

VPN Architectures

David Morgan

VPN Characteristics

- NETWORK
 - member workstations in touch by IP address
- VIRTUAL
 - physically *not* a network
 - geographically *dispersed*
 - *no* common hub/wire
 - piggybacks *somebody else's* wire (eg, internet)
- PRIVATE
 - *but* traffic on that wire can't be tapped

Technical Components

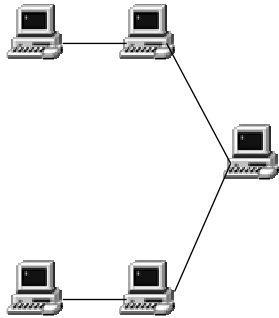
- Tunneling
- Authentication
- Access control
- Data security

Placement-based Architectures

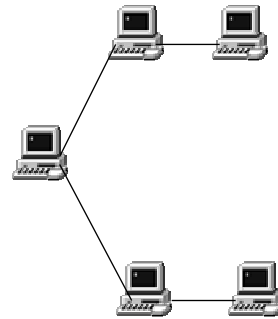
- Site-to-site Intranet VPN
- Remote access VPN
- Extranet VPN

Two Unconnected LANs

Network A

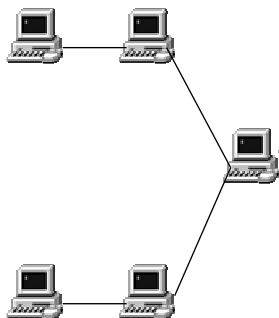


Network B

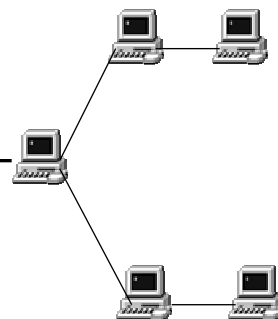


Site-to-site via traditional connection

Network A

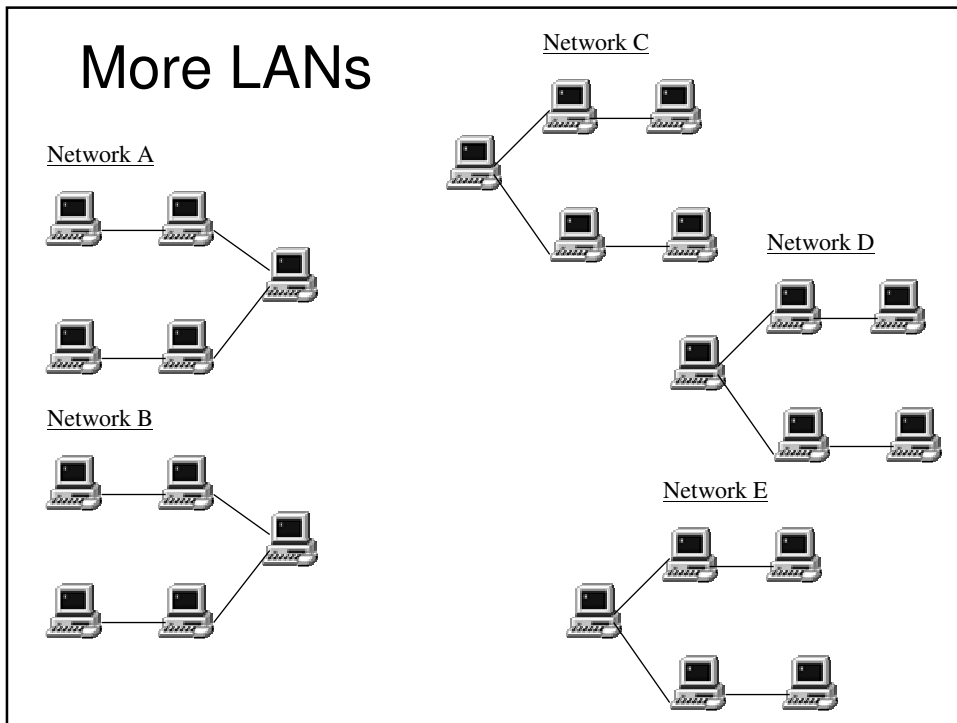


Network B



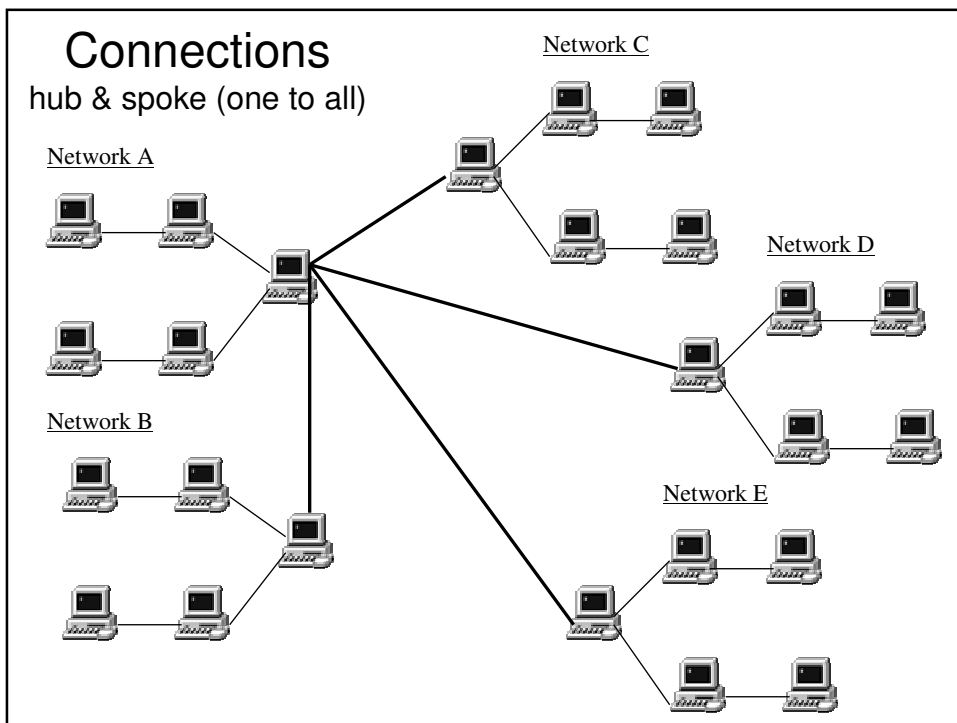
Dedicated leased line
or
Frame Relay circuit

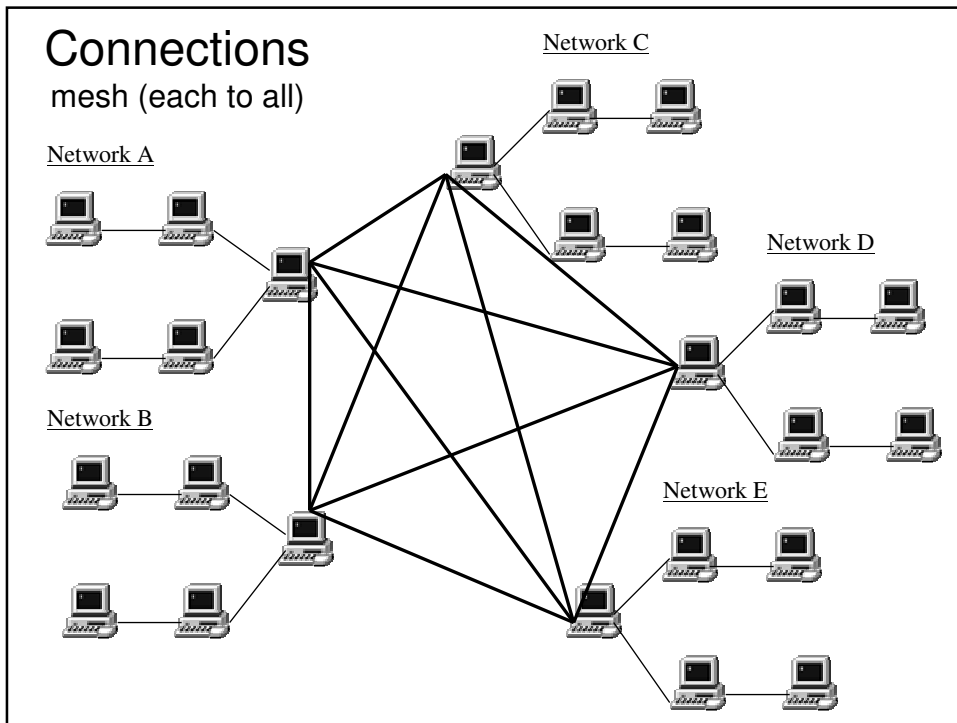
More LANs



Connections

hub & spoke (one to all)





Number of connections

- Hub & spoke
 $n-1$
- Full mesh
 $n(n-1)/2$

Number of connections

Nodes	Number of Connections	
	Hub/spoke	Full Mesh
3	2	3
5	4	10
10	9	45
20	19	190
50	49	1225

Traditional connections

- Dedicated leased lines
- Frame relay PVCs (private virtual circuits)

Dedicated leased lines

- DS-0, DS-1, DS-3
- Bandwidth availability
 - within contract pipe size: always
 - beyond it: never
 - unused bandwidth wasted
- Distance-based pricing
 - mesh is expensive
- Adding site affects existing sites
 - CPE impact
- Security – inherent in line security
- No inherent redundancy

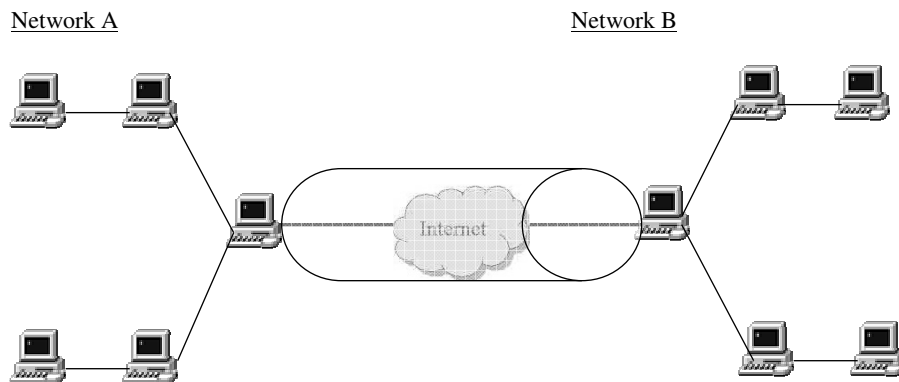
Frame relay

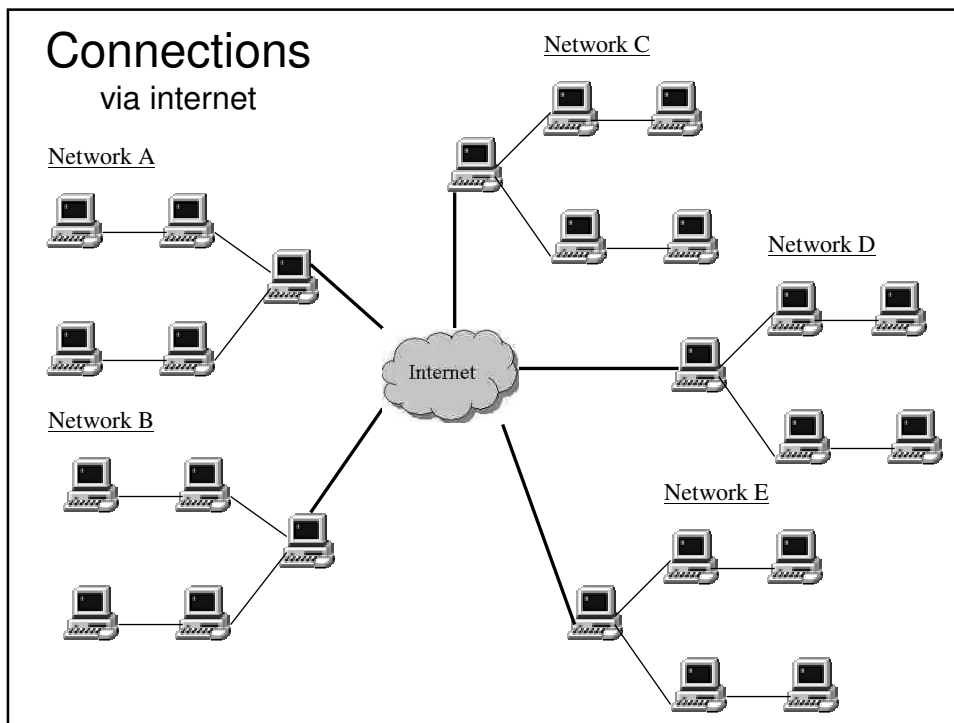
- Provides “virtual circuits”
- Bandwidth shared
 - no waste
 - no ceiling
 - committed information rate
- Less expensive
 - mesh is expensive
- Adding site, no CPE impact
- Security – inherent in line security
- No inherent redundancy

Nontraditional: internet based

- Now ubiquitous
- Business apps use its protocol (IP)
- Bandwidth
 - uncapped
 - unpredictable
 - unreliable
- “Free”
- Security
 - no inherent line security
 - must extrinsically/explicitly supply
- Inherently redundant

Site-to-site VPN via internet

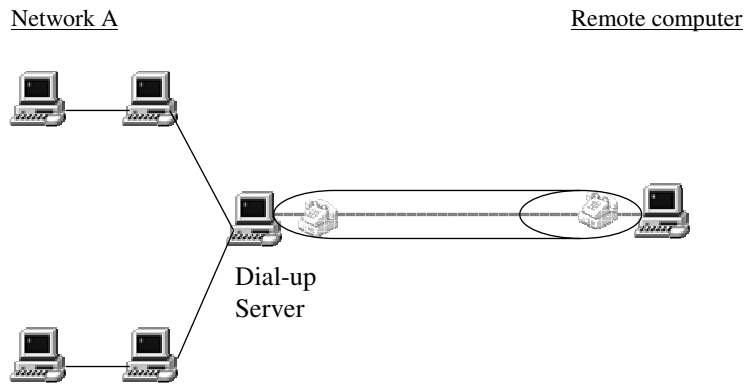




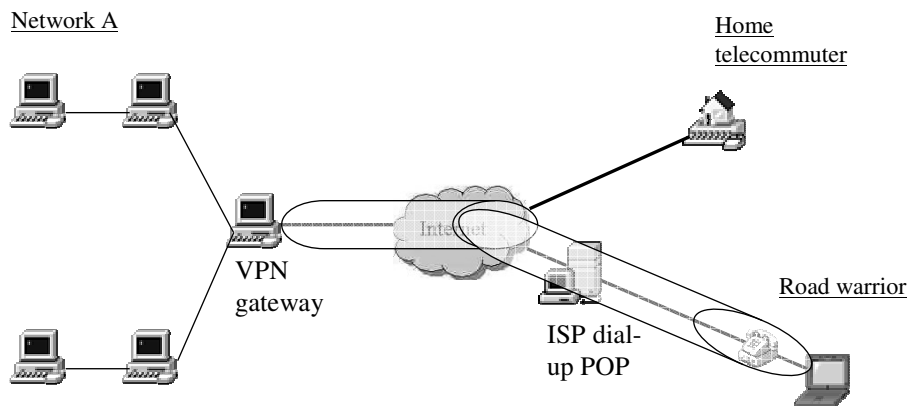
Remote access VPN

- Single-computer to network
- Connection
 - traditionally, using phone
 - recently, using internet

Remote access VPN via traditional connection



Remote access VPN via internet connection



Traditional: phone based

- Cost
 - toll call charge to network site
- Performance
 - at “modem speed” (56Kbps)

Nontraditional: internet based

- Cost
 - any connection to internet (if by phone, local toll)
- Performance
 - at “internet speed”
 - connection-type dependent
 - no chain faster than its slowest link