Network Security I

Ethernet/IP Routing, ARP
Basics of Ethernet

● 48-bit MAC (Media Access Control) Addresses
  ○ Globally unique, assigned by manufacturer

● Broadcast medium
  ○ Everybody connected to a wire
  ○ Everybody hears all traffic
  ○ Ignores everything not for them
Hey, that’s for me!

Ethernet is a broadcast medium
Hey, that’s for me!

The broadcast address is **FF:FF:FF:FF:FF:FF:FF**
Basics of Ethernet

- 48-bit MAC (Media Access Control) Addresses
  - Globally unique, assigned by manufacturer

- Broadcast medium
  - Everybody connected to a wire
  - Everybody hears all traffic
  - Ignores everything not for them

- What about really large networks? Switches!
Each link is its own broadcast medium
- Each link is its own broadcast medium
- Problem: switches don’t know where anyone is
- Each link is its own broadcast medium
- Problem: switches don’t know where anyone is
- Solution: broadcast on all other links

- If you see a frame from a MAC you don’t know about, remember it!
- Future traffic to that MAC goes direct
- Each link is its own broadcast medium
- Problem: switches don’t know where anyone is
- Solution: broadcast on all other links

- If you see a frame from a MAC you don’t know about, remember it!
- Future traffic to that MAC goes direct
- Networks must not have loops!
Basics of IP Routing

- Internet Protocol: connects multiple networks
- “Network” here means link-layer network
  - e.g., Ethernet
  - WiFi
- Each link-layer protocol is different
- On top of the link layer, it’s all IP
- Enables communication between incompatible networks
“IP Hourglass”
Network Topology

Data Flow

Layer 1

Layer 2

Layer 3

Layer 4

Layer 5
Note the analogy to the previous slide, and which protocols are used where.
Basics of IP Routing

- Problem: $2^{32} = \sim 4\text{Bn}$ possible IP addresses
- How to remember where each one is?
Basics of IP Routing

● Solution: hierarchical division into “subnets”
● Idea: Similar IP addresses are near each other
● Addresses with a common prefix are in the same subnet
Basics of IP Routing

Subnet address: 192.168.1.0/24

Prefix length (in bits): 24

24-bit prefix: 11000000 10101000 00000001 00000000
Basics of IP Routing

Subnet address

192.168.1.0

Subnet “mask”

255.255.255.0

24-bit prefix

11000000 10101000 00000001 00000000
Basics of IP Routing

Algorithm:

\[ \text{address} \& \text{subnet\_mask} = \text{prefix} \]

Example:

\[
\begin{align*}
192.168.1.27 \\
\& 255.255.255.0 \\
\hline
192.168.1.0
\end{align*}
\]
Basics of IP Routing

Routing algorithm: “longest prefix match”

// route to exact IP address
route = in_route_db(prefix, 0);

// subnet with 31-bit prefix prefix
route = in_route_db(prefix, 1);

...
I don’t know where 192.168.1.27 is, but I know where 192.168.1.0/24 is!
Basics of IP Routing

- Problem: what subnet are the routers in?
Basics of IP Routing

- Problem: what subnet are the routers in?
- Answer: they aren’t...
Basics of IP Routing

- *Devices* don’t have IP addresses
- *Interfaces* have IP addresses
- “Multi-homed” devices have interfaces in multiple networks
Ethernet Network
(169.254.0.0/16)

Satellite Network
(10.1.0.0/16)

Ethernet Network
(192.168.1.0/24)

192.168.1.27
192.168.1.1
169.254.0.1
169.254.0.34
10.1.0.1
10.1.0.2
169.254.0.34
Combining Ethernet and IP

- Recall IP hourglass
- IP is agnostic to all other protocols (above and below in the protocol stack)
- Link layer protocols’ responsibility to interoperate with IP
Ethernet frame contains IP packet
Combining Ethernet and IP

- Scenario: host A wants to send to host B
- What should we do?
Combining Ethernet and IP

- Scenario: host A wants to send to host B
- What should we do?
  - First: are they in my LAN?
    - Send ethernet frame directly to their MAC
  - Second: if they aren’t in my LAN...
Combining Ethernet and IP

- Scenario: host A wants to send to host B
- What should we do?
  - First: are they in my LAN?
    - Send ethernet frame directly to their MAC
  - Second: if they aren’t in my LAN
    - What router in my LAN can talk to their subnet?
    - Send ethernet frame to this router’s MAC
Combining Ethernet and IP

- Two questions to answer:
  - Given an IP in my subnet, what’s the MAC?
  - Given an IP in another subnet, what router to use?
Combining Ethernet and IP

- Given an IP in my subnet, what’s the MAC?
  - Address Resolution Protocol (ARP)

- Given an IP in another subnet, what router to use?
  - Depends on the network
  - In most “edge” networks, only one router
  - Only two routes: “in here” or “out there” (the internet)
  - This single router is the “default gateway”
  - Often configured dynamically using DHCP
What happens in the two ethernet networks when 169.254.0.34 sends to 192.168.1.27?
ARP and MAC Spoofing

CS 166: Introduction to Computer Security
IP and Mac Address

• Devices that share a physical network have at the same time
  – IP addresses
  – MAC addresses (Physical addresses)
• IP addresses are used for high level protocols
• MAC addresses are used for low level protocols
• PROBLEM: How to translate IP Addresses in MAC addresses?
Address Resolution Protocol (ARP)

- **ARP** connects network layer to data layer.
  - It converts IP addresses to MAC addresses
- Defined as a part of **RFC 826**, allows for converting between IP addresses and MAC addresses
- IPv6 does not use ARP, and ARP is instead replaced by Neighbor Discovery Protocol.
- **RARP** converts MAC addresses to IP addresses and it was used if a machine does not know its own ip address
  - Now replaced by **dhcp**
ARP broadcast

- ARP broadcasts requests and caches responses, e.g. the message
  who has <IP addressC> tell <IP addressA>
- <IP addressC> or an ARP server broadcasts the response
  <IP addressC> is <MAC address>
- The requestor’s IP address
  <IP addressA> is contained in the packet header
ARP Cache

- The Linux, Windows and OSX command `arp -a` displays the ARP table
<table>
<thead>
<tr>
<th>Internet Address</th>
<th>Physical Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>128.148.31.1</td>
<td>00-00-0c-07-ac-00</td>
<td>dynamic</td>
</tr>
<tr>
<td>128.148.31.15</td>
<td>00-0c-76-b2-d7-1d</td>
<td>dynamic</td>
</tr>
<tr>
<td>128.148.31.71</td>
<td>00-0c-76-b2-d0-d2</td>
<td>dynamic</td>
</tr>
<tr>
<td>128.148.31.75</td>
<td>00-0c-76-b2-d7-1d</td>
<td>dynamic</td>
</tr>
<tr>
<td>128.148.31.102</td>
<td>00-22-0c-a3-e4-00</td>
<td>dynamic</td>
</tr>
</tbody>
</table>

- The command `arp -a -d` flushes the cache ARP
- The arp cache entries are stored for a configurable amount of time
- Network administrator needs to configure just the IP address and the subnet on every single machine, ARP allows the communication
DEMO

• Ping a machine with a new IP address in the same subnet
  – An IP address that is not stored in cache
• The system uses an ARP broadcast

• ARP packet format
  – Hlen: 6 bytes (48 bits)
  – Plen: 4 bytes (32 bits)
    • It is possible to use other protocol not just TCP/IP
  – Operation: ARP request or reply
  – HA: mac address
    • FF:FF:FF:FF:FF:FF is the broadcast
  – IA: IP address

<table>
<thead>
<tr>
<th>0</th>
<th>32</th>
</tr>
</thead>
<tbody>
<tr>
<td>hardware</td>
<td>protocol</td>
</tr>
<tr>
<td>hlen</td>
<td>plen</td>
</tr>
<tr>
<td>sender HA (byte 0-3)</td>
<td></td>
</tr>
<tr>
<td>sender HA (byte 4-5)</td>
<td>sender IA (byte 0-1)</td>
</tr>
<tr>
<td>sender IA (byte 2-3)</td>
<td>target HA (byte 0-1)</td>
</tr>
<tr>
<td>target HA (byte 2-5)</td>
<td></td>
</tr>
<tr>
<td>target IA (byte 0-3)</td>
<td></td>
</tr>
</tbody>
</table>
MAC Address Filtering

• A wifi Access Point uses a whitelist of authorized MAC addresses
  – The captive portal authenticates MAC addresses like a web server does for cookie sessionID

• A **MAC spoofing attack** impersonates target machine
  – Determine MAC address of target machine
  – Reconfigure MAC address of rogue machine
  – Disable target machine

• **Countermeasures**
  – Disable duplicate MAC addresses
Viewing and Changing MAC Addresses

• Viewing the MAC addresses of the interfaces of a machine
  – Linux: `ifconfig`
  – Windows: `ipconfig /all`

• Changing a MAC address in Linux
  – Stop the networking service: `/etc/init.d/network stop`
  – Change the MAC address: `ifconfig eth0 hw ether <MAC-address>`
  – Start the networking service: `/etc/init.d/network start`

• Changing a MAC address in Windows
  – Open the Network Connections applet
  – Access the properties for the network interface
  – Click “Configure …”
  – In the advanced tab, change the network address to the desired value

• Changing a MAC address requires administrator privileges