CS356: ARP

W. Michael Petullo

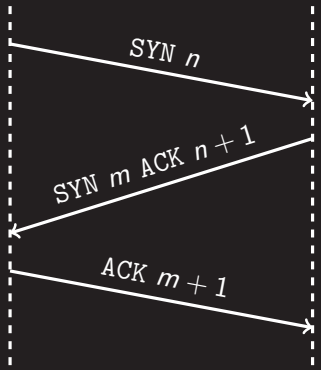
University of Wisconsin–La Crosse

As of October 21, 2021

ARP: Review

Aside from explicit reads and writes, when does OS send network messages in response to system calls?

More Networking: TCP Details



- Three-way handshake establishes initial sequence number, providing weak authenticator and preparing for reliability (`connect` system call).
- Subsequent segments contain `SYN` and `ACK` values (`recv`/`send`/`read`/`write`).
- Sender will at some point stop sending to allow `ACK` s to catch up (window size; transparent buffering).
- `FIN` flag indicates connection should close (`close`/`shutdown`).
- `RST` flag indicates something went wrong.

Wireshark demo: HTTPS (filter: `tcp.port==443`)

ARP: More Implicit Messages

Question: Who is 192.168.0.1 on local network?

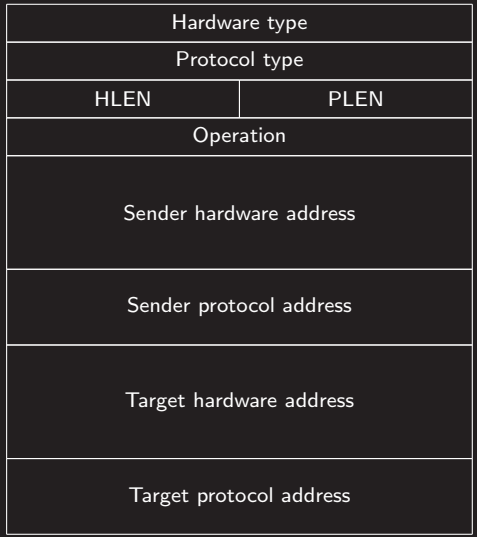
- Ethernet/MAC addresses are six bytes and are usually written like this: `01:23:45:ab:cd:ef`.
- Ethernet hosts discover peer hosts using Address Resolution Protocol (ARP).
- ARP makes use of Ethernet's broadcast address: `ff:ff:ff:ff:ff:ff`.
- Discovering peers in this way does not scale to the Internet; hence we have the higher-level protocols.

```
[user@host]$ ip neighbor
138.49.28.18 dev enp4s0 lladdr b8:27:eb:12:b0:d4 STALE
138.49.28.1 dev enp4s0 lladdr f0:b2:e5:0e:0e:da REACHABLE
```

- Another technique for passive network reconnaissance

Wireshark demo: ARP (filter: `arp`)

ARP: Format



Hardware type (2 bytes) Ethernet is 1

Protocol type (2 bytes) IPv4 is 0x0800

HLEN (1 byte) Length in bytes of hardware address (6 for Ethernet)

PLEN (1 byte) Length in bytes of protocol address (4 for IPv4)

Operation (2 bytes) Request is 1, reply is 2

SHA (6 bytes) Request: hardware address of sender; reply: "answer" address

SPA (4 bytes) protocol address of sender

THA (6 bytes) Request: ignored; reply: host that made request

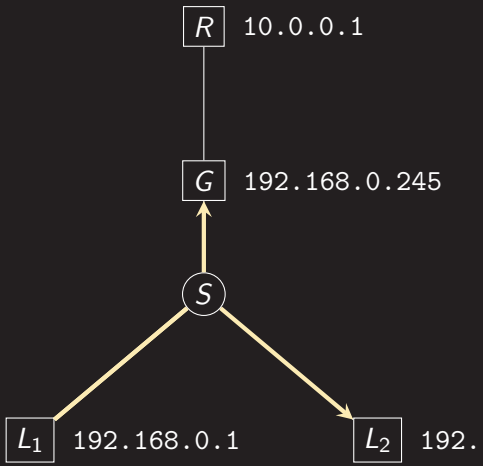
TPA (4 bytes) protocol address of receiver

ARP: Interplay with Routing

- R Remote host
- G Gateway router
- S Switch
- L_1 LAN host
- L_2 LAN host

L_1 wants to send message to `192.168.0.2`.

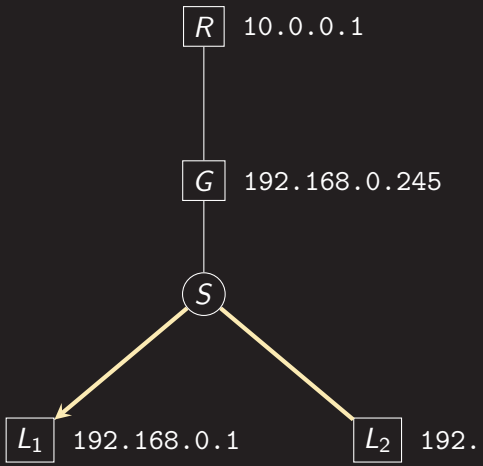
ARP: Interplay with Routing



- R Remote host
- G Gateway router
- S Switch
- L_1 LAN host
- L_2 LAN host

L_1 asks, "who has 192.168.0.2?" (ARP)

ARP: Interplay with Routing



R Remote host

G Gateway router

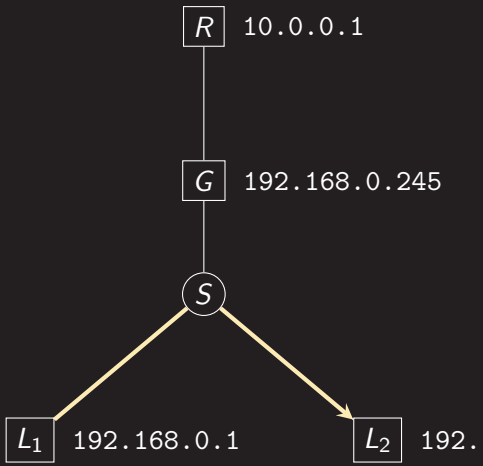
S Switch

L_1 LAN host

L_2 LAN host

L_2 responds, “bb:bb:bb:bb:bb:bb.” (ARP)

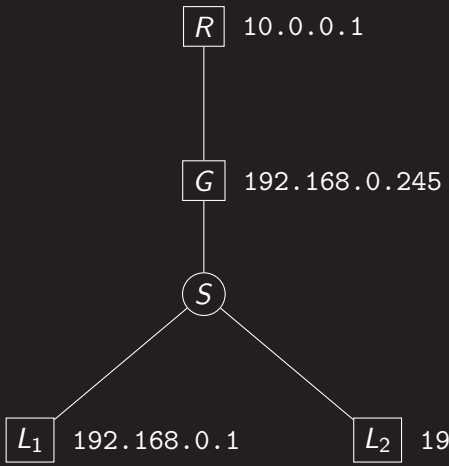
ARP: Interplay with Routing



- R Remote host
- G Gateway router
- S Switch
- L_1 LAN host
- L_2 LAN host

L_1 addresses message to `bb:bb:bb:bb:bb:bb`/`192.168.0.2` and sends.

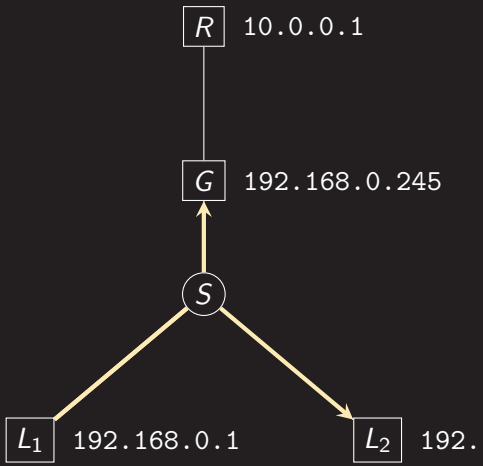
ARP: Interplay with Routing



- R Remote host
- G Gateway router
- S Switch
- L_1 LAN host
- L_2 LAN host

L_1 wants to send message to `10.0.0.1`, but realizes R is not on same LAN.

ARP: Interplay with Routing



- R Remote host
- G Gateway router
- S Switch
- L_1 LAN host
- L_2 LAN host

L_1 asks, "who has 192.168.0.254?" (ARP)

ARP: Interplay with Routing

- R Remote host
- G Gateway router
- S Switch
- L_1 LAN host
- L_2 LAN host

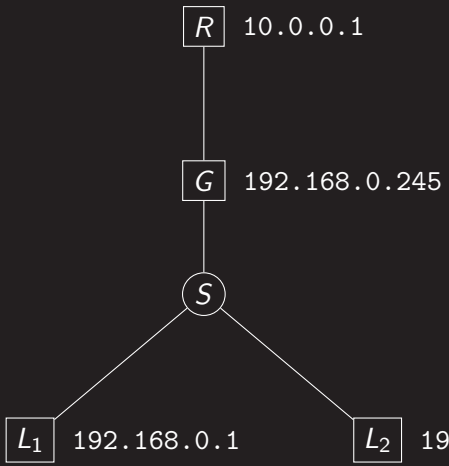
G responds, “ee:ee:ee:ee:ee:ee.” (ARP)

ARP: Interplay with Routing

- R Remote host
- G Gateway router
- S Switch
- L_1 LAN host
- L_2 LAN host

L_1 addresses message to `ee:ee:ee:ee:ee:ee`/`10.0.0.1` and sends.

ARP: Interplay with Routing



- R Remote host
- G Gateway router
- S Switch
- L_1 LAN host
- L_2 LAN host

G receives message, but realizes he is not `10.0.0.1`.

ARP: Interplay with Routing

- R Remote host
- G Gateway router
- S Switch
- L_1 LAN host
- L_2 LAN host

G asks, "who has 10.0.0.1?" (ARP)

ARP: Interplay with Routing

R Remote host
G Gateway router
S Switch
L_1 LAN host
L_2 LAN host

R responds, “11:11:11:11:11:11.” (ARP)

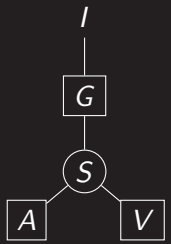
ARP: Interplay with Routing

- R Remote host
- G Gateway router
- S Switch
- L_1 LAN host
- L_2 LAN host

G re-addresses message to
`11:11:11:11:11:11/10.0.0.1` and forwards.

ARP: Attacks

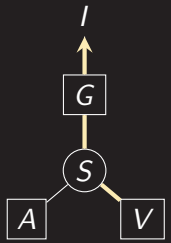
- What if you send spurious ARP replies to a host?
- What if your ARP replies designate your host as owning the gateway router's IP address?
- What if your host is able to route packets back to the real gateway router?



G Gateway router
S Switch
A Attacker host
V Victim host
I Internet

ARP: Attacks

- What if you send spurious ARP replies to a host?
- What if your ARP replies designate your host as owning the gateway router's IP address?
- What if your host is able to route packets back to the real gateway router?

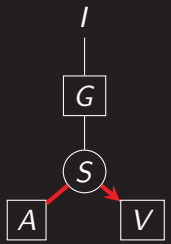


G Gateway router
S Switch
A Attacker host
V Victim host
I Internet

V sends messages to the Internet.

ARP: Attacks

- What if you send spurious ARP replies to a host?
- What if your ARP replies designate your host as owning the gateway router's IP address?
- What if your host is able to route packets back to the real gateway router?

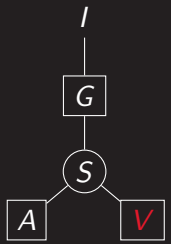


G Gateway router
S Switch
A Attacker host
V Victim host
I Internet

A sends spurious ARP reply to *V*.

ARP: Attacks

- What if you send spurious ARP replies to a host?
- What if your ARP replies designate your host as owning the gateway router's IP address?
- What if your host is able to route packets back to the real gateway router?

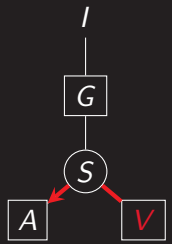


G Gateway router
S Switch
A Attacker host
V Victim host
I Internet

V's ARP cache is poisoned.

ARP: Attacks

- What if you send spurious ARP replies to a host?
- What if your ARP replies designate your host as owning the gateway router's IP address?
- What if your host is able to route packets back to the real gateway router?

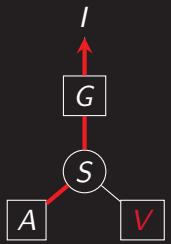


G Gateway router
S Switch
A Attacker host
V Victim host
I Internet

V sends messages to the Internet, but uses *A*'s MAC address.

ARP: Attacks

- What if you send spurious ARP replies to a host?
- What if your ARP replies designate your host as owning the gateway router's IP address?
- What if your host is able to route packets back to the real gateway router?



G Gateway router
S Switch
A Attacker host
V Victim host
I Internet

A observes message and forwards through *G*.

ARP: Exercise

1. Prepare Aquinas VM; see `https://www.aquinas.dev/project/computer`.
2. Use Aquinas interface to register a second SSH key.
3. From the VM, install Wireshark: `sudo dnf install wireshark`.
4. Set `student`'s ability to run Wireshark:
   `sudo usermod -a -G wireshark student`. Sign out and back in.

---

5. Identify your adapter name, IP address, and gateway: `ip address; ip route`.
6. Start Wireshark, start a capture on the proper interface, and filter on `arp`.
7. Flush the ARP cache: `sudo ip neighbor flush dev enp0s3`.
8. Ping your default gateway. Observe the ARP traffic in Wireshark.
9. Review your ARP cache: `ip neighbor`. Do you see a record for the gateway?
10. Remove Wireshark's `arp` filter. Ping 8.8.8.8, and observe the MAC addreses.
11. Use Wireshark to observe traffic associated with your Aquinas network programs.

ARP: Assignments

Graded Homework Aquinas: udpscan

Reading Read 0x400–0x433

https://www.flyn.org/courses/cs356/schedule