LAB MANNUAL

SYSTEM & NETWORK ADMINISTRATION

System and Network Administration Lab.

IT 407-E

L	T	P		
-	-	3		Class Work: 50
				Exam:50
				Total: 100
				Duration of exam:3 hrs.

- Management of the users & the domain.
- Configuring DHCP.
- Setting up the local security policy.
- Start and stop services from user window and command prompt.
- Use of event viewer.
- Use of the performance monitor.
- Management of the IIS and FJP server.
- Setting up of local area network.
- Setting up of router in Window 2000 server.
- Use of utilities (a) Ping (b) Trocert (c) netstat (d) net (e) IP configuration (f) Path ping
  - Use of network monitor.
  - Setting up of a DNS.
  - Setting up and use "Terminal Client Services".

RATIONALE BEHIND S&NA LAB

A network consists of the infrastructure components through which computer systems and shared peripherals communicates with each other. System and Network Administration is the basic level of an IT infrastructure without network facilities there is no infrastructure. Network Administration focused on the operation of this basic service and provides processes for administering a network environment on a day-to-day basis. S&NA Lab provides facilities and services to Monitor and manage the network, troubleshoot and repair faults in the network environment. This Lab provides guidance for the configuration and maintenance of the hardware and software components of a network. Through effective implementation of the Network Administration, IT organizations can expect to:

- Improve their deployment of network infrastructure.

- Improve troubleshooting processes and associated incident-management processes.

- Increase network reliability.

- Enhance availability of IT solutions and services.

HARDWARE REQUIREMENTS :

Processor	:	P-IV (2.4 GHZ)
RAM	:	256 MB
Hard Disk	:	40 GB
Monitor	:	15”
Keyboard	:	Normal
Mouse	:	Scroll
Cabinet	:	ATX
CD-Writer	:	Writer
Switches	:	16 PORT (2)
LAN Card		
ROUTER		
CAT 5/ CAT 6 Cables		
RJ-45 Connectors		

SOFTWARE REQUIREMENTS :

Operating System	:	Microsoft Windows 2003 Server Microsoft Windows XP Microsoft Windows 2000, Linux, Perl/Python

LIST OF PRACTICALS

1. USE OF TCP/IP UTILITIES IN SYSTEM ADMINISTRATION.
2. USE OF EVENT VIEWER.
3. HOW TO SET LOCAL SECURITY POLICIES.
4. HOW TO START & STOP SERVICES FROM WINDOWS AND COMMAND PROMPT.
5. LAN SETTING AND CONFIGURATION.
6. USE OF THE PERFORMANCE MONITOR.
7. MANAGEMENT OF USERS AND DOMAIN.
8. SETTING UP OF TERMINAL SERVICES.
9. USE OF THE NETWORK MONITOR.
10. SETTING UP OF DHCP.

Practical 1.

USE OF TCP/IP UTILITIES FOR SYSTEM ADMINISTRATION

1. IPCONFIG

Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. Used without parameters, ipconfig displays the IP address, subnet mask, and default gateway for all adapters.

ipconfig [/all] [/renew [*Adapter*]] [/release [*Adapter*]] [/flushdns] [/displaydns] [/registerdns] [/showclassid *Adapter*] [/setclassid *Adapter* [*ClassID*]]

```
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.113
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.254

C:\>ipconfig /all
Windows IP Configuration
        Host Name . . . . . . . . . . . . : lab1com20
        Primary Dns Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Unknown
        IP Routing Enabled. . . . . . . . : No
        WINS Proxy Enabled. . . . . . . . : No
Ethernet adapter Local Area Connection:
        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Realtek RTL8139 Family PCI
Fast Ethernet NIC
        Physical Address. . . . . . . . . : 00-11-09-16-6B-73
        Dhcp Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 192.168.1.113
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.254
        DNS Servers . . . . . . . . . . . : 192.168.1.254
```

2. PING

Verifies IP-level connectivity to another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo Request messages. The receipt of corresponding Echo Reply messages are displayed, along with round-trip times. Ping is the primary TCP/IP command used to troubleshoot connectivity, reachability, and name resolution. Used without parameters, ping displays help.

ping [-t] [-a] [-n *Count*] [-l *Size*] [-f] [-i *TTL*] [-v *TOS*] [-r *Count*] [-s *Count*] [{-j *HostList* **|** -k *HostList*}] [-w *Timeout*] [*TargetName*]

```
C:\>ping 192.168.1.110
Pinging 192.168.1.110 with 32 bytes of data:

Reply from 192.168.1.110: bytes=32 time<1ms TTL=128
Reply from 192.168.1.110: bytes=32 time<1ms TTL=128
Reply from 192.168.1.110: bytes=32 time<1ms TTL=128
Reply from 192.168.1.110: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.110:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3. TRACERT

Determines the path taken to a destination by sending Internet Control Message Protocol (ICMP) Echo Request messages to the destination with incrementally increasing Time to Live (TTL) field values. The path displayed is the list of near-side router interfaces of the routers in the path between a source host and a destination. The near-side interface is the interface of the router that is closest to the sending host in the path. Used without parameters, tracert displays help.

tracert [-d] [-h *MaximumHops*] [-j *HostList*] [-w *Timeout*] [*TargetName*]

```
C:\>tracert 192.168.1.110
Tracing route to 192.168.1.110 over a maximum of 30 hops
1    <1 ms    <1 ms    <1 ms  192.168.1.110
Trace complete.
```

4. PATHPING

Provides information about network latency and network loss at intermediate hops between a source and destination. Pathping sends multiple Echo Request messages to each router between a source and destination over a period of time and then computes results based on the packets returned from each router. Because pathping displays the degree of packet loss at any given router or link, you can determine which routers or subnets might be having network problems. Pathping performs the equivalent of the tracert command by identifying which routers are on the path. It then sends pings periodically to all of the routers over a specified time period and computes statistics based on the number returned from each. Used without parameters, pathping displays help.

pathping [-n] [-h *MaximumHops*] [-g *HostList*] [-p *Period*] [-q *NumQueries* [-w *Timeout*] [-T] [-R] [*TargetName*]

```
C:\>pathping 192.168.1.110

Tracing route to 192.168.1.110 over a maximum of 30 hops
0  lab1com20 [192.168.1.113]
1  192.168.1.110
Computing statistics for 25 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           lab1com20 [192.168.1.113]
                                0/ 100 =  0%   |
  1    0ms     0/ 100 =  0%     0/ 100 =  0%  192.168.1.110
Trace complete.
```

5. NET

You can use the net user command to create and modify user accounts on computers. When you use this command without command-line switches, the user accounts for the computer are listed. The user account information is stored in the user accounts database. This command works only on servers.

```
C:\>NET HELP
The syntax of this command is:
NET HELP
command
      -or-
NET command /HELP
   Commands available are:
   NET ACCOUNTS               NET HELP             NET SHARE
   NET COMPUTER               NET HELPMSG          NET START
   NET CONFIG                  NET LOCALGROUP        NET STATISTICS
   NET CONFIG SERVER           NET NAME              NET STOP
   NET CONFIG WORKSTATION      NET PAUSE             NET TIME
   NET CONTINUE                NET PRINT             NET USE
   NET FILE                    NET SEND              NET USER
   NET GROUP                   NET SESSION           NET VIEW
   NET HELP SERVICES lists some of the services you can start.
   NET HELP SYNTAX explains how to read NET HELP syntax lines.
   NET HELP command | MORE displays Help one screen at a time.

C:\>NET SEND 192.168.1.104 hi!
The message was successfully sent to 192.168.1.104.

C:\>NET ACCOUNTS
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          0
Maximum password age (days):                          42
Minimum password length:                              0
Length of password history maintained:                None
Lockout threshold:                                    Never
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                        WORKSTATION
The command completed successfully.

C:\>NET CONFIG
The following running services can be controlled:
   Server
   Workstation
The command completed successfully.

C:\>NET STATISTICS
Statistics are available for the following running services:
   Server
   Workstation
The command completed successfully.

C:\>NET USE
New connections will be remembered.
There are no entries in the list.

C:\>NET USER
User accounts for \\LAB1COM20
-----------------------------------------------------------------------
----
Admin                    Administrator            Guest
HelpAssistant            Rajat                    SUPPORT_388945a0
user
The command completed successfully.
C:\>NET VIEW
Server Name            Remark
-----------------------------------------------------------------------
----
\\LAB1COM10
\\LAB1COM11
\\LAB1COM12
\\LAB1COM13
```

```
\\LAB1COM14
\\LAB1COM15
\\LAB1COM16
\\LAB1COM17
\\LAB1COM18
\\LAB1COM2
\\LAB1COM20
\\LAB1COM23
\\LAB1COM24
\\LAB1COM25
\\LAB1COM3
\\LAB1COM4
\\LAB1COM5
\\LAB1COM6
\\LAB1COM7
\\LAB1COM8
The command completed successfully.
```

6. NETSAT

Displays active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, IPv4 statistics (for the IP, ICMP, TCP, and UDP protocols), and IPv6 statistics (for the IPv6, ICMPv6, TCP over IPv6, and UDP over IPv6 protocols). Used without parameters, **netstat** displays active TCP connections.

netstat [**-a**] [**-e**] [**-n**] [**-o**] [**-p** *Protocol*] [**-r**] [**-s**] [*Interval*]

```
C:\>NETSTAT -a
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    lab1com20:epmap        lab1com20:0            LISTENING
  TCP    lab1com20:microsoft-ds  lab1com20:0            LISTENING
  TCP    lab1com20:1025         lab1com20:0            LISTENING
  TCP    lab1com20:5000         lab1com20:0            LISTENING
  TCP    lab1com20:netbios-ssn  lab1com20:0            LISTENING
  UDP    lab1com20:epmap        *:*
  UDP    lab1com20:microsoft-ds *:*
  UDP    lab1com20:isakmp       *:*
  UDP    lab1com20:1026         *:*
  UDP    lab1com20:1027         *:*
  UDP    lab1com20:1032         *:*
  UDP    lab1com20:1054         *:*
  UDP    lab1com20:1059         *:*
  UDP    lab1com20:ntp          *:*
  UDP    lab1com20:1900         *:*
  UDP    lab1com20:ntp          *:*
  UDP    lab1com20:netbios-ns   *:*
  UDP    lab1com20:netbios-dgm  *:*
  UDP    lab1com20:1900         *:*
```

```
C:\>NETSTAT -e
Interface Statistics

                           Received            Sent
Bytes                       1283397          315664
Unicast packets                2596            2617
Non-unicast packets            5408             136
Discards                          0               0
Errors                            0               0
Unknown protocols                36

C:\>NETSTAT -RN
Route Table
=======================================================================
====
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 11 09 16 6b 73 ...... Realtek RTL8139 Family PCI Fast
Ethernet NIC - P
acket Scheduler Miniport
=======================================================================
====
=======================================================================
====
Active Routes:
Network Destination        Netmask          Gateway       Interface   Metric
          0.0.0.0          0.0.0.0    192.168.1.254   192.168.1.113       20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
      192.168.1.0    255.255.255.0    192.168.1.113   192.168.1.113       20
    192.168.1.113  255.255.255.255        127.0.0.1       127.0.0.1       20
    192.168.1.255  255.255.255.255    192.168.1.113   192.168.1.113       20
        224.0.0.0        240.0.0.0    192.168.1.113   192.168.1.113       20
  255.255.255.255  255.255.255.255    192.168.1.113   192.168.1.113       1

Default Gateway:     192.168.1.254
=======================================================================
====
Persistent Routes:
  None

C:\>NETSTAT -O
Active Connections
  Proto  Local Address          Foreign Address        State
PID

C:\>NETSTAT -N
Active Connections
  Proto  Local Address          Foreign Address        State

C:\>NETSTAT -P TCP
Active Connections
  Proto  Local Address          Foreign Address        State

C:\>NETSTAT -R
Route Table
=======================================================================
====
Interface List
0x1 ........................... MS TCP Loopback interface
0x2 ...00 11 09 16 6b 73 ...... Realtek RTL8139 Family PCI Fast
Ethernet NIC - P
acket Scheduler Miniport
=======================================================================
====
=======================================================================
====
Active Routes:
Network Destination        Netmask          Gateway       Interface
Metric
          0.0.0.0          0.0.0.0    192.168.1.254   192.168.1.113
20
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1
1
      192.168.1.0    255.255.255.0    192.168.1.113   192.168.1.113
20
    192.168.1.113  255.255.255.255        127.0.0.1       127.0.0.1
20
    192.168.1.255  255.255.255.255    192.168.1.113   192.168.1.113
20
        224.0.0.0        240.0.0.0    192.168.1.113   192.168.1.113
20
  255.255.255.255  255.255.255.255    192.168.1.113   192.168.1.113
1
Default Gateway:     192.168.1.254
=======================================================================
====
Persistent Routes:
None
```

C:\>NETSTAT -S

```
IPv4 Statistics
  Packets Received                   = 6912
  Received Header Errors             = 0
  Received Address Errors            = 123
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 0
  Received Packets Delivered         = 6873
  Output Requests                    = 2727
  Routing Discards                   = 0
  Discarded Output Packets           = 0
  Output Packet No Route             = 0
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

ICMPv4 Statistics
                            Received    Sent
  Messages                  223         235
  Errors                    0           0
  Destination Unreachable   1           1
  Time Exceeded             0           0
  Parameter Problems        0           0
  Source Quenches           0           0
  Redirects                 0           0
  Echos                     3           231
  Echo Replies              219         3
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0

TCP Statistics for IPv4
  Active Opens                        = 211
  Passive Opens                       = 7
  Failed Connection Attempts          = 22
  Reset Connections                   = 26
  Current Connections                 = 0
  Segments Received                   = 1446
  Segments Sent                       = 1451
  Segments Retransmitted              = 8

UDP Statistics for IPv4
  Datagrams Received    = 5141
  No Ports              = 280
  Receive Errors        = 0
  Datagrams Sent        = 1027
```

Practical 2.

USE OF EVENT VIEWER

Event Viewer

Using the event logs in Event Viewer, you can gather information about hardware, software, and system problems. You can also monitor Windows XP security events.

A computer running any version of Windows XP records events in three kinds of logs:

1. Application log:

The application log contains events logged by applications or programs. For example, a database program might record a file error in the application log. Program developers decide which events to monitor.

2. Security log:

The security log records events such as valid and invalid logon attempts, as well as events related to resource use such as creating, opening, or deleting files or other objects. An administrator can specify what events are recorded in the security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the security log.

3. System log:

The system log contains events logged by Windows XP system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. The event types logged by system components are predetermined by Windows XP.

A computer running Windows configured as a domain controller records events in two additional logs:

- Directory service log:

The directory service log contains events logged by the Windows directory service. For example, connection problems between the server and the global catalog are recorded in the directory service log.

- File Replication service log:

The File Replication service log contains events logged by the Windows File Replication service. For example, file replication failures and events that occur while domain controllers are being updated with information about sysvol changes are recorded in the file replication log.

A computer running Windows configured as a Domain Name System (DNS) server records events in an additional log:

DNS server log
The DNS server log contains events logged by the Windows DNS service. Events associated with resolving DNS names to Internet Protocol (IP) addresses are recorded in this log.

Event Viewer displays these types of events:

- Error
  A significant problem, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error event will be logged.

- Warning
  An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning event will be logged.

- Information
  An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged.

- Success Audit
  An audited security access attempt that succeeds. For example, a user's successful attempt to log on to the system will be logged as a Success Audit event.

- Failure Audit
  An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.

The Event Log service starts automatically when you start Windows. All users can view application and system logs. Only administrators can gain access to security logs.

By default, security logging is turned off. You can use Group Policy to enable security logging. The administrator can also set auditing policies in the registry that cause the system to halt when the security log is full.

Notes

- The EventLog service starts automatically when you start Windows.
- All users can view application and system logs. Security logs are accessible only to system administrators.
- By default, security logging is turned off. To enable security logging, use Group Policy to set the Audit policy. The administrator can also set auditing policies in the registry that cause the system to halt when the security log is full.

The Event Header:

Information *Meaning*

Date The date the event occurred.

Time The local time the event occurred.

User The user name of the user on whose behalf the event occurred. This name is the client ID if the event was actually caused by a server process, or the primary ID if impersonation is not taking place. Where applicable, a security log entry contains both the primary and impersonation IDs. Impersonation occurs when Windows XP allows one process to take on the security attributes of another.

Computer The name of the computer where the event occurred. The computer name is usually your own, unless you are viewing an event log on another Windows XP computer.

Event ID A number identifying the particular event type. The first line of the description usually contains the name of the event type. For example, 6005 is the ID of the event that occurs when the Event log service is started. The first line of the description of such an event is "The Event log service was started." The Event ID and the Source can be used by product support representatives to troubleshoot system problems.

Source The software that logged the event, which can be either a program name such as "SQL Server," or a component of the system or of a large program such as a driver name. For example, "Elnkii" indicates an EtherLink II driver.

Type A classification of the event severity: Error, Information, or Warning in the system and application logs; Success Audit or Failure Audit in the security log. In the Event Viewer normal list view, these are represented by a symbol.

Category A classification of the event by the event source. This information is primarily used in the security log. For example, for security audits, this corresponds to one of the event types for which success or failure auditing can be enabled in Group Policy.

The Event Description:

The format and contents of the event description vary, depending on the event type. The description is often the most useful piece of information, indicating what happened or the significance of the event.

The event logs record five types of events:

Event type *Description*

Error A significant problem, such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error will be logged.

Warning An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning will be logged.

Information An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, an Information event will be logged.

Success Audit An audited security access attempt that succeeds. For example, a user's successful attempt to log on the system will be logged as a Success Audit event.

Failure Audit An audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt will be logged as a Failure Audit event.

Notes

- If used, the optional data field contains binary data, which can be displayed in bytes or words. This information is generated by the program that was the source of the event record. The data appears in hexadecimal format. Its meaning can be interpreted by a support technician familiar with the source program.
- When viewing an application or system log on a LAN Manager 2.*x* server, only the date, time, source, and event ID are shown. When viewing a security log on a LAN Manager 2.*x* server, only the date, time, category, user, and computer are shown.

Setting options for logging events

Application and system logging start automatically when you start the computer. Logging stops when an event log becomes full and cannot overwrite itself, either because it has been set for manual clearing or because the first event in the log is not old enough. You use Group Policy to set up security logging.

To define logging parameters for each kind of log, in the Event View console tree, right-click the type of log, and then click Properties. On the General tab, you can set the maximum size of the log and specify whether the events are overwritten or stored for a certain period of time.

The default logging policy is to overwrite logs as needed, provided events are at least seven days old. You can customize this policy for different logs.

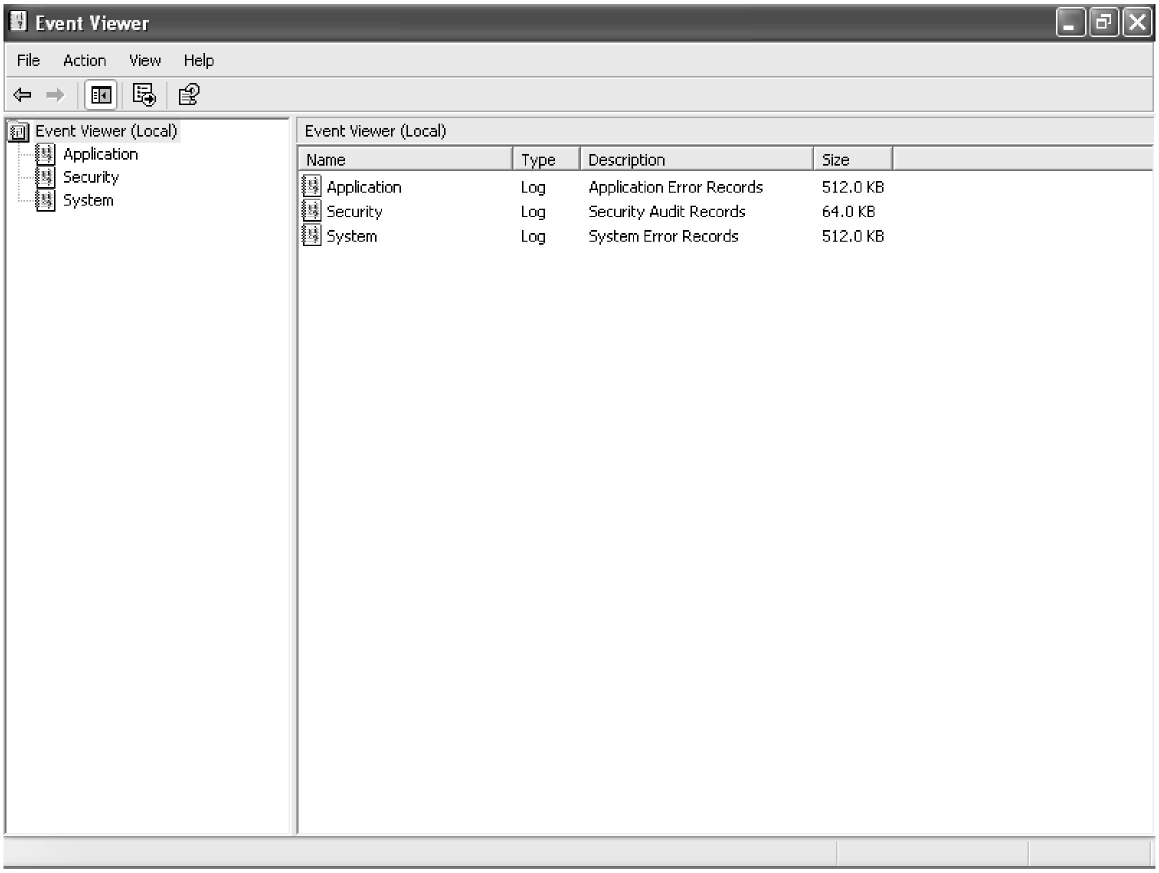
The Event log wrapping options include the following.

Use	To
Overwrite events as needed	Have new events continue to be written when the log is full. Each new event replaces the oldest event in the log. This option is a good choice for low-maintenance systems.
Overwrite events older than [*x*] days	Retain the log for the number of days you specify before overwriting events. The default is seven days. This option is the best choice if you want to archive log files weekly. This strategy minimizes the chance of losing important log entries and at the same time keeps log sizes reasonable.
Do not overwrite events	Clear the log manually rather than automatically. Select this option only if you cannot afford to miss an event (for example, for the security log at a site where security is extremely important).

Notes:

- When a log is full and no more events can be logged, you can free the log by clearing it. Reducing the amount of time you keep an event also frees the log if it allows the next record to be overwritten.
- Each log file has an initial maximum size of 512 KB. You can increase the maximum log size to the capacity of the disk and memory, or you can decrease the maximum log size. Before decreasing a log's size, you must clear the log.
- Event Viewer Window :

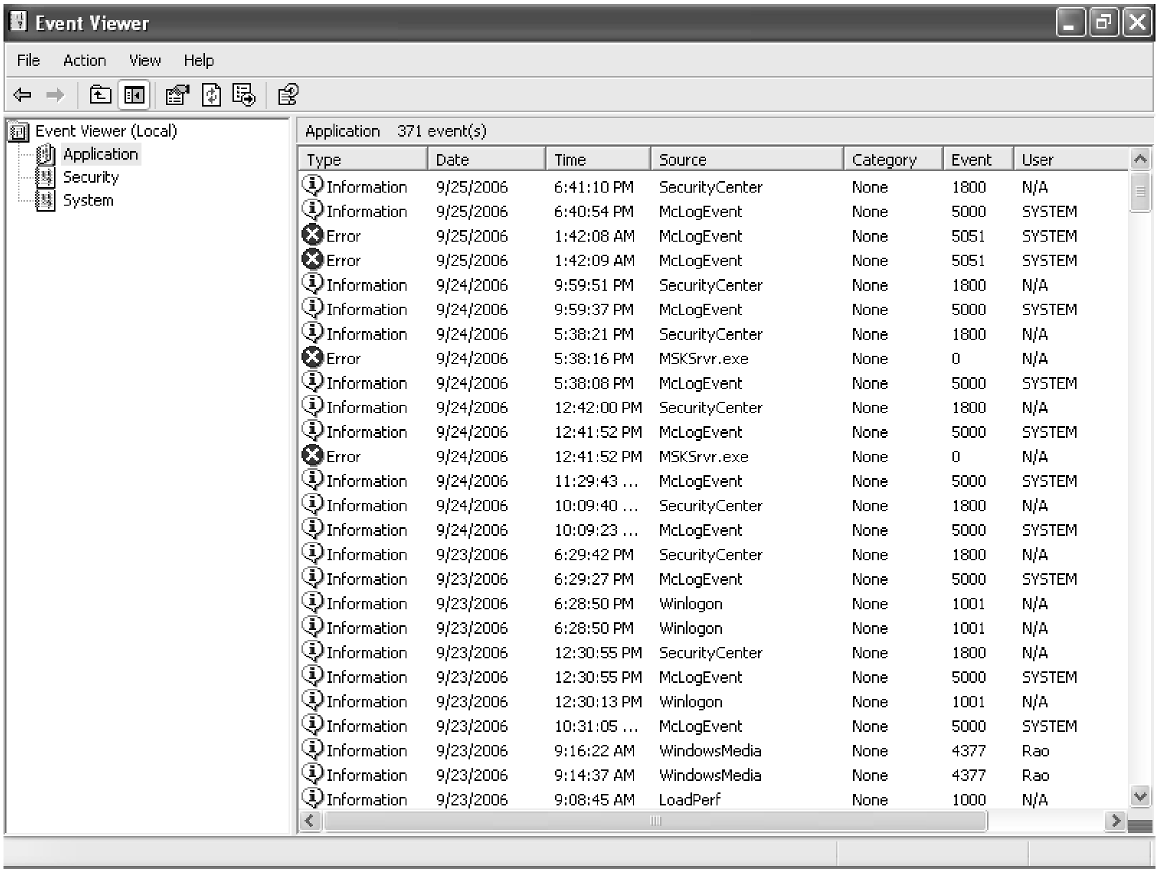
Start → Control Panel → Administrative Tools → Event Viewer → Open



Name	Type	Description	Size
Application	Log	Application Error Records	512.0 KB
Security	Log	Security Audit Records	64.0 KB
System	Log	System Error Records	512.0 KB

Application Log Window:

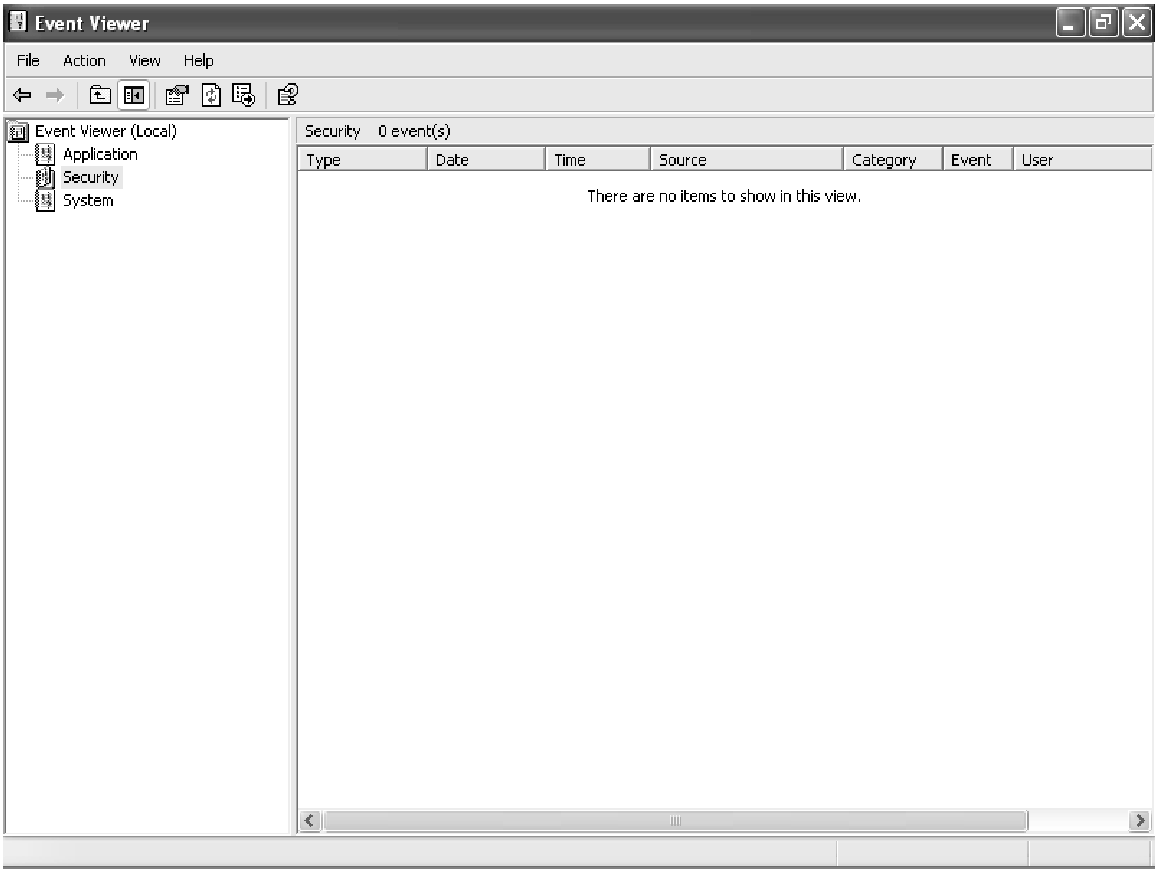
It contains events logged by applications or programs.



Type	Date	Time	Source	Category	Event	User
Information	9/25/2006	6:41:10 PM	SecurityCenter	None	1800	N/A
Information	9/25/2006	6:40:54 PM	McLogEvent	None	5000	SYSTEM
Error	9/25/2006	1:42:08 AM	McLogEvent	None	5051	SYSTEM
Error	9/25/2006	1:42:09 AM	McLogEvent	None	5051	SYSTEM
Information	9/24/2006	9:59:51 PM	SecurityCenter	None	1800	N/A
Information	9/24/2006	9:59:37 PM	McLogEvent	None	5000	SYSTEM
Information	9/24/2006	5:38:21 PM	SecurityCenter	None	1800	N/A
Error	9/24/2006	5:38:16 PM	MSKSrvr.exe	None	0	N/A
Information	9/24/2006	5:38:08 PM	McLogEvent	None	5000	SYSTEM
Information	9/24/2006	12:42:00 PM	SecurityCenter	None	1800	N/A
Information	9/24/2006	12:41:52 PM	McLogEvent	None	5000	SYSTEM
Error	9/24/2006	12:41:52 PM	MSKSrvr.exe	None	0	N/A
Information	9/24/2006	11:29:43 ...	McLogEvent	None	5000	SYSTEM
Information	9/24/2006	10:09:40 ...	SecurityCenter	None	1800	N/A
Information	9/24/2006	10:09:23 ...	McLogEvent	None	5000	SYSTEM
Information	9/23/2006	6:29:42 PM	SecurityCenter	None	1800	N/A
Information	9/23/2006	6:29:27 PM	McLogEvent	None	5000	SYSTEM
Information	9/23/2006	6:28:50 PM	Winlogon	None	1001	N/A
Information	9/23/2006	6:28:50 PM	Winlogon	None	1001	N/A
Information	9/23/2006	12:30:55 PM	SecurityCenter	None	1800	N/A
Information	9/23/2006	12:30:55 PM	McLogEvent	None	5000	SYSTEM
Information	9/23/2006	12:30:13 PM	Winlogon	None	1001	N/A
Information	9/23/2006	10:31:05 ...	McLogEvent	None	5000	SYSTEM
Information	9/23/2006	9:16:22 AM	WindowsMedia	None	4377	Rao
Information	9/23/2006	9:14:37 AM	WindowsMedia	None	4377	Rao
Information	9/23/2006	9:08:45 AM	LoadPerf	None	1000	N/A

<u>Security Log Window:</u>

It records events such as valid and invalid logon attempts, as well as events related to resource use such as creating, opening, or deleting files or other objects. An administrator can specify what events are recorded in the security log.



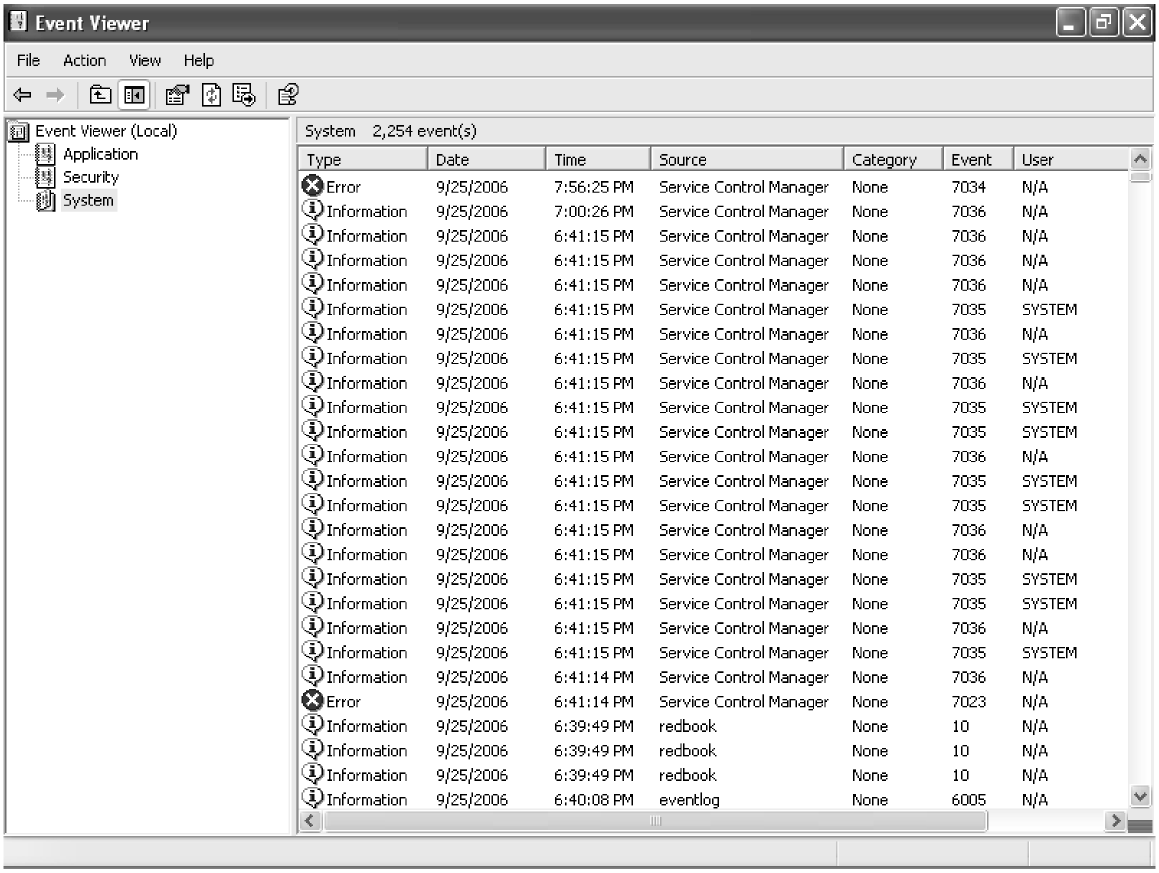
Security 0 event(s)

Type	Date	Time	Source	Category	Event	User

There are no items to show in this view.

System Log Window:

It contains events logged by Windows XP system components.



Type	Date	Time	Source	Category	Event	User
Error	9/25/2006	7:56:25 PM	Service Control Manager	None	7034	N/A
Information	9/25/2006	7:00:26 PM	Service Control Manager	None	7036	N/A
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7036	N/A
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7036	N/A
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7036	N/A
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7035	SYSTEM
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7036	N/A
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7035	SYSTEM
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7036	N/A
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7035	SYSTEM
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7035	SYSTEM
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7036	N/A
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7035	SYSTEM
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7035	SYSTEM
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7036	N/A
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7036	N/A
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7035	SYSTEM
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7035	SYSTEM
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7036	N/A
Information	9/25/2006	6:41:15 PM	Service Control Manager	None	7035	SYSTEM
Information	9/25/2006	6:41:14 PM	Service Control Manager	None	7036	N/A
Error	9/25/2006	6:41:14 PM	Service Control Manager	None	7023	N/A
Information	9/25/2006	6:39:49 PM	redbook	None	10	N/A
Information	9/25/2006	6:39:49 PM	redbook	None	10	N/A
Information	9/25/2006	6:39:49 PM	redbook	None	10	N/A
Information	9/25/2006	6:40:08 PM	eventlog	None	6005	N/A

Practical 3.

HOW TO SET LOCAL SECURITY POLICIES

ACCOUNT POLICIES

All security policies are computer-based policies. Account policies are defined on computers, yet they affect how user accounts can interact with the computer or domain. Account policies contain three subsets:

- Password policy. Used for domain or local user accounts. Determines settings for passwords, such as enforcement and lifetimes.
- Account lockout policy. Used for domain or local user accounts. Determines the circumstances and length of time that an account will be locked out of the system.
- Kerberos policy. Used for domain user accounts. Determines Kerberos-related settings, such as ticket lifetimes and enforcement. Kerberos policies do not exist in local computer policy.

For domain accounts, there can be only one account policy. The account policy must be defined in the Default Domain policy and is enforced by the domain controllers that make up the domain. A domain controller always obtains the account policy from the Default Domain Policy Group Policy object, even if there is a different account policy applied to the organizational unit that contains the domain controller. By default, workstations and servers joined to a domain (such as member computers) will also receive the same account policy for their local accounts. However, local account policies can be different from the domain account policy, such as when you define an account policy specifically for the local accounts.

There are two policies in Security Options that also behave like account policies. These are:

- Network Access: Allow anonymous SID/NAME translation
- Network Security: Force Logoff when Logon Hours expire

Password Policy

Enforce password history

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy

Description:
Determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. The value must be between 0 and 24 passwords.
This policy enables administrators to enhance security by ensuring that old passwords are not reused continually.
To maintain the effectiveness of the password history, do not allow passwords to be changed immediately when you configure the Minimum password age.

Maximum password age

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy
Description
Determines the period of time (in days) that a password can be used before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0.

Minimum password age

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy
Description
Determines the period of time (in days) that a password must be used before the user can change it. You can set a value between 1 and 999 days, or you can allow changes immediately by setting the number of days to 0.
The minimum password age must be less than the Maximum password age.
Configure the minimum password age to be more than 0 if you want Enforce password history to be effective. Without a minimum password age, users can cycle through passwords repeatedly until they get to an old favorite. The default setting does not follow this recommendation, so that an administrator can specify a password for a user and then require the user to change the administrator-defined password when the user logs on. If the password history is set to 0, the

user does not have to choose a new password. For this reason, password history is set to 1 by default.
Default: 0.

Minimum password length

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy
Description
Determines the least number of characters that a password for a user account may contain. You can set a value of between 1 and 14 characters, or you can establish that no password is required by setting the number of characters to 0.
Default: 0.

Password must meet complexity requirements

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy
Description
Determines whether passwords must meet complexity requirements.
If this policy is enabled, passwords must meet the following minimum requirements:

- Not contain all or part of the user's account name
- Be at least six characters in length
- Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Nonalphanumeric characters (e.g., !, $, #, %)

Complexity requirements are enforced when passwords are changed or created.
To create custom password filters, see the Microsoft Platform Software Development Kit and the Microsoft Technet.
Default: Disabled.

Store password using reversible encryption for all users in the domain

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy

Description

Determines whether Windows 2000 Server, Windows 2000 Professional, and Windows XP Professional store passwords using reversible encryption.

This policy provides support for applications that use protocols that require knowledge of the user's password for authentication purposes. Storing passwords using reversible encryption is essentially the same as storing plaintext versions of the passwords. For this reason, this policy should never be enabled unless application requirements outweigh the need to protect password information.

This policy is required when using CHAP authentication through remote access or IAS services. It is also required when using Digest Authentication in Internet Information Services (IIS).

Default: Disabled.

Account Lockout Policy

Account lockout duration

Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy

Description

Determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is 1 to 99,999 minutes. You can specify that the account will be locked out until an administrator explicitly unlocks it by setting the value to 0.

If an account lockout threshold is defined, the account lockout duration must be greater than or equal to the reset time.

Default: None, because this policy setting only has meaning when an Account lockout threshold is specified.

Account lockout threshold

Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy

Description
Determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 1 and 999 failed logon attempts, or you can specify that the account will never be locked out by setting the value to 0.
Failed password attempts against workstations or member servers that have been locked using either CTRL+ALT+DELETE or password-protected screen savers do not count as failed logon attempts.
Default: Disabled.

Reset account lockout counter after

Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy
Description
Determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts. The available range is 1 minute to 99,999 minutes.
If an account lockout threshold is defined, this reset time must be less than or equal to the Account lockout duration.
Default: None, because this policy setting only has meaning when an Account lockout threshold is specified.

LOCAL POLICIES

Local Security Policy overview

Security policy ia a combination of security settings that affect the security on a computer. You can use Local Security Policy to edit account policies and local policies on your local computer.

With Local Security Policy, you can control:

- Who accesses your computer.
- What resources users are authorized to use on your computer.
- Whether or not a user or group's actions are recorded in the event log.

How policy is applied to a computer that is joined to a domain

If your local computer is joined to a domain, you are subject to obtaining security policy from the domain's policy or from the policy of any organizational unit that you are a member of. If you are getting policy from more than one source, then any conflicts are resolved in this order of precedence, from highest to lowest:

- Organizational unit policy
- Domain policy
- Site policy
- Local computer policy

When you modify the security settings on your local computer using **Local security policy**, then you are directly modifying the settings on your computer, therefore, the settings take effect immediately, but this may only be temporary. The settings will actually remain in effect on your local computer until the next refresh of Group Policy security settings, when the security settings that are received from Group Policy will override your local settings wherever there are conflicts. The security settings are refreshed every 90 minutes on a workstation or server and every 5 minutes on a domain controller. The settings are also refreshed every 16 hours, whether or not there are any changes.

AUDIT POLICY

Determines whether security events are logged into the Security log on the computer. Also determines whether to log successful attempts, failed attempts or both. (The Security log is part of Event Viewer.)

Audit account logon events

Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy

Description

Determines whether to audit each instance of a user logging on to or logging off from another computer in which this computer is used to validate the account.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when an account logon attempt succeeds. Failure audits generate an audit entry when an account logon attempt fails. To set this value to no auditing, in the **Properties** dialog box for this policy setting, select the **Define these policy settings** check box and clear the **Success** and **Failure** check boxes.

If success auditing for account logon events is enabled on a domain controller, an entry is logged for each user who is validated against that domain controller, even though the user is actually logging on to a workstation that is joined to the domain.

Default:

- No auditing for domain controllers.
- Undefined for a member computer.

Audit logon events

Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy

Description

Determines whether to audit each instance of a user logging on to, logging off from, or making a network connection to this computer.

If you are logging successful Audit account logon events on a domain controller, workstation logon attempts do not generate logon audits. Only interactive and network logon attempts to the domain controller itself generate logon events. In short, "account logon events" are generated where the account lives; "logon events" are generated where the logon attempt occurs.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when a logon attempt succeeds. Failure audits generate an audit entry when a logon attempt fails. To set this value to no auditing, in the **Properties** dialog box for this policy setting, select the **Define these policy settings** check box and clear the **Success** and **Failure** check boxes.

Default: No auditing.

USER RIGHTS

Determines which users or groups have logon rights or privileges on the computer.

Access this computer from the network

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Description

Determines which users and groups are allowed to connect to the computer over the network.

Important

- Modifying this setting may affect compatibility with clients, services, and applications. For compatibility information about this setting, see Access this computer from network (http://go.microsoft.com/fwlink/?LinkId=24267) at the Microsoft website.

Default:

- On workstations and servers:
    - Administrators
    - Backup Operators
    - Power Users
    - Users
    - Everyone
- On domain controllers:
    - Administrators
    - Authenticated Users
    - Everyone

Allow logon through Terminal Services

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Description

Determines which users or groups have permission to log on as a Terminal Services client.

Default:

- On workstation and servers: Administrators, Remote Desktop Users.
- On domain controllers: Administrators.

Important

- This setting does not have any effect on Windows 2000 computers that have not been updated to Service Pack 2.

Change the system time

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Description

Determines which users and groups can change the time and date on the internal clock of the computer.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

Default:

- On workstations and servers:
    - Administrators
    - Power Users

- On domain controllers:
    - Administrators
    - Server Operators

Debug programs

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Description

Determines which users can attach a debugger to any process. This privilege provides powerful access to sensitive and critical operating system components.

Default:

- Administrators
- Local System

Force shutdown from a remote system

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Description

Determines which users are allowed to shut down a computer from a remote location on the network.

This user right is defined in the Default Domain Controller Group Policy object (GPO) and in the local security policy of workstations and servers.

Default:

- On workstations and servers: Administrators.
- On domain controllers: Administrators, Server Operators.

Log on locally

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Description

Determines which users can log on to the computer.

Important

- Modifying this setting may affect compatibility with clients, services, and applications. For compatibility information about this setting, see Allow log on locally (http://go.microsoft.com/fwlink/?LinkId=24268) at the Microsoft website.

Default:

- On workstations and servers: Administrators, Backup Operators, Power Users, Users, and Guest.
- On domain controllers: Account Operators, Administrators, Backup Operators, and Print Operators.

Load and unload device drivers

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Description

Determines which users can dynamically load and unload device drivers. This privilege is necessary for installing drivers for Plug and Play devices.

Default: Administrators.

Manage auditing and security log

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Description

Determines which users can specify object access auditing options for individual resources, such as files, Active Directory objects, and registry keys.

This policy does not allow a user to enable file and object access auditing in general. For such auditing to be enabled, the Audit object access setting in Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policies must be configured.

You can view audited events in the security log of the Event Viewer. A user with this privilege can also view and clear the security log.

Default: Administrators.

Shut down the system

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Description

Determines which users who are logged on locally to the computer can shut down the operating system using the **Shut Down** command.

Default:

- Workstations and servers: Administrators, Backup Operators, Power Users, Users.
- Domain controllers: Account Operators, Administrators, Backup Operators, Server Operators, Print Operators.

Take ownership of files or other objects

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Description

Determines which users can take ownership of any securable object in the system, including Active Directory objects, files and folders, printers, registry keys, processes, and threads.

Default: Administrators.

Restore files and directories

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Description

Determines which users can circumvent file and directory permissions when restoring backed up files and directories, and determines which users can set any valid security principal as the owner of an object.

Default:

- Workstations and servers: Administrators, Backup Operators.
- Domain controllers: Administrators, Backup Operators, Server Operators.

Profile system performance

Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

Description

Determines which users can use performance monitoring tools to monitor the performance of system processes.

Default: Administrators, Local System.

SECURITY OPTIONS

Enables or disables security settings for the computer, such as digital signing of data, Administrator and Guest account names, floppy drive and CD-ROM access, driver installation, and logon prompts.

Accounts: Administrator account status

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Description

Determines whether the Administrator account is enabled or disabled under normal operation. Under safe mode boot, the Administrator account is always enabled, regardless of this setting.

Default: Enabled.

Notes

- If you try to reenable the Administrator account after it has been disabled, and if the current Administrator password does not meet the password requirements, you cannot reenable the account. In this case, an alternative member of the Administrators group must set the password on the Administrator account by using the Local Users and Groups user interface.
- Disabling the Administrator account can become a maintenance issue under certain circumstances. For example, in a domain environment, if the secure channel that constitutes your join fails for any reason, and there is no other local Administrator account, you must restart in safe mode to fix the problem that is causing your join status to be broken.

Accounts: Guest account status

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Description

Determines if the Guest account is enabled or disabled.

Default: Disabled.

Note

- If the Guest account is disabled and the security option "Network Access: Sharing and Security Model" is set to "Guest Only," network logons, such as those performed by the Microsoft Network Server (SMB Service), will fail.

Audit: Shut down system immediately if unable to log security audits

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Description

Determines whether the system shuts down if it is unable to log security events.

If this policy is enabled, it causes the system to stop if a security audit cannot be logged for any reason. Typically, an event fails to be logged when the security audit log is full and the retention method that is specified for the security log is either "Do Not Overwrite Events" or "Overwrite Events by Days."

If the security log is full and an existing entry cannot be overwritten, and this security option is enabled, the following Stop error appears:

STOP: C0000244 {Audit Failed}
An attempt to generate a security audit failed.

To recover, an administrator must log on, archive the log (optional), clear the log, and reset this option as desired.

Default: Disabled.

Devices: Prevent users from installing printer drivers

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Description

For a computer to print to a network printer, the driver for that network printer must be installed on the local computer. This security setting determines who is allowed to install a printer driver as part of adding a network printer. If this setting is enabled, only Administrators and Power Users can install a printer driver as part of adding a network printer. If this setting is disabled, any user can install a printer driver as part of adding a network printer. This setting can be used to prevent unprivileged users from downloading and installing an untrusted printer driver.

Default:

- Enabled on servers.
- Disabled on workstations.

Notes

- If an administrator has configured a trusted path for downloading drivers, this setting has no impact. When trusted paths are used, the print subsystem attempts to use the trusted path to download the driver. If the trusted path download succeeds, the driver is installed on behalf of any user. If the trusted path download fails, the driver is not installed and the network printer cannot be added.

- If this setting is enabled, but the driver for a network printer already exists on the local machine, users can still add the network printer.

Domain controller: Refuse machine account password changes

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Description

Determines whether or not a Domain Controller will accept password change requests for computer accounts. If enabled on all Domain Controllers in a domain, then domain members will not be able to change their machine account passwords leaving those passwords susceptible to attack.

Default: Disabled.

Interactive logon: Do not require CTRL+ALT+DEL

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Description

Determines whether pressing CTRL+ALT+DEL is required before a user can log on.

If this policy is enabled on a computer, a user is not required to press CTRL+ALT+DEL to log on. Not having to press CTRL+ALT+DEL leaves users susceptible to attacks that attempt to intercept the users' passwords. Requiring CTRL+ALT+DEL before users log on ensures that users are communicating by means of a trusted path when entering their passwords.

If this policy is disabled, any user is required to press CTRL+ALT+DEL before logging on to Windows (unless they are using a smart card for Windows logon).

Default:

- Disabled on workstations and servers that are joined to a domain.
- Enabled on stand-alone workstations.

Network security: Force logoff when logon hours expire

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Description

Determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the Server Message Block (SMB) component.

When this policy is enabled, it causes client sessions with the SMB server to be forcibly disconnected when the client's logon hours expire.

If this policy is disabled, an established client session is allowed to be maintained after the client's logon hours have expired.

Default: Enabled.

Note

- For domain accounts, there can be only one account policy. The account policy must be defined in the Default Domain Policy, and it is enforced by the domain controllers that make up the domain. A domain controller always pulls the account policy from the Default Domain Policy Group Policy object (GPO), even if there is a different account policy applied to the organizational unit that contains the domain controller. By default, workstations and servers that are joined to a domain (i.e., member computers) also receive the same account policy for their local accounts. However, local account policies for member computers can be different from the domain account policy by defining an account policy for the organizational unit that contains the member computers. Kerberos settings are not applied to member computers.

Interactive logon: Message text for users attempting to log on

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Description

Specifies a text message that is displayed to users when they log on.

This text is often used for legal reasons, for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited.

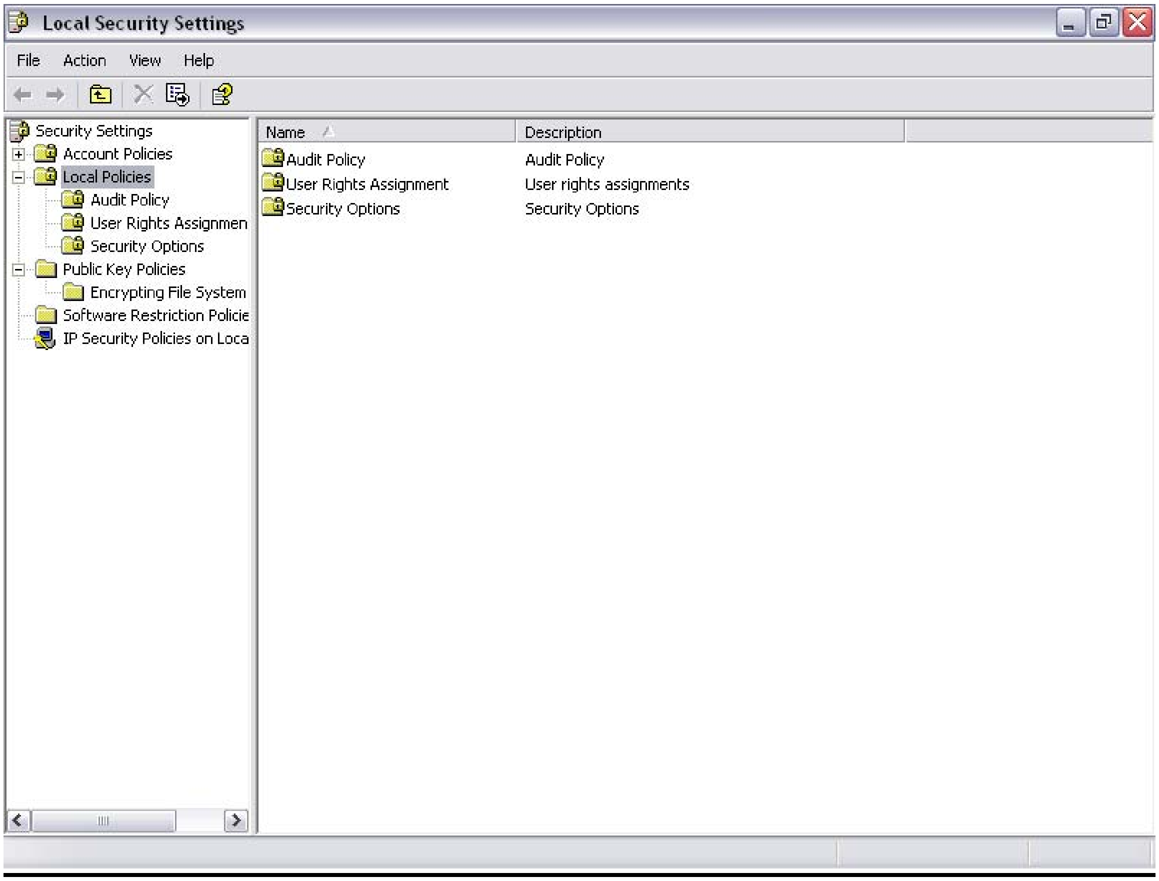
Default: No message.

Caution

- Windows XP Professional adds support for configuring logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000 clients cannot interpret and display message text that is created by Windows XP Professional computers. You must use a Windows 2000 computer to create a logon message policy that applies to Windows 2000 computers. If you inadvertently create a logon message policy using a Windows XP Professional computer, and you discover that it does not display properly on Windows 2000 computers, do the following:

- Undefine the setting.
- Redefine the setting using a Windows 2000 computer.

Simply changing a Windows XP Professional-defined logon message policy using a Windows 2000 computer does not work. The setting must be undefined first.



Name	Description
Audit Policy	Audit Policy
User Rights Assignment	User rights assignments
Security Options	Security Options

Practical 4.

HOW TO START AND STOP SERVICES FROM USER WINDOW AND COMMAND PROMPT

Services Overview

A service is an application type that runs in the background and is similar to UNIX daemon applications. Service applications typically provide features such as client/server applications, Web servers, database servers, and other server-based applications to users, both locally and across the network.

> **Service :** A program, routine, or process that performs a specific system function to support other programs, particularly at a low (close to the hardware) level.

You can use Services to:

- Start, stop, pause, resume, or disable a services on remote and local computers. You must have the appropriate permissions to start, stop, pause, restart, and disable services.
- Manage services on local and remote computers (on remote computers running Windows XP, Windows 2000, or Windows NT 4.0 only).
- Set up recovery actions to take place if a service fails, for example, restarting the service automatically or restarting the computer (on computers running Windows XP or Windows 2000 only).
- Enable or disable services for a particular hardware profile.
- View the status and description of each service.

Services permissions

Each service has special permissions that you can grant or deny for each user or group. You can set permissions for individual services by using Security Templates.
Services must log on to an account in order to access resources and objects on the operating system. Some services are configured by default to log on to the Local System account, which is a powerful account that has full access to the system. If a service logs on to the Local System account on a domain controller, that service has access to the entire domain. Other services are configured to log on to LocalService or NetworkService accounts, which are special built-in accounts that are similar to authenticated user accounts. These accounts have the same level of access to resources and objects as members of the Users groups. This limited access helps safeguard your system if individual services or processes are compromised.

Services running as the LocalService account access network resources as a null session with no credentials. Services running as the NetworkService account access network resources using the credentials of the machine account.

- Changing the account under which a service is run might prevent the service from running properly.

The following table lists the individual service permissions that you can apply.

Permission	**Allows you to**
Full Control	Perform all functions. This permission automatically grants all service permissions to the user.
Query Template	Determine the configuration parameters associated with a service object.
Change Template	Change the configuration of a service.
Query Status	Access information about the status of the service.
Enumerate Dependents	Determine all of the other services that are dependent on the specified service.
Start	Start a service.
Stop	Stop a service.
Pause and Continue	Pause and continue the service.
Interrogate	Report the current status information for the service.
User-Defined Control	Send a user-defined control request, or a request that is specific to the service, to the service.
Delete	Delete a service.
Read Permissions	Read the security permissions assigned to the service.
Change Permissions	Change the security permissions assigned to the service.
Take Ownership	Change a security key or change permission on a service that is not owned by the user.

Steps to be performed before Starting and Stopping Services

1. *Save the default settings.*

2. Perform testing & back up.

3. Check dependencies.

4. Check connected users.

5. Give application start up for disabled.

To configure how a service is started

1. Open Services.
2. Right-click the service that you want to configure, and then click **Properties**.
3. On the **General** tab, in the **Startup type** box, click **Automatic**, **Manual**, or **Disabled**.
4. To specify the user account that the service can use to log on, click the **Log On** tab, and then do one of the following:
   - To specify that the service use the LocalSystem account, click **Local System account**.
   - To specify that the service use the LocalService account, click **This account**, and then type **NT AUTHORITY\LocalService**.
   - To specify that the service use the NetworkService account, click **This account**, and then type **NT AUTHORITY\NetworkService**.
   - To specify another account, click **This account**, click **Browse**, and then specify a user account in the **Select User** dialog box. When you are finished, click **OK**.
5. Type the password for the user account in the **Password** box and in the **Confirm password** box, and then click **OK**.

Important

- Changing the default service settings might prevent key services from running correctly. It is especially important to use caution when changing the Startup Type and Log On As settings of services that are configured to start automatically.

Notes

- To open Services, click **Start**, click **Control Panel**, click **Performance and Maintenance**, click **Administrative Tools**, and then double-click **Services**.
- You must be logged on as an administrator or a member of the Administrators group in order to complete this procedure. If your computer is connected to a

network, network policy settings might also prevent you from completing this procedure.

- If you enable or disable a service and you encounter a problem starting the computer, you might be able to start the computer in safe mode. Then you can change the service configuration or restore the default configuration. For more information, see Related Topics.
- If you select the **Allow service to interact with desktop** check box, the service is enabled to provide a user interface on a desktop. This feature is available only if you click **Local System account** and only if the service is configured to interact with the desktop.
- For more information about the user accounts that a service uses to log on, see Related Topics.

To start, stop, pause, resume, or restart a service

1. Open Services.
2. In the details panel, do one of the following:
   - Select the service. On the **Action** menu, click **Start**, **Stop**, **Pause**, **Resume**, or **Restart**.
   - Right-click the service, and then click **Start**, **Stop**, **Pause**, **Resume**, or **Restart**.

Important

- If you stop, start, or restart a service, any dependent services are also affected.
- Changing the default service settings might prevent key services from running correctly. It is especially important to use caution when changing the Startup Type and Log On As settings of services that are configured to start automatically.

Notes

- To open Services, click **Start**, click **Control Panel**, click **Performance and Maintenance**, click **Administrative Tools**, and then double-click **Services**.
- You must be logged on as an administrator or a member of the Administrators group in order to complete this procedure. If your computer is connected to a network, network policy settings might also prevent you from completing this procedure.
- To configure startup parameters for a service, right-click the service, click **Properties**, and then type the parameters in **Start parameters** before you click **Start**. These settings are used only once and are not saved. (A backslash (\) is treated as an escape character; type two backslashes for each backslash in a parameter.)

SC – Service Controller
Communicates with the Service Controller and installed services. SC.exe retrieves and sets control information about services. You can use SC.exe for testing and debugging service programs. Service properties stored in the registry can be set to control how service applications are started at boot time and run as background processes. SC.exe parameters can configure a specific service, retrieve the current status of a service, as well as stop and start a service. You can create batch files that call various SC.exe commands to automate the startup or shutdown sequence of services. SC.exe provides capabilities similar to Services in the Administrative Tools item in Control Panel.
For the command syntax, click any of the following **sc** commands:

sc start

Starts a service running.

Syntax

sc [*ServerName*] **start** *ServiceName* [*ServiceArguments*]

Parameters

ServerName

Specifies the name of the remote server on which the service is located. The name must use the UNC format ("\\myserver"). To run SC.exe locally, ignore this parameter.

ServiceName

Specifies the service name returned by the **getkeyname** operation.

ServiceArguments

Specifies service arguments to pass to the service to be started.

/?

Displays help at the command prompt.

Examples

The following example shows how you can use the **sc start** command:

sc start tapisrv

sc stop

Sends a STOP control request to a service.

Syntax

sc [*ServerName*] **stop** *ServiceName*

Parameters

ServerName

Specifies the name of the remote server on which the service is located. The name must use the UNC format ("\\myserver"). To run SC.exe locally, ignore this parameter.

ServiceName

Specifies the service name returned by the **getkeyname** operation.

/?

Displays help at the command prompt.

- Not all services can be stopped.

Examples

The following example shows how you can use the **sc stop** command:

sc stop tapisrv

sc pause

Sends a PAUSE control request to a service.

Syntax

sc [*ServerName*] **pause** [*ServiceName*]

Parameters

ServerName

Specifies the name of the remote server on which the service is located. The name must use the UNC format ("\\myserver"). To run SC.exe locally, ignore this parameter.

ServiceName

Specifies the service name returned by the **getkeyname** operation.

/?

Displays help at the command prompt.

Remarks

- Use the **pause** operation to pause a service before shutting it down.
- Not all services can be paused.
- Not all services perform the same when paused. Some continue to service existing clients, but refuse to accept new clients. Others cease to service existing clients and also refuse to accept new ones.

Examples

The following example shows how you can use the **sc pause** command:

sc pause tapisrv

sc continue

Sends a CONTINUE control request to a service in order to resume a paused service.

Syntax

sc [*ServerName*] **continue** [*ServiceName*]

Parameters

ServerName

Specifies the name of the remote server on which the service is located. The name must use the UNC format ("\\myserver"). To run SC.exe locally, ignore this parameter.

ServiceName

Specifies the service name returned by the **getkeyname** operation.

/?

Displays help at the command prompt.

Remarks

- Use the **continue** operation to resume a paused service.

Examples

The following example shows how you can use the **sc continue** command:

sc continue tapisrv

sc config

Modifies the value of a service's entries in the registry and in the Service Control Manager's database.

Syntax

sc [*ServerName*] **config** [*ServiceName*] [**type=** {**own**|**share**|**kernel**|**filesys**|**rec**|**adapt**|**interact type=** {**own**|**share**}}] [**start=** {**boot**|**system**|**auto**|**demand**|**disabled**}] [**error=** {**normal**|**severe**|**critical**|**ignore**}] [**binpath=** *BinaryPathName*] [**group=** *LoadOrderGroup*] [**tag=** {**yes**|**no**}] [**depend=** *dependencies*] [**obj=** {*AccountName*|*ObjectName*}] [**displayname=** *DisplayName*] [**password=** *Password*]

Parameters

ServerName

Specifies the name of the remote server on which the service is located. The name must use the Universal Naming Convention (UNC) format ("\\myserver"). To run SC.exe locally, ignore this parameter.

ServiceName

Specifies the service name returned by the **getkeyname** operation.

type= {**own**|**share**|**kernel**|**filesys**|**rec**|**adapt**|**interact type=** {**own**|**share**}}

Specifies the service type.

Value	Description
Own	The service runs in its own process. It does not share an executable file with other services. This is the default.
Share	The service runs as a shared process. It shares an executable file with other services.
kernel	Driver.
Filesys	File system driver.
Rec	File system-recognized driver (identifies file systems used on the computer).
Adapt	Adapter driver (identifies hardware items such as keyboard, mouse, and disk drive).
interact	The service can interact with the desktop, receiving input from users. Interactive services must be run under the LocalSystem account. This type must be used in conjunction with **type= own** or **type= shared** (for example, **type= interact type= own**). Using **type= interact** by itself will generate an invalid parameter error.

start= {**boot**|**system**|**auto**|**demand**|**disabled**} Specifies the start type for the service.

Value	Description
Boot	A device driver that is loaded by the boot loader.
system	A device driver that is started during kernel initialization.

Auto	A service that automatically starts each time the computer is restarted and runs even if no one logs on to the computer.
demand	A service that must be manually started. This is the default value if **start=** is not specified.
disabled	A service that cannot be started. To start a disabled service, change the start type to some other value.

error= {**normal**\|**severe**\|**critical**\|**ignore**} Specifies the severity of the error if the service fails to start during boot.

Value	**Description**
normal	The error is logged and a message box is displayed informing the user that a service has failed to start. Startup will continue. This is the default setting.
severe	The error is logged (if possible). The computer attempts to restart with the last-known-good configuration. This could result in the computer being able to restart, but the service may still be unable to run.
critical	The error is logged (if possible). The computer attempts to restart with the last-known-good configuration. If the last-known-good configuration fails, startup also fails, and the boot process halts with a Stop error.
Ignore	The error is logged and startup continues. No notification is given to the user beyond recording the error in the Event Log.

binpath= *BinaryPathName* :Specifies a path to the service binary file.

group= *LoadOrderGroup* :Specifies the name of the group of which this service is a member. The list of groups is stored in the registry in the HKLM\System\CurrentControlSet\Control\ServiceGroupOrder subkey. The default is null.

tag= {**yes**|**no**}

Specifies whether or not to obtain a TagID from the CreateService call. Tags are only used for boot-start and system-start drivers.

depend= *dependencies*

Specifies the names of services or groups which must start before this service. The names are separated by forward slashes (/).

obj= {*AccountName*|*ObjectName*} :Specifies a name of an account in which a service will run, or specifies a name of the Windows driver object in which the driver will run. The default is **LocalSystem**.

displayname= *DisplayName* :Specifies a friendly, meaningful name that can be used in user-interface programs to identify the service to users. For example, the subkey name of one service is wuauserv, which is not be helpful to the user, and the display name is Automatic Updates.

password= ***Password*** **:**Specifies a password. This is required if an account other than the LocalSystem account is used.

/? : Displays help at the command prompt.

Remarks

- Without a space between a parameter and its value (for example, **type= own**, not **type=own**), the operation will fail.

Examples

The following example shows how you can use the **sc config** command:

```
sc config NewService binpath= "ntsd -d c:\windows\system32\NewServ.exe"
```

sc failure

Specifies what action to take upon failure of the service.

Syntax

sc [*ServerName*] **failure** [*ServiceName*] [**reset=** *ErrorFreePeriod*] [**reboot=** *BroadcastMessage*] [**command=** *CommandLine*] [**actions=** *FailureActionsAndDelayTime*]

Parameters

ServerName

Specifies the name of the remote server on which the service is located. The name must use the UNC format ("\\myserver"). To run SC.exe locally, ignore this parameter.

ServiceName

Specifies the service name returned by the **getkeyname** operation.

reset= *ErrorFreePeriod*

Specifies the length of the period (in seconds) with no failures after which the failure count should be reset to 0. This parameter must be used in conjunction with the **actions=** parameter.

reboot= *BroadcastMessage*

Specifies the message to be broadcast upon failure of the service.

command= *CommandLine*

Specifies the command line to be run upon failure of the service. For more information about how to run a batch or VBS file upon failure, see Remarks.

actions= *FailureActionsAndDelayTime*

Specifies the failure actions and their delay time (in milliseconds) separated by the forward slash (/). The following actions are valid: **run**, **restart**, and **reboot**. This parameter must be used in conjunction with the **reset=** parameter. Use **actions= ""** to take no action upon failure.

/?

Displays help at the command prompt.

Remarks

- Not all services allow changes to their failure options. Some run as part of a service set.

- To run a batch file upon failure, specify *cmd***.exe** *Drive***:\***FileName***.bat** to the **command=** parameter, where *Drive***:\***FileName***.bat** is the fully qualified name of the batch file.
- To run a VBS file upon failure, specify *cscript drive***:\***myscript***.vbs** to the **command=** parameter, where *drive***:\***myscript***.vbs** is the fully qualified name of the script file.
- It is possible to specify three different actions to the **actions=** parameter, which will be used the first, second, and third time a service fails.
- Without a space between a parameter and its value (that is, **type= own**, not **type=own**), the operation will fail.

Examples

The following examples show how you can use the sc failure command:

```
sc failure msftpsvc reset= 30 actions= restart/5000
sc failure dfs reset= 60 command= c:\windows\services\restart_dfs.exe actions= run/5000
sc failure dfs reset= 60 actions= reboot/30000
sc failure dfs reset= 60 reboot= "The Distributed File System service has failed. Because
of this, the computer will reboot in 30 seconds." actions= reboot/30000
sc failure myservice reset= 3600 reboot= "MyService crashed -- rebooting machine"
command= "%windir%\MyServiceRecovery.exe" actions=
restart/5000/run/10000/reboot/60000
```

sc description

Sets the description string for a service.

Syntax

sc [*ServerName*] **description** [*ServiceName*] [*Description*]

Parameters

ServerName

Specifies the name of the remote server on which the service is located. The name must use the UNC format ("\\\\myserver"). To run SC.exe locally, ignore this parameter.

ServiceName

Specifies the service name returned by the **getkeyname** operation.

Description

Specifies a description for the specified service. If no string is specified, the description of the service is not modified. There is no limit to the number of characters that can be contained in the service description.

/?

Displays help at the command prompt.

Examples

The following example shows how you can use the **sc description** command:

```
sc description newserv "Runs quality of service control."
```

sc delete

Deletes a service subkey from the registry. If the service is running or if another process has an open handle to the service, then the service is marked for deletion.

Syntax

sc [*ServerName*] **delete** [*ServiceName*]

Parameters

ServerName

Specifies the name of the remote server on which the service is located. The name must use the UNC format ("\\myserver"). To run SC.exe locally, ignore this parameter.

ServiceName

Specifies the service name returned by the **getkeyname** operation.

/?

Displays help at the command prompt.

Remarks

- Use Add or Remove Programs to delete DHCP, DNS, or any other built-in operating system services. Add or Remove Programs will not only remove the registry subkey for the service, but it will also uninstall the service and delete any shortcuts to the service.

Examples

The following example shows how you can use the **sc delete** command:

sc delete newserv

sc getdisplayname

Gets the display name associated with a particular service.

Syntax

sc [*ServerName*] **getdisplayname** [*ServiceName*] [*BufferSize*]

Parameters

ServerName

Specifies the name of the remote server on which the service is located. The name must use the UNC format ("\\myserver"). To run SC.exe locally, ignore this parameter.

ServiceName

Specifies the service name returned by the **getkeyname** operation.

BufferSize

Specifies the size (in bytes) of the buffer. The default is 1024 bytes.

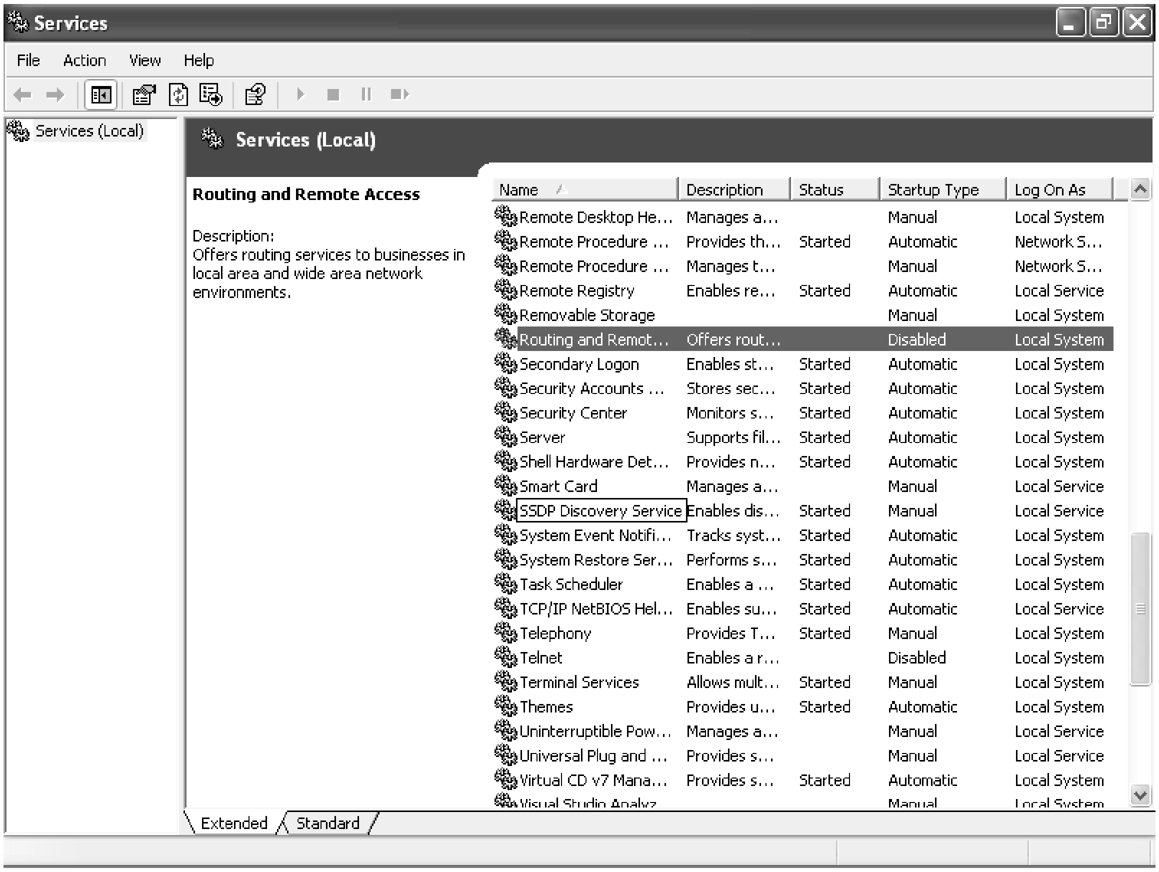
/?

Displays help at the command prompt.

Examples

The following examples show how you can use the **sc getdisplayname** command:

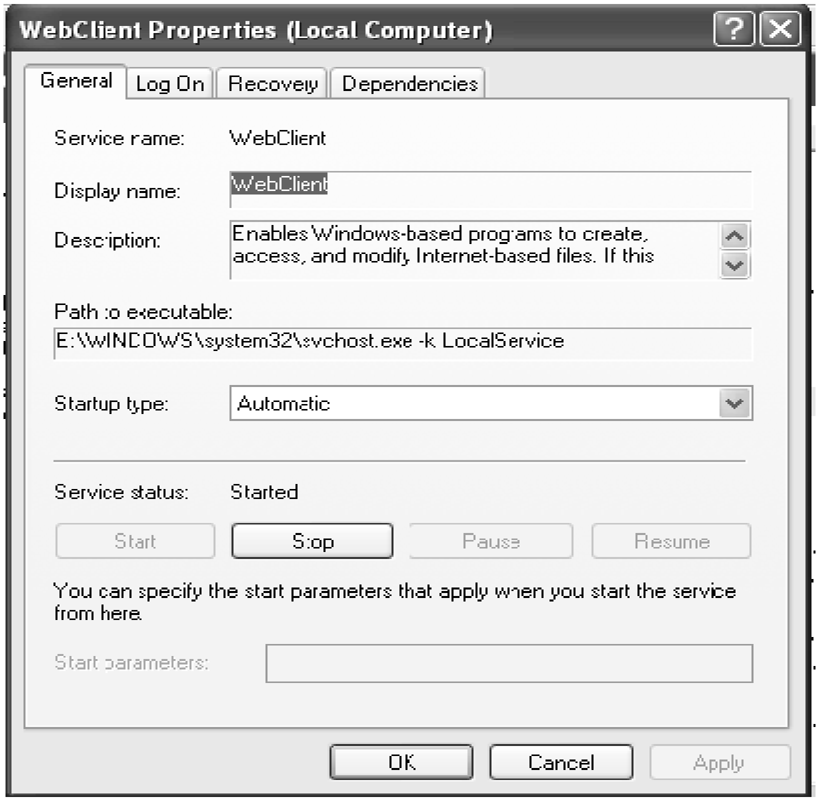
```
sc getdisplayname clipsrv
sc getdisplayname tapisrv
sc getdisplayname sharedaccess
```



Routing and Remote Access

Description:
Offers routing services to businesses in local area and wide area network environments.

Name	Description	Status	Startup Type	Log On As
Remote Desktop He…	Manages a…		Manual	Local System
Remote Procedure …	Provides th…	Started	Automatic	Network S…
Remote Procedure …	Manages t…		Manual	Network S…
Remote Registry	Enables re…	Started	Automatic	Local Service
Removable Storage			Manual	Local System
Routing and Remot…	Offers rout…		Disabled	Local System
Secondary Logon	Enables st…	Started	Automatic	Local System
Security Accounts …	Stores sec…	Started	Automatic	Local System
Security Center	Monitors s…	Started	Automatic	Local System
Server	Supports fil…	Started	Automatic	Local System
Shell Hardware Det…	Provides n…	Started	Automatic	Local System
Smart Card	Manages a…		Manual	Local Service
SSDP Discovery Service	Enables dis…	Started	Manual	Local Service
System Event Notifi…	Tracks syst…	Started	Automatic	Local System
System Restore Ser…	Performs s…	Started	Automatic	Local System
Task Scheduler	Enables a …	Started	Automatic	Local System
TCP/IP NetBIOS Hel…	Enables su…	Started	Automatic	Local Service
Telephony	Provides T…	Started	Manual	Local System
Telnet	Enables a r…		Disabled	Local System
Terminal Services	Allows mult…	Started	Manual	Local System
Themes	Provides u…	Started	Automatic	Local System
Uninterruptible Pow…	Manages a…		Manual	Local Service
Universal Plug and …	Provides s…		Manual	Local Service
Virtual CD v7 Mana…	Provides s…	Started	Automatic	Local System
Visual Studio Analyz			Manual	Local System



WebClient Properties (Local Computer)

Service name: WebClient

Display name: WebClient

Description: Enables Windows-based programs to create, access, and modify Internet-based files. If this

Path to executable:
E:\WINDOWS\system32\svchost.exe -k LocalService

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

Start parameters:

```
C:\>sc/?
*** Unrecognized Command ***
DESCRIPTION:
        SC is a command line program used for communicating with the
        NT Service Controller and services.
USAGE:
        sc <server> [command] [service name] <option1> <option2>...

        The option <server> has the form "\\ServerName"
        Further help on commands can be obtained by typing: "sc
[command]"
        Commands:
          query-----------Queries the status for a service, or
                          enumerates the status for types of services.
          queryex---------Queries the extended status for a service, or
                          enumerates the status for types of services.
          start-----------Starts a service.
          pause-----------Sends a PAUSE control request to a service.
          interrogate-----Sends an INTERROGATE control request to a
service.
          continue--------Sends a CONTINUE control request to a
service.
          stop------------Sends a STOP request to a service.
          config----------Changes the configuration of a service
persistant).
          description-----Changes the description of a service.
          failure---------Changes the actions taken by a service upon
failure
          qc--------------Queries the configuration information for a
service
          qdescription----Queries the description for a service.
          qfailure--------Queries the actions taken by a service upon
failure
          delete----------Deletes a service (from the registry).
          create----------Creates a service. (adds it to the registry).
          control---------Sends a control to a service.
          sdshow----------Displays a service's security descriptor.
          sdset-----------Sets a service's security descriptor.
          GetDisplayName--Gets the DisplayName for a service.
          GetKeyName------Gets the ServiceKeyName for a service.
          EnumDepend------Enumerates Service Dependencies.

        The following commands don't require a service name:
        sc <server> <command> <option>
          boot------------(ok | bad) Indicates whether the last boot
should
                          be saved as the last-known-good boot
configuration
          Lock------------Locks the Service Database
          QueryLock-------Queries the LockStatus for the SCManager
Database
EXAMPLE:
        sc start MyService

Would you like to see help for the QUERY and QUERYEX commands? [ y | n
]: y
```

```
QUERY and QUERYEX OPTIONS :
        If the query command is followed by a service name, the status
        for that service is returned.  Further options do not apply in
        this case.  If the query command is followed by nothing or one
of
        the options listed below, the services are enumerated.
    type=    Type of services to enumerate (driver, service, all)
             (default = service)
    state=   State of services to enumerate (inactive, all)
             (default = active)
    bufsize= The size (in bytes) of the enumeration buffer
             (default = 4096)
    ri=      The resume index number at which to begin the enumeration
             (default = 0)
    group=   Service group to enumerate
             (default = all groups)

SYNTAX EXAMPLES
sc query                - Enumerates status for active services &
drivers
sc query messenger      - Displays status for the messenger service
sc queryex messenger    - Displays extended status for the messenger
service
sc query type= driver   - Enumerates only active drivers
sc query type= service  - Enumerates only Win32 services
sc query state= all     - Enumerates all services & drivers
sc query bufsize= 50    - Enumerates with a 50 byte buffer.
sc query ri= 14         - Enumerates with resume index = 14
sc queryex group= ""    - Enumerates active services not in a group
sc query type= service type= interact - Enumerates all interactive
services
sc query type= driver group= NDIS     - Enumerates all NDIS drivers
```

Practical 5.

LAN – Setting up and configuration

In the modern office environment, each worker is equipped with a personal computer, containing its own disk drives and processor. Each of these computers can communicate with another by the way of a local area network (LAN), which is a computer network that covers a small area, usually a single building or group of buildings. In addition, the LAN may also connect the network of computers with a series of printers, a mainframe computer or file server with even greater processing power and memory storage, and with other devices that can send messages from the network over telephone lines to another location.

As the name suggests, a LAN is local, meaning that it is a proprietary system limited to a finite number of users. It generally serves an area of less than one mile. It is also a network, affording users both functional and communicative diversity through a distribution of resources. A LAN permits workers—isolated in separate offices—to operate off the same system, as if they were all sitting around a single computer.

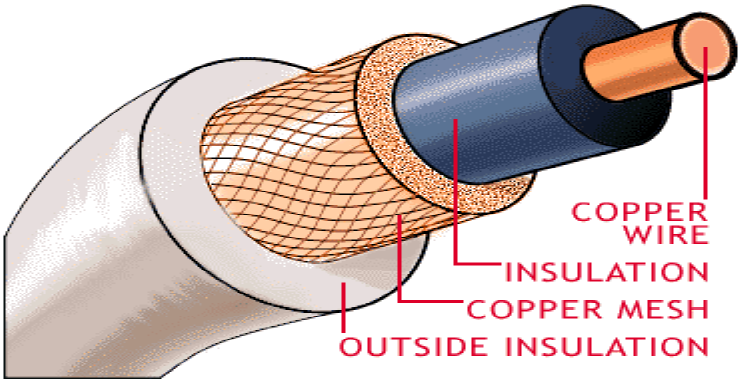
One of the great attributes of a LAN is that it may be installed simply, upgraded or expanded with little difficulty, and moved or rearranged without disruption. LANs are also useful because they can transmit data quickly. Perhaps most importantly, anyone familiar with the use of a personal computer can be trained to communicate or perform work over a LAN. But despite their great potential and capabilities, LANs have yet to demonstrate an increase in office productivity. They have certainly eliminated paper and speeded the flow of information, but in many cases they have also created additional work in terms of organization, maintenance, and trouble-shooting.

local area network (LAN), a computer network dedicated to sharing data among several single-user workstations or personal computers, each of which is called a node. A LAN can have from two to several hundred such nodes, each separated by distances of several feet to as much as a mile, and should be distinguished from connections among computers over public carriers, such as telephone circuits, that are used for other purposes. Because of the relatively small areas involved, the nodes in a LAN can be connected by special high-data-rate cables. A metropolitan area network (MAN) is defined as being restricted to a larger area (maximum distances of 50–60 miles) than a LAN but one still small enough so that dedicated links (such as microwave links) can be used.

Physical Components of Lans

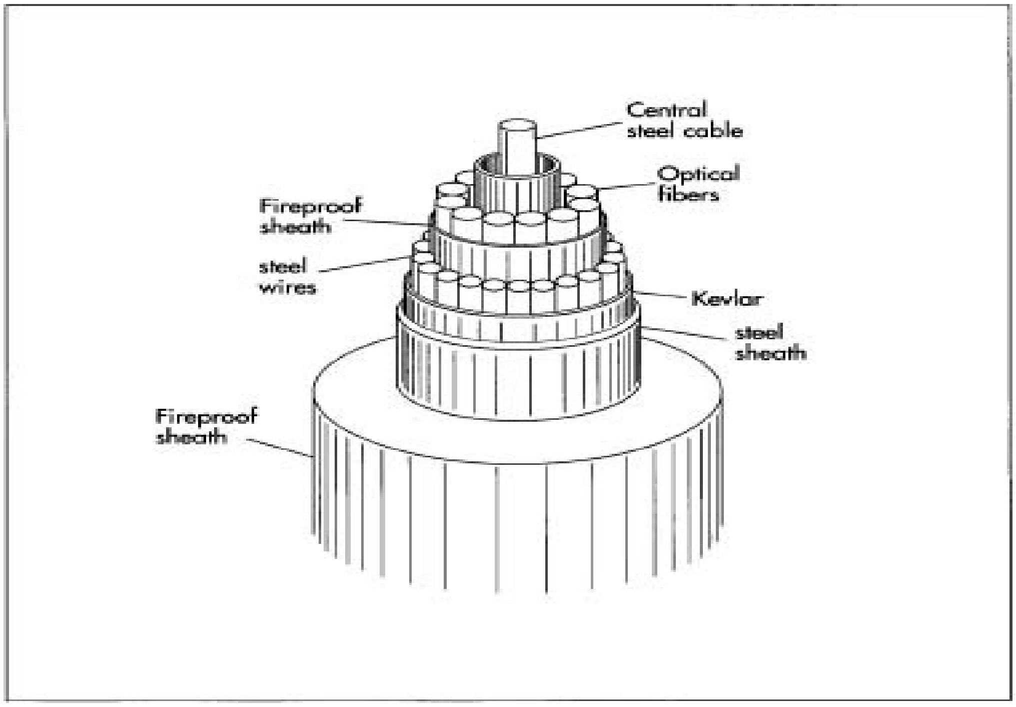
The physical properties of a LAN include network access units (or interfaces) that connect the personal computer to the network. These units are actually interface cards installed on computer motherboards. Their job is to provide a connection, monitor availability of access to the LAN, set or buffer the data transmission speed, ensure against transmission errors and collisions, and assemble data from the LAN into usable form for the computer.

The next part of a LAN is the wiring, which provides the physical connection from one computer to another, and to printers and file servers. The properties of the wiring determine transmission speeds. The first LANs were connected with coaxial cable, the same type used to deliver cable television. These facilities are relatively inexpensive and simple to attach. More importantly, they provided great bandwidth (the system's rate of data transfer), enabling transmission speeds initially up to 20 megabits per second.



Another type of wiring, developed in the 1980s, used ordinary twisted wire pair (commonly used for telephones). The primary advantages of twisted wire pair are that it is very cheap, simpler to splice than coaxial, and is already installed in many buildings. The downside of this simplicity is that its bandwidth is more limited.

A more recent development in LAN wiring is optical fiber cable. This type of wiring uses thin strands of glass to transmit pulses of light between terminals. It provides tremendous bandwidth, allowing very high transmission speeds and because it is optical rather than electronic, it is impervious to electromagnetic interference. Still, splicing it can be difficult and requires a high degree of skill. The primary application of fiber is not between terminals, but between LAN buses (terminals) located on different floors. As a result, fiber distributed data interface is used mainly in building risers. Within individual floors, LAN facilities remain coaxial or twisted wire pair.



When a physical connection cannot be made between two LANs, such as across a street or between buildings, microwave radio may be used. However, it is often difficult to secure frequencies for this medium. Another alternative in this application is light transceivers, which project a beam of light similar to fiber optic cable, but through the air rather than over cable. These systems do not have the frequency allocation or radiation problems associated with microwave, but they are susceptible to interference from fog and other natural obstructions.

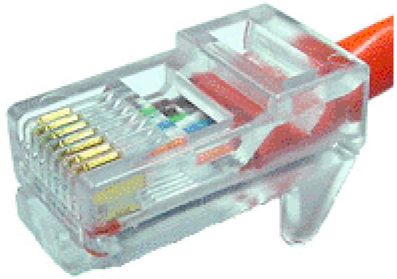
Lan Topologies

LANs are designed in several different topologies, or physical patterns, connecting terminals. These shapes can range from straight lines to a ring. Each terminal on the LAN contends with other terminals for access to the system. When it has secured access to the system, it broadcasts its message to all the terminals at once. The message is picked up by the one or group of terminal stations for which it is intended. The branching tree topology is an extension of the bus, providing a link between two or more buses.

A third topology, the star network, also works like a bus in terms of contention and broadcast. But in the star, stations are connected to a single, central node (individual computer) that administers access. Several of these nodes may be connected to one another. For example, a bus serving six stations may be connected to another bus serving 10 stations and a third bus connecting 12 stations. The star topology is most often used where the connecting facilities are coaxial or twisted wire pair.

The ring topology connects each station to its own node, and these nodes are connected in a circular fashion. Node 1 is connected to node 2, which is connected to node 3, and so on, and the final node is connected back to node 1. Messages sent over the LAN are regenerated by each node, but retained only by the addressees. Eventually, the message circulates back to the sending node, which removes it from the stream.

Registered **J**ack-**45**) A telephone connector that holds up to eight wires. RJ-45 plugs and sockets are used in Ethernet and Token Ring Type 3 devices.



A cross cable connects two PC’s on a network, whereas a straight cable connects switches and hubs.
The RJ 45 connector has color codings:
1st end: white-orange, orange, white-blue, blue, white-green, green, white-brown, brown.
2nd end: white-blue, green, white-orange, blue, white-green, orange, white-brown, brown.

Cabling may be done in two ways:

- Structured
- Unstructured

In Structured Cabling clipping in the RJ 45 is not needed, as the IO has color code specified. The basic requirements of structured cabling are a IO patch code, switches, hubs, RJ45 connector, cables, Patch Max and patch code.

In Unstructured Cabling the basic requirements are switches, hubs, RJ45 connectors and cables.

Procedure for LAN settings

1. Right click on the my computer icon on the desktop
2. select properties
3. click on the hardware tab
4. select Device manager
5. select the network adapter

Practical 6.

USE OF THE PERFORMANCE MONITOR

Performance Monitor/System Monitor
System Monitor is used to measure the performance of your own computer or other computers on a network.System Monitor supports detailed monitoring of utilization of OS resources.

System Monitor overview

System Monitor is used to do the following:

- Collect and view real-time performance data on a local computer or from several remote computers.
- View data collected either currently or previously in a counter log.
- Present data in a printable graph, histogram, or report view.
- Incorporate System Monitor functionality into applications that support ActiveX controls, such as Web pages, and Microsoft Word and other applications in the Microsoft Office suite.
- Create HTML pages from performance views.
- Create reusable monitoring configurations that can be installed on other computers using Microsoft Management Console.

With System Monitor, you can collect and view extensive data about the usage of hardware resources and the activity of system services on computers you administer. You can define the data you want the graph to collect in the following ways:

- **Type of data.** To select the data to be collected, you can specify performance objects, performance counters, and object instances.

  Performance object
  In System Monitor, a logical collection of counters that is associated with a resource or service that can be monitored. Performance objects are build into the OS and major hardware component like memory, processor, cache, physical disk.

  Performance counter
  In System Monitor, a data item that is associated with a performance object. For each counter selected, System Monitor presents a value corresponding to a particular aspect of the performance that is defined for the performance object. Each performance object provide performance counter that represent data on specific aspect of system for example Performance Time, Page per second counter provided by memory paging object tracks the rate memory paging.

Performance Object Instance
In System monitor, a term used to distinguish between multiple performance objects of the same type on the computer.

Some objects provide data about system resources (such as memory). Others provide data about the operation of applications (for example, system services or Microsoft BackOffice applications running on your computer).

- Source of data
  System Monitor can collect data from your local computer or from other computers on the network where you have permission to do so. (By default, administrative permission is required.) In addition, you can include real-time data or data collected previously using counter logs.
- Sampling parameters
  System Monitor supports manual, on-demand sampling or automatic sampling based on a time interval you specify. When viewing logged data, you can also choose starting and stopping times so that you can view data spanning a specific time range.

In addition to options for defining data content, you have considerable flexibility in designing the appearance of your System Monitor views. You can choose from among the following options:

- **Type of display.** System Monitor supports graph, histogram, and report views. The graph view is the default view; it offers the widest variety of optional settings.
- **Display characteristics.** For any of the three views, you can define the colors and fonts for the display. In graph and histogram views, you can select from many different options when you view performance data. These options include the following:
  - Provide a title for your graph or histogram and label the vertical axis.
  - Set the range of values depicted in your graph or histogram.
  - Adjust the characteristics of lines or bars plotted to indicate counter values, including color, width, style, and so on.

More About Performance objects and counters

Windows XP obtains performance data from components in your computer. As a system component performs work on your system, it generates performance data. That data is described as a performance object and is typically named for the component generating the data. For example, the Processor object is a collection of performance data about processors on your system.

A range of performance objects are built into the operating system, typically corresponding to the major hardware components, such as memory, processors, and so on. Other programs might install their own performance objects. For example, services such as Windows Internet Name Service (WINS), or server programs such as Microsoft Exchange provide performance objects, and performance graphs and logs can monitor these objects.

Each performance object provides counters that represent data on specific aspects of a system or service. For example, the Pages/sec counter provided by the Memory object tracks the rate of memory paging.

Although your system might make many more objects available, the following list provides the default objects you will use most frequently to monitor system components:

- Cache
- Memory
- Objects
- Paging File
- PhysicalDisk
- Process
- Processor
- Server
- System
- Thread

To add counters to System Monitor

1. Open Performance from the administrative tools in the control panel.
2. Right-click the System Monitor details pane and click **Add Counters**.
   Or, click the button on the toolbar.
3. To monitor any computer on which the monitoring console is run, click **Use local computer counters**.
   Or, to monitor a specific computer, regardless of where the monitoring console is run, click **Select counters from computer** and specify a computer name (the name of the local computer is selected by default).
4. In **Performance object**, click an object to monitor. The Processor object is selected by default.
5. To monitor all counters, click **All counters**.
   Or, to monitor only selected counters, click **Select counters from list** and select the counters you want to monitor. The % Processor Time counter is selected by default.
6. To monitor all instances of the selected counters, click **All instances**.
   Or, to monitor only selected instances, click **Select instances from list** and select the instances you want to monitor. The _Total instance is selected by default.
7. Click **Add**.

Notes

- To open Performance, click **Start**, click **Control Panel**, click **Performance and Maintenance**, click **Administrative Tools**, and then double-click **Performance**.
- By default, the following three counters are displayed in System Monitor -- Memory\Pages/sec, Physical Disk (_Total)\Avg. Disk Queue Length, and Processor (_Total)\%Processor Time.
- If you select an object on a remote computer, you might notice a short delay as System Monitor refreshes the list to reflect objects present on that computer.
- When creating a monitoring console for export, be sure to select **Use local computer counters**. Otherwise, System Monitor will obtain data from the computer named in the text box, regardless of where the console file is installed.
- For a description of a particular counter, click the name of the counter in **Add counters**, and then click **Explain**.

Choosing which counters to use
The following topics can help you determine which counters you should select to monitor the usage of a specific resource or the activity of a particular service and to investigate related problems.

Finding memory bottlenecks
Use the following counters to identify bottlenecked memory resources:

- Memory\Available Bytes
- Memory\Pages/sec

Finding disk bottlenecks
Use the following counters to identify bottlenecked disk resources:

- PhysicalDisk\ % Disk Time and % Idle Time
- PhysicalDisk\ Disk Reads/sec and Disk Writes/sec
- PhysicalDisk\ Avg. Disk Queue Length
- LogicalDisk\ % Free Space

Monitor memory counters to determine whether excessive paging is putting a strain on the **disk.**

Finding processor bottlenecks
Use the following counters to identify bottlenecked processor resources:

- Processor\ Interrupts/sec
- Processor\ % Processor Time
- Process(*process*)\ % Processor Time
- System\ Processor Queue Length

Finding network bottlenecks
Use the following counters to identify bottlenecked network resources:

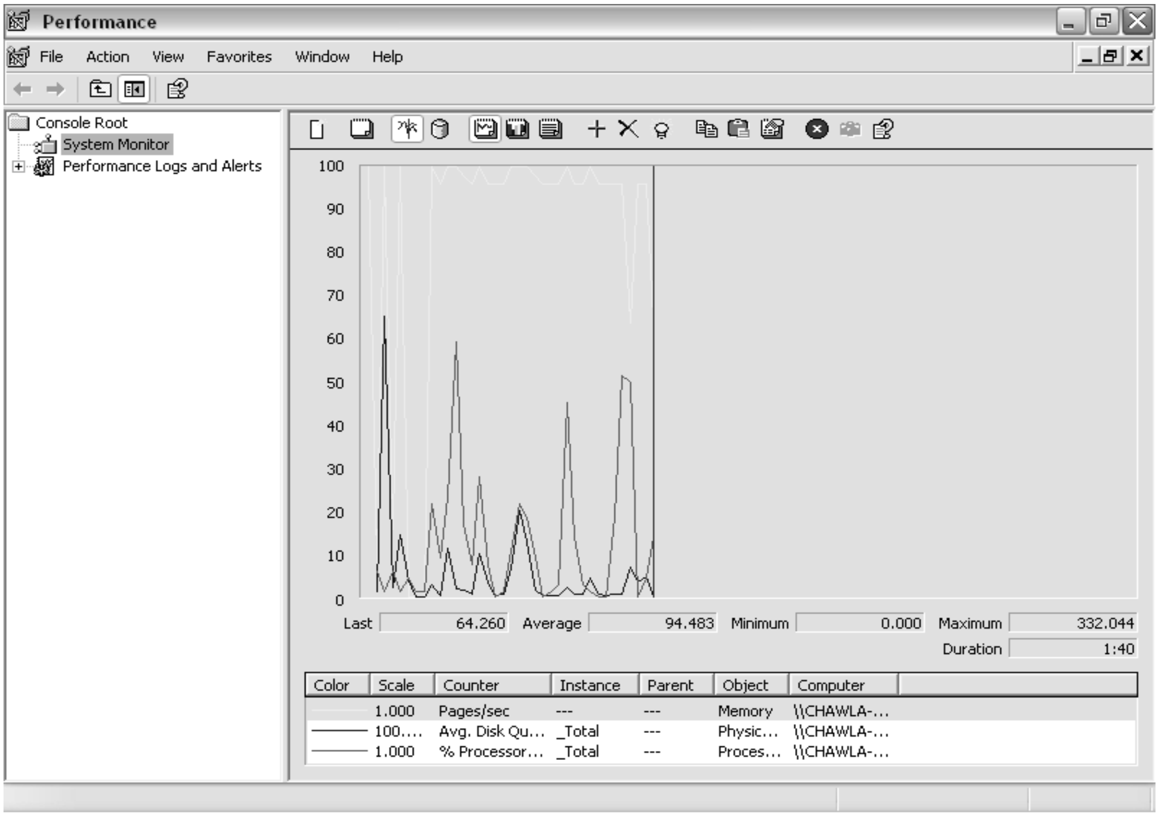
- Network Interface\ Bytes Total/sec, Bytes Sent/sec, and Bytes Received/sec

- *Protocol_layer_object*\ Segments Received/sec, Segments Sent/sec, Frames Sent/sec, and Frames Received/sec
  For NWLink performance objects, frame-related counters report only zeroes. Use datagram-based counters for these objects.
- Server\ Bytes Total/sec, Bytes Received/sec, and Bytes Sent/sec

Finding printer bottlenecks
Use the following counters to identify bottlenecked printer resources:

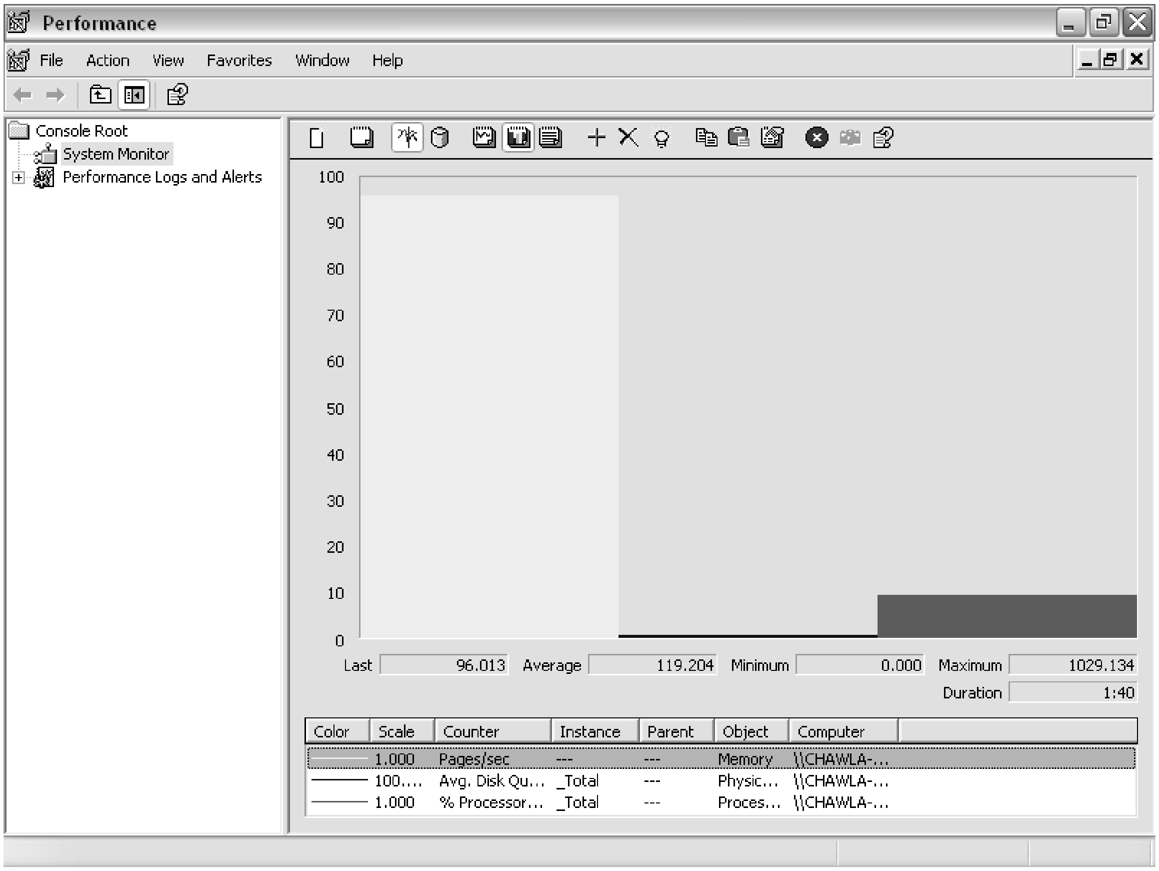
- Print Queue\ Bytes Printed/sec
- Print Queue\ Job Errors

Low values for Bytes Printed/sec can indicate a printer throughput problem. Note that this value varies based on the type of printer. Consult your printer documentation for acceptable values for printer throughput.
Job errors are typically caused by improper port configuration. Check your port configuration for invalid settings.



Last 64.260 Average 94.483 Minimum 0.000 Maximum 332.044
Duration 1:40

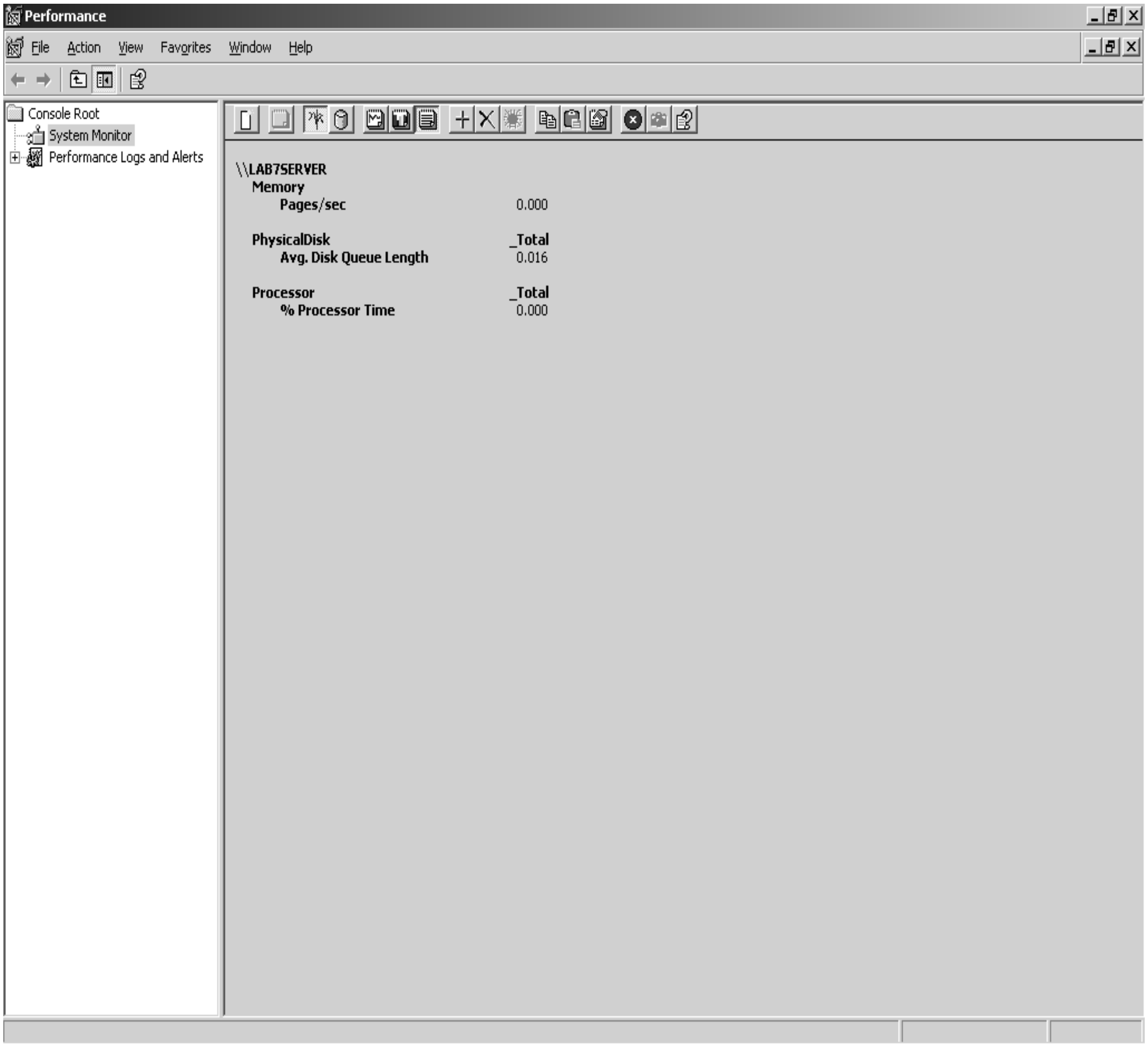
Color	Scale	Counter	Instance	Parent	Object	Computer
——	1.000	Pages/sec	---	---	Memory	\\CHAWLA-...
——	100....	Avg. Disk Qu...	_Total	---	Physic...	\\CHAWLA-...
——	1.000	% Processor...	_Total	---	Proces...	\\CHAWLA-...



Last 96.013 Average 119.204 Minimum 0.000 Maximum 1029.134

Duration 1:40

Color	Scale	Counter	Instance	Parent	Object	Computer
—	1.000	Pages/sec	---	---	Memory	\\CHAWLA-...
—	100....	Avg. Disk Qu...	_Total	---	Physic...	\\CHAWLA-...
—	1.000	% Processor...	_Total	---	Proces...	\\CHAWLA-...



```
\\LAB7SERVER
  Memory
      Pages/sec                      0.000

  PhysicalDisk                      _Total
      Avg. Disk Queue Length         0.016

  Processor                         _Total
      % Processor Time               0.000
```

Practical 7.

MANAGEMENT OF USERS & DOMAINS.

Local Users and Groups overview

Local Users and Groups is a tool you can use to manage local users and groups. It is available on the following operating systems:

- Windows 2000 Professional
- Windows XP Professional
- Member servers running Windows 2000 Server

A local user or group is an account that can be granted permissions and rights from your computer. Domain or global users and groups are managed by your network administrator. You can add local users, global users, and global groups to local groups. However, you cannot add local users and groups to global groups.

Local Users and Groups is an important security feature because you can limit the ability of users and groups to perform certain actions by assigning them rights and permissions. A right authorizes a user to perform certain actions on a computer, such as backing up files and folders or shutting down a computer. A permission is a rule associated with an object (usually a file, folder, or printer) and it regulates which users can have access to the object and in what manner.

Users overview

Users displays the two built-in user accounts, Administrator and Guest, as well as any user accounts you create. The built-in user accounts are created automatically when you install Windows 2000 or Windows XP.

Administrator account

The Administrator account is the one you use when you first set up a workstation or member server. You use this account before you create an account for yourself. The Administrator account is a member of the Administrators group on the workstation or member server.

The Administrator account can never be deleted, disabled, or removed from the Administrators local group, ensuring that you never lock yourself out of the computer by deleting or disabling all the administrative accounts. This feature sets the Administrator account apart from other members of the Administrators local group.

Guest account

The Guest account is used by people who do not have an actual account on the computer. A user whose account is disabled (but not deleted) can also use the Guest account. The Guest account does not require a password. The Guest account is disabled by default, but you can enable it.

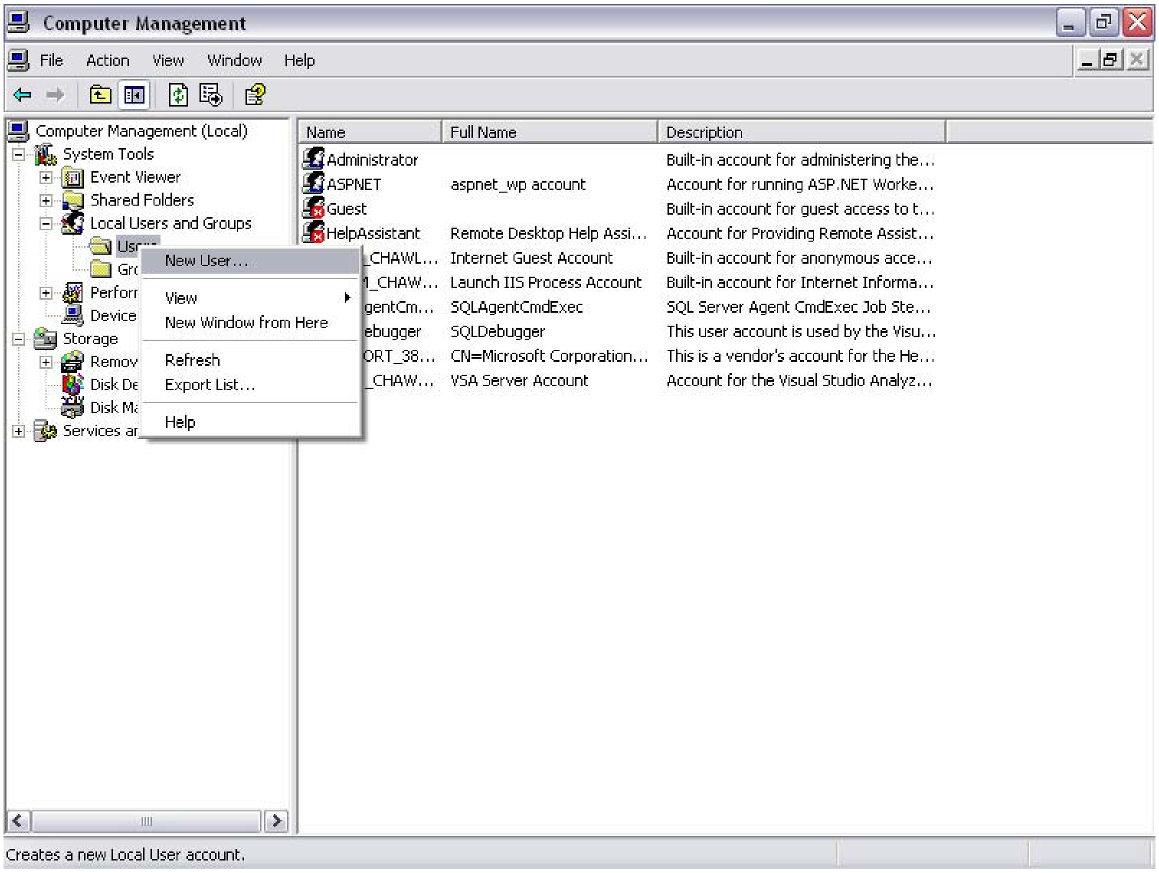
You can set rights and permissions for the Guest account just like any user account. By default, the Guest account is a member of the built-in Guests group, which allows a user to log on to a workstation or member server. Additional rights, as well as any permissions, must be granted to the Guests group by a member of the Administrators group.

Steps to create a new user account

1. Open Computer Management.
2. In the console tree, click **Users**.

   Where?

   - Computer Management
     - System Tools
       - Local Users and Groups
         - Users

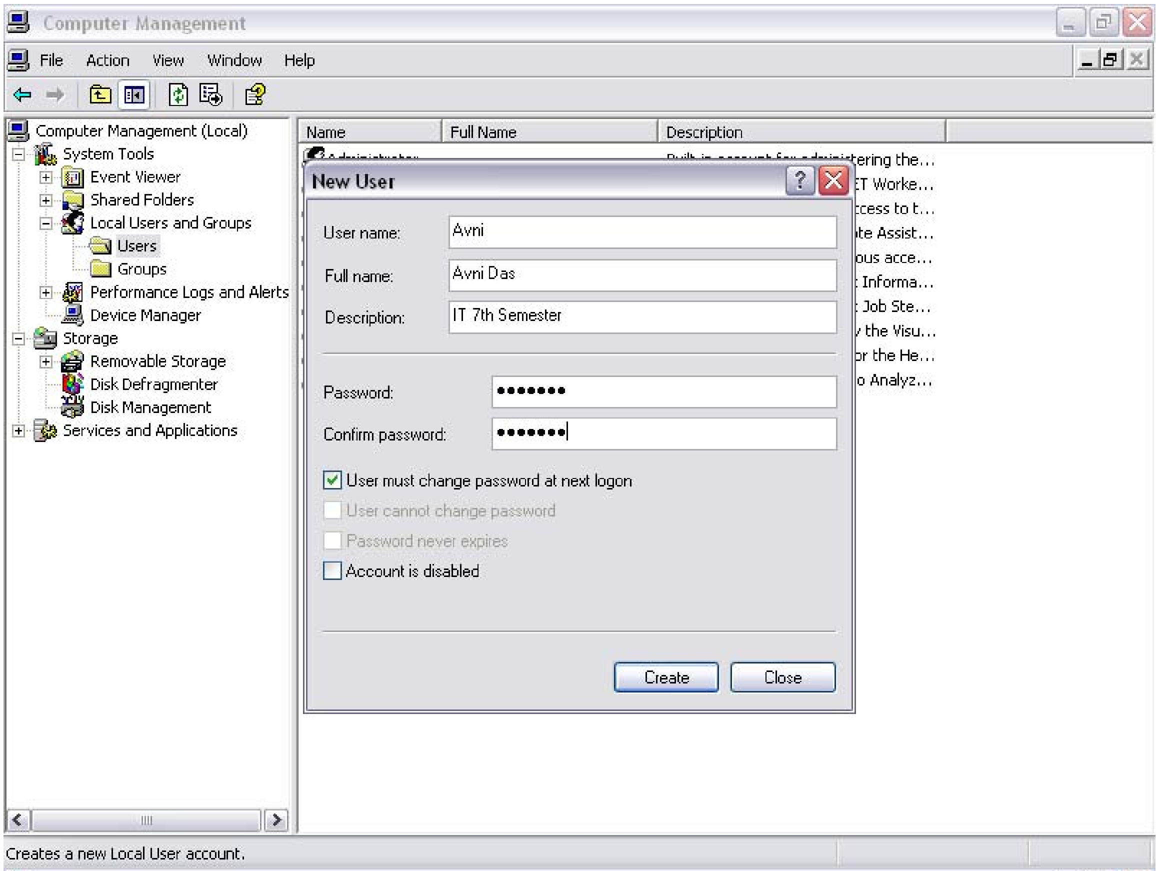


Name	Full Name	Description
Administrator		Built-in account for administering the…
ASPNET	aspnet_wp account	Account for running ASP.NET Worke…
Guest		Built-in account for guest access to t…
HelpAssistant	Remote Desktop Help Assi…	Account for Providing Remote Assist…
_CHAWL…	Internet Guest Account	Built-in account for anonymous acce…
_CHAW…	Launch IIS Process Account	Built-in account for Internet Informa…
gentCm…	SQLAgentCmdExec	SQL Server Agent CmdExec Job Ste…
ebugger	SQLDebugger	This user account is used by the Visu…
ORT_38…	CN=Microsoft Corporation,…	This is a vendor's account for the He…
_CHAW…	VSA Server Account	Account for the Visual Studio Analyz…

Creates a new Local User account.

3. On the Action menu, click New User.

4. Type the appropriate information in the dialog box.
5. Select or clear the check boxes for:
   - **User must change password at next logon**
   - **User cannot change password**
   - **Password never expires**
   - **Account is disabled**
6. Click **Create**, and then click **Close**.
7. This will create a user named **Avni**.



New User

User name: Avni

Full name: Avni Das

Description: IT 7th Semester

Password: •••••••

Confirm password: •••••••

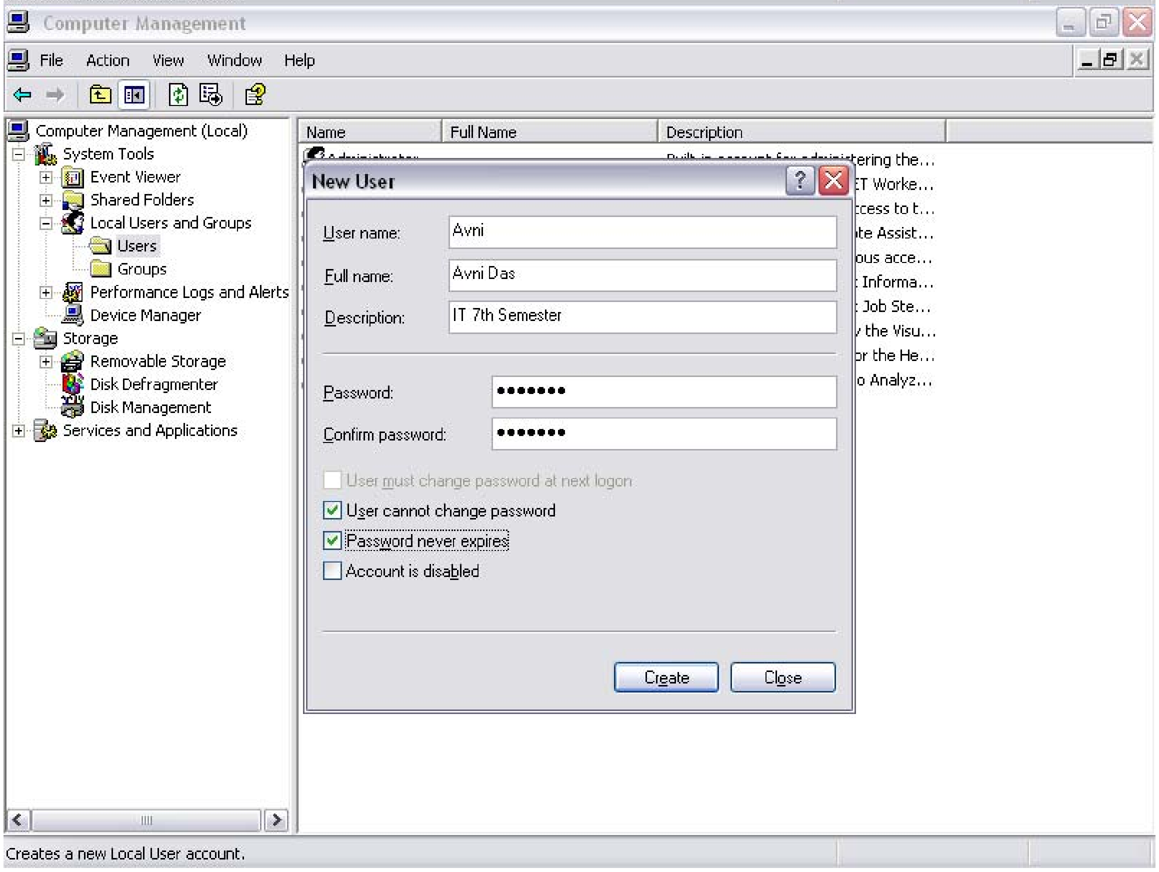
☑ User must change password at next logon

□ User cannot change password

□ Password never expires

□ Account is disabled

Creates a new Local User account.



New User

User name: Avni

Full name: Avni Das

Description: IT 7th Semester

Password: •••••••

Confirm password: •••••••

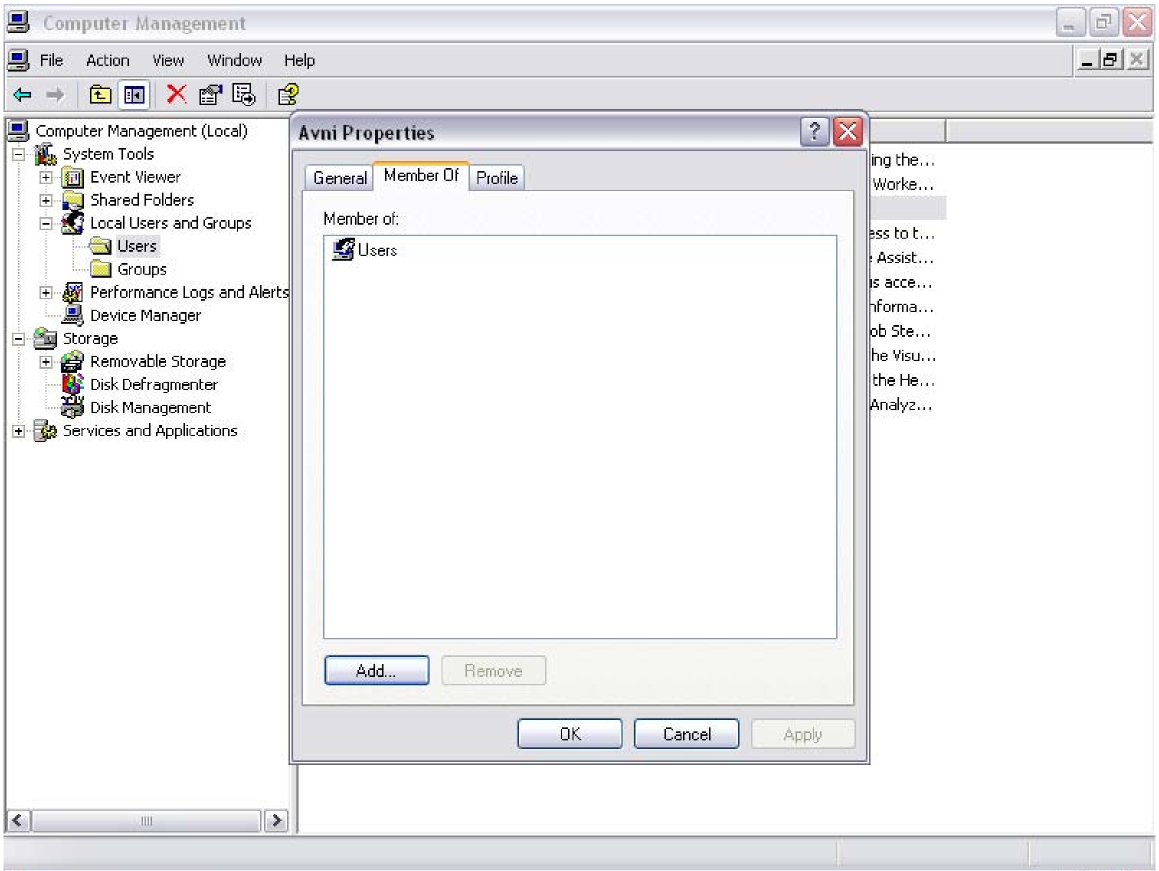
□ User must change password at next logon

☑ User cannot change password

☑ Password never expires

□ Account is disabled

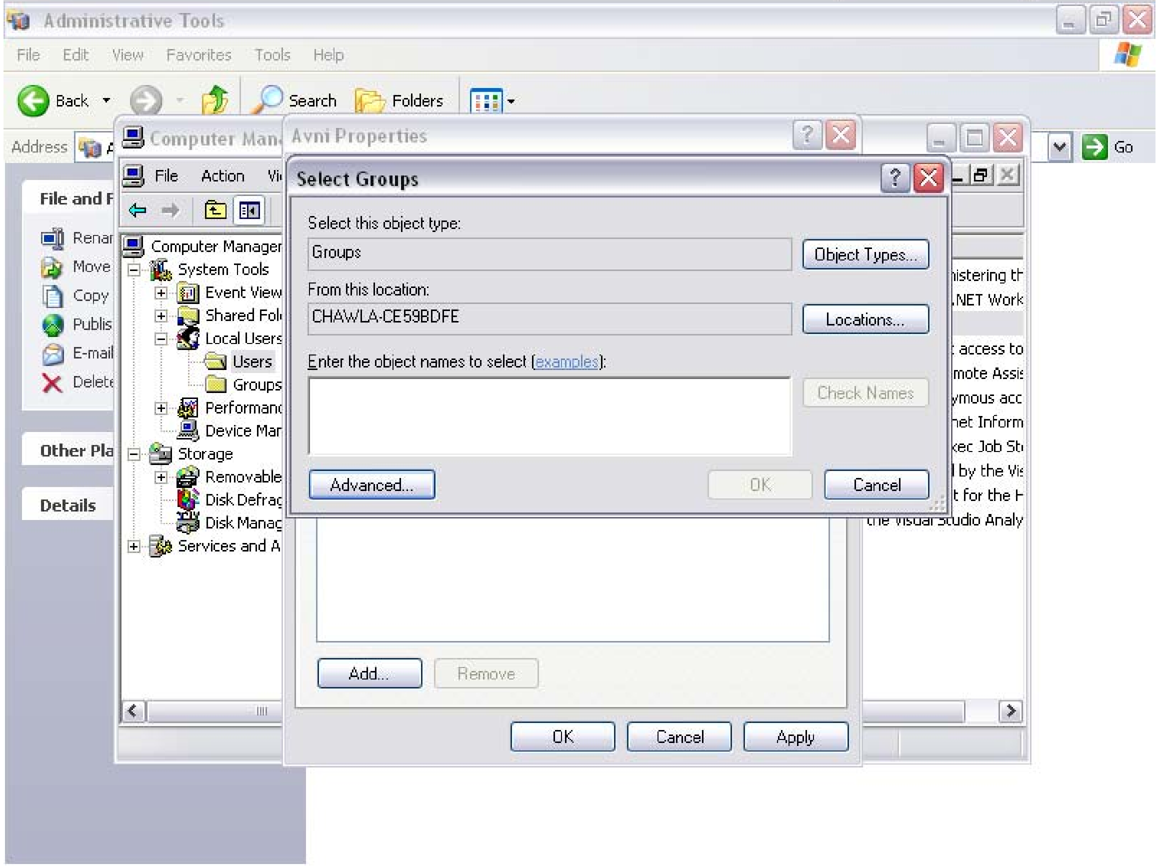
Creates a new Local User account.



Avni Properties

Member of:

Users

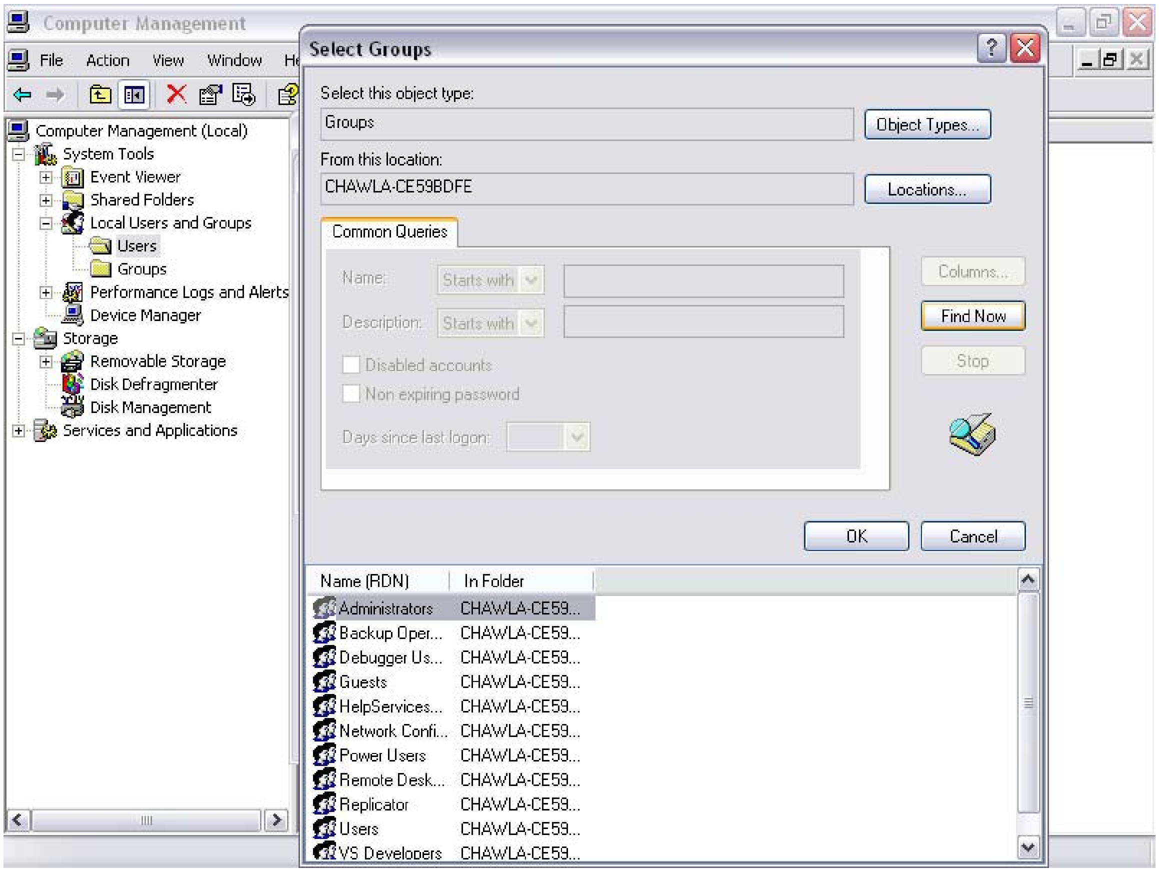


Select Groups

Select this object type:
Groups

From this location:
CHAWLA-CE59BDFE

Enter the object names to select (examples):



Select this object type:
Groups

From this location:
CHAWLA-CE59BDFE

Name: Starts with

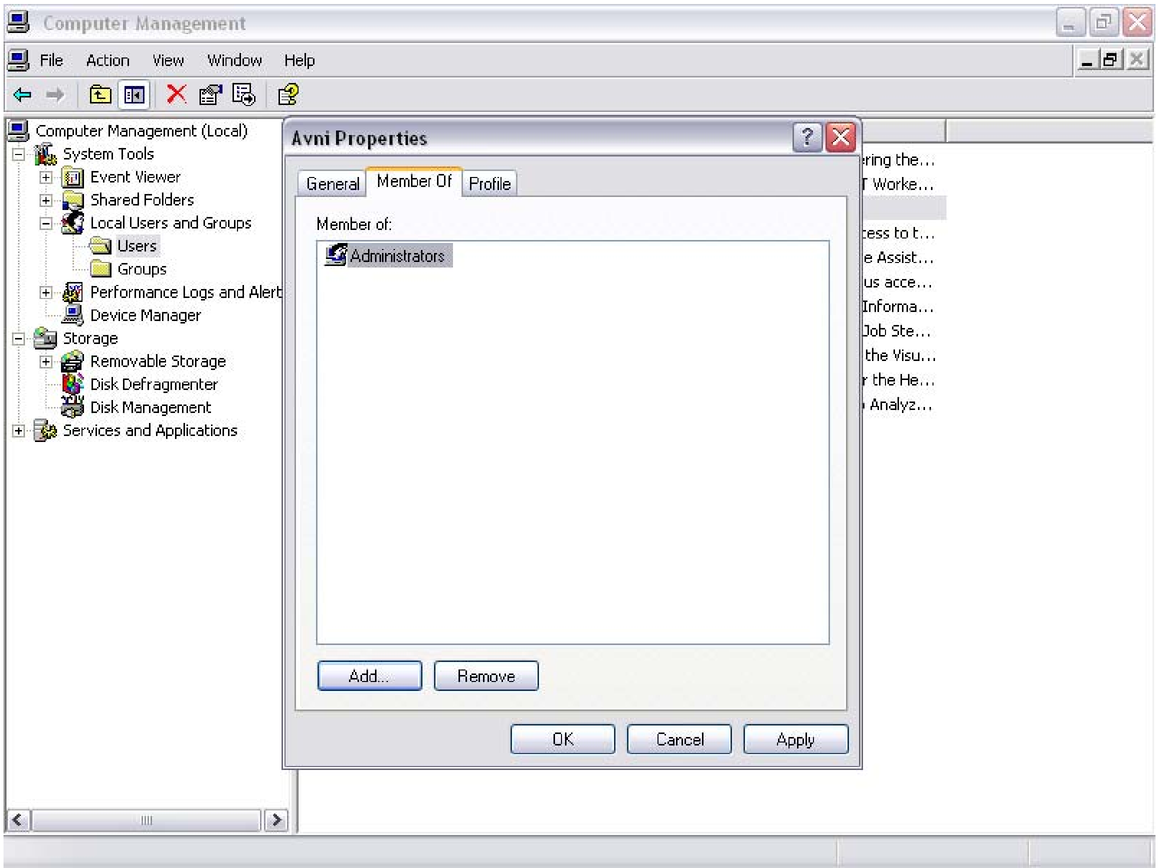
Description: Starts with

□ Disabled accounts

□ Non expiring password

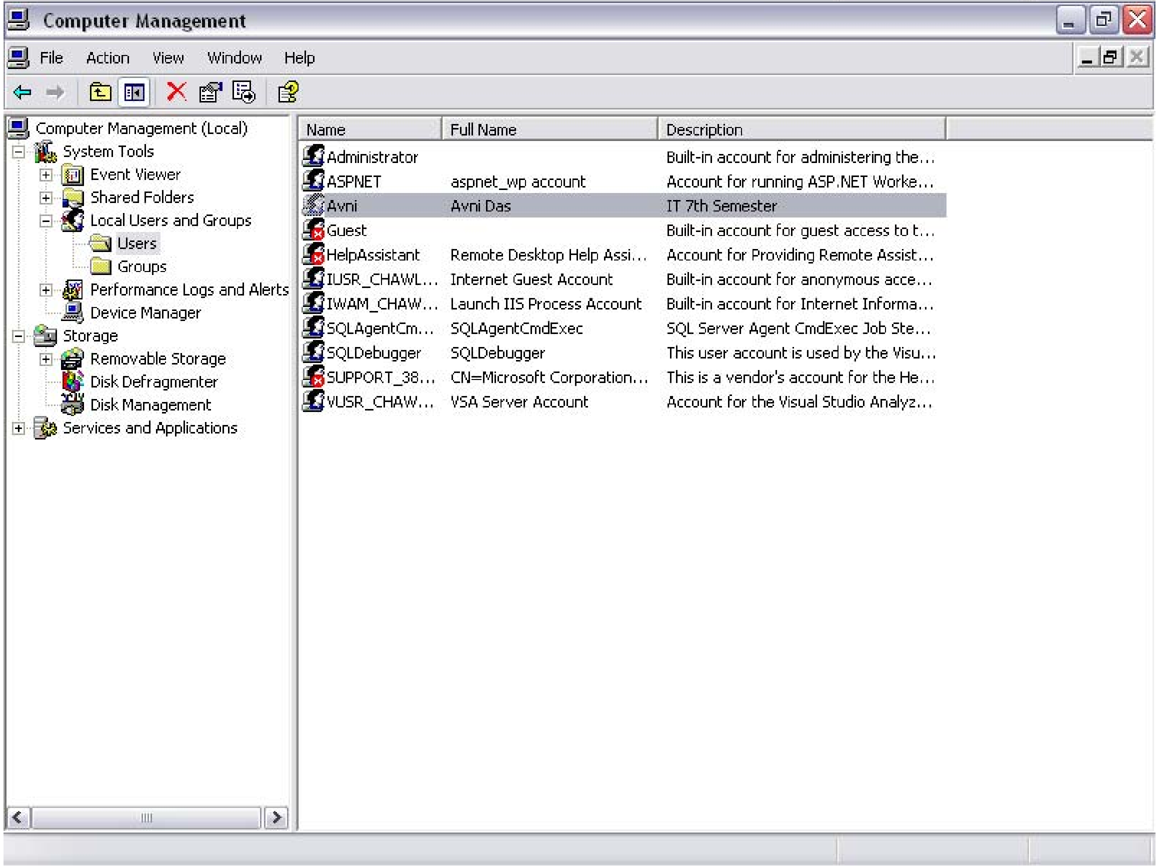
Days since last logon:

Name (RDN)	In Folder
Administrators	CHAWLA-CE59...
Backup Oper...	CHAWLA-CE59...
Debugger Us...	CHAWLA-CE59...
Guests	CHAWLA-CE59...
HelpServices...	CHAWLA-CE59...
Network Confi...	CHAWLA-CE59...
Power Users	CHAWLA-CE59...
Remote Desk...	CHAWLA-CE59...
Replicator	CHAWLA-CE59...
Users	CHAWLA-CE59...
VS Developers	CHAWLA-CE59...



Member of:

Administrators



Name	Full Name	Description
Administrator		Built-in account for administering the...
ASPNET	aspnet_wp account	Account for running ASP.NET Worke...
Avni	Avni Das	IT 7th Semester
Guest		Built-in account for guest access to t...
HelpAssistant	Remote Desktop Help Assi...	Account for Providing Remote Assist...
IUSR_CHAWL...	Internet Guest Account	Built-in account for anonymous acce...
IWAM_CHAW...	Launch IIS Process Account	Built-in account for Internet Informa...
SQLAgentCm...	SQLAgentCmdExec	SQL Server Agent CmdExec Job Ste...
SQLDebugger	SQLDebugger	This user account is used by the Visu...
SUPPORT_38...	CN=Microsoft Corporation...	This is a vendor's account for the He...
VUSR_CHAW...	VSA Server Account	Account for the Visual Studio Analyz...

- To open Computer Management, click **Start**, and then click **Control Panel**. Click **Performance and Maintenance**, click **Administrative Tools**, and then double-click **Computer Management**.
- A user name cannot be identical to any other user or group name on the computer being administered. It can contain up to 20 uppercase or lowercase characters except for the following:
  " / \ [ ] : ; | = , + * ? < >
  A user name cannot consist solely of periods (.) or spaces.
- In **Password** and **Confirm password**, you can type a password containing up to 127 characters. However, if you're using Windows 2000 or Windows XP on a network that also has computers using Windows 95 or Windows 98, consider using passwords not longer than 14 characters. Windows 95 and Windows 98 support passwords of up to 14 characters. If your password is longer, you may not be able to log on to your network from those computers.
- You should not add a new user to the Administrators group unless the user will perform only administrative tasks.

Practical 8.

SETTING UP OF TERMINAL SERVICES

Terminal Services overview

Terminal Services provides remote access to a Windows desktop through "thin client" software, allowing the client computer to serve as a terminal emulator. Terminal Services transmits only the user interface of the program to the client. The client then returns keyboard and mouse clicks to be processed by the server. Each user logs on and sees only their individual session, which is managed transparently by the server operating system and is independent of any other client session. Client software can run on a number of client hardware devices, including computers and Windows-based terminals. Other devices, such as Macintosh computers or UNIX-based workstations, can use additional third-party software to connect to a server running Terminal Server.

Remote Desktop for Administration (formerly known as Terminal Services in Remote Administration mode) provides remote access to the desktop of any computer running one of the Windows Server 2003 family operating systems, allowing you to administer your server—even a Microsoft® Windows 2000 server—from virtually any computer on your network.

Terminal Services benefits:

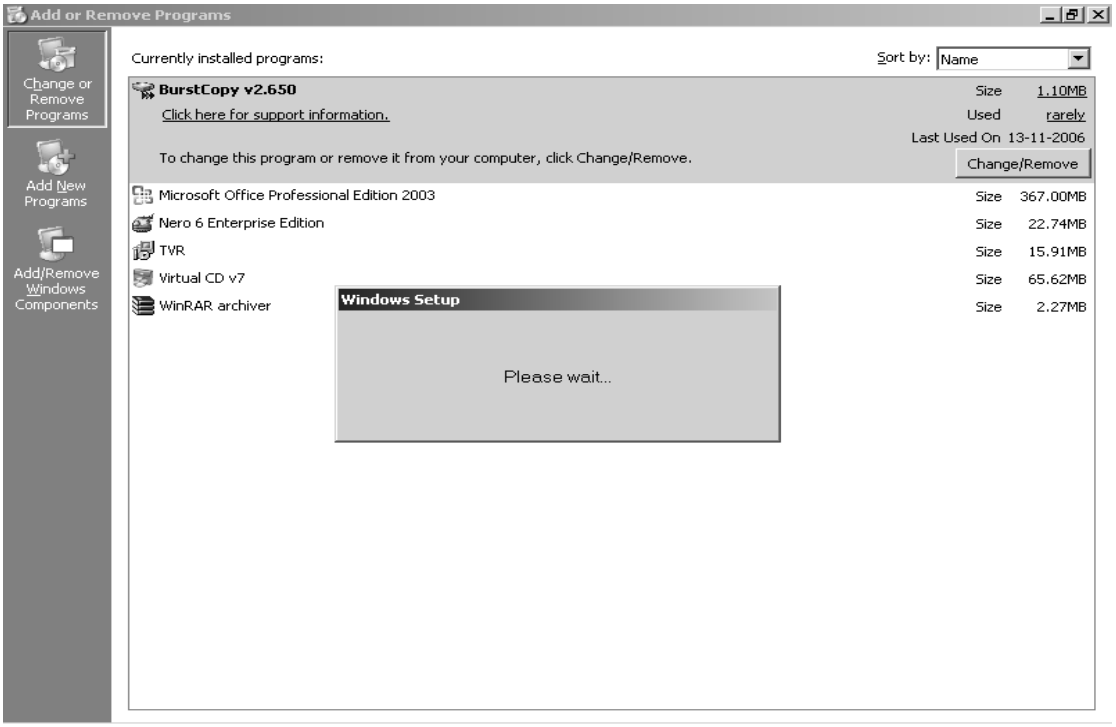
- **Brings Windows Server 2003 family operating systems to desktops faster.** Terminal Services helps bridge the gap while older desktops are migrated to Microsoft Microsoft® Windows® XP Professional, providing a virtual desktop experience of any Windows Server 2003 family operating system to computers that are running earlier versions of Windows.
- **Takes full advantage of existing hardware.** Terminal Services extends the model of distributed computing by allowing computers to operate as both thin clients and full-featured personal computers simultaneously. Computers can continue to be used as they have been within existing networks while also functioning as thin clients capable of emulating the Windows XP Professional desktop.

Requirements

Windows Server editio, NTFS (New Technology File System) partitioning, Number of Users at the time of installation.

Configuration of terminal services

1. Open the Control Panel.Then Go on Add/Remove Programs.



Currently installed programs:

BurstCopy v2.650 Size 1.10MB

Click here for support information. Used rarely

Last Used On 13-11-2006

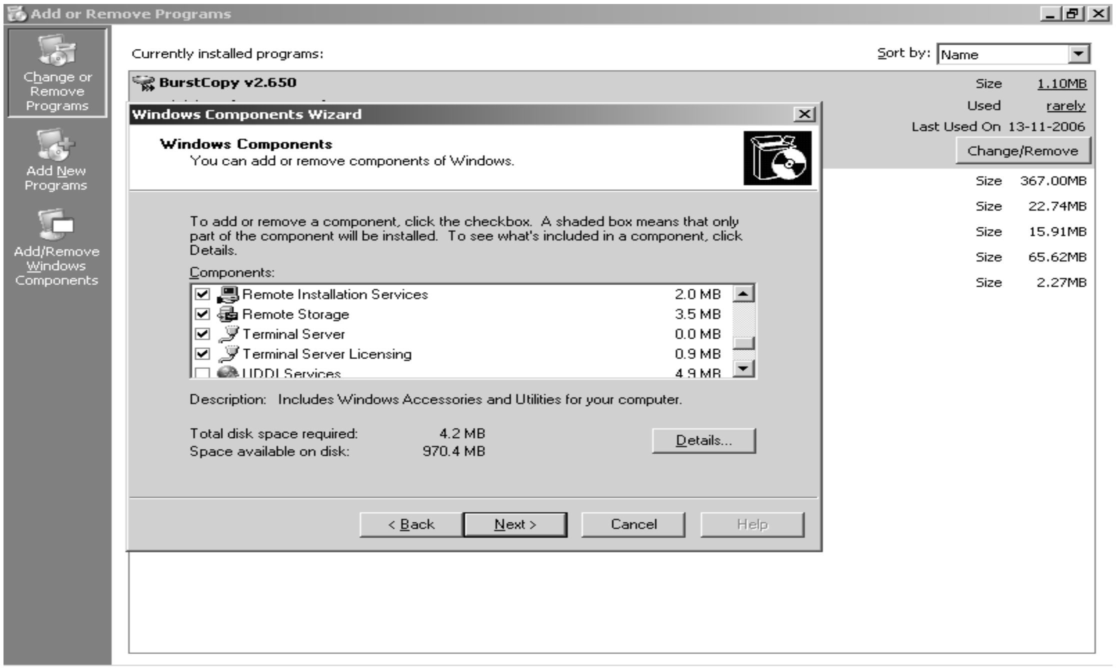
To change this program or remove it from your computer, click Change/Remove.

Microsoft Office Professional Edition 2003	Size	367.00MB
Nero 6 Enterprise Edition	Size	22.74MB
TVR	Size	15.91MB
Virtual CD v7	Size	65.62MB
WinRAR archiver	Size	2.27MB

Windows Setup

Please wait...

2. Click on Add/Remove Windows Components.Now check the four options Remote Installation, Remote Storage, Terminal Services, and Terminal Licensing.



Windows Components
You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

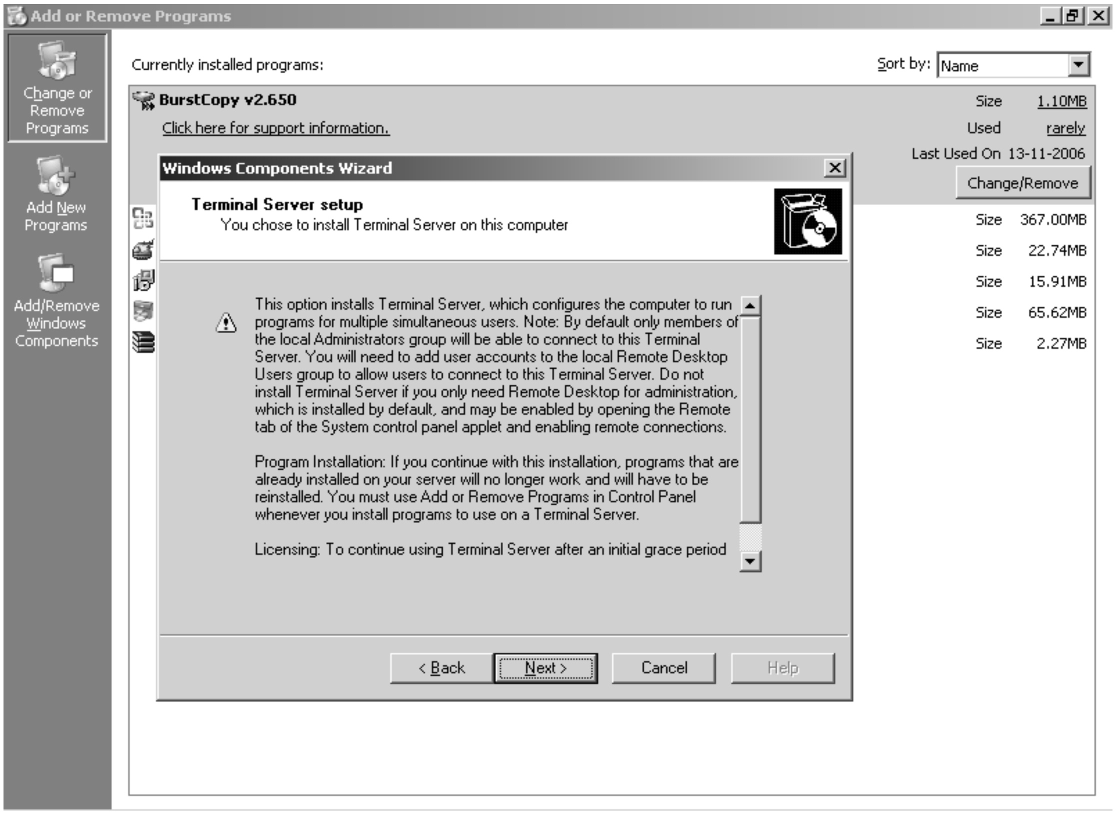
Components:

☑	Remote Installation Services	2.0 MB
☑	Remote Storage	3.5 MB
☑	Terminal Server	0.0 MB
☑	Terminal Server Licensing	0.9 MB
□	UDDI Services	4.9 MB

Description: Includes Windows Accessories and Utilities for your computer.

Total disk space required: 4.2 MB
Space available on disk: 970.4 MB

3. Now click on Next, the Windows Components Wizard get started, now Click on Next for Further installation.



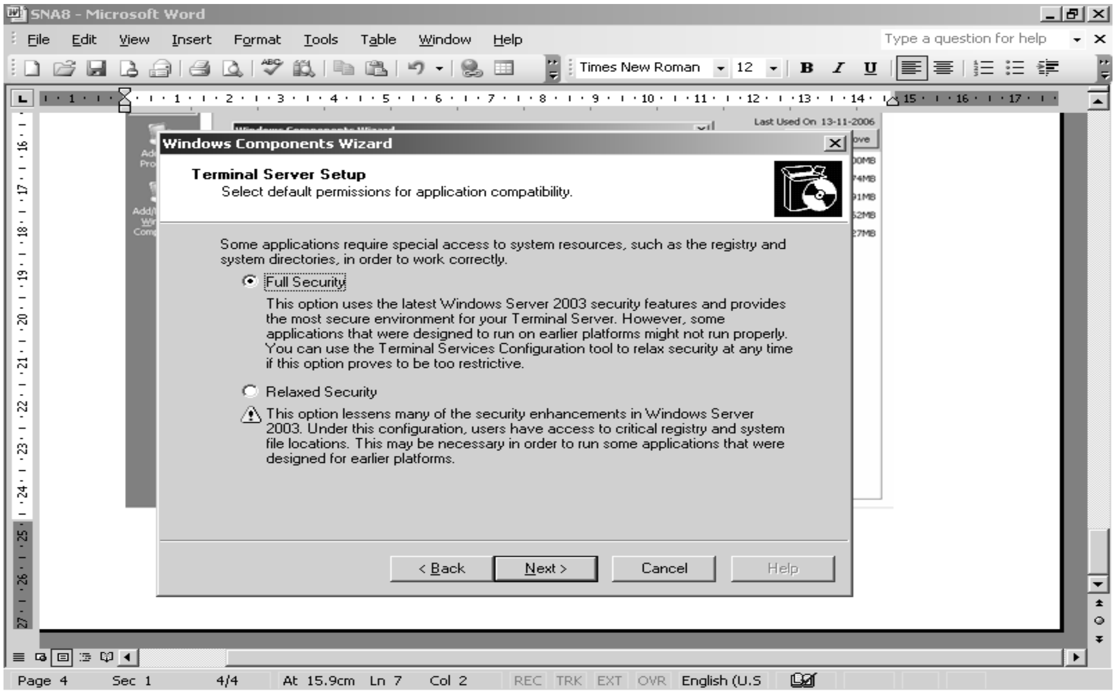
Terminal Server setup
You chose to install Terminal Server on this computer

This option installs Terminal Server, which configures the computer to run programs for multiple simultaneous users. Note: By default only members of the local Administrators group will be able to connect to this Terminal Server. You will need to add user accounts to the local Remote Desktop Users group to allow users to connect to this Terminal Server. Do not install Terminal Server if you only need Remote Desktop for administration, which is installed by default, and may be enabled by opening the Remote tab of the System control panel applet and enabling remote connections.

Program Installation: If you continue with this installation, programs that are already installed on your server will no longer work and will have to be reinstalled. You must use Add or Remove Programs in Control Panel whenever you install programs to use on a Terminal Server.

Licensing: To continue using Terminal Server after an initial grace period

4. Now you have to select the default permission for Applications Compatibility



SNA8 - Microsoft Word
File Edit View Insert Format Tools Table Window Help
Type a question for help
Times New Roman 12
Windows Components Wizard

Terminal Server Setup
Select default permissions for application compatibility.

Some applications require special access to system resources, such as the registry and system directories, in order to work correctly.

● Full Security

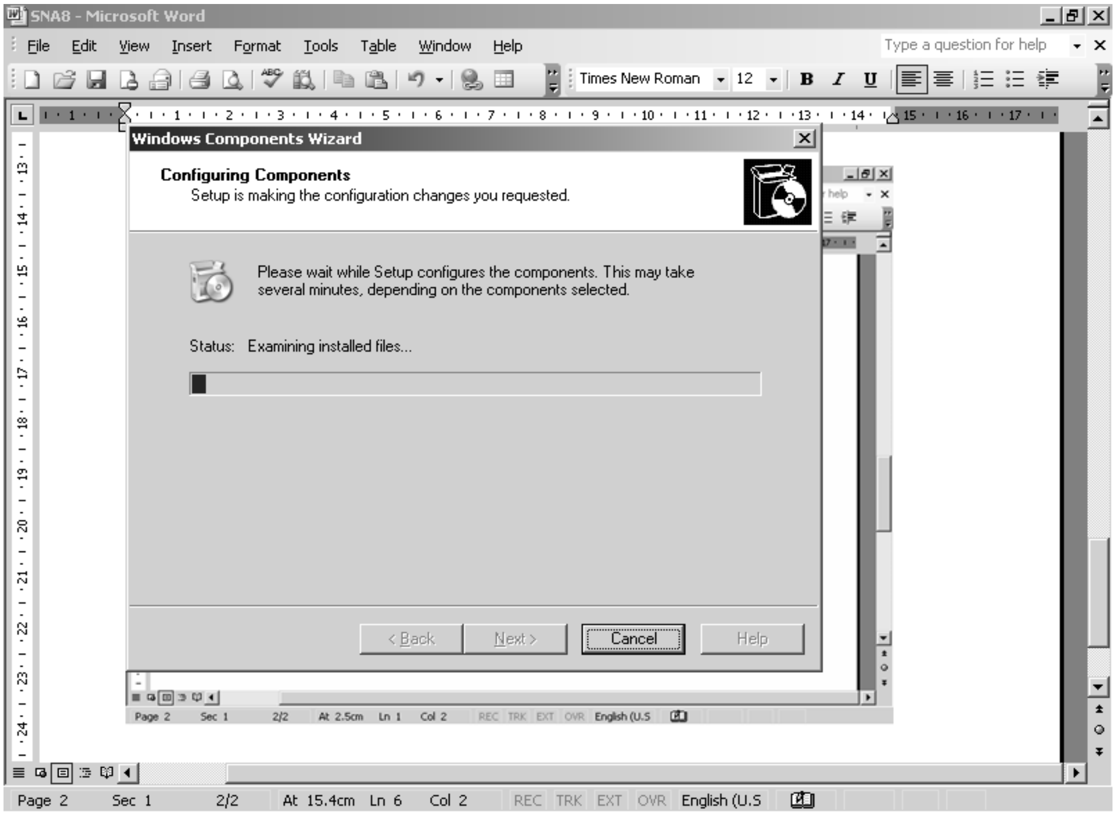
This option uses the latest Windows Server 2003 security features and provides the most secure environment for your Terminal Server. However, some applications that were designed to run on earlier platforms might not run properly. You can use the Terminal Services Configuration tool to relax security at any time if this option proves to be too restrictive.

○ Relaxed Security

This option lessens many of the security enhancements in Windows Server 2003. Under this configuration, users have access to critical registry and system file locations. This may be necessary in order to run some applications that were designed for earlier platforms.

< Back
Next >
Cancel
Help
Page 4 Sec 1 4/4 At 15.9cm Ln 7 Col 2 REC TRK EXT OVR English (U.S

4. Now, setup will start the configuration changes required for the Terminal Services.



SNA8 - Microsoft Word
File Edit View Insert Format Tools Table Window Help
Type a question for help
Times New Roman 12
Windows Components Wizard

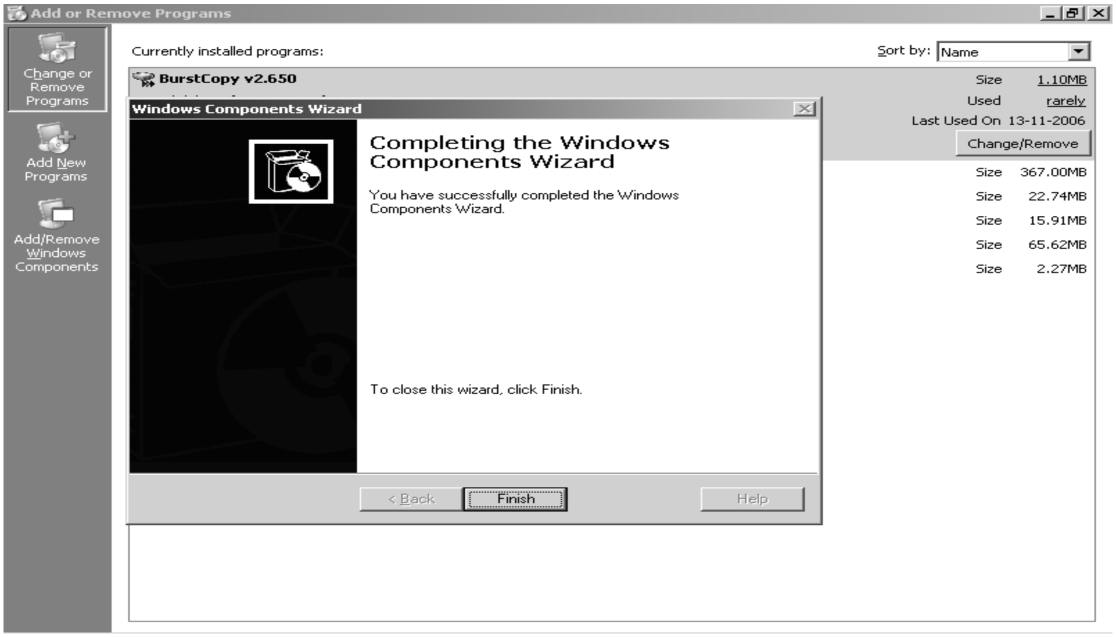
Configuring Components
Setup is making the configuration changes you requested.

Please wait while Setup configures the components. This may take several minutes, depending on the components selected.

Status: Examining installed files...

< Back
Next >
Cancel
Help
Page 2 Sec 1 2/2 At 15.4cm Ln 6 Col 2 REC TRK EXT OVR English (U.S

5. After this it asks for the Window 2003 server setup CD, to install all these components. Now click on Finish, it prompt for Restart the System.



Completing the Windows Components Wizard

You have successfully completed the Windows Components Wizard.

To close this wizard, click Finish.

6. Now on the Server all the Terminal services get installed, and is ready to use.

Remote Desktop for Administration

Remote Desktop for Administration (formerly known as Terminal Services in Remote Administration mode) provides remote access to the desktop of any computer running a Microsoft® Windows® Server 2003 family operating system, allowing you to administer your server from virtually any computer on your network.

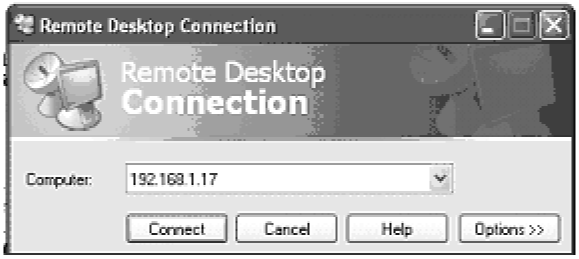
Remote Desktop Connection

With Remote Desktop Connection, you can easily connect to a terminal server or to any computer running Remote Desktop. All you need is network access and permissions to connect to the other computer. Optionally, you can specify special settings for your connection and then save the settings for the next time you connect.

To Create a New connection

Go to Start Menu→All Programs →Accessories→ Communications→Remote Desktop Connection. Open Remote Desktop Connection.In Computer, type a computer name or IP address. The computer can be a terminal server, or it can be a computer running Windows XP Professional or a Windows Server 2003 operating system that has Remote Desktop enabled and for which you have Remote Desktop permissions.

Click Connect.



Computer: 192.168.1.17

After Clicking on Connect The Log On to Windows dialog box appears.In the Log On to Windows dialog box, type your user name, password, and domain (if required), and then click OK.After this that terminal appears and you are ready to use that.

Practical 9.

USE OF THE NETWORK MONITOR

By using Network Monitor, you can gather information that helps you keep your network running smoothly, from identifying patterns to preventing or solving problems. Network Monitor provides information about the network traffic that flows to and from the network adapter of the computer on which it is installed. By capturing and analyzing that information, you can prevent, diagnose, and solve many types of network problems.

You can configure Network Monitor to provide specific types of information that are most relevant to you. For example, you can set up triggers so that Network Monitor starts or stops capturing information when a circumstance or set of circumstances arises. You can also set up filters to control what types of information Network Monitor captures or displays. To make analyzing the information easier, you can modify how information appears on the screen, and you can save or print the information for review at a later time.

The Network Monitor component that ships with Microsoft® Windows® Server 2003 family operating systems can capture frames that are sent to or from the computer on which Network Monitor is installed. If you want to capture frames that are sent to or from a remote computer, you must use the Network Monitor component that ships with Microsoft Systems Management Server, which can capture frames sent to or from any computer on which the Network Monitor driver is installed.

The information that Network Monitor provides comes from the network traffic itself, which is divided into frames. These frames contain information such as the address of the computer that sent the frame, the address of the computer to which the frame was sent, and the protocols that exist within the frame.

How Network Monitor works

Data sent over a network is divided into frames. Each frame contains the following information:

- **Source address** The address of the network adapter from which the frame originated.
- **Destination address** The address of the network adapter that is meant to receive the frame. This address can also specify a group of network adapters.
- **Header information** Information specific to each protocol used to send the frame.
- **Data** The information (or a portion of it) being sent.

Every computer on a network segment receives frames transmitted on that segment. The network adapter in each computer retains and processes only those frames that are addressed to that adapter. The rest of the frames are dropped and no longer processed. The network adapter also retains broadcast (and potentially multicast) frames.

After installing Network Monitor, users can capture to a file all the frames sent to, or retained by, the network adapter of the computer on which it is installed. These captured frames can then be viewed or saved for later analysis. Users can design a capture filter so that only certain frames are captured. This filter can be configured to capture frames based on criteria such as source address, destination address, or protocol. Network Monitor also makes it possible for a user to design a capture trigger to initiate a specified action when Network Monitor detects a particular set of conditions on the network. This action can include starting a capture, ending a capture, or starting a program.

By default, the size of the capture buffer is 1 MB. You can reduce the amount of data you capture by shrinking the capture buffer.

The Capture Process

The process by which Network Monitor copies frames is referred to as capturing. You can capture all network traffic to and from the local network adapter, or you can set a capture filter and capture a subset of frames. You can also specify a set of conditions that trigger an event. If you create triggers, Network Monitor can respond to events on your network. For example, you can make the operating system start an executable file when Network Monitor detects a particular set of conditions on the network. After you have captured data, you can view it. Network Monitor translates the raw capture data into its logical frame structure.

While Network Monitor captures frames from the network, statistics about the frames appear in the Capture window, which has four panes:

Pane	**Displays**
Graph	A graphical representation of frames sent to or from the local computer.
Session Statistics	Statistics about current individual sessions.
Station Statistics	Statistics about frames sent to or from the computer running Network Monitor.
Total Statistics	Summary statistics about frames sent to or from the local computer since the capture process began.

Network Monitor uses the Network Driver Interface Specification (NDIS) facility to copy all frames it detects to its capture buffer.

Capture window: Graph pane

The Graph pane graphically represents the total capture statistics of the current capture data. This pane appears in the upper-left corner of the Capture window, and it is on by default.

% Network Utilization

The percentage of your network adapter's capacity that the current capture uses. This percentage is calculated by dividing the rate at which your adapter is sending and receiving frames by the maximum rate at which your adapter can process those frames.

Frames Per Second

The number of frames that the adapter is capturing every second.

Bytes Per Second

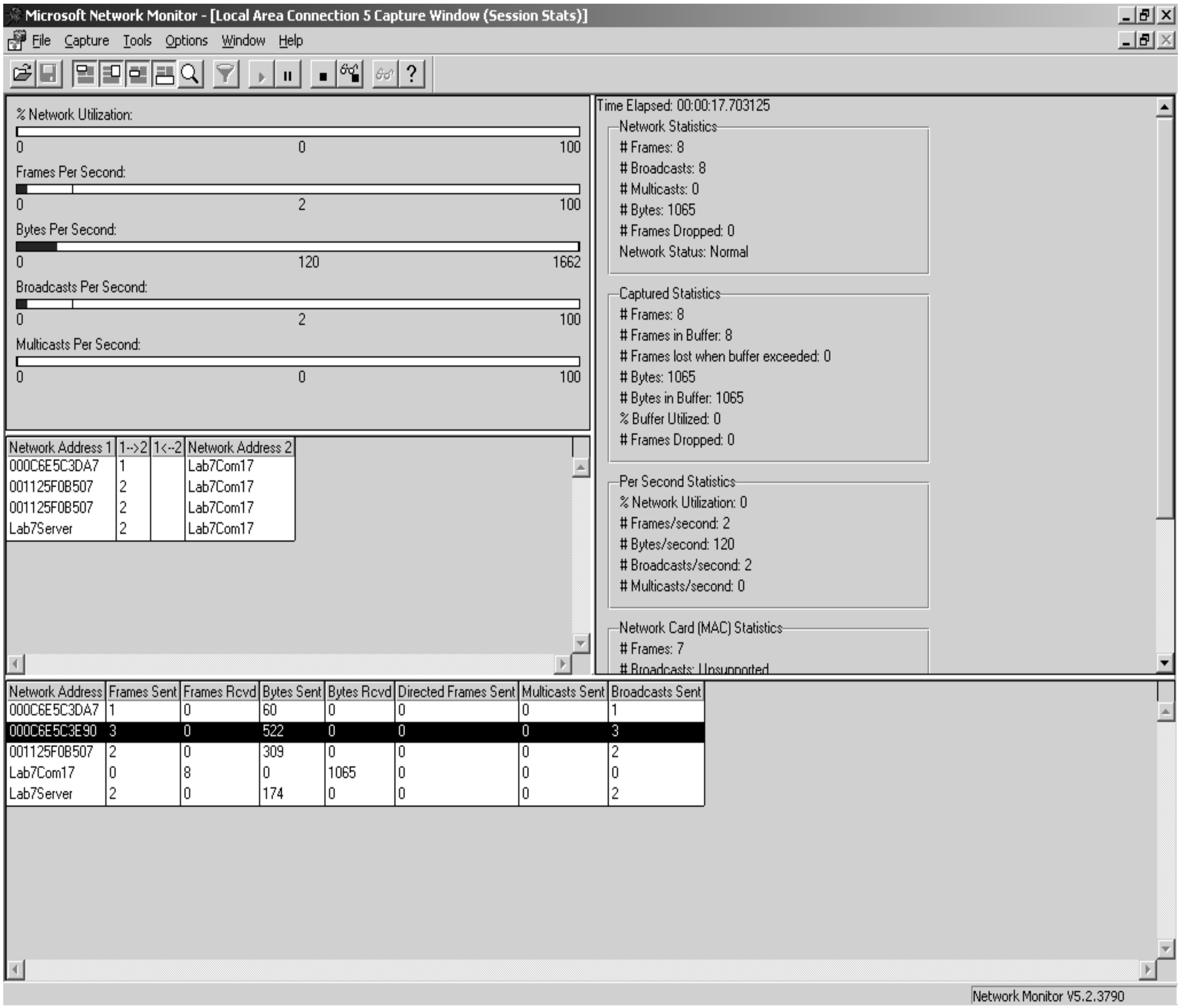
The number of bytes that the adapter is capturing every second.

Broadcasts Per Second

The number of broadcasts that the adapter is capturing every second.

Multicasts Per Second

The number of multicasts that the adapter is capturing every second.


Microsoft Network Monitor - [Local Area Connection 5 Capture Window (Session Stats)]
File
Capture
Tools
Options
Window
Help
Network Monitor V5.2.3790

% Network Utilization:
0 0 100

Frames Per Second:
0 2 100

Bytes Per Second:
0 120 1662

Broadcasts Per Second:
0 2 100

Multicasts Per Second:
0 0 100

Network Address 1	1-->2	1<--2	Network Address 2
000C6E5C3DA7	1		Lab7Com17
001125F0B507	2		Lab7Com17
001125F0B507	2		Lab7Com17
Lab7Server	2		Lab7Com17

Time Elapsed: 00:00:17.703125

Network Statistics
Frames: 8
Broadcasts: 8
Multicasts: 0
Bytes: 1065
Frames Dropped: 0
Network Status: Normal

Captured Statistics
Frames: 8
Frames in Buffer: 8
Frames lost when buffer exceeded: 0
Bytes: 1065
Bytes in Buffer: 1065
% Buffer Utilized: 0
Frames Dropped: 0

Per Second Statistics
% Network Utilization: 0
Frames/second: 2
Bytes/second: 120
Broadcasts/second: 2
Multicasts/second: 0

Network Card (MAC) Statistics
Frames: 7
Broadcasts: Unsupported

Network Address	Frames Sent	Frames Rcvd	Bytes Sent	Bytes Rcvd	Directed Frames Sent	Multicasts Sent	Broadcasts Sent
000C6E5C3DA7	1	0	60	0	0	0	1
000C6E5C3E90	3	0	522	0	0	0	3
001125F0B507	2	0	309	0	0	0	2
Lab7Com17	0	8	0	1065	0	0	0
Lab7Server	2	0	174	0	0	0	2

Capture window: Session Statistics pane

A session designates the data that is sent to or from the local computer. The Session Statistics pane displays statistics on a per-session basis. The pane also identifies both participants in a session and displays how much information passed in either direction between them.

This pane appears in the left-center portion of the Capture window, and it is on by default.

Network Address 1

The network address of the first participant in a network session.

1 --> 2

The number of frames sent from the address listed in the **Network Address 1** column to the address listed in the **Network Address 2** column.

1 <-- 2

The number of frames sent from the address listed in the **Network Address 2** column to the address listed in the **Network Address 1** column.

Network Address 2

The network address of the second participant in a network session.

Note

- Network Monitor reflects session statistics of only the first 100 unique addresses that it detects. To gather statistics on a specific workstation, design a capture filter. To reset statistics and view information about the next 100 detected network sessions, click the **Capture** menu, and then click **Clear Statistics**.

Capture window: Station Statistics pane

The Station Statistics pane displays statistics that describe the network activity of your workstation. This pane appears at the bottom of the Capture window, and it is on by default.

Network Address

The network address of the computer on which the frames were captured.

Frames Sent

The number of frames sent from the address listed in the **Network Address** column.

Frames Rcvd

The number of frames received by the address listed in the **Network Address** column.

Bytes Sent

The number of bytes sent by the address listed in the **Network Address** column.

Bytes Rcvd

The number of bytes received by the address listed in the **Network Address** column.

Directed Frames Sent

The number of non-broadcast, non-multicast frames transferred over the network from the associated address.

Multicasts Sent

The number of times the address listed in the **Network Address** column has sent frames to a subset of computers on the network, by sending "FFFFFFFFFFFF."

Broadcasts Sent

The number of times that the address listed in the **Network Address** column has sent frames to all computers on the network.

Note: Network Monitor reflects station statistics of only the first 128 unique addresses that it detects. To gather statistics on a specific workstation, design a capture filter.

Capture window: Total Statistics pane

The Total Statistics pane provides an overall view of network traffic sent to or from the local computer. This pane appears in the upper-right corner of the Capture window, and it is on by default.

Network Statistics

The total amount of traffic that has been sent to or from the local computer since the current capture began. These statistics include:

- The total number of frames sent to or from the local computer.
- The total number of broadcasts sent to or from the local computer.
- The total number of multicasts sent to or from the local computer.
- The total number of bytes sent to or from the local computer.
- The total number of frames dropped.
- The network status. On an Ethernet network, this entry will always be **Normal**. On a token ring network, this entry reflects whether the token is present locally.

Captured Statistics

Total statistics that describe the current capture, including:

- The total number of captured frames.
- The total number of frames in the temporary capture file.
- The number of frames dropped when the buffer was exceeded.
- The total number of captured bytes.
- The total number of bytes in the temporary capture file.
- The percentage of allotted buffer space that is in use.
- The number of frames dropped by Network Monitor.

Per Second Statistics

Statistical averages of current activity and continual updates of this average to reflect current per-second activity. The statistics in this panel include all frames (even frames that were excluded by a capture filter). Per-second statistics include:

- The average number of frames per second detected since the capture began.
- The average number of bytes per second detected since the capture began.
- The average number of broadcast messages per second detected since the capture began.
- The average number of multicast messages per second detected since the capture began.
- The percentage of network utilization. This statistic shows the percentage of your network adapter's capacity that the current

capture uses. This percentage is calculated by dividing the rate at which your adapter is sending and receiving frames by the maximum rate at which your adapter can process those frames.

Network Card (MAC) Statistics

Statistics that reflect average activity detected by your network adapter since the current capture began. The statistics in this pane reflect all the network activity that your network adapter can receive. These statistics include:

- Total frames detected by the network adapter.
- Total broadcast frames detected by the network adapter.
- Total multicast frames detected by the network adapter.
- Total bytes detected by the network adapter.

Network Card (MAC) Error Statistics

Statistics that reflect adapter-related errors that have occurred since the capture began. These statistics include:

- Number of errors that occurred because the cyclical redundancy check (CRC) did not match the actual bytes received.
- Number of frames that the network adapter detected but that were dropped because Network Monitor lacked sufficient buffer space.
- Number of frames that the network adapter detected but that were dropped because of hardware constraints.

Capture filters

A capture filter functions like a database query that you can use to specify the types of network information you want to monitor. For example, to see only a specific subset of computers or protocols, you can create an address database, use the database to add addresses to your filter, and then save the filter to a file. By filtering frames, you save both buffer resources and time. Later, if necessary, you can load the capture filter file and use the filter again.

Designing a capture filter

To design a capture filter, specify decision statements in the **Capture Filter** dialog box. This dialog box displays the filter's decision tree, which is a graphical representation of a filter's logic. When you include or exclude information from your capture specifications, the decision tree reflects these specifications.

Filtering by protocol

To capture frames sent using a specific protocol, specify the protocol on the **SAP/ETYPE=** line of the capture filter. For example, to capture only IP frames, disable all protocols and then enable **IP ETYPE 0x800** and **IP SAP 0x6**. By default, all of the protocols that Network Monitor supports are enabled. You can only specify protocols with ETYPE or SAP.

Filtering by address

To capture frames sent from a specific computer on your network to your computer or sent from your computer to a specific computer on your network, specify one or more address pairs in a capture filter. You can monitor up to four address pairs simultaneously.

An address pair consists of:

- The addresses of the two computers you want to monitor traffic between.
- Arrows that specify the traffic direction you want to monitor.
- The INCLUDE or EXCLUDE keyword, indicating how Network Monitor should respond to a frame that meets a filter's specifications.

Regardless of the sequence in which statements appear in the **Capture Filter** dialog box, EXCLUDE statements are evaluated first. Therefore, if a frame meets the criteria specified in an EXCLUDE statement in a filter containing both an EXCLUDE and INCLUDE statement, that frame is discarded. Network Monitor does not test that frame by INCLUDE statements to see if it meets that criterion also.

For example, to capture all the traffic from Joe's computer *except* the traffic from Joe to Anne, use the following capture filter address section:

Addresses

include Joe <----> Any

exclude Joe <----> Anne

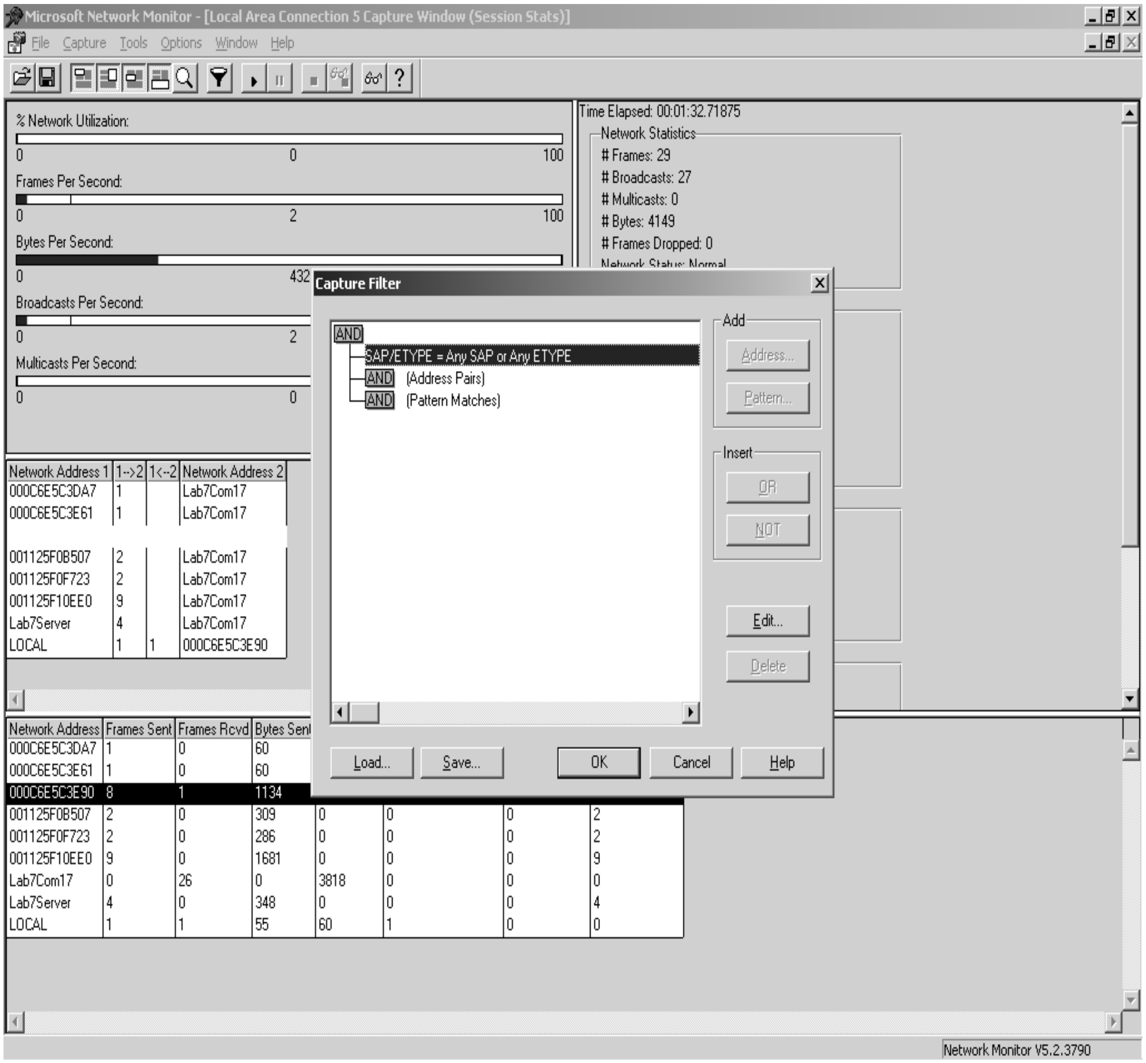
If there are no INCLUDE lines, *YourComputer* <----> Any is used implicitly.

Filtering by data pattern

By specifying a pattern match in a capture filter, you can:

- Limit a capture to only those frames containing a specific pattern of ASCII or hexadecimal data.
- Specify how many bytes (offsets) of the frame must be ignored before the search begins.

When you filter based on a pattern match, you must specify where, in the frame, the search for the pattern should begin. This setting specifies, in bytes, the distance from the beginning of the frame or the end of the topology header to the point at which the pattern might occur. If your network medium has a variable size in the media access control protocol, such as Ethernet or token ring, specify to count from the end of the topology header.



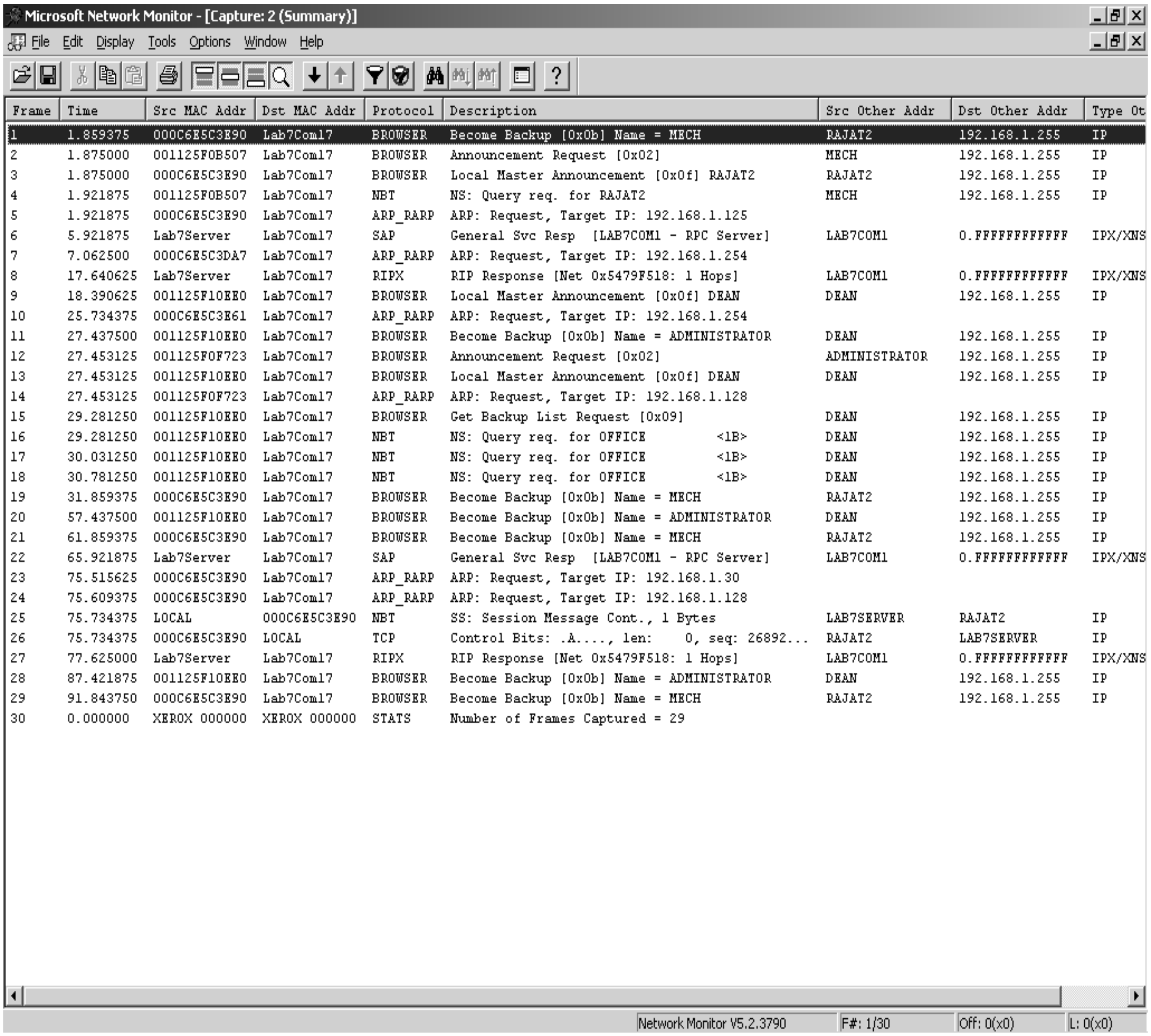
Time Elapsed: 00:01:32.71875

Network Statistics
Frames: 29
Broadcasts: 27
Multicasts: 0
Bytes: 4149
Frames Dropped: 0
Network Status: Normal

```
AND
 ├─SAP/ETYPE = Any SAP or Any ETYPE
 ├─AND  (Address Pairs)
 └─AND  (Pattern Matches)
```

Network Address 1	1-->2	1<--2	Network Address 2
000C6E5C3DA7	1		Lab7Com17
000C6E5C3E61	1		Lab7Com17
001125F0B507	2		Lab7Com17
001125F0F723	2		Lab7Com17
001125F10EE0	9		Lab7Com17
Lab7Server	4		Lab7Com17
LOCAL	1	1	000C6E5C3E90

Network Address	Frames Sent	Frames Rcvd	Bytes Sent				
000C6E5C3DA7	1	0	60				
000C6E5C3E61	1	0	60				
000C6E5C3E90	8	1	1134				
001125F0B507	2	0	309	0	0	0	2
001125F0F723	2	0	286	0	0	0	2
001125F10EE0	9	0	1681	0	0	0	9
Lab7Com17	0	26	0	3818	0	0	0
Lab7Server	4	0	348	0	0	0	4
LOCAL	1	1	55	60	1	0	0



Microsoft Network Monitor - [Capture: 2 (Summary)]
File
Edit
Display
Tools
Options
Window
Help
?
Network Monitor V5.2.3790
F#: 1/30
Off: 0(x0)
L: 0(x0)

Frame	Time	Src MAC Addr	Dst MAC Addr	Protocol	Description	Src Other Addr	Dst Other Addr	Type Ot
1	1.859375	000C6E5C3E90	Lab7Com17	BROWSER	Become Backup [0x0b] Name = MECH	RAJAT2	192.168.1.255	IP
2	1.875000	001125F0B507	Lab7Com17	BROWSER	Announcement Request [0x02]	MECH	192.168.1.255	IP
3	1.875000	000C6E5C3E90	Lab7Com17	BROWSER	Local Master Announcement [0x0f] RAJAT2	RAJAT2	192.168.1.255	IP
4	1.921875	001125F0B507	Lab7Com17	NBT	NS: Query req. for RAJAT2	MECH	192.168.1.255	IP
5	1.921875	000C6E5C3E90	Lab7Com17	ARP_RARP	ARP: Request, Target IP: 192.168.1.125			
6	5.921875	Lab7Server	Lab7Com17	SAP	General Svc Resp [LAB7COM1 - RPC Server]	LAB7COM1	0.FFFFFFFFFFFF	IPX/XNS
7	7.062500	000C6E5C3DA7	Lab7Com17	ARP_RARP	ARP: Request, Target IP: 192.168.1.254			
8	17.640625	Lab7Server	Lab7Com17	RIPX	RIP Response [Net 0x5479F518: 1 Hops]	LAB7COM1	0.FFFFFFFFFFFF	IPX/XNS
9	18.390625	001125F10EE0	Lab7Com17	BROWSER	Local Master Announcement [0x0f] DEAN	DEAN	192.168.1.255	IP
10	25.734375	000C6E5C3E61	Lab7Com17	ARP_RARP	ARP: Request, Target IP: 192.168.1.254			
11	27.437500	001125F10EE0	Lab7Com17	BROWSER	Become Backup [0x0b] Name = ADMINISTRATOR	DEAN	192.168.1.255	IP
12	27.453125	001125F0F723	Lab7Com17	BROWSER	Announcement Request [0x02]	ADMINISTRATOR	192.168.1.255	IP
13	27.453125	001125F10EE0	Lab7Com17	BROWSER	Local Master Announcement [0x0f] DEAN	DEAN	192.168.1.255	IP
14	27.453125	001125F0F723	Lab7Com17	ARP_RARP	ARP: Request, Target IP: 192.168.1.128			
15	29.281250	001125F10EE0	Lab7Com17	BROWSER	Get Backup List Request [0x09]	DEAN	192.168.1.255	IP
16	29.281250	001125F10EE0	Lab7Com17	NBT	NS: Query req. for OFFICE <1B>	DEAN	192.168.1.255	IP
17	30.031250	001125F10EE0	Lab7Com17	NBT	NS: Query req. for OFFICE <1B>	DEAN	192.168.1.255	IP
18	30.781250	001125F10EE0	Lab7Com17	NBT	NS: Query req. for OFFICE <1B>	DEAN	192.168.1.255	IP
19	31.859375	000C6E5C3E90	Lab7Com17	BROWSER	Become Backup [0x0b] Name = MECH	RAJAT2	192.168.1.255	IP
20	57.437500	001125F10EE0	Lab7Com17	BROWSER	Become Backup [0x0b] Name = ADMINISTRATOR	DEAN	192.168.1.255	IP
21	61.859375	000C6E5C3E90	Lab7Com17	BROWSER	Become Backup [0x0b] Name = MECH	RAJAT2	192.168.1.255	IP
22	65.921875	Lab7Server	Lab7Com17	SAP	General Svc Resp [LAB7COM1 - RPC Server]	LAB7COM1	0.FFFFFFFFFFFF	IPX/XNS
23	75.515625	000C6E5C3E90	Lab7Com17	ARP_RARP	ARP: Request, Target IP: 192.168.1.30			
24	75.609375	000C6E5C3E90	Lab7Com17	ARP_RARP	ARP: Request, Target IP: 192.168.1.128			
25	75.734375	LOCAL	000C6E5C3E90	NBT	SS: Session Message Cont., 1 Bytes	LAB7SERVER	RAJAT2	IP
26	75.734375	000C6E5C3E90	LOCAL	TCP	Control Bits: .A...., len: 0, seq: 26892...	RAJAT2	LAB7SERVER	IP
27	77.625000	Lab7Server	Lab7Com17	RIPX	RIP Response [Net 0x5479F518: 1 Hops]	LAB7COM1	0.FFFFFFFFFFFF	IPX/XNS
28	87.421875	001125F10EE0	Lab7Com17	BROWSER	Become Backup [0x0b] Name = ADMINISTRATOR	DEAN	192.168.1.255	IP
29	91.843750	000C6E5C3E90	Lab7Com17	BROWSER	Become Backup [0x0b] Name = MECH	RAJAT2	192.168.1.255	IP
30	0.000000	XEROX 000000	XEROX 000000	STATS	Number of Frames Captured = 29			

Practical 10.

SETTING UP OF DHCP

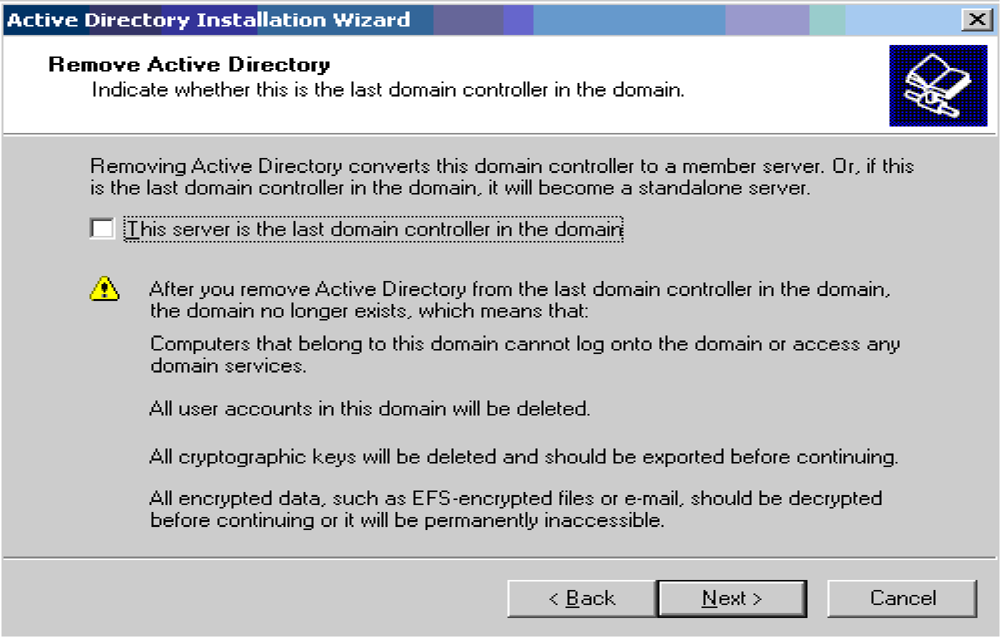
The Dynamic Host Configuration Protocol (DHCP) automates the assignment of IP addresses, subnet masks, default routers, and other IP parameters. The assignment usually occurs when the DHCP configured machine boots up or regains connectivity to the network. The DHCP client sends out a query requesting a response from a DHCP server on the locally attached network. The query is typically initiated immediately after booting up and before the client initiates any IP based communication with other hosts. The DHCP server then replies to the client with its assigned IP address, subnet mask, DNS server and default gateway information.

The assignment of the IP address usually expires after a predetermined period of time, at which point the DHCP client and server renegotiate a new IP address from the server's predefined pool of addresses. Configuring firewall rules to accommodate access from machines who receive their IP addresses via DHCP is therefore more difficult because the remote IP address will vary from time to time. Administrators must usually allow access to the entire remote DHCP subnet for a particular TCP/UDP port.

Most home routers and firewalls are configured in the factory to be DHCP servers for a home network. An alternative to a home router is to use a computer as a DHCP server. ISPs generally use DHCP to assign clients individual IP addresses.

DHCP is a broadcast-based protocol. As with other types of broadcast traffic, it does not cross a router unless specifically configured to do so. Users who desire this capability must configure their routers to pass DHCP traffic across UDP ports 67 and 68.

Before we can use the DHCP, we need to install the active directory and DNS.



Remove Active Directory

Indicate whether this is the last domain controller in the domain.

Removing Active Directory converts this domain controller to a member server. Or, if this is the last domain controller in the domain, it will become a standalone server.

□ This server is the last domain controller in the domain

After you remove Active Directory from the last domain controller in the domain, the domain no longer exists, which means that:

Computers that belong to this domain cannot log onto the domain or access any domain services.

All user accounts in this domain will be deleted.

All cryptographic keys will be deleted and should be exported before continuing.

All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.

The following steps are carried out for installing active directory

1. In the run command type ‘dcpromo’, click OK, an installation wizard opens.

2. In the wizard enter you domain name and type. Your type of domain may be either
   a. Forest Domain
   b. Child Domain
   c. Tree Domain

3. Enter your domain name

4. Select domain or workgroup, here we select domain

   Deciding Between Workgroups and Domains

   A *domain* is a grouping of accounts and network resources under a single domain name and security boundary. A *workgroup* is a more basic grouping, intended only to help users find objects such as printers and shared folders within that group. Domains are the recommended choice for all networks except very small ones with few users.

   In a workgroup, users might have to remember multiple passwords, one for each network resource. (In addition, different users can use different passwords for each resource.) In a domain, passwords and permissions are simpler to keep track of, since a domain has a single, centralized database of user accounts, permissions, and other network details. The information in this database is replicated automatically among domain controllers. You determine which servers are domain controllers and which are simply members of the domain. You can determine these roles not only during Setup but afterward.

Domains, and the Active Directory directory system of which they are a part, provide many options for making resources easily available to users while maintaining good monitoring and security.

5. In the control panel select ‘Add or Remove Programs’, select ‘Networking Services’, click on details and select all the options.
6. The next window that opens, enter your domain name, here we have our domain name ‘Lab7server.com’
7. The active directory is now being installed and the DNS is also configured, this takes about 20 minutes to install.

DHCP Requirements

The following requirements need to be met by the **DHCP server:**

- The DHCP server service is running on a Windows NT Server on at least one computer within the TCP/IP internetwork.
- A DHCP scope exists on the DHCP server.
  A DHCP scope consists of a pool of IP addresses the DHCP server can assign or lease to DHCP clients. For example:
  192.168.1.25 through 192.168.1.25
  where xxx is any valid number for the first octet of the IP address.

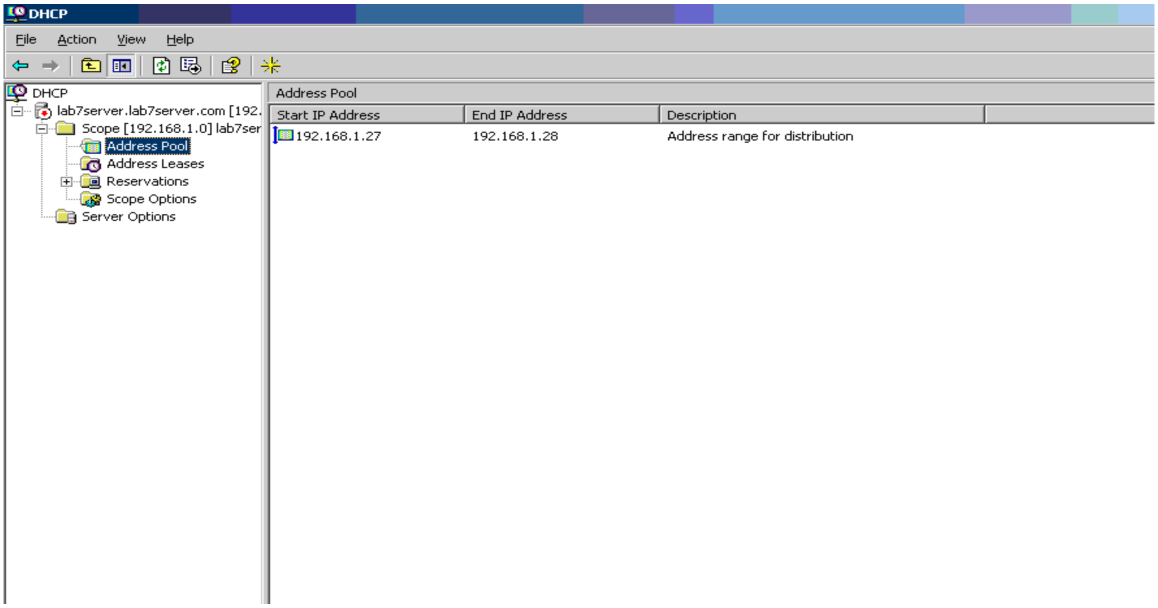
The following requirements need to be met by the **DHCP client:**

- The client computer has a DHCP supported operating system. The following operating systems are capable of being a DHCP client with DHCP enabled at the client:
  - Windows NT Server 3.5, 3.51, and 4.0
  - Windows NT Workstation 3.5, 3.51, and 4.0
  - Windows 95
  - Windows for Workgroups 3.11 with the Microsoft TCP/IP-32 for Windows for Workgroups installed
  - MS Network Client 3.0 for MS-DOS with the real mode TCP/IP driver installed
  - LAN Manager 2.2c

Start Using DHCP

ON THE SERVER

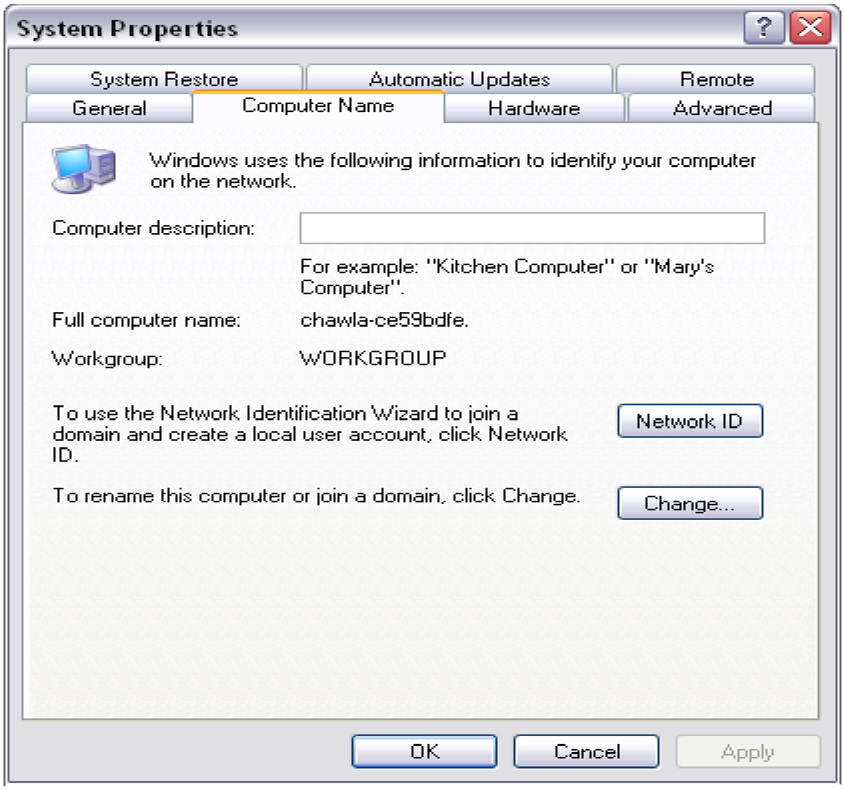
1. Goto the control panel, select administrative tools, select DHCP.
2. Click on the left hand side list on the domain name ‘Lab7server.com
3. Right click on the scope properties, select address pool.
4. Enter the scope name
5. Enter the starting IP address and the ending IP address for the network.



Start IP Address	End IP Address	Description
192.168.1.27	192.168.1.28	Address range for distribution

ON THE CLIENT SIDE

1. Right click on ‘My Computer’
2. Select Properties
3. Enter the computer Name
4. Select Change



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: chawla-ce59bdfe.

Workgroup: WORKGROUP

To use the Network Identification Wizard to join a domain and create a local user account, click Network ID.

To rename this computer or join a domain, click Change.

REFERENCES

- “Principles of Network and System Administration”, Mark Burgess, 2000, John Wiley and Sons Ltd,
- “TCP/IP Network Administration” (3rd Edition), Craig Hunt, O’Reilly and Associates Inc., 2002.
- “Windows 2000 Administration”, George Splading, 2000, McGraw-Hill.
- “Linux Network Administrator’s Guide”, Olaf Kirch and Terry Dawson, (2nd Edition), O’Reilly and Associates Inc., 2000, (Shroff Publishers and Distributors, Culcutta),

NEW IDEAS/EXPERIMENTS FOR RESPECTIVE LAB BESIDES UNIVERSITY SYLLABUS

In this lab we can have some more practicals on new technologies in the field of network administration. Few of them are as follows:

1. Installation & configuration of Windows 2003 server.
2. Setting up of Remote Access Server (RAS) for remote login.
3. How to apply IPSec Policies.
4. How to apply group policies.
5. How to implement FIREWALLS.

FAQs

1. Which command is used to resolve IP address to host name.
2. What is the difference between tracert & pathping command.
3. Which command is used to display physical address of the system.
4. Which command displays the routing table.
5. What is INFORMATION event.
6. How to overwrite an event in event viewer.
7. How to start a service from command prompt.
8. What is SC .
9. What is the minimum length of password in DOMAIN.
10. How we can secure password in DOMAIN.
11. What is the difference between HUB & SWITCH.
12. Which class of IP addresses is used for LAN.
13. What is difference between CROSS cable and STRAIGHT cable.
14. What is the range of CAT-5 cables.
15. How to assign IP addresses in LAN.
16. How to add performance object in system monitor.
17. How to create an ADMINISTRATOR account in DOMAIN.
18. What is the difference between FAT32 & NTFS.
19. Difference between Rlogin & TELNET.
20. Difference between Terminal service and Remote Access.
21. How to capture data transmission between to particular systems on network through network monitor.
22. Why do we use DHCP to allocate IP addresses.
23. What is the difference between workgroup and domain.
24. Why do we install DNS before DHCP installation.
25. Do we need to make any changes on client side for DHCP.