**Performance Monitoring and Analysis**

**Introduction**

Monitoring performance is a necessary part of preventive maintenance for a computer network system. Through monitoring, you obtain performance data that is useful in diagnosing system problems and in planning for the growth in demand for system resources. The data you collect about system performance provides important indicators as to the efficiency of the system. However, data can sometimes be misleading and needs to be analyzed carefully if you are to have an accurate picture of the health of your system and to correctly diagnose problems.

A systematic approach to testing is necessary based on some knowledge of the effects of system components and subsystems on performance. For a typical server system analysis a base line report is created for comparison purposes and then selected data is captured on a regular basis and stored in a database so that trends in performance can be analyzed to detect problems or need for upgrades.

**Performance Monitoring Concepts**

Regular performance monitoring ensures that you always have up-to-date information about how your system is operating. When you have performance data for your system over a range of activities and loads, you can define the **baseline** — a range of measurements that represent acceptable performance under typical operating conditions. This baseline provides a reference point that makes it easier to spot problems when they occur. In addition, when you are troubleshooting system problems, performance data gives you information about the behavior of system resources at the time the problem occurs, which is useful in pinpointing the cause. Finally, monitoring system performance provides you with data to project future growth and to plan for how changes in your system configurations might affect future operation. Figure 1 shows the different system resources to monitor.

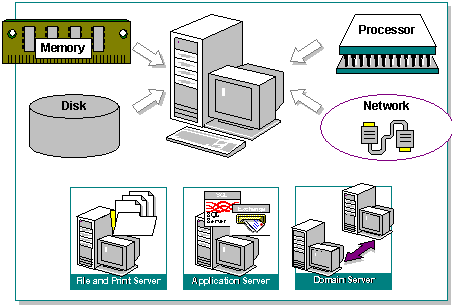


Figure 1 System Resources to monitor

**System Resource Implications**

The choice of components may have a great effect on overall system performance depending on what the systems main function is. For example memory and processor have the greatest impact on file and print servers and careful matching of computer components with motherboard is very important.

**Memory**

Random Access Memory (RAM) and cache memory can have a great effect on performance. In general, the more of each the better.

The legacy main memory technology for PCs is SDRAM (Synchronous Dynamic RAM). This is rated in MHz rather than the access time in ns to make it easier to correlate with system bus speed. E.g. 100MHz SDRAM (PC100) has an access time of 1/100M = 10ns and PC133 has a 7ns access time.

The current main memory is Double Data Rate (DDR) which pumps 2x data by clocking on both edges of the system clock and DDR2 gives 4x the speed and lower power consumption. DDR3 gives 8x the speed and lower power consumption. Care should be taken when using SDRAM since mixing different speed DIMMs may require BIOS changes to make it work and then at the speed of the slowest chips. Also, when using multiple DDR DIMMS each channel should have the same capacity for the fastest (interleaved) mode of operation.

The size and location of the paging file is important too - it is generally recommended to move the paging file from the system partition to another position for performance improvement and spread it across separate hard drives if possible.

**Processor**

The type of system processor, as well as the number of processors, affects the overall performance of the system. For example, an Intel i7 6th Generation processors will provide better performance than an Intel i7 5th Generation processors. Intel i7s have Hyper-Threading capability giving effectively two virtual processors to improve performance when executing two separate tasks in parallel e.g. performing an office app while transferring files. Multiple processors are often used on servers so that if a system has multiple applications running concurrently, or applications that are multithreaded, the overall processor power is shared. The recently introduced dual and quad core processors give even better performance and don’t require multiple socket motherboards

**Disc Subsystem**

Several factors affect disk subsystem performance not just the speed of the drive. Disk performance is generally measured in disk access time (ms) and transfer speed (bytes/s). Choosing the fastest drive available is a good idea but implementing drives that complement the rest of the architecture, such as the controller is just as important. Until recently parallel ATA drives have been used for desktop PCs and the faster more reliable SCSI drives for servers. Now Serial ATA (SATA) is being used for desktop and low end servers and SAS (Serial Attached SCSI) for servers to give better performance and easier connectivity. Fibre channel is another option for SANs.

*Controller* type and the number of controllers affect the overall system responsiveness when responding to information requests being read from or written to disk drives. Installing multiple disk controllers can result in higher throughput. Typical controller throughput ranges from 2.5MB per second for IDE controllers for ATA to 100 MB per second for Fast/wide SCSI controllers and now 320MBps for the latest Ultra 320 SCSI devices.

*Q. What are the latest SAS and solid state HDDs capable of? Find out.*

*Busmaster disc* controllers have an on-board processor that handles all interrupts until data is ready to be passed to the CPU for processing. This helps the processor to avoid interruptions for data. *Caching* also helps improve disk responsiveness as data is cached on the controller and does not require RAM or internal cache*.*

*RAID* (Redundant Array of Inexpensive Disks) controllers can improve performance by implementing striping where data can be transferred simultaneously to several physical disks.

*N.B. matching a Fast/Wide SCSI HDD( 100MBps) to a Fast Controller(10MBps) will limit the transfer rate to that of the controller.*

Network Subsystem

Overall network performance and capacity may be affected by a number of factors not just by the maximum data transmission rate of the network segment.

*Network Adapters* - High bandwidth cards (such as 32-bit bus mastering types) provide better performance than old 8 or 16 bit programmed input/output (PIO) adapters. E.g. a 10BaseT 8-bit network adapter can transfer up to 400 Kbps whereas 10BaseT 32-bit adapters transfer up to 1.2 Mbps. The latest Gigabit Ethernet (1000BaseT) cards also support 10 and 100Mbps operation via auto-speed sensing functions. They may have other features to improve system performance such as teaming, FDX operation and off-loading the CPU of some TCP/IP functions such as error checking and encryption or use jumbo size frames to increase throughput.

Multiple network adapters are also beneficial in a server environment because they allow the server to process network requests over the multiple adapters simultaneously.

***N.B.*** *Care should be taken with auto-sensing as it often causes problems in mixed speed environments. Also older computers may not be able to handle Gigabit speeds due to IO and system bus limitations of the motherboard.*

***Routers, Bridges and Switches***- can affect performance of the network, by introducing latency as can other data communications facilities such as WAN interface devices, VPN devices and Firewalls. Care should be taken when buying budget devices as they may not be able to handle the throughput e.g. check that the switching bandwidth of a switch is adequate for the number of switch ports.

***Protocols***tend vary in performance, so consider the amount of traffic generated to perform a given function. Reducing the number of protocols installed can increase performance as can the binding order of the client. Setting the TCP MTU (Maximum Transfer Unit) to the optimum size can have marked effects on throughput.

***Network Services***such as RAS, DHCP, DNS, WINS and *Network Applications* such as Internet Services, Messaging and Directory Services all add memory and processor overhead on the system.

***Domain Controllers***  Multiple DCs may speed up log ins but more account synchronization traffic is generated and this can be a major problem when using limited bandwidth WAN links since account synchronization can consume a lot of it.

**Performance Data**

In general, performance monitoring concentrates on how the operating system and any applications/services use the resources of the system, such as the disks, memory, processors, and network components.

*Throughput*, *queue*, and *response time* are terms that describe resource usage.

**Throughput**

Throughput is a measure of the work done in a unit of time, typically evaluated from the server side in a client/server environment. Throughput tends to increase as the load increases up to a peak level. It then begins to fall, and a queue might develop. Throughput in an end-to-end system, such as client/server, depends on how each component performs. The slowest point in the system sets the throughput rate for the system as a whole. Often this slow point is referred to as a bottleneck. Performance monitoring tells you where bottlenecks occur in your system. The resource that shows the highest use is often the bottleneck, but not always — it can also mean a resource is successfully handling a lot of activity. As long as no queues develop, there is no bottleneck. Microsoft Windows Operating systems report throughput data on resources such as disks and network components e.g. PhysicalDisc\Bytes/sec

**Queue**

A queue can form under a few different circumstances. For example, a queue can develop when requests come in for service by the resource at a faster rate than the resource's throughput, or if requests demand differing, particularly longer, amounts of time from the resource. A queue can also form if requests occur at random intervals in large batches for a time and then none at all. When a queue becomes long, work is not being handled efficiently, and you might experience delays in response time. Windows reports queue development on disks and processors.

**Response Time**

Response time is the measure of time required to do work from start to finish. In a client/server environment, you typically measure response time on the client side. Response time generally increases as the load increases. You can measure response time by dividing the queue length by the resource throughput. As an alternative, the trace log feature in the Windows performance tools allows you to track units of work from start to finish in order to determine response times.

**Data Collection and Reporting**

Depending on the tools used, you can configure data collection to occur almost immediately or according to a predefined schedule. Performance data reported is sampled, meaning that data is collected periodically rather than traced, whereby data is obtained as events occur. This collection method has the advantage of keeping overhead low, but it might occasionally overestimate or underestimate values when activity falls outside the sampling interval.

Event tracing can measure activity as it happens, eliminating the inaccuracies of sampling and making it possible to correlate resource usage such as page faults, disk input/output (I/O), and processor time with workload that can include threads, processes, or transactions. This capability supplements counter-based monitoring methods. You can configure trace logs in Windows Performance Logs and Alerts but running trace logs of page faults and file I/O data incurs some performance overhead so only log data for brief periods .

*N.B. an additional program is required to parse the log output into readable form.*

**Establishing the Baseline and Trend analysis**

Routine monitoring over periods ranging from days to weeks to months allows you to establish a baseline for system performance.

A baseline is a measurement that is derived from the collection of data over an extended period during varying but typical types of workloads and user connections. The baseline is an indicator of how individual system resources or a group of resources are used during periods of normal activity.

When determining your baseline, it is important to know the types of work being done and the days and times when the work is being done. That will help you to associate work with resource usage and to determine the reasonableness of performance during those intervals.

For example, if you find that performance diminishes somewhat for a brief period at a given time of day, and you find that at that time many users are logging on or off, it might be an acceptable slowdown. Similarly, if you find that performance is poor every evening at a certain time and you can tell that time coincides with nightly backups when no users are logged on to the system; again that performance loss might be acceptable. But you can make that determination only when you know the degree of performance loss and its cause.

When you have built up data on performance over a period, with data reflecting periods of low, average, and peak usage, you can make a subjective determination of what constitutes acceptable performance for your system. That determination is your baseline. Use your baseline to detect trends when bottlenecks are developing or to watch for long-term changes in usage patterns that require you to increase capacity.

Trend analysis is the term used to describe the analysis of long term data to reveal problems which occur over time due to increased network use etc. and the need for upgrades to maintain performance.

Some Windows performance counters used for a baseline test of the workload of a typical network system are shown in Table 1.

|  |  |  |
| --- | --- | --- |
| **Resource** | **Object\Counter** | **Comments** |
| Disk | PhysicalDisk\% DiskTime | Amount of disc activity |
| Disc | PhysicalDisk\Bytes/s | Data Throughput |
| Disc | Physical Disk\Avg Disc Queue Length | Read and write requests queued |
| Memory | Memory\ Available Bytes | Memory usage |
| Memory | Memory\ Pages/sec | Rate of paging from disc |
| Network | Network Segment\% Net Utilization | Network bandwidth in use |
| Network | NetworkSegment\Bytes Total/s | Data Throughput |
| Processor | Processor\% Processor Time | Processor activity |
| Processor | Processor\ Interrupts/sec | Average rate of interrupts |
| Paging | PagingFile\%Usage | Amount of page file in use |

Table 1 Some Performance counters

**Analysis of Monitoring Results**

The baseline you develop establishes the typical counter values you should expect to see when your system is performing satisfactorily.

When you are collecting and evaluating data to establish a valid performance baseline, consider the following guidelines:

Do not give too much weight to occasional spikes in data. These might be due to the start-up of a process and are not an accurate reflection of counter values for that process over time. The effect of spikes can linger over time when using counters that average.

For monitoring over an extended period of time, use graphs (chart view, see Figure 2.) instead of reports or histograms because these views only show last values and averages. As a result, they might not give an accurate picture of values if you are looking for spikes.

Unless you specifically want to include start-up events in your baseline, exclude these events because the temporary high values tend to skew overall performance results.

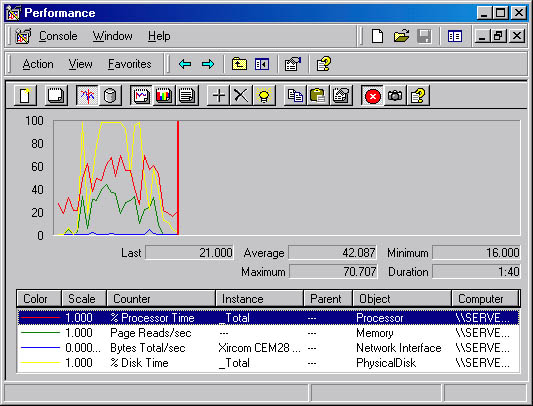


Figure 2 System monitor Graph view

**Bottlenecks**

A bottleneck exists if a particular component's limitation is keeping the entire system from performing more quickly. Therefore, even if one component in your system is heavily used, if other components or the system as a whole show no adverse effects, then there is no bottleneck.

Investigating performance problems should always start with monitoring the whole system before looking at individual components.

Factors involved in the development of a bottleneck are the number of requests for service, the frequency with which requests occur, and the duration of each request. As long as these are perfectly synchronized, no queue will develop and no bottleneck will arise. The device with the smallest throughput ratio is probably the primary source of the bottleneck.

Poor response time on a workstation is most likely to result from memory and processor problems. Servers are more susceptible to disk and network problems.

Also, problems in one component might be the result of problems in another component, not the cause. For example, when memory is scarce, the system begins moving pages of code and data between disks and physical memory. The memory shortage becomes evident from increased disk and processor use, but the problem is memory, not the processor or disk.

**Potential Bottlenecks and Thresholds**

Deviations from the baseline provide the best indicator of performance problems. However, as a secondary reference, monitor thresholds for some common object counters. Table 2 identify when a performance problem is developing on a system. If the values listed are consistently reported then there may be a problem.

|  |  |  |  |
| --- | --- | --- | --- |
| **Resource** | **Object\Counter** | **Suggested Threshold** | **Comments** |
| Disk | LogicalDisk\ % Free Space | 15 percent | None |
| Disk | LogicalDisk\ % Disk Time | 90 percent | None |
| Memory | Memory\ Available Bytes | < 4 MB | Research memory usage and add memory if needed. |
| Memory | Memory\ Pages/ sec | 20 | Research paging activity. |
| Network | Network Segment\% Net Utilization | Depends on type of network | Depends on type of network - e.g. for Ethernet 30 percent is the recommended threshold. |
| Paging File | Paging File\% Usage | >70 percent | Review this value in conjunction with Available Bytes and Pages/sec to understand paging activity on your computer. |
| Processor | Processor\% Processor Time | 85 percent | Find the process that is using a high percentage of processor time. Upgrade to a faster processor or install an additional processor. |
| Processor | Processor\ Interrupts/sec | Current CPUs, use a threshold of 1500 | A dramatic increase in this counter value without a corresponding increase in system activity indicates a hardware problem. Identify the network adapter or disk controller card causing the problem. |
| Server | Server\Bytes Total/sec |  | If the sum of Bytes Total/sec for all servers is roughly equal to the maximum transfer rates of your network, you might need to segment the network. |
| Server | Server Work Queues\Queue Length | 4 | If the value reaches this threshold, there might be a processor bottleneck. This is an instantaneous counter; observe its value over several intervals. |
| Multiple Processors | System\Processor Queue Length | 2 | This is an instantaneous counter; observe its value over several intervals. |

Table 2 Some counter threshold values for Windows systems

**Further Investigations**

If you identify a resource that is out of range for your baseline or based on the recommended thresholds, you need to investigate the activity of that resource in greater detail. This includes the following steps:

1. Analyze your hardware and software configurations.
2. Review entries in the event log for the time period when you begin seeing out-of-range counter values.
3. Examine the kinds of applications you are running and what resources they demand.
4. Consider variables in your workload, such as processing different jobs at different times.
5. For immediate diagnosis and problem solving of situations such as shutdowns and logon failures, log or monitor for a shorter time. Sampling should be frequent when monitoring over a short period. Similarly, for long-term planning and trend analysis, log for a longer period and set the update interval accordingly.
6. Consider network or disk utilization or other activities occurring at the times that you see increasing resource utilization. Try to understand the usage patterns. Are they associated with specific protocols or computers?
7. Approach bottleneck correction in a scientific manner. For example, never make more than one change at a time, always repeat monitoring after a change to validate the results, eliminate results that are suspect, and keep good records of what you have done and what you have learned.
8. When investigating bottlenecks in specific resources, focus on the performance objects and counters that pertain to the specific resource that appears to be your bottleneck.

**Network Traffic Simulation, Emulation and Benchmarks**

Testing a live client server system is not easy. The usual procedure is to simulate typical traffic before the system goes live. Benchmark programmes from companies such as Veritest allow performance comparisons to be made.

Veritest's NetBench is a benchmark programme used to assess performance of a file server by loading the server with typical application traffic from one or more clients, see Figure 3 for typical results comparing file servers of differing specs.

Profile tools are used to capture network file behaviour and then a script is created to mimic that behaviour.

Scripts are employed which stress the server in various ways to see how it performs under load, a difficult task under real live conditions. Standard scripts are available or you can develop custom scripts to emulate the way your particular system operates.

WebBench does the same job for web server testing.

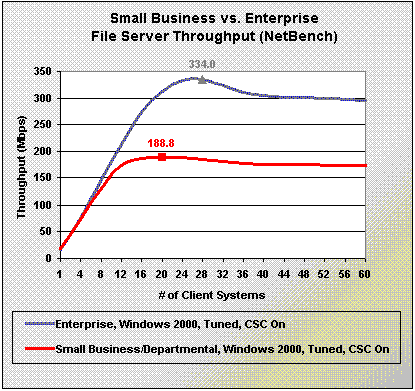


Figure 3 NetBench results

The following shows the results for a Veritest study for Intel of the effects of Hyper-Threading and Intel Gigabit cards. Figure 4 provides the detailed results of the server resources test while using Web Bench. The blue bars represent the average number of active connections per second over the course of the test (smaller is better) and the dark red bars represent the average number of connections per second the web server delivered to the test clients (larger is better).

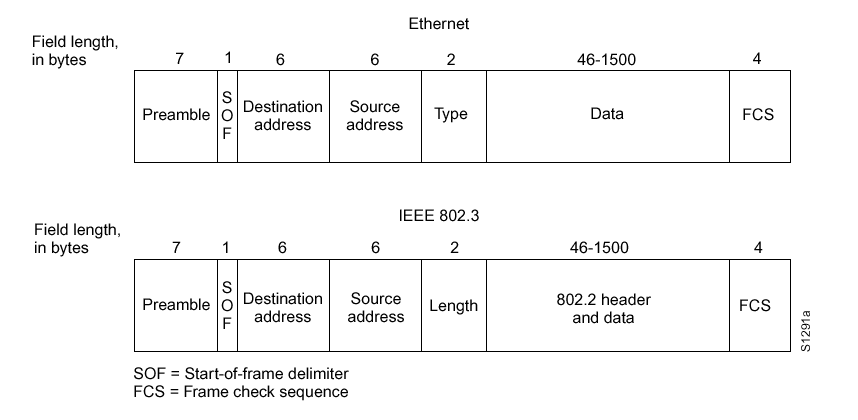


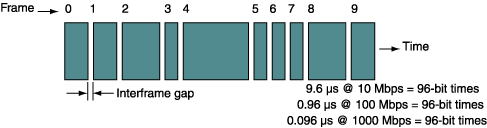
Figure 4

Emulation utilities such as NIST Net provide the ability to emulate common network effects such as packet loss, duplication or delay; router congestion; and bandwidth limitations. They are designed to offer sufficient capabilities and performance to reproduce a wide range of network behaviours requiring only basic PC hardware and operating systems. This provides an intermediate solution between real world testing and simulation, giving you the ability to emulate real world 'badness' on a laboratory network or a means for simulations to interact with a live environment.

**Exercises: Ethernet Performance Questions and Investigations**

**1. Complete the following details for each Ethernet PHY and answer the associated questions**

****

****

10BaseT

Raw bandwidth (transmission speed) = 10M/8 = 1.25MBps

minimum frame size = 64 Bytes (6+6+2+46+4)

maximum frame size = 1518 Bytes (6+6+2+1500+4)

interframe gap = 9.6µs (equiv to 12 byte times @10Mbps)

preamble = 8 bytes (7+1)

total bytes per min frame = 64+12+8 = 84 bytes

maximum frame rate = 1.25M/84 = 14880 frames/sec

minimum frame rate = 1.25M/? = ? frames/sec

100BaseTx

Raw bandwidth (transmission speed) = ………..Bps

minimum frame size = ………...Bytes

maximum frame size =…………Bytes

interframe gap =……….µs (equiv to 12 byte times @100Mbps)

preamble =………bytes

total bytes per min frame = ……….bytes

maximum frame rate = frames/sec

Min frame rate =………… frames/sec

1000BaseT

Raw bandwidth (transmission speed) = ………..Bps

minimum frame size = ………...Bytes - be careful

maximum frame size = ………..Bytes

interframe gap =……….µs

preamble =………bytes

total bytes per min frame = ……….bytes

maximum frame rate = frames/sec

Min frame rate =………… frames/sec

Questions

* Determine the bandwidth efficiency (%utilization) and frame transfer rate for standard (shared) Ethernet for min and max frame sizes.
* What is the most efficient frame size?
* What is the inter-frame gap for?
* Why is it best to keep average utilization down below about 40%?
* Why does a switch usually improve performance?

**2. Host computer memory was often the limiting factor on network performance in older PCs NOT the network adaptor. Many older PCs can't use the full potential of a Gigabit network card.**



The advertised performance spec of the memory subsystem may not be all it's claimed to be - a few calculations can reveal the effective throughput.......

NIC has potential to transfer at Gigabit speed (1000Mbps)

I/O has potential to transfer at Gigabit speed (1056Mbps)

So why is the effective bandwidth only 704 Mbps for 64byte frame transfers?

The memory/CPU interface seems to have enough BW to cope with Gigabit transfers (235x8=1880bps) but in reality this can also be a bottleneck since the OS, device drivers and applications may not utilize it efficiently.

The PC may use several clock cycles to gain access to the PCI bus before data transfer can begin.

e.g. if 8 clock cycles are needed then the total to transfer a 64byte frame is 16+8 =24 cycles. The effective throughput is then only 16/24 x 1056 Mbps = 704 Mbps.

**3. 'Gigabit Ethernet and HyperThreading Technology in the Desktop for Improved Office Productivity' A Report by Veritest on the effectiveness of combing the two technologies showing a marked increase in productivity and a 5x performance increase over a Fast Ethernet/PIII baseline system.**

**4. Look at Intel Dual Core processors and find out why it is such an improvement over earlier Pentium processor technology.**

**5. How do the Dell lab PCs compare?**

**6. SMB (CIFS) and FTP file transfer efficiency can impair an Ethernet LAN’s ability to carry data.**

Read the following and determine which is the best for large file transfer over a LAN.

**The Server Message Block (SMB)** protocol is a network file sharing protocol, and as implemented in Microsoft Windows is known as Microsoft SMB Protocol. The set of message packets that defines a particular version of the protocol is called a dialect. **The Common Internet File System (CIFS)** Protocol is a dialect of SMB. Both SMB and CIFS are also available on several versions of Unix, and other operating systems.

The Microsoft SMB Protocol is a client-server implementation and consists of a set of data packets, each containing a request sent by the client or a response sent by the server. These packets can be broadly classified as follows:

* Session control packets—Establishes and discontinues a connection to shared server resources.
* File access packets—Accesses and manipulates files and directories on the remote server.
* General message packets—Sends data to print queues, mailslots, and named pipes, and provides data about the status of print queues.

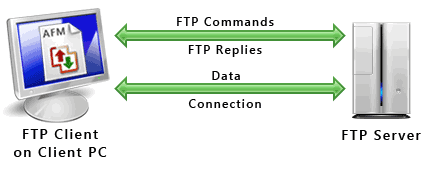
The following steps are an overview of the process of reading a file over a network:

1. The client and server establish a NetBIOS session.
2. The client and server negotiate the Microsoft SMB Protocol dialect.
3. The client logs on to the server.
4. The client connects to a share on the server.
5. The client opens a file on the share.
6. The client reads from the file.

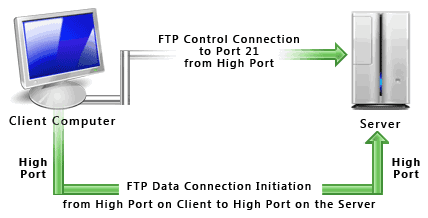
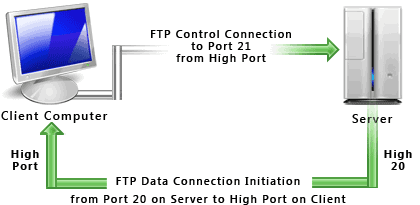
First, a full-duplex TCP connection is established by the client with the server. Then the client builds and sends a NetBIOS session request packet over the TCP connection. If the packet was formatted correctly, the server then returns a packet that contains a message acknowledging that the session has been established. After this, the client sends the first of many Microsoft SMB Protocol packets to the server.

SMB/CIFS is very convenient, as it is fully integrated into Windows, but is not the lightest or fastest method of transferring data. You can use FTP or many other methods to transfer data quickly, but most of them are not nearly as convenient as SMB. SMB 2 which Microsoft introduced in Vista and Windows Server 2008 is much better. There are several enhancements in SMB 2.0, including sending multiple SMB commands in the same packet which reduces the number of packets sent between a client and server and larger buffer sizes

**The FTP (File Transfer Protocol)** can transfer files between any computers that have an Internet connection, and also works between computers using totally different operating systems. Transferring files from a client computer to a server computer is called uploading and transferring from a server to a client is downloading**.**



FTP uses one connection for commands and the other for sending and receiving data. FTP server "listens" for connections on TCP port 21 and is used only for sending commands and is called the **command port.** The port that is used for transferring data is referred to as a **data port.** The number of the data port will vary depending on the "mode" of the connection, Active or Passive. Most FTP servers support the Passive mode.



**Active Passive**

When a user wishes to transfer a file, FTP sets up a TCP connection to the target system for the exchange of control messages. These allow used ID and password to be transmitted and allow the user to specify the file and file action desired. Once file transfer is approved, a second TCP connection is set up for data transfer. The file is then transferred over the data connection, without the overhead of headers, or control information at the application level. When the transfer is complete, the control connection is used to signal the completion and to accept new file transfer commands.

