)
14	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
15	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Solicitation for fe80::a:46 from 00:0c:29:4b:d6:e3
16	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Advertisement fe80::a:46 (rtr, sol)
17	fd00:b0b0:bebe::f8ca:539	2001:67c:1220:efff::b	TCP	44423 > 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=24641428 TSecr=0 WS=64
18	fe80::a:46	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 from 00:0c:29:7c:39:92
19	fd00:b0b0:bebe::f8ca:539	fe80::a:46	ICMPv6	Neighbor Advertisement fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 (sol, ovr) is at 00:0c:29:4b:c
20	2001:67c:1220:efff::b	fd00:b0b0:bebe::f8ca:539	TCP	80 > 44423 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 SACK_PERM=1 TSval=7772697 TSecr

SLAAC

Autoconfiguration IPv4 x IPv6

No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

- IPv6 – DAD, RS/RA, DHCPv6, MLDv2, ND

No.	Source	Destination	Protocol	Info
1	::	ff02::16	ICMPv6	Multicast Listener Report Message v2
2	::	ff02::1:ff4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3
3	fe80::20c:29ff:fe4b:d6e3	ff02::2	ICMPv6	Router Solicitation from 00:0c:29:4b:d6:e3
4	fe80::a:39	ff02::1	ICMPv6	Router Advertisement from 00:0c:29:7c:39:92
5	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Solicit XID: 0x8d6417 CID: 000100011550b198000c294bd6e3
6	fe80::20c:29ff:fe7c:3992	f	DHCPv6	Advertise XID: 0x8d6417 IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000
7	fe80::20c:29ff:fe4b:d6e3	f	DHCPv6	Request XID: 0xad993c CID: 000100011550b198000c294bd6e3 IAA: fd00:b0b0:bebe::f8ca:5391:b4
8	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Reply XID: 0xad993c IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000c294
9	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
10	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
11	::	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2
12	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3 from 00:0c:29:7c:39:92
13	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Advertisement fe80::20c:29ff:fe4b:d6e3 (sol)
14	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
15	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Solicitation for fe80::a:46 from 00:0c:29:4b:d6:e3
16	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Advertisement fe80::a:46 (rtr, sol)
17	fd00:b0b0:bebe::f8ca:539	2001:67c:1220:efff::b	TCP	44423 > 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=24641428 TSecr=0 WS=64
18	fe80::a:46	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 from 00:0c:29:7c:39:92
19	fd00:b0b0:bebe::f8ca:539	fe80::a:46	ICMPv6	Neighbor Advertisement fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 (sol, ovr) is at 00:0c:29:4b:c
20	2001:67c:1220:efff::b	fd00:b0b0:bebe::f8ca:539	TCP	80 > 44423 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 SACK_PERM=1 TSval=7772697 TSecr

DHCPv6

Autoconfiguration IPv4 x IPv6

No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

- IPv6 – DAD, RS/RA, DHCPv6, MLDv2, ND

No.	Source	Destination	Protocol	Info
1	::	ff02::16	ICMPv6	Multicast Listener Report Message v2
2	::	ff02::1:ff4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3
3	fe80::20c:29ff:fe4b:d6e3	ff02::2	ICMPv6	Router Solicitation from 00:0c:29:4b:d6:e3
4	fe80::a:39	ff02::1	ICMPv6	Router Advertisement from 00:0c:29:7c:39:92
5	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Solicit XID: 0x8d6417 CID: 000100011550b198000c294bd6e3
6	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Advertise XID: 0x8d6417 IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b19800
7	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Request XID: 0xad993c CID: 000100011550b198000c294bd6e3 IAA: fd00:b0b0:bebe::f8ca:5391:b4
8	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Reply XID: 0xad993c IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000c294
9	fe80::20c:29ff:fe4b:d6e3		ICMPv6	Multicast Listener Report Message v2
10	fe80::20c:29ff:fe4b:d6e3		ICMPv6	Multicast Listener Report Message v2
11	::	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2
12	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3 from 00:0c:29:7c:39:92
13	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Advertisement fe80::20c:29ff:fe4b:d6e3 (sol)
14	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
15	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Solicitation for fe80::a:46 from 00:0c:29:4b:d6:e3
16	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Advertisement fe80::a:46 (rtr, sol)
17	fd00:b0b0:bebe::f8ca:539	2001:67c:1220:efff::b	TCP	44423 > 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=24641428 TSecr=0 WS=64
18	fe80::a:46	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 from 00:0c:29:7c:39:92
19	fd00:b0b0:bebe::f8ca:539	fe80::a:46	ICMPv6	Neighbor Advertisement fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 (sol, ovr) is at 00:0c:29:4b:c
20	2001:67c:1220:efff::b	fd00:b0b0:bebe::f8ca:539	TCP	80 > 44423 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 SACK_PERM=1 TSval=7772697 TSecr

MLDv2

G: ff02::1:ffb0:5ec2

G: ff02::1:ffb0:5ec2

Autoconfiguration IPv4 x IPv6

No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

- IPv6 – DAD, RS/RA, DHCPv6, MLDv2, ND

No.	Source	Destination	Protocol	Info
1	::	ff02::16	ICMPv6	Multicast Listener Report Message v2
2	::	ff02::1:ff4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3
3	fe80::20c:29ff:fe4b:d6e3	ff02::2	ICMPv6	Router Solicitation from 00:0c:29:4b:d6:e3
4	fe80::a:39	ff02::1	ICMPv6	Router Advertisement from 00:0c:29:7c:39:92
5	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Solicit XID: 0x8d6417 CID: 000100011550b198000c294bd6e3
6	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Advertise XID: 0x8d6417 IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b19800
7	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Request XID: 0xad993c CID: 000100011550b198000c294bd6e3 IAA: fd00:b0b0:bebe::f8ca:5391:b4
8	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Reply XID: 0xad993c IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000c294
9	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
10	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
11	::	[illegible]	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2
12	fe80::a:46	[illegible]:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3 from 00:0c:29:7c:39:92
13	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Advertisement fe80::20c:29ff:fe4b:d6e3 (sol)
14	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
15	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Solicitation for fe80::a:46 from 00:0c:29:4b:d6:e3
16	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Advertisement fe80::a:46 (rtr, sol)
17	fd00:b0b0:bebe::f8ca:539	2001:67c:1220:efff::b	TCP	44423 > 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=24641428 TSecr=0 WS=64
18	fe80::a:46	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 from 00:0c:29:7c:39:92
19	fd00:b0b0:bebe::f8ca:539	fe80::a:46	ICMPv6	Neighbor Advertisement fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 (sol, ovr) is at 00:0c:29:4b:d
20	2001:67c:1220:efff::b	fd00:b0b0:bebe::f8ca:539	TCP	80 > 44423 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 SACK_PERM=1 TSval=7772697 TSecr

ND

Autoconfiguration & neighbor discovery

No.	Source	Destination	Protocol	Info
1	0.0.0.0	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0x7d5bd263
2	192.168.0.1	192.168.0.20	DHCP	DHCP Offer - Transaction ID 0x7d5bd263
3	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x7d5bd263
4	192.168.0.1	192.168.0.20	DHCP	DHCP ACK - Transaction ID 0x7d5bd263
5	00:0c:29:7c:39:92	00:0c:29:4b:d6:e3	ARP	Who has 192.168.0.20? Tell 192.168.0.1
6	00:0c:29:4b:d6:e3	00:0c:29:7c:39:92	ARP	192.168.0.20 is at 00:0c:29:4b:d6:e3
7	192.168.0.20	147.229.94.185	TCP	53503 > 80 [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM=1 TSval=24646422 TSecr=0 WS=64
8	147.229.94.185	192.168.0.20	TCP	80 > 53503 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=7777286 TSecr

- IPv6 – DAD, RS/RA, DHCPv6, MLDv2, ND

No.	Source	Destination	Protocol	Info
1	::	ff02::16	ICMPv6	Multicast Listener Report Message v2
2	::	ff02::1:ff4b:d6e3	ICMPv6	Neighbor Solicitation for fe80::20c:29ff:fe4b:d6e3
3	fe80::20c:29ff:fe4b:d6e3	ff02::2	ICMPv6	Router Solicitation from 00:0c:29:4b:d6:e3
4	fe80::a:39	ff02::1	ICMPv6	Router Advertisement from 00:0c:29:7c:39:92
5	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Solicit XID: 0x8d6417 CID: 000100011550b198000c294bd6e3
6	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Advertise XID: 0x8d6417 IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b19800
7	fe80::20c:29ff:fe4b:d6e3	ff02::1:2	DHCPv6	Request XID: 0xad993c CID: 000100011550b198000c294bd6e3 IAA: fd00:b0b0:bebe::f8ca:5391:b4
8	fe80::20c:29ff:fe7c:3992	fe80::20c:29ff:fe4b:d6e3	DHCPv6	Reply XID: 0xad993c IAA: fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 CID: 000100011550b198000c294
9	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
10	fe80::20c:29ff:fe			t Listener Report Message v2
11	::			Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2
12	fe80::a:46			Solicitation for fe80::20c:29ff:fe4b:d6e3 from 00:0c:29:7c:39:92
13	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Advertisement fe80::20c:29ff:fe4b:d6e3 (sol)
14	fe80::20c:29ff:fe4b:d6e3	ff02::16	ICMPv6	Multicast Listener Report Message v2
15	fe80::20c:29ff:fe4b:d6e3	fe80::a:46	ICMPv6	Neighbor Solicitation for fe80::a:46 from 00:0c:29:4b:d6:e3
16	fe80::a:46	fe80::20c:29ff:fe4b:d6e3	ICMPv6	Neighbor Advertisement fe80::a:46 (rtr, sol)
17	fd00:b0b0:bebe::f8ca:539	2001:67c:1220:efff::b	TCP	44423 > 80 [SYN] Seq=0 Win=14400 Len=0 MSS=1440 SACK_PERM=1 TSval=24641428 TSecr=0 WS=64
18	fe80::a:46	ff02::1:ffb0:5ec2	ICMPv6	Neighbor Solicitation for fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 from 00:0c:29:7c:39:92
19	fd00:b0b0:bebe::f8ca:539	fe80::a:46	ICMPv6	Neighbor Advertisement fd00:b0b0:bebe::f8ca:5391:b4b0:5ec2 (sol, ovr) is at 00:0c:29:4b:d
20	2001:67c:1220:efff::b	fd00:b0b0:bebe::f8ca:539	TCP	80 > 44423 [SYN, ACK] Seq=0 Ack=1 Win=5712 Len=0 MSS=1440 SACK_PERM=1 TSval=7772607 TSecr

Regular traffic (http)

DAD – DoS attack

- Step 1, **Host**: Can I use IPv6 address AA:BB::CC
- Step 2, **Attacker:** No the address is used
- Step 3, **Host:** Can I use IPv6 address AA:BB::DD
- Step 4, **Attacker:** No the address is used
- …
- Existing tool from thc-toolkit (http://thc.org/thc-ipv6/):

```
# ./dos-new-ipv6 eth0
```

DAD – DoS attack

No.	Source	Destination	Info
1	::	ff02::1:ffca:426b	Neighbor Solicitation for fe80::2c40:10fa:40ca:426b
2	fe80::2c40:10fa:40ca:426b	ff02::2	Router Solicitation from 00:0c:29:49:49:ab
3	fe80::2c40:10fa:40ca:426b	ff02::16	Multicast Listener Report Message v2
4	fe80::2c40:10fa:40ca:426b	ff02::1	Neighbor Advertisement fe80::2c40:10fa:40ca:426b (ovr) is at 00:0c:56:4b:70:0c
5	fe80::3156:bb8f:9ebc:f653	ff02::16	Multicast Listener Report Message v2
6	fe80::a:39	ff02::1	Router Advertisement from 00:0c:29:7c:39:92
7	fe80::2c40:10fa:40ca:426b	ff02::1	Neighbor Advertisement fe80::2c40:10fa:40ca:426b (ovr) is at 00:0c:56:4b:70:0c
8	::	ff02::1:ffbc:f653	Neighbor Solicitation for fe80::3156:bb8f:9ebc:f653
9	fe80::3156:bb8f:9ebc:f653	ff02::16	Multicast Listener Report Message v2
10	fe80::3156:bb8f:9ebc:f653	ff02::1	Neighbor Advertisement fe80::3156:bb8f:9ebc:f653 (ovr) is at 00:0c:3c:6a:10:87
11	fe80::3156:bb8f:9ebc:f653	ff02::1	Neighbor Advertisement fe80::3156:bb8f:9ebc:f653 (ovr) is at 00:0c:3c:6a:10:87
12	fe80::ecc9:1f2:bc8b:d0e3	ff02::16	Multicast Listener Report Message v2
13	::	ff02::1:ff8b:d0e3	Neighbor Solicitation for fe80::ecc9:1f2:bc8b:d0e3
14	fe80::ecc9:1f2:bc8b:d0e3	ff02::16	Multicast Listener Report Message v2
15	fe80::ecc9:1f2:bc8b:d0e3	ff02::1	Neighbor Advertisement fe80::ecc9:1f2:bc8b:d0e3 (ovr) is at 00:0c:6b:3c:95:ee
16	fe80::ecc9:1f2:bc8b:d0e3	ff02::1	Neighbor Advertisement fe80::ecc9:1f2:bc8b:d0e3 (ovr) is at 00:0c:6b:3c:95:ee
17	fe80::41e1:b64c:848f:55fb	ff02::16	Multicast Listener Report Message v2
18	::	ff02::1:ff8f:55fb	Neighbor Solicitation for fe80::41e1:b64c:848f:55fb
19	fe80::41e1:b64c:848f:55fb	ff02::16	Multicast Listener Report Message v2
20	fe80::41e1:b64c:848f:55fb	ff02::1	Neighbor Advertisement fe80::41e1:b64c:848f:55fb (ovr) is at 00:0c:d3:0d:6a:63
21	fe80::41e1:b64c:848f:55fb	ff02::1	Neighbor Advertisement fe80::41e1:b64c:848f:55fb (ovr) is at 00:0c:d3:0d:6a:63
22	fe80::c8a:7e5b:c82d:a699	ff02::16	Multicast Listener Report Message v2
23	::	ff02::1:ff2d:a699	Neighbor Solicitation for fe80::c8a:7e5b:c82d:a699
24	fe80::c8a:7e5b:c82d:a699	ff02::1	Neighbor Advertisement fe80::c8a:7e5b:c82d:a699 (ovr) is at 00:0c:1d:bf:ac:f6
25	fe80::c8a:7e5b:c82d:a699	ff02::16	Multicast Listener Report Message v2
26	fe80::c8a:7e5b:c82d:a699	ff02::1	Neighbor Advertisement fe80::c8a:7e5b:c82d:a699 (ovr) is at 00:0c:1d:bf:ac:f6
27	fe80::cd3:bf52:8c6e:b1a4	ff02::16	Multicast Listener Report Message v2
28	::	ff02::1:ff6e:b1a4	Neighbor Solicitation for fe80::cd3:bf52:8c6e:b1a4
29	fe80::cd3:bf52:8c6e:b1a4	ff02::16	Multicast Listener Report Message v2

DAD – DoS attack

No.	Source	Destination	Info
1	::	ff02::1:ffca:426b	Neighbor Solicitation for fe80::2c40:10fa:40ca:426b
2	fe80::2c40:10fa:40ca:426b	ff02::2	Router Solicitation from 00:0c:29:49:49:ab
3	fe80::2c40:10fa:40ca:426b	ff02::16	Multicast Listener Report Message v2
4	fe80::2c40:10fa:40ca:426b	ff02::1	Neighbor Advertisement fe80::2c40:10fa:40ca:426b (ovr) is at 00:0c:56:4b:70:0c
5	fe80::3156:bb8f:9ebc:f653	ff02::16	Multicast Listener Report Message v2
6	fe80::a:39	ff02::1	Router Advertisement from 00:0c:29:7c:39:92
7	fe80::2c40:10fa:40ca:426b	ff02::1	Neighbor Advertisement fe80::2c40:10fa:40ca:426b (ovr) is at 00:0c:56:4b:70:0c
8	::	ff02::1:ffbc:f653	Neighbor Solicitation for fe80::3156:bb8f:9ebc:f653
9	fe80::3156:bb8f:9ebc:f653	ff02::16	Multicast Listener Report Message v2
10	fe80::3156:bb8f:9ebc:f653	ff02::1	Neighbor Advertisement fe80::3156:bb8f:9ebc:f653 (ovr) is at 00:0c:3c:6a:10:87
11	fe80::3156:bb8f:9ebc:f653	ff02::1	Neighbor Advertisement fe80::3156:bb8f:9ebc:f653 (ovr) is at 00:0c:3c:6a:10:87

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : domain.org
   Description . . . . . . . . . . . : Intel(R) PRO/1000 MT Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-49-49-AB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.0.119(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 3. května 2011 18:44:05
   Lease Expires . . . . . . . . . . : 4. května 2011 0:29:14
   Default Gateway . . . . . . . . . : fe80::a:39%11
                                       192.168.0.1
   DHCP Server . . . . . . . . . . . : 192.168.0.1
   DHCPv6 IAID . . . . . . . . . . . : 234884137
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-13-E7-A4-5F-00-0C-29-49-49-AB
   DNS Servers . . . . . . . . . . . : 192.168.0.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

29	fe80::cd3:bf52:8c6e:b1a4	ff02::16	Multicast Listener Report Message v2
30	fe80::cd3:bf52:8c6e:b1a4	ff02::1	Neighbor Advertisement fe80::cd3:bf52:8c6e:b1a4 (ovr) is at 00:0c:d3:dc:2c:aa

DAD – DoS attack

- Widows platform
  - Tries 5 attempts ant them gives up (DHCPv6, SLAAC)
- Linux
  - Depends on distribution – usually ignores DADs by default
- HP L3 switches (ProCurve platform)
  - Disables IPv6 address on the interface forever

- Result:
  - User is not able communicate over IPv6 network.

RA flood

- Flooding IPv6 hosts with Router Advertises
- thc-toolkit (http://thc.org/thc-ipv6/):

```
# ./flood_router6 eth0
```

- All Windows Vista/7/8 boxes will freeze
- Other platforms will have problems with IPv6 connectivity
- The problem is known for more than 3 years – no patch/update yet.
- More info:
  http://samsclass.info/ipv6/proj/flood-router6a.htm

Microsoft, Juniper urged to patch dangerous IPv6 DoS hole

Despite growing pressure from security experts, Microsoft and Juniper have so far refused to patch a dangerous hole that can freeze a Windows network in minutes.

By Julie Bort, Network World
May 03, 2011 05:26 PM ET

2 Comments Print + Briefcase What's this?

Security experts are urging Microsoft and Juniper to patch a year-old IPv6 vulnerability so dangerous it can freeze any Windows machine on a LAN in a matter of minutes.

Microsoft has downplayed the risk because the hole requires a physical connection to the wired LAN. Juniper says it has delayed a patch because the hole only affects a small number of its products and it wants the IETF to fix the protocol instead.

SEE IT YOURSELF: How to use a known IPv6 hole to fast-freeze a Windows network

The vulnerability was initially discovered in July 2010 by Marc Heuse, an IT security consultant in Berlin. He found that products from several vendors were vulnerable, including all recent versions of Windows, Cisco routers, Linux and Juniper's Netscreen. Cisco issued a patch in October 2010, and the Linux kernel has since been fixed as well. Microsoft and Juniper have acknowledged the vulnerability, but neither have committed to patches.

The hole is in a technology known as router advertisements, where routers broadcast their IPv6 addresses to help clients find and connect to an IPv6 subnet. The DoS attack involves

VIDEO

IPv6 Attack Tools

- **THC IPv6 Attack Toolkit** – parasite6, alive6, fake_router6, redir6, toobig6, detect-new-ip6, dos-new-ip6, fake_mld6, fake_mipv6, fake_advertiser6, smurf6, rsmurf6

  http://www.thc.org/thc-ipv6/

- **SI6 Networks' IPv6 Toolkit** – flow6, frag6, icmp6, jumbo6, na6, ni6, ns6, ra6, rd6, rs6, scan6, tcp6

  http://www.si6networks.com/tools/ipv6toolkit/

Abuse of IPv6 autoconfiguration

- More than 90% of devices supports dualstack
  - Most of them use autoconfiguration (SLAAC) to get IP address (MS Vista/7, Linux, Mac OS, iOS, BSD*)
- Steps to make an attack:
  - Setup attacker’s IP to act as a RA sender
  - Prepare a DHCPv6 server on the attacker's PC; as DNS servers provide attacker’s addresses
  - Modify the behavior of DNS server to return A or AAAA records for www.google.com, www.yahoo.com, etc. to your attacker’s address
  - Transparent proxy service allows attacker to modify content of webpages, …

VIDEO

It is not a problem!

IPv4 has very similar issues related to autoconfiguration. There is no difference between IPv6 and IPv4.

It is true, but …

First hop security in IPv4

	DHCP snooping
Rogue DHCP server	✔
ARP poisoning	
Forces users to use DHCP	
Source IPv4 address spoofing	
Source MAC address spoofing	
Require support on access port	✔

- IPv4 autoconfiguration = DHCP + protection on switches
  - **DHCP snooping**
    - **Blocking DHCP answers on access port**
    - **Building binding database (MAC-IP) related to access port**
  - **Dynamic ARP protection/ARP inspection**
    - MAC-IP address database based on DHCP leases
    - Checking content of ARP packets on client access port
  - **Dynamic lock down, IP source guard**
    - The MAC-IP database is used for inspection of client source MAC and IP address.

First hop security for IPv6

- SeND (RFC 3971, March 2005)
  - Based on cryptography CGA keys
  - Requires PKI infrastructure
    - How client obtains his own certificate?
  - Can **not** work with
    - Manually configured, EUI 64 and Privacy Extension addresses
- RA-Guard, PACL (RFC 6105, February 2011)
  - Dropping fake RA messages on access port (RA Snooping)
  - Can be easily avoided using fragmentation and extension headers (http://tools.ietf.org/html/draft-gont-v6ops-ra-guard-evasion-01)
- SAVI (draft-ietf-savi-*, divided into more drafts)
  - Complex solution including source addres validation
  - ND Inspection (Cisco devices) provides similar level of protection

First hop security for IPv6

Fragment reassembling or *undetermined traffic* option must be used (Cisco).

	RA-Guard	ACL/PACL	SAVI, ND inspection	SEND
Rogue DHCPv6 server		✔	✔	
Accidently rogue router advertise	✔	✔		✔
Intentional rouge router advertise				✔
ND cache poisoning			✔	✔
Source IPv6 address spoofing			✔	✔
DAD DOS attack			✔	
Neighbour cache overload			✔	
Source MAC address spoofing			✔	
Requires support on access switches	✔	✔	✔	
Requires support or configuration on client side				✔

Do we really need first hop security ?

- Fact: 15 years ago we did not have first hop security for IPv4 as well. We need more time while those features will be widely available for IPv6 (for good price).

but…

- Today we do not build networks that will be operated in 1998.
- Requirements on networks are extremely different than 15 years ago.
- **Today, we are building networks that should work for next 5 years!**

Cost of first hop security for IPv6

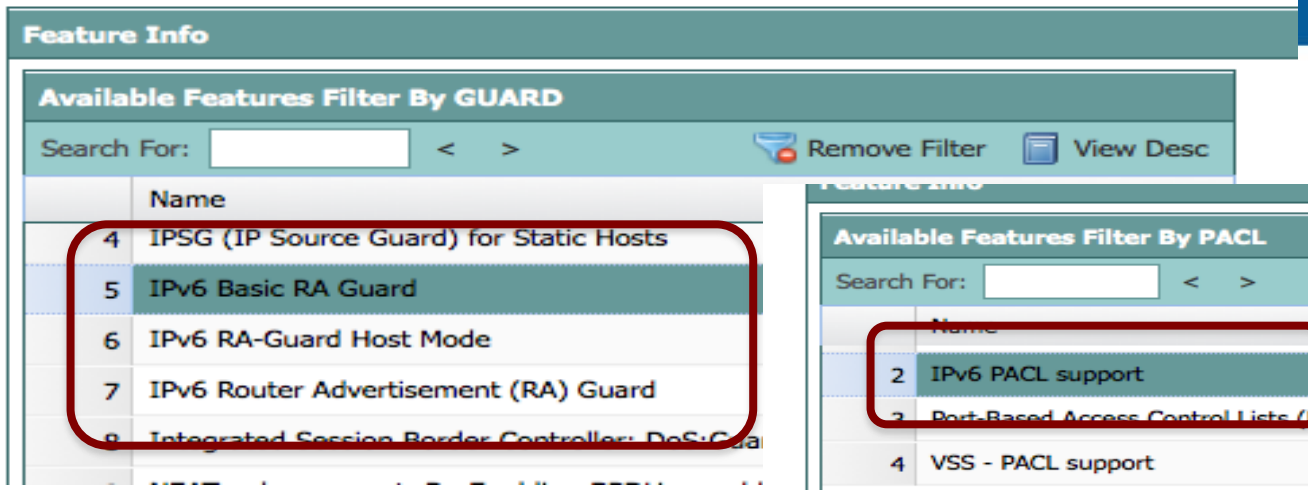
- Real example: access switches for 150 users 168 ports, 1Gb/s, non PoE

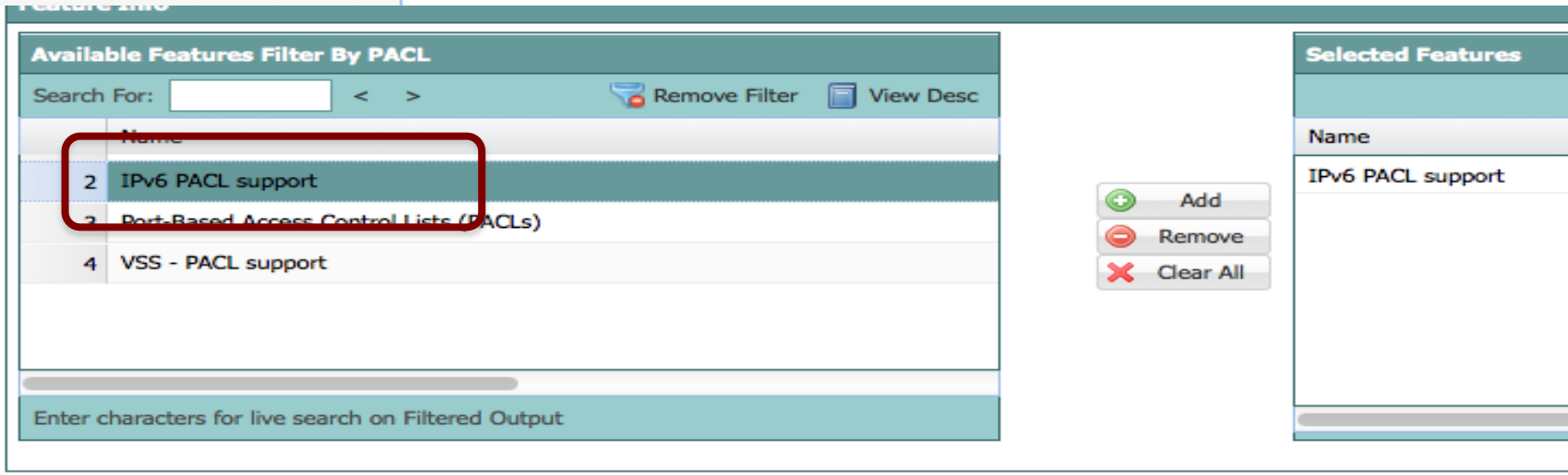
	price per port	RA guard	PACL	SAVI, ND inspection	DHCP snooping	ARP inspection, ARP protection	IP source guard, dynamic IP lockdown
1x HP 4208-96 vl Switch (J8775B) 3x HP 24-port Gig-T vl Module (J8768A)	**$58.90**				✔	✔	
1x HP 2910-48G al Switch (J9147A) 3x HP 2910-24G al Switch (J9145A)	**$96.23**				✔	✔	✔

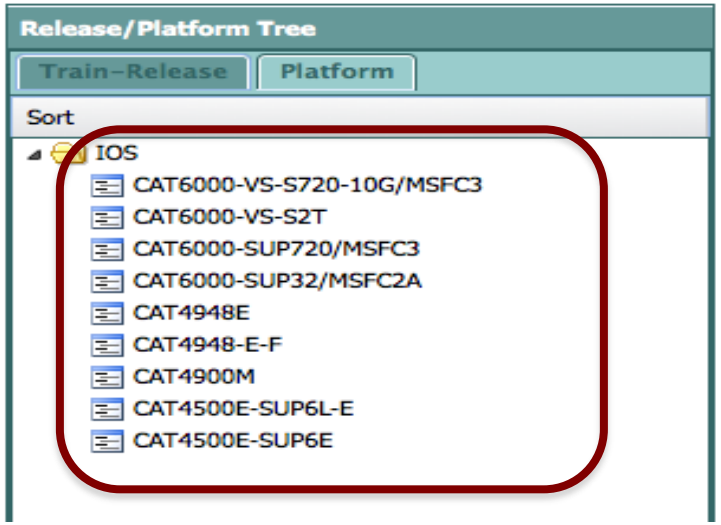
Prices taken from http://www.amazon.com/ (list prices)

Search by Feature | Search by Technology | Search by Software

Objective :
Find releases/platforms that support selected features.







How to mitigate impact of those attacs

- Setup an native connectivity into network
- Prefix monitoring and sending alerts
  - ramond - http://ramond.sourceforge.net/
  - rafixd - http://www.kame.net/
  - ndpmon - http://ndpmon.sourceforge.net/
  - scapy6 - http://hg.natisbad.org/scapy6/
- In many cases the only thing we can do today

Conclusion

- Deploying IPv6 can bring some new security threats
  - Rules applied for IPv4 are not applied for IPv6 by default
    - Firewall rustles, policies, DS, IPS, access policies
  - We should apply same security rules for both IPv4 and IPv6
- Unattended IPv6 traffic could be blocked, unused IPv6 services should be disabled
  - Transition techniques can bring a new risk (tunnels enabled by default)
- IPv6 enthusiasts are not responsible your security policy
  - In case of troubles you will be in trouble
- Consider environment you working in
  - Universities – more open, not attractive target
  - Enterprise – strict rules, high lever or risks

BELGRADE SECURITY WORKSHOP 2015