Tracking an Offender
Communication Between Layers in Different Hosts

sender

Application

Presentation

Session

Transport

Network

Data link

Physical

receiver

Application

Presentation

Session

Transport

Network

Data link

Physical

AH data

PH data

SH data

TH data

NH data

DH data

BITS

DT
TCP/IP Family
Network Class

32 Bits

<table>
<thead>
<tr>
<th>Class</th>
<th>Network</th>
<th>Host</th>
<th>Range of host addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>0</td>
<td></td>
<td>1.0.0.0 to 127.255.255.255</td>
</tr>
<tr>
<td>B</td>
<td>10</td>
<td></td>
<td>128.0.0.0 to 191.255.255.255</td>
</tr>
<tr>
<td>C</td>
<td>110</td>
<td></td>
<td>192.0.0.0 to 223.255.255.255</td>
</tr>
<tr>
<td>D</td>
<td>1110</td>
<td></td>
<td>224.0.0.0 to 239.255.255.255</td>
</tr>
<tr>
<td>E</td>
<td>1111</td>
<td></td>
<td>240.0.0.0 to 255.255.255.255</td>
</tr>
</tbody>
</table>

Multicast address

Reserved for future use
## IP Address

<table>
<thead>
<tr>
<th>IP address</th>
<th>Binary Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>138.77.37.21</td>
<td>10001010 01001101 00100101 00100101</td>
</tr>
<tr>
<td>netmask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>network address</td>
<td></td>
</tr>
<tr>
<td>host address</td>
<td></td>
</tr>
</tbody>
</table>
Subnetting

- Add another level to address/routing hierarchy: \textit{subnet}
- \textit{Subnet masks} define variable partition of host part
- Subnets visible only within site

<table>
<thead>
<tr>
<th>Network number</th>
<th>Host number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class B address</td>
<td></td>
</tr>
<tr>
<td>111111111111111111111111111</td>
<td>00000000</td>
</tr>
</tbody>
</table>

Subnet mask (255.255.255.0)

<table>
<thead>
<tr>
<th>Network number</th>
<th>Subnet ID</th>
<th>Host ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subnetted address</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Basic Concepts

- Media Access Control
- ARP
- TCP/IP, UDP
- DHCP
- DNS
- ping, traceroute, dig
- whois
Investigating Emails

- Increasing volume of fraudulent email
- Virus propagation
- Spam in the workplace
- Increased successful prosecution of spammers
- Deleting email
Email System

- One example open source email system:
  - [http://www.qmailrocks.com/](http://www.qmailrocks.com/)
Analyzing Message Headers

• Envelope header information
  – Added by sender
  – Often forged

• Message header
  – Added by receiver
  – Use these for analysis

• Sample message header
  – http://www.stopspam.org/email/headers.html
Spam Tools

• Robomail: mass mailer
  – http://www.inter7.com/

• Email harvester
  – http://www.lencom.com/

• http://www.paulgraham.com/

• CAN-SPAM Act: Requirements for Commercial Emailers
Email Phishing

• Serious threat of financial loss
• Newest, most damaging type of spam
• Rely on “Social Engineering”
• http://www.antiphishing.org/
URL Obfuscation With @

• What is the format of a URL?
  [protocol]://[user@]system[:portnum]/file

• If we are accessing a web site…
  – Protocol is http
  – User is blank and port number is blank (defaults to 80)

• Therefore, we get something like:
  – http://www.microsoft.com

• Hide real destination inside the URL:
  – http://www.microsoft.com&item=q122134@www.phrack.org
Fighting Spam

• Spam Filter

CAN-SPAM Do’s

• Accurate Header
  – From
  – Subject
  – Origin, routing, destination

• Include Opt-Out Method

• Include real business address

• Clearly note that the email is advertisement