Designing Manageable Protocols

Andrew Cormack

Chief Security Adviser

UKERNA

Why Manage Networks?

Networks have production uses

- Teaching, assessment, administration, video conferencing, …
- Time-critical, bandwidth-criticial, reliability-critical

Bandwidth is finite

Some things are more important than others

- Different priorities in different organisations

Important things should have priority

- Helps if priorities are written down!

Management Tools?

Manager told – “Service X is important”

Manager sees – IP packets

Packets have

- Source & destination address
- Source & destination port
- Initial TCP packet has a direction

How to map packets to services?

- Need help from protocol design

Management Requirements

Identifiable

- Services give rise to recognisable network flows

Controllable

- Services can be permitted on some network segments
- Services can be denied from some network segments

Non-hazardous

- My use of a service must not be a hazard to others
- My use of a service should not be a hazard to me

Management Assumptions

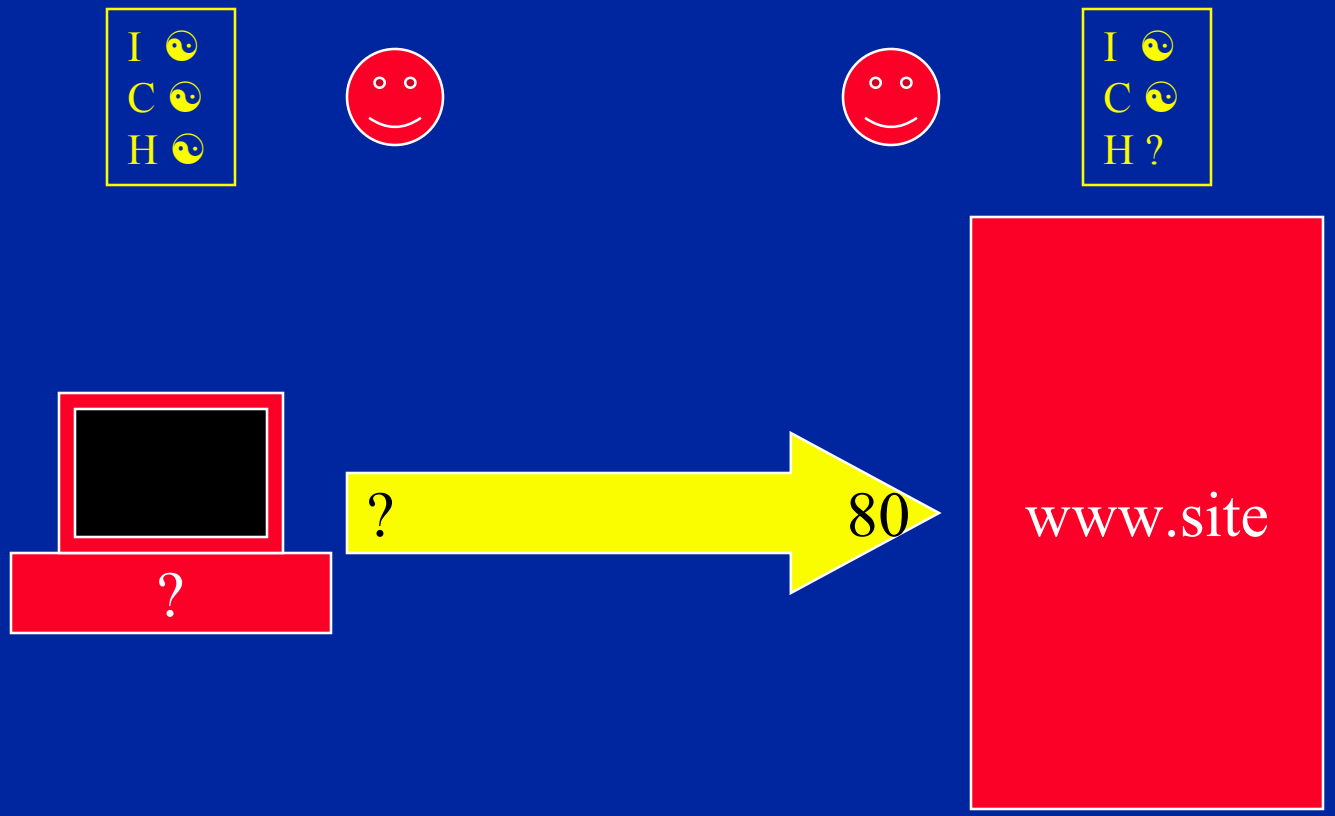
Least-worst assumptions

- Port number identifies service
  - E.g. port 80 = web
- IP address(es) identify location on network
- Source is client; destination is server [TCP only]

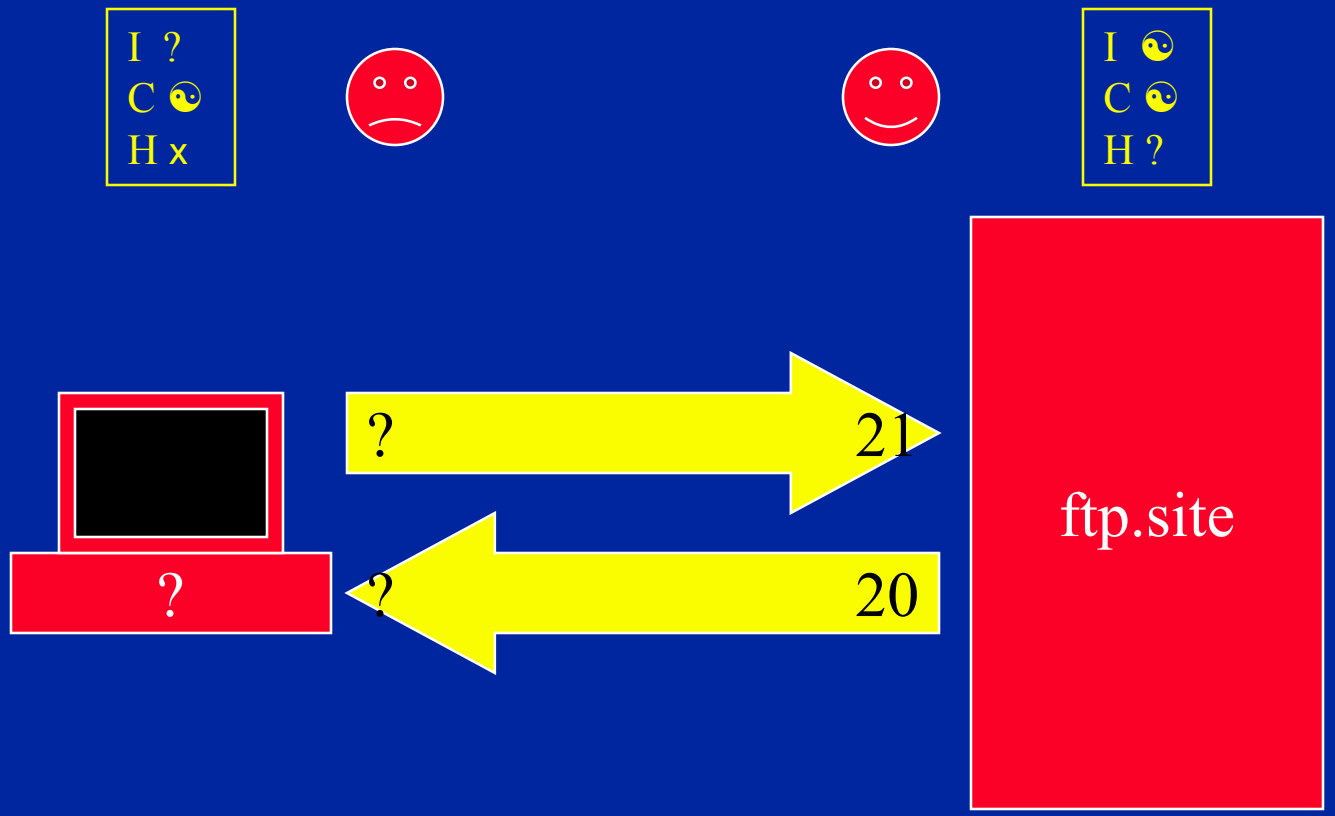
Dangerous assumptions

- IP address identifies person
- Port <1024 means trusted

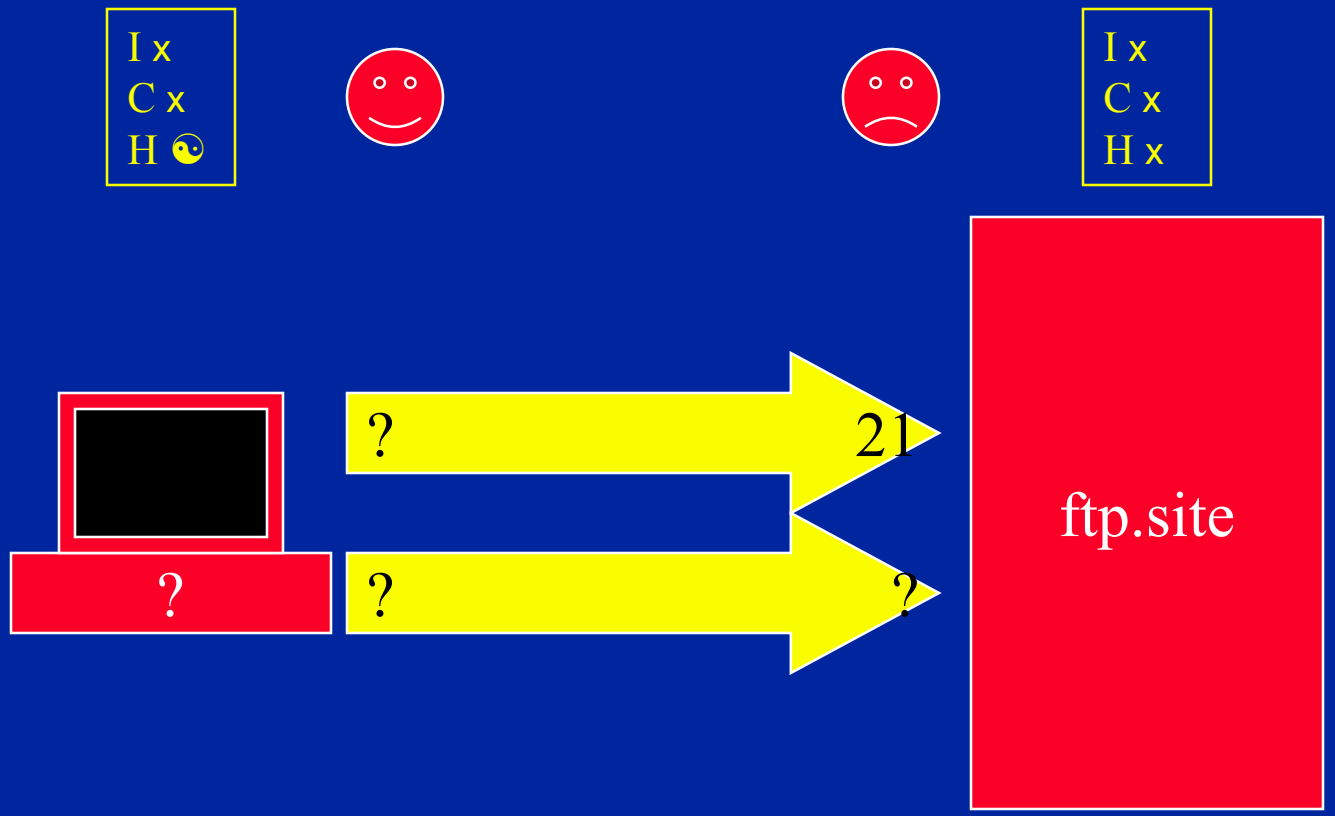
Case Studies – HTTP



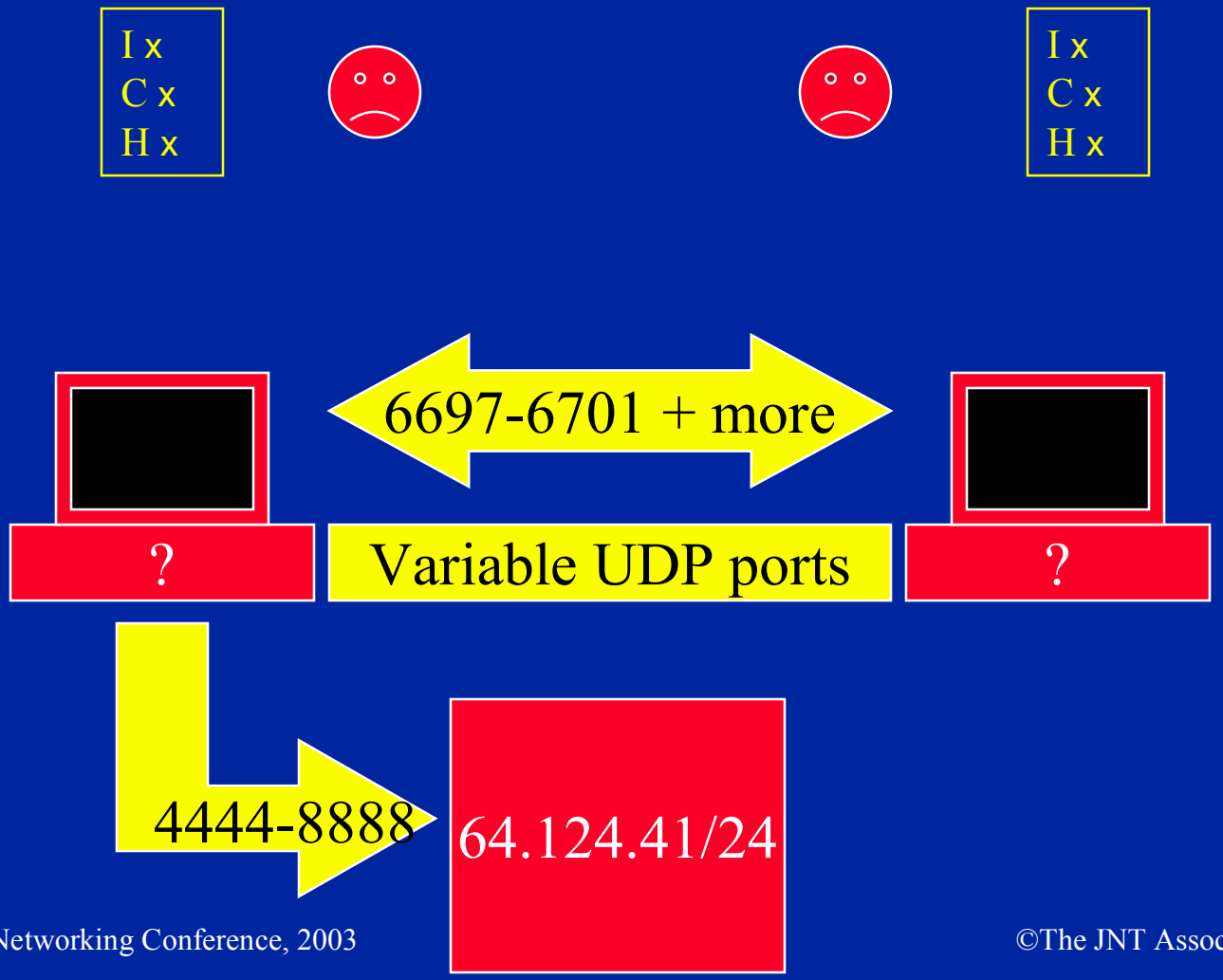
Case Studies – FTP



Case Studies – passive FTP



Case Studies – P2P (Napster)



Future developments

Dynamic address allocation

- DHCP or NAT
- Must align address allocation with managed groups

IP version 6

- Little change to manageability
- Port numbers may be buried in a chain of headers
- Encryption may make application layer invisible
- Mobility is extreme dynamic address allocation

Conclusion: Protocols need

- Identifiable traffic flows
  - Well defined, appropriate use of reserved ports
- Clarity over relationship between hosts
  - Direction of initiation must be apparent
- Support for layered protection
  - Expect to meet firewalls; work with proxies
  - Application proxies may be only option

Give managers options

YES/NO is not enough