Tunneling

Why?

∑ support unsupported but routable network protocol
e.g., AppleTalk, IPX, CLNP
get around network managers
get across the Internet

∑ support unroutable protocol in an internet
e.g., NetBios, LAT

∑ support protocol with complex routing
e.g., SNA, APPN

∑ keep backbone simple

∑ build private network over public network

∑ mobile hosts

∑ provider selection

How?

∑ most setup TCP (reliable) session between 2 devices

∑ some do UDP

∑ encapsulate packet in TCP or UDP

∑ send to 'other end' to be dis-encapsulated

∑ can be a problem if original packet large
    encapsulating agent must fragment the packet
    'other end' must reassemble

∑ or small MTU in path
    router along the way must fragment
    'other end' must reassemble

Where?

∑ often in user-controlled device
e.g., Gator box

∑ Gator box could be under control of NOC

∑ sometimes in NOC controlled router
e.g., AURP

∑ sometimes at originating host
more in future

Advantages?

∑ keeps backbone pure

∑ minimizes expertise required to run backbone

∑ utilize hostile backbones

∑ allow powerfull IP routing to maintain path
route around breaks

∑ gives reliable transport path
e.g., SDLC passthrough

Advantages?, contd.

∑ reduces parallel network requirements
e.g., DLSw

∑ user can control access
can configure to filter out unwanted nodes

∑ support for experimental protocols

∑ support for security
can encrypt encapsulated packet
can stop traffic analysis
useful in mobility, hides location

∑ support for private networks
encapsulate IP in IP

Use in IPng

∑ part of transition plan

∑ single IPng host on IPv4 network
can tunnel over IPv4 to IPng router
can tunnel over IPv4 to IPng host
can be used for debugging
can be used to support expanded IPng functionality

∑ IPv4/IPng router with IPv4 backbone
can tunnel to another IPng router
can build virtual IPng backbone before backbone routers support IPng
can build virtual IPng backbone before backbone routing protocols support IPng

Use on the Internet

∑ support for OSI CLNP
- NSF routers do not support CLNP
- CLNP support required by NSF
- external encapsulating device on regional's DMZ
- encapsulates CLNP in IP
- talks to other similar boxes
- static routing

∑ security
- products implement encrypted virtual enterprise networks
    - over the Internet
- encrypted point to point tunnels
- looks just like private enterprise network
    - only slower & much cheaper

Use in Enterprises

∑ most common to support AppleTalk & IPX over enterprise
backbone that does not support them

∑ single protocol backbones
TCP/IP, SNA or DECNET only backbone

∑ limited protocols backbones
TCP/IP & DECNET only

∑ few devices
only have 5% Macs

∑ Data Link Switching (DLSw)
someday

Why not Native?

∑ political

want a 'pure' network
boss said no
network manager said no
committee said OSI

∑ knowledge

don't want to learn AppleTalk routing

∑ bias

not a 'real' protocol
too chatty

∑ better control

backbone network routers can't filter well

Why not Native? contd.

∑ organizational
no strong central management
no way to enforce addressing plan
network by IS dept
Macs in CS & research

∑ security
students use Macs, administration uses PCs
can isolate pesky students

∑ scale
there just is not enough of that strange protocol

∑ ex-cathedra
everyone can/should run TCP/IP

Why Native?

- better control (assuming good routers)
    - filter the hell out of it

- for each LAN
    - only accept specific routing information
        - only assigned LAN numbers
    - only pass specific traffic
        - block bogon packets

- can be a performance problem for some routers

- most common problem in PC LANs is duplicate LAN numbers
    - router can limit effect

Why Native? contd.

∑ service advertizements can be a problem
    why does LA need to know the printers in NYC?

∑ filter in routers
    only advertize out side of LAN what should be known

∑ security
    can specifically block particular networks or hosts
    (not hosts with AppleTalk)

Why Native? contd.

∑ statistics
    can see actual trafÆc

∑ with encapsulation, it's all IP

∑ can see usage patterns
    can identify bottlenecks and performance problems

∑ encapsulated packets larger
    more load on WAN links

∑ encapsulation does not reduce chatty nature
    just hides it in IP
    AURP-like protocols can help

Summary

∑ sometimes have to encapsulate

  CLNP over NSFnet backbone
  to get past that ogre of a network manager
  routers do not support protocol (e.g., DLSw)
  using commercial service for intra-enterprise network
  virtual network on real network
  security on public network

∑ but when you don't don't

  better control
  better statistics
  better picture of network functions
  compartmentalize services
  better access control