

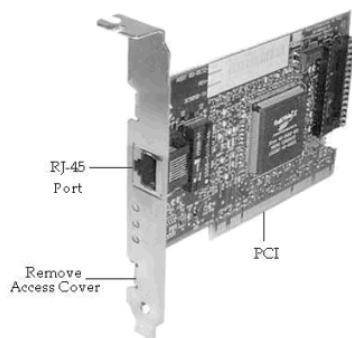
Windows Networking Session (Concepts)

We will start with the absolute basics, and work toward building a functional network. In this article we will begin by discussing some of the various networking components and what they do.

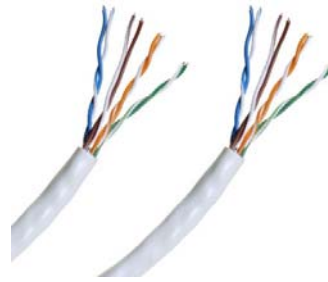
Network Hardware

Network refers to two or more computers connected so that they can communicate with each other and share information, software, peripheral devices, and/or processing power.

Network Adapters referred to by many different names for network adapters, including network cards, Network Interface Cards, NICs. These are all generic terms for the same piece of hardware. A network card's job is to physically attach a computer to a network, so that the computer can participate in network communications.



CAT 5 Cable most networks use twisted pair cabling containing eight wires. These wires are arranged in a special order, and an RJ-45 connector is crimped onto the end of the cable. An RJ-45 cable looks like the connector on the end of a phone cord, but it's bigger.



Hubs generally speaking a hub is nothing more than a box with a bunch of RJ-45 ports. Each computer on a network would be connected to a hub via an Ethernet cable.



A **switch** performs all of the same basic tasks as a hub. The difference is that when a PC on the network needs to communicate with another PC, the switch uses a set of internal logic circuits to establish a dedicated, logical path between the two PCs. What this means is that the two PCs are free to communicate with each other, without having to worry about collisions.



RJ45 is a standard type of connector for network cables. RJ45 connectors are most commonly seen with Ethernet cables and networks.



A **router's** job is to move packets of data from one network to another.



Workstations are computers that use network resources, but that do not host resources of their own. For example, a computer that is running Windows XP would be considered a workstation so long as it is connected to a network and is not sharing files or printers.

Servers are computers that are dedicated to the task of hosting network resources.

A **peer machine** is a computer that acts as both a workstation and a server.

Network Software

Networking Operating System (NOS) is an operating system that contains components and programs that allows a computer on a network to serve requests from other computers for data and provide access to other resources such as printer and file systems.

Windows Networking refers to a collection of interconnected computers using a windows

based operating system as its Network Operating System (NOS).

Workgroups and Domains

Domains, and workgroups, represent different methods for organizing computers in networks. The main difference among them is how the computers and other resources on the networks are managed.

In a workgroup:

- All computers are peers; no computer has control over another computer.
- Each computer has a set of user accounts. To log on to any computer in the workgroup, you must have an account on that computer.
- There are typically no more than twenty computers.
- A workgroup is not protected by a password.
- All computers must be on the same local network or subnet.

In a domain:

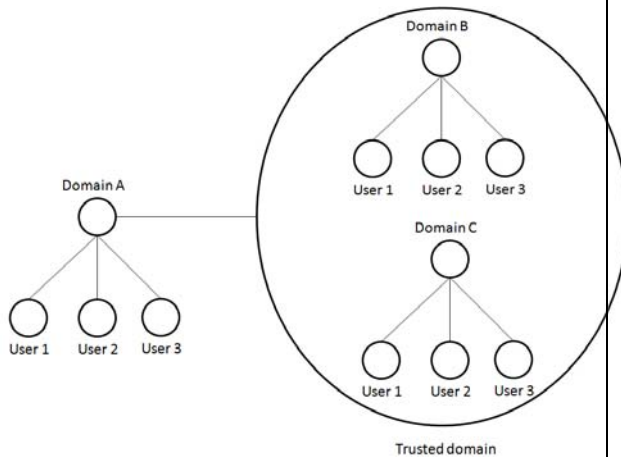
- One or more computers are servers. Network administrators use servers to control the security and permissions for all computers on the domain. This makes it easy to make changes because the changes are automatically made to all computers. Domain users must provide a password or other credentials each time they access the domain.
- If you have a user account on the domain, you can log on to any computer on the domain without needing an account on that computer.
- You probably can make only limited changes to a computer's settings

because network administrators often want to ensure consistency among computers.

- There can be thousands of computers in a domain.
- The computers can be on different local networks.

Windows domain

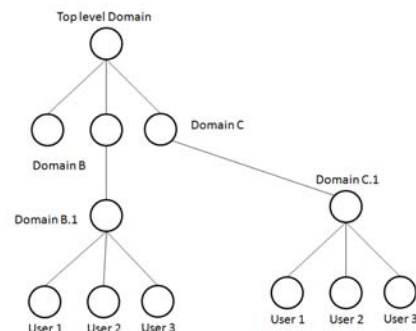
A domain contains a group of computers that can be accessed and administered with a common set of rules. For example, a company may require all local computers to be networked within the same domain so that each computer can be seen from other computers within the domain or located from a central server. Setting up a domain may also block outside traffic from accessing computers within the network, which adds an extra level of security.



Active Directory Service

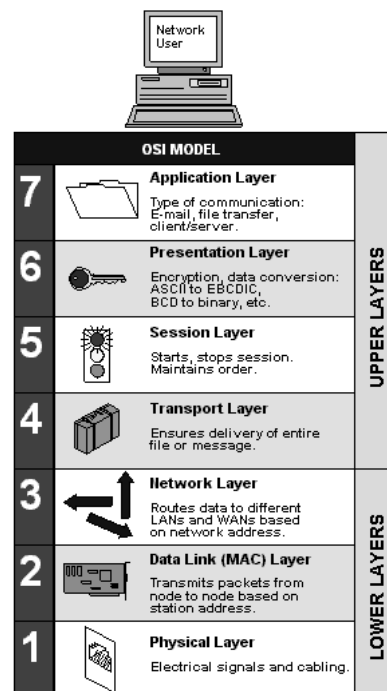
A service unique to Microsoft Windows 200x servers that provide a centrally managed directory for management of user identities, and computer objects, as well as the permissions each user or computer may be

granted to access distributed network resources.



Windows and the OSI Model

OSI Model. A seven layer reference model used to standardize communication networks.



The Application Layer The top layer of the OSI model is the Application layer. The first thing that you need to understand about the application layer is that it does not refer to the actual applications that users run. Instead, it provides the framework that the actual applications run on top of.

To understand what the application layer does, suppose for a moment that a user wanted to use Internet Explorer to open an FTP session and transfer a file. In this particular case, the application layer would define the file transfer protocol. This protocol is not directly accessible to the end user. The end user must still use an application that is designed to interact with the file transfer protocol. In this case, Internet Explorer would be that application.

The Presentation Layer The presentation layer does some rather complex things, but everything that the presentation layer does can be summed up in one sentence. The presentation layer takes the data that is provided by the application layer, and converts it into a standard format that the other layers can understand. Likewise, this layer converts the inbound data that is received from the session layer into something that the application layer can understand. The reason why this layer is necessary is because applications handle data differently from one another. In order for network communications to function properly, the data needs to be structured in a standard way.

The Session Layer Once the data has been put into the correct format, the sending host must establish a session with the receiving host. This is where the session layer comes into play. It is responsible for establishing, maintaining, and eventually terminating the session with the remote host.

The interesting thing about the session layer is that it is more closely related to the application layer than it is to the physical layer. It is easy to think of connecting a network session as being a hardware function, but in actuality, sessions are usually established between applications. If a

user is running multiple applications, several of those applications may have established sessions with remote resources at any time.

The Transport Layer The Transport layer is responsible for maintaining flow control. As you are no doubt aware, the Windows operating system allows users to run multiple applications simultaneously. It is therefore possible that multiple applications, and the operating system itself, may need to communicate over the network simultaneously. The Transport Layer takes the data from each application, and integrates it all into a single stream. This layer is also responsible for providing error checking and performing data recovery when necessary. In essence, the Transport Layer is responsible for ensuring that all of the data makes it from the sending host to the receiving host.

The Network Layer The Network Layer is responsible for determining how the data will reach the recipient. This layer handles things like addressing, routing, and logical protocols. Since this series is geared toward beginners, I do not want to get too technical, but I will tell you that the Network Layer creates logical paths, known as virtual circuits, between the source and destination hosts. This circuit provides the individual packets with a way to reach their destination. The Network Layer is also responsible for its own error handling, and for packet sequencing and congestion control.

Packet sequencing is necessary because each protocol limits the maximum size of a packet. The amount of data that must be transmitted often exceeds the maximum packet size. Therefore, the data is fragmented into multiple packets. When this happens, the Network Layer assigns each packet a sequence number.

When the data is received by the remote host, that device's Network layer examines the sequence numbers of the inbound packets, and uses the sequence number to reassemble the data and to figure out if any packets are missing.

If you are having trouble understanding this concept, then imagine that you need to mail a large document to a friend, but do not have a big enough envelope. You could put a few pages into several small envelopes, and then label the envelopes so that your friend knows what order the pages go in. This is exactly the same thing that the Network Layer does.

The Data Link Layer The data link layer can be sub divided into two other layers; the Media Access Control (MAC) layer, and the Logical Link Control (LLC) layer. The MAC layer basically establishes the computer's identity on the network, via its MAC address. A MAC address is the address that is assigned to a network adapter at the hardware level. This is the address that is ultimately used when sending and receiving packets. The LLC layer controls frame synchronization and provides a degree of error checking.

The Physical Layer The physical layer of the OSI model refers to the actual hardware specifications. The Physical Layer defines characteristics such as timing and voltage. The physical layer defines the hardware specifications used by network adapters and by the network cables (assuming that the connection is not wireless). To put it simply, the physical layer defines what it means to transmit and to receive data.

Sharing Resources

Share level security applies directly to the share point that you have created. When the users connect to the SharePoint to access the files, the share level permissions that you have set are applied.

In contrast, file level permissions are applied directly to files and folders rather than to the share.