

# DEFJAM - A Community Effort

Todd MacDermid - Syn Ack Labs

# DEFJAM Talk Overview

- What I want DEFJAM to be
- Convince you of the need for DEFJAM (aka “The Status Quo Sucks”)
- Convince you we can do it
- Convince you to join us in doing it
- Discuss the design

# What Is DEFJAM?

- **Distributed, Encrypted File Journaling And Messaging** (Many apologies for the bad acronym. I needed a name)
- A peer to peer method of exchanging files, voice, text, and eventually video communication, all over secure channels
- “Free.” BSD license
- Not yet written...

The Dream...





# DEFJAM Design Goals

- Easy enough to use for broad adoption
- “Supported.” Avoid tweaky APIs
- Secure by default, encrypted channels
- Useful. Transmits sound, files, text.
- Extendable (both in functionality and paranoia)
- Not dependent on central servers



How Much of Your  
Traffic do  
**YOU**  
Encrypt?

# “The Competition”

- WASTE
- Skype
- Haxial KDX (Formerly Netfone)
- Jabber
- GnomeMeeting and other Free VoIP
- And More!

# WASTE

The Good	The Bad
<p data-bbox="323 870 1292 1038">Encrypted, peer-to-peer file transfer</p> <p data-bbox="323 1156 858 1242">Cross-platform</p> <p data-bbox="323 1351 1190 1436">Code is broadly available</p>	<p data-bbox="1385 870 2354 1038">Licensing issues are fuzzy, at best</p> <p data-bbox="1385 1156 2184 1336">No way of removing someone from a group</p> <p data-bbox="1385 1447 2184 1533">Key exchange is painful</p>

# Skype

The Good	The Bad
<p data-bbox="323 874 1163 1038">Encrypted, peer-to-peer voice</p> <p data-bbox="323 1160 1256 1324">UI is a marvel of simplicity, both in install and use</p>	<p data-bbox="1385 782 2376 854">Licensing terms are onerous</p> <p data-bbox="1385 966 2390 1140">Traffic is dependent on a few corporate servers</p> <p data-bbox="1385 1252 2403 1528">Windows and PDA-only (and only some Windows platforms, at that)</p> <p data-bbox="1385 1641 2390 1712">Only 5-way conference, max.</p>

# Haxial KDX

The Good	The Bad
Encrypted, peer-to-peer voice, file transfer, and text	Windows-only Not free software (Annoyware) Key management. (All symmetric, OOB management). Voice is over TCP, and laggy

# Jabber

The Good	The Bad
<p data-bbox="323 770 812 844">Free software</p> <p data-bbox="323 962 1210 1044">standards-based protocol</p> <p data-bbox="323 1152 902 1330">Multiplatform implementations</p> <p data-bbox="323 1438 1141 1616">Cryptographic controls available via SSL</p>	<p data-bbox="1385 770 2326 948">No real structure provided for voice transmission</p> <p data-bbox="1385 1056 2390 1418">Focused primarily on IM/chat. File transfer is stubbed out, but dependent on HTTP connection</p> <p data-bbox="1385 1535 2326 1712">SSL is only supported trust model</p>

# Free VoIP Implementations

The Good	The Bad
<p data-bbox="323 870 812 942">Free software</p> <p data-bbox="323 1064 1037 1136">Standards-compliant</p> <p data-bbox="323 1259 1256 1422">Can interface to the POTS network</p>	<p data-bbox="1385 870 2088 1044">Cryptography is not supported</p> <p data-bbox="1385 1156 2390 1524">Due to standards requirements, it will be difficult to add cryptographic support</p>

# The Current DEFJAM Team

- Todd MacDermid
- Jack Lloyd
- Kathy Wang
- Carson Zimmerman
- John Schweitzer

# Past DEFJAM Team Projects

- Stegtunnel - Covert channels in real TCP connections
- Botan - C++ cryptographic library
- Morph - OS fingerprinting defeating tool (Presented yesterday!)
- Lsrscan and Lsrtunnel - Source-routed packet manipulation tools

# More DEFJAM Team Projects...

- GPG-Ezmlm - An encrypted mailing list
- OpenCM - Integrity-controlled content-management system
- <fnord> - Kernel module rootkit detector
- and more!

# Defend The Bill of Rights!



# Join the DEFJAM List

Send email to:

[defjam-subscribe@synacklabs.net](mailto:defjam-subscribe@synacklabs.net)

Operators are standing by  
Please have your GPG/PGP key ready!

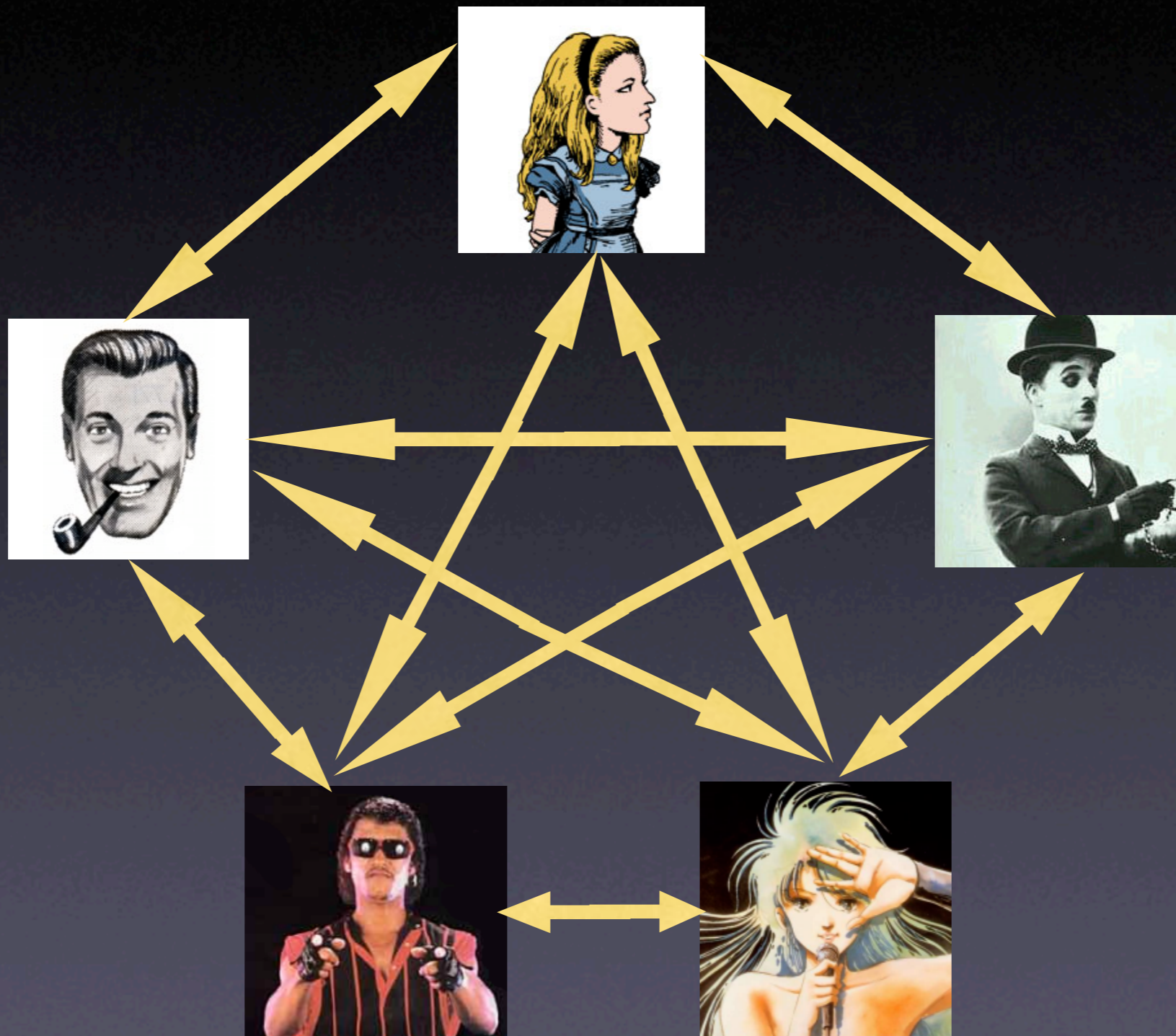
And if nothing else, we need help picking a new name

- EMP?
- Dead Drop?

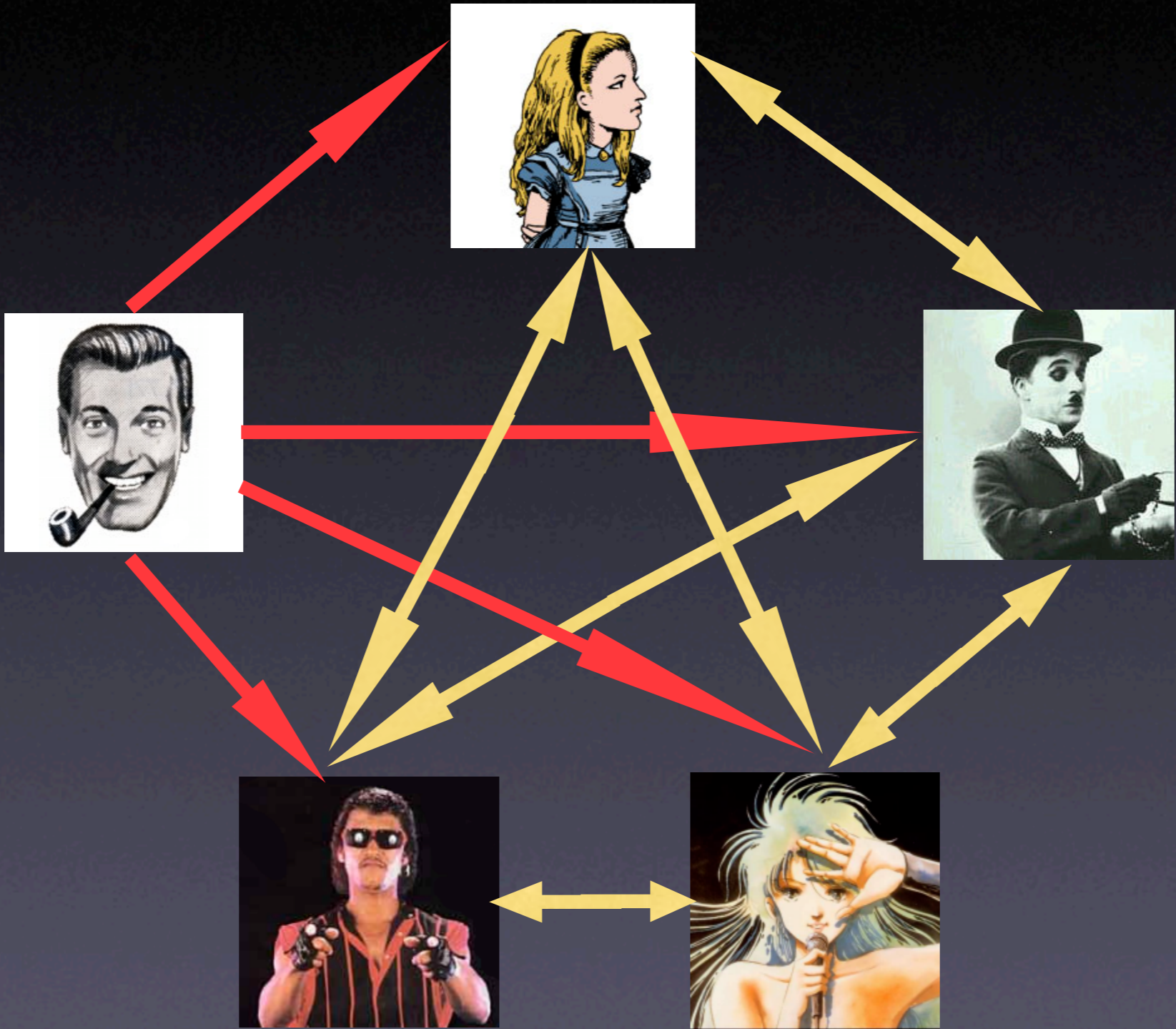
# DEFJAM Protocol Overview

- Default of UDP for all traffic
- Allows anonymizing and traffic analysis defeating measures, but not enabled by default
- Allows individual and group messages/transfers
- Allows sound, file, and text transfers

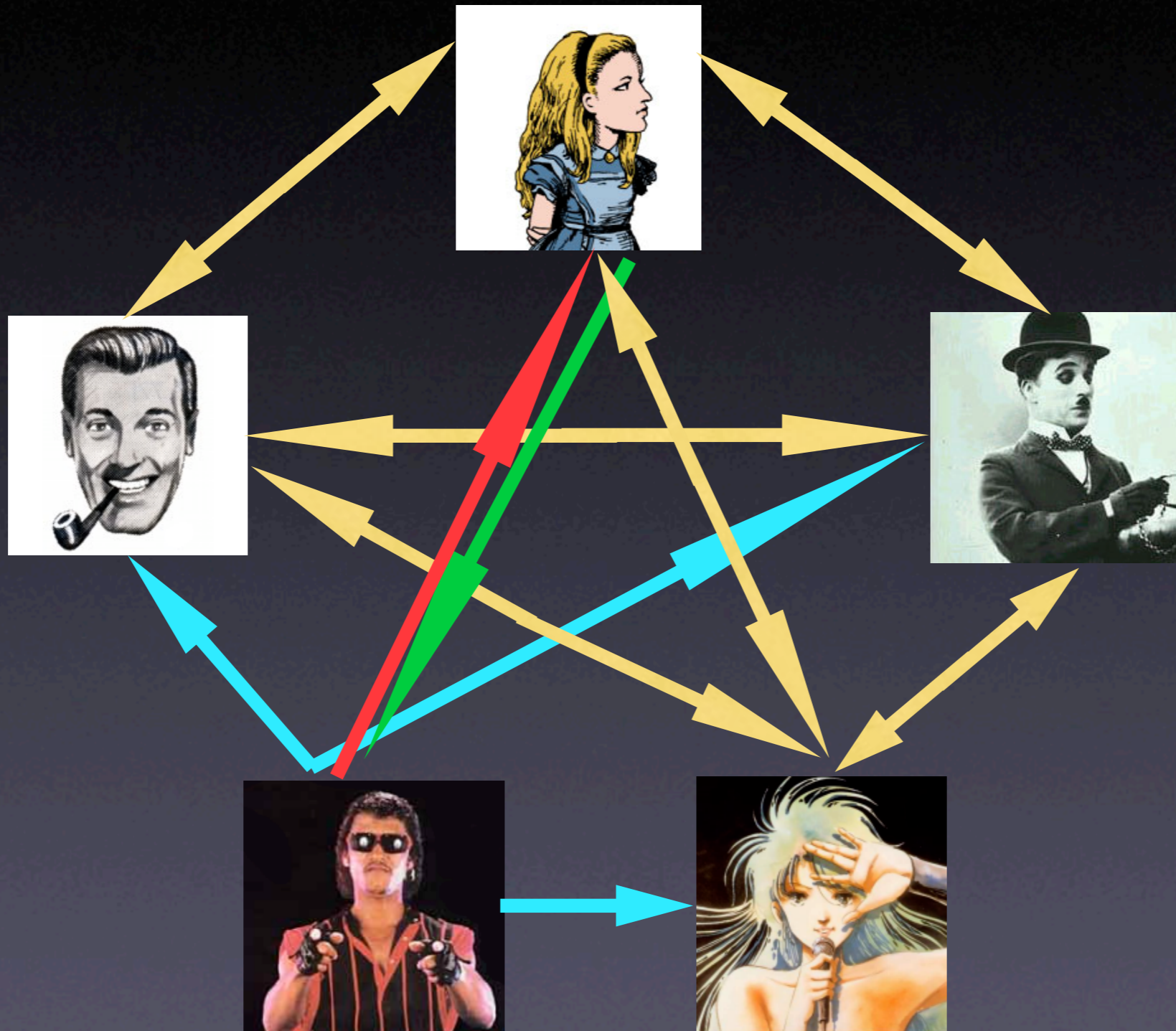
# Best Case: Fully Meshed Communications



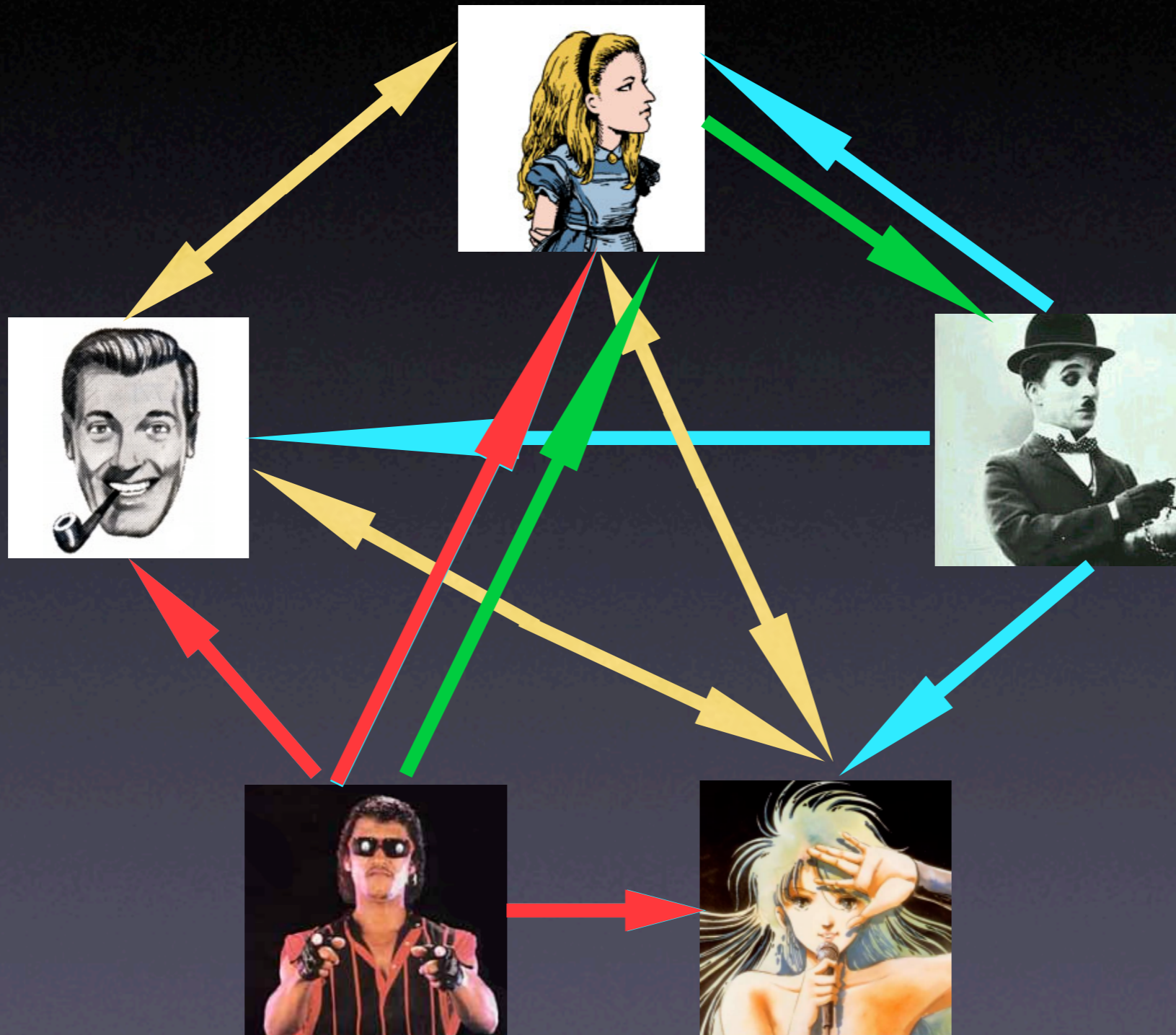
# Bob Talks to the Group



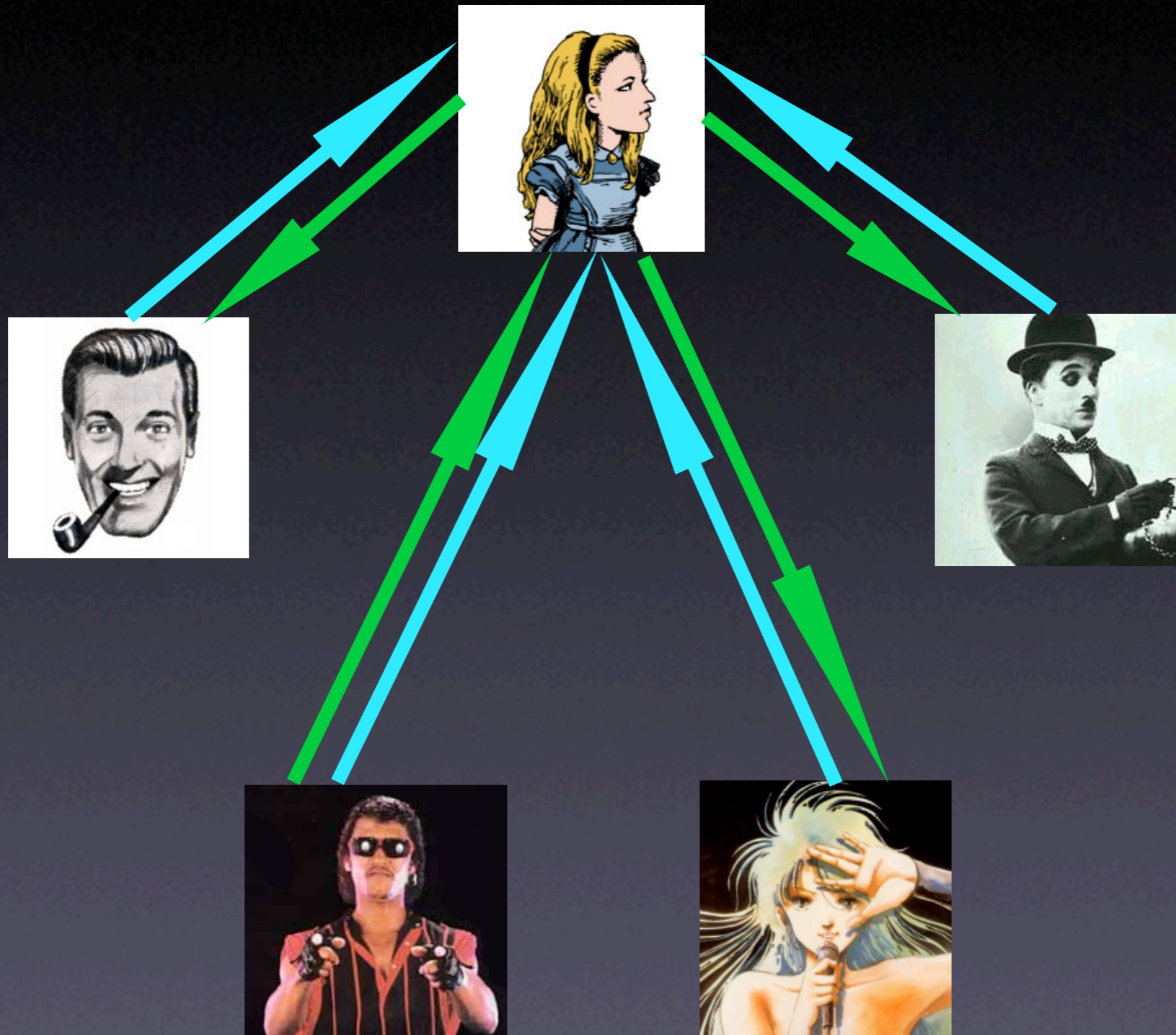
# Dave Behind NAT



# Dave and Charlie Behind NAT



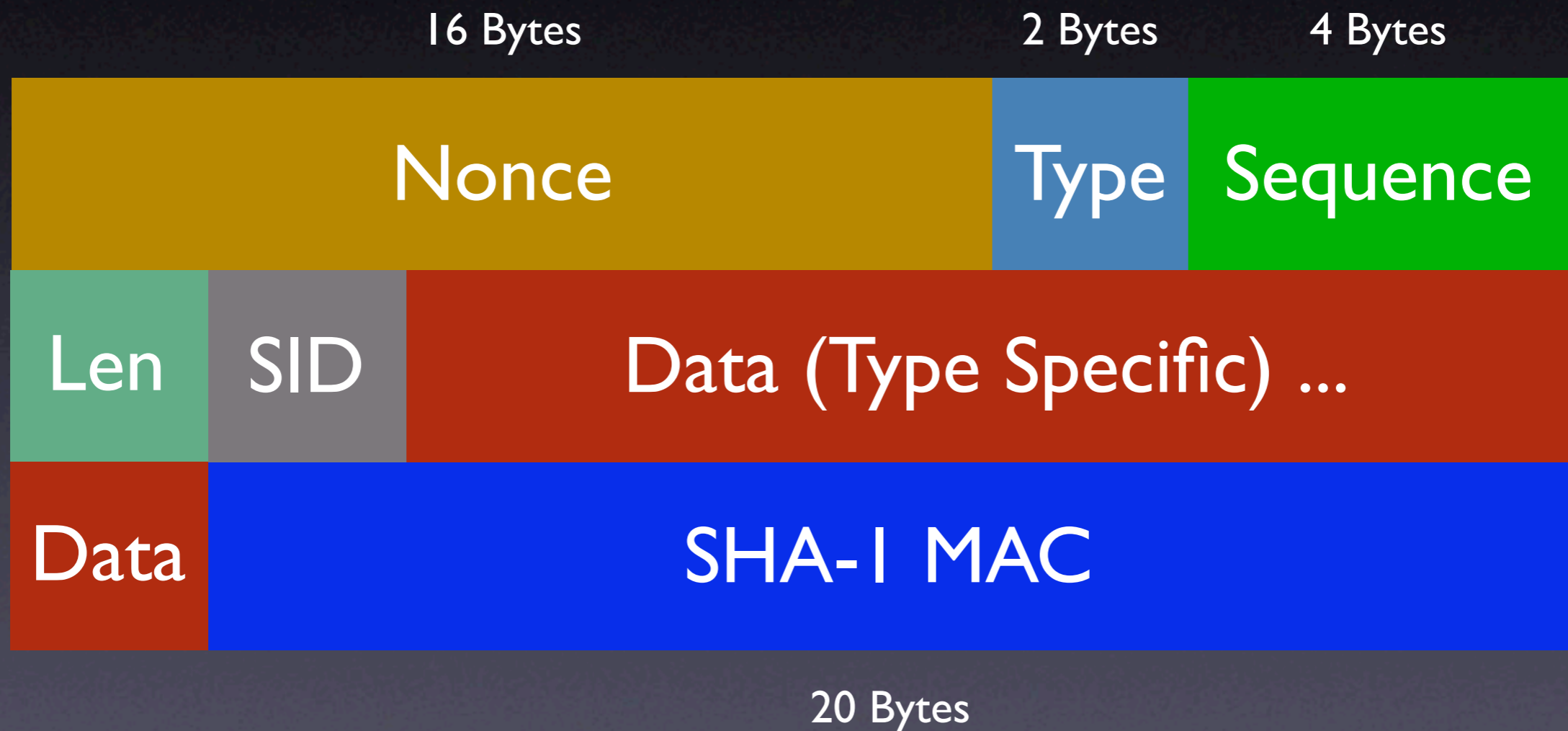
# Everyone Behind NAT Except Alice



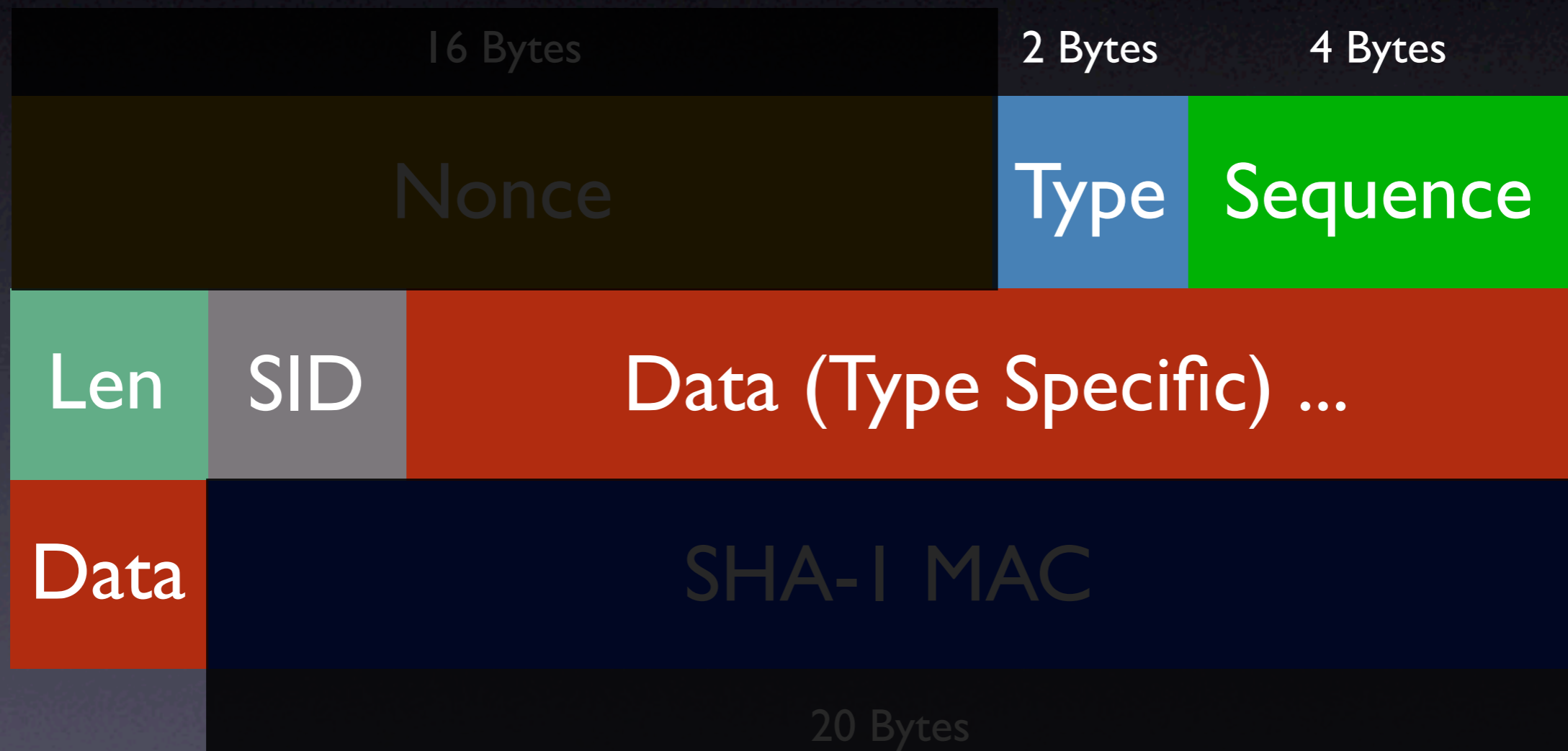
# Crypto Models

- SSL - “One key to rule them all”
- PGP - “Trust no one”
- SSH - “First time’s free, kid”

# DEFJAM Packet Structure



# DEFJAM Packet Encrypted Portions



# DEFJAM Packet Types

- Text Message
- Audio
- File Transfer
- Ping/Pong
- Ack
- Please Forward

# Future DEFJAM Types

- Video
- (Your data type here)

# Here Be Dragons...

- How do we initiate group advertisement/joining?
- How do we “administer” groups?
- What does our file transfer protocol look like? Can we swipe BitTorrent ideas?
- What is the user experience?