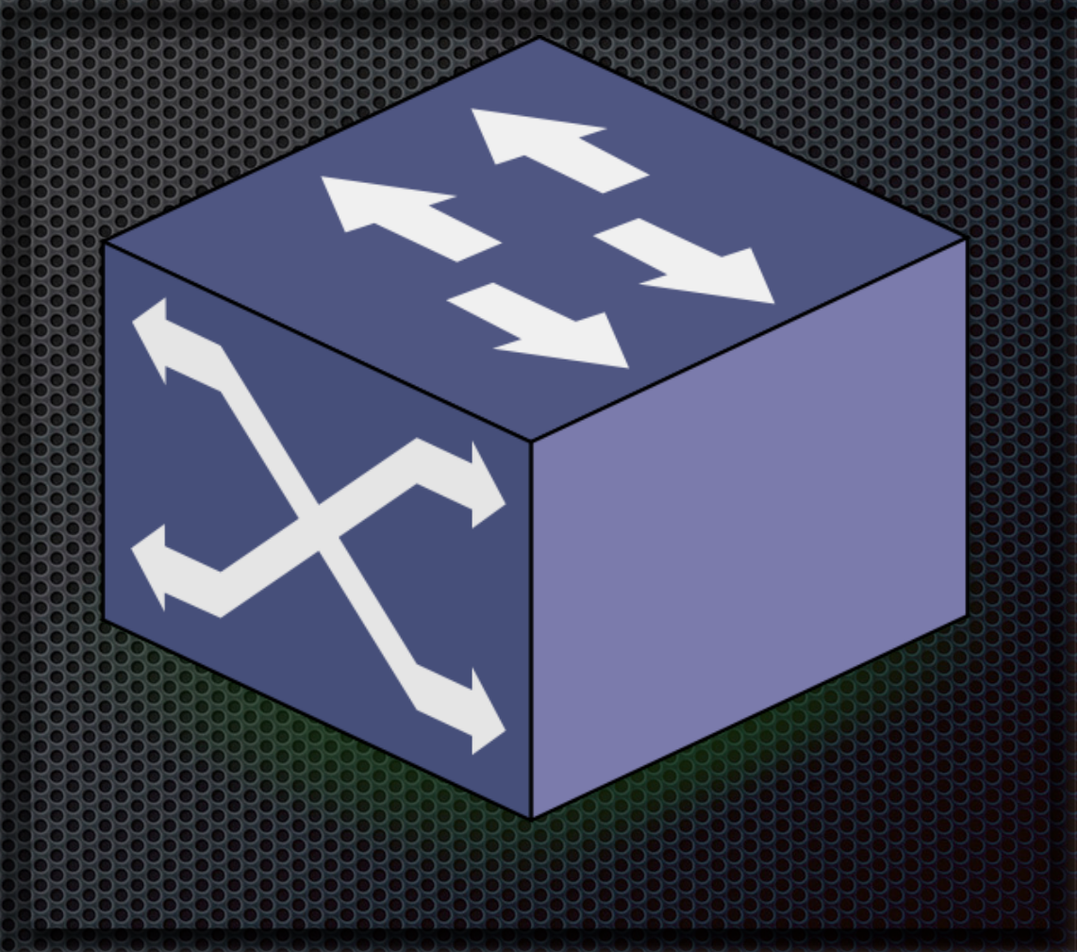
ARP Storm Project

Minimizing ARP traffic using OpenFlow

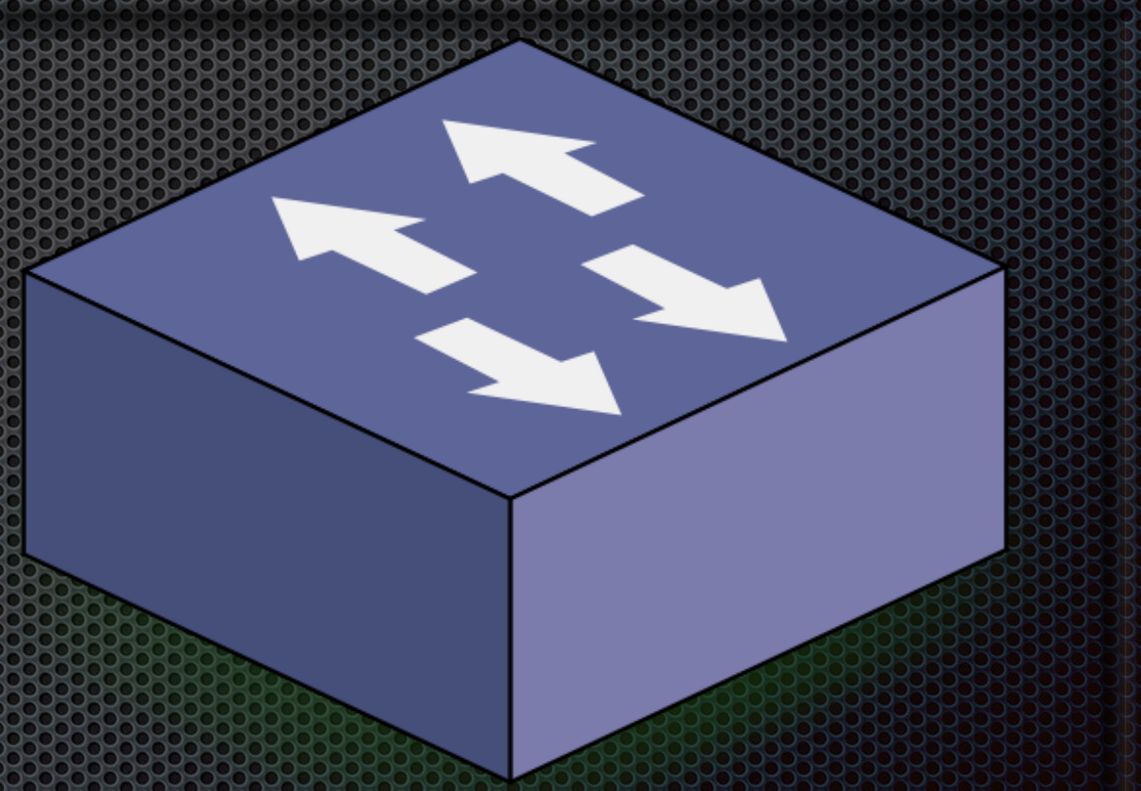
Hub

- Device for connecting multiple ethernet devices
- Operates at the physical layer (layer 1 of the OSI model)
- Rebroadcasting any incoming packet to all other ports
- Packet collisions are more frequent



Switch

- Considered more advanced than a Hub
- Operates at the data link layer (layer 2 of the OSI model)
- Creates a separate collision domain for each port
- Transmitting a received message only through the intended port



From Hub to Switch

- Maintain a mapping table between MACs and Ports
- Learn the ports packets arrive from
- In case destination has not seen yet, act like Hub (flood)
- In case destination already seen (stored in mapping table), resend packet on the specified port

Problem: ARP Storm

- In large networks, it can be expected to have nodes down
- ARP requests for IPs which are no longer in use
- This causes severe broadcast traffic in the network
- Many nodes process the packets and waste CPU cycles

47	2.75363500	Ubiquiti_2c:00:10	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.7.1
48	2.80194600	Ubiquiti_2c:ca:cc	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.50.1
49	2.82510400	Ubiquiti_2c:ca:d8	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.28.1
50	2.83491400	Ubiquiti_84:09:54	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.1.9
51	2.94478700	Ubiquiti_2c:ca:f0	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.10.1
52	3.00091900	Ubiquiti_8a:40:de	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.3.1
53	3.03280600	Ubiquiti_84:09:b5	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.1.8
54	3.12863500	Ubiquiti_2c:ca:f4	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.23.1
55	3.16212600	Ubiquiti_36:fb:1a	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.1.10
56	3.24772500	Ubiquiti_2c:ca:c8	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.47.1
57	3.38063800	Ubiquiti_8a:40:23	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.68.1
58	3.50781000	Ubiquiti_8a:43:b4	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.62.1
59	3.58463200	Ubiquiti_36:a9:70	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.67.1
60	3.66758300	Ubiquiti_36:f9:ff	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.57.1
61	3.68881200	Ubiquiti_2c:00:10	Broadcast	ARP	60	Who has 10.10.1.100? Tell 10.10.7.1
62	3.75357400	Ubiquiti_2c:00:10	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.7.1
63	3.80193200	Ubiquiti_2c:ca:cc	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.50.1
64	3.82625700	Ubiquiti_2c:ca:d8	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.28.1
65	3.94792200	Ubiquiti_2c:ca:f0	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.10.1
66	4.01579500	Ubiquiti_3e:2d:2a	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.9.1
67	4.03275200	Ubiquiti_84:09:b5	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.1.8
68	4.11931000	Ubiquiti_4a:b9:39	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.63.1
69	4.12857100	Ubiquiti_2c:ca:f4	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.23.1
70	4.16186500	Ubiquiti_36:fb:1a	Broadcast	ARP	60	Who has 10.10.1.25? Tell 10.10.1.10

Solution: ARP Proxy/Sponge

- Act as a “black hole” for ARP Requests
- Maintain a mapping table between IPs and MACs
- If a MAC for a given IP is yet unknown, flood
- Otherwise, answer (ARP Reply) on the behalf of the destination unit

h1.pcap [Wireshark 1.8.2]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:00:00_00:00:01	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.1
2	0.036595	00:00:00_00:00:01	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.1
3	0.039481	00:00:00_00:00:02	00:00:00_00:00:01	ARP	42	10.0.0.2 is at 00:00:00:00:00:02
4	0.039489	10.0.0.1	10.0.0.2	ICMP	98	Echo (ping) request id=0x07a3, seq=1/256, ttl=64
5	0.042532	10.0.0.2	10.0.0.1	ICMP	98	Echo (ping) reply id=0x07a3, seq=1/256, ttl=64
6	2.879187	00:00:00_00:00:02	00:00:00_00:00:03	ARP	42	10.0.0.2 is at 00:00:00:00:00:02
7	2.882289	00:00:00_00:00:03	00:00:00_00:00:02	ARP	42	10.0.0.3 is at 00:00:00:00:00:03
8	5.059211	00:00:00_00:00:02	00:00:00_00:00:01	ARP	42	Who has 10.0.0.1? Tell 10.0.0.2
9	5.059226	00:00:00_00:00:01	00:00:00_00:00:02	ARP	42	10.0.0.1 is at 00:00:00:00:00:01

h2.pcap [Wireshark 1.8.2]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:00:00_00:00:01	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.1
2	0.000082	00:00:00_00:00:02	00:00:00_00:00:01	ARP	42	10.0.0.2 is at 00:00:00:00:00:02
3	0.004447	10.0.0.1	10.0.0.2	ICMP	98	Echo (ping) request id=0x07a3, seq=1/256, ttl=64
4	0.004469	10.0.0.2	10.0.0.1	ICMP	98	Echo (ping) reply id=0x07a3, seq=1/256, ttl=64
5	2.842593	00:00:00_00:00:02	00:00:00_00:00:03	ARP	42	10.0.0.2 is at 00:00:00:00:00:02
6	2.844224	10.0.0.3	10.0.0.2	ICMP	98	Echo (ping) request id=0x07a4, seq=1/256, ttl=64
7	2.844312	00:00:00_00:00:02	Broadcast	ARP	42	Who has 10.0.0.3? Tell 10.0.0.2
8	2.845696	00:00:00_00:00:03	00:00:00_00:00:02	ARP	42	10.0.0.3 is at 00:00:00:00:00:03
9	2.845703	10.0.0.2	10.0.0.3	ICMP	98	Echo (ping) reply id=0x07a4, seq=1/256, ttl=64
10	5.018343	00:00:00_00:00:02	00:00:00_00:00:01	ARP	42	Who has 10.0.0.1? Tell 10.0.0.2
11	5.025182	00:00:00_00:00:01	00:00:00_00:00:02	ARP	42	10.0.0.1 is at 00:00:00:00:00:01

h3.pcap [Wireshark 1.8.2]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:00:00_00:00:01	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.1
2	2.834451	00:00:00_00:00:03	Broadcast	ARP	42	Who has 10.0.0.2? Tell 10.0.0.3
3	2.842593	00:00:00_00:00:02	00:00:00_00:00:03	ARP	42	10.0.0.2 is at 00:00:00:00:00:02
4	2.842609	10.0.0.3	10.0.0.2	ICMP	98	Echo (ping) request id=0x07a4, seq=1/256, ttl=64
5	2.845697	00:00:00_00:00:03	00:00:00_00:00:02	ARP	42	10.0.0.3 is at 00:00:00:00:00:03
6	2.847535	10.0.0.2	10.0.0.3	ICMP	98	Echo (ping) reply id=0x07a4, seq=1/256, ttl=64

Number of ARP-Message in a simple flooding algorithm

values

ARP-Messages

Number of ARP-Messages

400000.0

300000.0

200000.0

100000.0

10.0 20.0 30.0 40.0 50.0 60.0 70.0 80.0 90.0

Number of hosts

Number of ARP-Message in our implemented algorithm

values

ARP-Messages

Number of ARP-Messages

9000.0
8000.0
7000.0
6000.0
5000.0
4000.0
3000.0
2000.0
1000.0

10.0
20.0
30.0
40.0
50.0
60.0
70.0
80.0
90.0

Number of hosts

“The End”

–Elad Hayun
–Avihad Menahem