

# A small network in JANET

Workshop 31, York  
April 2003

Rodney Tillotson  
JANET-CERT  
R.Tillotson@ukerna.ac.uk

# A small network in JANET

- " Networks
- " Considerations
- " Scenarios

# Networks

- „ Minimal network
- „ Not so small
  
- „ Distribution of functions
- „ Security
- „ Cost

# Minimal network

- „ Home dialup
- „ What do you get?
- „ Who does it?
- „ How is it secure?

# Minimal requirements

- " IP address[es]
- " Web access
- " Mail
- " Web server
  
- " Domain name
- " Security provisions

# IP address

- Single address
- DHCP
  - dynamically assigned
  - DNS resolver[s]
  - gateway (default route)

# Web access

- eg `http://www.ja.net/`
  - query ISP DNS resolver
  - route to gateway
  - get IP
  - connect to IP
- May be a cache
- May be a proxy

# Outbound mail

- ISP smarthost

# Incoming mail

- Delivered to ISP
  - POP3, Web access, IMAP
- 'MX' record to IP (ISP's)

# Incoming mail domain

- Shared domain
  - ukerna@hotmail.com
- Divided domain
  - rodney@ukerna.isp.co.uk
- Arbitrary domain
  - rt@ukerna.ac.uk

# Web publishing URL

- Shared domain
  - <http://www.isp.co.uk/~ukerna/>
- Divided domain
  - <http://www.ukerna.isp.co.uk/>
- Arbitrary domain
  - <http://www.ukerna.ac.uk/>

# Web publishing IP

- „ 'A' record to IP
- „ ISP's server
- „ Upload process
  - mail, FTP, Web service

# Security

- Integrity and privacy of data
- Impersonation
- Control of your network

# Integrity and privacy

- „ Physical (storage)
- „ Passwords (access)
- „ Encryption (transit)
  - wireless
  - mail
  - Web upload

# Impersonation

- Authentication for connection
  - CLI
  - MAC
  - Password

# Control of your network

- Denial of Service
  - disconnection
- Network device
- PC

# Network device

- Simple
- Update (monitor?)
- Incorporate firewall

# PC

- " OS update
- " Anti-virus
- " Personal firewall
- " Backup
  
- " No server functions

# Simplest security

- Simple services
- Others may be harder
  - NetMeeting
  - IM
  - Games
  - P2P

# Solved problem

- Server functions all SEP
- Configuration mostly SEP
  - DHCP, PnP, USB
- Few people
- Few devices

# Networks (reprise)

- (Minimal network)
- Not so small
- More people
- More services

# Consumer market offers:

- More IP addresses
  - and static addresses
- NAT and firewall
- Instant gratification
- Internet servers not expected

# Small business market offers also:

- „ Outsourcing
- „ DNS delegation
- „ Internet server presence
  - mail, Web servers
- „ Appliances

# JANET offers:

- „ DNS delegation
- „ Limited outsourcing
- „ Internet server presence

# Not so small requirements

- „ External services
- „ Internal services
- „ Supporting services
  
- „ Considerations
  - cost
    - „ capital, ongoing
  - security

# External services

- Nameservers
- Web server
  - Web services
- Mail
  - inbound, outbound
- Outbound Web proxy

# Internal services

- DNS resolver
- Mail reading
- Internal Web
- Filestore
- Applications

# Supporting services

- " Authentication
- " Time
- " Remote access
- " Backup
- " Firewall[s]
- " Monitoring
- " Address management

# The solution network

- 16 (8?) global IP addresses
  - NAT for the rest
- External
- Internal servers
- Staff
- Students

# Generic network

- External firewall
  - external addresses
- NAT
- Firewall internal servers
  - firewall staff
  - firewall students

# Generic network (2)

- Default deny policy
  - hard to stick to,  
but a good starting point
  
- *Building Internet Firewalls*
  - Figs 4-5, 4-7, 4-8, 4-12

# Networks (reprise)

- „ (Minimal network)
- „ (Not so small)
  
- „ Distribution of functions
- „ Security
- „ Cost

# Combining functions

- Cheaper
- More complicated

# OK to combine

- „ Inbound and outbound mail
- „ Primary NS and resolver
- „ Outbound proxy and NAT
  
- „ Products expect these

# Not so good to combine

- „ Web server and outbound proxy
- „ External and internal Web servers
- „ External mail and mail reading
  
- „ But you may have no choice

# Outsourcing functions

- „ Web server
- „ Mail in, out partly
- „ Probably not mail reading
- „ Probably not primary DNS
- „ Not DNS resolver

# Outsource Web server

- „ Technically straightforward
- „ Many recent problems
  
- „ Commercial or community
- „ Combine with maintenance
  - or devise out-of-band update
- „ Combine with site design

# Outsource mail transfer

- „ Get filtering and blocking
  - AV, UBE, content
- „ Still need server
  - but a little simpler
- „ Failures may look a little odd
  
- „ JANET MailerShield
- „ MessageLabs

# Outsource mail reading

- Web mail
  - Hotmail
  - JANET?
- Provider has to maintain account details

# Outsource DNS

- Primary nameserver
  - JANET
  
- Resolver, probably not
  - internal names
  - failure of connection
  
- Retain on-site secondary

# Outsource management

- Switches and firewalls
- Servers
- Clients
  
- Bundled management
  - small business market

# Management of outsourcing

- „ Service level
  - responsibility
- „ Flexibility
- „ Interaction between providers

# Security policy

- No policy, no security
- Aims
- Responsibilities
  - authority
- Routers, servers, clients, users

# Other policies

- „ Some may be procedures
- „ Monitoring and logging
  - data retention, access
  - legislation
- „ System and network administration
- „ Disaster recovery
- „ Business continuity

# System admin procedures

- " Patches, AV
- " Backup, restore
- " User management
- " Response to security alerts
- " Change management
  - adding, removing things
- " Response to component failures
  - risk analysis

# Scenarios

- „ Minimum technical skill
- „ Minimum equipment
- „ Minimum external dependencies
- „ Minimum Internet involvement

# Minimum technical skill

- „ Outsource everything
- „ Minimum skill is not zero
- „ Contract management

# Minimum equipment

- No server
  - NAT firewall, switch
- Think about server functions
- Partition your network
- NAT and firewall on server
  - two or more interfaces

# Minimum dependencies

- Primary nameserver
  - mechanics of delegation
- Keep servers simple
- Backup MX?
  - perhaps not desirable

# Minimum Internet

- Web access only?
  - proxy
  - filtering
  - NAT

# Skills are critical

- Invest in people
  - long-term commitment

or

- Buy services
  - stable budgeting

# Brain cell filler

- If you only remember one thing . . .
- Patch and update
- Default deny

# References

- Windows 2000 server documentation
- Building Internet Firewalls
  - 2nd edition June 2000
  - Elizabeth D Zwicky, Simon Cooper, D Brent Chapman
  - ISBN 1-56592-871-7
  - 890 pages, £35.50
  - <http://www.oreilly.com/catalog/fire2>

# References (2)

- JANET security policy
  - [http://www.ja.net/documents/JANET\\_security\\_policy.html](http://www.ja.net/documents/JANET_security_policy.html)
- Sample security policies
  - <http://www.ja.net/CERT/JANET-CERT/regulation/aups.html>

# References (3)

- „ Use of Firewalls in an Academic Environment
  - [http://www.jisc.ac.uk/index.cfm?name=project\\_firewalls](http://www.jisc.ac.uk/index.cfm?name=project_firewalls)
- „ Domain Name Service
  - [http://www.ja.net/documents/tg\\_dns.pdf](http://www.ja.net/documents/tg_dns.pdf)