The Internet and Sockets

It’s quite hard to explain what the Internet actually is

“The Internet is not something that you just dump something on. It’s not a big truck. It’s a series of tubes.”

Ted Stevens, US Senator

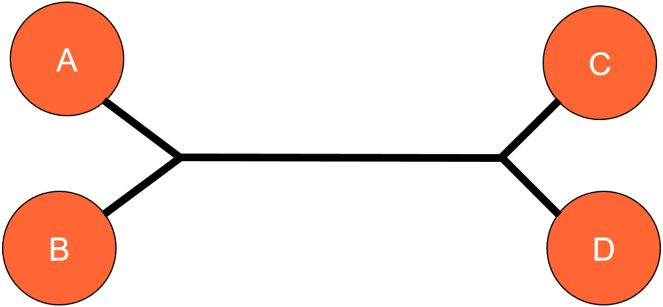
Before the Internet

- Computer Networks:
  - local networks
  - telephone line connections
  - leased line.

The Start 1969

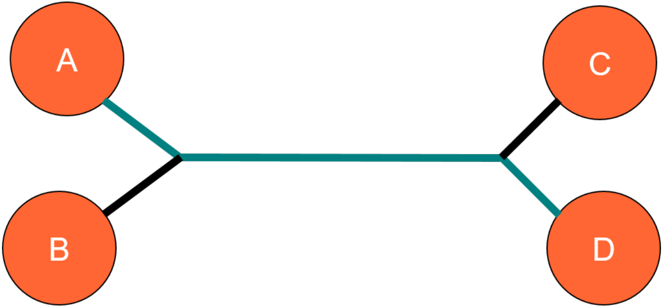
- The US Defense Advanced Research Projects Agency (then ARPA now DARPA) gives research grants to universities to buy computers.
- They decide to link their computers.
- But how?

The Problem With Leased Lines



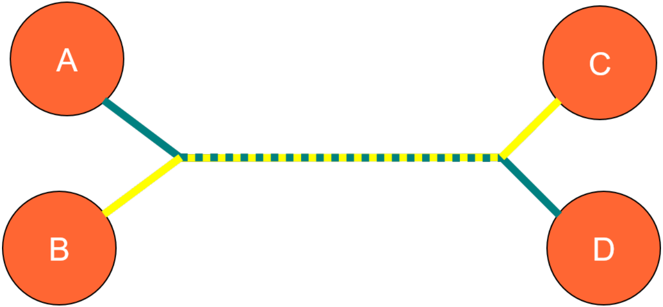
The Problem With Leased Lines

If A and D use the line, then C and B cannot.

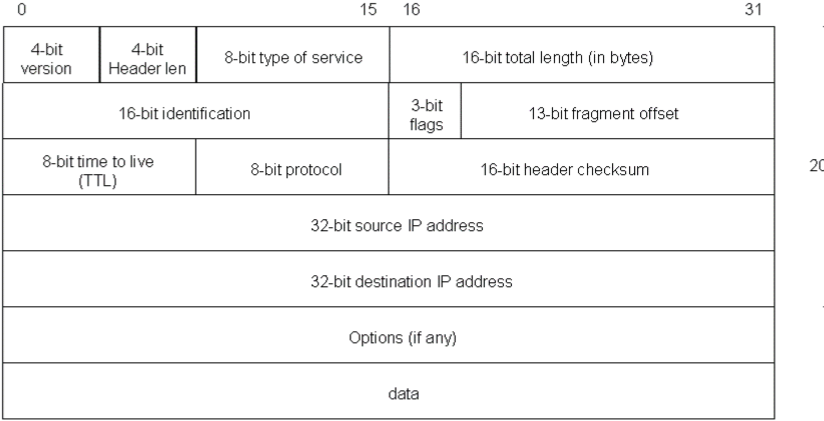


The problem with Leased Lines

But if everone just sends a small packet of data, they can both use the line at the same time.



IP PACKET HEADER



4-bit version | 4-bit Header len | 8-bit type of service | 16-bit total length (in bytes)

16-bit identification | 3-bit flags | 13-bit fragment offset

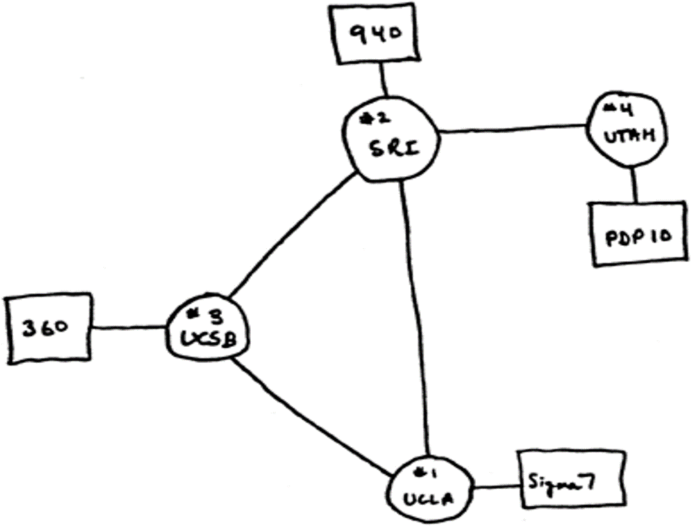
8-bit time to live (TTL) | 8-bit protocol | 16-bit header checksum

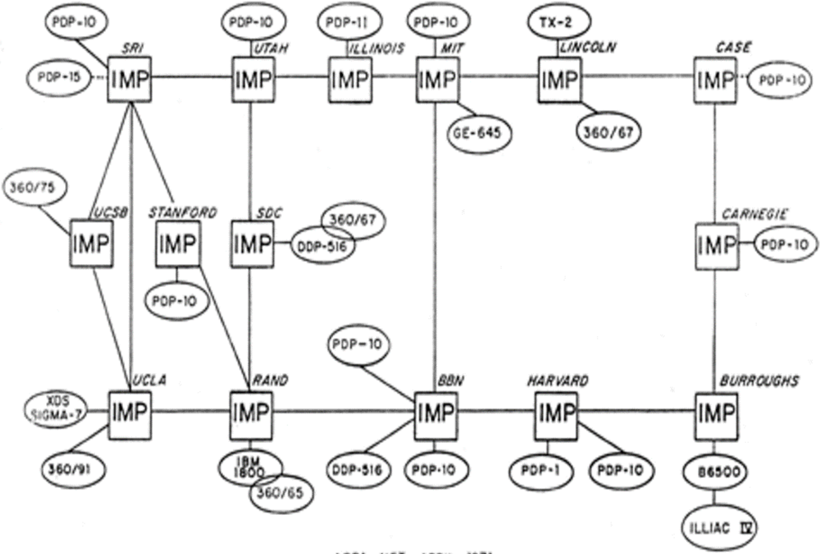
32-bit source IP address

32-bit destination IP address

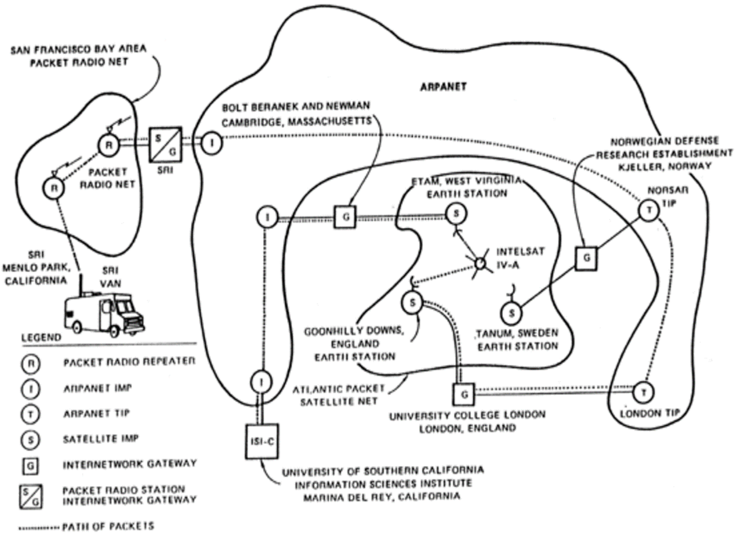
Options (if any)

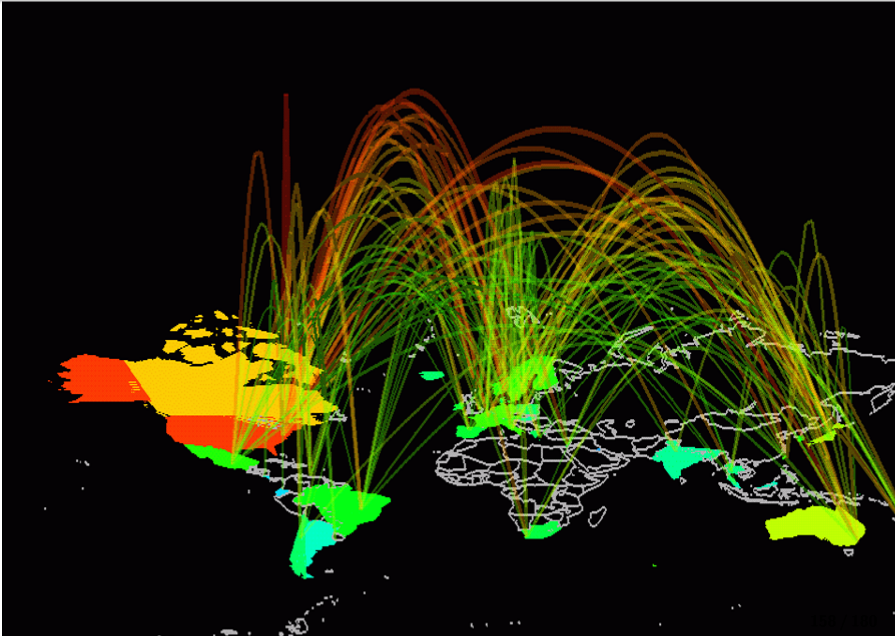
data

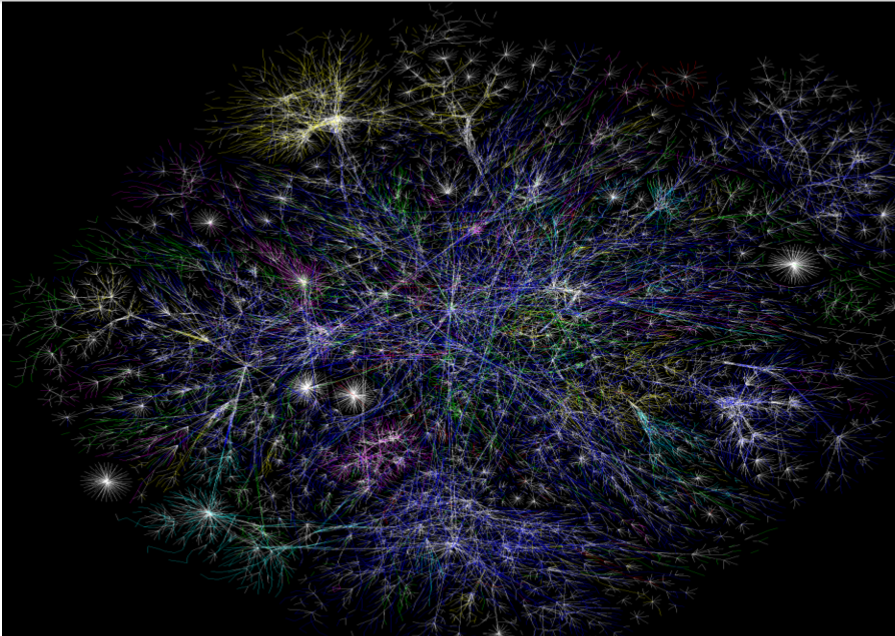

940
#2
SRI
#4
UTAH
PDP 10
360
#3
UCSB
#1
UCLA
Sigma7



ARPA NET, APRIL 1971


SAN FRANCISCO BAY AREA PACKET RADIO NET
ARPANET
BOLT BERANEK AND NEWMAN CAMBRIDGE, MASSACHUSETTS
R
S
G
I
SRI
R
PACKET RADIO NET
NORWEGIAN DEFENSE RESEARCH ESTABLISHMENT KJELLER, NORWAY
ETAM, WEST VIRGINIA EARTH STATION
NORSAR TIP
T
I
G
S
INTELSAT IV-A
G
SRI MENLO PARK, CALIFORNIA
SRI VAN
S
S
GOONHILLY DOWNS, ENGLAND EARTH STATION
TANUM, SWEDEN EARTH STATION
LEGEND
R PACKET RADIO REPEATER
I ARPANET IMP
T ARPANET TIP
S SATELLITE IMP
G INTERNETWORK GATEWAY
S/G PACKET RADIO STATION INTERNETWORK GATEWAY
PATH OF PACKETS
I
ATLANTIC PACKET SATELLITE NET
G
T
UNIVERSITY COLLEGE LONDON LONDON, ENGLAND
LONDON TIP
ISI-C
UNIVERSITY OF SOUTHERN CALIFORNIA INFORMATION SCIENCES INSTITUTE MARINA DEL REY, CALIFORNIA





Traceroute

BT and Vodafone among telecoms companies passing details to GCHQ

Fears of customer backlash over breach of privacy as firms give GCHQ unlimited access to their undersea cables

The document identified for the first time which telecoms companies are working with GCHQ's "special source" team. It gives top secret codenames for each firm, with BT ("Remedy"), Verizon Business ("Dacron"), and Vodafone Cable ("Gerontic"). The other firms include Global Crossing ("Pinnage"), Level 3 ("Little"), Viatel ("Vitreous") and Interoute ("Streetcar"). The companies refused to comment on any specifics relating to Tempora, but several noted they were obliged to comply with UK and EU law.

http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq

Transmission Control Protocol

- 1974: daily traffic more than 3 million packets a day. Many are getting lost.
- TCP is a protocol than runs on top on IP, if an IP packet gets lost. It requests that it is resent.
- TCP/IP becomes standard and allows Inter network connections.

Domain Name Servers (DNS)

- Remembering IP address is hard.
- So people associate names with addresses.
  e.g. `news.bbc.com` → 212.58.226.141
- A hierarchy of servers list handle requests
- The route for most of Europe is RIPE based in Amsterdam.

Ports

- To allow multiple connections TCP uses “ports”
- A TCP “Socket” connection is defined by: `(destination IP, destination port, source IP, source port)`
- The destination port normally depends on the service: WWW runs on port 80, ssh on port 22, dns on 53. . .
- The source port is normally chosen at random.

Netcat

- Netcat is a tool to make Internet connections.
- Syntax varies between OS.
- listen on 1337: `nc -l 1337`
- connect to machine 127.0.0.1 on port 1337: `nc 127.0.0.1 1337`

Nmap

- Check if 1000 most common ports are open:

  ```
  nmap 127.0.0.1
  ```

- Additionally send messages to ports to find out what the service is:

  ```
  nmap -A 127.0.0.1
  ```

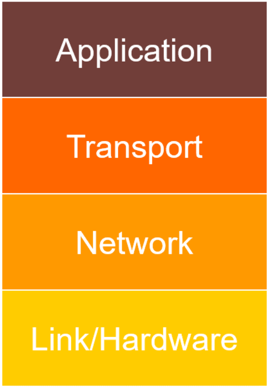
- Scan all ports

  ```
  nmap -p- 127.0.0.1
  ```

Nmap demo

The Internet Protocol Stack

- Internet communication uses a stack of protocols.
- Each protocol uses the protocol below it to sent data.



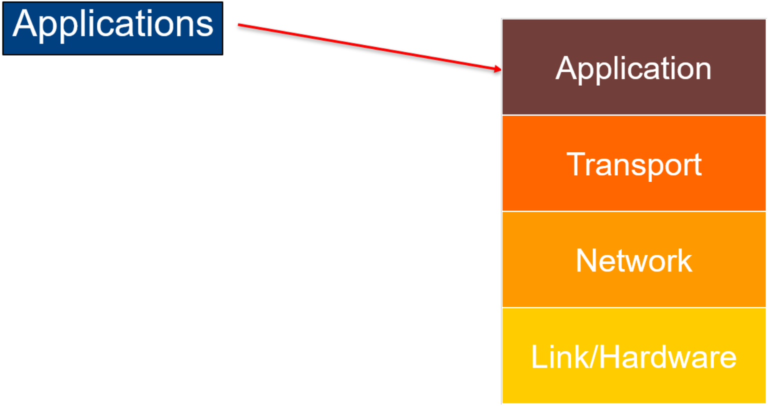
Application

Transport

Network

Link/Hardware

The Stack, Most of the Time



Applications

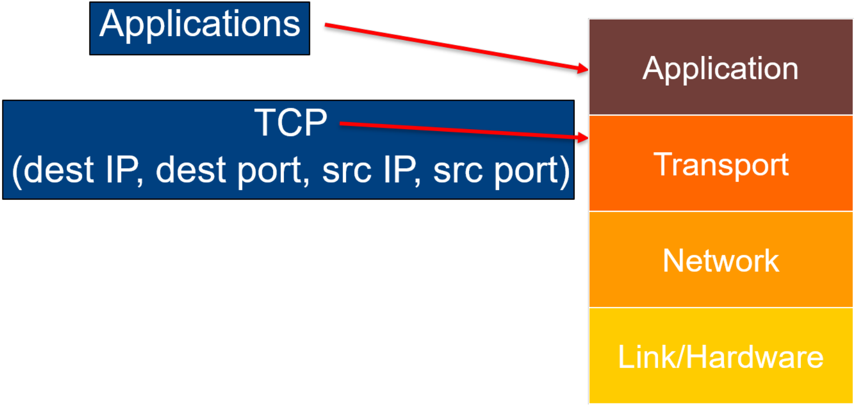
Application

Transport

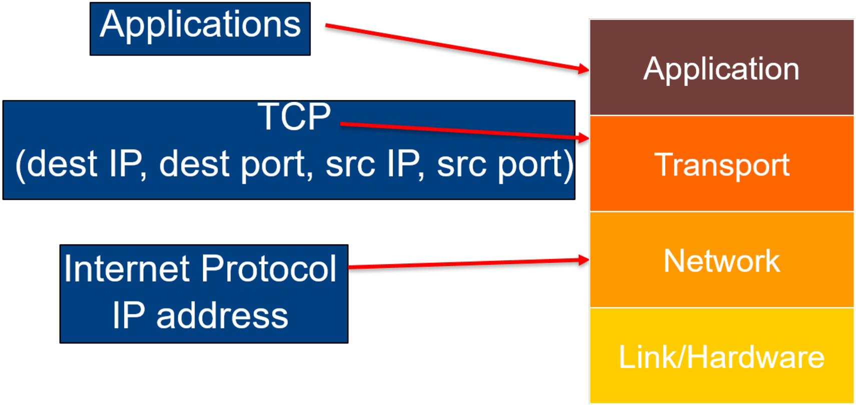
Network

Link/Hardware

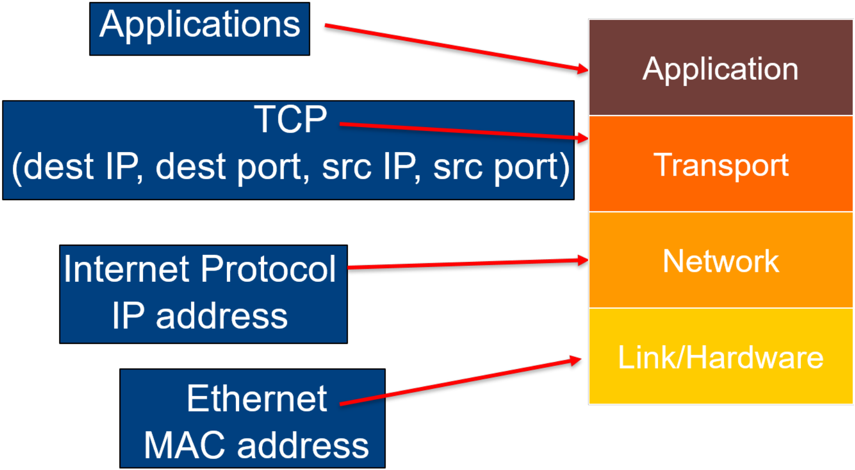
The Stack, Most of the Time



The Stack, Most of the Time



The Stack, Most of the Time



MAC and IP Addresses

- Every machine has a unique MAC address (media access control) e.g. 48:d7:05:d6:7a:51.
- Every computer on the Internet has an IP address, e.g., 147.188.193.15.
- NAT address 10.*.*.* and 192.168.*.* are not unique local addresses.

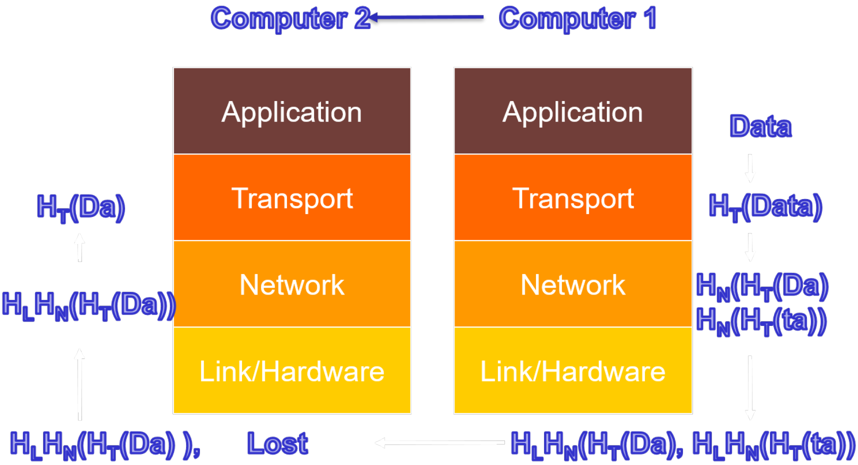
DHCP and ARP

- Dynamic Host Configuration Protocol:
    - Assigns an IP address to a new machine (MAC address). Not stored long term.
- Address Resolution Protocol (ARP)
    - Lets router find out which IP address is being used by which machine.
    - ARP spoofing lets one machine steal the IP address of another on the same network.

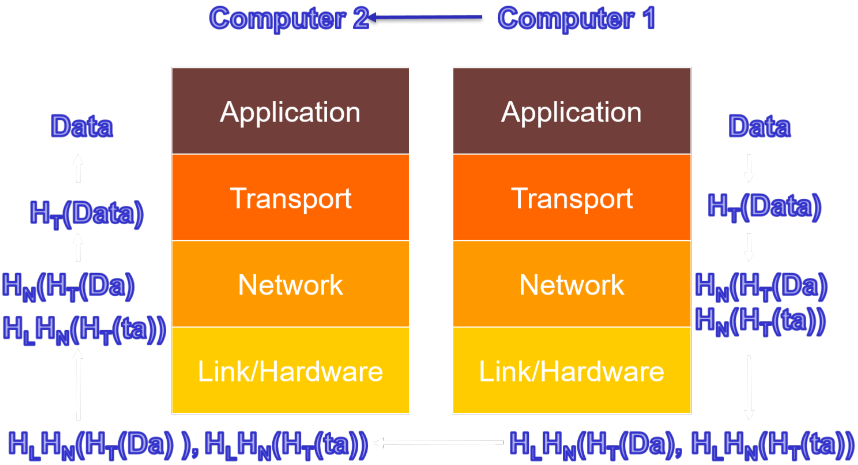
Wireshark

- A network protocol analyzer: It records all Internet traffic, so it can then be viewed and analysed.
- Excellent for debugging protocols and network problems
- See also tcpdump, which writes packets directly to disk.

Using the Stack to Send Data



Using the Stack To Send Data



Computer 2 ← Computer 1

Computer 2	Computer 1
Application	Application
Transport	Transport
Network	Network
Link/Hardware	Link/Hardware

Computer 2:

Data

H_T(Data)

H_N(H_T(Da)

$H_L H_N$(H_T(ta))

Computer 1:

Data

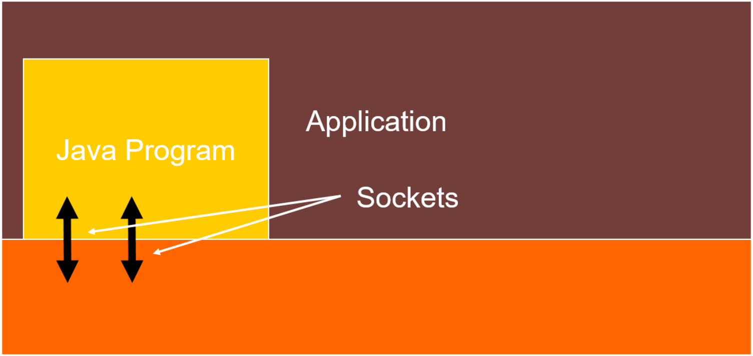
H_T(Data)

H_N(H_T(Da)

H_N(H_T(ta))

$H_L H_N$(H_T(Da)), $H_L H_N$(H_T(ta)) ← $H_L H_N$(H_T(Da), $H_L H_N$(H_T(ta))

Our View of the Stack in Java



Java Sockets demo

“The Attacker Owns the Network”

- The Internet was not designed with security in mind.
- Traffic may be monitored or altered.
- All good security products assume that the attacker has complete control over the network (but can’t break encryption)