What About Computer Networks or Why Network Computers?

From the Cursor November Issue – History

Share resources or peripherals between users / computers

Total network bears the cost of sharing

How many users may share?

Sharing equipment resulted in sharing applications

Application sharing lead to development of “shared” applications

User licensing — *EULA*

Lead to: *Group or seat licensing*

PC Networking: How It All Began or Who Invented Networking?

Xerox – in 1976, at the Palo Alto Research Center (PARC), researcher Bob Metcalfe and his assistant, Dave Boggs, published a paper titled “*Ethernet: Distributed Packet-Switching for Local Computer Networks.*”

Further development was shared by Xerox, Intel, and DEC and remains the most popular PC networking architecture in the world.

Not only did they create the Alto, a computer with a GUI and a mouse, they also developed the hardware and software necessary to connect computers and laser printers together into a LAN.

IBM – IBM brought the IBM PC to the business world as a decentralized computing device in 1981 but all it did was

legitimize the PC as a business tool versus a hobbyist toy.

Word processors became all the rage as a new way to produce documents for marketing. These units were basically hardwired boxes with limited computing power.

Remember these names: NBI; Wang? But by the mid -1980s the IBM system had advanced into the Token-Ring network. This used a star configuration that operates in a logical ring with a MAU or Multistation Access Unit at the center. It looks like a Star but works as a logical circle.

Peer Products Come and Go – The DOS operating system did not provide for P2P so add-on products were required to provide the functionality for sharing files or printers over a small network. Products such as Artisoft's LANtastic and Novell's NetWare Lite and Personal NetWare were available in the late 80's and early 90's.

Other names to remember: *ARCNet; Bay Networks; Banyan Vines; 3Com* and *Cisco*. Even Intel has offered networking products and kits.

Microsoft Windows for Workgroups 1992 – actually ran on top of DOS but offered built-in workgroup networking which meant that printers and files could be shared by users without buying additional software.

Subsequent client versions of Windows 9x, NT, 2000 Professional, ME and XP are all network ready.

Servers

Application Servers

– Scientific and/or Engineering applications

– Adobe's Acrobat Server

– Microsoft's MS Project Server

– Novell Netware Server

– Microsoft's Exchange Server for corporate E-mail

– Domino Server purchased from Lotus by IBM

– Linux/Unix: SendMail; Postfix; Qmail

Print Server **–** Shares a printer to all or specific clcients/ groups/domains

File Server **–** Shares file space or file/folder

Web Server **–** Shares published files to requests from the Internet

Communication Server **–** In the early days... Shares a communication link DCE/DTE between LAN nodes.

Types of Networks

Peer-to-peer: All computers are equal and no specific computer is in control. Each computer is responsible for its own security. Each user must have an account on each computer accessed. In wireless networks, this is known as an *"ad hoc"* configuration.

P2P networks are used primarily for smaller networks which is usually 10 users or less

PROS

- Less Expensive hardware — no servers
- Resources distributed over all the computers

- All computers are equal
- Relative easy (simple) to setup and administer (less than 10 systems)
- Each computer provides its own administration and security
- Network administration is widely distributed to many people

No Network Operating System (NOS) required

- P-2-P networks are built using Windows 95 or newer operating systems
- Or using all Macintosh computers or Unix/Linux based systems
- It's not simple to mix systems and protocols

Built-in Redundancy

- Assume 10 to 20 computers with important data.
- Some system failures leaves most data available on remaining systems
- Fewer single points of failure affect the entire network and users

CONS

- May hurt user's performance (if frequently used data is on system)
- Not very secure (depending on the OS)
- Self administration not secure
- Hard to back up data if left to individual users — no centralized scheme or process

Client/Server Networks

A server controls access to the network and its resources. Cli-

ents gain connection to the network after being authenticated by the server and are then granted access to the network and its resources. In a wired and wireless network this is called an *"infrastructure"* configuration

Used for networks of 10 users or more. Client / Server networks offer the opportunity for centralized administration using equipment suited to managing and controlling the network

PROS

- Very Secure due to centralized administration – usually located in a central secure facility / area
- Managing multiple resources is easier if they're located on one or two servers.
- Physical security is as important as secure access. Peer-to-peer computers (as PCs) are not protected from physical access
- Networking Operating Systems are designed to be secure and have the necessary features to provide strong network security
- While dedicated servers are more expensive that desktop units, they offer better performance because they are optimized for the needs of many simultaneous users.
- Backing up a computer's critical data is much easier when it is located on a centralized server. Depending on the software, complex backups may be run unattended perhaps overnight, when the server is not being used

CONS

- Cost of the server equipment, network OS, and the client licenses

- Cost of a network administrator to setup, control and administer the network.
- If the main server goes down, so does access to the network and the network resources

Which configuration is right for you? Determined by your needs and how much time and money you want to spend

Networks are built using standards. For normal use, ALWAYS use the TCP/IP network protocol. Its the standard and based on the Open System Interconnection model

Layer1 – Physical: Manages the process of sending and receiving bits over the physical network media (wire and other physical devices)

Layer2 – Data Link: Responsible for the framing of data packets and their movement across the physical layer (*MAC Addressing fits here)*

Layer3 – Network: Provides the logical addressing system used to route data on the network.

Layer4 – Transport: Responsible for end-to-end data transmission, flow control, error checking, and recovery.

Layer5 – Session: Establishes and maintains the communication link between the sending and receiving nodes.

Layer6 – Presentation: Serves as the translator layer of the OSI model and is responsible for data conversion and encryption

Layer7 – Application: Provides the interface and services that support user applications and provides general access to the network

How to remember the model?

Please **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way