CS314-10-32

Summing up: How the Internet Works

- Important protocols we haven't got time for
  - We haven't said nearly enough about security
- How things fit together
- Guiding principles
- Questions?

314 s2c Exam, 2010

- Exam Date: Thursday 28 October 2010
- Time: 2:15 - 4:30 p.m.
- 11 short-answer questions
    - 100 marks total
    - 20 for part 1, 40 each for parts 2 and 3
- Material covered includes
    - All the lecture slides
    - Assignments

Other infrastructure topics

Background slide

- PPP (point-to-point protocol)
- EAP, RADIUS, DIAMETER
  - Authentication, authorisation
- IPSec, IKE (Shay 11.3)
  - Applies to IPv4 *or* IPv6
- VPN (virtual private networks)
- NAT
  - Network address translation
- Firewalls
- SOCKS (firewall traversal)
- Multicast (Shay 11.2)
- Mobile IP, mobility in general
- SASL (simple auth & security)
- SLP (service location)
- RSVP (Shay 11.2)
- ROHC (header compression)
- iSCSI (SCSI over IP)
- RDMA (remote DMA)

Other application topics

Background slide

- MIME (multimedia formats)
- SIP, ENUM
  - standards for voice over IP
- Video over IP
- PGP, S/MIME (secure email)
- Internationalised email
- Anti-spam solutions
- LDAP (directory)
- NTP (network time protocol)
- IPP (Internet printing protocol)
- NFS, AFS
  - Remote file systems
- NNTP (network news)
- RSS, ATOMPUB (feeds)
- Instant messaging
- Language tags
- Web Services
  - XML-based distributed computing over SOAP+HTTP
- Peer to Peer protocols
- Grid computing protocols

The kitchen sink - a list of topics

Background slide

- This is only to illustrate the complexity and richness of Internet protocols; don't learn it ...

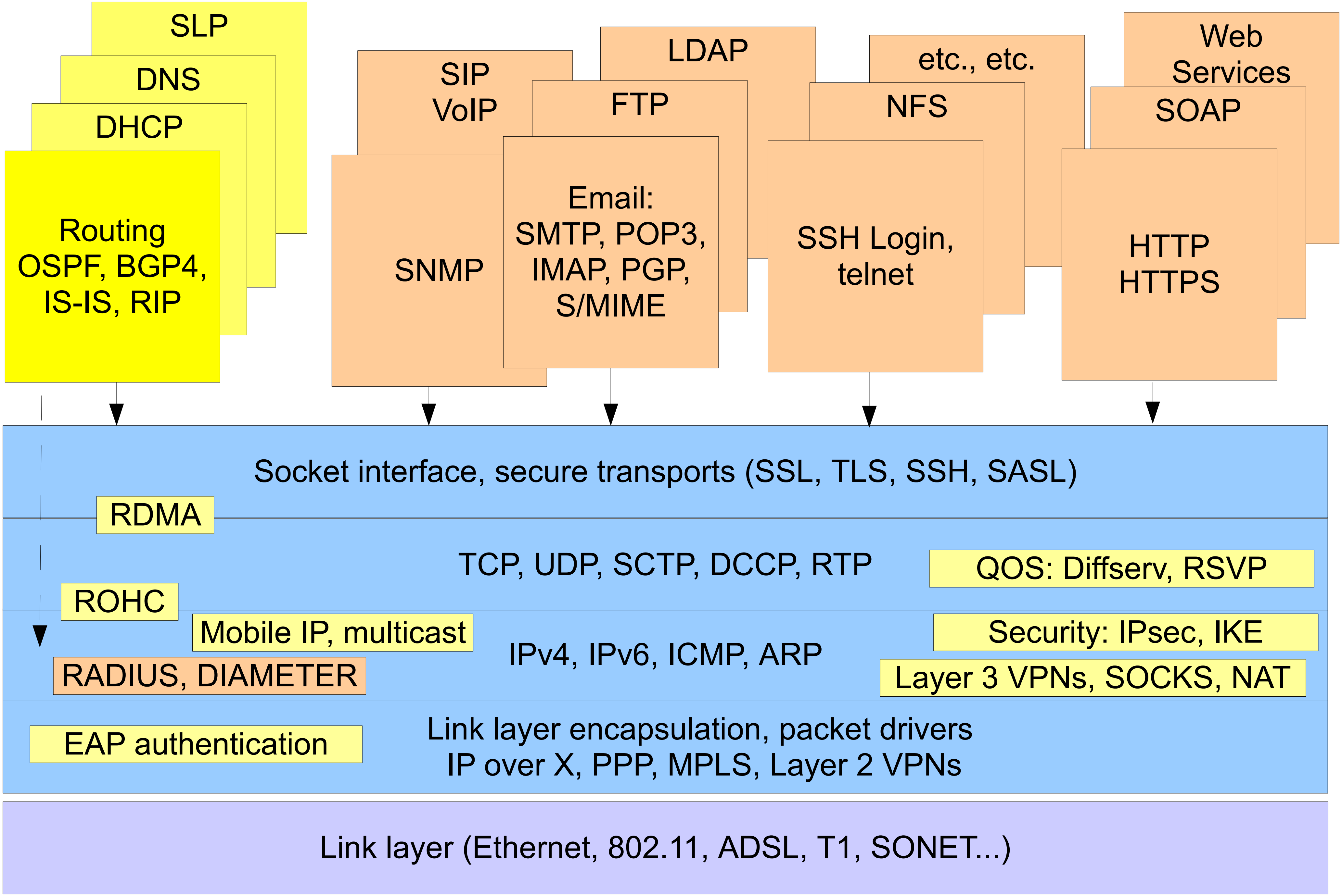
ACAP
APEX
ATOM
BEEP
CALSCH
CIP
DKIM
DNS
EDIINT
Email and MIME
ENUM
FAX
FTP
GEOPRIV
HTTP
Instant messaging
IPP
LDAP
Language Tags
Multimedia
NFS
NNTP
NTP
OPES
RSERPOOL
SEAMOBY
SIP, SIPPING, PPSIP
SLP
TELNET
TFTP
TIP

TN3270
URI, URL, URN issues
VoIP
WEBDAV
WIDEX
FECFRAME
iSCSI, iFCP
MIDCOM, STUN
ONCRPC
RDDP
ROHC
RMT
RTP, RTSP, SDP
SCTP
TCP
UDP
BEHAVE
BFD
BGP
DHCP
DIFFSERV, PCN
FORCES
GROW
HIP
ICMP
IPv4
IPv6
IPMTUD iscovery
IP multicast
IS-IS
L2VPN, L3VPN

MANET/AUTOCONF
MobileIP
NEMO
NETLMM
OSPF
PPP
PTOMAINE
PWE
RIP
Router Discovery
RSVP, IntegratedServices,
NSIS
SOFTWIREs
UDLR
VRRP
ZEROCONF
16ng (IP over IEEE 802.16)
6lowpan (IPv6 over 802.15.4)
GMPLS
IP over X
IPoIB
IMSS
MPLS
TRILL
ANCP
BMWG
CAPWAP
COPS
GSMP
IPFIX, PSAMP
IPPM
MIBs

NETCONF
POLICY
SNMP
Traffic Engineering
DIAMETER
EAP
IDX
IEPREP, ECRIT
INCH
IPSEC, IKE
KERBEROS and GSS-API
KEYPROV
LTANS
NEA
OPENPGP
OPSEC
OTP
PANA
PKI
RADIUS
RPSEC, SIDR
SACRED
SASL
SEND
SOCKS
SSH
SSL/TLS and HTTPS
SYSLOG
S/MIME
XMLDSIG

Protocol stack



SLP

DNS

DHCP

Routing
OSPF, BGP4,
IS-IS, RIP

SIP
VoIP

SNMP

LDAP

FTP

Email:
SMTP, POP3,
IMAP, PGP,
S/MIME

etc., etc.

NFS

SSH Login,
telnet

Web
Services

SOAP

HTTP
HTTPS

Socket interface, secure transports (SSL, TLS, SSH, SASL)

RDMA

TCP, UDP, SCTP, DCCP, RTP

QOS: Diffserv, RSVP

ROHC

Mobile IP, multicast

IPv4, IPv6, ICMP, ARP

Security: IPsec, IKE

RADIUS, DIAMETER

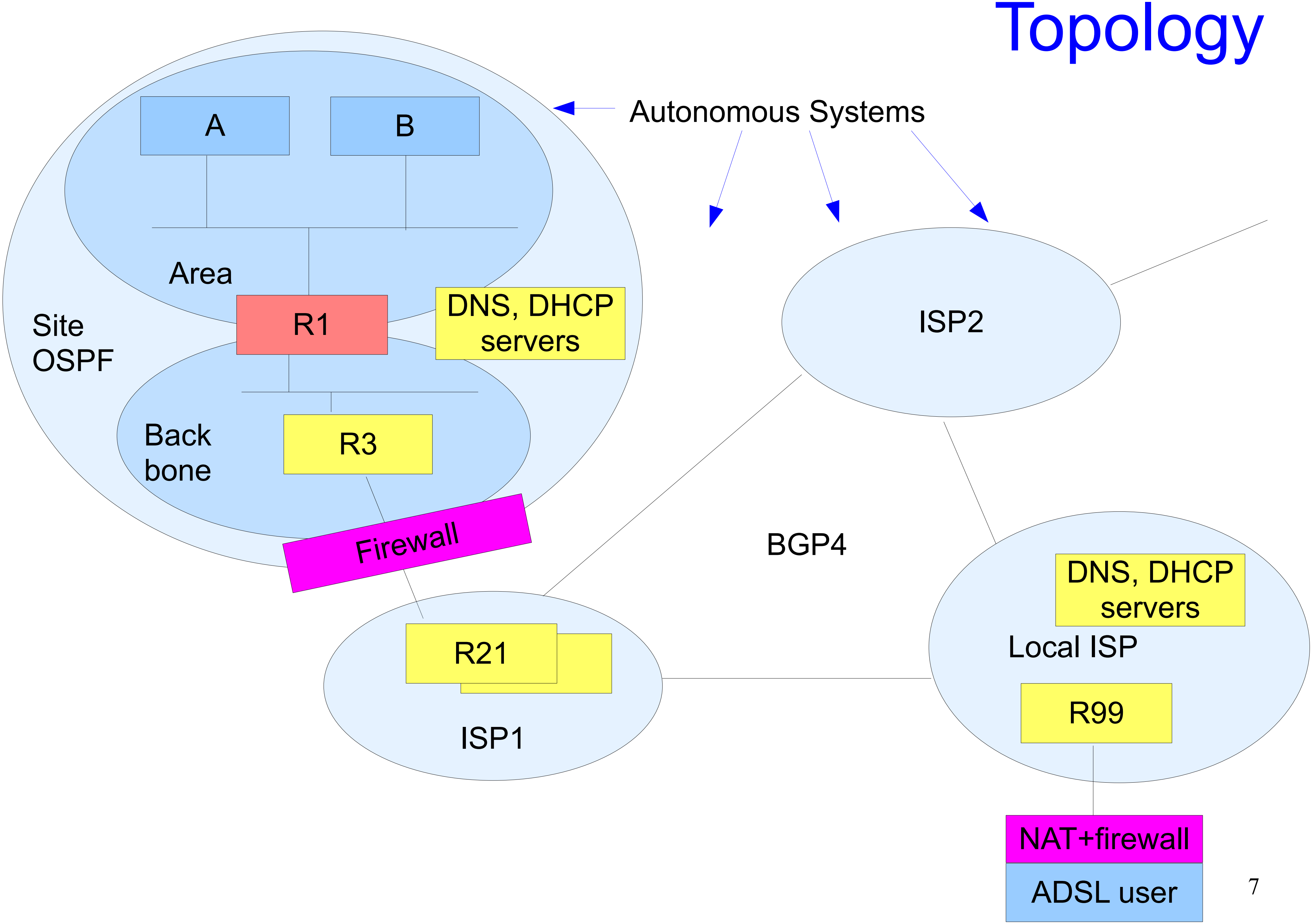
Layer 3 VPNs, SOCKS, NAT

EAP authentication

Link layer encapsulation, packet drivers
IP over X, PPP, MPLS, Layer 2 VPNs

Link layer (Ethernet, 802.11, ADSL, T1, SONET...)

Topology


Autonomous Systems
A
B
Area
Site
OSPF
R1
DNS, DHCP
servers
Back
bone
R3
Firewall
ISP2
BGP4
R21
ISP1
DNS, DHCP
servers
Local ISP
R99
NAT+firewall
ADSL user

The end-to-end principle (1)

Background slide

- Note how TCP works - it *assumes* that packets may be lost, delayed, corrupted or delivered out of order. The two ends of a TCP connection cooperate to overcome this
- Note how SSH works - it *assumes* that messages may be intercepted and that attackers may try to insert false messages. The two ends of an SSH connection cooperate to overcome this
- Note how DNS works - if a DNS (UDP) message is lost, no harm results except a delay.
- These are all examples of the end-to-end principle at work

The end-to-end principle* (2)

Background slide

- Certain required end-to-end functions can only be performed correctly by the end-systems themselves
- Any network, however carefully designed, will be subject to failures of transmission at some statistically determined rate. The best way to cope with this is to give responsibility for the integrity of communication to the end systems. A similar argument applies to intrusions
- No solution buried inside the network can give the same level of assurance as the end systems
  - For example, *end-to-end* encryption is intrinsically safer than *router-to-router* encryption

* *see References*

Other principles (1)

Background slide

- Heterogeneity by design
- Avoid duplicate solutions
- Scaleable designs
- Performance and cost must be considered as well as functionality
- KISS (keep it simple, stupid!)
- Modularity is good
- Good enough is enough (don't seek perfection)
- Minimise use of options
- Be strict when sending and tolerant when receiving

Other principles (2)

Background slide

- Be parsimonious with unsolicited packets, especially multicasts and broadcasts
- Circular dependencies must be avoided
- Objects should be self-describing (type and size)
- Nothing gets fully standardised until there are multiple instances of running code
- Avoid design that requires hard coded addresses
- Addresses must be unambiguous (NAT breaks this!)
- Designs should be fully international
- All protocols need strong security (early ones didn't!)

References

Background slide

- RFC 1958: Architectural principles of the Internet
  - End-to-end principle paraphrased from "End-To-End Arguments in System Design", J.H. Saltzer, D.P.Reed, D.D.Clark, ACM TOCS, Vol 2, Number 4, 1984
- "Why the Internet only just works" by Prof. Mark Handley, University College London

  http://www.cs.ucl.ac.uk/staff/M.Handley/papers/only-just-works.pdf

Questions?

- What haven't you understood in this course?