Network Structure
Challenges
Security
Ethernet
Sensors
Check List
Network Structure
Network Structure

http://www.caida.org/tools/visualization/mapnet/Backbones/

Contents – Index – Review2 – Structure →
Network Structure

BGP

Transit; Peering Agreements; Customer-Provider
Challenges

Providing new services

- Ubiquitous telepresence
- Sensored universe
- Virtualized environments
  - naming, management
- Adding resilience

[Don Towsley – NSF Workshop – April 2003]
Challenges

- **Mathematical theories to:**
  - understand performance limits
    - compute/communication/sensing tradeoffs with power constraints
  - understand network as a complex system
- **How to design evolvable networks**
- **How to design resilient (tolerate *any* fault) networks**
- **How to design markets and network mechanisms to support future heterogeneous apps**

[Don Towsley – NSF Workshop – April 2003]
Security

- Threats
- DDOS
- Cryptography
- Systems
## Threats

<table>
<thead>
<tr>
<th>Against</th>
<th>Type</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network</td>
<td>Link – DDOS</td>
<td>Detect/Filter</td>
</tr>
<tr>
<td></td>
<td>- Physical</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Routers – Tables</td>
<td>Detect/Isolate</td>
</tr>
<tr>
<td></td>
<td>DNS – DDOS</td>
<td></td>
</tr>
<tr>
<td>Computers</td>
<td>Physical</td>
<td>Physical security</td>
</tr>
<tr>
<td></td>
<td>Infection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intrusion</td>
<td>Virus detection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Firewall, passport</td>
</tr>
<tr>
<td>Users</td>
<td>Identity</td>
<td>Signature, password</td>
</tr>
<tr>
<td></td>
<td>Privacy</td>
<td>watermark</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encryption, relay</td>
</tr>
<tr>
<td>Documents</td>
<td>Integrity</td>
<td>Message</td>
</tr>
<tr>
<td></td>
<td>Confidentiality</td>
<td>authentication code</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encryption</td>
</tr>
</tbody>
</table>
DDOS

Distributed Denial of Service Attack

- Basic Mechanism
  - Saturate a link to a host by sending requests from many nodes across the Internet

- Effect
  - Host is incapacitated

- Remedies
  - Verify that source IP exists (i.e., is not spoofed)
  - Block packets that DDOS tools use (some ICMPs)
  - Limit rate of ICMP flows
  - Limit rate of SYNs
  - Trace back from last router upstream to block packets toward that link
Cryptography

Bob \[\rightarrow [ E(.;K) ] \rightarrow C \rightarrow [D(.;K)] \rightarrow P\]

Alice

Secret Key: K known only to Bob and Alice
- Examples: One-time Pad; DES
- Key Distribution: Trusted Channel; SK; PK; Diffie-Hellman

Public Key: Alice advertises K
- Example: RSA

Note: PK is more complex \(\rightarrow\) use PK for SK exchange
Systems

Signed(P)

**Integrity:** Alice —— D(P*H(P); Alice) —— Bob  \( (1) \)

**Key Exchange:**

\[
A = z^a \mod p \\
B = z^b \mod p
\]

Signed(A, B) ——

Signed(A, B)

\[
K = B^a \mod p \\
K = A^b \mod p
\]

**Notes:**

(1) \( D(P; Alice) \) is not secure: Find \( P' = E(C'; Alice) \)

(2) Simple Diffie-Hellman (\( \rightarrow a \) and \( \leftarrow b \)) is not secure: Man-in-Middle
Systems

Authentication:

Alice

Bob

--- Alice, psswd ---

Check $H(psswd)$ (1)

$F(X,K)$

$X$

K shared secret

$E(X; Alice)$

$X$

$Signed(X)$

$X$

Note: (1) Can be intercepted
Ethernet

- Internetworking
- Random Multiple Access
- Switching
- Bridged Ethernet
- 802.11
Internetworking
Indirect Delivery

Note: Fragmentation may be required at R1
Random Multiple Access

- How to share a channel?
  - Multiple Access ≠ Multiplexing

- ALOHA: First random multiple access system
  - Efficient for many users, each with low utilization
  - Try; If collide, wait random time then repeat (CD)
  - Analysis: Slotted Aloha efficiency ≈ 1/e = 36%

\[ P(\text{success}) = Np(1 - p)^{N-1} \approx \frac{1}{e} \text{ if } p = \frac{1}{N} \]
Random Multiple Access

Ethernet: First version – CSMA/CD

- Wait until channel is idle; try; if collide, stop, wait, repeat
- Idea: CS should improve efficiency if fast enough
- Wait random multiple of 512 bit times (exponential back off)
- Analysis: Efficiency \( \approx \frac{1}{1 + 5a} \), \( a = \text{PROP/TRANS} \)
Switching

Ethernet: Later versions – Switched

- Larger aggregate throughput
- VLANs: partition in disjoint logical LANs
- Link Aggregation
- Fast, GE, 10GE
  - Improved modulation schemes
Bridged Ethernet

- Flat Addressing
- Learning
  - Watch source addresses
- Avoiding Loops
  - Spanning Tree Protocol
  - (ID, presumed root ID, distance to presumed root ID)
  - Note: Not very efficient; Not very fast
Spanning Tree Example

Format: [my ID | presumed root ID | distance to presumed root]
802.11

- a - 5GHz, up to 54Mbps
- b - 2.5GHz, up to 11Mbps
- g - 2.5GHz, up to 54Mbps
- MAC: RTS/CTS
  - Distributed: maintain network allocation vector
  - Centralized: access point polls nodes
Sensor Networks

- Application-Specific
- New problems because
  - Limited energy, memory, CPU
  - Many nodes: naming, addressing
  - Location: triangulation
- New architecture: layers?
- In-network processing
- MAC
  - Sleep & wake up
- Routing
  - Directed diffusion, Ant algorithm, …
Check List

- Switching:
  - Internetworking
  - Learning & Spanning Tree in Ethernet

- Security:
  - Public vs. Secret
  - RSA; Diffie-Hellman
  - Integrity; Key Distribution; Authentication

- MAC
  - ALOHA; CSMA/CD; RTS-CTS

- Sensors
  - Key issues