

Applied Networks & Security

Introduction

<http://condor.depaul.edu/~jkristof/it263/>

John Kristoff
jtk@depaul.edu

Science, humanities or a trade?

- Various disciplines may appear in this course
 - Physics
 - Mathematics
 - Engineering
 - Skilled labor
 - Philosophy
 - Art
 - History
 - Economics
 - Politics

What do we mean by network?

- Actually there are different classes of networks
 - Telephone network
 - Road system
 - Postal service
 - Neural network
 - Computer network
- We care about so-called *computer* networks
- We examine some communications technologies that allow computers to *talk* to each other

Typical peer communication

- <a> Hello?
- Hi.
- <a> yadda yadda yadda
- blah blah blah

No answer

- <a> Hello?
- <a> Hello??
- <a> Are you there?!?
- <a> Cat got your tongue? Can you hear me?!?!
- <a> *sigh* Oh forget it, I give up

Unwelcome

- `<a>` Hello?
- `` Not interested, good day.

Impersonation

- <a> Hello, is that you?
- Uhm, yeah, it's me *snicker*

Warriors of the Net

- <http://www.warriorsofthe.net>
- It is a neat video, but misleading in some details

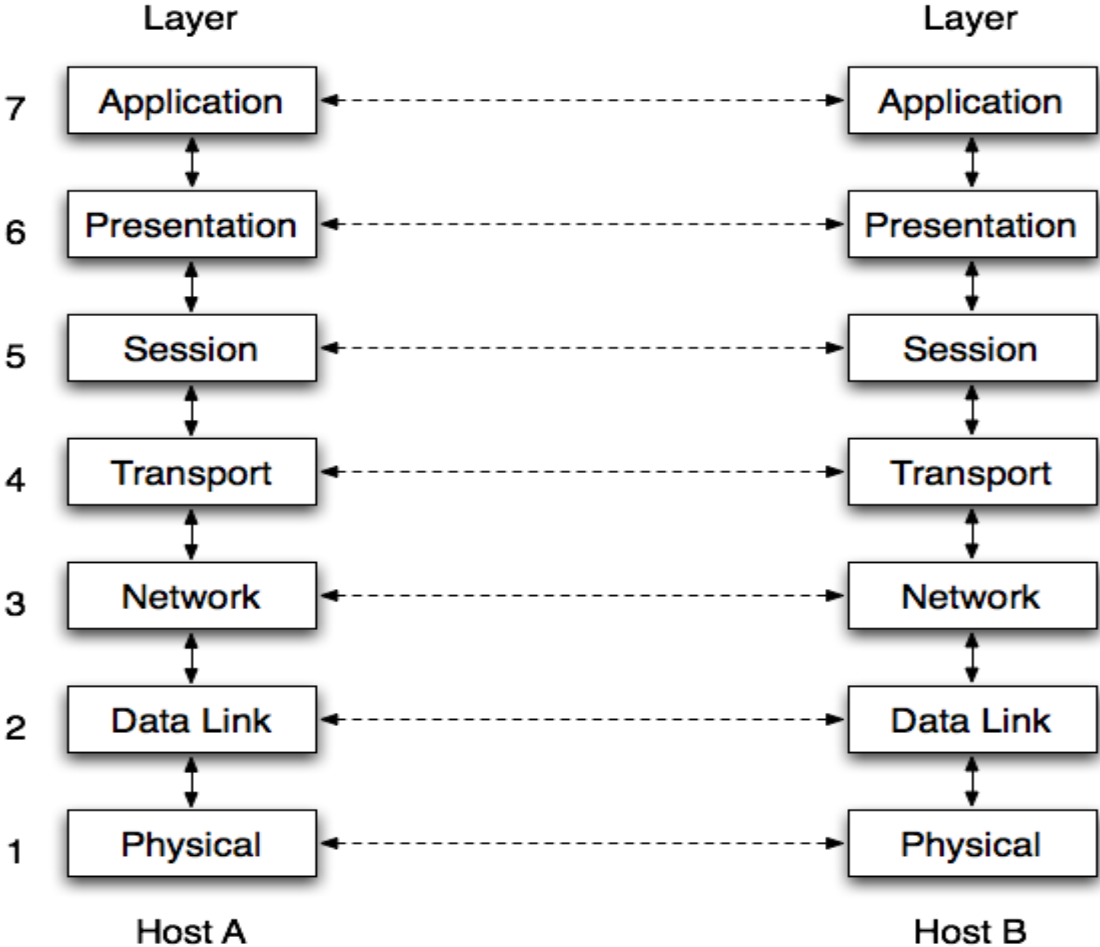
What is a protocol?

- Usually an agreed upon language and formats
- Computer networks use various sets of protocols
- Some in the set are complimentary
- Some may tend to compete
 - e.g. Token Ring versus Ethernet
 - e.g. TCP/IP versus IPX/SPX
 - e.g. AIM versus Yahoo! IM
- Why are there so many standards?!?!

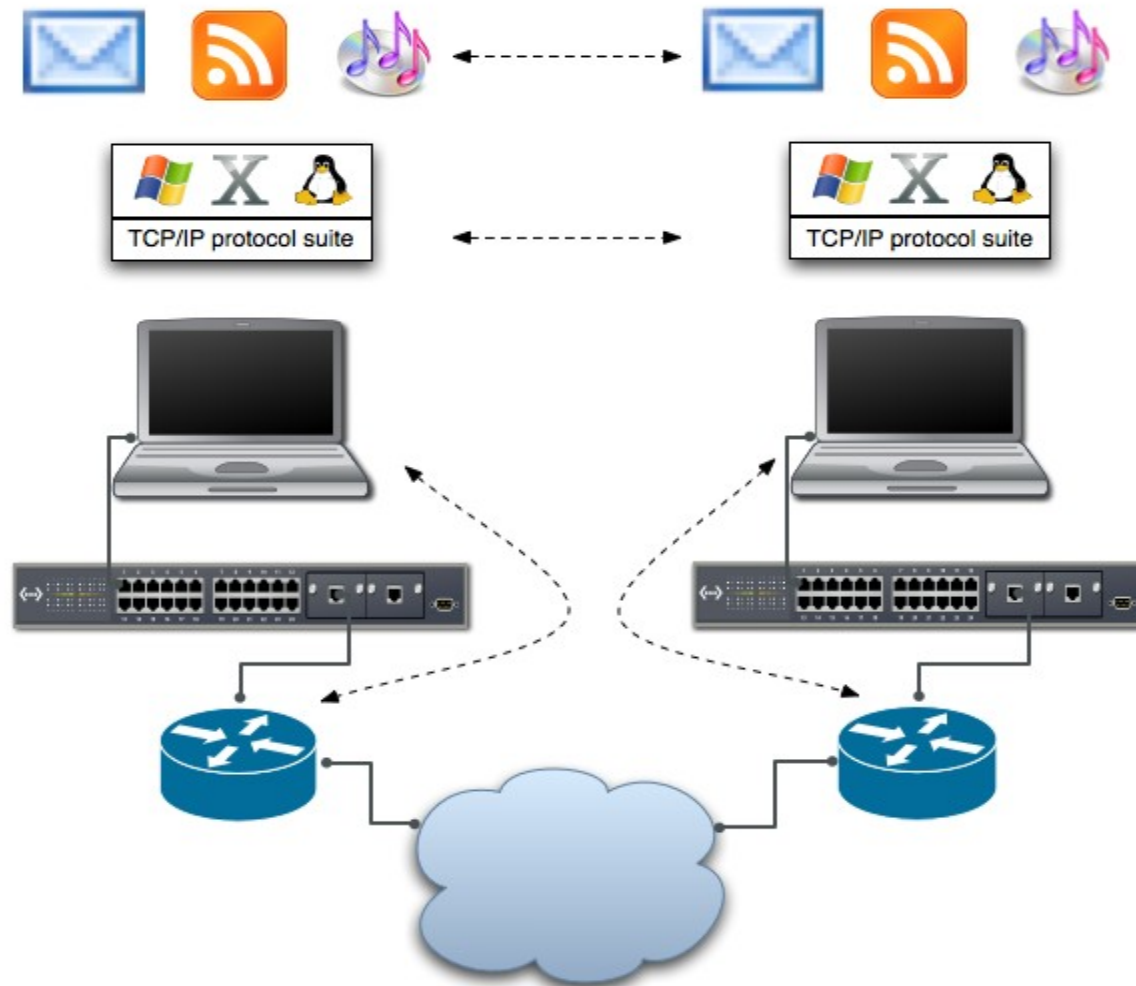
Are protocols immutable?

- Hindsight is 20/20 – tech advances, market changes
- Protocol definitions are sometimes vague
- Implementors may interpret documents differently
- Implementors may make mistakes
- Implementors may disagree with the standards
- Sometimes *conventional wisdom*, which is not always written down in an easy to find location, “fix” protocols as needed

Obligatory OSI Reference Model



A more practical model



Protocol layers and layering

- We tend to talk/think about protocols in layers
- Implementation however may not be so modular
- To really understand a protocol, be an implementor

Encapsulation visual

- Protocols are sometimes encapsulated within others
- If you're just looking at these slides outside of class with no video, well, you should have been here

An aside on terms

- Frames, packets, datagrams, messages, cells, PDU
- Headers, trailers, payload, data
- “What's your IP address?” (not “What's your IP?”)
- Host, workstation, PC, node, terminal
- Bandwidth versus capacity
- Pronouncing router (ROOT-er or ROUT-er?)
- Kludge, hack and a PoS
- BFR

Addresses, names and identities

- There is much confusion on what these are
- We'll punt and just discuss some of the issues
- Fixed size versus variable length
- Centralized or distribution assignment/allocation
- Problems when coupling locator and identifier?
- What about using a search (e.g. Google)
- Mapping issues? (e.g. domain name to IP address)

Forwarding and routing

- Source-based versus network-based
- Distance-vector versus link-state
- Policy controls and knobs
- Route advertisement authorization

Flow control

- How to go fast, but not saturate a bottleneck?
- Implicit versus explicit
- Windowing
- End-to-end control
- Network-based control, admission and enforcement
- Timers and retransmissions

Error control

- Detection
- Correction and recovery
- Performance considerations
- What are the causes of errors?
- Link-based or end-to-end controls?

Wireshark

- If you can, download and install this
- <http://www.wireshark.org>
- Now let's take a look at some traces

Fragmentation

- Maximum transmission unit (MTU) discovery
- Where does fragmentation occur?
- Any interoperability or performance impacts?

Network management

- Simplicity versus complexity
- In-band versus out-of-band
- Class-of-Service / Quality-of-Service
- Billing
- Automated configuration and type checking

Security

- Placement of security services
- Defense-in-depth
- Belt-and-suspenders
- Obscurity
- Walled gardens
- Risk assessment
- We will have much more to say about security later

Underground economy

- Quick look at what is going on in the underground
- If you were falling asleep, this might wake you up

Numbering systems

- Binary numbers are essential to computers
 - Two digits, one and zero
- Decimal numbers are what we're used
 - Ten digits, one through nine inclusive
- Hexadecimal numbers, often shorthand for binary
 - Sixteen digits, decimal numbers plus A through F
- Octal (eight), not as widely used, we'll ignore it

TELNET packet, one bit per inch

- What would a TELNET packet look like on the wire?
- If you're just looking at these slides outside of class with no video, well, you should have been here
- *note: this visual exercise lifted from Rich Seifert