

System Integration

Mini Case Studies © 2010

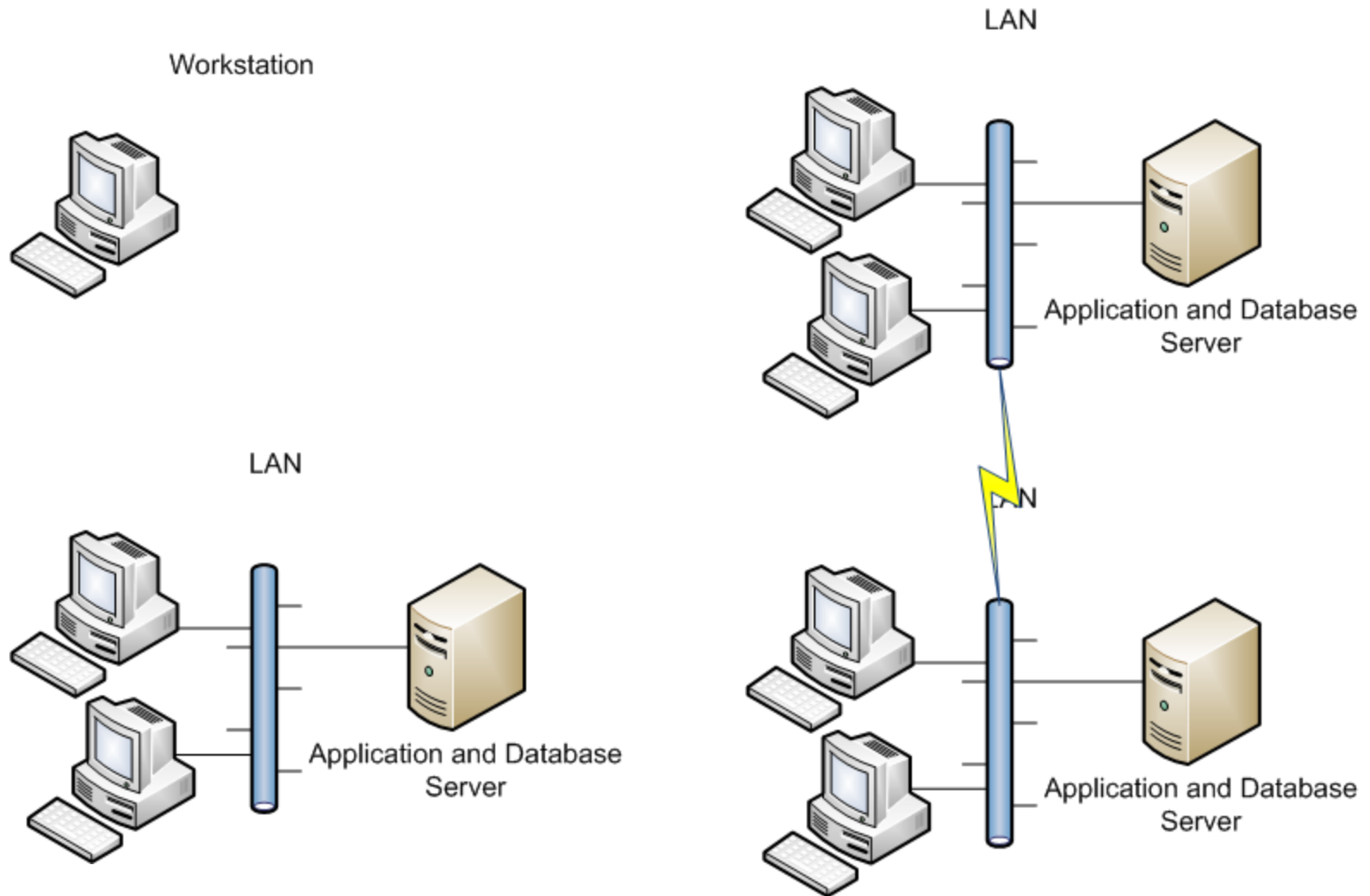
Network Integration

Shawn A. Butler, Ph.D.
Senior Lecturer, Executive Education Program
Institute for Software Research
Carnegie Mellon University

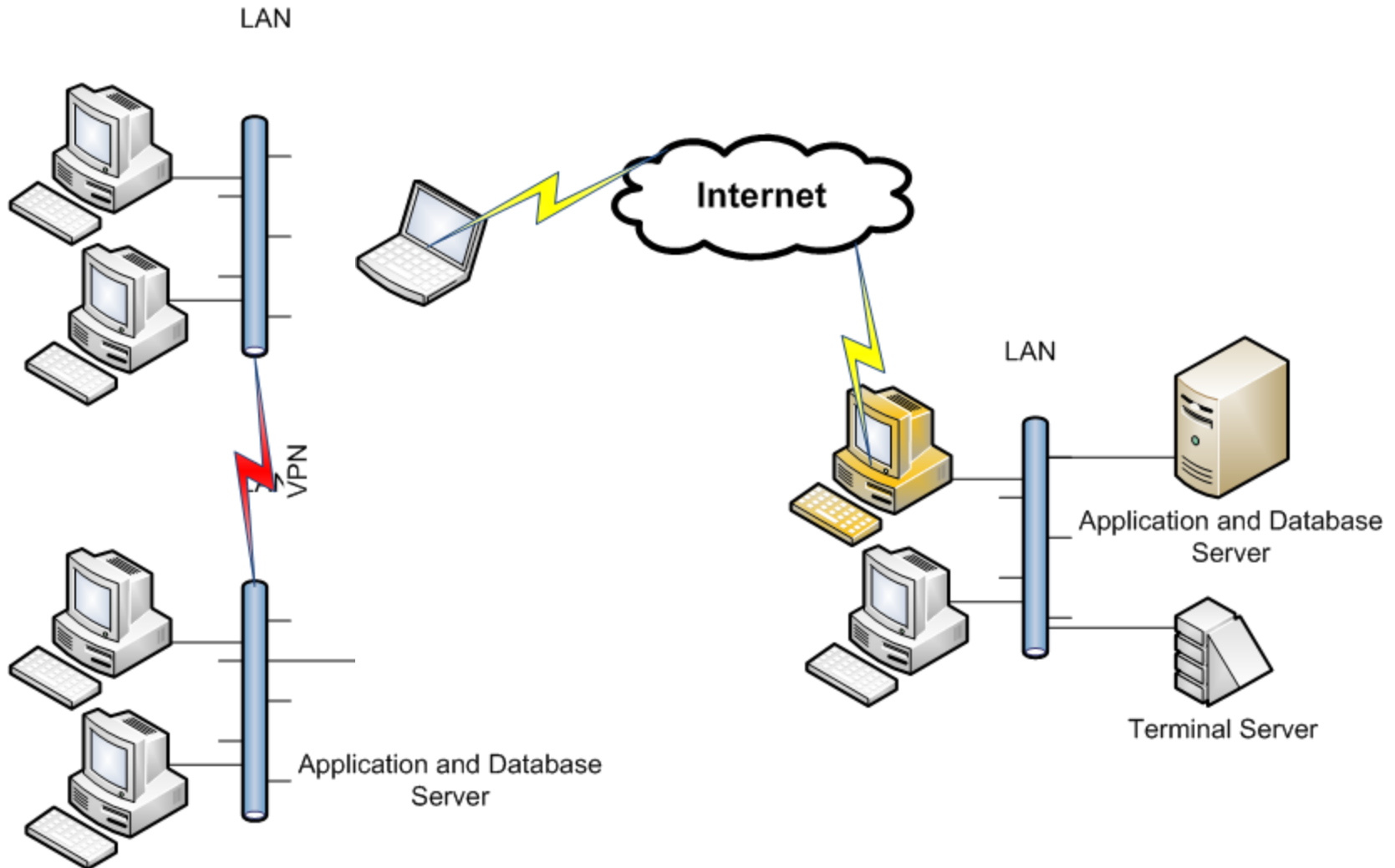
Objectives

- To understand how network infrastructures support integrated systems
- Learn how system services are integrated in networks
- Learn how various services support information management for integrated systems
- Learn about some of the strengths and weaknesses of some network capabilities

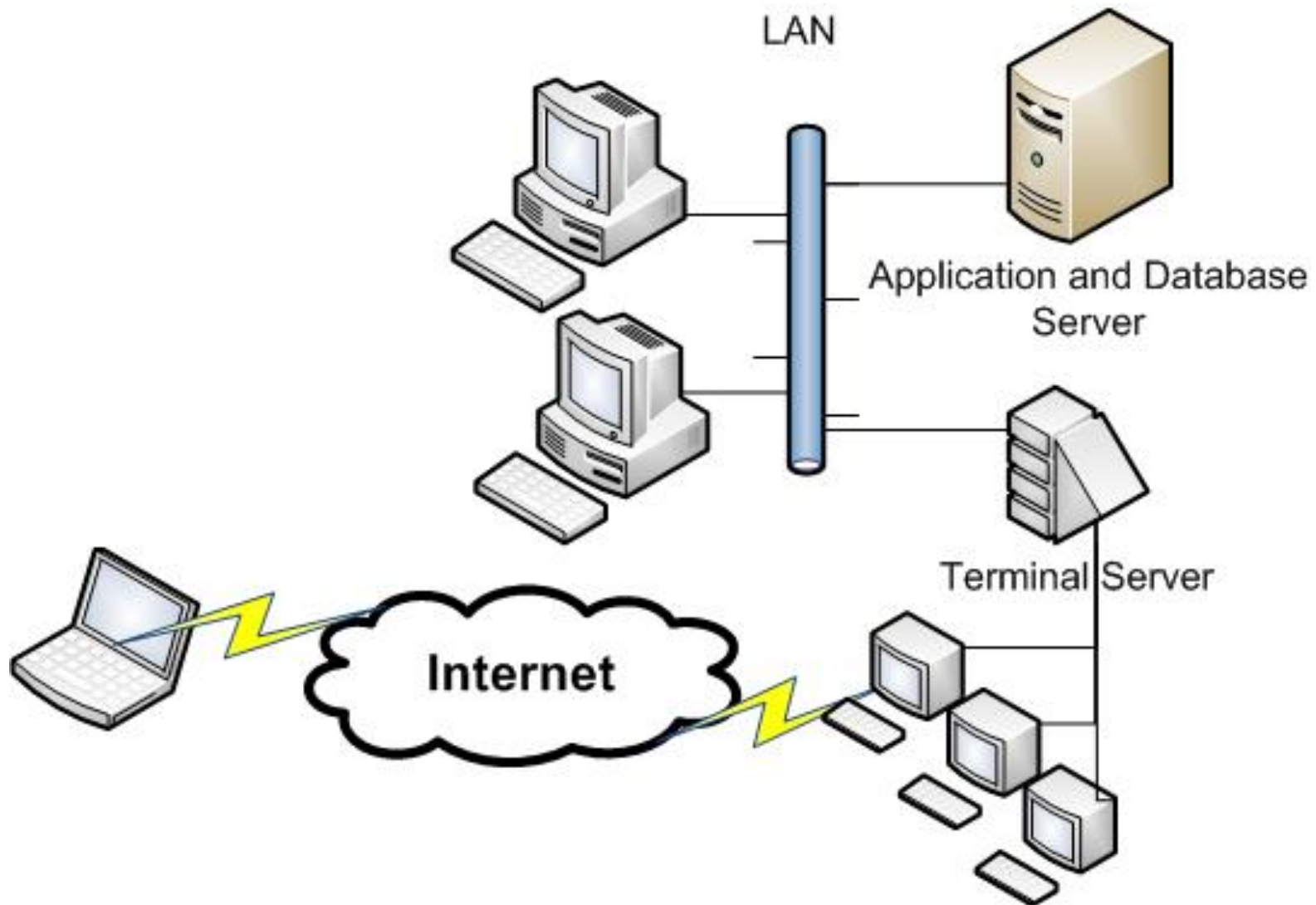
Lots of Models for Accessing Data




VPN's and RDP's




Terminal Services



Single Workstation or LAN

- Single Workstation
 - Inexpensive
 - Only one user
 - Not scalable
- Single Local Area Network
 - More users
 - Simultaneous  access
 - Takes advantage of idle resources
 - Processing can be distributed
 - Client/Server Model works well
 - All users must be physically connected to network
 - Very easy to set up

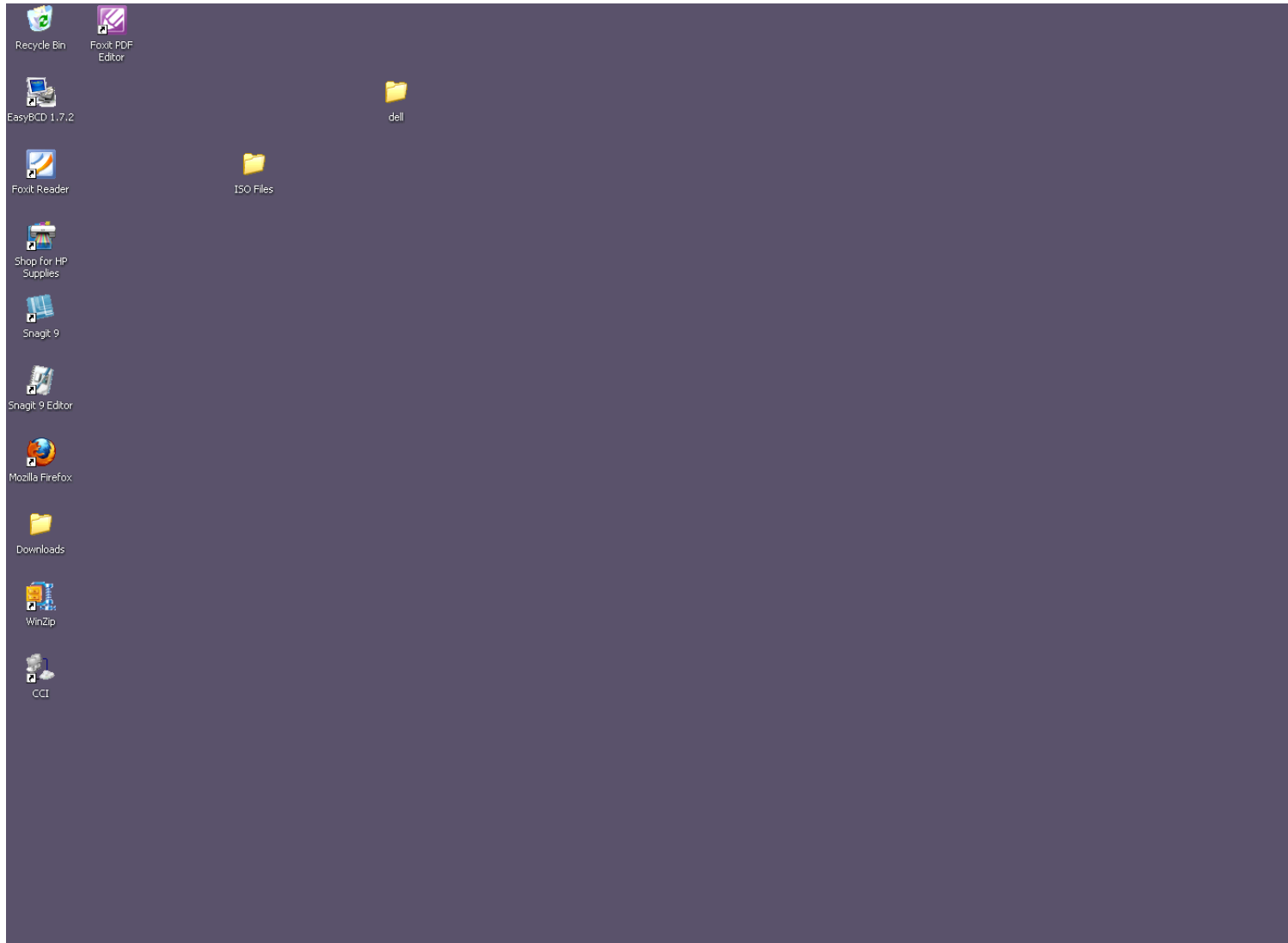
Two LAN's and VPN

- All workstations can access a single server
- All workstations are part of a single network
- Authentication and Access Control simplified
- Security Policy enforcement  through VPN
- All network resources are available, as are local resources
- Communication Costs!!
- Reduced cost of server offset by special hardware or software to establish a VPN
- Client software installed on workstation has easy access to data server and application

Remote Desktop Protocol

- Remote user can see and use application running on internal network computer
 - Client installed on remote workstation
- Standard capability with Windows OS
- No one else can use the computer
- Must anticipate each user on the PC
- Computers can be virtualized
 - A software implementation of a physical machine
- Local resources, such as printers, scanners, and hard drives are available
- Slow user interaction

RDP To My Desktop in Alaska While in Pittsburgh



Terminal Services

- Virtual desktops – software emulating workstations
- Similar to RDP, but on a set of virtual desktops
- Multiple users can access the system simultaneously, depends on licensing
- License costs
- No communication costs
- Clients installed on the virtual desktops
 - Some clients require administrator roles
- Access to local resources slow and limited
- Slow response to user input
- Secure access to system variety of system resources
- Cisco has similar solution called 'Citrix'

System Services

- Naming Services: Provide unique identifiers and location for all network objects
 - Internet Protocol (IP) addresses provide a unique identifier for all network objects
 - Application objects usually need additional unique names, but IP and TCP/UDP ports get closed
- Routers are responsible for directing messages and traffic to the right host
 - Provide other security services
- Domain Name Services translates human remember able addresses into computer addresses
- All networks have internal and external facing IP addresses

IP Addressing

- How do sender and receivers find each other?
 - IP addressing hides the details of physical networks
 - Provides a seamless communication system
 - Integrated systems can span large networks that are really composed of small networks
 - Internet Protocol (IP) provides a uniform addressing scheme that assigns each host a unique protocol address
 - Users, application programs, and higher layers of protocol software use the abstract protocol addresses to communicate
 - Example of IP Address: 192.168.111.34

Routers

- Routing tables enable each router to pass the IP packet forward to the next hop in the route
- Routers send packets to the local area network for the recipient host to receive
- Routers can assign IP addresses dynamically or statically
- Routers can block unwanted packets
- Routers can receive specific types of requests and ensure that those requests are only serviced by designated hosts
- Routers have external and internal facing IP addresses
 - External IP address 209.34.23.45
 - Internal IP address 10.50.20.104, 10.50.20.81


Domain Name Service

- Domain names represent:
 - Computers
 - Services such as File Transfer Protocol (FTP) or Web servers
 - Organizations can assign names to computers or change without informing a central authority
 - DNS uses client-server model to maintain autonomy 📄
 - Model is really a large, distributed database

Name Resolution

- The translation of a domain name into an equivalent IP address is called name resolution
- Software that performs the translation is called name resolver, or simply resolver
- Each resolver is configured with the address of a local domain name server
- The resolver generates a DNS request message
- The DNS server responds with a DNS reply message
- DNS request messages are generated at each level of the DNS hierarchy until the request meets the DNS authority for that domain's IP address

DNS Information


- Each DNS entry contains a quintuplet: 
- {domain name, time-to-live, Class, domain type, ip address}
- The resolver must specify the type that is desired and only entries that match the specified type are returned
- Type A binds a domain name with an IP address
- Aliases allow organizations to change the machine for a service without having to change the domain name

www.cmu.edu → cs.cmu.edu

Principle DNS Resource Record Types for IPv4

Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-bit integer
MX	Mail Exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical Name	Domain Name
PTR	Pointer	Alias for an IP address
HiINFO	Host description	CPU and OS in ACSII
TXT	Text	Uninterpreted ASCII text

Domain Name Servers

- Locality of Reference applies to the domain name system
 - Users tend to look up local names more often than distant names 
 - Users tend to look up the same name repeatedly
 - Therefore, multiple servers are within an organization since they can be placed within groups
- One server cannot be split – One server is responsible for all computers with a given suffix
- Servers use the client-server model to find the other domains
- All domain servers are linked together to form a unified system

DNS and Routing

- Routers connect local area networks (or workstations) to other networks
- Routers enforce security policies governing traffic in and out of the network
- Some routers have DNS capabilities
- Routers assign IP addresses to the local hosts
- DNS servers translate domain names into IP addresses that the router understands
- Both services are essential to connecting remote hosts to the appropriate application servers
- DNS records must be updated to reflect important servers between networks that are in separate domains

Active Directory

- Provides systems with authentication and limited access control functionality
- Stores and enforces security policies on individuals and objects
- Active Directory services can communicate and share authentication and access control services across domains
 - These services must be configured to trust each other!!!

File Servers and Replication

- Access to data or files can be restricted through access controls
- Replication of data or files closer to user servers can improve performance
- Data bases have inherent replication capabilities
- File systems require additional software for replication
- Replication can also support disaster recovery, but network must have the bandwidth to support replication
- Replication can also be used for load balancing within one site

Accessing the System

- On the network
 - Local Area Networks
 - Standing Virtual Private Networks
- Remotely
 - Remote Desktop Protocol (RDP)
 - Terminal Services
 - Virtual Private Networks
 - VNC (very popular)

Putting it All Together - Access

- How many concurrent users will there be?
- How will the client perform using different access mechanisms?
- Will overlapping services need to be reconfigured?
- Will the performance be tolerable?
- Should there be a stable network connection between the user and network?
- How large should the bandwidth be?
- Will DNS and routers need to be configured to find resources and change security policies?

Summary

- There are many tools that allow remote users to access information systems
 - Remote Procedure Protocol (RDP)
 - Virtual Private Networks (VPN)
 - Terminal Services or Citrix
- Each has advantages and disadvantages
- Domain Name Server translates domain names into IP addresses
- Routers direct IP packets to the appropriate next hop
- Routers implement security policies that allow access to resources in and out of the network